Deploying Avaya Oceana® Solution

Release 3.6.1
Issue 1.2
October 2019

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: 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 You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

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

Hosted Service

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

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

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

Heritage Nortel Software

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

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER’S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

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

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

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: 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 Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: 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

Contents

Chapter 1: Introduction

Purpose

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

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

Change history

Issue	Date	Summary of changes
1.2	October 29, 2019	Updates to Creating Avaya Oceana® Cluster 3 on page 75.
1.1	July 25, 2019	Minor updates to Planning and preconfiguration on page 29.

Changes in this release

Avaya Oceana® Solution Release 3.6.1 includes the following changes:

Support for Callback Assist

Avaya Oceana® Solution provides the callback functionality. If Avaya Oceana® Solution does not find an available agent during a voice call, the caller is presented with the option to leave a voicemail or request a callback. If the caller selects the callback option, the caller is dropped from the call and Callback Assist makes a new media-less call to Avaya Oceana® Solution for routing to a suitable agent. After the agent answers the call, the customer is out-dialed and connected to the agent.

Support for Post Call Survey

Avaya Oceana® Solution provides the Post Call Survey feature. With this feature, the caller can provide a rating based on the interaction with the agent.

Export and import of multiple workflows

Avaya Oceana® Solution now provides an option to export and import multiple workflows. If you want to move workflows from one server to another server, you can now select multiple workflows to export into a file and import them back into another server. You can export or import multiple deployed workflows and export multiple drafted workflows.

Routing rule enhancements

In the current release, you can use the IF This Then That (IFTTT) task of Engagement Designer and create multiple rules when you have multiple Treatment VDNs.

Support for Oceana Data Viewer

The current release of Avaya Oceana® Solution includes the Oceana Data Viewer service. This service acts as a debugging and visualization tool for Avaya Oceana® Solution. With this tool, you can view the Chat, Email, SMS, Social, and Generic contacts that are in Omnichannel Database.

Diff Tool enhancements

Engagement Designer Diff Tool displays the changes made in the nodes of a workflow.

The tool indicates:

- The changes in the Input or Output Mapping, Properties, and Label attributes of the workflow.
- The differences in the functions and templates in data mappings.
- The changes in the nodes of gold stamped workflows.

  Workflow gold stamping defines a workflow released by Avaya as a Gold Standard workflow.

Support for automated migration process

The current release of Avaya Oceana® Solution supports automated migration process. You can run the automated script to upgrade Avaya Breeze® platform nodes and the services of Avaya

Oceana® Solution clusters. Administrators can use simple script commands to migrate Avaya Breeze® platform and Avaya Oceana® Solution components to the latest release.

The automated migration script also supports ZangSmsConnector and CRMGateway snap-ins of Avaya Oceana® Cluster 5, and the OceanaDataViewer snap-in of Avaya Oceana® Cluster 3.

Discontinued support for 25-agent deployments

From the current release, Avaya Oceana® Solution does not support 25-agent deployments. The 100-agent deployment is the direct replacement of the 25-agent single-node deployment. Also, Avaya Oceana® Solution does not support migration for 25 to 100 agent deployments.

Oracle Restricted Use License

Avaya Analytics™ uses certain embedded Oracle programs. The Oracle programs included in Avaya Analytics™ are subject to a restricted use license and can be used solely in conjunction with Avaya Analytics™.

In Customer environments with administrative practices for functions such as: backup, security, authentication and similar operational aspects, the Customer’s administrator may access an Oracle database embedded in Avaya Analytics™ for the sole purpose of configuring the embedded database for use solely with Avaya Analytics™. Customer (or its administrator) may not add or make changes to the Oracle database schemas, metadata or data models other than through and/or as an extension of the functionality of Avaya Analytics™, including but not limited to: incorporating implementation reference data, dimensional and fact tables.

With regards to visual tools, including but not limited to Data Visualization and Stream Analytics, Customer will be permitted to access and administer the tools solely within the scope of Avaya Analytics™. The foregoing is meant to allow Customer access to metadata for visual tools; however, in the case of Avaya Analytics™ that distributes Oracle Database Enterprise Edition, Customer may not access or change the database schema other than through and/or as an extension of the functionality of Avaya Analytics™, including but not limited to: incorporating implementation reference data, dimensional and fact tables solely related to Avaya Analytics™.

Customer is fully responsible and liable to Avaya, its affiliates, and Oracle for any damages or losses caused by any unauthorized use of any of the Oracle programs embedded in Avaya Analytics™.

Chapter 2: Overview

Avaya Oceana® Solution overview

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

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

With these routing strategies, you can:

- Obtain customer information from Customer Relationship Management (CRM) of the enterprises 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® Solution provides:

- Functionality to map customer journey across various self-service and assisted service channels by storing the related data crumbs in the in-memory data grid. These data crumbs are used by resources and routing workflows.
- 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.

You can deploy Avaya Oceana® Solution in an Amazon Web Services (AWS) environment. For more information about AWS deployments, see *Deploying Avaya Oceana® Solution on Amazon Web Services*.

Avaya Oceana® Solution architecture

The following diagram depicts the high-level architecture of Avaya Oceana® Solution:

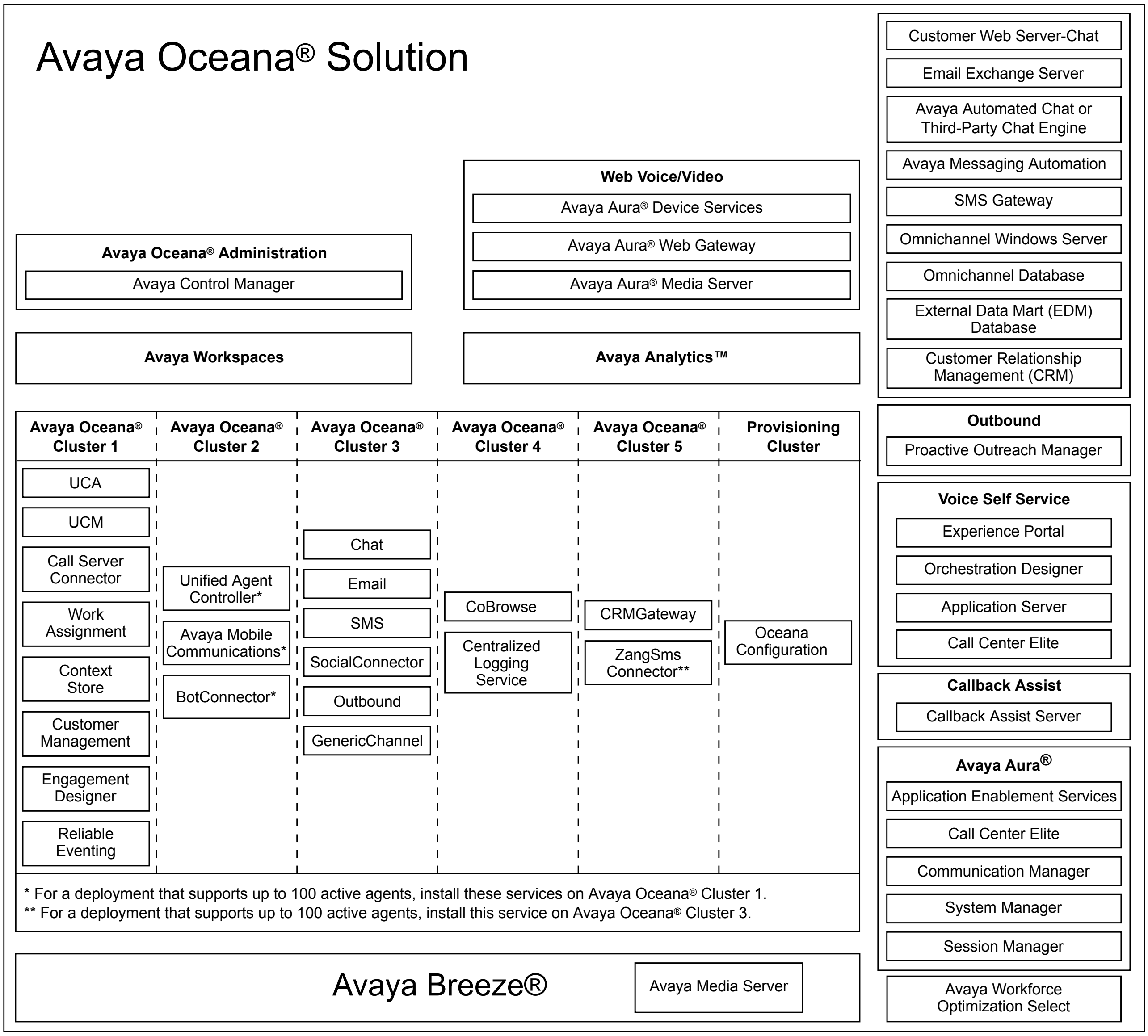


Figure 1: Avaya Oceana® Solution architecture

Important:

- Do not install any third-party or custom Service Archives (SVARs) on Avaya Breeze® platform nodes and clusters that are used in Avaya Oceana® Solution, because these nodes and clusters are for the exclusive use of Avaya Oceana® Solution.
- Do not add additional Avaya Breeze® platform nodes to the specified Avaya Oceana® clusters.

- Do not use Context Store for additional data storage for other purposes

Chapter 3: Deployment process

Deployment process

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

The configuration of Communication Manager and Call Center Elite, Application Enablement Services, Avaya Control Manager, and Avaya Workspaces is common to both PSTN and Web Voice/Video.

❗ **Important:**

Avaya Oceana® Solution must have the campus Avaya Control Manager applications and associated databases, and Omnichannel Database Servers in the same physical data center as the Avaya Breeze® platform nodes.

Avaya does not support physically locating the Avaya Control Manager or Omnichannel campus applications from Avaya Breeze® platform. This requirement does not apply to a Disaster Recovery solution that has two interdependent deployment connected over a WAN.

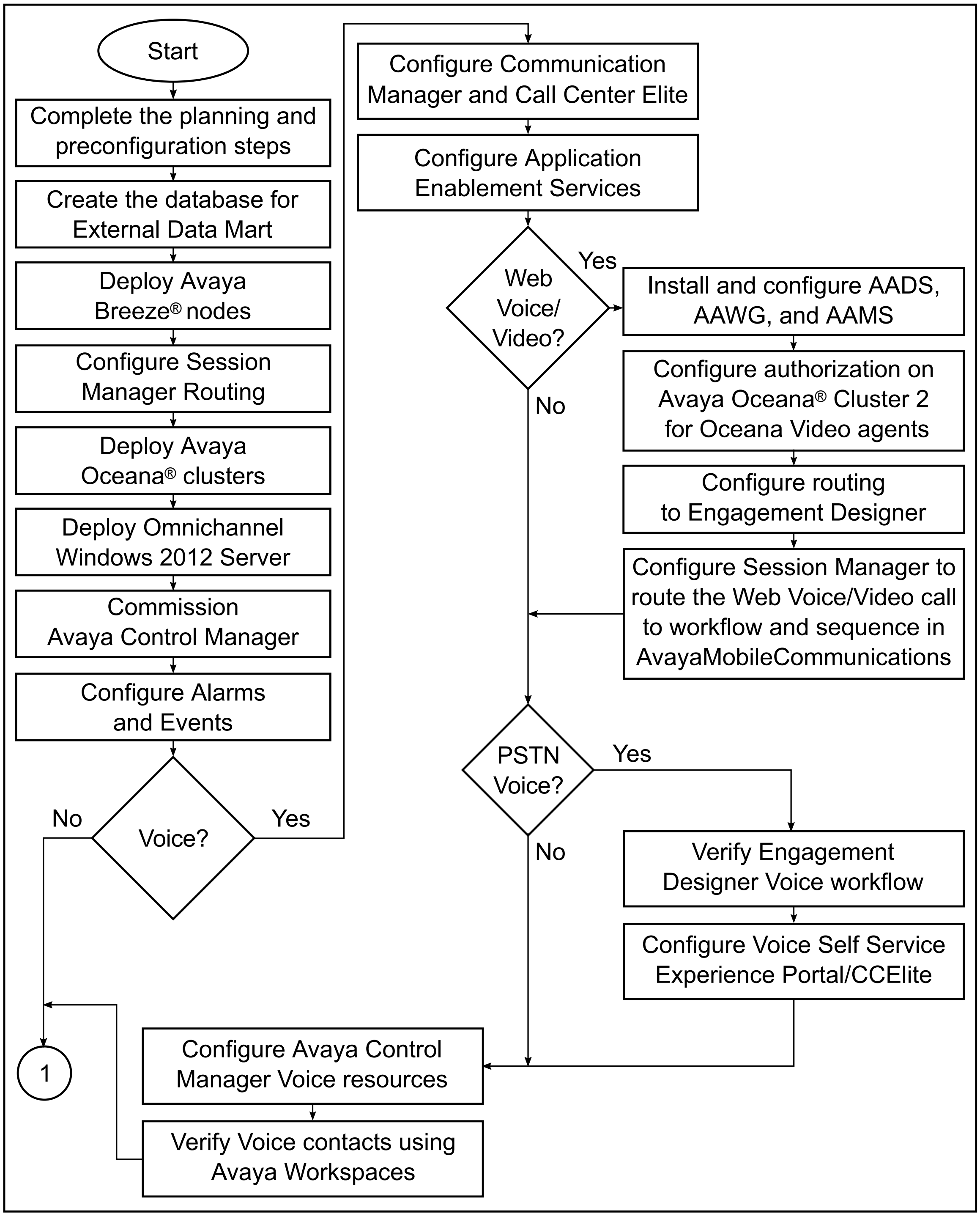
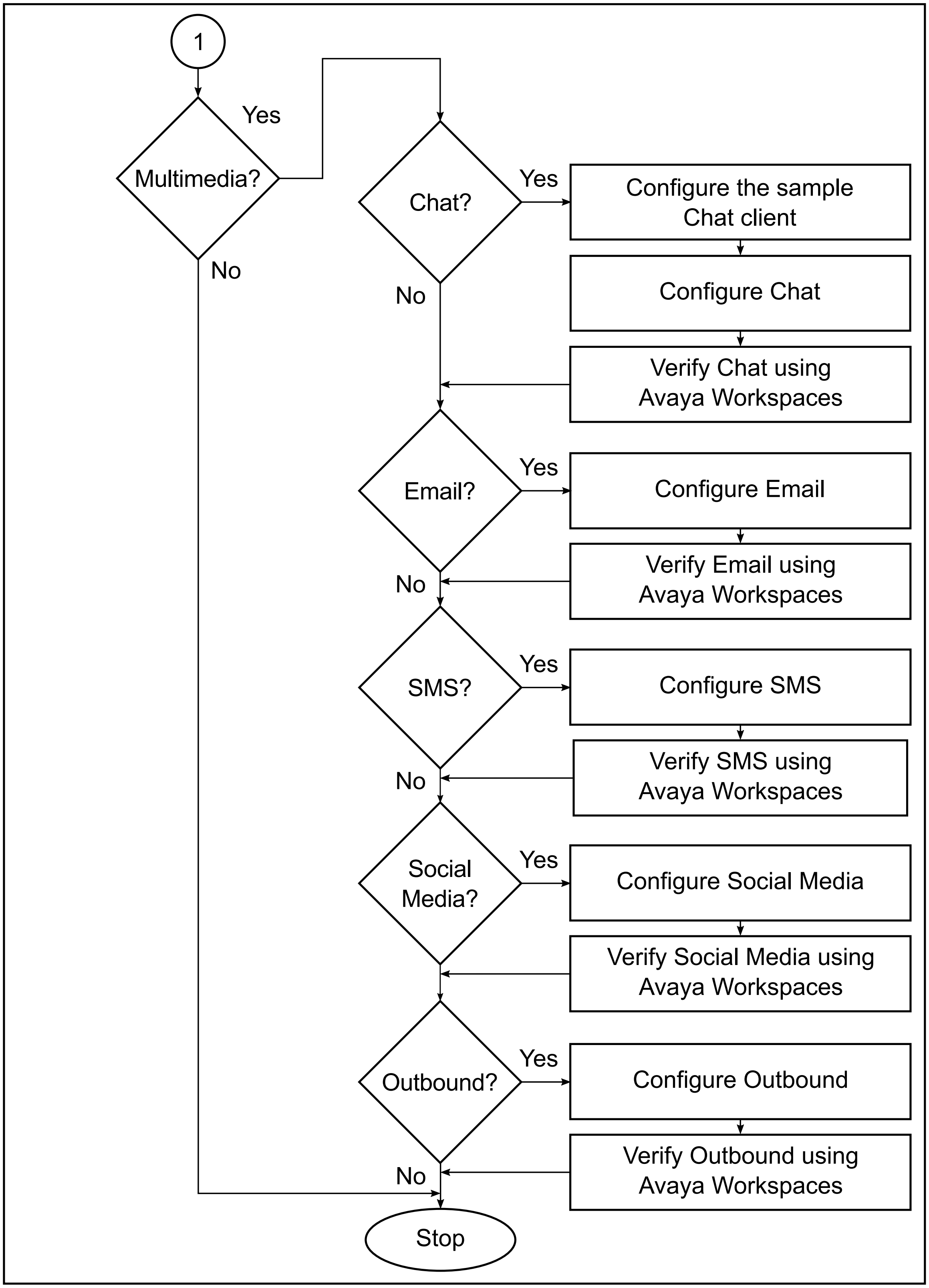

Start
Complete the planning and preconfiguration steps
Create the database for External Data Mart
Deploy Avaya Breeze® nodes
Configure Session Manager Routing
Deploy Avaya Oceana® clusters
Deploy Omnichannel Windows 2012 Server
Commission Avaya Control Manager
Configure Alarms and Events
Voice?
No
Yes
1
Configure Communication Manager and Call Center Elite
Configure Application Enablement Services
Web Voice/ Video?
Yes
No
Install and configure AADS, AAWG, and AAMS
Configure authorization on Avaya Oceana® Cluster 2 for Oceana Video agents
Configure routing to Engagement Designer
Configure Session Manager to route the Web Voice/Video call to workflow and sequence in AvayaMobileCommunications
PSTN Voice?
Yes
No
Verify Engagement Designer Voice workflow
Configure Voice Self Service Experience Portal/CCElite
Configure Avaya Control Manager Voice resources
Verify Voice contacts using Avaya Workspaces

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
Configure Social Media
Verify Social Media using Avaya Workspaces
Outbound?
Yes
No
Configure Outbound
Verify Outbound using Avaya Workspaces
Stop

Chapter 4: Planning and preconfiguration

Planning and preconfiguration

This section provides information about Avaya Breeze® platform specifications for Avaya Oceana® Solution.

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

Component	Supported release
Avaya Aura® System Manager	8.0.x and 8.1
Avaya Aura® Communication Manager	6.3.x, 7.x, 8.0.x, and 8.1
Avaya Aura® Call Center Elite	6.3.x, 7.x, 8.0.x, and 8.1
Avaya Aura® Session Manager	6.3.x, 7.x, 8.0.x, and 8.1
Avaya Aura® Application Enablement Services	6.3.x, 7.x, 8.0.x, and 8.1
Avaya Aura® Experience Portal	7.2, 7.2.1, and 7.2.2
Avaya Control Manager	8.1.0.1
Avaya Aura® Orchestration Designer	7.1 and 7.2
Avaya Aura® Session Border Controller	7.1
Avaya Proactive Outreach Manager	3.1.1 and 3.1.2
Avaya Workforce Optimization Select	5.2.2
Avaya Aura® Workforce Optimization	15.2 and 15.2.1
Avaya Agent for Desktop	1.7

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® Solution when deployed on-premise:

Parameter	On-Premise only			
	4500-agents	2000-agents	1000-agents	100-agents
Maximum number of active Avaya Workspaces Agents including Supervisors and Agents (Supervisors logged in as active Agents)	4500 **Note:** Of this maximum figure, 1000 agents can be digital agents with a maximum of 3 digital channels per agent.	2000	1000	100
Maximum number of active Avaya Workspaces users including Supervisors and Agents (Supervisors not logged in as active Agents)	4950	2200	1100	110
Maximum number of configured users (Agents and Supervisors)	14850	6600	3300	330
Maximum number of configured Agents	13500	6000	3000	300
Maximum number of configured Supervisors	1350	600	300	30
Maximum number of configured Social Agents	300	300	300	100
Maximum number of configured Outbound Agents	300	300	300	NA
Maximum number of active Supervisors using Avaya Workspaces	1350	200	100	10
Maximum number of active Social Agents	300	300	300	30
Maximum number of active Outbound Agents	100	100	100	10
Maximum number of concurrent contacts controlled by Avaya Oceana® Solution simultaneously	3300	3300	3300	1000

Table continues…

Parameter	On-Premise only			
	4500-agents	**2000-agents**	**1000-agents**	**100-agents**
Maximum number of concurrent Avaya Workspaces instances per Agent	1	1	1	1
Maximum number of concurrent Avaya Workspaces instances per Supervisor	1	1	1	1
Maximum supported Voice Busy Hour Call Completion (BHCC) - Self Service	45000	30000	30000	3000
Maximum supported Voice Busy Hour Call Completion (BHCC) - Assisted Service	20000	20000	10000	1000
Maximum supported Busy Hour Call Completion (BHCC) - Outbound	1500	1500	1500	150
Maximum supported Chat/ Email/SMS/Social interactions per hour	12000	12000	6000	600
Maximum supported Chat per hour Assumes no other multimedia channel is active.	12000	12000	6000	600
Maximum supported Email per hour Assumes no other multimedia channel is active.	12000	12000	6000	600
Maximum supported SMS per hour Assumes no other multimedia channel is active.	12000	12000	6000	600
Maximum supported Social per hour Assumes no other multimedia channel is active.	1800	1800	6000	600
Maximum supported Generic Channel per hour	3600	3600	3600	600
Maximum number of concurrent Web Voice sessions	300	300	300	300
Maximum number of concurrent Web Video sessions	100	100	100	100

Table continues…

Parameter	On-Premise only			
	4500-agents	**2000-agents**	**1000-agents**	**100-agents**
Maximum number of concurrent Chat sessions per agent	3	3	3	3
Maximum number of concurrent Emails per agent	3	3	3	3
Maximum number of concurrent SMS sessions per agent	3	3	3	3
Maximum number of concurrent Social sessions per agent	3	3	3	3
Maximum number of concurrent Generic Channel sessions per agent	3	3	3	3
Maximum number of Ad-hoc Email per Agent	1	1	1	1
Maximum deferred Email	12000	6000	3000	500
Maximum number of Observe Chat per Agent	3	3	3	3
Number of concurrent Co-Browse sessions per node	200	200	200	20
Maximum number of concurrent Chat sessions	6000	6000	3000	300
Maximum number of concurrent Chat sessions per customer	10	10	10	10
Total number of services supported	5000	5000	5000	1000
Number of services supported per Agent	2000	2000	2000	1000
Maximum number of attributes per Service	10 Channel + 9 attributes	10 Channel + 9 attributes	10 Channel + 9 attributes	10 Channel + 9 attributes
Maximum number of attributes per Agent	100	100	100	100
Maximum queued contacts across all channels	8000	8000	4000	400
Maximum queued Voice contacts	8000	8000	4000	400
Maximum queued Chat contacts	2000	2000	1000	100
Maximum queued Email contacts	1000	1000	1000	100

Table continues…

Parameter	On-Premise only			
	4500-agents	2000-agents	1000-agents	100-agents
Maximum queued Social contacts	1000	1000	1000	100
Maximum queued SMS contacts	1000	1000	1000	100
Maximum queued Generic Channel contacts	1000	1000	1000	200
Maximum number of WebRTC agents for each deployment	500	500	500	500
Number of concurrent Chatbot sessions with 2 Automated Chat Servers and 2 Chatbot Servers	1500	1500	1500	150
Maximum number of Communication Managers	• 1 CM/CCElite Simplex • 1 CM/CCElite Duplex • 1 CM/CCElite Simplex or Duplex with associated ESS	• 1 CM/CCElite Simplex • 1 CM/CCElite Duplex • 1 CM/CCElite Simplex or Duplex with associated ESS	• 1 CM/CCElite Simplex • 1 CM/CCElite Duplex • 1 CM/CCElite Simplex or Duplex with associated ESS	• 1 CM/CCElite Simplex • 1 CM/CCElite Duplex • 1 CM/CCElite Simplex or Duplex with associated ESS
Maximum number of Transfer to Service	1000			

Avaya Oceana® Solution hardware requirements

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

Component	Platform	Requirement	Avaya Oceana® Solution					
			4500 Agents	2000 Agents	1000 Agents	500 Agents	250 Agents	100 Agents
Avaya Oceana® Cluster 1	Avaya Breeze® platform	Number of nodes	3	3	3	3	3	3
		Memory/ node	96 GB	96 GB	64 GB	48 GB	48 GB	32 GB
		Minimum disk size/ node	500 GB	500 GB	500 GB	500 GB	500 GB	500 GB
		vCPU's/ node	16	12	12	8	8	8

Table continues…

Component	Platform	Requirement	Avaya Oceana® Solution					
			4500 Agents	2000 Agents	1000 Agents	500 Agents	250 Agents	100 Agents
Avaya Oceana® Cluster 2	Avaya Breeze® platform	Number of nodes	2	2	2	2	2	n/a
		Memory/ node	32 GB	32 GB	24 GB	24 GB	16 GB	n/a
		Minimum disk size/ node	350 GB	350 GB	350 GB	350 GB	350 GB	n/a
		vCPU's/ node	8	8	4	4	4	n/a
Avaya Oceana® Cluster 3	Avaya Breeze® platform	Number of nodes	2	2	2	2	2	2
		Memory/ node	32 GB	32 GB	16 GB	16 GB	16 GB	12 GB
		Minimum disk size/ node	400 GB	400 GB	400 GB	400 GB	400 GB	400 GB
		vCPU's/ node	8	8	4	4	4	4
Avaya Oceana® Cluster 4	Avaya Breeze® platform	Number of nodes	3	3	2	2	2	1
		Memory/ node	16 GB	16 GB	16 GB	16 GB	16 GB	8 GB
		Minimum disk size/ node	400 GB	400 GB	400 GB	400 GB	400 GB	100 GB
		vCPU's/ node	4	4	4	4	4	4
Avaya Oceana® Cluster 5	Avaya Breeze® platform	Number of nodes	2	2	2	2	2	2
		Memory/ node	12 GB	12 GB	12 GB	12 GB	12 GB	8 GB
		Minimum disk size/ node	300 GB	300 GB	300 GB	300 GB	300 GB	300 GB
		vCPU's/ node	4	4	4	4	4	4
Omnichannel Datastore	Windows	Number of nodes	2	2	2	2	2	1

Table continues…

Component	**Platform**	**Requirement**	**Avaya Oceana® Solution**					
			4500 Agents	**2000 Agents**	**1000 Agents**	**500 Agents**	**250 Agents**	**100 Agents**
		Memory/ node	16 GB	16 GB	16 GB	16 GB	16 GB	12 GB
		Minimum disk size/ node	4 Disks (100 GB, 60 GB, 1 TB, and 60 GB)	4 Disks (100 GB, 60 GB, 1 TB, and 60 GB)	4 Disks (100 GB, 60 GB, 1 TB, and 60 GB)	4 Disks (100 GB, 60 GB, 100 GB, and 60 GB)	4 Disks (100 GB, 60 GB, 100 GB, and 60 GB)	4 Disks (100 GB, 60 GB, 100 GB, and 60 GB)
		vCPU's/ node	8	8	4	4	4	4
Avaya Control Manager	Windows	Number of nodes	2	2	2	2	2	2
		Memory/ node	12 GB	12 GB	12 GB	12 GB	12 GB	12 GB
		Minimum disk size/ node	300 GB	300 GB	300 GB	300 GB	300 GB	300 GB
		vCPU's/ node	8	8	8	8	8	8
Avaya Control Manager Database	Windows	Number of nodes	2	2	2	2	2	2
		Memory/ node	12 GB	12 GB	12 GB	12 GB	12 GB	12 GB
		Minimum disk size/ node	300 GB	300 GB	300 GB	300 GB	300 GB	300 GB
		vCPU's/ node	8	8	8	8	8	8
Avaya Aura® Media Server for Avaya Breeze® platform	Red Hat Enterprise Linux	Number of nodes	1	1	1	1	1	1
		Memory/ node	8 GB	8 GB	8 GB	8 GB	8 GB	8 GB
		Minimum disk size/ node	50 GB	50 GB	50 GB	50 GB	50 GB	50 GB

Table continues…

Component	Platform	Requirement	Avaya Oceana® Solution					
			4500 Agents	2000 Agents	1000 Agents	500 Agents	250 Agents	100 Agents
		vCPU's/ node	8	8	8	8	8	8
Avaya Aura® Device Services	Red Hat Enterprise Linux	Number of nodes	1	1	1	1	1	1
		Memory/ node	4 GB	4 GB	4 GB	4 GB	4 GB	4 GB
		Minimum disk size/ node	85 GB	85 GB	85 GB	85 GB	85 GB	85 GB
		vCPU's/ node	6	6	6	6	6	6
Avaya Aura® Media Server for Web Voice/Video (Avaya Aura® Web Gateway)	Red Hat Enterprise Linux	Number of nodes	1	1	1	1	1	1
		Memory/ node	16 GB	16 GB	16 GB	16 GB	8 GB	8 GB
		Minimum disk size/ node	50 GB	50 GB	50 GB	50 GB	50 GB	50 GB
		vCPU's/ node	16	16	16	16	8	8
Avaya Aura® Web Gateway	Red Hat Enterprise Linux	Number of nodes	1	1	1	1	1	1
		Memory/ node	8 GB	8 GB	8 GB	8 GB	6 GB	6 GB
		Minimum disk size/ node	100 GB	100 GB	100 GB	100 GB	100 GB	100 GB
		vCPU's/ node	8	8	8	8	4	4
Avaya Aura® Session Border Controller	Red Hat Enterprise Linux	Number of nodes	2	2	2	2	2	2
		Memory/ node	16 GB	16 GB	16 GB	16 GB	16 GB	16 GB
		Minimum disk size/ node	100 GB	100 GB	100 GB	100 GB	100 GB	100 GB
		vCPU's/ node	6	6	6	6	6	6

Note:

- For Avaya Oceana® Solution deployments that support up to 100 agents, install the ZangSmsConnector SVAR on Avaya Oceana® Cluster 3.
- Each Avaya Breeze® platform node of a cluster must reside on a different virtual server.
- For Red Hat Enterprise Linux (RHEL), Avaya Oceana® Solution only supports the version that Avaya ships with the solution.
- Oceana Monitoring Service is a prerequisite for Avaya Oceana® Cluster 5.
- Avaya recommends using 15000 RPM disks. Avaya Oceana® Solution does not support Solid State Drives (SSD).

For hardware requirement information about other products in Avaya Oceana® Solution, see individual product deployment guides.

Virtual Machine requirements

The section describes the minimum number of nodes that must be provisioned for the deployment of Avaya Oceana® Solution. 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® Solution 4500 Agents	Number of nodes for Avaya Oceana® Solution 2000 Agents	Number of nodes for Avaya Oceana® Solution 1000 Agents	Number of nodes for Avaya Oceana® Solution 500 Agents	Number of nodes for Avaya Oceana® Solution 250 Agents	Number of nodes for Avaya Oceana® Solution 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	3	3	2	2	2	1
Avaya Oceana® Cluster 5	2	2	2	2	2	2

Note:

For Avaya Oceana® Solution 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	Intel Xeon E5-2697 2.60GHz
Network Interface	Network Interface Controller (NIC)
Disk type and speed	SATA, Minimum 15000 RPM

Virtual resource allocation in vSphere

RAM

On a Virtual Machine, the following two values are associated with RAM:

- Allocated RAM (ARAM)
- Reserved RAM (RRAM)

If RRAM is less than ARAM, VMware creates a file of size ARAM - RRAM, and uses the file as RAM if there is contention for RAM resources. The performance is impacted as you switch from RAM I/O to file I/O. Therefore, you must always reserve the ARAM.

CPU

- Ensure that Hyperthreading is turned on.
- Ensure that CPU meets or exceeds the benchmark rating for Intel Xeon E5-2697 (first edition) 2.60GHz.

  You can find a sample benchmark on https://www.cpubenchmark.net. For Avaya Oceana® Solution, the baseline CPU mark on this website is 28701.
- Refer to 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: Ensure that the Physical CPU usage does not exceed 80%. The performance is impacted if the Physical CPU consistently exceeds the 80% level.
- 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.

A lot of data is available through esxtop and VMware Infrastructure Client for all levels of granularity, from host through Virtual Machine and per vCPU.

VMware configuration

VMware feature	Supported on Avaya Oceana® Solution clusters on VM with live traffic in production	Supported on Avaya Oceana® Solution clusters in maintenance mode**
Cloning	No	Yes
Distributed Power management (DPM)	No	No
Distributed Resource Scheduler (DRS)	Partial - DRS Separation Rules only	Partial - DRS Separation Rules only
Distributed Switch	No	No
Fault Tolerance	No	No
High Availability (HA)*	No	No
Snapshot	No	Yes***
Storage DRS	No	No
Storage Thin Provisioning	No	No
Storage vMotion	No	Yes
Suspend & Resume	No	NA
vMotion	No	Yes

* Avaya Oceana® Solution provides its own HA mechanism.

** Maintenance mode 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® Solution 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 does not process any contacts or operations.

*** You must delete snapshots from Avaya Oceana® Solution virtual machines before placing Avaya Oceana® Solution back into 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® Solution 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 the applicable ContextStoreManager attributes in the **External Data Mart Configuration** group.

Context Store supports the following three databases for External Data Mart:

- PostgreSQL 9.1 and later

- Oracle 11g and later
- Microsoft SQL Server 2008 and later

For information on how to install an EDM database and create tables, see *Avaya Context Store Snap-in Reference* and *Avaya Context Store Snap-in Release Notes*.

Important:

In an Avaya Oceana® Solution deployment, EDM is a mandatory requirement.

Deploying the External Data Mart schema in the Avaya Analytics™ database

Procedure

1. In the Avaya Analytics™ database, navigate to the unzipped installation folder containing the `base_install.sql` file.

   The Context Store scripts are available in the `<AVAYA_ANALYTICS_BUILD_DIRECTORY>/context_store_schema_scripts/` directory.
2. Run the following command as a system administrator:

   ```
   sqlplus sys/<password>@orcl as sysdba @base _install.sql
   ```

   In this command, replace *<password>* with the current password.

   The default user name is `context_store` and the default password is `ContextStoreAv33`.
3. **(Optional)** To update the default user name and password, do the following:
   a. Modify the details in the `create_schemas.sql` script located in the general folder.
   b. Run the `base_install.sql` script again.

Planning tasks

- Read *Avaya Oceana® Solution Description*.
- Ensure that the time on all servers in Avaya Oceana® Solution is synchronized.
- Do the following if you use third-party certs:
  - Select the **Only allow secure web communications** check box while creating each cluster in Avaya Oceana® Solution
  - Set up DNS to resolve all FQDNs

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® Solution.

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	

Table continues…

Name	Your value
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 Aura® Experience Portal

Name	Your value
Hostname	

Table continues…

Name	Your value
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	
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	

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® Solution 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:
    1. In the **Datasource Name** field, enter the name to identify Active Directory.
    2. In the **Host** field, enter the FQDN address of your LDAP server.

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

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

       For example, CN=myDomain.com,DC=myDomain,DC=com
    7. In the **Search Filter** field, enter the LDAP search string.

       For example, CN=Alex*.
    8. Select the **Use SSL** check box.
    9. Click **Test Connection**.
8. On the New User Synchronization Datasource page, in the Attribute Parameters section, perform the following steps:
    1. Click **Add Mapping** to add a row.
    2. From the drop-down list on the left, select **cn**.
    3. From the corresponding drop-down list on the right, select **sourceUserKey**.
    4. Click **Add Mapping** to add another row.
    5. From the drop-down list on the left, select **mail**.
    6. From the corresponding drop-down list on the right, select **loginName**.

       Note:

       Instead of the **mail** field pointing to **loginName**, you might also need to use **userPrincipalName** depending on the configuration of the LDAP server. For example, if the **mail** field is not set in the LDAP server.
    7. Click **Add Mapping** to add another row.
    8. From the drop-down list on the left, select **givenName**.

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 **givenName**.
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.

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® Solution

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*

Upgrade considerations

In Avaya Oceana® Solution, 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® Solution, 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 375.
Chat	See Configure the sample Chat client on page 338.
SMS	See Configuring SMS Gateway on page 392.
Social Media	See Configuring Social Media for Avaya Messaging Automation on page 411.

Table continues…

Channel	Description
Web Voice	See Configuring an Implicit User Route Point for inbound Web Voice on page 315.
Web Video	See Configuring an Implicit User Route Point for inbound Web Video on page 327.
Generic Channel	See the SDK documentation for information about using Route Points with the Generic Channel.

Chapter 5: Deploy Avaya Breeze® nodes

Deploy Avaya Breeze® platform nodes

This section describes how to deploy the Avaya Breeze® platform nodes for the following clusters of Avaya Oceana® Solution:

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

For an Avaya Oceana® Solution 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
  - CRMConnector

  Configure the Lightweight Directory Access Protocol (LDAP) server certificates for Avaya Oceana® Cluster 1 nodes.
- 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 ESX.

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 describing how to create the common certificate, import 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® Solution:

No.	Task	Notes	✔
1	Download *Avaya Oceana® Solution Description*	-	
2	Download *Deploying Avaya Breeze® platform*	-	
3	Review Avaya Breeze® platform and server requirements for your solution	See *Avaya Oceana® Solution Description*.	
4	Review Avaya Oceana® Solution 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 a number of 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 Solution hardware requirements on page 33. **Important:** These Avaya Breeze® platform nodes are for the exclusive use of Avaya Oceana® Solution. 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.

Configuring LDAP server certificates for Avaya Breeze® platform nodes

About this task

Configure the Avaya Breeze® platform nodes to trust your LDAP server certificates.

Note:

- For an Avaya Oceana® Solution deployment that supports up to 100 active agents, add the LDAP server certificates to the three Avaya Breeze® platform nodes of Avaya Oceana® Cluster 1.
- For an Avaya Oceana® Solution deployment that supports up to 4500, 2000, 1000, 500, or 250 active agents, add the LDAP server certificates to the two Avaya Breeze® platform nodes of Avaya Oceana® Cluster 2.

The actual clusters do not exist at this point of the deployment. This procedure is intended to prepare the nodes for the cluster configuration.

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 check box for one of the nodes of the proposed cluster, 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 of your LDAP server.
    d. Click **Retrieve Certificate**.

   e. Click **Commit**.

5. Repeat Step 3 to Step 5 for the other nodes of the proposed cluster.

Configuring the WebSphere certificate for Centralized Logging

About this task

To run Centralized Logging in the secure mode, you must configure the WebSphere certificate for each node of the cluster where you plan to install CentralizedLoggingService.

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 **WebSphere** and click **Replace**.
4. On the Replace Identity Certificate page, do the following:
   a. Select the **Replace this Certificate with Internal CA Signed Certificate** option.
   b. In the **Key Algorithm** and **Key Size** fields, select the appropriate values.
   c. In the **Subject Alternative Name** field, select the **IP Address** check box.
   d. In the **IP Address** field, enter the Management IP address of the Avaya Breeze® platform node.
   e. Click **Commit**.
5. Repeat Step 2 to Step 4 for the other nodes.

Creating the common certificate

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, Oceana_Authorization
   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 the cluster that AuthorizationService is installed on.

h. In the first **DNS Name** field, enter the Security Module FQDN for one of the nodes of the cluster.

i. In the second **DNS Name** field, enter the Security Module FQDN for the other node of the cluster.

j. In the **IP Address** field, enter the IP address of the cluster.

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.

Importing the common certificate in Avaya Breeze® platform nodes

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, do the following:

   a. Select the **Import third party certificate** option.

   b. In the **Please select a file (PKCS#12 format)** field, browse and select the common certificate that you generated.

   c. In the **Password** field, enter the password that you specified while creating the end entity.

   d. Click **Commit**.

5. Repeat Step 2 to Step 4 for the other nodes of the cluster.

Exporting the Avaya Breeze® platform Authorization Identity 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 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 6: Configure Session Manager routing

Configure Session Manager routing

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

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

In an enterprise solution, the various SIP network components are represented as SIP Entities and the connections/trunks between Session Manager and those components are represented 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 dial plan and trunking administration needed on each SIP Entity, and consolidates administration in a central place, namely Avaya Aura® System Manager.

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

Important:

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

Creating a routing location

Before you begin

Session Manager uses the origination location to determine which dial pattern to use when routing calls. Locations are also used 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. Verify the location for Avaya Oceana® Solution.

   If the location is not configured for Avaya Oceana® Solution, complete the remainder of this procedure.
3. On the Location page, click **New**.
4. In the **Name** field, enter the location name.
5. In the **Notes** field, enter a description about the location.
6. In the Dial Plan Transparency in Survivable Mode section, specify DPT parameters.
7. In the Overall Managed Bandwidth section, specify the parameters for the location.
8. In the Per-Call Bandwidth Parameters section, specify the average bandwidth per call for the location.
9. In the Alarm Threshold section, specify the alarm threshold percentage for audio and multimedia calls for the location.
10. To add a location pattern:
    a. In the Location Pattern section, click **Add**.
    b. In the **IP address Pattern** field, enter the IP address pattern to match.
    c. In the **Notes** field, enter a description about the location pattern.
    d. Continue adding location pattern by clicking **Add** until you configure all the required location patterns.
11. Click **Commit**.

Creating a 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. Verify the SIP entity for Session Manager.

   If a SIP entity is not configured for Session 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.

   To add a SIP entity for Session Manager, you must enter the Security Module IP address instead of the Management IP address.

6. In the **Type** field, select **Session Manager**.
7. 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 define 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 define 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 7: Deploy Avaya Oceana® clusters

Deploy Avaya Oceana® clusters

Avaya Oceana® Solution 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® Solution. Therefore, do not install any third-party or custom Service Archives (SVARs) on these clusters.

For an Avaya Oceana® Solution 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® Solution 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® Solution deployment that supports up to 4500, 2000, 1000, 500, or 250 active agents.
    - Omnichannel Windows 2012 R2 Server
    - 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.
2. Verify that System Manager can resolve the host name of Avaya Breeze® platform nodes.

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® Solution.

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:
    1. Browse to the location of the license that you want to install and select the license file.
    2. Click **Accept the License Terms & Conditions**.
    3. Click **Install**.

       The system installs the license.
4. In the left 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
    - Chatbot_For_Automated_Chat_System
6. In the left 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:
    1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
    2. On the Services page, verify that the **License Mode** column for all the services displays a check mark.

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 • OceanaCoreDataService • OceanaMonitorService • OmniCenterProvisioningCollector (Required only for Avaya Analytics™) • PacketbeatService • UCAStoreService • UCMDataCollector (Required only for Avaya Analytics™) • UCMService • WAIMRestService • WorkAssignmentManagerService
Avaya Oceana® Cluster 2	• AuthorizationService • AvayaMobileCommunications (Required only for Web Voice/Video) • BotConnector • MetricbeatService • OceanaMonitorService • PacketbeatService • UnifiedAgentContextService • UnifiedAgentController

Table continues…

Cluster name	SVAR
Avaya Oceana® Cluster 3	• AgentControllerService • AutomationController (Required only for the Avaya Automated Chat integration) • CustomerControllerService • EmailService (Required only for Email) • GenericChannelAPI • MessagingService (Required only for Short Message Service and Social Media) • MetricbeatService • OBCService (Required only for Outbound) • OCPDataServices • ORCRestService • OceanaDataViewer • OceanaMonitorService • PacketbeatService • SocialConnector (Required only for Social Media) • ZangSmsConnector
Avaya Oceana® Cluster 4	• CentralizedLoggingService (Required only for Centralized Logging) • 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® clusters

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® Solution and ensure that you do not use the selected cluster group for any non-Avaya Oceana® Solution 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. 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. Clear the **Is session affinity enabled** check box.

f. 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® Solution deployment that supports up to 100 active agents, change the value of the **Limit on the memory (GB) to allocate for WAS** field to 3.

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
   - OceanaCoreDataService
   - OceanaMonitorService
   - OmniCenterProvisioningCollector
   - PacketbeatService
   - UCAStoreService
   - UCMDataCollector
   - UCMService
   - WAIMRestService
   - WorkAssignmentManagerService

   For an Avaya Oceana® Solution 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

   For an Avaya Oceana® Solution deployment that supports 1000 active agents or less, ensure that you also add the CentralizedLoggingService SVAR to Avaya Oceana® Cluster 1.

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 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® Solution 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® Solution and ensure that you do not use the selected cluster group for any non-Avaya Oceana® Solution 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. 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. 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
   - OceanaMonitorService
   - PacketbeatService

- 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® Solution and ensure that you do not use the selected cluster group for any non-Avaya Oceana® Solution 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. Select or clear the **Only allow secure web communications** check box based on your requirement.
   c. 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*.

   d. For only the Avaya Oceana® Solution 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
   - OBCService
   - OCPDataServices
   - ORCRestService
   - OceanaDataViewer

- OceanaMonitorService
- PacketbeatService
- SocialConnector

For an Avaya Oceana® Solution 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® Solution deployment that supports up to 1000 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.

Before you begin

For successful installation of CentralizedLoggingService, ensure that Avaya Breeze® platform nodes and their Security IP addresses are active.

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® Solution and ensure that you do not use the selected cluster group for any non-Avaya Oceana® Solution 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. Select or clear the **Only allow secure web communications** check box based on your requirement.

   b. 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.

   c. 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
   - CentralizedLoggingService
   - 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.

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

c. 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® Solution and ensure that you do not use the selected cluster group for any non-Avaya Oceana® Solution 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® Solution individually. For information about the attributes of the services that you install on Avaya Oceana® Solution clusters, see Service attributes on page 510.

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® Solution deployment that supports up to 4500 active agents, select `3X Large`. • For an Avaya Oceana® Solution deployment that supports up to 2000 active agents, select `Extra Large`. • For an Avaya Oceana® Solution deployment that supports up to 1000, 500, or 250 active agents, select `Large`. • For an Avaya Oceana® Solution 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`.

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® Solution deployment that supports up to 100 active agents, select Avaya Oceana® Cluster 1. • For an Avaya Oceana® Solution 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® Solution deployment that supports up to 100 active agents, select Avaya Oceana® Cluster 1. • For an Avaya Oceana® Solution 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.

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.
Cluster Monitor 4	The fourth cluster that you want to monitor through OceanaMonitorService. To set this attribute, select Avaya Oceana® Cluster 4.

Table continues…

Name	Description
Cluster Monitor 5	The fifth cluster that you want to monitor through OceanaMonitorService. Do not select any value for this attribute.

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 IP address or FQDN of Omnichannel Database.
Username for the Omnichannel Database	The user name for Omnichannel Database. The default user name for Omnichannel Database is `mmJava`.

Table continues…

Name	Description
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 Omni Channel 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 Database Type	The type of the External Data Mart (EDM) database. The available values are: • PostgreSQL • Microsoft SQL Server • Oracle Database
External Data Mart FQDN	The FQDN of the EDM database.
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.
External Data Mart Password	The password of the EDM database.

Engagement Designer

Name	Description
Completed instance to be deleted or not	The attribute that enables or disables the deletion of completed instances. For Avaya Oceana® Solution, select `false`.
Media Server Inclusion	The attribute that enables or disables the inclusion of Avaya Aura® Media Server. To configure Avaya Oceana® Solution for Web Voice/Video, select `true`.
Chatbot Site Identifier	The Site ID of the BotConnector service followed by :FriendlyName.

Automated Chat

Name	Description
Automated Chat Base URL	The base URL of the Avaya Automated Chat system starting with http or https.

Messaging Connection Service

Name	Description
Snap-in Service 1 Name	The name of the first MessagingConnector snap-in service.

Table continues…

Name	Description
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. For example, if you set this attribute for Social Media, you must enter the name of the snap-in that you create while configuring Social Media for Avaya Messaging Automation.
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`.
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 on page 510.

OBCService

Name	Description
POM Server	The IP address or FQDN 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.

CRM Gateway

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`.

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`.
Maintenance Mode	The attribute to enable the maintenance mode. The supported values are true and false. The default value is false. Used for Oceana mode.
Oceana Mode	The attribute to enable Oceana support for Zang. The supported values are true and false. The default value is false.

Table continues…

Name	Description
Key for Oceana Messaging Service	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 Breeze node IP or Cluster IP of the cluster that hosts the Oceana Messaging snap-in. This option is mandatory to support the Oceana mode.
Oceana Messaging Service Name	The name of the MessagingService snap-in. This option is mandatory to support the Oceana mode.

Setting CentralizedLoggingService attributes

About this task

Use this procedure to configure the attributes of CentralizedLoggingService.

Important:

The OceanaConfiguration service does not cover the configuration of CentralizedLoggingService attributes. Therefore, you must configure these attributes separately.

Before you begin

- For an Avaya Oceana® Solution deployment that supports more than 1000 active agents, install the CentralizedLoggingService SVAR on Avaya Oceana® Cluster 4.
- For an Avaya Oceana® Solution deployment that supports 1000 active agents or less, install the CentralizedLoggingService SVAR on Avaya Oceana® Cluster 1.

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 CentralizedLoggingService.
   b. In the **Service** field, select **CentralizedLoggingService**.
3. Configure CentralizedLoggingService attributes.
4. Click **Commit**.

CentralizedLoggingService attributes

Name	Description
Days To Retain Logs in Filebeat Index	The number of days for which the logs must be retained in the Filebeat index. The system deletes the logs that are older than the number of days specified in this field.
Days To Retain Logs in Metricbeat Index	The number of days for which the logs must be retained in the Metricbeat index. The system deletes the logs that are older than the number of days specified in this field.
Days To Retain Logs in Packetbeat Index	The number of days for which the logs must be retained in the Packetbeat index. The system deletes the logs that are older than the number of days specified in this field.
Kibana User name	The user name to log in to the Kibana user interface.
Kibana user password	The password to log into the Kibana user interface.
Logstash security	The attribute that enables or disables the security (SSL) mode for the Logstash service.
Maximum Log Space(in GB) for Filebeat Index	The maximum permissible log space for the logs in the Filebeat index. This value is in GB. The system starts deleting the older logs after the space specified in this field is occupied.
Maximum Log Space(in GB) for Metricbeat Index	The maximum permissible log space for the logs in the Metricbeat index. This value is in GB. The system starts deleting the older logs after the space specified in this field is occupied.
Maximum Log Space(in GB) for Packetbeat Index	The maximum permissible log space for the logs in the Packetbeat index. This value is in GB. The system starts deleting the older logs after the space specified in this field is occupied.

Adding Avaya Breeze® platform nodes to clusters

Adding nodes to Avaya Oceana® Cluster 1

Before you begin

For an Avaya Oceana® Solution deployment that supports up to 1000 active agents, you install CentralizedLoggingService 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® Solution deployment that supports more than 1000 active agents, you 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® Solution 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.

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**.

Certificate-based authentication

For the certificate-based authentication, you must perform the following procedures in the System Manager web portal:

1. Configure the client certificate challenge in Avaya Breeze® platform Element Manager.

   The configuration is available on the **Avaya Breeze®** > **Configuration** > **HTTP Security** page.
2. Create a client keystore.
3. Download the Avaya Breeze® platform trusted certificate from System Manager.
4. Authenticate browsers.

Ensure that client applications that access the snap-in operations provide the location and credentials of the client certificate and trusted certificate to establish a secure session with the cluster.

For information about Avaya Breeze® platform certificate-based authentication, see the *Security* chapter in *Avaya Breeze® platform Overview and Specification*.

For information about Avaya Aura® System Manager certificate-based authentication, see the *Security Enhancement* section in *Avaya Aura® System Manager Overview and Specification*.

Viewing Oceana Monitor Service pages

Procedure

1. In your web browser, enter the following URL to view the Monitor Service page:

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

2. Do one of the following:

   - If the **Authorization Required to view Monitor output** attribute of OceanaMonitorService is set to `true`, log in to the Authorization Service page.
   - If the **Authorization Required to view Monitor output** attribute of OceanaMonitorService is set to `false`, go to Step 3.

3. On the Monitor Service page, click the cluster node to view the information about the cluster.
4. In your web browser, enter the following URL to view the Oceana Services Overview page:

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

Monitor Service page

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

- 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

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.

Table continues…

Button name	Description
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® Solution:

- Name of the snap-in
- Symbol specifying whether Oceana Monitor Service has detected the snap-in
    - The ✓ symbol indicates that Oceana Monitor Service has detected the snap-in.
    - The ✗ symbol 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. Heartbeat background indicates the status of the Heartbeat.

Chapter 8: 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 do not need to do this if the DNS is configured properly 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 Engagement Designer **Admin Console**:

   `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 Engagement Designer **Designer Console**, 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 Engagement Designer **Designer Console**:

   `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® Solution 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
SelfService workflow	OceanaVoiceSelfService
Video workflow	OceanaVideoAssistedService
Generic Channel workflow	OceanaGenericAssistedService
Transfer to Service workflow for Voice	OceanaVoiceTransfer
Transfer to Service workflow for Chat	OceanaChatTransfer
Transfer to Service workflow for Email	OceanaEmailTransfer
Transfer to Service workflow for SMS	OceanaSMSTransfer
Transfer to Service workflow for Web Voice	OceanaWebVoiceTransfer
Transfer to Service workflow for Social Media	OceanaSocialTransfer
Transfer to Service workflow for Video	OceanaVideoTransfer
Transfer to Service 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 Engagement Designer **Admin Console**:

   `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 gets saved into a zipped file.

Importing multiple workflows

About this task

Use this procedure to import multiple drafted or deployed workflows into the Engagement Designer **Admin Console**. After importing deployed workflows, do not deploy the workflow again.

Procedure

1. In your web browser, enter the following URL to open the Engagement Designer **Admin Console**:

   ```
   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.

Chapter 9: Deploy Omnichannel Windows Server

Deploy Omnichannel Windows Server

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.

Note:

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 453. For information about the optimum configuration where you configure an HA setup on the local data center and a backup on a remote data center, see *Avaya Oceana® Solution Disaster Recovery*.

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 Solution hardware requirements on page 33.

Installing Microsoft Windows Server 2012 R2

About this task

Install the Microsoft Windows Server 2012 R2 Standard or Datacenter edition and configure it to support the Omnichannel software.

The following table lists the main inputs to consider while installing Microsoft Windows Server 2012:

Name	Description
Computer name	The name of the server where you want to install Microsoft Windows Server 2012. 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.

Table continues…

Name	Description
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.

Before you begin

- Ensure that you have a newly formatted server that meets the specifications for installing Microsoft Windows Server 2012 R2.
- Ensure that you have a DVD of the Microsoft Windows Server 2012 R2 Standard or Datacenter edition.
- Ensure that you have a product key for Microsoft Windows Server 2012 R2.
- Obtain the IP addresses for the Omnichannel subnet.

Procedure

1. Insert the Microsoft Windows Server 2012 R2 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 the **Time and currency format** field, select the appropriate time and currency.
5. In the **Keyboard or input method** field, select an appropriate value.
6. Click **Next**.
7. Click **Install now**.
8. Select a version of Windows Server 2012 R2 that includes a Graphical User Interface (GUI).
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 Windows Setup screen, read the terms of the license agreement and select **I accept the license terms**.
13. Click **Next**.
14. Select **Custom: Install Windows only (advanced)** to for a new installation.
15. Select the disk partition where you want to install Windows Server 2012 R2.

    Important:

    You can use the partition management options to configure the partitions on your server.
16. Click **Next**.

    The installation proceeds and automatically restarts the server several times.
17. After completing the installation, log on to the server as Administrator by entering and confirming the Administrator password.
18. Select **Set time zone** and complete the information as required for your system.
19. Select **Configure Networking** and complete the information for your Network Interface Card (NIC) with the server IP address.
20. Select **Provide computer name and domain** and complete the information for your server name and network settings.
21. 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.
22. Configure the hard disk drives and partitions for this server using the Windows Server 2012.
23. Install other required drivers for your hardware configuration.

Installing the most recent supported operating system service packs

About this task

To install the most recent supported operating system service packs, you must download the supported operating system service pack from the Avaya hotfixes list and ensure that your Omnichannel software functions correctly with the supported operating system patches.

Before you begin

- Access the Avaya hotfixes list on http://support.avaya.com.
- Install and configure Microsoft Windows Server 2012 R2 on your server.

Procedure

1. Review the Service Packs Compatibility and Security Hotfixes Applicability List to determine the most recent supported patches or service packs.

2. Download the appropriate Microsoft Windows Server 2012 R2 patches for the Omnichannel software installed on this server.
3. Install the most recent Windows Server 2012 R2 service pack that is validated with Omnichannel by following the Microsoft Installation instructions.

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. On the Start screen, select **Administrative Tools** > **Server Manager**.
3. In the left pane, click **Local Server**.
4. In the right pane, in the Properties section, double-click the **Domain** or **Workgroup** value.
5. In the System Properties dialog box, click the **Computer Name** tab.
6. Click **Change**.
7. To add the server to a domain, in the Member of dialog box, click **Domain**.
8. Type the domain name.

   You must provide the fully qualified domain name that includes the prefix and suffix.
9. Click **OK**.
10. Type the domain administrator user name and password.
11. Click **OK**.
12. Restart the server when you are prompted.

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. On the Start screen, click **Control Panel** > **Network and Internet** > **Network and Sharing Center** > **Change adapter settings**.
3. Right-click the unused Network Adapter and click **Disable**.
4. Repeat step 2 through 3 to disable the other 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.

Note:

This procedure is optional. An Administrator can determine whether to enable Microsoft Remote Desktop connection.

Procedure

1. Log on to the server with administrator privileges.
2. On the Start screen, click **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**.

Installing the Omnichannel server software

About this task

Use this procedure to install the latest version of the Omnichannel server software on the Omnichannel server.

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.

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 **Journal Database Drive** field, select the hard disk partition for the Journal database.
8. In the **Oceana Database Drive** field, select the hard disk partition for the Omnichannel database.
9. Click **Install**.
10. On the AVAYA GLOBAL SOFTWARE LICENSE TERMS screen, click **I ACCEPT THE LICENSE TERMS**.
11. After the installation is complete, click **Restart**.

Manage Security and TLS certificates

This section describes how to configure secure Chat and Omnichannel Windows 2012 Server security. 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 the information on how to install the root certificate. To add a server and certificate to System Manager, see the information on 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 and installing the default root certificate

About this task

A default root certificate can be generated when 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*.

Procedure

1. In your web browser, enter the following URL for the System Manager installation of EJBCA:

   ```
   https://<SMGR FQDN>/ejbca/
   ```

2. In the Retrieve Certificates section, click **Fetch CA Certificates**.
3. Based on your browser, perform one of the following steps:

   - To install the certificate in the certificate manager of Firefox, click the **Download to Firefox** link.
   - To install the certificate on a Windows machine containing Microsoft Internet Explorer, Edge, and Chrome, click the **Download to Internet Explorer** link.

   The system prompts you to save the certificate.

4. Save the certificate.
5. Right-click the certificate file and click **Install Certificate**.
6. Select **Local Machine** and click **Next**.
7. Select **Place all certificates in the following store** and click **Browse**.
8. Select the **Show physical stores** check box and scroll up until you find **Trusted Root Certification Authorities**.
9. Expand **Trusted Root Certification Authorities** and select **Registry**.
10. Click **OK**.
11. Click **Finish**.
12. Open the Windows hosts file in a text editor such as Notepad.

    Note:

    Ensure that you run the text editor as Administrator.

13. Add the host names of the lab to your hosts file in the following format.

    ```
    <IP Address> FQDN
    ```

14. In your web browser, browse to a known service URL to verify if the browser accepts the certificate.

    Microsoft Internet Explorer tries to download the JSON response. However, Firefox and Chrome display the result.

15. In your web browser, browse to the chat URL.

    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.

16. **(Optional)** For Firefox, if you do not click the **Download to Firefox** link, perform the following steps to manually install the certificate:

    a. Download the certificate.

    b. Open the Firefox Settings page.

    c. Click **Advanced**.

    d. Click **Certificates**.

    e. Click **View Certificates**.

    f. Select the **Authorities** tab and then click **Import** at the bottom of the screen.

    g. Locate and select the certificate.

    h. Click **Open**.

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.

Procedure

1. On the System Manager web console, click **Services** > **Security** > **Certificates** > **Authority**.

2. In the left 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 a name that matches the full hostname of the server.
8. In the **DNS Name** and **IP Address** fields, enter appropriate values.
9. 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 Windows 2012 R2 server for Omnichannel Provider (OCP).
2. Download a Windows version of OpenSSL to this Windows 2012 R2 server.
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.pem -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.
openssl req -new -in mmdev1.pem -key mmdev1.pem -passin pass:testing -out
mmdev1.csr
```

Creating a certificate from a CSR

Procedure

1. Export the CSR file from the server using an FTP client.
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 left 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.
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**.

   Optionally, you can download the certificate to your browser. System Manager installs the certificate on the host cluster.

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 left 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. Click the **Install certificate** link to download the keystore as a certificate.

This can be installed in the same manner as a root certificate. However, in this case, you need to 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, enter the following text:

   `about:config`

2. On the Warning page, click **I accept the risk!**.
3. In the **Search** field, type `security.enterprise_roots`.
4. Set the value of the **security.enterprise_roots.enabled** row to `true`.

Configuring Cache to use TLS

The Omnichannel Windows 2012 server contains a Cache instance and 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 Cache 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 Cache Superserver to use TLS

About this task

Use this procedure to configure Cache Superserver to use TLS.

Important:

The system does not retain this configuration on upgrade. Therefore, you must do this configuration after every upgrade.

Procedure

1. In your web browser, enter the following URL to open Cache 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 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. Click **System Administration** > **Security** > **SSL/TLS Configurations**.
4. Click **Create New Configuration**.
5. In the **Configuration Name** field, type `%SuperServer`.
6. In the **Type** field, select **Server**.
7. Ensure that the **Client certificate validation** field is set to **None**.
8. To set the certificate, click **Browse** next to the field for the server's certificate.
9. To set the private key, click **Browse** next to the field for the associated private key.
10. In the **Private key password** field, enter the password for the private key.
11. Ensure that only the **TLSv1** check box is selected.
12. In the **Enabled ciphersuites** field, change the value to `TLSv1:TLSv1.1:TLSv1.2:!ADH:!LOW:!EXP:@STRENGTH`.
13. Click **Save**.
14. Click **System Administration** > **Security** > **System Security** > **System-wide Security Parameters**.
15. Set the **Superserver SSL/TLS support** option to **Enabled**.

    With this configuration, you can use secure and non-secure connections to debug certificate issues.
16. Click **Save**.

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
- OCPDataService
- 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 Cache 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 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. 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. In the **User Name** field, 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.

Chapter 10: Commission Avaya Control Manager

This section describes how to commission Avaya Control Manager for Avaya Oceana® Solution.

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® Solution 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:
   1. In the **Username** field, enter the user name.

      The initial user name is `itnv`.
   2. In the **Password** field, enter the password.

      The initial password is `itnv`.
   3. 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® Solution

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 site, department, and team to Avaya Control Manager

About this task

Use this procedure to add the site, department and team information in the 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 left pane, click **Organization tree**.
4. Click the ⏬ button next to the **Add** button.
5. Click the **Add Organization Chart Items** ⊞ button.
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 Communication Manager that you created in the previous procedures.
    d. Click **Save**.
    e. Click **Close**.
7. In the left pane, click the newly created site.
8. Click the ⏬ button next to the **Add** button.
9. Click the **Add Organization Chart Items** ⊞ button.
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 left pane, click the newly created department.
12. Click the ⏬ button next to the **Add** button.
13. Click the ⊞ 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.
- This procedure must be performed 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 left 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 the Avaya Oceana® Solution. Control Manager uses the UCA ReST API to add agent, attribute, provider, and resource information to the Avaya Breeze® platform components in the Avaya Oceana® Solution. Therefore, you must configure the Avaya Oceana® Solution UCA 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 **Alias** field, enter an alias name for the server.
5. 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® Solution deployment and the Avaya Analytics™ deployment are using the same UCA server (Common setup), then the URLs configured for the Avaya Oceana® Solution UCA server must use the exact same URL as the Avaya Analytics™ streams server. That is, the Avaya Oceana® Solution UCA server URL and the Avaya Analytics™ stream server URL must use either an IP address or an FQDN. You cannot use an IP address on one server and the FQDN on the other server.
6. In the **Version** field, select the Avaya Oceana® Solution release that you are managing through Control Manager.
7. 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 the Avaya Oceana Solution on page 127.
8. Click **Save**.

Adding an Avaya Oceana® Solution UCA server to a location

About this task

Control Manager supports multiple Avaya Oceana® Solution UCA server instances. Each Avaya Oceana® Solution UCA server must be assigned to a different location in Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in 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 which you want to add the Avaya Oceana® Solution UCA 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 the **System Type** field, select **Avaya Oceana**.

       The **System Name** field populates the name of the newly created UCAServer Manager Server.
5. Leave the **Sync Schedule** field blank and click **Save**.
6. Click **Confirm** on the Warning message dialog box.

Adding connectors to Provisioning Server

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in 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 the Avaya Oceana® Solution

The Avaya Oceana® Solution requires configuration of token-based access to UCA and OCPDataServices REST APIs. After the configuration has been done, all REST requests must contain a valid token within the request header or the requests are rejected. Token-based access affects Control Manager management of the Avaya Oceana® Solution and agent logins.

About this task

Token enforcement requires that the client of the REST API 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 that it wants 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:

- Install signed certificates on the Control Manager deployment.
- Install the root certificate from the Avaya Breeze® platform cluster hosting the Authorization service as a trusted root certificate authority on the Control Manager application server.
- Import the Control Manager public key into 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.

Before you begin

- Ensure that signed certificates are installed on the Control Manager deployment. For information about certificate installation, see the Control Manager installation and upgrade documents.
- 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.

Procedure

Create trust between Control Manager and the Authorization Service

1. Log on to Windows on the Control Manager server where you must install certificates.
2. Click **Start** > **Run**.

3. In the Run dialog box, type `mmc` and click **OK**.

   The system displays the Microsoft Management Console.
4. In the Console window, click **File** > **Add/Remove Snap-in**.
5. In the Add or Remove Snap-ins dialog box, do the following:
   a. In the Available snap-ins pane, select **Certificates**.
   b. Click **Add**.
6. In the Certificates snap-ins dialog box, do the following:
   a. Select **Computer account**.
   b. Click **Next**.
7. In the Select Computer dialog box, do the following:
   a. Select **Local computer**.
   b. Click **Finish**.
8. In the Add or Remove Snap-ins dialog box, click **OK**.

   The system displays the Certificates snap-in in the Console window.
9. Expand the **Certificates** folder.
10. Click **Trusted Root Certification Authorities** > **All Tasks** > **Import**.

    The system displays the Certificate Import Wizard Welcome screen.
11. Click **Next**.

    The system displays the File to Import screen.
12. Click **Browse** to locate the root certificate you requested from the CA.
13. Click **Next**.
14. Select **Place all certificates in the following store**.
15. Click **Browse** and select **Trusted Root Certification Authorities**.
16. Click **Next**.
17. Click **Finish**.
18. Try accessing the Authorization URL from a browser using the following URL

    `https://`*`BreezeClusterFQDN`*`:9443/services/AuthorizationService/token`

    The link must appear as secure in the browser. If you see Error 401, ignore it.

Add the Authorization client to System Manager

19. Log on to System Manager.
20. Navigate to **Elements** > **Avaya Breeze®** > **Configuration** > **Authorization**.
21. On the Authorization Configuration page, click **New**.

22. On the New External Authorization Client page, do the following:
    1. In the **Name** field, enter the name of the Control Manager server.
    2. In the **Certificate** field, browse to the certificate containing the public key that was exported from the Control Manager certificate manager.
    3. Click **Commit**.

       The new client now appears in the list of authorized clients.

Add Grants to the Control Manager application

23. On the Authorization Configuration page, select the Control Manager client that you added to System Manager.
24. Click **Edit Grants**.
25. On the Edit Grants for Authorization Client page, click **New**.
26. On the Create Grant for Authorization Client page, do the following:
    1. In the **Resource Name** field, select **UCAStoreService**.
    2. In the **Resource Cluster** field, select the cluster that hosts UCAStoreService.
    3. In the **Feature** field, select **ACM**.
    4. In the **Values** field, select the **delete**, **read**, and **write** check boxes.
27. Click **Commit**.
28. On the Edit Grants for Authorization Client page, click **New**.
29. On the Create Grant for Authorization Client page, do the following:
    1. In the **Resource Name** field, select **OCPDataServices**.
    2. In the **Resource Cluster** field, select the cluster that hosts OCPDataServices.
    3. In the **Feature** field, select **access**.
    4. In the **Values** field, select the **read** and **write** check boxes.
30. Click **Commit**.
31. Click **Done**.
32. On the Authorization Configuration page, do the following:
    1. In the **Name** column, locate the entry for the Control Manager client.
    2. 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.

Add Grants to the Authorization Service

33. Navigate to **Elements** > **Avaya Breeze®** > **Configuration** > **Authorization**.
34. Select **AuthorizationService** from the list of clients.

35. Click **Edit Grants**.
36. Click **New**.
37. 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 **UserAuthentication**.
    d. In the **Values** field, select the **read** check box.
38. Click **Commit**.
39. Click **Done**.

Configuring the Control Manager identity

40. Log on to Control Manager.
41. Navigate to **Configuration** > **Avaya Oceana** > **Server Details**.
42. Either double-click the administered Avaya Oceana® Solution UCA server, or select the administered Avaya Oceana® Solution UCA server and click **Edit**.
43. On the Connection Details tab, do the following:
    a. Select the **Enable Authorization** check box.
    b. In the **Authorization Service URL** field, enter the following value:

    ```
    https://BreezeClusterFQDN:9443/services/AuthorizationService/
    token
    ```

    BreezeClusterFQDN is the FQDN of the cluster that hosts the Authorization service.

    c. In the **ACM Instance ID on Breeze** field, enter the ID value of the Control Manager client that you noted from the Authorization Configuration page in System Manager.
44. Click **Save**.

Enable token enforcement in UCA

45. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
46. On the Service Clusters tab, select **UCAStoreService**.
47. In the **Advanced** group, set the **Enable Tokenless Access** attribute to **FALSE**.
48. Click **Commit**.

Assigning a Communication Manager location to the UCA proxy server

About this task

Use this procedure only if Avaya Control Manager servers are segregated based on Communication Manager locations.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in running and accepting state.

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration** > **Services** > **UCA Proxy**.
3. Either 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 Communication Manager 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 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 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 running and accepting state.

Procedure

Perform one of the following steps to view all Providers:

- In your web browser, enter the following URL:

  ```
  https://<AvayaOceanaCluster1_FQDN>/services/UCAStoreService/uca/
  providers
  ```

- 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 the 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 a number of 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® Solution contact routing.

Important:

If you want 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 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® Solution contact routing.

Important:

- If you want use the sample self-service applications or workflows to validate contact routing, you must the add values for the Language, Service and Location categories. For the Location category, you must add the 'Inhouse' value for the sample workflows to function correctly.
- Avaya Oceana® Solution 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 enquiry 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

Ensure that Avaya Oceana® Cluster 1 is in running and accepting state.

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 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. Move the required attributes from the **Available Attributes** list to the **Included Attributes** list.
    c. 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 name 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

- Recommendation 2: Omit system or functional attributes from the name of the service. For example, instead of creating:

Displayname	Attributes
NoviceSupportGroup	Department.Support, AgentExpertise.Novice
RegularSupportGroup	Department.Support, AgentExpertise.Regular
ExpertSupportGroup	Department.Support, AgentExpertise.Expert

Create:

Displayname	Attributes
Support	Department.Support

Configuring Properties in Avaya Control Manager

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in 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.
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 a secure connection between Avaya Control Manager and UCA Server

Obtaining the root certificate from UCA

Procedure

1. In your web browser, enter the following URL:

`https://<AvayaOceanaCluster1_FQDN>/services/UCAStoreService/uca/channels`

The web browser displays an error on the URL bar to indicate that the connection is not secure.

2. Click on the **Insecure Cert** icon and select the root certificate that the system displays.
3. On the Certification Path tab, click **View Certificate**.
4. On the Details tab, click **Copy to File**.
5. On the Certificate Export Wizard screen, perform the following steps:
    a. Click **Next**.
    b. Select the required format for the certificate and click **Next**.
    c. Browse to the location where you want to export the certificate.
    d. Specify a name for the certificate and click **Next**.
    e. Click **Finish**.

Adding the UCA root certificate to the Trusted Root Certification Authorities list on Avaya Control Manager

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/Remove Snap-in 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 left 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 the certificate is placed.
    c. Select the certificate and click **Next**.
    d. Select **Place all certificates in the following store** and click **Next**.

e. Click **Finish**.

Updating the Avaya Oceana® Solution UCA server URL

About this task

After the root certificate is installed on the Avaya Control Manager server, the Avaya Oceana® Solution UCA server URL that is used for the communication between Control Manager and the Avaya Oceana® Solution UCA 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® Solution UCA server, or select the administered Avaya Oceana® Solution UCA 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® Solution deployment and the Avaya Analytics™ deployment are using the same UCA server (Common setup), then the URLs configured for the Avaya Oceana® Solution UCA server must use the exact same URL as the Avaya Analytics™ streams server. That is, the Avaya Oceana® Solution UCA server URL and the Avaya Analytics™ stream server URL must use either an IP address or an FQDN. You cannot use an IP address on one server and the FQDN on the other server.

Configuring Avaya Oceana® Solution system properties using Control Manager

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration** > **Avaya Oceana™** > **Server Details**.
3. Either double-click the administered Avaya Oceana® Solution UCA server, or select the administered Avaya Oceana® Solution UCA 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 OmniDB server as administered in the HTTPS certificate installed on the OmniDB 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 **Https** check box to have a secure communication between Avaya Control Manager and your Omnichannel server.

    ❗ **Important:**

    Verify that you are able to communication with the OmniDB 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.
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. In the **After Contact Work Timer (Seconds)** field, enter the After Contact Work time in seconds.

    The range is 5 to 9999 seconds.
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 webpage 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. The maximum value 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® Solution Release 3.5 to Avaya Oceana® Solution Release 3.6.1.

    c. Select the **Enable mandatory disposition code for contacts** check box to force the agents to set a disposition code on an interaction before ending it.

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 screenpops 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.
22. In the **Avaya Workforce Optimization Select (AWFOS)** area, select the **Avaya Work Force Optimization Select Enabled** check box to indicate that Avaya Workforce Optimization Select is available as part of the Avaya Oceana® Solution deployment.
23. Expand **Thresholds**.
24. In the **Short Not Ready** field, enter the appropriate value in 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 created the not ready reason code in the UCA as the User Codes field. The drop-down contains a list of all user codes created in the UCA.

27. 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.

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 area, do the following:
   a. In the **Omni Channel Database Server** field, enter the FQDN of the Omnichannel Windows 2012 server.

   b. In the **Omni Channel Database Server Port Number** field, enter 443.

   c. Select the **Https** check box to have a secure communication between Avaya Control Manager and your Omnichannel Windows 2012 server.
7. Click **Save**.

Starting Omnichannel Administration Utility

About this task

Use this procedure to start Omnichannel Administration Utility from the Avaya Control Manager web interface.

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. Ensure that you open the Oceana Customer Management Tool using Microsoft Internet Explorer or Microsoft Edge browsers.

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.

Work Codes and Disposition Codes

Work Codes are tags that an agent can set at any point in a contact. Work Codes describe what is going on with the contact at that time. For example, if a customer calls a television service provider to complain about poor service, the agent can tag the first part of the call as

`ServiceComplaint`. After resolving the complaint, the agent can inform the customer about a special offer and tag the call as `UpSell`. If the customer agrees to renew the subscription, the agent can further tag the call as `SubscriptionRenewal`.

Disposition Codes are tags that indicate the final state of the contact when the agent closes the contact. For example, `ComplaintResolved`, `DissatisfiedCustomer`, and `FollowUp`. Agents can also set Disposition Codes during the course of a contact to capture the actions that the agents need to do. For example, `PostBrochure`, `CustomerCallback`, and `LikeOnSocial`.

Defer Codes are tags that an agent can set when deferring an email. For example, `WarehouseContact`, `In-store`, `PhoneRepair`, and `LoyaltyCustomer`.

Chapter 11: Configure Alarms and Events

Configure Alarms and Events

System Manager provides an Operating System (OS)-level SNMP Master (Net-SNMP) agent for platform monitoring, notification sending, and notification destination & SNMPv3 user management.

If you change the Trap Listener settings as an administrator, you must create a new SNMP target profile for the System Manager IP address and a new SNMPv3 user profile for System Manager. The values in the new profiles must match the values in the Trap Listener settings. In addition, you must attach the System Manager SNMPv3 user profile to the System Manager target profile, and then attach the new SNMP target profile to all Serviceability Agents.

For more information about creating SNMP user profiles and target profiles and attaching the target profiles to Serviceability Agents, see *Administering Avaya Aura® System Manager*.

For more information about SNMP, see *Avaya Aura® System Manager Fault Management and monitoring using SNMP*.

Creating an SNMPv3 user profile

About this task

Use this procedure to create a user profile with read and write privileges for SNMP MIBs.

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Serviceability Agents** > **SNMPv3 User Profiles**.
2. On the SNMPv3 User Profiles page, click **New**.
3. On the New User Profile page, perform the following steps:
    a. In the **User Name** field, enter the user name.

    Specify the user name as initial.

    b. In the **Authentication Protocol** field, select the authentication protocol.

    c. In the **Authentication Password** field, enter an authentication password.

    d. In the **Confirm Authentication Password** field, re-enter the authentication password.

    e. In the **Privacy Protocol** field, select the privacy protocol.

f. In the **Privacy Password** field, enter a privacy password.

g. In the **Confirm Privacy Password** field, re-enter the privacy password.

h. In the **Privileges** field, select `Read/Write`.

i. Click **Commit**.

Creating an SNMP target profile

About this task

The System Manager TrapListener service receives traps from different applications and displays the information on the System Manager Alarming page.

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Serviceability Agents** > **SNMP Target Profiles**.
2. On the SNMP Target Profiles page, click **New**.
3. On the New Target Profile page, on the Target Details tab, perform the following steps:
    a. In the **Name** field, enter a name for the target profile.

    b. In the **Description** field, enter a description for the target profile.

    c. In the **IP Address** field, enter the appropriate IP address

    d. In the **Port** field, enter the appropriate port number.

    e. In the **Notification Type** field, select the notification type.

    f. In the **Protocol** field, select the protocol.

    This information must match with the Trap Listener profile. You can view the Trap Listener profile by clicking **Services** > **Configurations** > **Settings** > **SMGR** > **TrapListener**
4. On the New Target Profile page, on the Attach/Detach User Profile tab, perform the following steps:
    a. Select the initial user profile.

    b. Click **Assign**.

    c. Click **Commit**.

Assigning Serviceability Agents

About this task

The Serviceability Agent is an enhanced version of the SAL agent for forwarding logs, harvesting logs, and alarming. The Serviceability Agent sends SNMPv3 traps and notifies the configured NMS destinations. System Manager and the SAL gateway are the two mandatory destinations.

Using the Serviceability Agent user interface you can:

- Manage and configure SNMPv3 users remotely
- Manage and configure SNMP trap destinations remotely
- Create, edit, view, and delete user and target profiles

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Serviceability Agents** > **Serviceability Agents**.
2. On the Serviceability Agents page, select the relevant nodes and click **Manage Profiles**.
3. On the Manage Profile page, perform the following steps:
    a. Select the **SNMP Target Profiles** tab.
    b. Select the SNMP target profile that you created.
    c. Click **Assign**.
    d. Select the **SNMPv3 User Profiles** tab.
    e. Select the user profile that you created.
    f. Click **Assign**.
    g. Click **Commit**.

Verifying the configuration

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Serviceability Agents** > **Serviceability Agents**.
2. Select the nodes for which you want to generate alarms.
3. Click **Generate Test Alarm**.

    System Manager generates a test alarm. You can view the alarm by clicking **Services** > **Events** > **Alarms**.

Chapter 12: Configure Communication Manager and Call Center Elite for Avaya Oceana® Solution

This section provides information about how to configure Communication Manager and Call Center Elite contact center to integrate with Avaya Oceana® Solution. 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® Solution supports the agents in a single Hunt Group on a single Communication Manager. Avaya Oceana® Solution 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® Solution 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® Solution only. There are many other basic administration requirements on Communication Manager that are outside the scope of Avaya Oceana® Solution.
- The starting digit of the calling station must be in both public and private numbering.

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® Solution.

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. Run **`change system-parameters features`**.
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. Run **`change system-parameters customer-options`**.
7. On page 10 of the ASAI PROPRIETARY FEATURES screen, verify that the **Proprietary?** field is set to `y`.

    Note:

    You must use material code 232301 to activate the Proprietary features, for example Agent States.
8. Save the settings.

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® Solution 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. Run **`change route-pattern n`**.

   n is the number of the Route Pattern that you want to configure. The assumption is that there are existing Route Patterns created in Communication Manager.
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. Run **`change locations`**.
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® Solution, 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. Run **`change COR n`**.

   n is the number of COR being used on Communication Manager.
2. Set the **Direct Agent Calling** field to `y`.
3. Save the settings.

Configuring a Hunt Group

About this task

Since all Work Assignment agents must be in a single pool, they must be in the same Hunt Group or Skill. Therefore, you must configure a single Hunt Group for Avaya Oceana® Solution.

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. Run **`add agent-loginID next`** or **`add agent-loginID agent-loginID`**.

   agent-loginID is based on the individual Communication Manager dial plan.
2. 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`.
3. 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.
4. Save the settings.

Configuring Agent Phone-sets

About this task

Use this procedure to configure agent phones to support Avaya Oceana® Solution and Call Center Elite.

Procedure

1. Configure the Avaya Oceana® Solution agent phones to support the following Call Center Elite capabilities:
   - Call Appearance

     Avaya Oceana® Solution 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 13: Configure Application Enablement Services

Configure Application Enablement Services

This section provides information about how to configure Application Enablement Services to enable off-the-shelf and custom integration with Avaya Oceana® Solution.

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.

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

Creating an end entity

Procedure

1. On the System Manager web console, click **Services** > **Security** > **Certificates** > **Authority**.
2. In the left 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® Solution, 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 14: Configure wait treatments for Voice contacts

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® Solution. 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	
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® Solution 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® Solution 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® Solution.

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

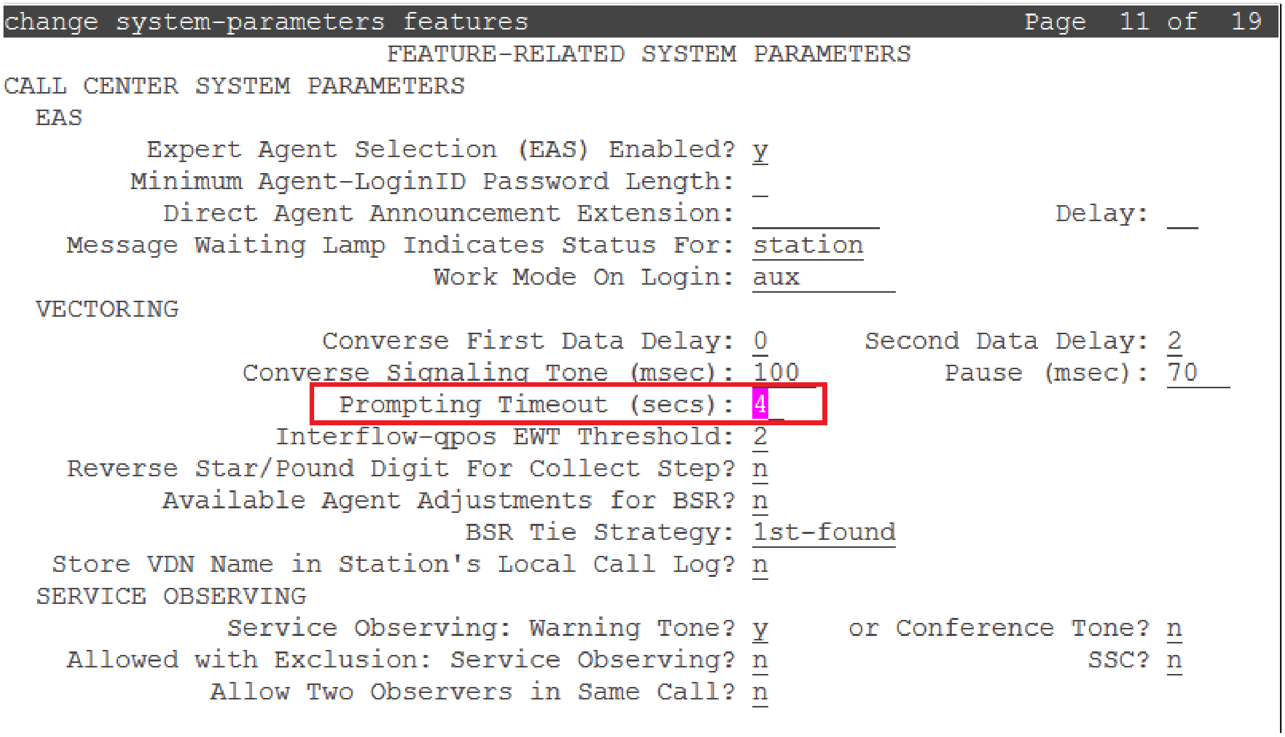
About this task

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® Solution has a number of initial vectors. These vectors require the following variables:

- Routing Vector requires a variable used to collect Agent ID.
- Avaya Oceana® Solution 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® Solution 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® Solution 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® Solution 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`.

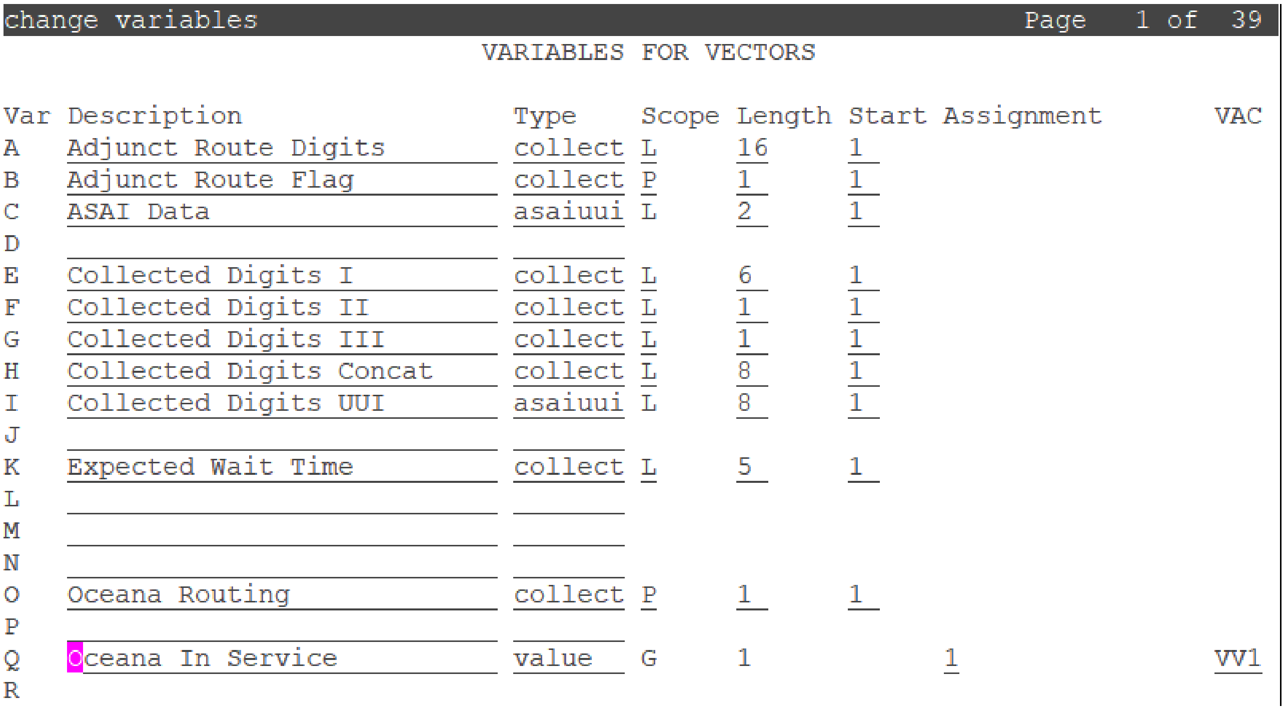
      This value enables you to use a Feature Access Code (FAC) to change the variable assignment. For example, you can use a FAC to take Avaya Oceana® Solution out of service for voice. For more information, see Take Avaya Oceana Solution out of service for voice on page 563.

   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® Solution resources from Avaya DevConnect, refer to the Avaya Oceana® Solution 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, 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 left 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 left 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 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.

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® Solution 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® Solution resources from Avaya DevConnect, refer to the Avaya Oceana® Solution 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:**

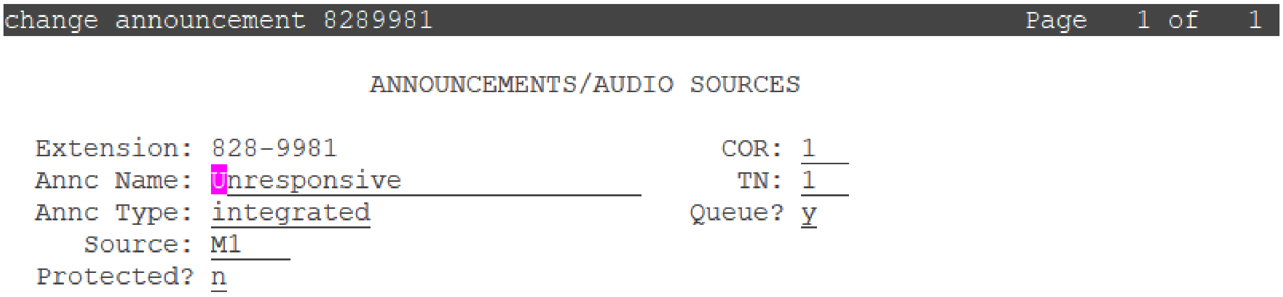
If you use a Media Gateway, you can use the standard procedure to upload the media files.

Procedure

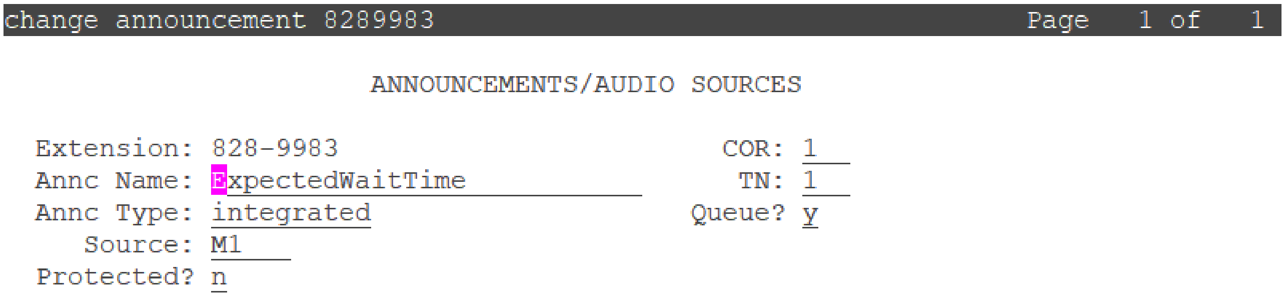
1. Use the System Access Terminal (SAT) interface to add announcements. Use the **`add announcement`** command.
2. In the **Annc Name** field, type the name of the announcement file that you loaded on Avaya Aura® Media Server.
3. In the **Annc Type** field, type `integrated`.
4. In the **Source** field, 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

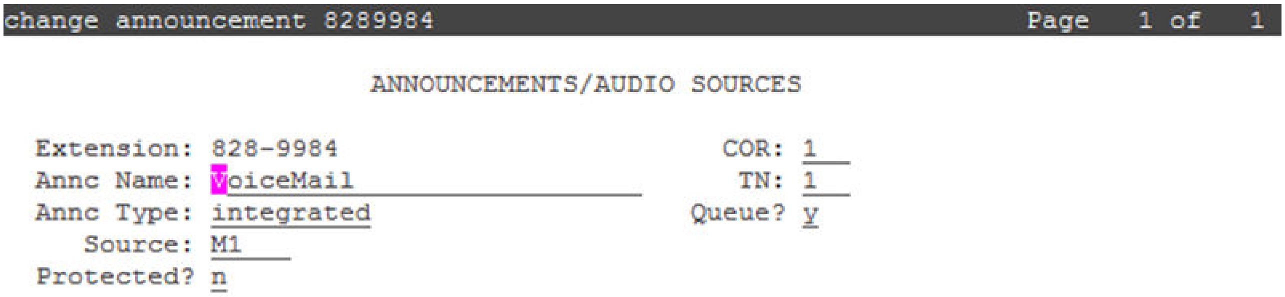
The examples below show announcements for handling cases where fallback to Elite skills-based routing occurs, for advising the customer of expected wait time (EWT) while waiting for an Avaya Oceana® Solution agent, and for offering the option to leave a voice mail.



```
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:

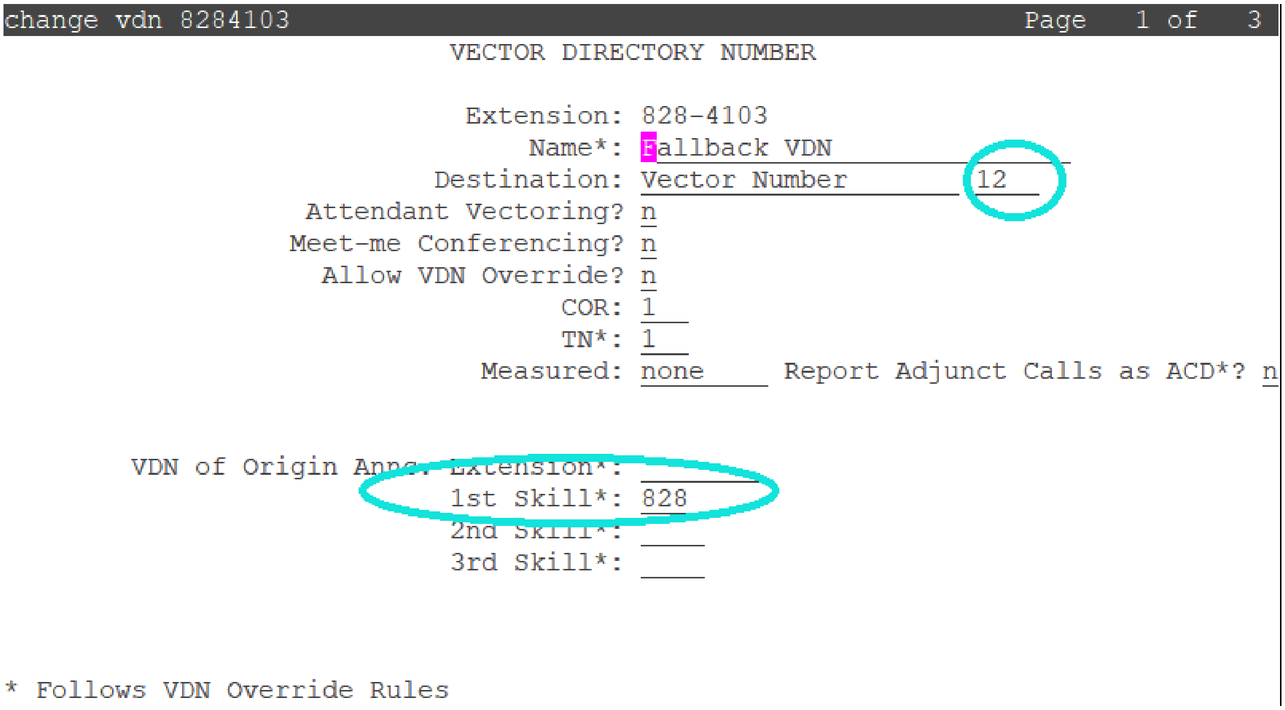
   a. In the **Name** field, enter the name of the VDN.

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



```
change vdn 8284103                                              Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 828-4103
                                 Name*: Fallback VDN
                           Destination: Vector Number        12
                   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 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® Solution is down or call routing fails.

Procedure

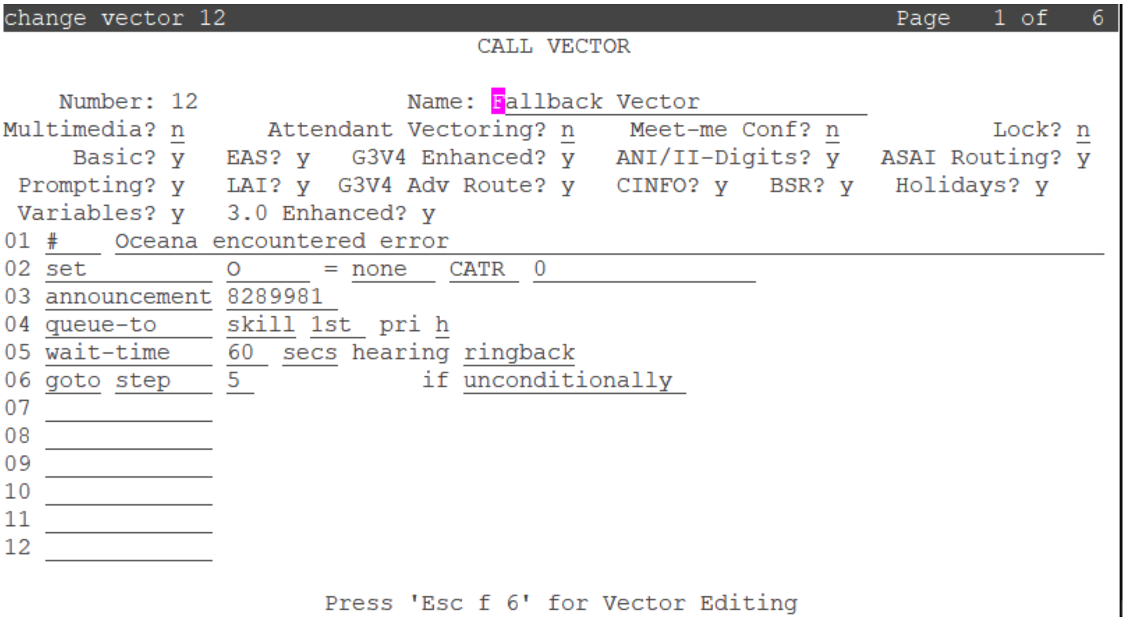
1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.

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          O     = 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.

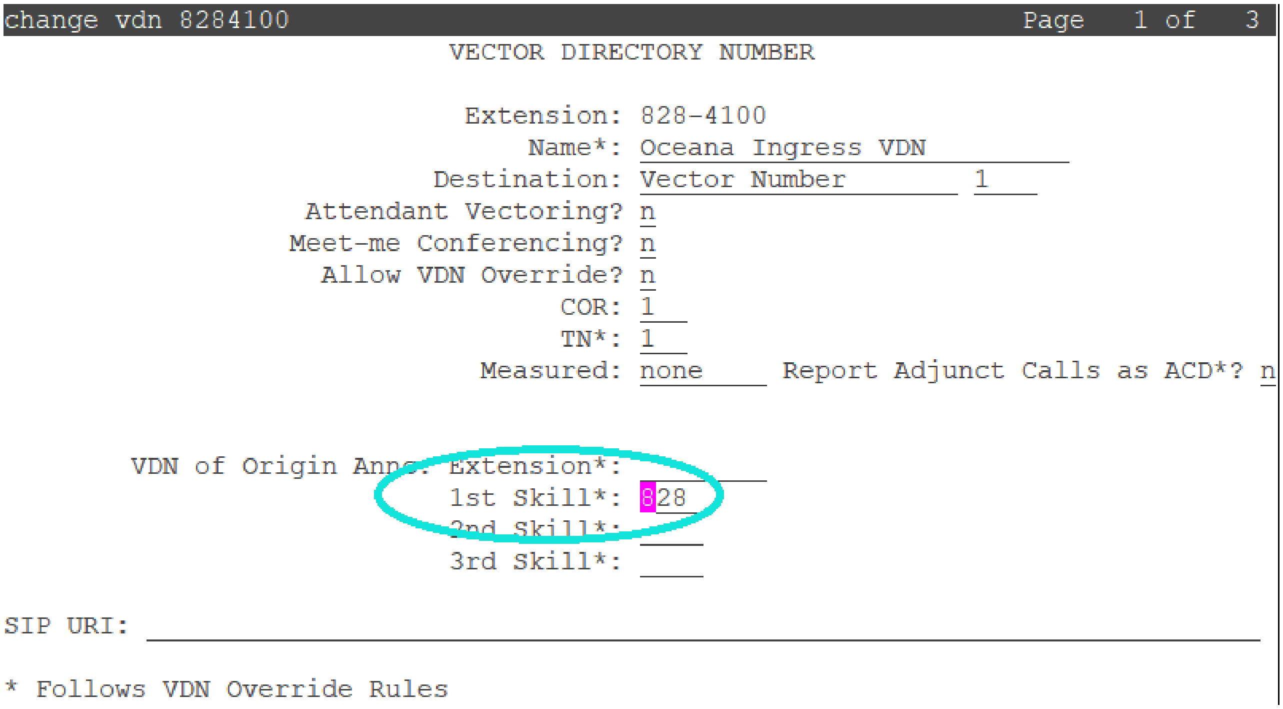
Procedure

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® Solution.

Procedure

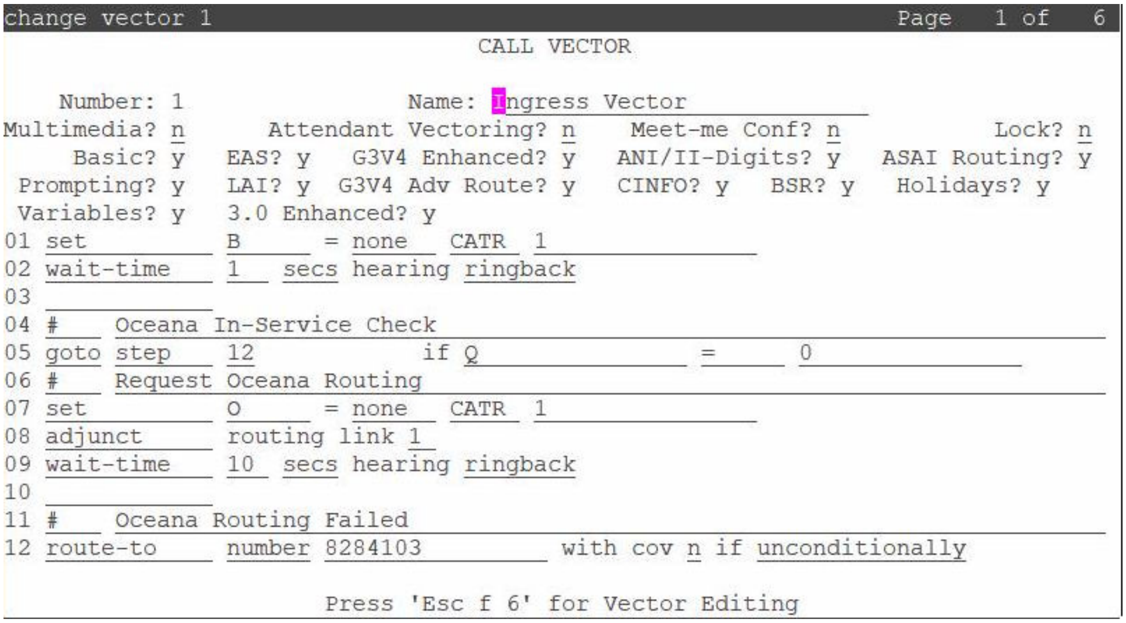
1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change vector n`**.

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:

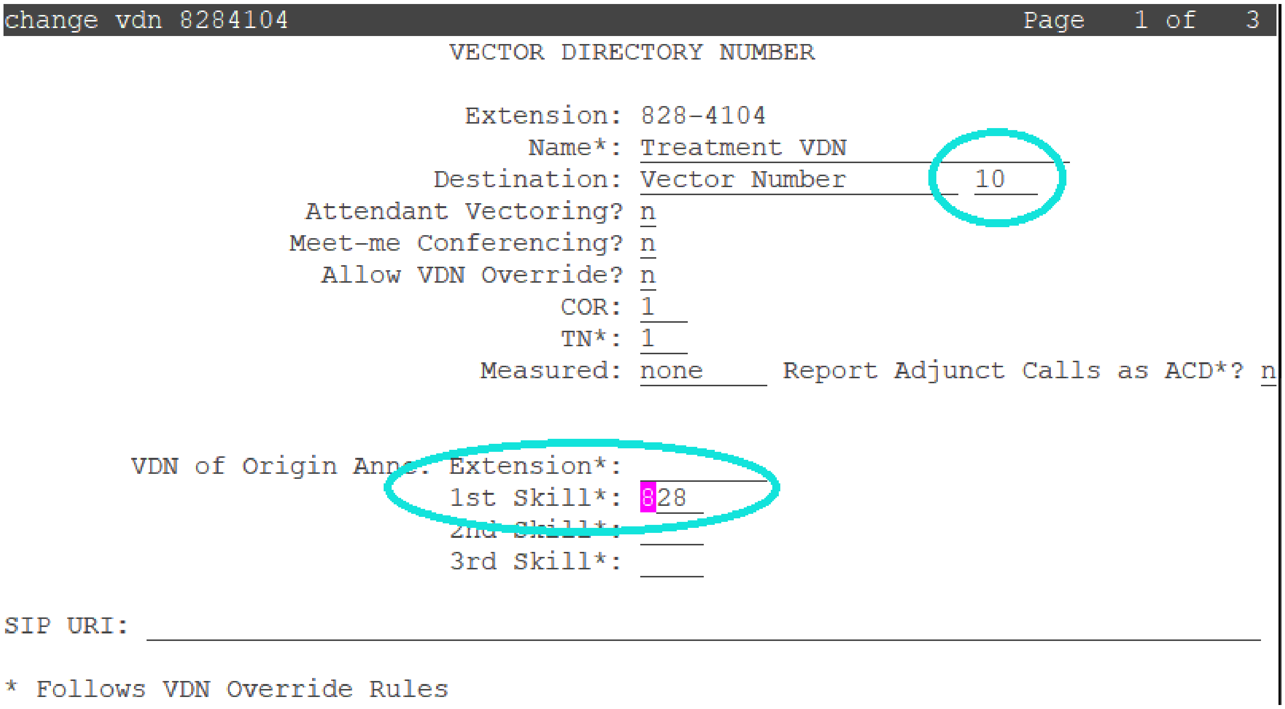
   a. In the **Name** field, enter the name of the VDN.

   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® Solution.

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.

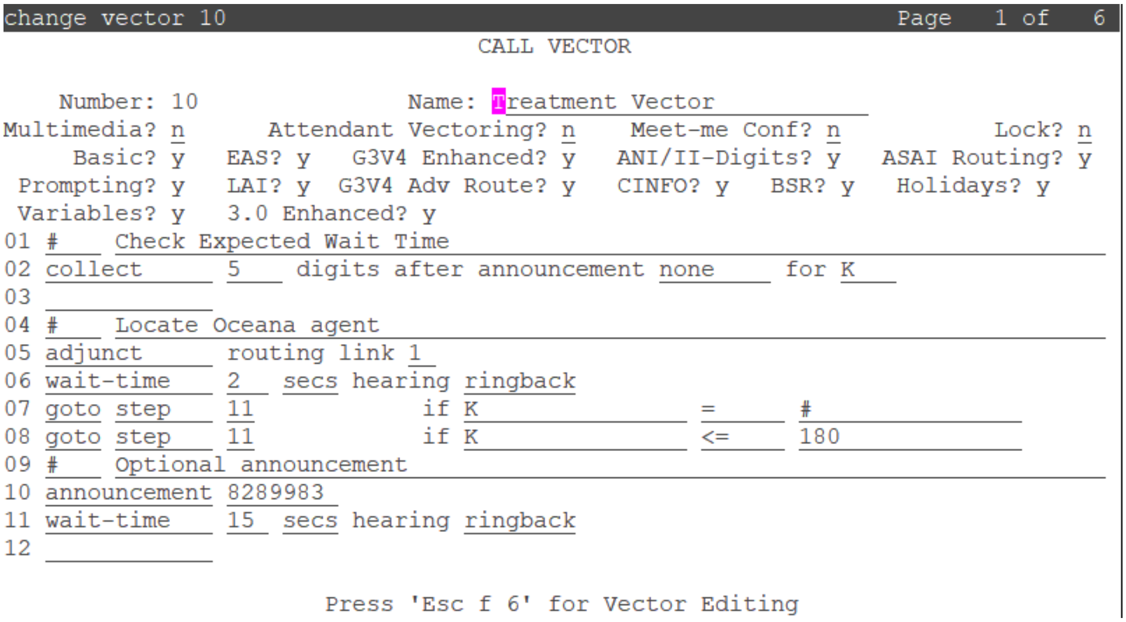
Procedure

1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change vector n`**.

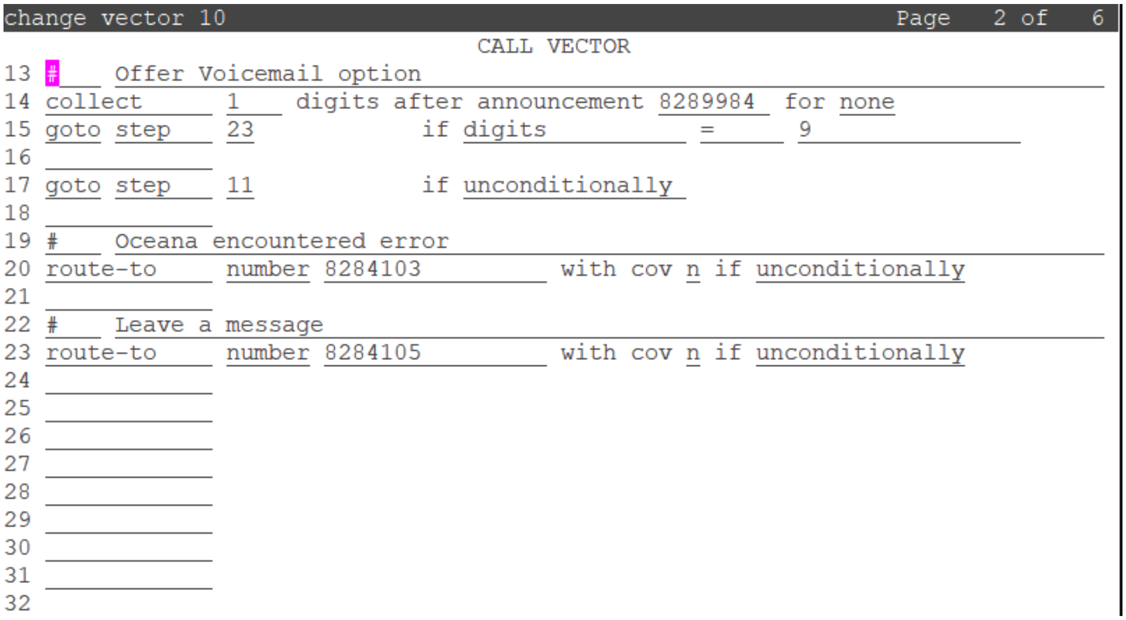
   n is the number that you entered in the **Destination** field of the VECTOR DIRECTORY NUMBER screen while creating the Treatment VDN. In this example, the vector number is 10.
3. On page 1 of the CALL VECTOR screen, perform the following steps:
   a. In the **Name** field, enter the name of the vector 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.

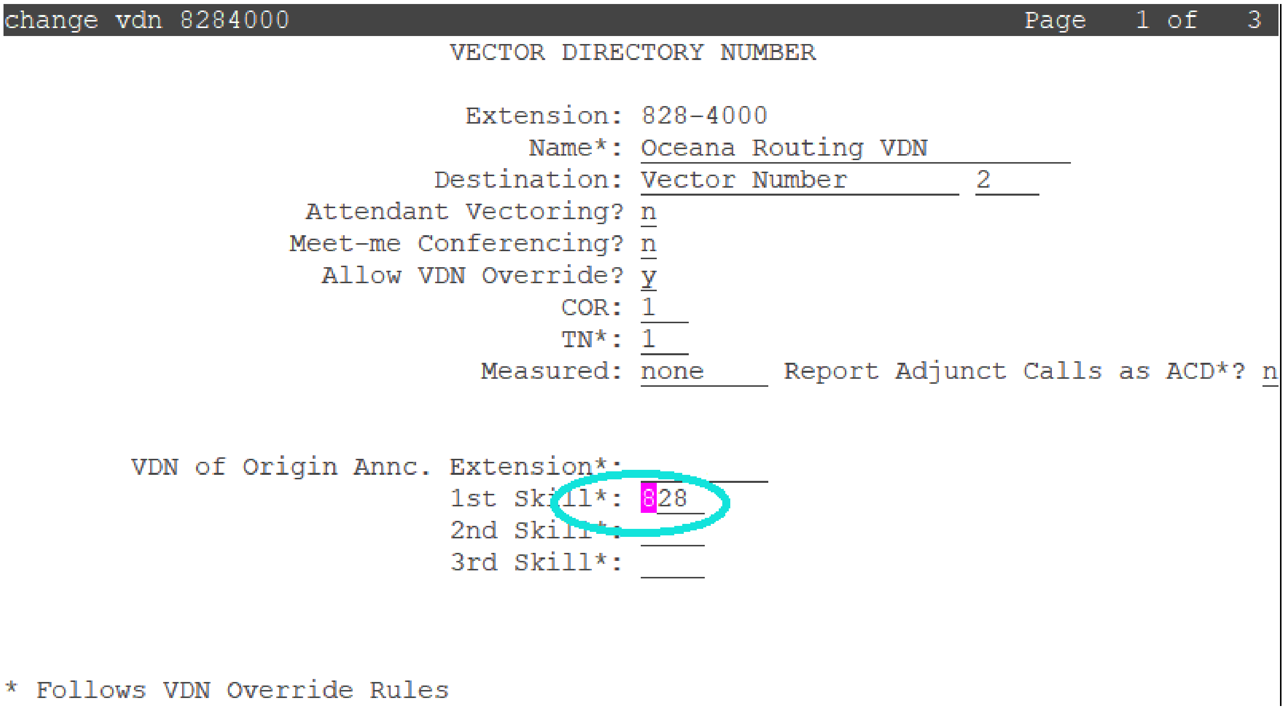
   b. In the **Destination** field, set the destination to a vector number which is not in use. This example uses 2.

   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.

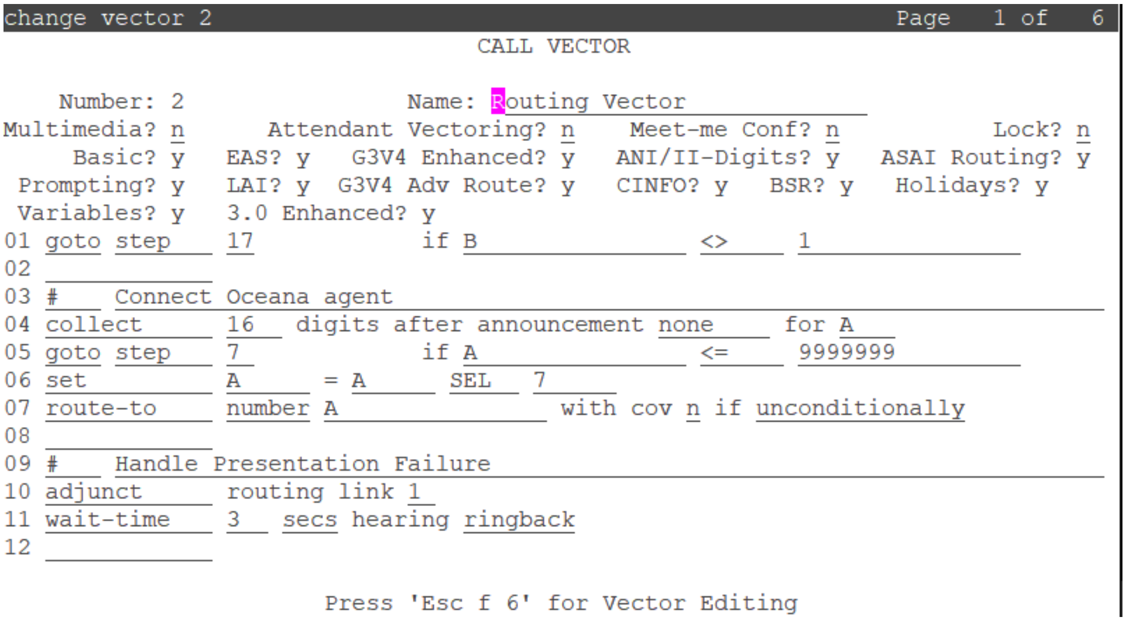
Procedure

1. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change vector n`**.

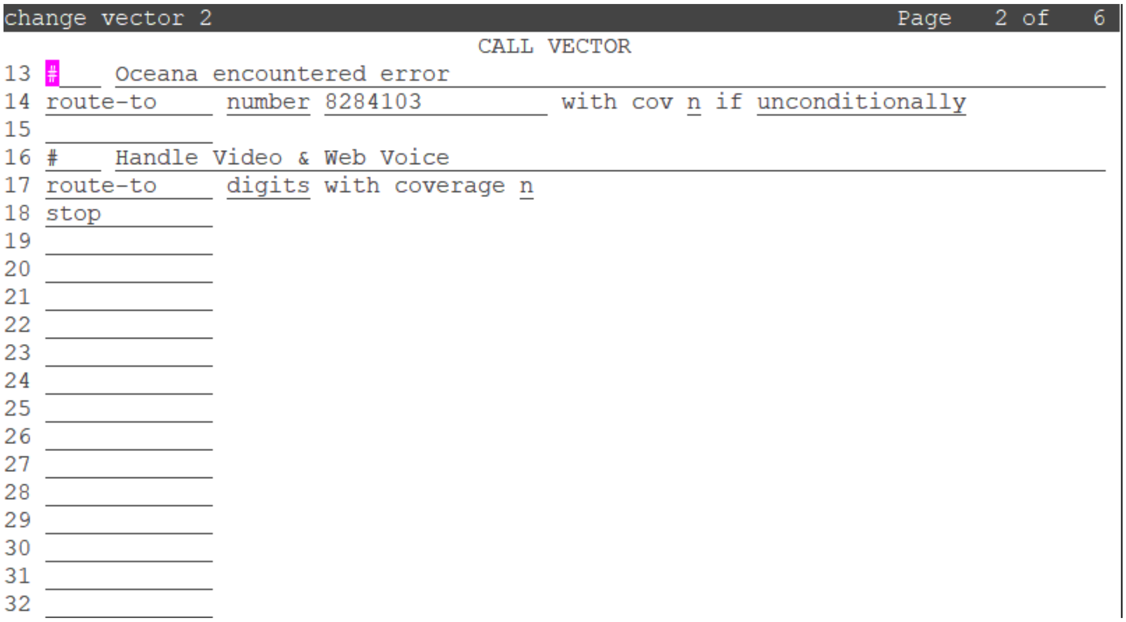
   n is the number that you entered in the **Destination** field of the VECTOR DIRECTORY NUMBER screen while creating the Routing VDN. In this example, the vector number is 2.
3. On page 1 of the CALL VECTOR screen, perform the following steps:
   a. In the **Name** field, enter the name of the vector as `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:

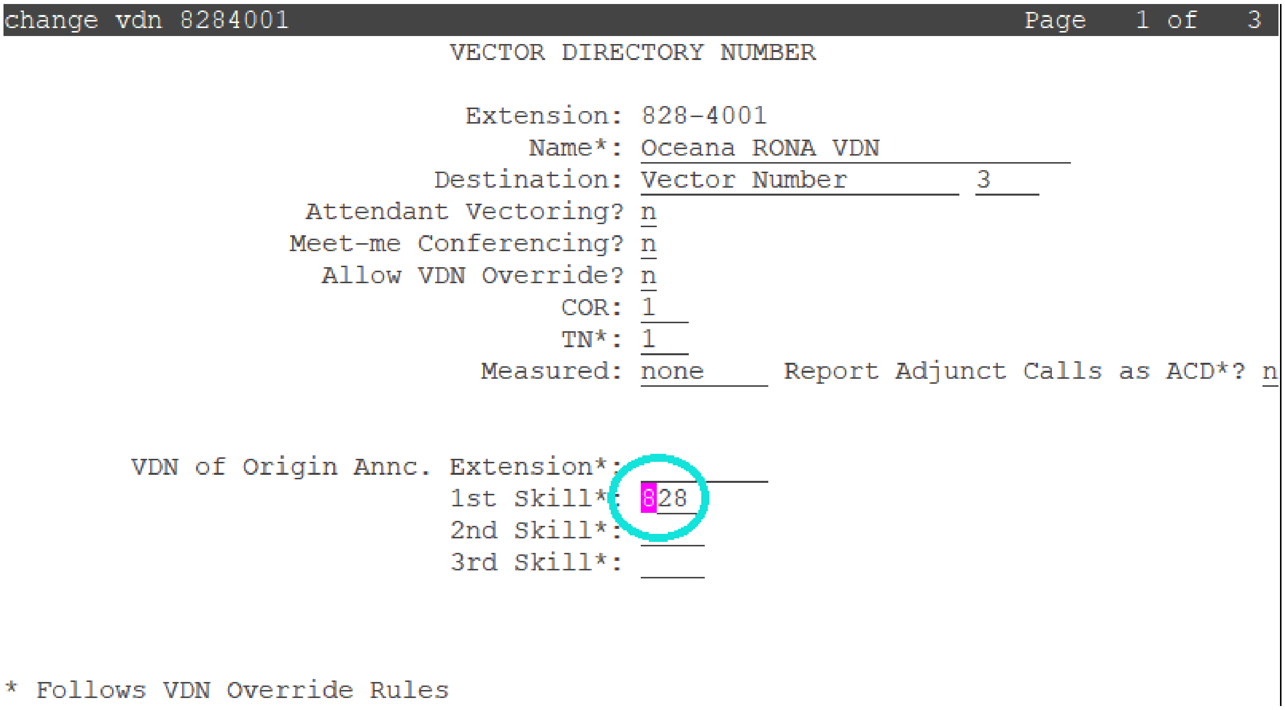
   a. In the **Name** field, enter the name of the VDN.

   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.

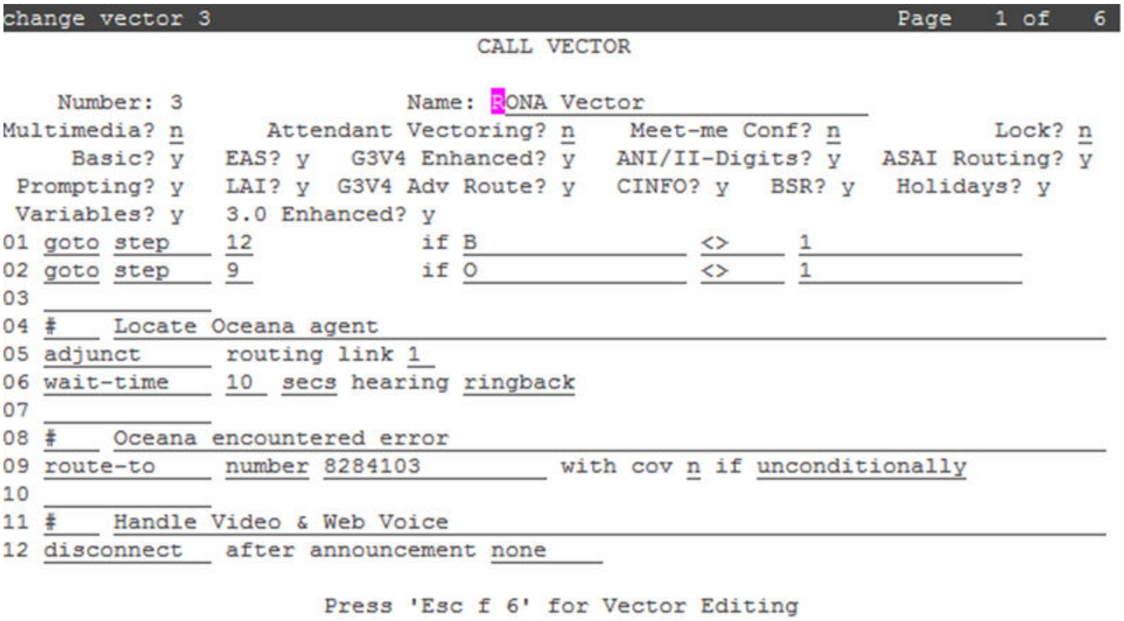
Procedure

1. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change vector n`**.

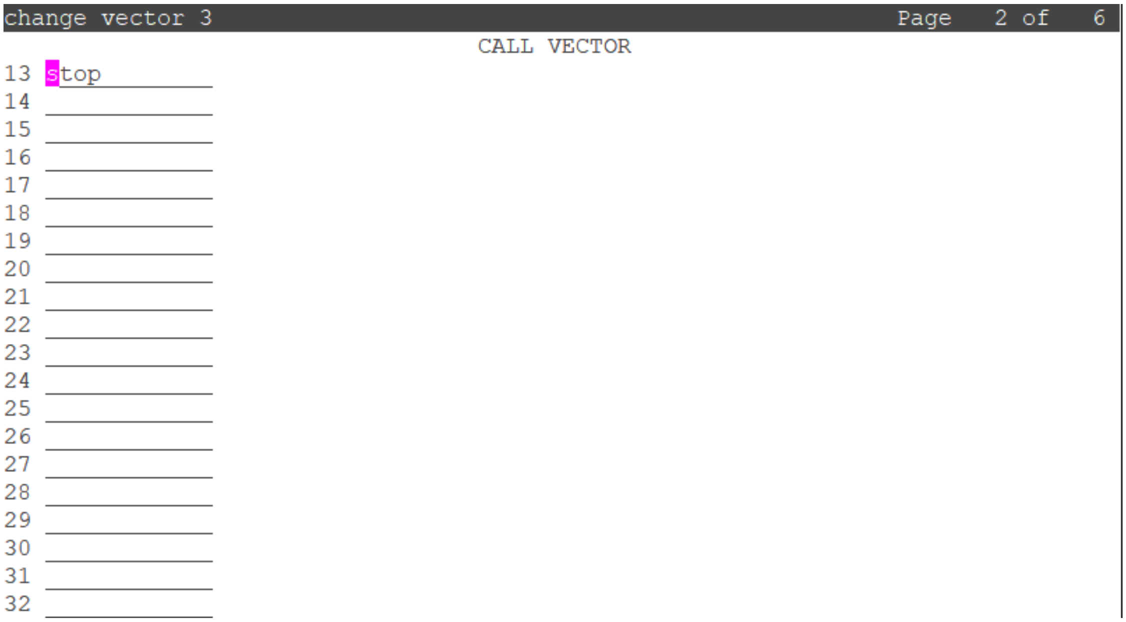
   n is the number that you entered in the **Destination** field of the VECTOR DIRECTORY NUMBER screen while creating the RONA VDN. In this example, the vector number is 3.
3. On page 1 of the CALL VECTOR screen, perform the following steps:
   a. In the **Name** field, enter the name of the vector as `RONA 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® Solution 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® Solution 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.

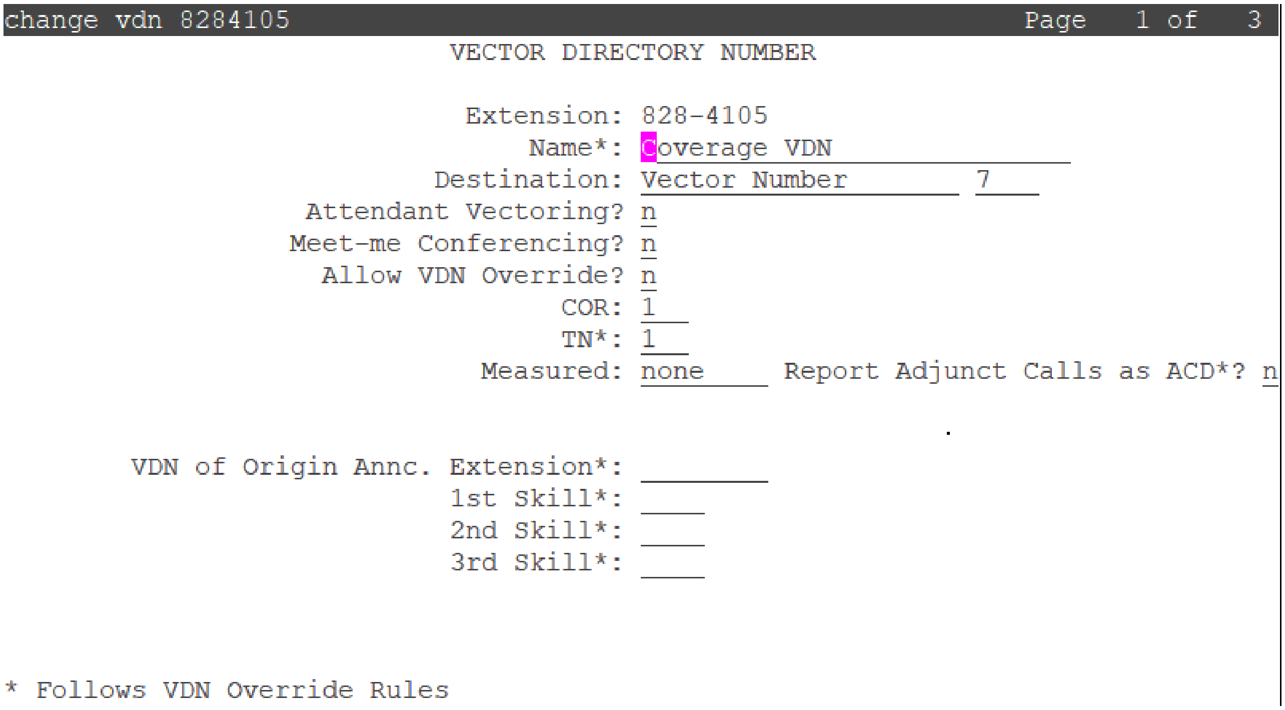
2. On page 1 of the VECTOR DIRECTORY NUMBER screen, perform the following steps:

   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:

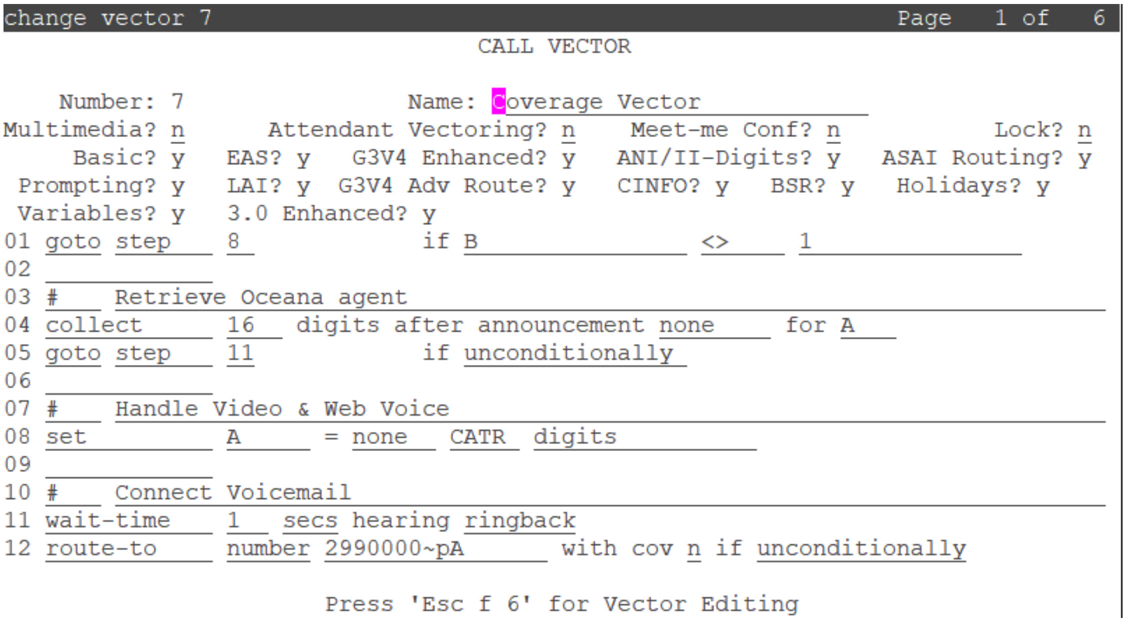
   a. In the **Name** field, enter the name of the vector as `Coverage Vector`.

      This standard name makes maintenance and troubleshooting easier.

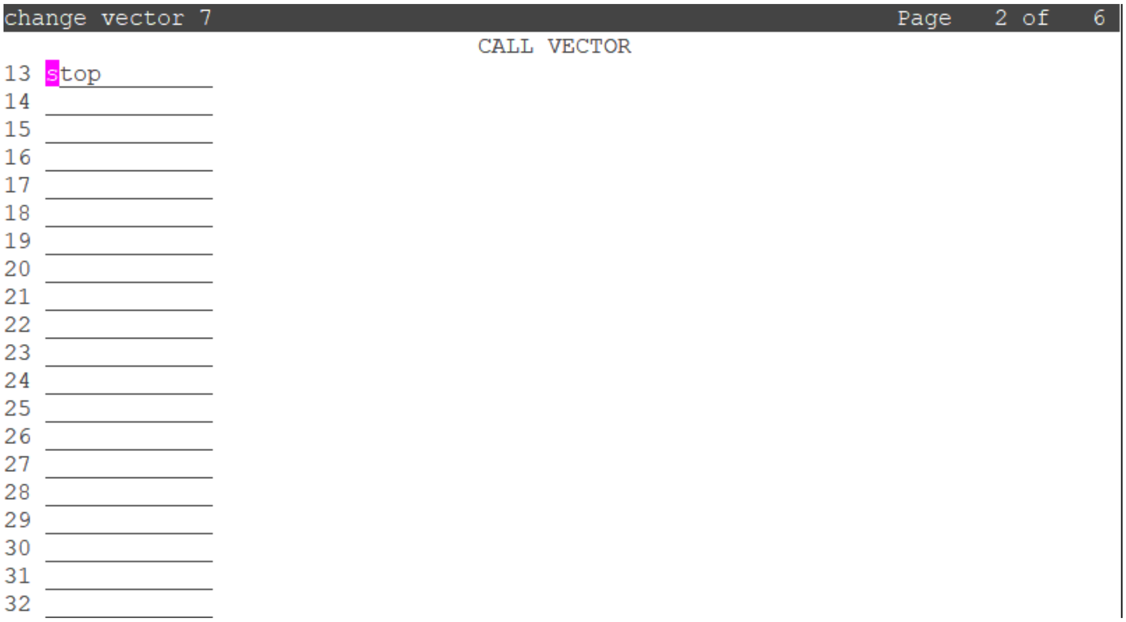
   b. Enter the details required from line 01 to line 13 as shown in the following figure:

      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 176.



```
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 the Transfer Vector Directory Number

About this task

Use this procedure to create the Transfer 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 8284101.

2. On page 1 of the VECTOR DIRECTORY NUMBER screen, perform the following steps:

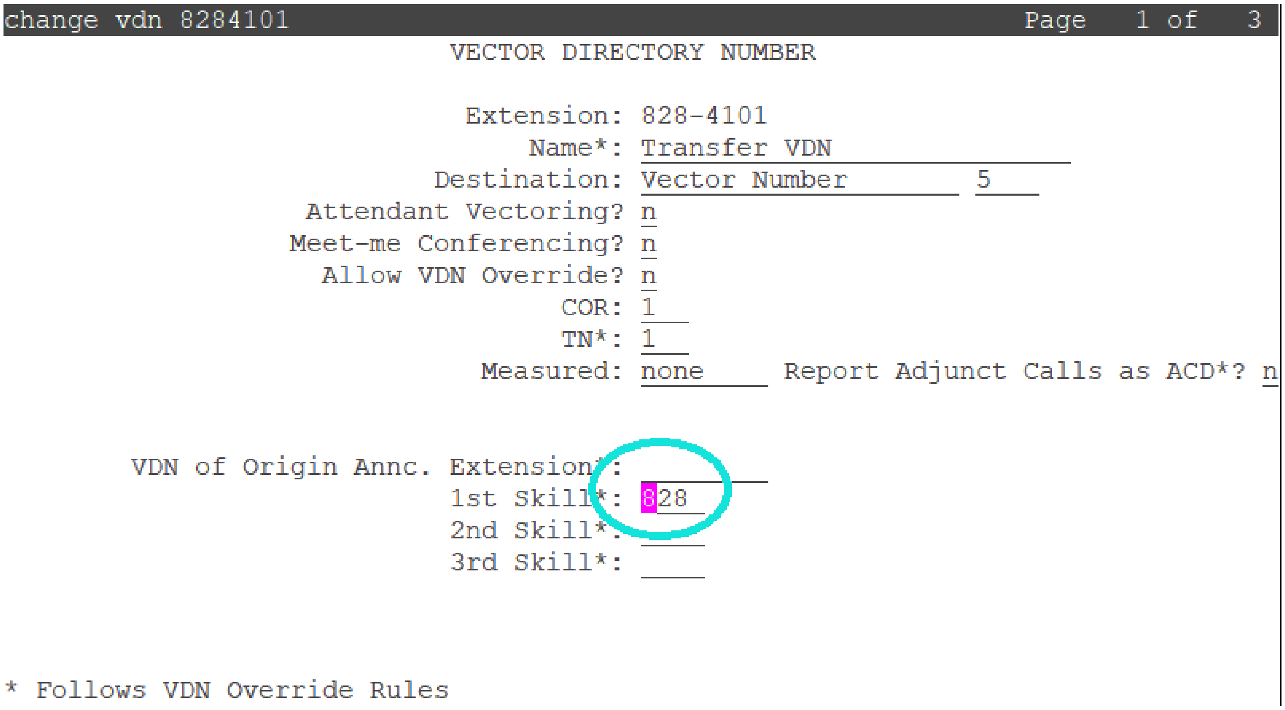
   a. In the **Name** field, enter the name of the VDN.

   b. In the **Destination** field, set the destination to a vector number which is not in use. This example uses 5.

   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 8284101                                              Page   1 of   3
                           VECTOR DIRECTORY NUMBER

                            Extension: 828-4101
                                Name*: Transfer VDN
                          Destination: Vector Number        5
                  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 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® Solution.

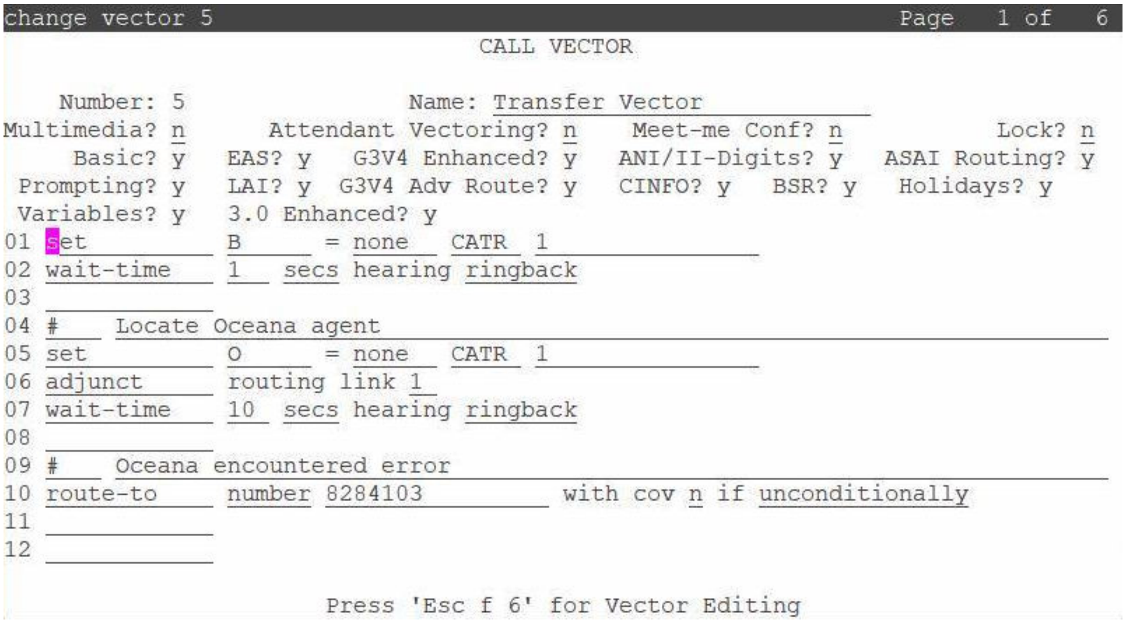
Procedure

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 `Transfer 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:



```
change vector 5                                                  Page   1 of   6
                                  CALL VECTOR

    Number: 5                  Name: Transfer 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 15: Deploy the sample workflows for Voice

Deploying the sample Voice workflow

About this task

Use this procedure to deploy and configure the sample Voice workflow. You can use the same procedure to deploy the other sample workflows of Avaya Oceana® Solution.

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® Solution resources from Avaya DevConnect, refer to the Avaya Oceana® Solution Release Notes.

Procedure

1. In your web browser, enter the following URL to open the Engagement Designer **Designer Console**:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`
2. Click **Import**.
3. On the Import Workflow dialog box, click **Choose File**.
4. Browse to the sample workflow and click **Import**.
5. Click **Save Workflow**.
6. On the Save Workflow dialog box, do the following:
   a. In the **Workflow Name** field, type `OceanaVoiceAssistedService`.

      You can also provide any other name for the workflow.

   b. Select the folder where you want to save the workflow.

   c. Click **Save**.
7. Click **Deploy**.
8. On the Deployment Details dialog box, click **Deploy**.
9. In your web browser, enter the following URL to open the Engagement Designer **Admin Console**:

`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 **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.

    c. 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`.

    d. In the **WaitTime** field, enter the value `20`.

    e. 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.

This example shows how to modify the OceanaVoiceAssistedService workflow for the Treatment VDN used for a customer.

When you deploy the OceanaVoiceAssistedService workflow, Engagement Designer creates an empty rule set called OceanaTreatments. This rule set is available on the Rules tab in the Engagement Designer **Admin Console**.

When 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. However, when you have multiple Treatment VDNs, you must add rules to easily administer which Treatment is applied for a caller, without having to redeploy the workflow.

Before you begin

Deploy the sample Voice workflow.

Procedure

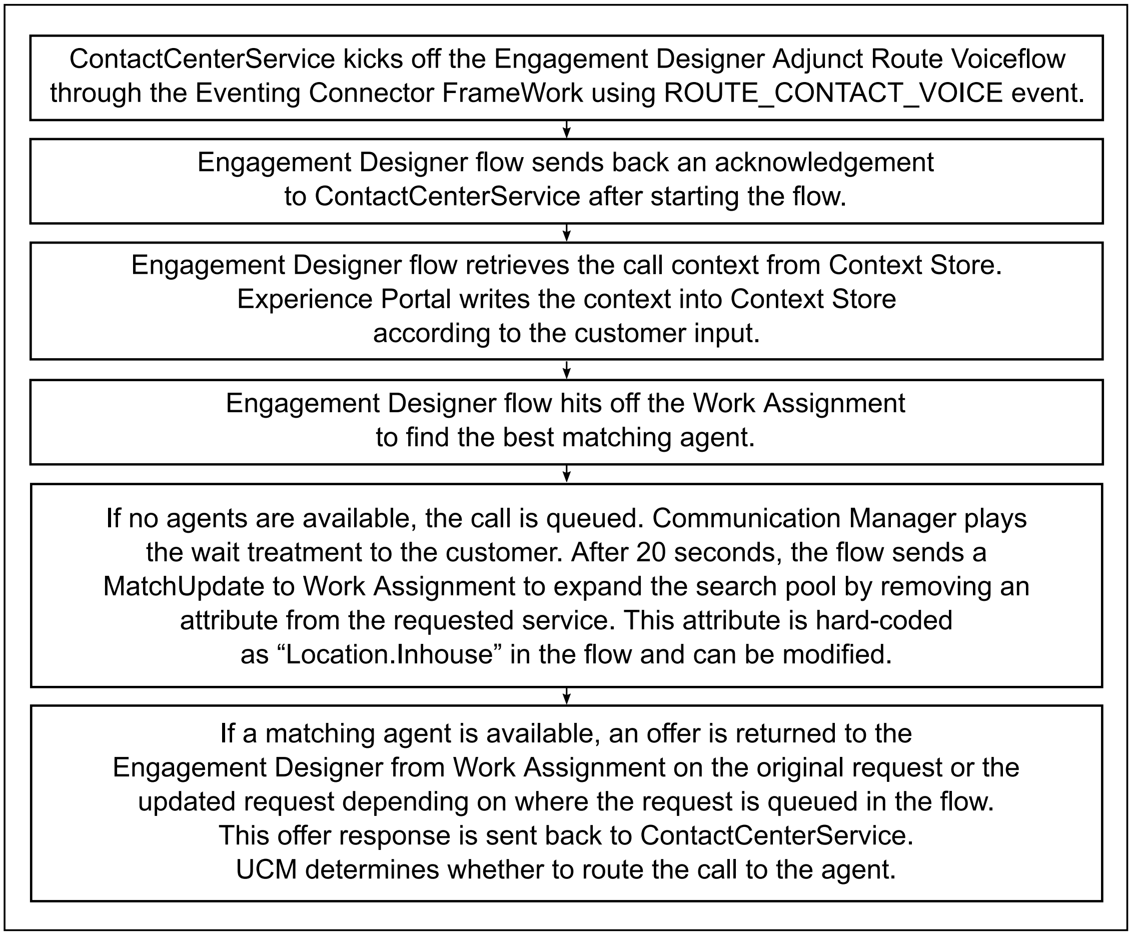
1. In your web browser, enter the following URL to open the Engagement Designer **Admin Console**:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`
2. Select the **Rules** tab.
3. On the Rules tab, click **Create**.

   Engagement Designer displays the Create Rules Editor dialog box.
4. Click the Set RuleSet Name area.
5. In the text box, type a name for the rule set and click the **Check Mark** icon.
6. In the **Select Workflow** field, select the OceanaVoiceAssistedService workflow.
7. Click **Add Rule**.
8. Click the Set Rule Name area.
9. In the text box, type a name for the rule and click the **Check Mark** icon.
10. In the If area, do the following:
    a. In the **Select variable** field, select the variable for the Ingress VDN.
    b. In the **Select function** field, select `is equal to`.
    c. In the **Enter value** field, enter the Ingress VDN.
11. In the Then area, do the following:
    a. Click **Add More**.
    b. In the **Select Variable** field, select the variable for the Treatment VDN.
    c. In the **Enter value** field, enter the Treatment VDN.
12. Click **Save**.
13. Repeat Step 7 to Step 12 to add rules for the other Treatment VDNs.
14. Click **Save**.

Sample Voice workflow

The following diagram depicts the process flow for a Voice workflow:



ContactCenterService kicks off the Engagement Designer Adjunct Route Voiceflow through the Eventing Connector FrameWork using ROUTE_CONTACT_VOICE event.

Engagement Designer flow sends back an acknowledgement to ContactCenterService after starting the flow.

Engagement Designer flow retrieves the call context from Context Store. Experience Portal writes the context into Context Store according to the customer input.

Engagement Designer flow hits off the Work Assignment to find the best matching agent.

If no agents are available, the call is queued. Communication Manager plays the wait treatment to the customer. After 20 seconds, the flow sends a MatchUpdate to Work Assignment to expand the search pool by removing an attribute from the requested service. This attribute is hard-coded as “Location.Inhouse” in the flow and can be modified.

If a matching agent is available, an offer is returned to the Engagement Designer from Work Assignment on the original request or the updated request depending on where the request is queued in the flow. This offer response is sent back to ContactCenterService. UCM determines whether to route the call to the agent.

Figure 3: Sample Voice workflow

Note:

To customize the wait time of 20 seconds, you must open the Engagement Designer administration web console, select the workflow on the Workflows tab, and click **Attributes**.

Deploying the sample Transfer to Service workflow for Voice

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® Solution resources from Avaya DevConnect, refer to the Avaya Oceana® Solution 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 Engagement Designer **Designer Console**:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`

2. Click **Import**.
3. On the Import Workflow dialog box, click **Choose File**.
4. Browse to the sample workflow and click **Import**.
5. Click **Save Workflow**.
6. On the Save Workflow dialog box, do the following:
   a. In the **Workflow** field, type `OceanaVoiceTransfer`.

      You can also provide any other name for the workflow.

   b. Select the folder where you want to save the workflow.
   c. Click **Save**.
7. Click **Deploy Workflow**.
8. On the Deployment Details dialog box, click **OK**.
9. In your web browser, enter the following URL to open the Engagement Designer **Admin Console**:

   `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_TO_SERVICE**.

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**.

    The system displays the newly created rule in the list of rules.

Chapter 16: Configure Voice Self Service for Avaya Oceana® Solution

In Avaya Oceana® Solution, you can use any of the following options for Voice Self Service:

- Avaya Aura® 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 134 and Adding Attributes to Avaya Control Manager on page 135.

Configure Avaya Aura® Experience Portal

Avaya Aura® Experience Portal provides an Interactive Voice Response (IVR) front-end for voice calls in Avaya Oceana® Solution.

To install and commission Experience Portal, see:

- *Implementing Avaya Aura® Experience Portal on a single server*
- *Implementing Avaya Aura® Experience Portal on multiple servers*
- *Deploying Avaya Aura® Experience Portal in an Avaya Customer Experience Virtualized Environment*
- *Administering Avaya Aura® Experience Portal*

Sample Self-Service Application (SSA)

Avaya provides a sample Voice Self-Service Application (SSA) as part of Avaya Oceana® Solution. 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® Solution.

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.

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 `runtimeSupportTomcat8.zip` file containing the run-time support files 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.

2. On the application server, go to the `<TOMCAT_HOME>` folder and unzip the `runtimeSupportTomcat8.zip` file.

   The system extracts the run-time support jars to the `<TOMCAT_HOME>/runtimeSupportTomcat8/lib` folder.

3. From the `<TOMCAT_HOME>/runtimeSupportTomcat8/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 Aura® 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:
   1. On the command line, type `cd /opt/AppServer/tomcat/bin` and press **Enter**.
   2. Type `./shutdown.sh` and press **Enter**.
   3. After waiting for a few seconds, type `./startup.sh` and press **Enter**.
5. **(Optional)** If you use the web interface method, do the following:
   1. On the Experience Portal Management web console, click **System Management** > **Application Server**.
   2. Select the check box for the application server that you want to restart and click **Stop**.
   3. 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® Solution, 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® Solution, 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® Solution 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 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 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 Context Store PDC plug-in is 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, click **Context Store Connector**.
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 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 Context Store PDC plug-in, see *Avaya Context Store Snap-in Developer's Guide*.

Next steps

Customize the Avaya Oceana® Solution sample Self-Service Application to your requirements using the Orchestration Designer flows.

For more information, see:

- *Getting Started with Avaya Aura® Orchestration Designer*
- *Avaya Aura® Orchestration Designer Developer's Guide*
- *Administering Avaya Aura® Experience Portal*
- *Avaya Context Store Snap-in Developer's Guide*

Exporting the sample application project

Before you begin

Stop the Tomcat server on the Avaya Aura® 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® Solution, 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® Solution 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® Solution resources from Avaya DevConnect, refer to the Avaya Oceana® Solution 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® Solution resources from Avaya DevConnect, refer to the Avaya Oceana® Solution 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.

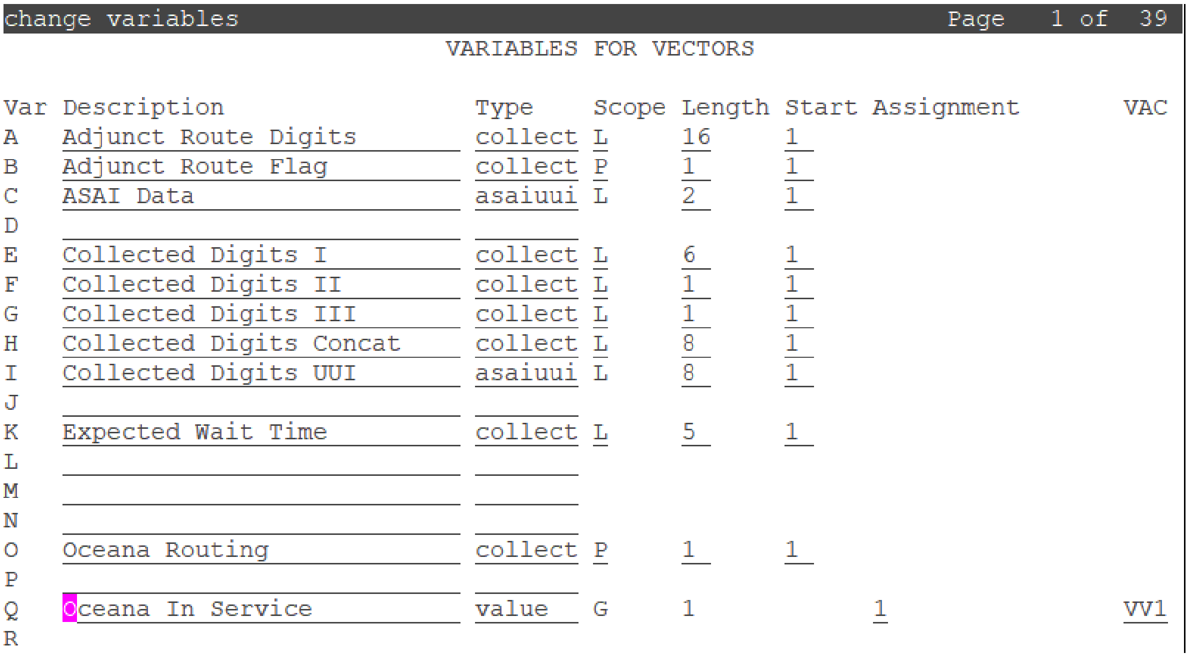
If the variables used in this example are already in use on Communication Manager, use different variables. Ensure that you use these different variables in your Avaya Oceana® Solution vectors.

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

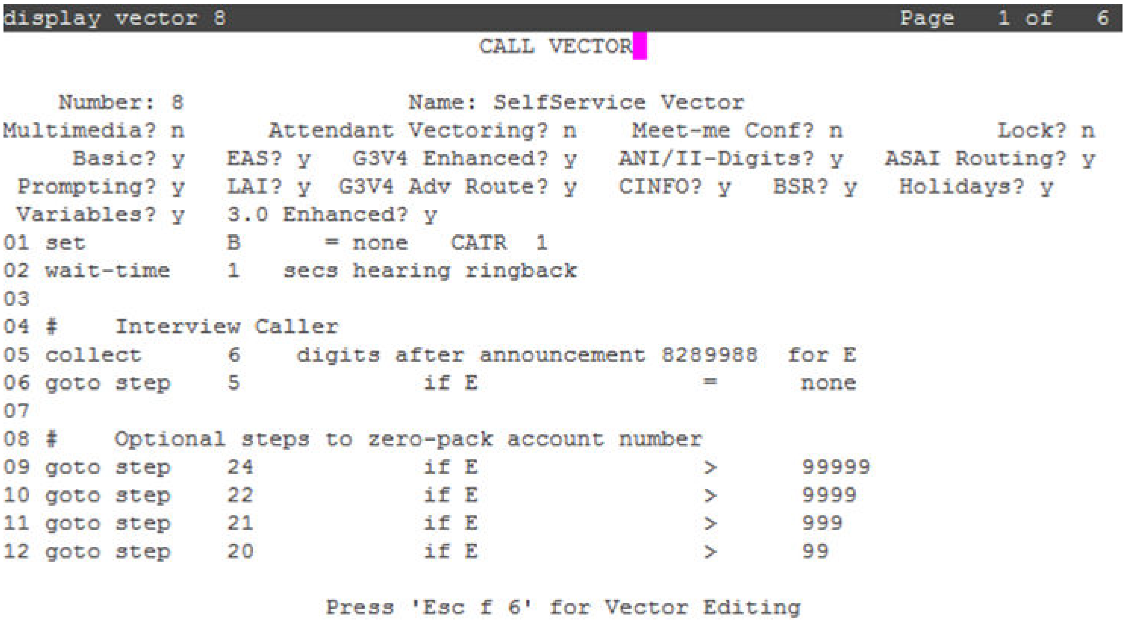
1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change vector n`**.

   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:

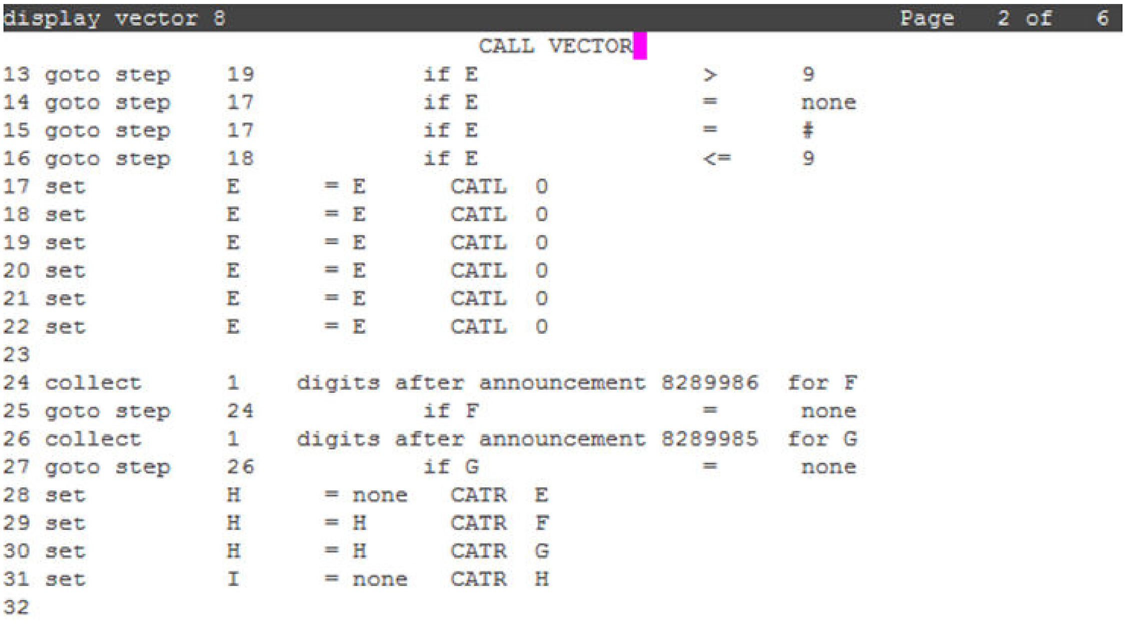
   a. In the **Name** field, enter the name of the vector as `SelfService Vector`.

   This standard name makes maintenance and troubleshooting easier.

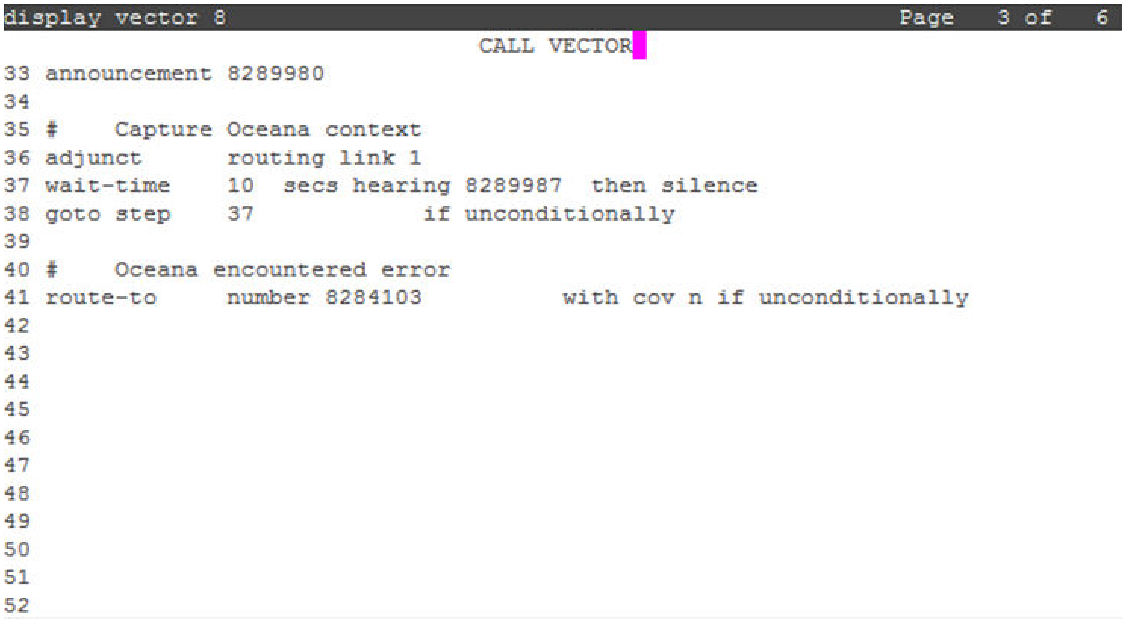
   b. Enter the details required from line 01 to line 41 as shown below:



```
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 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® Solution resources from Avaya DevConnect, refer to the Avaya Oceana® Solution 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 Engagement Designer **Designer Console**:

```
https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/
index.html
```

2. Click **Import**.
3. On the Import Workflow dialog box, click **Choose File**.
4. Browse to the sample workflow and click **Import**.
5. Click **Save Workflow**.
6. On the Save Workflow dialog box, do the following:
    a. In the **Workflow** field, type `OceanaVoiceSelfService`.

       You can also provide any other name for the workflow.

    b. Select the folder where you want to save the workflow.
    c. Click **Save**.
7. Click **Deploy Workflow**.
8. On the Deployment Details dialog box, click **OK**.
9. In your web browser, enter the following URL to open the Engagement Designer **Admin Console**:

    ```
    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. On 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® Solution, keep the default value `True`.
    - For a Voice-only deployment of Avaya Oceana® Solution, 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**.

    The system 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® Solution 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 209
- Creating the SelfService Vector Directory Number on page 210
- Configuring a vector for the SelfService VDN on page 211
- Adding the SelfService VDN to Avaya Control Manager on page 213

Chapter 17: Configure Callback Assist

Callback Assist overview

Callback Assist integrates with Avaya Oceana® Solution 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 voicemail 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.

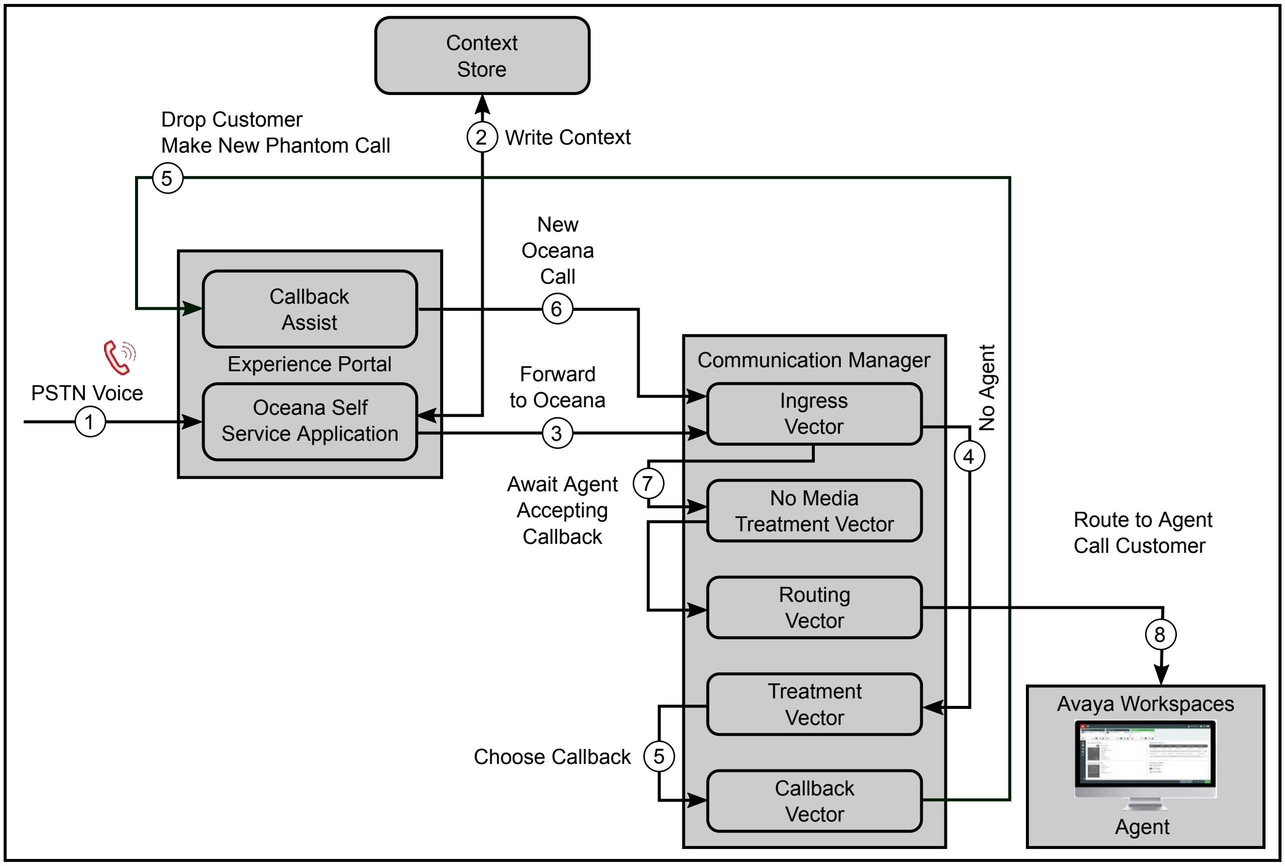
For the Immediate callback option, Callback Assist makes a new media-less call to Avaya Oceana® Solution for routing to a suitable agent. After the agent answers the call, the customer is out-dialled and connected to the agent.

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 Oceana®-specific parameters

About this task

Use this procedure to set the parameters that are specific to Avaya Oceana® Solution.

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® Solution.

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® Solution 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® Solution.
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.

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

Use this procedure to 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 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 Callback applications in Experience Portal

About this task

Use this procedure to add the following applications in Experience Portal and ensure that the shared UUI option is set for these applications:

- OceanaCallback
- Outbound Callback

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, specify the name of the Outbound Callback application that you noted down from the Avaya Callback Assist Administration interface.
5. In the **Type** field, select `CCXML`.
6. In the **CCXML URL** field, enter the following value:

   `http://`*`<IP address of the Callback Assist server>`*`:8080/CBAScripts/cbaCallControl`
7. In the Speech Servers area, in the **TTS** field, select `No TTS`.

8. In the **Application Launch** field, select `Outbound`.
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 **OceanaCallback** row, click the **Edit** icon.
15. In the **CBA Offer Application URL** field, enter the following value:

    ```
    http://<IP address of the Callback Assist server>:8080/CBAIPOffer/Start
    ```
16. In the **Emergency Destination** field, enter the Fallback VDN or an appropriate emergency destination.
17. In the **Callback Configuration DNIS or OD ApplicationName for Experience Selection** field, enter the appropriate value.
18. In the **Vpms** field, enter the IP address of the EPM server.
19. Click **Save**.

Verifying the dial plan for Avaya Oceana® Solution

About this task

Use this procedure to verify that the dial plan for Avaya Oceana® Solution 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

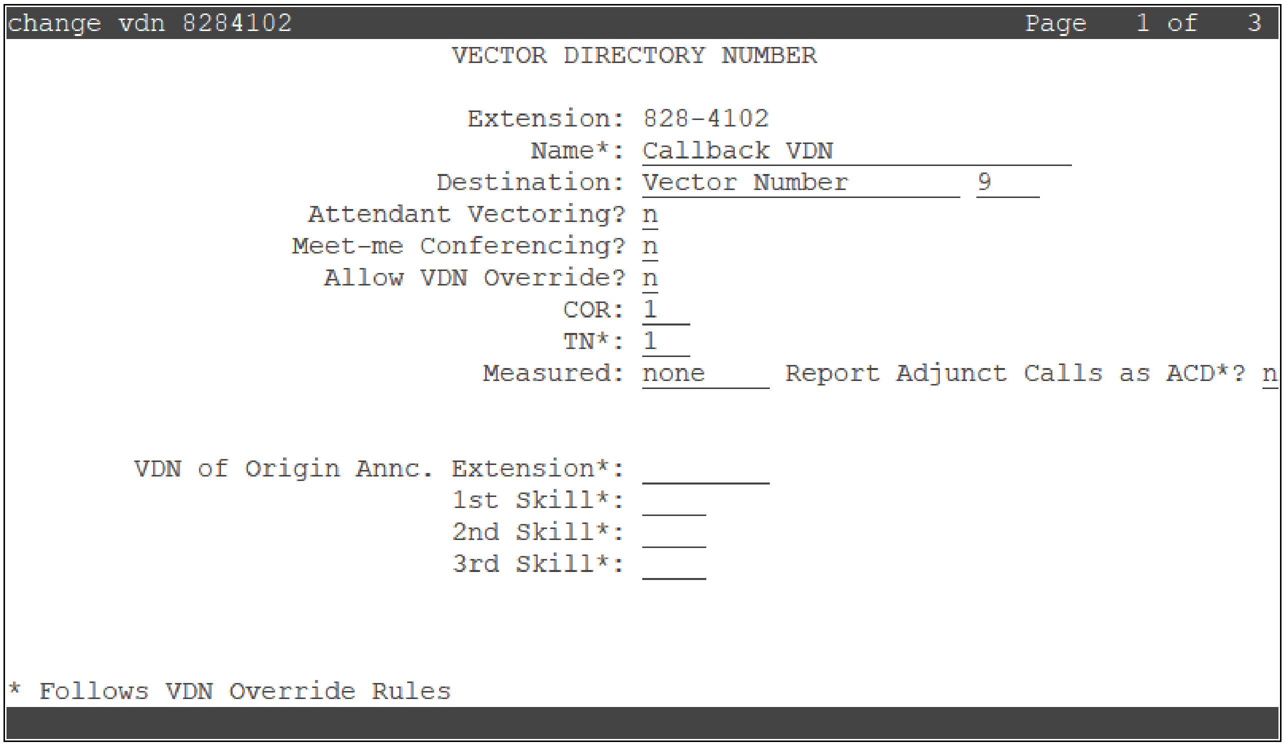
Use this procedure to create the Callback Vector Directory Number (VDN).

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.

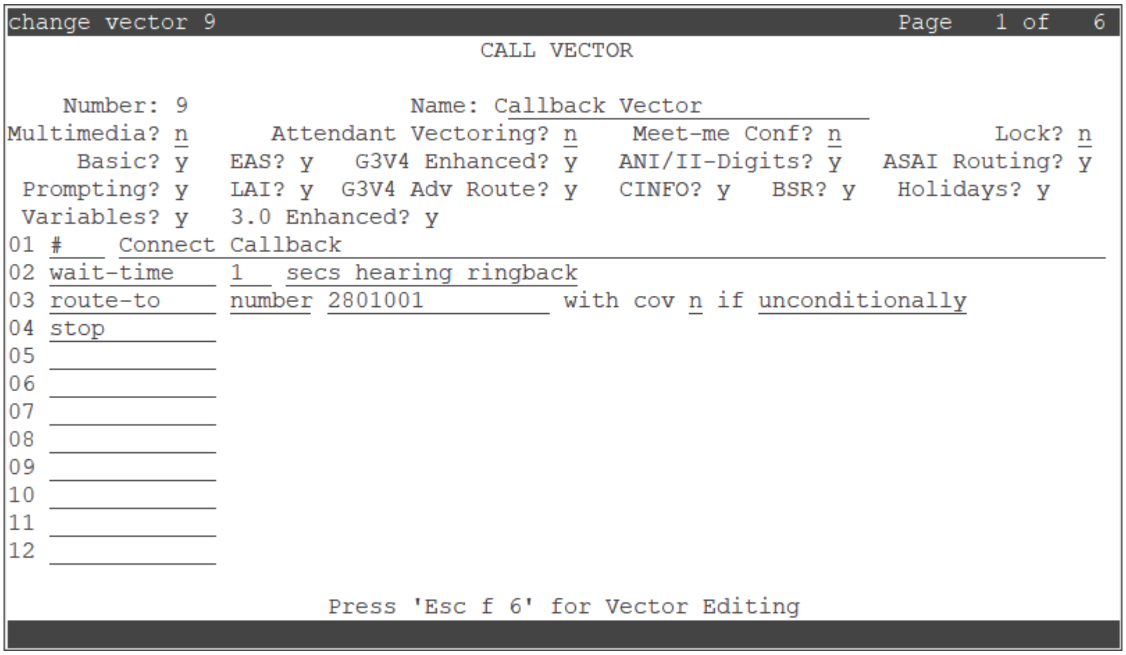
Procedure

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

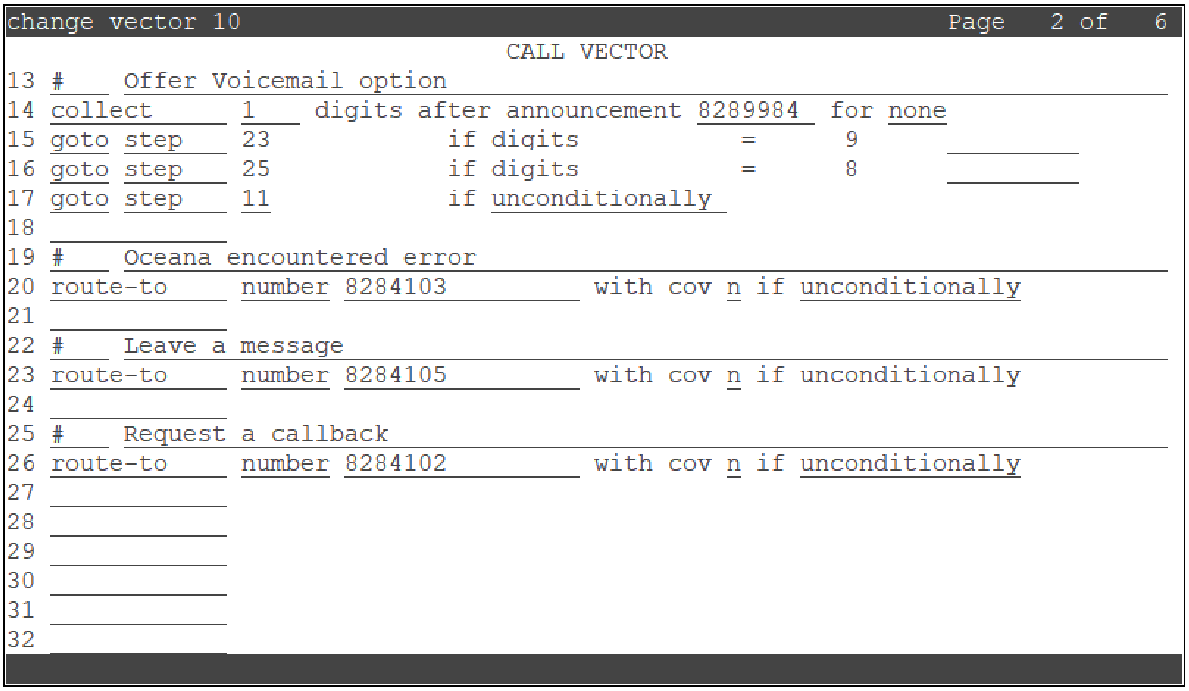
About this task

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 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

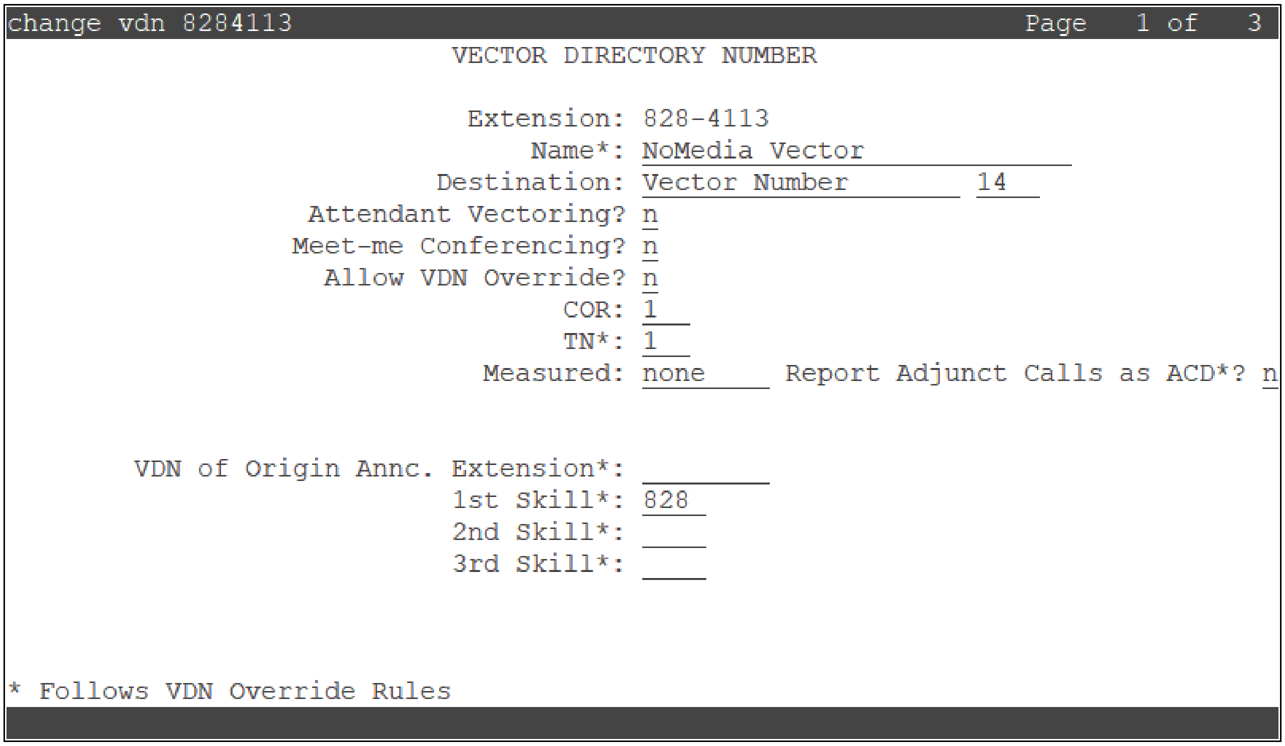
Use this procedure to create the No Media Treatment Vector Directory Number (VDN).

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.

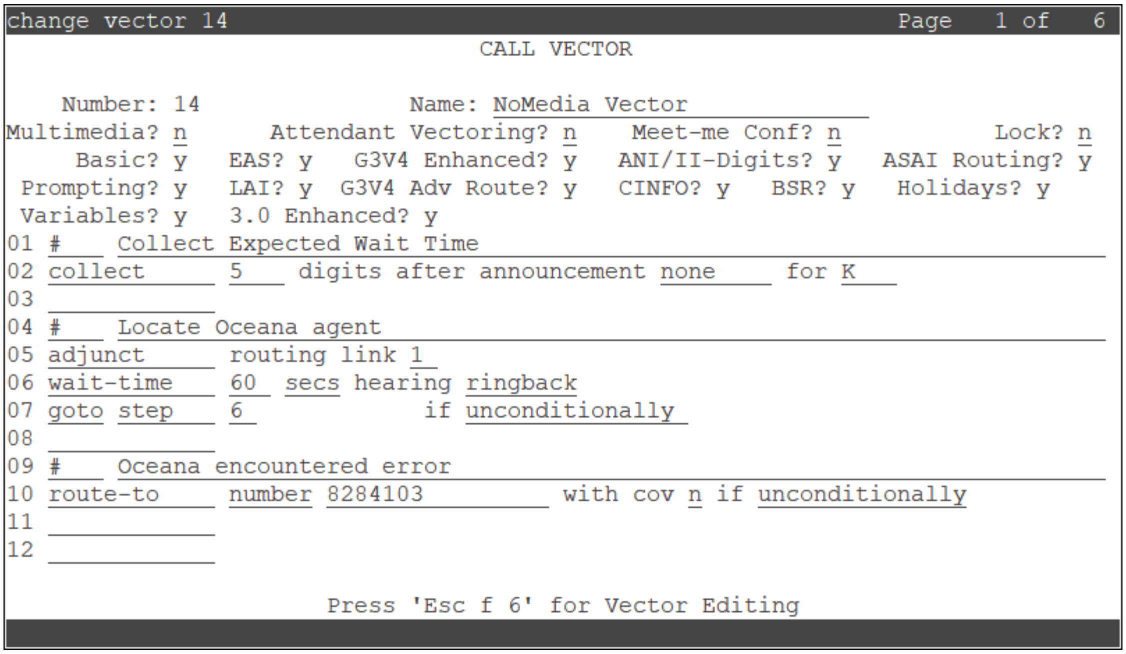
Procedure

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 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® Solution to support the Callback Assist feature.

Procedure

1. In your web browser, enter the following URL to open the Engagement Designer **Admin Console**:

   `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:
   1. 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.
   2. 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 18: Configure Post Call Survey

Post Call Survey overview

Avaya Oceana® Solution provides the Post Call Survey feature. This feature shows how to integrate Avaya Oceana® Solution 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.

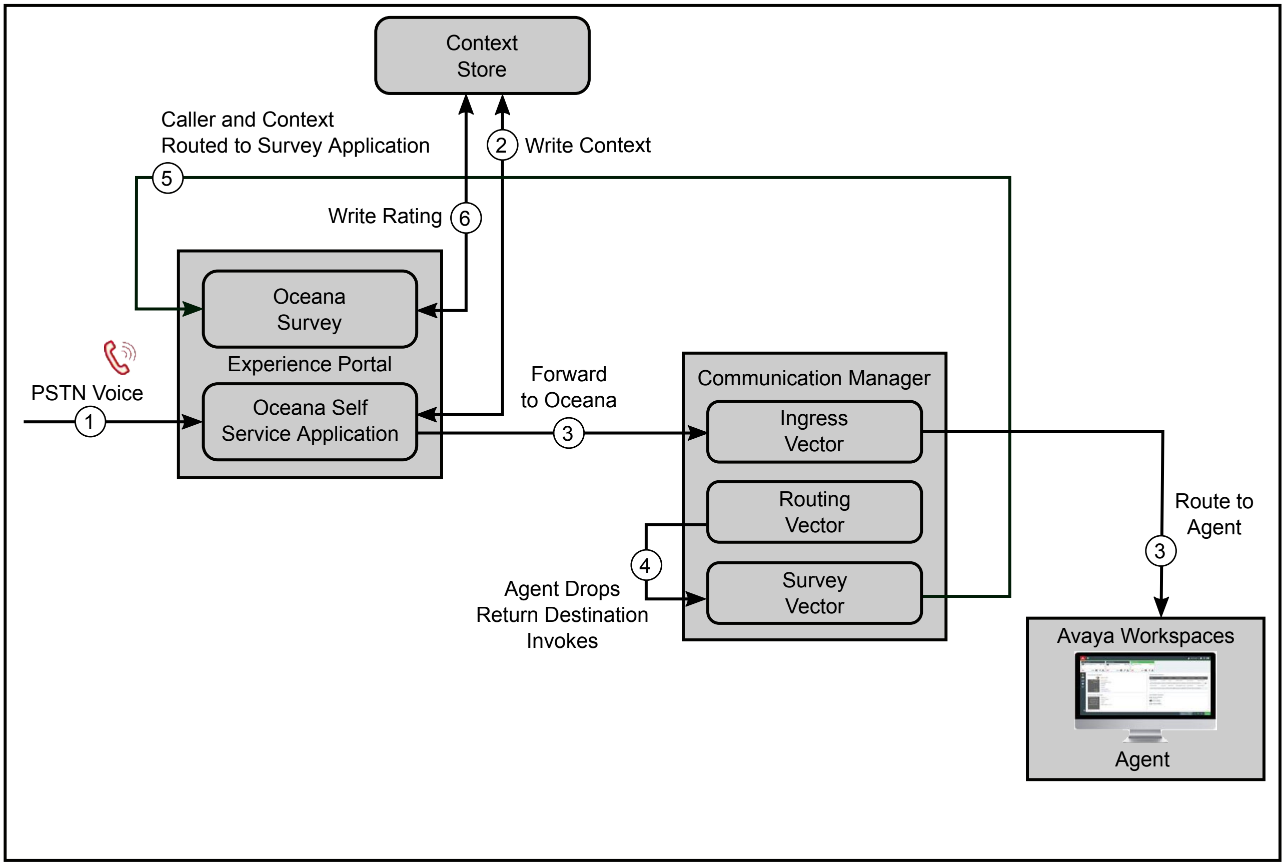
When Communication Manager detects that the agent is dropped from a voice call, the customer is kept connected and is directed the configured survey application. Calls that terminate in coverage or callback must not connect to the survey application. Therefore, you must carefully administer the Vector Return Destination (VRD).

Avaya Oceana® Solution 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 Oceana® out-of-service

Table continues…

Survey Applied	Vector	Comment
Yes	Ingress > Routing > Transfer > Routing	Call transfer, Agent surplus
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 at any point will follow the above rules

You must configure the Allow VDN Override and Return Destination parameters for 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

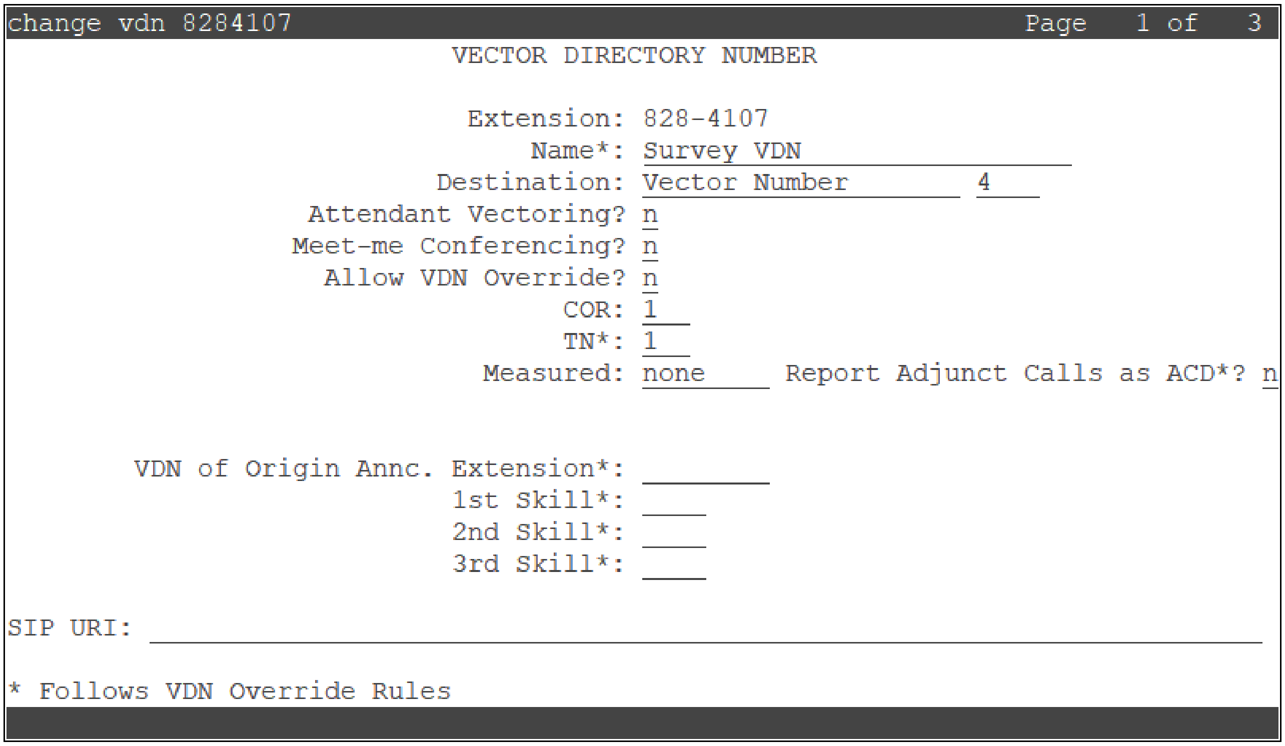
Use this procedure to create the Survey Vector Directory Number (VDN).

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.

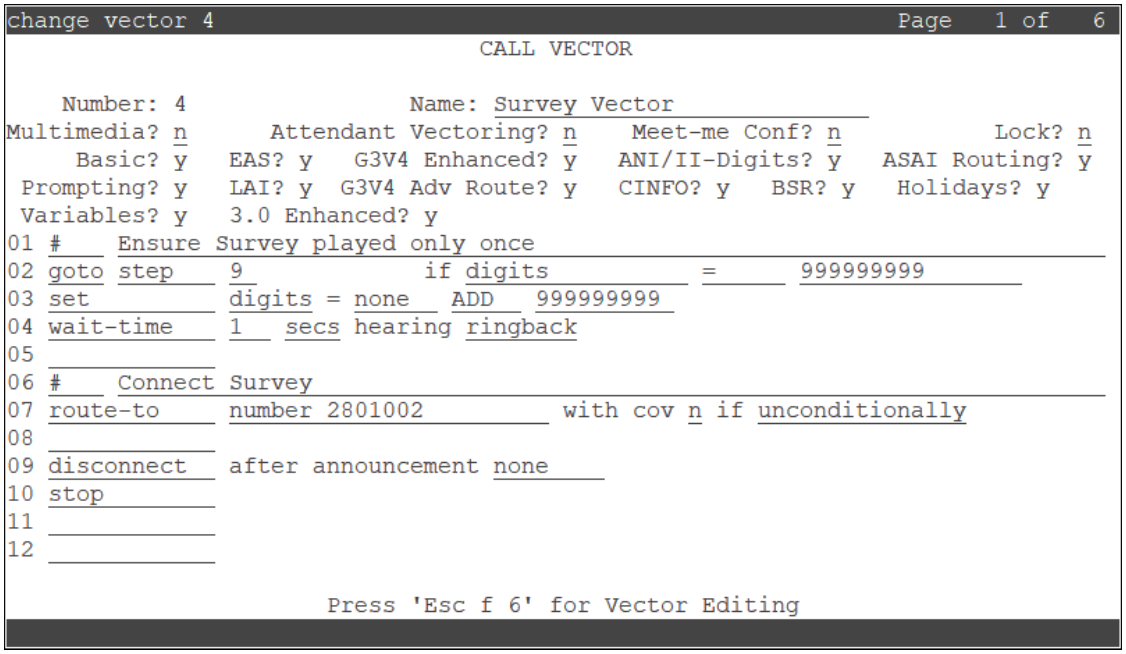
Procedure

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`**.

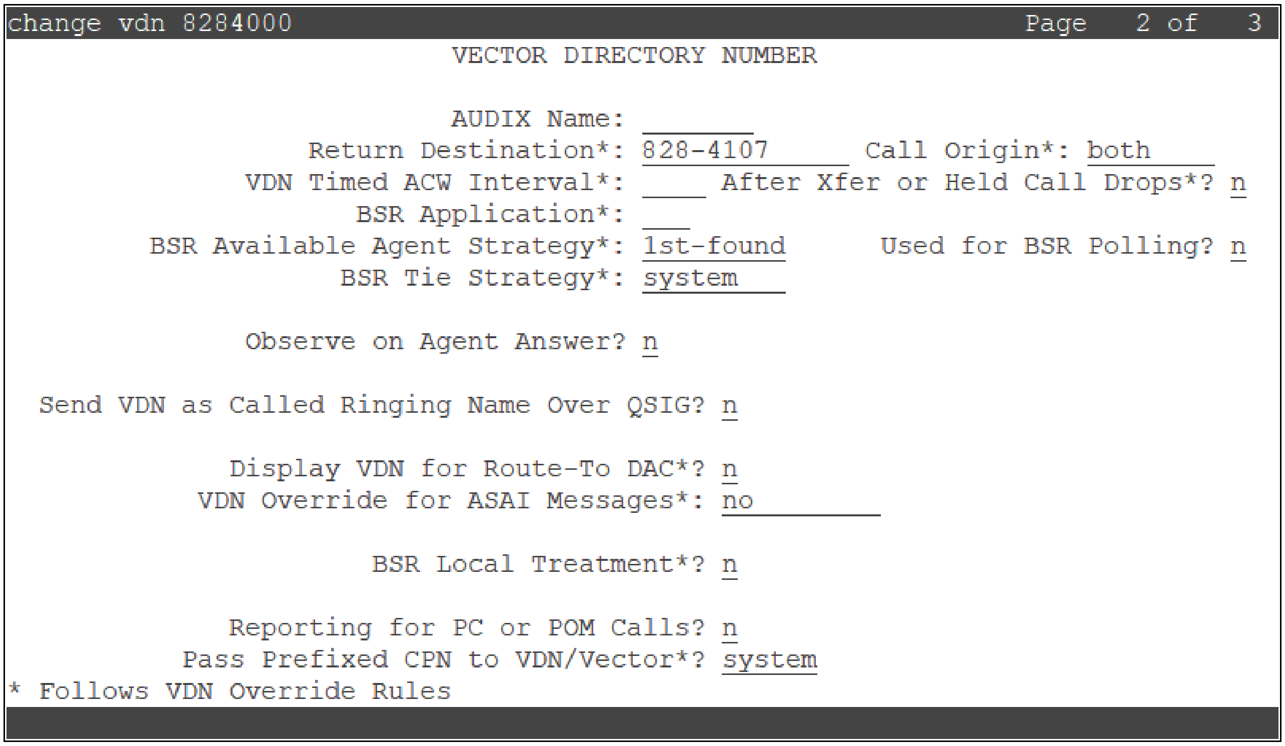
   n is the number that you entered in the **Destination** field of the VECTOR DIRECTORY NUMBER screen while creating the Routing VDN.
3. On page 2 of the VECTOR DIRECTORY NUMBER screen, do the following:

   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 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 19: 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® Solution agent and Voice contact resources.

✱ **Note:**

You can use Avaya Control Manager Conversation Sphere to import the Avaya Oceana® Solution 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® Solution 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® Solution has a number of initial vectors:

- Fallback Vector - Automatically routes calls to Elite when Avaya Oceana® Solution is down
- Ingress Vector - Initiates the Adjunct Route
- Treatment Vector - Provides treatments for calls that route to Avaya Oceana® Solution

- 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® Solution 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`.

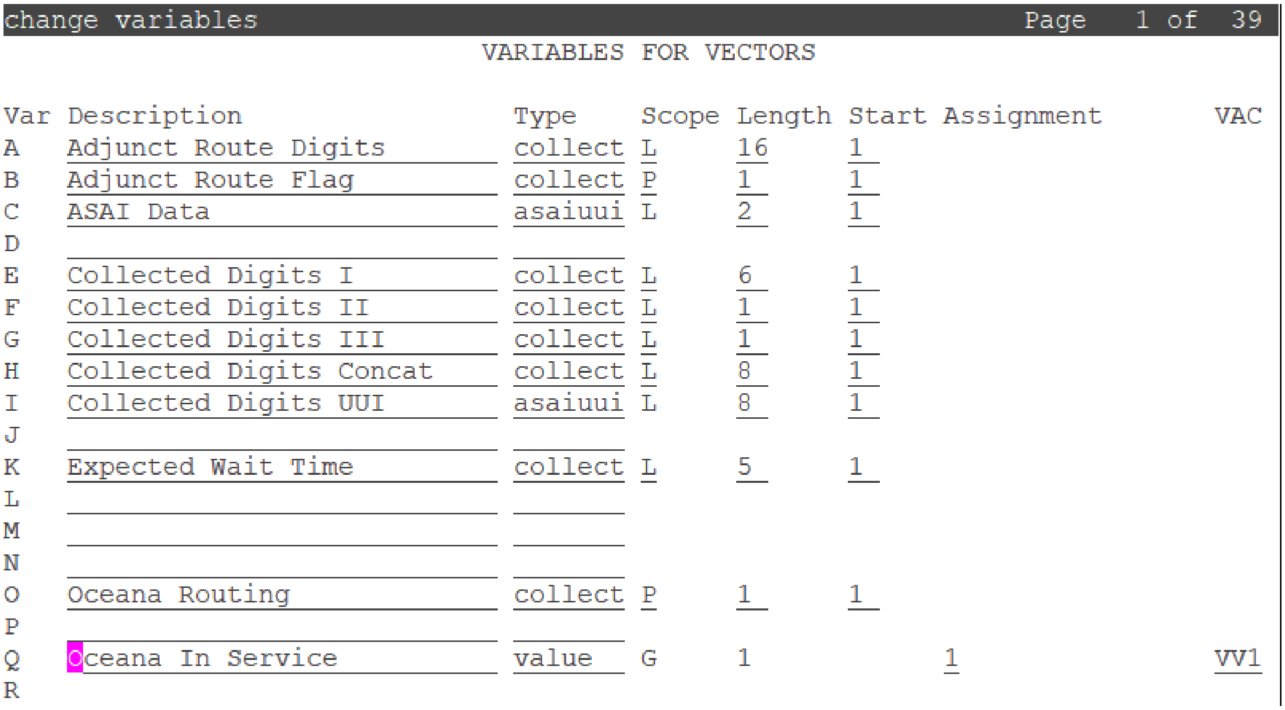
    This standard description makes maintenance and troubleshooting easier.
13. In the **Type** field, select `collect`.

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® Solution. 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 10 to add more VDNs.

Adding Provider, Skills, VDN, and Extensions to the Avaya Oceana® Solution

About this task

Use this procedure to configure the required voice resources for Avaya Oceana® Solution.

You can select and use 1 Routing VDN only for voice. You can select multiple VDNs for every other VDN type. If you want 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 callers number, routing attributes, or any other available data.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in running and accepting state.

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration** > **Avaya Oceana™** > **Server Details**.
3. Either double-click the administered Avaya Oceana® Solution UCA server, or select the administered Avaya Oceana® Solution UCA server and click **Edit**.

4. Select the **Providers** tab.
5. To add the Voice Communication Manager, perform the following steps:
    a. Click **Add**.
    b. In the **Type** field, select **CM**.
    c. In the **Name** field, enter 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, enter the address in the following format:

       `<Oceana Routing VDN>@<domain name>.com`

       For example, 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 that you configure in Step 12 and Step 13.
    e. **(Optional)** In the **Voice mail Access** field, enter the number to access the voice mail system through Avaya Workspaces.
    f. **(Optional)** In the **External Access Code** field, enter 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 in addition to 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, you must 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.
8. Click **Save**.
9. Select the **VDN** tab.
10. In the **Avaya Oceana VDN Type** field, 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. Click **Save**.
25. Select the **Extensions** tab.
26. To add DMCC extensions, select the **Recorder Extension** check box.
27. Move the required extensions from the **Available Extensions** list to the **Selected Extensions** list.
28. Click **Save**.

Creating a user to handle Voice contacts

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in 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® Solution Voice contacts. This type of agent can handle only Multimedia contacts.

j. 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.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in 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 20: Verify Voice contacts using Avaya Workspaces

Verify Voice contacts using Avaya Workspaces

This section describes how to use Avaya Workspaces to verify the Avaya Oceana® Solution deployment and configuration for Voice contacts. This section also describes how to use Avaya Workspaces to verify Voice calls.

Deploying Avaya Workspaces

Procedure

1. Install and commission Avaya Workspaces.

   For information about how to install and commission Avaya Workspaces, see the following documents:

   - *Deploying Avaya Workspaces for Oceana®*
   - *Using Avaya Workspaces for Oceana®*
   - *Administering Avaya Workspaces for 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® Solution deployment that supports up to 100 active agents, enter `https://<AvayaOceanaCluster1_FQDN>/services/UnifiedAgentController/workspaces/#/login`.

- For an Avaya Oceana® Solution 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® Solution 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® Solution 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® Solution. Therefore, to make a test call, you must use a station that is not monitored by Avaya Control Manager or Avaya Oceana® Solution.

   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 Oceana® station, the CallServerConnector service identifies all configured agent stations, and also identifies when the stations are used with 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 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 Oceana® resource, the call fails at the retrieving context step in the Engagement Designer workflow and does not get routed to an 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:

   The Customer Journey View in Avaya Workspaces requests the journey data from an External Data Mart (EDM) when the interaction is present on the client. The system only retrieves the data which is available at this time. There is no refresh or notification mechanism.

Chapter 21: WebRTC configurations

WebRTC configurations

Avaya Oceana® Solution provides the following WebRTC configurations. Based on your requirements, you can choose a configuration and complete all tasks related to the configuration.

- Configuration of Avaya Oceana® Solution with WebRTC agents.

  With this configuration, WebRTC agents can answer PSTN voice calls.

- Configuration of Avaya Oceana® Solution 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.

- Configuration of Avaya Oceana® Solution with web and mobile voice calls and WebRTC agents.

  With this configuration, WebRTC and phone-enabled agents can answer PSTN, web, and mobile voice calls.

- Configuration of Avaya Oceana® Solution with web and mobile video calls and WebRTC agents.

  With this configuration, WebRTC agents can answer web and mobile video calls.

Important:

- Before doing any of these configurations, you must deploy the Elite voice solution.
- WebRTC agents do not support the Auto answer feature. Therefore, do not configure WebRTC agents to use this feature.
- Avaya Oceana® Solution supports web and mobile video calls only if you have Avaya Aura® 7.1.3 or later.
- Hot Desking configuration is not applicable to WebRTC 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.

Chapter 22: Configure Avaya Oceana® Solution with WebRTC agents

Checklist for configuring Avaya Oceana® Solution with WebRTC agents

Use the following checklist to configure Avaya Oceana® Solution with WebRTC agents so that WebRTC agents can answer PSTN 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 on page 264. • Avaya Aura Media Server deployment on page 265. • Avaya Aura Device Services deployment on page 265.	
2	Configure authorization on Avaya Aura® Web Gateway.	See Enable authorization on Avaya Aura Web Gateway on page 265.	
3	Create WebRTC agents that can use media in browsers.	See Creating a WebRTC agent on page 268.	
4	Publish the COMM_ADDR_HANDLE values of the WebRTC agent on Avaya Aura® Device Services.	See Publishing COMM_ADDR_HANDLE values on Avaya Aura Device Services on page 269.	
5	Configure the voice media path.	See the following: • Configuring codecs in Avaya Aura Web Gateway on page 270. • Prioritizing codecs in Avaya Aura Media Server on page 270. • Prioritizing codecs in Communication Manager on page 271.	

Avaya Aura® Web Gateway deployment

Avaya Oceana® Solution requires Avaya Aura® Web Gateway to provide WebRTC Signaling Gateway services to Video-enabled SIP agents through a browser endpoint.

For more information on Avaya Aura® Web Gateway, see the following information in *Deploying the Avaya Aura® Web Gateway*:

- Topology of Avaya Aura® Web Gateway
- Information about the following components related to Avaya Oceana® Solution:
    - Avaya Aura® components
    - Avaya Aura® Session Border Controller
- Planning checklist to complete the site preparation ensuring that you:
    - Deploy Oceana Elite Voice solution and Avaya Aura® Device Services.
    - Do not deploy Avaya Aura® Presence Services.
    - Use the medium resource profile on VMware.
- VMware deployment of Avaya Aura® Web Gateway

    Important:

    WebRTC does not support the AWS deployment. Therefore, you must skip the information related to the AWS deployment
- Installation of Avaya Aura® Web Gateway

    To provide High Availability of the Avaya Aura® Web Gateway server, install one additional node in the Avaya Aura® Web Gateway cluster.
- Configuration of System Manager, Avaya Aura® Device Services, and Avaya Aura® Media Server that includes:
    - Adding Avaya Aura® Web Gateway to System Manager.
    - Configuring SIP Trunks for Avaya Aura® Web Gateway in System Manager.
    - Configuring Avaya Aura® Media Server in System Manager.
    - Configuring Avaya Aura® Web Gateway on Avaya Aura® Device Services.

Note:

- To enable Web Voice and Web Video in Avaya Oceana® Solution, you must install Avaya Aura® Web Gateway, Release 3.5.1 or later.
- Avaya Oceana® Solution must have a dedicated instance of Avaya Aura® Web Gateway and any non-Avaya Oceana® Solution application must not use that instance.
- To make web and mobile calls, customer applications must have the Avaya Oceana Customer Web Voice Video SDK.

Avaya Aura® Media Server deployment

For information about how to install and configure Avaya Aura® Media Server for Avaya Aura® Web Gateway, see the relevant section in *Deploying the Avaya Aura® Web Gateway.*

Note:

To support Avaya Aura® Web Gateway, you must install Avaya Aura® Media Server Release 8.0, Large OVA profile 5.

Avaya Aura® Device Services deployment

Avaya Oceana® Solution requires Avaya Aura® Device Services to provide login services to Video-enabled SIP agents through a browser endpoint. For information about how to install and configure a standalone Avaya Aura® Device Services, see *Quick Install for Avaya Aura® Device Services*.

Enable authorization on Avaya Aura® Web Gateway

When a request is made between a client and the Avaya Aura® Web Gateway server, an authorization token is passed with the request. The authorization is handled through the cluster that host 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.

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 and then import this certificate in Avaya Aura® Web Gateway.

Creating the common certificate

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, Oceana_Authorization

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 the cluster that AuthorizationService is installed on.

h. In the first **DNS Name** field, enter the Security Module FQDN for one of the nodes of the cluster.

i. In the second **DNS Name** field, enter the Security Module FQDN for the other node of the cluster.

j. In the **IP Address** field, enter the IP address of the cluster.

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.

Importing the common certificate in Avaya Breeze® platform nodes

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, do the following:
    a. Select the **Import third party certificate** option.
    b. In the **Please select a file (PKCS#12 format)** field, browse and select the common certificate that you generated.
    c. In the **Password** field, enter the password that you specified while creating the end entity.
    d. Click **Commit**.
5. Repeat Step 2 to Step 4 for the other nodes of the cluster.

Exporting the Avaya Breeze® platform Authorization Identity 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 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.

Importing Avaya Breeze® platform Authorization Identity Certificate in Avaya Aura® Web Gateway

About this task

Use this procedure to import Avaya Breeze® platform Authorization Identity Certificate in Avaya Aura® Web Gateway.

Note:

The Avaya Aura® Web Gateway administration portal does not display **Security Settings** if the LDAP configuration of Avaya Aura® Web Gateway is incorrect. Therefore, you must ensure that you navigate to **General Network Settings** > **LDAP Configuration** > **Security Administrator Role** and specify a security administrator role. You must also ensure that your Avaya Aura® Web Gateway Web admin user is a member of the Security Administrator Role group in LDAP.

Procedure

1. In your web browser, enter the following URL:

```
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 **Security Settings** > **Authorization**.
4. Click **Choose File**.
5. Browse and select the `.pem` file that you exported from the Avaya Breeze® platform node.
6. Click **Save**.

Creating a WebRTC agent

Before you begin

- Ensure that Avaya Oceana® Cluster 1 is in running and accepting state.
- For each WebRTC 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 **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® Solution Voice contacts. This type of agent can handle only Multimedia contacts.

j. Click **Save**.

5. Scroll to the right and select the **Avaya Oceana** tab.
6. Select the channels to be assigned to the WebRTC agent.
7. Select the **Allow browser only login** check box.
8. Click **Save**.

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**.

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 Web 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 identified.
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 one in 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.

Chapter 23: Configure Avaya Oceana® Solution with web and mobile voice calls

Checklist for configuring Avaya Oceana® Solution with web and mobile voice calls

Use the following checklist to configure Avaya Oceana® Solution 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 on page 264. • Avaya Aura Media Server deployment on page 265.	
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 273.	
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 283.	
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 301.	
5	Route web and mobile voice calls to WebRTC Engagement Designer workflows sequencing the AvayaMobileCommunications service.	See Route web and mobile voice calls to WebRTC workflows on page 306.	

Table continues…

No.	Task	Description	✔
6	Configure the voice media path.	See the following: • Configuring codecs in Avaya Aura Web Gateway on page 270. • Prioritizing codecs in Avaya Aura Media Server on page 270. • Prioritizing codecs in Communication Manager on page 271.	
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 316.	

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 Avaya Aura® Web Gateway
- A trust certificate for System Manager that manages the cluster containing Avaya Mobile Communications Snap-in.

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® Solution.

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 webserver that is hosting the token service.

   b. In the **Token Service Port** field, enter the port number of the webserver 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 webserver 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 webserver

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 WebRTC Voice or 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 Avaya Aura® Web Gateway
  - A trust certificate for System Manager that manages the cluster containing Avaya Mobile Communications Snap-in.

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® Solution.
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® Solution.

   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 webserver that is hosting the token service.

   b. In the **Token Service Port** field, enter the port number of the webserver 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 webserver 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 webserver

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 WebRTC 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 Avaya Aura® Web Gateway
  - A trust certificate for System Manager that manages the cluster containing Avaya Mobile Communications Snap-in.

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® Solution 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® Solution.

> **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 webserver that is hosting the token service.

   b. In the **Token Service Port** field, enter the port number of the webserver 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 webserver 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 webserver

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 WebRTC Voice/Video call.

Configure the reference authorization service

Configuring Guest SIP Proxy in Avaya Aura® Web Gateway

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** > **Guest SIP Domain**.
3. In the **Default Guest Sip Domain** field, enter the SIP domain.
4. Click **Save**.
5. On the Avaya Aura® Web Gateway administration portal, click **External Access** > **Guest SIP Proxy**.
6. In the **SIP Address** field, enter the Entity IP of your Session Manager.
7. In the **SIP Port** field, type `5061`.
8. In the **SIP Protocol** field, click `TLS`.
9. In the **Location** field, specify the relevant location.
10. Specify the weight as `100`.
11. Click **Save**.

Configuring security settings in Avaya Aura® Web Gateway

About this task

Token Generation Service supplied with Avaya Aura® Web Gateway must be trusted through TLS. Therefore, it must be verified that the certificate and certificate FQDN are trusted.

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 **Security Settings** > **Trusted Hosts**.
3. On the Trusted Hosts page, click **Add**.

Avaya Aura® Web Gateway displays a new row to add the host.

4. In the new row, enter the FQDN of Avaya Aura® Web Gateway as a trusted host.
5. Click **Save**.
6. On the Avaya Aura® Web Gateway administration portal, click **Security Settings** > **HTTP Clients**.
7. In the Client-Device Certificate Policy area, in the **REST** field, change the value from `NONE` to `OPTIONAL`.
8. Click **Save**.
9. On the Avaya Aura® Web Gateway administration portal, click **General Network Settings** > **Location**.
10. In the Web Gateway Locations area, verify that a location is selected for the Avaya Aura® Web Gateway server.
11. In the Location Assignments and Priorities area, verify that the same location is added to the **Assigned Locations** list.

Enabling Avaya Aura® Web Gateway TestApp and Token Generation Service

Procedure

1. Log on to Avaya Aura® Web Gateway by using your SSH credentials.
2. Go to `/opt/Avaya/CallSignalingAgent/version/mss/8.0.1-4_8.0.26/telportal/webapps`.
3. Rename the `token-generation-service.undeploy` file as `token-generation-service.war`.
4. Rename the `devclient.undeploy` file as `devclient.war`.
5. Run the following command to restart Avaya Aura® Web Gateway services:

   ```
   svc csa restart
   ```

Making a test call to verify the Web Voice operation

About this task

Use this procedure to make a test call by using the standalone Avaya Aura® Web Gateway TestApp.

Before you begin

Enable Avaya Aura® Web Gateway TestApp and Token Generation Service.

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?remoteAddress=<Destination_Number>&identity=<Caller_Identity>`, where:

- *<Avaya Aura Web Gateway_FQDN>* is the FQDN of the Avaya Aura® Web Gateway server.
- *<Destination_Number>* is the destination number where you want to call.
- *<Caller_Identity>* is the identity of the caller.

2. Run the following command to activate calls:

   ```
   ac
   ```

3. Run the following command for an audio call:

   ```
   call <Destination_Number>
   ```

4. Answer the call and verify that the test call is established successfully.

Install and configure Avaya Aura® Session Border Controller

Avaya Oceana® Solution 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 for Enterprise*.

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

Procedure

1. Log in 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 in 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 client profile for the Avaya Aura® Web Gateway reverse proxy

Procedure

1. Log in 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 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 in 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 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**.

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 SBCE.
    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 SBCE.
    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**.

Create a client profile for the AvayaMobileCommunications reverse proxy relay

Procedure

1. Log in 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 that will act 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 in 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 TURN for WebRTC

Avaya Oceana® Solution supports both Client side TURN and server side TURN for WebRTC calls from the public internet. Avaya recommends the use of Client side TURN unless there is a specific reason where Server side TURN is required. Follow one of the procedures below to configure either WebRTC Client side TURN OR WebRTC Server side TURN.

Configure WebRTC Client Side TURN

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 appropriate certificate.

   Important:

   Ensure that the certificate associated with the profile includes the external (B1) Interface IP. This B1 IP acts as an listen IP for the TLS client TURN requests. Hence, port 443 must not be in use on this B1 IP for any other SBC function such as reverse proxy.
6. In the **Peer Verification** field, select **None**.
7. Leave all others fields to default values.
8. Click **Next**.

9. Click **Finish**.

Adding a TURN/STUN service for WebRTC 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 profile 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 created in Creating a server profile for the TLS TURN relay on page 288.
   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 WebRTC Client side TUTN on 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 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**.

Configure WebRTC Server Side TURN

Adding a TURN/STUN service for WebRTC calls to Avaya Aura® Session Border Controller

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 profile name.
    b. In the **UDP Listen Port** field, type `3478`.
    c. Keep the **TCP/TLS Listen Port** and **TLS Server Profile** fields blank.
    d. In the **Media Relay Port Range** field, type a value between 50000 to 55000.
    e. In the **Authentication** field, enable the authentication.
    f. In the **Server Authentication** field, enable the authentication.
    g. In the **UserName** field, enter a user name for server authentication.
    h. In the **Password** field, enter a password for server authentication.
    i. In the **Confirm Password** field, reenter the password for server authentication.
    j. In the **Realm** field, specify the SIP domain.
    k. In the **UDP Relay** field, enable the UDP relay.
    l. Click **Finish**.
4. On the TURN Relay tab, click **Add** and do the following:
    a. In the **Listen IP** field, enter the internal interface IP configured on Avaya Aura® Session Border Controller that Avaya Aura® Media Server uses for media.
    b. In the **Media Relay IP** field, enter the external IP configured on Avaya Aura® Session Border Controller that Avaya Aura® Web Gateway external clients use 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**.

Adding the STUN server 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. 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** > **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 either of the following:

   - The external IP that you used 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**.

Adding the STUN server configuration 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 Avaya Aura® Media Server Element Manager interface, do the following:
   a. Click **System Configuration** > **Server Profile** > **General Settings**.
   b. Select the **Firewall NAT Tunneling Media Processor** check box.
   c. Click **Save**.
   d. Click **System Configuration** > **Media Processing** > **ICE** > **STUN/TURN Servers** > **Accounts**.
   e. Click **Add** to add a an Account.
   f. In the **Alias** field, enter the alias for the account name.

g. In the **User ID** field, enter the user ID that was configured on the SBC TURN/STUN profile earlier.

h. In the **Password** field, enter the password that was configured on the SBC TURN/STUN profile earlier.

i. Click **Save**.

j. Click **System Configuration** > **Media Processing** > **ICE** > **STUN/TURN Servers** > **Servers**.

k. Click **Add** to add a STUN/TURN server.

l. In the **Name** field, enter the name of the server.

m. In the **Description** field, enter the description of the server.

n. In the **Type** field, select `STUN/TURN`.

o. In the **Transport Protocol** field, select `UDP`.

p. In the **Address** field, enter the IP address that you configured as the listen IP for the TURN Relay on Avaya Aura® Session Border Controller.

q. In the **Port** field, type `3478`.

r. In the **Priority** field, type `0`.

s. In the **Weight** field, type `10`.

t. In the **Account** field, select the **Use an existing account (alias/user ID)** check box, and then select the account that you created.

u. Click **Save**.

Creating a server profile for the Avaya Aura® Session Border Controller signaling interface

Procedure

1. Log in 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 internal interface IP that is to be used to communicate with Session Manager.
6. In the **Peer Verification** field, click **None**.
7. Keep the default values in the other fields.

8. Click **Finish**.

Creating the Avaya Aura® Session Border Controller signaling interface

Procedure

1. Log in 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 in 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 in 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 in 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 in 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 in 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 in 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 in 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 `Truck 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:
    1. Select the **Enable Grooming** check box.
    2. In the **Interworking Profile** field, select the newly created interworking profile with remote SBC disabled.
    3. 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 in 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 `Truck 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 in 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 in 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 in 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 293
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 Controllersignaling 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**

Enable Port for remote access on Avaya Aura Web Gateway HTTP Reverse Proxy

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 **Enable port for remote access** check box.
4. 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.
5. Click **Save**.

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® Solution, 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, 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® Solution resources from Avaya DevConnect, see *Avaya Oceana® Solution 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 left 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 left 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

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 Engagement Designer **Designer Console**:

```
https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/
index.html
```

2. Click **Import**.
3. On the Import Workflow dialog box, click **Choose File**.
4. Browse to the sample workflow and click **Import**.
5. Click **Save Workflow**.
6. On the Save Workflow dialog box, do the following:
    a. In the **Workflow** field, type `OceanaWebVoiceAssistedService`.

       You can also provide any other name for the workflow.

    b. Select the folder where you want to save the workflow.

    c. Click **Save**.
7. Click **Deploy Workflow**.
8. On 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 can not 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 Engagement Designer **Admin Console**:

    ```
    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. On the Workflow Attributes dialog box, 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.

Deploying the sample Transfer to Service workflow for Web Voice

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 Engagement Designer **Designer Console**:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`

2. On the toolbar, click **Import Workflow from File**.
3. On the Import Workflow dialog box, click **Choose File**.
4. Browse to the sample workflow and click **Import**.
5. Click **Save Workflow**.
6. On the Save Workflow dialog box, do the following:
   a. In the **Workflow** field, type `OceanaWebVoiceTransfer`.

      You can also provide any other name for the workflow.

   b. Select the folder where you want to save the workflow.
   c. Click **Save**.
7. Click **Deploy Workflow**.
8. On the Deployment Details dialog box, click **OK**.
9. In your web browser, enter the following URL to open the Engagement Designer **Admin Console**:

   `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. On the Workflow Attributes dialog box, 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.

13. Click **Close**.

Configuring a WebRTC service profile

About this task

Use this procedure to create a WebRTC service profile for all WebRTC contacts and all WebRTC 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 **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**.

Route web and mobile voice calls to WebRTC workflows

Configuring routing to Engagement Designer

About this task

In a typical Avaya Oceana® Solution, 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 left 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 left 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 left 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 left pane, click **Dial Patterns**.

16. On the Dial Patterns page, click **New**.

17. On the Dial Pattern Details page, perform the following steps:

   a. In the **Pattern** field, enter a pattern that Web Voice users dial to access Engagement Designer workflows.

      Important:

      At the end of this WebRTC 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.

   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 Originating Locations and Routing Policies section, click **Add**.

   e. 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**.

   f. 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 WebRTC 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 WebRTC service profile that you have already created.

    b. In the **Pattern** field, enter the pattern as defined when configuring the WebRTC Routing pattern to Engagement Designer.

    This allows multiple numbers within the defined WebRTC 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$^{®}$ Solution, 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$^{®}$ Solution 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 left 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 left 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® Solution 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® Solution deployment that supports up to 100 active agents.

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 WebRTC Routing pattern as defined when configuring routing to Engagement Designer.

   This allows multiple numbers within the defined WebRTC 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 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

Web Voice Transfer and Conference capability in Avaya Oceana® Solution

Web and Mobile Voice calls		Avaya Workspaces phone agent with active call		Avaya Workspaces WebRTC agent with active call		
Target	**Transfer/ Conference**	**PSTN Voice call**	**Web Voice call**	**PSTN Voice call**	**Web Voice call**	**Web Video call**
Agent	Blind/single step Transfer	Yes	Yes	No	No	No
	Blind/single step Conference	No	No	No	No	No
	Consult Transfer	Yes	Yes	Yes	Yes	No
	Consult Conference	Yes	Yes	Yes	Yes	No
Servi ce	Blind/single step Transfer	Yes	Yes	Yes	Yes	Yes
	Blind/single step Conference	No	No	No	No	No
	Consult Transfer	No	No	No	No	No
	Consult Conference	No	No	No	No	No

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 WebRTC 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 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`.

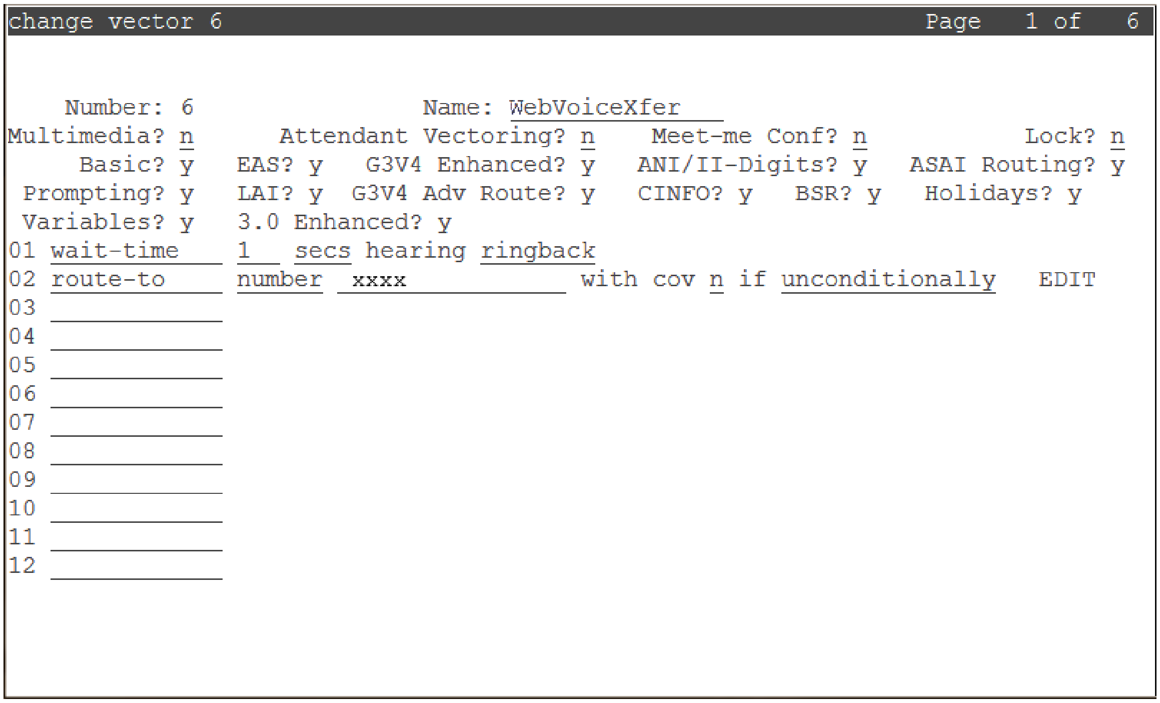
   n is the number that you entered in the **Destination** field of the VECTOR DIRECTORY NUMBER screen while creating the Web Voice Transfer VDN.

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 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 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 24: Configure Avaya Oceana® Solution with web and mobile voice calls and WebRTC agents

Checklist for configuring Avaya Oceana® Solution with web and mobile voice calls and WebRTC agents

Use the following checklist to configure Avaya Oceana® Solution with web and mobile voice calls and WebRTC agents so that WebRTC 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 on page 264. • Avaya Aura Media Server deployment on page 265. • Avaya Aura Device Services deployment on page 265.	
2	Configure authorization on Avaya Aura® Web Gateway.	See Enable authorization on Avaya Aura Web Gateway on page 265.	
3	Create WebRTC agents that can use media in browsers.	See Creating a WebRTC agent on page 268.	
4	Configure the voice media path.	See the following: • Configuring codecs in Avaya Aura Web Gateway on page 270. • Prioritizing codecs in Avaya Aura Media Server on page 270. • Prioritizing codecs in Communication Manager on page 271.	

Table continues…

No.	Task	Description	✔
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 273.	
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 283.	
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 301.	
8	Route web and mobile voice calls to WebRTC Engagement Designer workflows sequencing the AvayaMobileCommunications service.	See Route web and mobile voice calls to WebRTC workflows on page 306.	
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 316.	

Chapter 25: Configure Avaya Oceana® Solution with web and mobile video calls and WebRTC agents

Checklist for configuring Avaya Oceana® Solution with web and mobile video calls and WebRTC agents

Use the following checklist to configure Avaya Oceana® Solution with web and mobile video calls and WebRTC agents so that WebRTC 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 on page 264. • Avaya Aura Media Server deployment on page 265. • Avaya Aura Device Services deployment on page 265.	
2	Configure authorization on Avaya Aura® Web Gateway.	See Enable authorization on Avaya Aura Web Gateway on page 265.	
3	Create WebRTC agents that can use media in browsers.	See Creating a WebRTC agent on page 268.	
4	Configure the voice media path.	See the following: • Configuring codecs in Avaya Aura Web Gateway on page 270. • Prioritizing codecs in Avaya Aura Media Server on page 270. • Prioritizing codecs in Communication Manager on page 271.	

Table continues…

No.	Task	Description	✔
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 273.	
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 283.	
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 301.	
8	Route web and mobile voice calls to WebRTC Engagement Designer workflows sequencing the AvayaMobileCommunications service.	See Route web and mobile voice calls to WebRTC workflows on page 306.	
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 316.	
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 325.	
11	Route web and mobile video calls to WebRTC Engagement Designer workflows sequencing the AvayaMobileCommunications service.	See Route web and mobile video calls to WebRTC workflows on page 326.	
12	Create WebRTC video agents.	See Create WebRTC video agents on page 327.	
13	Configure the video media path.	See Configure the video media path on page 330.	
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 332.	

Deploying the sample Web Video 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 Engagement Designer **Designer Console**:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`

2. Click **Import**.
3. On the Import Workflow dialog box, click **Choose File**.
4. Browse to the sample workflow and click **Import**.
5. Click **Save Workflow**.
6. On the Save Workflow dialog box, do the following:
   1. In the **Workflow** field, type `OceanaVideoAssistedService`.

      You can also provide any other name for the workflow.
   2. Select the folder where you want to save the workflow.
   3. Click **Save**.
7. Click **Deploy Workflow**.
8. On 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 can not 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 Engagement Designer **Admin Console**:

   `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 WebRTC 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 WebRTC 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 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 WebRTC 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® Solution SIP agents

In Avaya Oceana® Solution, agents handle Video contacts using a Video enabled SIP station. Therefore, you must first configure SIP agents for Avaya Oceana® Solution 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 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® Solution agent

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in 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 Web 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 identified.
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 one in 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

Deploying the sample Transfer to Service workflow for Web Video

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 Engagement Designer **Designer Console**:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`
2. Click **Import**.
3. On the Import Workflow dialog box, click **Choose File**.
4. Browse to the sample workflow and click **Import**.
5. Click **Save Workflow**.

6. On the Save Workflow dialog box, do the following:
    a. In the **Workflow** field, type `OceanaVideoTransfer`.

       You can also provide any other name for the workflow.
    b. Select the folder where you want to save the workflow.
    c. Click **Save**.
7. Click **Deploy Workflow**.
8. On the Deployment Details dialog box, click **OK**.
9. In your web browser, enter the following URL to open the Engagement Designer **Admin Console**:

   `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 WebRTC 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 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`**.

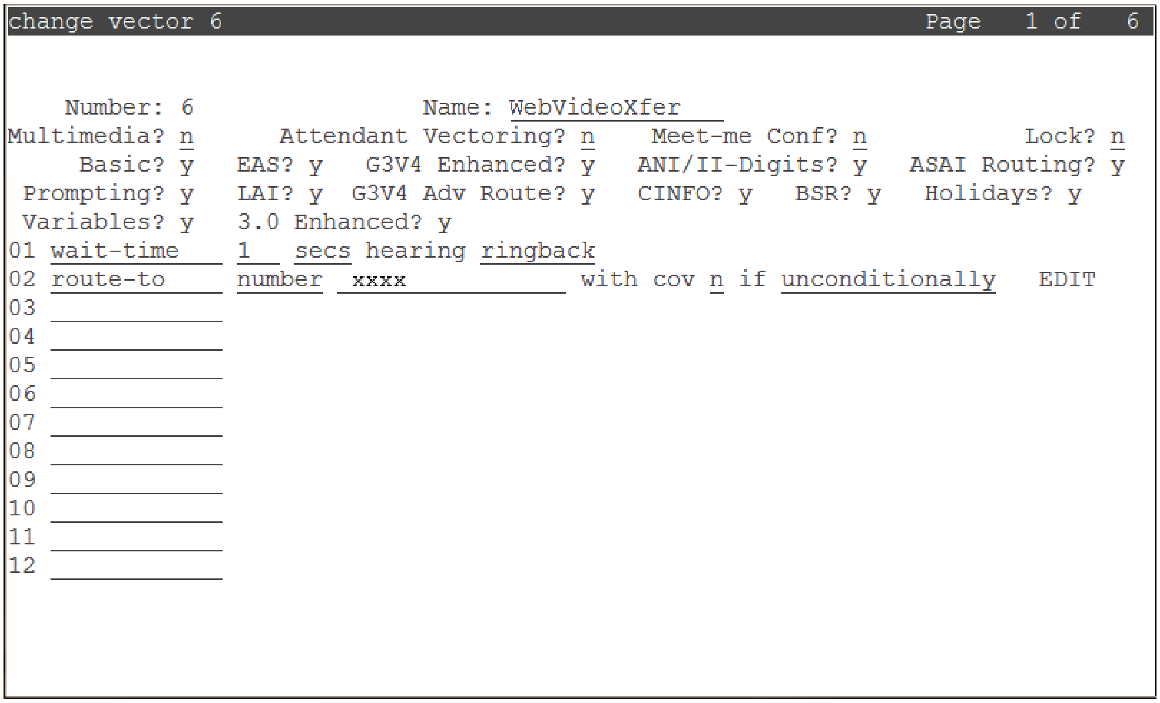
   n is the number that you entered in the **Destination** field of the VECTOR DIRECTORY NUMBER screen while creating the Web Video Transfer VDN.

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 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 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 26: Configure the sample Chat client

Configure the sample Chat client

This section describes how to configure an Apache web server to host a sample Chat client for Avaya Oceana® Solution. 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 might 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:
   1. Click the **Click here to configure URLs** option.
   2. 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.
   3. 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® Solution 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.

Creating certificates for Avaya Oceana® Cluster 3 to secure Chat

About this task

Secure WebSocket connections require a certificate. Use this procedure to create certificates for Avaya Oceana® Cluster 3.

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.

   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 a name that matches the full hostname of the server.

   h. In the **DNS Name** and **IP Address** fields, enter appropriate values.

   i. Click **Add**.

2. Create a private key and Certificate Signing Request (CSR) for the server by performing the following steps:

   a. SSH into the server for which you want to create a certificate.

   b. Generate a private key using the **`OpenSSL genpkey`** command.

   c. 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.pem -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.
openssl req -new -in mmdev1.pem -key mmdev1.pem -passin pass:testing -out
mmdev1.csr
```

3. Create a certificate from the CSR file by performing the following steps:
    a. Export the CSR file from the server using an FTP client.
    b. Open the CSR file in a text editor such as Notepad.
    c. In your web browser, enter the following URL for the System Manager installation of EJBCA:

        `https://<SMGR FQDN>/ejbca`

    d. In the navigation pane, in the Enroll section, click **Create Certificate from CSR**.
    e. In the **Username** field, enter the user name.
    f. In the **Enrollment code** field, enter the password.
    g. From the text editor, copy the content of the CSR file placed between the `---BEGIN CERTIFICATE REQUEST---` and `---END CERTIFICATE REQUEST---` lines.
    h. Paste the copied content into the list.
    i. Click **OK**.
4. Download the root certificate for System Manager by performing the following steps:
    a. In your web browser, enter the following URL for the System Manager installation of EJBCA:

        `https://`*`<SMGR FQDN>`*`/ejbca/`

    b. In the Retrieve Certificates section, click **Fetch CA Certificates**.
    c. Based on your browser, perform one of the following steps:
        - To install the certificate in the certificate manager of Firefox, click the **Download to Firefox** link.
        - To install the certificate on a Windows machine containing Microsoft Internet Explorer, Edge, and Chrome, click the **Download to Internet Explorer** link.

        The system prompts you to save the certificate.
    d. Save the certificate.
    e. Right-click the certificate file and click **Install Certificate**.
    f. Select **Local Machine** and click **Next**.

g. Select **Place all certificates in the following store** and click **Browse**.

h. Select the **Show physical stores** check box and scroll up until you find **Trusted Root Certification Authorities**.

i. Expand **Trusted Root Certification Authorities** and select **Registry**.

j. Click **OK**.

k. Click **Finish**.

l. Open the Windows hosts file in a text editor such as Notepad.

   Note:

   Ensure that you run the text editor as Administrator.

m. Add the host names of the lab to your hosts file in the following format.

   ```
   <IP Address> FQDN
   ```

n. In your web browser, browse to a known service URL to ensure that there are no errors about the validity of the certificate.

   Microsoft Internet Explorer tries to download the JSON response. However, Firefox and Chrome display the result.

o. In your web browser, browse to the following URL:

   ```
   https://<AvayaOceanaCluster3_Hostname>/services/customer/chat
   ```

   The browser does not actually open a WebSocket to this URL. However, if the browser console does not display any errors about the validity of the certificate, the WebSocket must open when using the Web UI.

Chapter 27: Configure Chat

Configure Chat

This section describes how to configure Chat contacts and the optional Avaya Automated Chat and Avaya Co-Browsing Snap-in integration.

Locating the Avaya Automated Chat Site Code

About this task

Avaya BotConnector Snap-in functions as a proxy for an Avaya Automated Chat system. Avaya BotConnector Snap-in connects to the automated system using an IP address and a unique site code. For more information about Avaya Automated Chat, see *Avaya Automated Chat Reference Manual*.

Note:

Perform this procedure only if you are using an Avaya Automated Chat system in the Avaya Oceana® Solution.

Procedure

1. In your web browser, enter the following URL to log in to the Avaya Automated Chat management console:

   ```
   https://<Automated Chat System IP>/ABMI/
   ```

2. Browse to **administer sites** and locate the **Site Code** identifier.
3. Note the **Site Code** identifier.

   You need this information to configure Avaya BotConnector Snap-in. For example, the **Site Code** identifier is “iasljety4so7”.

Installing the Avaya Automated Chat Server HTTPS certificate

About this task

Export a security certificate from the Avaya Automated Chat Server and install the certificate on the cluster containing Avaya BotConnector Snap-in, so that Avaya BotConnector Snap-in can communicate with the Avaya Automated Chat system.

Note:

Perform this procedure only if you are using an Avaya Automated Chat system in Avaya Oceana® Solution.

Procedure

1. Access the Automated Chat Server URL using a web browser and obtain the Avaya Automated Chat Server HTTPS certificate.
2. Save and download the certificate as a `.cer` format file to your local drive.
3. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
4. Select the cluster containing Avaya BotConnector Snap-in.
5. Perform the following steps to install the Automated Chat Server certificate:
    a. Click **Certificate Management**.
    b. Click **Install Trusted Certificate**.
    c. Click **Choose File** and locate the Avaya Automated Chat HTTPS certificate.
    d. Click **Retrieve Certificate**.
    e. Click **Commit**.
    f. Ensure that following message is displayed on the System Manager Cluster Administration page.

    ```
    Successfully installed trust certificate from file. Please
    note that a restart of the remote application may be required
    for the changes to take effect.
    ```
6. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Server Administration**.
7. Select the Avaya Breeze® platform node containing Avaya BotConnector Snap-in.
8. Click **Shutdown System** > **Reboot**.

Configuring BotConnector Snap-in licenses

About this task

For an Avaya Oceana® Solution that uses Avaya Automated Chat, you must 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 left 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

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 Engagement Designer **Designer Console**:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`
2. Click **Import**.
3. On the Import Workflow dialog box, click **Choose File**.
4. Browse to the sample workflow and click **Import**.
5. Click **Save Workflow**.
6. On the Save Workflow dialog box, do the following:
    a. In the **Workflow** field, type `OceanaChatAssistedService`.

       You can also provide any other name for the workflow.
    b. Select the folder where you want to save the workflow.
    c. Click **Save**.
7. Click **Deploy Workflow**.
8. On the Deployment Details dialog box, click **OK**.

9. In your web browser, enter the following URL to open the Engagement Designer **Admin Console**:

   `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 Avaya Automated Chat support.

11. On the Workflows tab, select the check box for the OceanaChatAssistedService workflow and click **Attributes**.

12. On the Workflow Attributes dialog box, do the following:

    a. In the **BotEnabled** field, keep the default value `True`, which specifies that the workflow always tries 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 **MaintenanceMode**, keep the default value `False`.

       If the site is down for maintenance, you must set this attribute to `True`.

    c. In the **WaitTime**, set the time for which Communication Manager must play the wait treatment to the customer before the workflow sends a MatchUpdate to Work Assignment.

Deploying the sample Transfer to Service workflow for Chat

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 Engagement Designer **Designer Console**:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`

2. Click **Import**.
3. On the Import Workflow dialog box, click **Choose File**.
4. Browse to the sample workflow and click **Import**.
5. Click **Save Workflow**.

6. On the Save Workflow dialog box, do the following:
   a. In the **Workflow** field, type `OceanaChatTransfer`.

      You can also provide any other name for the workflow.
   b. Select the folder where you want to save the workflow.
   c. Click **Save**.
7. Click **Deploy Workflow**.
8. On the Deployment Details dialog box, click **OK**.
9. In your web browser, enter the following URL to open the Engagement Designer **Admin Console**:

   `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 **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.

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 Engagement Designer **Admin Console**:

   `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_TO_SERVICE**.
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 running and accepting state.

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration** > **Avaya Oceana™** > **Server Details**.
3. Either double-click the administered Avaya Oceana® Solution UCA server, or select the administered Avaya Oceana® Solution UCA server and click **Edit**.
4. Select the **Providers** tab.
5. To add the Chat Provider, perform the following steps:
    a. Click **Add**.
    b. In the **Type** field, select **Chat**.
    c. In the **Name** field, keep the value `OCP Chat`.
    d. In the **Address** field, enter `chat`.
    e. Click **Save**.

    > **Important:**
    >
    > To make the new provider available to Avaya Workspaces agents, you must restart the clusters.

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 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® Solution.
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**.

Omnichannel Administration Utility

Use the Omnichannel Administration Utility to commission and maintain multimedia resources.

To assist agents with Chat contacts, you can use automatic phrases to configure text so that agents can automatically insert the automatic phrases in the text-based conversation. You can also configure page push URLs that are commonly sent to customers. The automatic phrases and page push URLs save the typing time of agents when they are communicating with customers.

The automatic phrases and page push URLs include the following:

- A Web On Hold URL group that creates a list of webpages that are sent to the customer’s desktop, while the customer waits for an agent to respond to their initial contact.
- A Web On Hold comfort group that creates a list of messages that are sent to the customer’s desktop, while the customer waits for a specified period for an agent to respond to their initial contact.
- A Chat comfort group that creates a list of messages that are sent to the customer's desktop, while the customer waits for a specified period for an agent to respond, either to their initial contact or during the communication.

Creating Web On Hold URL groups using Omnichannel Administration Utility

About this task

A Web On Hold URL group is a sequence of URLs that can be presented in the web browser of a customer while the customer waits for an agent in a web communication. You can define the time for which each URL must appear on the web browser of the customer.

Web On Hold URLs can include multimedia files, such as audio or video files. To run the multimedia files, customers must download the required plug-ins on their web browsers.

The maximum number of URLs that you can add to a Web On Hold URL group is 50. However, you must ensure that you do not add more than 25 URLs to a Web On Hold URL group.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **Web Chat**.
3. Click **Web On Hold**.
4. Click the **On Hold URLs** tab.
5. Click **New**.
6. In the **Tag** field, type a name for the Web On Hold URL group.
7. In the **Description** field, type a description for the Web On Hold URL group.
8. In the **Hold Time** field, type the number of seconds to display each URL in the customer's browser.
9. In the **URL** field, type the URL to display on the web browser of the customer.
10. Click **Add**.
11. Repeat Step 2 to Step 10 to add all URLs to the current Web On Hold URL group.
12. In the Edit Attributes area, select the required attributes.

    For example, select `Language.English`.
13. Click **Save**.

Creating Web On Hold comfort groups using Omnichannel Administration Utility

About this task

A Web On Hold comfort group consists of a list of sequential messages that are sent to the customer’s desktop, while the customer waits for an agent to respond, for a specified period of time to their initial contact.

You can set the time for which messages display on the customer’s desktop.

Procedure

1. Start Omnichannel Administration Utility.
2. In the left pane, click **Web Chat**.
3. Click **Web On Hold**.
4. Select the **On Hold Comfort Groups** tab.
5. In the Comfort Group section, click **New**.
6. In the **Name** field, type a name for a new Web On Hold comfort group.
7. In the **Delay** field, type the number of seconds to display each comfort message in the customer's desktop.

8. In the **Message Text** field, type the comfort message.
9. Click **Add**.
10. Repeat this procedure to add messages to the current Web On Hold comfort group.
11. In the Edit Attributes section, select the required attributes.

    For example, select `Language.English`.
12. Click **Save**.

Creating Web communications comfort groups using Omnichannel Administration Utility

About this task

A Chat comfort group consists of a list of sequential messages that are sent to the customer's desktop while they wait for an agent to respond, for a specified period of time, either to their initial contact or during the communication.

You can set the time for which the messages must display on the customer’s desktop.

Procedure

1. Start Omnichannel Administration Utility.
2. In the left pane, click **Web Chat**.
3. Click **Comfort Messages**.
4. In the Comfort Group section, click **New**.
5. In the **Name** field, type a name for the comfort group.
6. In the **Delay** field, type the number of seconds for which each comfort message must display on the customer's desktop.
7. In the **Message Text** field, type the comfort message.
8. Click **Add**.
9. Repeat this procedure to add messages to the current Web communications comfort group.
10. In the Group Messages section, use the arrow keys to configure the sequence of messages.
11. In the Edit Attributes section, select the required attributes.

    For example, select `Language.English`.
12. Click **Save**.

Creating automatic phrases using Omnichannel Administration Utility

About this task

Configure automatic phrases by attributes. You can create a list of commonly used phrases for agents to insert into their Web communications contacts instead of typing individual responses.

To assist agents with Chat contacts, you can use automatic phrases to configure text for agents to automatically insert in the text-based conversation. The automatic phrases save the agent typing time when communicating with the customer.

Procedure

1. Start Omnichannel Administration Utility.
2. In the left pane, click **Web Chat**.
3. Click **Auto Phrases**.
4. Perform one of the following steps:
   - From the drop-down list, select an existing Phrase Group.
   - In the **Name** field, type a name for the Phrase Group and click **Create**.
5. In the Create Auto Phrase section, perform the following steps to create an Auto Phrase:
   a. In the **Name** field, type a name to represent the Auto Phrase.
   b. In the **Phrase Text** field, type the text that is commonly used for the contacts based on the selected attributes.
   c. Click **Create**.

      The system adds the Auto Phrase in the Phrase not in this group section.
6. In the Phrase not in this group section, select the Auto Phrase and click the **<<** button to add the Auto Phrase to the Phrase Group:

   The system moves the Auto Phrase in the Phrase in this group section.
7. In the Edit Attributes section, select the required attributes that you want to add to the Phrase Group.
8. Click **Save**.

Creating a Page Push URL for Co-Browsing

About this task

An agent can start a Co-browsing session to assist a customer. The agent and customer can browse the same web pages simultaneously to collaborate and accomplish certain tasks. The agent can assist the customer to navigate through the web pages and, if required, in filling out forms. In Avaya Workspaces, an agent can choose a web page, from a list of Page Push URLs, to share and Co-browse with the customer.

Configure the Page Push URLs and ensure that the names are descriptive to assist agents when using Avaya Workspaces.

You can configure maximum 50 URLs.

Procedure

1. Start Omnichannel Administration Utility.
2. In the left pane, click **Web Chat**.

3. Click **Page Push URLs**.
4. In the **Group Name** field, enter a descriptive group name.
5. Click **Create**.
6. In the **Page Push Group** field, select the group.
7. In the **URL** field, enter a URL to test Co-browsing.
8. In the **Description** field, enter a descriptive name for the URL.
9. Click **Create**.

   The system adds the test URL to the URLs not in Group section.
10. In the URLs not in Group section, select the test URL and click **Add**.

    The system moves the test URL to the URLs in Group section.

    Ensure that the **Co-Browse** check box for the test URL is selected.
11. In the Edit Attributes section, select the required attributes for the agents with access to this Co-Browsing Group and URL.
12. Click **Save**.

Creating Chat Headers using Omnichannel Administration Utility

Before you begin

- Configure at least one Chat History Header prepared response.
- Configure an email inbox.

Procedure

1. Start Omnichannel Administration Utility.
2. In the left pane, click **Web Chat**.
3. Click **Chat Headers**.
4. In the **Chat Header** field, select the Chat History Header prepared response that you configured.
5. In the **From Address** field, select the email inbox that you configured.
6. In the **Edit Attributes** field, select the attributes for the chat header.
7. In the **Default Chat Header** field, select the default chat header.
8. In the **Default From Address** field, select the default email inbox.
9. Click **Save**.

Related links

Configuring a Chat History Header prepared response on page 380
Configuring Email inboxes on page 374

Configuring CORS for the sample Chat client

About this task

Use this procedure to Configure Cross-origin Resource Sharing (CORS) for the sample Chat client. 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.

Procedure

1. Start Omnichannel Administration Utility.
2. In the left pane, click **Web Chat**.
3. Click **Config**.
4. In the Web Chat Security section, in the **External Web Server Domain** field, enter one of the following values:
   - To allow all domains, enter an asterisk wildcard `*`.

     Important:

     - If you keep this field blank, the system does not allow any domains and refuses all chats.
     - Do not perform this step in Production.
   - To allow a single external server or domain, enter the IP address or FQDN of the server where the sample Chat client is hosted.

Removing attributes and routepoints from Omnichannel Database

About this task

When you remove attributes and routepoints from Avaya Control Manager, they are not removed from Omnichannel Database. Therefore, you must use this procedure to permanently remove them from Omnichannel Database.

Procedure

1. Start Omnichannel Administration Utility.
2. In the left pane, click **General Administration** > **System** > **Attribute cleanup**.
3. On the Attributes tab, select the check box for the attribute that you want to remove.
4. In the Groups section, check if any groups are attached to the attribute.
5. If no groups are attached to the attribute, click **Delete**.
6. If any groups are attached to the attribute, do the following:
   a. Select the group and click **Edit**.

      Omnichannel Administration Utility redirects you to the edit page of the group.

   b. On the edit page of the group, unassign the attribute and click **Save**.

   c. In the left pane, click **General Administration** > **System** > **Attribute cleanup**.

   d. On the Attributes tab, select the check box for the attribute.
   e. In the Groups section, check if any groups are attached to the attribute.
   f. Repeat Step a to Step e until you unassign the attribute from all groups.
   g. After you unassign the attribute from all groups, click **Delete** to remove the attribute.

7. Select the **Routepoints** tab.
8. On the Routepoints tab, select the check box for the routepoint that you want to remove.
9. In the Rules section, check if any rules are attached to the routepoint.
10. If no rules are attached to the routepoint, click **Delete**.
11. If any rules are attached to the routepoint, do the following:
    a. Select the rule and click **Edit**.

       Omnichannel Administration Utility redirects you to the edit page of the rule.

    b. On the edit page of the rule, unassign the routepoint and click **Save**.
    c. In the left pane, click **General Administration** > **System** > **Attribute cleanup**.
    d. On the Routepoints tab, select the check box for the routepoint.
    e. In the Rules section, check if any rules are attached to the routepoint.
    f. Repeat Step a to Step e until you unassign the routepoint from all rules.
    g. After you unassign the routepoint from all rules, click **Delete** to remove the routepoint.

Deploying the sample Chat application

About this task

Avaya provides a sample Chat application for Avaya Oceana® Solution. You must deploy, configure, and use this sample web application to verify your Chat implementation. The sample application also includes Developer documentation for reference.

Note:

Before you start customizing your solution, ensure that you use the sample Chat application to verify Chat contact routing in your solution.

Procedure

1. Download the sample Chat application for Avaya Oceana® Solution from the Avaya DevConnect portal at http://www.avaya.com/devconnect.

   For example, `ocp-web-ui-xx.xx.xx.war`.

   For information about Avaya DevConnect, see *Avaya DevConnect Program Guide* available on https://support.avaya.com.

2. Obtain an Apache HTTP server for Chat in Avaya Oceana® Solution.

3. Deploy the sample Chat war file on the server.
4. In your web browser, enter the following URL to open the sample Chat client:

   `<Apache HTTP Server IP Address>:8080/WebUI/home.html`

Configuring the sample Chat user interface

About this task

Use this procedure to configure the sample application user interface for Chat.

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.

Configuring messaging transcripts

Procedure

1. Start Omnichannel Administration Utility.
2. In the left pane, click **Transcripts**.
3. Click **Config**.
4. Navigate to the Messaging Transcript Access section.
5. In the **Web Service** field, type the complete URL of the filtering service.

   For example, `http://127.0.0.1/CustomerFilterMessages/filter`. If your service listens on a port other than 80 or 443, include the port number.
6. In the **Send Option** field, select the appropriate option:
   - `Do not send`
   - `Legacy transcript`
   - `Enhanced transcript`
7. Click **Save**.

Configuring regular retry of failed messaging transcripts

About this task

Use this procedure to configure regular retry of failed messaging transcripts.

Before you begin

Ensure that you enable messaging transcripts and configure the messaging transcript web service.

Procedure

1. Start Omnichannel Administration Utility.
2. In the left pane, click **Transcripts**.
3. Click **Config**.
4. **(Optional)** In the **Number of days to retry** field, set the number of days the CustomerControllerService retries to send a transcript to the transcript service.

   After reaching this limit, the transcript is set to *Failed* and the CustomerControllerService stops the retry. This value applies to email and messaging.
5. Navigate to the **Transcript Resend Schedule** section.
6. In the **Messaging retry time** field, select the start and end time.

The start time and end time in the **Messaging retry time** field must be different from the start time and end time in the **Email retry time** field. Any change in the start or end time takes 15 minutes to get updated.

7. 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 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`.
    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 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**.

Chapter 28: Verify Chat contacts using Avaya Workspaces

Verify Chat contacts using Avaya Workspaces

This section describes how to use Avaya Workspaces to verify that the Avaya Oceana® Solution 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:

   - *Deploying Avaya Workspaces for Oceana®*
   - *Using Avaya Workspaces for Oceana®*
   - *Administering Avaya Workspaces for 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® Solution deployment that supports up to 100 active agents, enter `https://<AvayaOceanaCluster1_FQDN>/services/UnifiedAgentController/workspaces/#/login`.
   - For an Avaya Oceana® Solution 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® Solution 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 Avaya Automated Chat, proceed to step 5.

   For solutions using Avaya Automated Chat 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 Avaya Automated Chat.

   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 29: Configure Email

Configure Email

This section describes how to configure Avaya Oceana® Solution to support Email contacts.

❗ **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® Solution, they can impact the performance or can cause damage to your contact center solution. Do not use the Avaya Oceana® Solution Email Service as a SPAM filtering tool.

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 running and accepting state.

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration** > **Avaya Oceana™** > **Server Details**.
3. Either double-click the administered Avaya Oceana® Solution UCA server, or select the administered Avaya Oceana® Solution UCA server and click **Edit**.
4. Select the **Providers** tab.
5. To add the Email Provider, perform the following steps:
    a. Click **Add**.
    b. In the **Type** field, select **Email**.
    c. In the **Name** field, keep the value `OCP Email`.
    d. In the **Address** field, enter `email`.
    e. Click **Save**.

Important:

To make the new provider available to Avaya Workspaces agents, you must restart the clusters.

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 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

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 the **IP Address** field, enter the IP address of your Email server.
    c. In the **Port** field, 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® Solution.

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 want to retain active instances	3	24	Default value
WorkAssignmentManagerService	IMPU WorkItem Queued state for Email 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 email contacts supported by Avaya Oceana® Solution 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 29.

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 Email timeout in milliseconds** attribute.
12. Select **Override Default**.
13. Type the maximum number of milliseconds to retain active Work Assignment EmailWorkItems. The maximum time is 2073600000 ms (24 days).

    For more information, see WorkAssignmentManagerService attributes on page 531.
14. Click **Commit**.
15. Reboot Avaya Oceana® Cluster 1.

Configuring an Outbound SMTP server

About this task

The Outbound SMTP server delivers the Email messages that are sent from the Contact Center.

Procedure

1. Start Omnichannel Administration Utility.
2. In the left pane, click **General Administration**.
3. Click **Server Settings**.
4. Click **New**.
5. From the drop-down 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 so that you can poll multiple Email servers for the Email messages to be routed to agents. The Inbound Mail server handles Email messages coming into the Contact Center.

Procedure

1. Start Omnichannel Administration Utility.
2. In the left pane, click **General Administration**.
3. Click **Server Settings**.
4. Click **New**.
5. From the drop-down 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 left 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

Procedure

1. Start Omnichannel Administration Utility.
2. In the left 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-Response - Regular** or **Auto-Response - Out of Hours**.
    d. In the **Subject** field, enter the appropriate subject.
    e. In the **Body** field, enter the appropriate text.
    f. Click **Save**.

Configuring an automatic suggestion response

Procedure

1. Start Omnichannel Administration Utility.
2. In the left 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 left pane, click **E-mail**.
3. Click **Recipient Addresses**.
4. Click **New**
5. In the **Mailbox Type** field, select `Mail Store`.
6. In the Mailbox Details section, perform the following steps:
    a. In the **Mailbox** field, enter the SMTP mailbox name.
    b. In the **Domain** field, enter the domain for your Email server.
    c. In the **Display Name** field, enter the name to appear in the Email From address.

    Note:

    Avaya Oceana® Solution or EmailService logs in to a specific mailbox on the configured mail store by using `username@domain` instead of `username`.
7. In the Password section, perform the following steps:
    a. In the **Password** field, enter the password for the mailbox.

    Important:

    When you change a password on the Email server, you must update the password in this field.

    b. In the **Confirm Password** field, re-enter the password for the mailbox.

8. In the Servers section, perform the following steps:

    a. In the **Inbound (POP3) Server** field, select the host name of your POP3 or IMAP server along with the respective security protocol.

    b. In the **Inbound Mail Threshold** field, enter 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.

    c. In the **Outbound SMTP Server** field, select the host name of your SMTP server.

9. In the **Rule Group** field, select the name of the Rule Group to assign to the recipient mailbox.
10. Select the **Agent Initiated Email** check box.
11. **(Optional)** If the mailbox is shared, do the following:

    a. Select the **Shared** check box.

    b. In the **Username** field, enter the user name of the account used to connect to the mailbox.

12. Click **Save**.

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.

Before you begin

Configure an automatic response and an automatic suggestion response.

Procedure

1. Start Omnichannel Administration Utility.
2. In the left 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 Rules section, perform one of the following steps:
   - Click the plus sign **(+)** button.
   - Select an existing rule.
6. In Current Search Criteria section, click **New**.
7. To add a 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 weightage must add up to 100 percent.
8. To add a 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 weightage must add up to 100 percent.
9. In Current Search Criteria Summary section, click the rule name to view the details of each criterion 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 **>**.

    You can remove an automatic suggestion for the rule by clicking **<**.
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.
19. In the right pane, select the attributes.

    For example, Language.English.
20. Click **Save**.

Configuring Email Open Interfaces

Before you begin

- Configure a custom Web service that conforms to the Web Service Description Language (WSDL) standards.
- Configure the rule associated with the Web service from the Rule Groups section in the Omnichannel Administration Utility.

Procedure

1. Start Omnichannel Administration Utility.
2. In the left pane, click **E-mail**.
3. Click **Open Interfaces**.
4. Click **New**
5. In the **WSDL URL** field, enter the URL of the WSDL.
6. Click **Discover**.

   The system sends a query to the WSDL URL and lists the methods retrieved from the URL in the Open Interfaces method discovery dialog box.
7. In the Open Interfaces method discovery dialog box, select the methods that you want to add to the Web service and click **Add**.

   To add all methods, you can click **Add all**.
8. In the Methods section, click **New** to create a new method.

   To edit an existing method, you can select the method and click **Edit**.
9. In the **Method** field, enter a name for the method.
10. In the **Display Name** field, enter the name that you want to display for the method.

    Note:

    The display name must be unique across all Web services.
11. In the Input Parameters section, do the following:

    a. Select the parameter that you want to move to the list of parameters that must be passed to the Web service.

    b. Click **>**.

    The Input parameter list is a static list of the fields from the email.

    To remove a parameter from the list of parameters, you can select the parameter and click **<**.

12. In the Output Parameters section, do the following:
    a. Select the parameter that you want to move to the list of parameters that must be returned from the Web service.
    b. Click **>**.

    Output parameters replace or complement the original rule output. For example, the Web service can determine a different skillset or priority for the email, manipulate the body of the email, or return a screen pop or knowledge base links.

    To remove a parameter from the list of parameters, you can select the parameter and click **<**.
13. Click **Save**.
14. 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 left pane, click **E-mail**.
3. In the left pane, click **Sender Groups**.
4. Click **New**
5. 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**.

6. In the left pane, click **Rule Groups**.
7. Select an existing Rule Group and click **Edit**.
8. In Rules section, click the plus sign (**+**) button.
9. In New Rule section, click **New**.
10. In the **Add New Criterion** field, select **Sender Group** and click **Go**.
11. In the Sender Groups section, select the Sender Group that you created and click **>**.
12. Click **OK**.
13. Click **Next**.
14. Click **Next**.
15. Select the **Will Close Contact** check box.
16. Click **Next**.
17. 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.

Configuring a Chat History Header prepared response

Procedure

1. Start Omnichannel Administration Utility.
2. In the left pane, click **E-mail**.
3. Click **Prepared Responses**.
4. Perform the following steps to configure a Chat History Header prepared response:
   a. Click **New Response**.
   b. In the **Name** field, enter a name for the response.
   c. In the **Type** field, click **Chat History Header**.
   d. In the **Subject** field, enter the appropriate subject.

e. In the **Body** field, enter the appropriate text.

f. Click **Save**.

Enabling the backup for inbound emails

About this task

When Avaya Oceana® Solution processes an email from a mailbox, the email is deleted from the mail server. Omnichannel Administration Utility provides an option to retain a copy of the email in a new backup folder in the mail server.

Other external business processes can continue to have access to the original email. This option is applicable only for IMAP but not for POP3. Customers must ensure that they manage the size of the backup folder.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Click **General Settings**.
4. In the content pane, select the **Backup inbound mails in separate mail store folder** check box.
5. Click **Save**.

Deploying the sample Email 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 Engagement Designer **Designer Console**:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`

2. Click **Import**.
3. On the Import Workflow dialog box, click **Choose File**.
4. Browse to the sample workflow and click **Import**.
5. Click **Save Workflow**.

6. On the Save Workflow dialog box, do the following:
    a. In the **Workflow** field, type `OceanaEmailAssistedService`.

       You can also provide any other 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. On the Deployment Details dialog box, click **OK**.
10. In your web browser, enter the following URL to open Engagement Designer **Admin Console**:

    `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.

Deploying the sample Transfer to Service workflow for Email

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 Engagement Designer **Designer Console**:

    `https://`*`<AvayaOceanaCluster1_FQDN>`*`/services/EngagementDesigner/index.html`
2. Click **Import**.
3. On the Import Workflow dialog box, click **Choose File**.
4. Browse to the sample workflow and click **Import**.
5. Click **Save Workflow**.
6. On the Save Workflow dialog box, do the following:
    a. In the **Workflow** field, type `OceanaEmailTransfer`.

       You can also provide any other name for the workflow.
    b. Select the folder where you want to save the workflow.

   c. Click **Save**.

7. Click **Deploy Workflow**.
8. On the Deployment Details dialog box, click **OK**.
9. In your web browser, enter the following URL to open the Engagement Designer **Admin Console**:

   `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 Engagement Designer **Admin Console**:

   `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_TO_SERVICE**.
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.

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 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® Solution.
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 transcripts

Procedure

1. Start Omnichannel Administration Utility.
2. In the left pane, click **Transcripts**.
3. Click **Config**.
4. Navigate to the Email Transcript Access section.
5. In the **Web Service** field, type the complete URL of the filtering service.
6. In the **Send Option** field, select the `Send` option.
7. Click **Save**.

Configuring regular retry of failed email transcripts

About this task

Use this procedure to configure regular retry of failed email transcripts.

Before you begin

Ensure that you enable email transcripts and configure the email transcript web service.

Procedure

1. Start Omnichannel Administration Utility.

2. In the left pane, click **Transcripts**.
3. Click **Config**.
4. **(Optional)** In the **Number of days to retry** field, set the number of days the EmailService retries to send a transcript to the transcript service.

   After reaching this limit, the transcript is set to *Failed* and the EmailService stops the retry. This value applies to email and messaging.
5. Navigate to the **Transcript Resend Schedule** section.
6. In the **Email retry time** field, select the start and end time.

   The start time and end time in the **Messaging retry time** field must be different from the start time and end time in the **Email retry time** field. Any change in the start or end time takes 15 minutes to get updated.
7. 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 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`.
   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 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**.

Sending email transcripts

Procedure

1. Start Omnichannel Administration Utility.
2. In the left pane, click **E-mail**.
3. Click **General settings**.
4. Navigate to the **Transcript properties** section.
5. Select the **Send email transcript** check box.
6. In the **Transcript Location** field, type the location of the transcripts.
7. Click **Save**.

Chapter 30: Verify Email contacts using Avaya Workspaces

Verify Email contacts using Avaya Workspaces

This section describes how to use Avaya Workspaces to verify that the Avaya Oceana® Solution 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:

   - *Deploying Avaya Workspaces for Oceana®*
   - *Using Avaya Workspaces for Oceana®*
   - *Administering Avaya Workspaces for 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® Solution deployment that supports up to 100 active agents, enter `https://<AvayaOceanaCluster1_FQDN>/services/UnifiedAgentController/workspaces/#/login`.
   - For an Avaya Oceana® Solution 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® Solution 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 31: Configure SMS

Configure SMS

This section describes how to configure Avaya Oceana® Solution to support Short Message Service (SMS) contacts.

Avaya provides the following two options:

- ZangSmsConnector Snap-in: To support Inbound and Outbound messaging through Avaya Oceana® Solution.
- 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 Zang.	For information about how to create an account, see *Getting Started with Zang Cloud* at https://zang.io/products/cloud/messaging.
An SMS capable number in the required region.	Purchase an SMS capable number from the Zang account, and configure the number in the OCP administration tool and set it as a default sender number.

Configuring Zang for inbound messages

About this task

To receive incoming messages using ZangSmsConnector, you must include the SMS Request Url for your phone number on the Zang.io dashboard.

Procedure

1. Log on to Zang.io.
2. Click **Numbers** > **Manage Numbers**.
3. Click the **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/<Account SID>/SMS/Incoming`.

Where <Account SID> is the Account SID displayed for the Zang account on the Zang dashboard.

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 running and accepting state.

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration** > **Avaya Oceana™** > **Server Details**.
3. Either double-click the administered Avaya Oceana® Solution UCA server, or select the administered Avaya Oceana® Solution UCA server and click **Edit**.
4. Select the **Providers** tab.
5. To add the SMS Provider, perform the following steps:
    a. Click **Add**.
    b. In the **Type** field, select **SMS**.
    c. In the **Name** field, keep the value `OCP ShortMessageService`.
    d. In the **Address** field, enter `sms`.
    e. In the **Auto Answer Timer (sec)** field, enter the time in seconds after which the interaction must be answered automatically.
    f. Click **Save**.

    Important:

    To make the new provider available to Avaya Workspaces agents, you must restart the clusters.

Configuring SMS Gateway

About this task

This is used to tie accounts to a snap-in and also used by the snap-in when querying for their account details.

Procedure

1. Start Omnichannel Administration Utility.
2. In the left pane, click **Messaging**.
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.

Note:

ZangSmsConnector snap-in uses only the API ID, API Password, and Snapin fields.

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.
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 10.
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 Snap-in or SMSVendorSnapin SVAR

About this task

Use this procedure to load the ZangSmsConnector Snap-in SVAR 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.

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 OceanaConfiguration service does not cover the configuration of SMSVendorSnapin attributes. Therefore, you must configure these attributes separately.

- 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.

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 checkbox.
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.

Table continues…

Name	Description
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.

ZangSmsConnector attributes

You must configure the Snap-In attributes in System Manager and configure the Zang account gateway attributes through Omnichannel Administration Utility.

DEFAULT_GROUP

Name	Description
Default Sender number	The default sender number for sending requests. Used for Breeze mode.
Maintenance Mode	The attribute to enable the maintenance mode. The supported values are true and false. The default value is false. Used for Oceana mode.
Test mode enabled	The attribute to enable or disable the test mode. To enable the test mode, set this attribute to true. To disable the test mode, set this attribute to false. The default value is false.
Zang Account SID	The account SID for Zang. This SID must correspond to the account created on www.zang.io. If the GlobalZangConfig snap-in is loaded in System Manager, the default value of ZangSmsConnector is updated with the value of the GlobalZangConfig meta-attribute. The GlobalZangConfig meta-attribute mentions the Account SID for ZangSmsConnector. Used for Breeze mode.

Table continues…

Name	Description
Zang Authentication Token	The attribute where you can specify the authentication token associated with the account created on www.zang.io. If the GlobalZangConfig snap-in is loaded in System Manager, the default value of ZangSmsConnector is updated with the value of the GlobalZangConfig meta-attribute. The GlobalZangConfig meta-attribute mentions the Account SID for ZangSmsConnector. Used for Breeze 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.

OCEANA

Name	Description
Oceana Mode	The attribute to enable Oceana support for Zang. 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 Breeze node IP or Cluster IP of the cluster that hosts the Oceana Messaging snap-in. This option is mandatory to support the Oceana mode.
Oceana Messaging Service name	The name of the MessagingService snap-in. This option is mandatory to support the Oceana mode.

Verifying the SMSVendorSnapin deployment

About this task

Use this procedure to verify the deployment of the SMSVendorSnapin service.

Important:

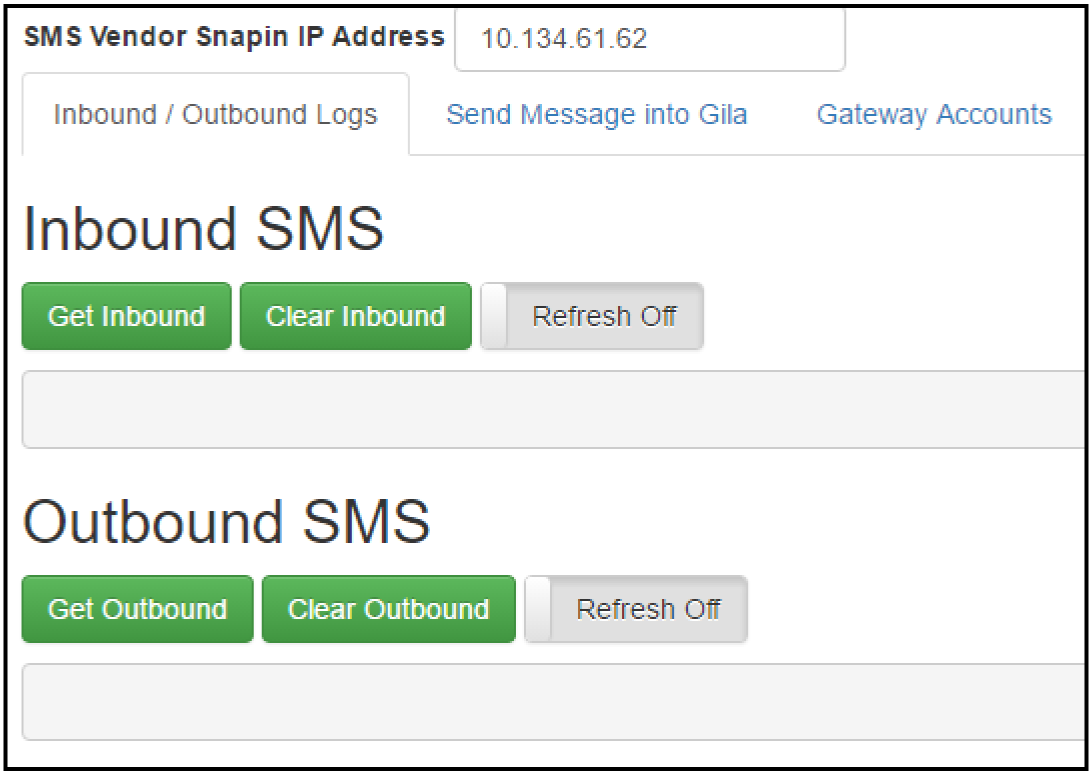
The SMSVendorSnapin service is only for testing purposes. Therefore, do not use this service in your production environment.

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:



SMS Vendor Snapin IP Address: 10.134.61.62

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

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 Engagement Designer **Designer Console**:

   ```
   https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/
   index.html
   ```

2. Click **Import**.
3. On the Import Workflow dialog box, click **Choose File**.
4. Browse to the sample workflow and click **Import**.
5. Click **Save Workflow**.
6. On the Save Workflow dialog box, do the following:
   a. In the **Workflow** field, type `OceanaSMSAssistedService`.

      You can also provide any other name for the workflow.

   b. Select the folder where you want to save the workflow.

   c. Click **Save**.
7. Click **Deploy Workflow**.
8. On the Deployment Details dialog box, click **OK**.
9. In your web browser, enter the following URL to open the Engagement Designer **Admin Console**:

   ```
   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 **BotEnabled** field, keep the default value `True`, which specifies that the workflow always tries 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`.

Deploying the sample Transfer to Service workflow for SMS

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 Engagement Designer **Designer Console**:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`
2. Click **Import**.
3. On the Import Workflow dialog box, click **Choose File**.
4. Browse to the sample workflow and click **Import**.
5. Click **Save Workflow**.
6. On the Save Workflow dialog box, do the following:
   a. In the **Workflow** field, type `OceanaSMSTransfer`.

      You can also provide any other name for the workflow.

   b. Select the folder where you want to save the workflow.

   c. Click **Save**.
7. Click **Deploy Workflow**.
8. On the Deployment Details dialog box, click **OK**.
9. In your web browser, enter the following URL to open the Engagement Designer **Admin Console**:

   `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 **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.

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 Engagement Designer **Admin Console**:

   `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_TO_SERVICE**.
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.

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 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® Solution.
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 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`.
   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 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**.

Chapter 32: Verify SMS contacts using Avaya Workspaces

Verify SMS contacts using Avaya Workspaces

This section describes how to use Avaya Workspaces to verify that the Avaya Oceana® Solution 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:

   - *Deploying Avaya Workspaces for Oceana®*
   - *Using Avaya Workspaces for Oceana®*
   - *Administering Avaya Workspaces for 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® Solution deployment that supports up to 100 active agents, enter `https://<AvayaOceanaCluster1_FQDN>/services/UnifiedAgentController/workspaces/#/login`.
   - For an Avaya Oceana® Solution 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® Solution 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 Message into Gila** 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 **Messaging** > **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 33: Configure Social Media

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 running and accepting state.

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration** > **Avaya Oceana™** > **Server Details**.
3. Either double-click the administered Avaya Oceana® Solution UCA server, or select the administered Avaya Oceana® Solution UCA server and click **Edit**.
4. Select the **Providers** tab.
5. To add the Social Media Provider, perform the following steps:
    a. Click **Add**.
    b. In the **Type** field, select **Social**.
    c. In the **Name** field, keep the value `OCP Social`.
    d. In the **Address** field, enter `OCP Social`.
    e. Click **Save**.

    Important:

    To make the new provider available to Avaya Workspaces agents, you must restart the clusters.

Enabling language routing for Social Media interactions

About this task

Use this procedure to enable language routing for Social Media interactions originating from Avaya Messaging Automation.

Before you begin

Configure the attributes for all languages in Avaya Control Manager.

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 **MessagingService**.
3. For **Social Analyze Language**:
    a. Select **Override Default**.
    b. In the **Effective Value** field, select `true` if you want to enable language identification.
4. For **Social language and attributes map**:
    a. Select **Override Default**.
    b. In the **Effective Value** field, enter the values for the languages in the following format:

    `<Language1_Code>,Language.<Language1_Name>;<Language2_Code>,Language.<Language2_Name>`;

    - *<Language1_Code>* and *<Language2_Code>* are the language codes that Avaya Messaging Automation sends to Avaya Oceana® Solution.
    - *Language.<Language1_Name>* and *Language.<Language2_Name>* are the attributes that you configured in Avaya Control Manager.

    For example, to configure this attribute for English and French languages, type `en,Language.English;fr,Language.French;`.

    Social Media contacts are routed based on the language of the contact. When a customer sends a Social Media message, Avaya Messaging Automation analyzes the language of the contact, generates the language code, and sends the code to Avaya Oceana® Solution. Avaya Oceana® Solution maps the language code with the relevant language attribute configured in the **Social language and attributes map** field.

    For example, Avaya Oceana® Solution maps the `en` language code received from Avaya Messaging Automation with the `Language.English` attribute.

    Note:

    If the language code that Avaya Messaging Automation sends to Avaya Oceana® Solution does not match any of the language attributes configured in this field, Avaya Oceana® Solution does not use the language attribute for routing the contact.
5. Click **Commit**.

Configuring Social Media for Avaya Messaging Automation

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **Messaging**.
3. Click **Social Configuration**.
4. Click **Create**.
5. On the Account tab, do the following:
    a. In the **Create Snapin** section, in the **Name** field, enter the same name that you configured for Social Media in the **Messaging Snapin Key** attribute of MessagingService or **Snap-in Key** attribute of the OceanaConfiguration service.

    You can enter 1 to 100 characters in this field.

    b. Click **Create**.

    c. In the **Snapin** field, select the snap-in that you created.

    d. 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.

    e. In the **Secret Access Key** field, enter the secret access key from the queue.

    You can enter 1 to 100 characters in this field.

    f. In the **Gateway Name** field, enter the name of the gateway.

    You can enter 1 to 100 characters in this field.

    g. In the **Zone** field, enter the AWS zone where Avaya Messaging Automation is communicating.

    You can enter 0 to 100 characters in this field.

    h. In the **Social Type** field, type `Slate`.

    You can enter 0 to 200 characters in this field.

    i. In the **Account** field, enter the AWS account where Avaya Messaging Automation is communicating.

    You can enter 0 to 100 characters in this field.

    j. In the **Region** field, enter the Amazon Web Services (AWS) region where Avaya Messaging Automation is communicating.

    You can enter 0 to 20 characters in this field.

    For information about AWS regions, see https://docs.aws.amazon.com/general/latest/gr/rande.html.

k. In the **Tenants** field, enter the AWS tenants where Avaya Messaging Automation is communicating.

   You can enter 0 to 100 characters in this field.

l. In the **Domain Name** field, do the following:

   - For China (Beijing) and China (Ningxia) regions, enter the value `cn`.
   - For all other regions, do not enter any value.

   You can enter 0 to 100 characters in this field.

   For China (Beijing) and China (Ningxia) regions, you must enter the values manually because the Amazon SQS endpoints for these regions ends with the extension cn. For example, sqs.cn-north-1.amazonaws.com.cn.

   For more information about Amazon SQS endpoints, see https://docs.aws.amazon.com/general/latest/gr/rande.html.

m. In the **Header Access Key** field, enter the unique access key for this channel.

   You can enter 0 to 100 characters in this field.

n. In the **Access Key ID** field, enter the access ID to read data from the queue.

   You can enter 0 to 100 characters in this field.

o. In the **Callback URL** field, enter the URL hosted by the gateway.

   You can enter 0 to 100 characters in this field.

p. In the **Priority** field, select the priority from 1 to 10.

6. Click **Save**.
7. Select the **Details** tab.
8. On the Details tab, do the following:

   a. Click **Create**.

   b. In the **Social Handle** field, enter the social handle.

      You can enter 1 to 100 characters in this field.

      For example:

      - For Twitter, enter your Twitter handle.

        If your Twitter handle is `SocialPage`, you must type `SocialPage` in this field.

      - For Facebook, enter the page ID instead of your Facebook handle.

        If your Facebook handle is `SocialPage` and the page URL is `https://www.facebook.com/SocialPage-369854850048396/?fref=nf`, you must type `369854850048396` in this field.

   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.

You can enter 0 to 100 characters in this field.

d. In the **Routepoint** field, select the Route Point name to apply for the rule. You must select the Route Point that you configured using Avaya Control Manager.

   ❗ **Important:**

   You must select a Route Point when configuring Social Gateways.

e. In the **Gateway Account** field, select the account that you created in Step 5.

f. In the **Edit Attributes** section, select the attributes based on which the incoming Social Media messages must be routed.

   ❗ **Important:**

   Skip this step if you already configured the language attributes in MessagingService.

g. Click **Save**.

Configuring secure communication to Avaya Messaging Automation

Procedure

1. In your web browser, open the following URL:

   `https://sqs.<Region>.amazonaws.com/`

   <Region> is the Amazon Web Services (AWS) region that you specified in the **Region** field while configuring Social Media for Avaya Messaging Automation.

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.

Configuring Social Media for third-party gateways

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **Messaging**.
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.
    e. In the **Social Type** field, type `Devconnect`.
    f. In the **Header Access Key** field, enter the unique access key for this channel.
    g. In the **Callback URL** field, enter the URL hosted by the third-party gateway.
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. 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

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 Engagement Designer **Designer Console**:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`

2. Click **Import**.
3. On the Import Workflow dialog box, click **Choose File**.
4. Browse to the sample workflow and click **Import**.
5. Click **Save Workflow**.
6. On the Save Workflow dialog box, do the following:
   a. In the **Workflow** field, type `OceanaSocialAssistedService`.

      You can also provide any other name for the workflow.

   b. Select the folder where you want to save the workflow.
   c. Click **Save**.
7. Click **Deploy Workflow**.
8. On the Deployment Details dialog box, click **OK**.
9. In your web browser, enter the following URL to open the Engagement Designer **Admin Console**:

   `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 **BotEnabled** field, keep the default value `True`, which specifies that the workflow always tries 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`.

Deploying the sample Transfer to Service workflow for Social Media

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 Engagement Designer **Designer Console**:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`

2. Click **Import**.
3. On the Import Workflow dialog box, click **Choose File**.
4. Browse to the sample workflow and click **Import**.
5. Click **Save Workflow**.
6. On the Save Workflow dialog box, do the following:
   1. In the **Workflow** field, type `OceanaSocialTransfer`.

      You can also provide any other name for the workflow.
   2. Select the folder where you want to save the workflow.
   3. Click **Save**.
7. Click **Deploy Workflow**.
8. On the Deployment Details dialog box, click **OK**.
9. In your web browser, enter the following URL to open the Engagement Designer **Admin Console**:

   `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 **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.

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 Engagement Designer **Admin Console**:

   `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_TO_SERVICE**.
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.

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 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® Solution.
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 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`.
    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 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**.

Chapter 34: Verify Social Media contacts using Avaya Workspaces

Verify Social Media contacts using Avaya Workspaces

This section describes how to use Avaya Workspaces to verify that the Avaya Oceana® Solution 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:

   - *Deploying Avaya Workspaces for Oceana®*
   - *Using Avaya Workspaces for Oceana®*
   - *Administering Avaya Workspaces for 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® Solution deployment that supports up to 100 active agents, enter `https://<AvayaOceanaCluster1_FQDN>/services/UnifiedAgentController/workspaces/#/login`.
   - For an Avaya Oceana® Solution 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® Solution 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

Use this procedure to verify that the Social Media messages are routed to agents.

Procedure

1. Access the social page using a social media account.
2. Send a test message through the social page.

   After some time, the system presents the test message to a ready agent.
3. Answer the Social Media contact.

Chapter 35: Configure Outbound

Configure Outbound

This section describes how to enable the Outbound voice capability in Avaya Oceana® Solution by integrating Avaya Proactive Outreach Manager (POM) with Avaya Oceana® Solution.

Install and configure POM

To integrate POM with Avaya Oceana® Solution, you must install and configure POM in Oceana mode. For more information, see:

- *Implementing Avaya Proactive Outreach Manager*
- *Avaya Proactive Outreach Manager Integration*

Configuring the POM server certificate for Avaya Oceana® Cluster 3

Before you begin

Log in to the POM server web interface and export the POM server 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 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 running and accepting state.

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration** > **Avaya Oceana™** > **Server Details**.
3. Either double-click the administered Avaya Oceana® Solution UCA server, or select the administered Avaya Oceana® Solution UCA server and click **Edit**.
4. Select the **Providers** tab.
5. To add the Outbound Provider, perform the following steps:
   a. Click **Add**.
   b. In the **Type** field, select **Outbound**.
   c. In the **Name** field, keep the value `POM`.
   d. In the **Address** field, enter `POM`.
   e. Click **Save**.

      Important:

      To make the new provider available to Avaya Workspaces agents, you must restart the clusters.

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 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® Solution 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® Solution through Avaya Control Manager.

    When creating a POM campaign, the campaign must contain the complete list of all POM Completion Codes.

    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 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® Solution.
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® Solution 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® Solution UCA server, or select the administered Avaya Oceana® Solution 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.
8. Click **Save**.

Chapter 36: Verify Outbound contacts using Avaya Workspaces

Verify Outbound contacts using Avaya Workspaces

This section describes how to use Avaya Workspaces to verify that the Avaya Oceana® Solution 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:

   - *Deploying Avaya Workspaces for Oceana®*
   - *Using Avaya Workspaces for Oceana®*
   - *Administering Avaya Workspaces for 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® Solution deployment that supports up to 100 active agents, enter `https://<AvayaOceanaCluster1_FQDN>/services/UnifiedAgentController/workspaces/#/login`.
   - For an Avaya Oceana® Solution 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® Solution 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 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® Solution.
2. Configure attributes in Avaya Oceana® Solution 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.

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 37: Access Oceana Data Viewer

Oceana Data Viewer overview

Oceana Data Viewer is a debugging and visualization tool for Avaya Oceana® Solution. With this tool, you can view the Chat, Email, SMS, Social, and Generic contacts that are in Omnichannel Database.

With this tool, administrators and support engineers can directly:

- Reply to Email contacts if there is an issue in routing emails.
- Close or requeue Email and Generic contacts.
- Close Social Media, Chat, and SMS contacts.
- View transcripts for Email or Chat contacts that are sent to an external filtering service, and to mark them as permanently or temporarily failed.

Oceana Data Viewer is not a real-time application. Therefore, you must manually refresh the Oceana Data Viewer page to view updated statistics.

Supported browsers

Oceana Data Viewer supports the following browsers:

- Mozilla Firefox 66
- Google Chrome 72
- Microsoft Edge 38

It does not support Microsoft Internet Explorer and mobile browsers.

Logging in to Oceana Data Viewer

About this task

Use this procedure to log in to Oceana Data Viewer to view the Chat, Email, SMS, Social, and Generic contacts in Omnichannel Database.

By default, only one user can be logged in to Oceana Data Viewer at a time. When a new user logs in, any previously logged-in user is automatically logged out. To allow multiple users to log in at the same time, you must configure the **Maximum concurrent user sessions** attribute of the OceanaDataViewer service through System Manager.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, in the **Service URL** column on Avaya Oceana® Cluster 3, select **Oceana Data Viewer**.

   System Manager opens the Avaya Breeze® platform authentication page in a new browser window.
3. On the Avaya Breeze® platform authentication page, do the following:
   a. In the **Username** field, enter the user name of the Avaya Workspaces administrator configured in Avaya Control Manager.
   b. In the **Password** field, enter the password of the Avaya Workspaces administrator configured in Avaya Control Manager.
   c. Click **SIGN IN**.

      The browser window displays the Oceana Data Viewer home page.

Oceana Data Viewer home page

The following table lists the buttons on the Oceana Data Viewer home page:

Button	Description
EMAIL	The button to view the Email home page containing the details of all Email contacts.
SMS	The button to view the SMS home page containing the details of all SMS contacts.
SOCIAL	The button to view the Social home page containing the details of all Social contacts.
GENERIC	The button to view the Generic home page containing the details of all Generic contacts.
CHAT	The button to view the Chat home page containing the details of all Chat contacts.
STATISTIC	The button to view high-level statistics about contact centre operations.

Email contacts management

The following table lists the buttons on the Email home page:

Button	Description	Measures in Avaya Analytics™
New	The button to view actions from Email contacts that are not routed to an agent.	Avaya Analytics™ reports these contacts as new contacts when queuing. When alerting on Avaya Workspaces, they are offered or alerting.
Open	The button to view actions from Email contacts that are answered by an agent and are in progress.	Avaya Analytics™ reports these contacts as active or answered contacts.
Transferred	The button to view actions from Email contacts that are transferred to another agent. These are effectively new contacts that are not routed to an agent. When an agent answers, they are marked as open.	Avaya Analytics™ reports these contacts as new transferred-to-service or waiting contacts.
Failed	The button to view actions from Email contacts that failed to be routed to an agent.	Avaya Analytics™ reports these contacts as completed. If there is one failed Email contact listed here, Avaya Analytics™ reports 0 waiting or new contacts.
Closed	The button to view actions from email contacts that are answered by an agent and are closed.	Avaya Analytics™ reports these contacts as completed, offered, and answered contacts.
Agent Replied	The button to view actions from Email contacts to which an agent has replied.	Avaya Analytics™ does not display these contacts.
In Queue	The button to view actions from email outbound Email contacts that are ready to be sent.	Avaya Analytics™ reports these contacts as the contacts that are waiting but not offered.
Not Sent	The button to view actions from email outbound Email contacts that could not be sent because of a reason such as invalid address.	Avaya Analytics™ does not display these contacts.
Agent Created	The button to view actions from adhoc Email contacts that are created by an agent.	Avaya Analytics™ reports these contacts as adhoc emails.
Failed Transcripts	The button to view actions that failed to be sent out to an external transcript filtering service.	Avaya Analytics™ does not display these contacts.
Successful Transcripts	The button to view actions that are successfully sent out to an external transcript filtering service.	Avaya Analytics™ does not display these contacts.
Permanently Failed Transcripts	The button to view actions that permanently failed to be sent to an external transcript filtering service. The Email Service repeatedly failed to send the transcript over a 30-day period.	Avaya Analytics™ does not display these contacts.

Viewing the details of an email

About this task

When viewing the list of emails in Omnichannel Database, you can view the content of an email. You can also reply to the email contact if the routing is not functional.

Procedure

1. Log in to Oceana Data Viewer.
2. On the Oceana Data Viewer home page, click **EMAIL**.
3. On the Email home page, click the button based on your requirement.

   For example, to view the list of open emails, click **Open**.
4. In the list of emails, locate the required email and click **Details**.

   Oceana Data Viewer displays the Email Details page.

   For transcripts, the Email Details page does not display the body of the email.
5. To reply to the email contact, click **Direct Reply**.

   Oceana Data Viewer opens a new window in your email client to draft a new email.

   ! **Important:**

   Your email client must be able to access the mail server.
6. Copy the content of the original email from the Email Details page to the new window in your email client.

Resending a transcript

About this task

If a temporary failure occurs in sending a transcript, you can resend the transcript.

Oceana Data Viewer rejects the request to resend the transcript if:

- The transcript filtering service URL is empty.
- Omnichannel Administration Utility is set to not allow transcripts to be sent.
- The transcript is already sent successfully.

Procedure

1. Log in to Oceana Data Viewer.
2. On the Oceana Data Viewer home page, click **EMAIL**.
3. On the Email home page, click **Failed Transcripts**.
4. In the list of emails, locate the required email and click **Resend transcripts**.

Oceana Data Viewer reads the configuration from Omnichannel Database and takes the appropriate actions.

Changing the status of a transcript

About this task

With this procedure, you can mark:

- A failed transcript as permanently failed
- A permanently failed transcript as failed.

The purpose of changing the status of a transcript is to prevent corrupted emails from being sent out to the transcript filtering service and repeatedly failing to filter.

Procedure

1. Log in to Oceana Data Viewer.
2. On the Oceana Data Viewer home page, click **EMAIL**.
3. On the Email home page, click **Failed Transcripts**.
4. In the list of emails, locate the required email and click **Mark permanently failed**.

Messaging contacts management

The following table lists the buttons on the Chat, SMS and Social home pages:

Button	Description	Measures in Avaya Analytics™
New	The button to view contacts that are not routed to an agent.	Avaya Analytics™ reports these contacts as new contacts when queuing. When alerting on Avaya Workspaces, they are offered or alerting.
Open	The button to view contacts that are answered by an agent and are in progress.	Avaya Analytics™ reports these contacts as active or answered contacts.
Transferred	The button to view contacts that are transferred to another agent or service. These are effectively new contacts that are not routed to an agent. When an agent answers, they are marked as open.	Avaya Analytics™ reports these contacts as new transferred-to-service or waiting contacts.
Failed	The button to view contacts that failed to be routed to an agent.	Avaya Analytics™ reports these contacts as completed.
Closed	The button to view contacts that are answered by an agent and are closed.	Avaya Analytics™ reports these contacts as completed, offered, and answered contacts.

Table continues…

Button	Description	Measures in Avaya Analytics™
Successful Transcripts	The button to view transcripts for this channel type that are successfully sent out to an external transcript filtering service.	Avaya Analytics™ does not display these contacts.
Failed Transcripts	The button to view transcripts for this channel type that failed to be sent out to an external transcript filtering service.	Avaya Analytics™ does not display these contacts.
Permanently Failed Transcripts	The button to view transcripts for this channel type that permanently failed to be sent to an external transcript filtering service. This status is reserved for the transcripts that repeatedly failed over a 30-day period or the transcripts that are marked as such in Oceana Data Viewer.	Avaya Analytics™ does not display these contacts.

Closing Social Media, SMS, and Chat contacts

About this task

With this procedure, you can close Social Media, SMS, and Chat contacts that are in a new or transferred state. The purpose of closing the contacts is to close old contacts that will never be answered.

After you complete this procedure, the contacts are closed in the OmniResourceConnector service and Avaya Oceana® Solution.

Procedure

1. Log in to Oceana Data Viewer.
2. On the Oceana Data Viewer home page, click **SOCIAL**.
3. On the Social home page, click **New**.
4. In the list of Social contacts, select the check boxes for the contacts that you want to close, and click **Close all checked contacts**.

   The header displays that the contacts are closed and Oceana Data Viewer redirects you to the Social home page.
5. On the Oceana Data Viewer home page, click **SMS**.
6. On the SMS home page, click **New**.
7. In the list of SMS contacts, select the check boxes for the contacts that you want to close, and click **Close all checked contacts**.

   The header displays that the contacts are closed and Oceana Data Viewer redirects you to the SMS home page.
8. On the Oceana Data Viewer home page, click **CHAT**.

9. On the Chat home page, click **New**.
10. In the list of Chat contacts, select the check boxes for the contacts that you want to close, and click **Close all checked contacts**.

    The header displays that the contacts are closed and Oceana Data Viewer redirects you to the Chat home page.

Transcripts page for messaging contacts

The following table lists the fields on the Transcripts page for messaging contacts:

Field	Description
ContactId	The current ID for this contact in Omnichannel Database.
Customer ID	The customer ID.
Work Request ID	The global ID used in Avaya Oceana® Solution to identify contacts. This ID is also referred to as a context ID.
Drilldown	The button to view the drill-down information such as timestamp, sender, message length, and message type.
Resend	The button to resent the transcript.
Mark permanently failed	The button to change the status of the transcript from failed to permanently failed.

Generic contacts management

The following table lists the buttons on the Generic home page:

Button	Description	Measures in Avaya Analytics™
New	The button to view actions from Generic contacts that are not routed to an agent.	Avaya Analytics™ reports these contacts as new contacts when queuing. When alerting on Avaya Workspaces, they are offered or alerting.
Open	The button to view actions from Generic contacts that are answered by an agent and are in progress.	Avaya Analytics™ reports these contacts as active or answered contacts.
Closed	The button to view actions from Generic contacts that are answered by an agent and are closed.	Avaya Analytics™ reports these contacts as completed, offered, and answered contacts.

Table continues…

Button	Description	Measures in Avaya Analytics™
Transferred	The button to view actions from Generic contacts that are transferred to another agent. These are effectively new contacts that are not routed to an agent. When an agent answers, they are marked as open.	Avaya Analytics™ reports these contacts as new transferred-to-service or waiting contacts.
Failed	The button to view actions from Generic contacts that failed to be routed to an agent.	Avaya Analytics™ reports these contacts as completed. If there is one failed email listed here, Avaya Analytics™ reports 0 waiting or new contacts.

Statistics home page

The Statistics home page of Oceana Data Viewer displays the following high-level statistics about contact centre operations:

Statistic	Description
Customers	The total number of customers in Omnichannel Database.
Contacts	The total number of contacts in Omnichannel Database.
Attachments	The total number of attachments in Omnichannel Database.
Oldest Waiting Contact Time	The list of contacts that are not yet answered by agents.
Contacts per Customer	The list of customers with a large number of contacts. Avaya recommends not to have more than 100 contacts per customer.
Contacts closed by DataViewer	The list of contacts that are closed through Oceana Data Viewer.

Chapter 38: Integrate Avaya Workforce Optimization Select with Avaya Oceana® Solution

Integrate Avaya Workforce Optimization Select with Avaya Oceana® Solution

Avaya Workforce Optimization Select integrates with Avaya Oceana® Solution, so that Avaya Workspaces supervisors or agents can access the call recording features of Avaya Workforce Optimization Select.

For information on how to deploy Avaya Workforce Optimization Select and integrate it with Avaya Oceana® Solution, see *Deploying Avaya Workforce Optimization Select with Avaya Aura® Communication Manager and Avaya Oceana® Solution*.

Chapter 39: Configure Centralized Logging for Avaya Oceana® Solution

Centralized Logging is a feature that you can use to view the logs for all services of Avaya Oceana® clusters through a centralized interface. To use this feature, you must first install CentralizedLoggingService on Avaya Oceana® Cluster 4 and set its attributes. After setting the attributes, you must configure Avaya Oceana® Cluster 1, Avaya Oceana® Cluster 2, and Avaya Oceana® Cluster 3 for Centralized Logging.

Note:

- For an Avaya Oceana® Solution deployment that supports 1000 active agents or less, you must install CentralizedLoggingService to Avaya Oceana® Cluster 1 and configure Avaya Oceana® Cluster 3 and Avaya Oceana® Cluster 4 for Centralized Logging.
- The cluster containing CentralizedLoggingService must always have minimum n/2+1 active nodes, where n is the number of Avaya Breeze® platform nodes in the cluster.

  For example, in a three-node cluster, Centralized Logging works only if the cluster has minimum 3/2+1=2 active nodes.

Configuring Avaya Oceana® clusters for Centralized Logging

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 that you want to configure for Centralized Logging and click **Edit**.
3. On the Cluster Editor page, select the **General** tab.
4. In the Cluster Attributes section, perform the following steps:
   a. Select or clear the **Use secure connection for centralized logging** check box based on your requirement.
   b. In the **Centralized logging destination** field, select `Breeze Cluster`.

For a deployment where you install CentralizedLoggingService on an external server, you must select `External Cluster`.

c. In the **Breeze cluster as destination for centralized logging** field, select the cluster that hosts CentralizedLoggingService.

   The system enables this field only if you select `Breeze Cluster` in the **Centralized logging destination** field.

   If you select `External Cluster` in the **Centralized logging destination** field, the system enables the **External destination for centralized logging** field where you must enter the destination of the external cluster in the following format:

   `<Server_IP>``:`*`<Port>`*

   <Server_IP> is the IP address of the external server and *<Port>* is the logstash listening port.

5. 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.

6. Click **OK**.

7. Repeat Step 2 to Step 6 for the other clusters that you want to configure for Centralized Logging.

Security configuration for Centralized Logging

To run Centralized Logging in the secure mode, you must:

- Configure the WebSphere certificate for each node of the cluster that hosts CentralizedLoggingService.
- Select the **Use secure connection for centralized logging** check box while configuring Avaya Oceana® clusters for Centralized Logging.
- Enable the Logstash security while setting CentralizedLoggingService attributes.

Note:

- If you configure only one of the later two, the connection fails.
- If you modify the certificates, you must disable and then enable the security on the cluster and the snap-in to use the new certificates.

Loading and installing MetricbeatService and PacketbeatService SVARs

About this task

Use this procedure if MetricbeatService and PacketbeatService SVARs are not installed on Avaya Oceana® Cluster 1, Avaya Oceana® Cluster 2, and Avaya Oceana® Cluster 3.

With MetricbeatService and PacketbeatService, you can view information such as CPU usage, memory, disk IO, and network analysis.

Before you begin

Ensure that CentralizedLoggingService is operational.

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 MetricbeatService SVAR and click **Open**.
    c. Click **Browse**.
    d. Select the PacketbeatService SVAR and click **Open**.
    e. Click **Load**.
4. In the Accept End User License Agreement dialog box, click **Accept**.
5. On the Services page, do the following:
    a. Verify that the state of the SVARs is `Loaded`.
    b. Select the check box for the MetricbeatService SVAR and click **Install**.
6. In the Confirm install service: MetricbeatService dialog box, select the check box of the cluster where you want to install the SVAR.
7. 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. Repeat Step 6 to Step 9 to install the PacketbeatService SVAR.

Setting MetricbeatService 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 MetricbeatService.
   b. In the **Service** field, click **MetricbeatService**.
3. **(Optional)** For **Enable module - system**, if the effective value is set to `false`, do the following:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, select `true`.
4. Click **Commit**.

Logging in to Kibana

About this task

Use this procedure to log in to Kibana to view the logs for all services of Avaya Oceana® clusters.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, in the **Service URL** column on the cluster that hosts CentralizedLoggingService, select **Kibana URL**.
3. On the Kibana login page, do the following:
   a. In the **Username** field, enter the user name that you configured while setting CentralizedLoggingService attributes.
   b. In the **Password** field, enter the password that you configured while setting CentralizedLoggingService attributes.
   c. Click **Log in**.

Creating an index pattern in Kibana

About this task

Use this procedure to create an index pattern in Kibana. You can create index patterns only for the indices for which logs are available.

Procedure

1. Log in to Kibana.
2. Click **Management** > **Index Patterns**.

   Kibana displays the Create index pattern page.
3. In the Define index pattern area, do the following:
   1. In the **Index pattern** field, type the name of the index for which you want to create an index pattern.

      For example, `metricbeat`.

      Kibana displays the list of indices for which logs are available. It activates the **Next step** button only when the specified index name matches an item in the list of indices.
   2. Click **Next step**.
4. In the Configure settings area, do the following:
   1. In the **Time Filter field name** field, click `@timestamp`.
   2. Click **Show advanced options**.
   3. In the **Custom index pattern ID** field, do the following to properly show all visualizations on dashboards:
      - For MetricbeatService, type `metricbeat-*`.
      - For PacketbeatService, type `packetbeat-*`.
   4. Click **Create index pattern**.

Searching logs in Kibana

Procedure

1. Log in to Kibana.
2. In the navigation pane, click **Discover**.
3. In the content pane, click the time picker on the upper-right of the screen.
4. On the Time Range screen, choose the date and time range for which you want to view logs.
5. In the **Available Fields** list, click the **add** button next to a log field to move the field to the **Selected Fields** list.

   Kibana updates the content pane to display the logs with the log field that you moved.
6. In the **Search** field, type the search text in the lucene query syntax and click the **Search** button.

   Kibana highlights the related logs in the content pane.

Viewing statistics on the Metricbeat dashboard

Before you begin

Create an index pattern for Metricbeat.

Procedure

1. Log in to Kibana.
2. In the navigation pane, click **Dashboard**.
3. On the Dashboard page, click **[Metricbeat System] Overview** to view the metrics overview of the servers where MetricbeatService is running.

Viewing statistics on the Packetbeat dashboard

Before you begin

Create an index pattern for Packetbeat.

Procedure

1. Log in to Kibana.
2. In the navigation pane, click **Dashboard**.
3. On the Dashboard page, click **[Packetbeat] HTTP** to view the HTTP requests from the servers where PacketbeatService is running.

Chapter 40: Deploy Avaya Oceana® Solution for High Availability

Avaya Oceana® Solution High Availability overview

Avaya Oceana® Solution provides the Campus High Availability (HA) functionality. Using this functionality, Avaya Oceana® Solution 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 Avaya Breeze® platform.

This functionality provides mitigation for the following failure scenarios:

- A single Avaya Oceana® Solution 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® Solution HA:

- Avaya Oceana® Solution 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® Solution 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® Solution does not detect the network latency directly. 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 the physical server reconnects to the network. When a network failure isolates a virtual machine or a physical server from the network, Avaya Oceana® Solution 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® Solution. 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® Solution only supports a single failure event. Therefore, if two simultaneous failure events occur, Avaya Oceana® Solution components can not operate in HA mode.

Avaya Oceana® Solution 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 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:

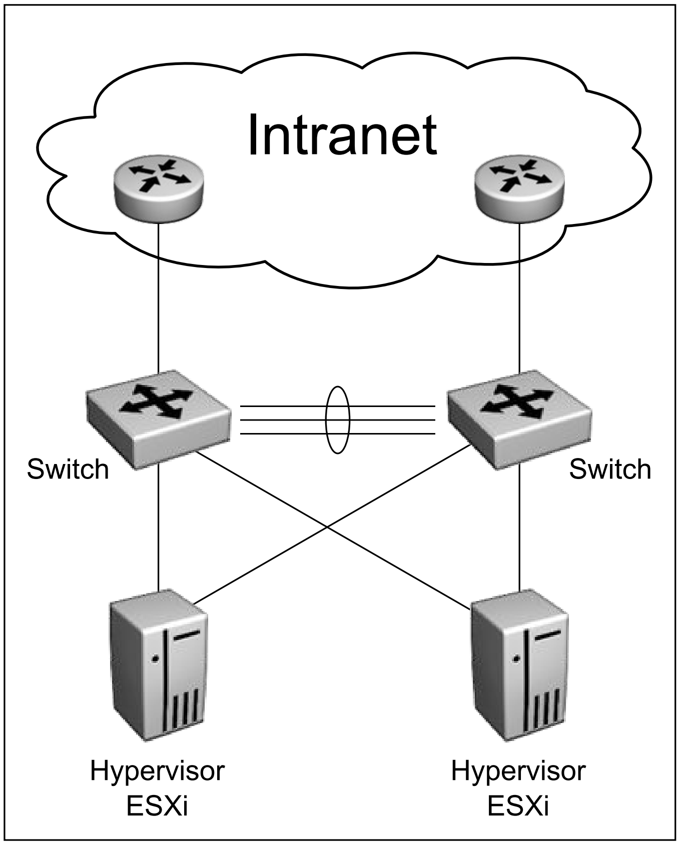
Failure type	Recovery mechanism	Notes	Example
Process Failure	Automatic	-	GigaSpaces PU failure, WebSphere process failure, and Nginx process failure
Virtual Machine Failure	Manual	If an Avaya Breeze® platform node in an Avaya Oceana® cluster becomes faulty or is shut down for testing, you must reboot 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® Solution. Therefore, you must plan the reboot during a maintenance window.	Accidental shutdown
Physical Server Failure	Automatic	After you clear the fault and restart the physical server and virtual machines.	Power failure on a physical server

Table continues…

Failure type	Recovery mechanism	Notes	Example
Network Failure	Manual	Recommission the physical server or the virtual machine.	Accidental disconnection of all network cards of a physical server

In Avaya Oceana® Solution, 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.

Oracle Database HA

Avaya Analytics™ uses Oracle Real Application Cluster (RAC) for Campus HA. RAC consists of two or more RAC nodes running the Oracle Database Application software with an additional server that utilizes Automatic Storage Management (ASM) to manage database files. Both RAC nodes access the ASM shared storage. Therefore, if one instance becomes unavailable, the other instance takes over.

- Avaya Analytics™ database HA is built on the Oracle RAC infrastructure.
- Database failover is automatic and transparent to consumers and producers.
- RAC has an active-active cluster architecture.

Oracle Streams Analytics HA

In Oracle Streams Analytics (OSA) HA, two instances of OSA run active/active. Only the primary instance writes to the Database, JMS, Kafka, and Open Interface RealTime (OSART). Failover occurs automatically and can take up to 10 seconds. However, no data is lost because of the secondary instance. For more information about OSA HA, see *Deploying Avaya Analytics™ for Oceana®*.

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® Solution 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® Solution 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® Solution Disaster Recovery*.

In Omnichannel Database HA, Omnichannel Database:

- Records the transcripts of Chat, Email, 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	Install the Arbiter service on the Avaya Control Manager application server.	See Installing the Arbiter service on page 454.	
2	Configure Cache Mirroring on the active Omnichannel Database server.	See Configuring Cache Mirroring on the active Omnichannel Database server on page 456.	
3	Configure Cache Mirroring on the standby Omnichannel Database server.	See Configuring Cache Mirroring on the standby Omnichannel Database server on page 458.	
4	Configure the Virtual IP address in Cache Mirror on the active Omnichannel Database server.	See Configuring the Virtual IP address on page 460	
5	Configure the network interface on Cache Mirror on the standby Omnichannel Database server.	See Configuring the network interface on page 461.	
6	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 462.	
7	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 463.	
8	Secure the Cache Mirror on the active Omnichannel Database server using TLS.	See Securing the Cache Mirror on the active Omnichannel Database server on page 463.	
9	Secure the Cache Mirror on the standby Omnichannel Database server using TLS.	See Securing the Cache Mirror on the standby Omnichannel Database server on page 464.	

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\Cache2015` folder.
4. In the folder, double-click the `cache_x64.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 Caché Instance Name screen, keep the default instance name and click **Next**.
8. On the Destination Folder screen, keep the default location and click **Next**.
9. On the Setup Type screen, select **Custom** and click **Next**.
10. On the Custom Setup screen, do the following:
    a. Expand the **Caché Database Engine** group.
    b. For the **Agent Service** feature, click the drop-down icon and then click **This feature will be installed on local hard drive**.
    c. For all other features in all groups, click the respective drop-down icons and then click **This feature will not be available**.
    d. Click **Next**.
11. On the Install Unicode Support screen, select **8-bit** and click **Next**.
12. On the Enter port numbers screen, keep the default port numbers and click **Next**.
13. On the Initial Security Settings screen, keep the default value and click **Next**.
14. On the Ready to Install the Program screen, click **Install**.
15. Click **Finish**.
16. 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**.

17. 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.

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** > **Enable Mirror Service**.
4. On the Edit Service dialog box, select the **Service Enabled** check box and click **Save**.
5. 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**.

6. 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**.

7. On Cache Management Portal, click **System Administration** > **Configuration** > **Mirror Settings** > **Create Mirror**.

8. On the Create Mirror page, do the following:

   a. In the **Mirror Name** field, type `AOCMIRROR`.

   b. **(Optional)** If you do not require a secure connection, clear the **Use SSL/TLS** check box.

      If you select this check box, you must provide the details of the certificate to use for TLS.

   c. Select the **Use Arbiter** check box.

   d. In the **Address** field, enter the IP address of the server where you installed the Arbiter service.

   e. In the **Port** field, enter the port number as `2188`.

   f. Ensure that you do not select the **Use Virtual IP** check box.

   g. Click **Advanced Settings**.

   h. In the **Quality of Service Timeout (msec)** field, set the value to `8000`.

   i. Click **Save**.

9. On Cache Management Portal, take a backup of the database by doing the following:

   a. Click **Menu** > **Configure Databases** > **Add to mirror**.

   b. Select the **MULTIMEDIA_DATA** and **COBROWSE_DATA** check boxes, and then click **Add**.

10. Go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\Oceana\BackupAndRestore` folder.

11. Double-click the `BackupAndRestore.exe` file.
12. In the **Select/create file to backup to** field, click **Browse**.
13. 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**.
14. Click **Backup Database**.

    The Backup and Restore application displays the `Backup complete!` message when the backup process is complete.
15. Verify that the backup `zip` file is created at the specified location.

    Note:

    The space required for the backup is twice the size of the database. Therefore, ensure that the server has sufficient disk space. If the server does not have sufficient disk space, the Backup and Restore application displays a warning that there is not enough space for creating the `cbk` file.

    The Backup and Restore application does not display any warning after it creates the `cbk` file and starts the zipping process. Therefore, after the `zip` file is created, you must check its validity.

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.

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** > **Enable Mirror Service**.
4. On the Edit Service dialog box, select the **Service Enabled** check box and click **Save**.
5. 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**.
6. In the Services window, do the following:
   a. Double-click the ISCAgent service.
   b. In the Properties dialog box, click **Start**.
   c. In the **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**.
7. On Cache Management Portal, click **System Administration** > **Configuration** > **Mirror Settings** > **Join as Failover**.
8. On the Join as Failover page, do the following:
   a. In the **Mirror Name** field, type `AOCMIRROR`.
   b. In the **Agent Address on Other System** field, enter the IP address of the active Omnichannel Database server.
   c. In the **Cache Instance Name** field, type `CCDSINSTANCE`.
   d. Click **Save**.
9. Close the Cache Management Portal window before starting the restore process.

   If you do not close the Cache Management Portal window, Cache Management Portal displays an error message.
10. Copy the backup `zip` file from the active server to the standby server.

    Note:

    The drive where you store the backup `zip` file must have sufficient space to store the backup `zip` file and the `cbk` file that you extract from the `zip` file.

11. Go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\Oceana\BackupAndRestore` folder.
12. Double-click the `BackupAndRestore.exe` file.
13. In the **Select file to restore from** field, click **Browse**.
14. On the Open dialog box, do the following:
    a. Browse to the location containing the backup file.
    b. Select the backup `zip` file.
    c. Click **Open**.
15. On the Backup and Restore screen, click **Restore Database**.
16. For **Are you restoring a mirrored backup**, click **Yes**.
17. On the Drive restore screen, do the following:
    a. In the **Select your database drive letter** field, select the drive where you installed the Intersystem Cache database.

       For example, `(MULTIMEDIA drive):\Avaya\CCMM\Databases\CCMM\COBROWSE\DATA`.
    b. Click **Restore**.

    The system displays the `Restore complete!` message after the restore process is completed.
18. 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® Solution databases in the list.

Configuring the Virtual IP address

About this task

Use this procedure to configure the Virtual IP address in the Cache Mirror on the active Omnichannel Database server.

Before you begin

Configure Cache Mirroring on 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**.
4. On the Edit Mirror page, do the following:
    a. Select the **Use Virtual IP** check box.
    b. In the **IP Address** field, enter a Virtual IP address.

        Important:

        Ensure that you enter a virtual IP address that is not assigned to any other machine and is listed on the Domain Name System (DNS) server.
    c. In the **Mask (CIDR format)** field, enter the mask value in CIDR format.

        For example, the mask value for 255.255.255.0 in CIDR format is `24`.
    d. In the **Network Interface** field, select **Ethernet**.
    e. Click **Save**.

Configuring the network interface

About this task

Use this procedure to configure the network interface in the Cache Mirror on the standby Omnichannel Database server.

Before you begin

Configure Cache Mirroring on 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** > **Edit Mirror**.
4. On the Edit Mirror page, do the following:
    a. Select the **Use Virtual IP** check box.
    b. In the **Network Interface** field, select **Ethernet**.
    c. Click **Save**.

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 virtual IP address of Omnichannel Database.
4. Click **Commit**.
5. Repeat Step 2 to Step 4 for the following services:
    - AutomationController
    - CustomerControllerService
    - EmailService
    - GenericChannelAPI
    - MessagingService
    - OCPDataServices
    - ORCRestService
    - OceanaDataViewer
    - CoBrowse

6. Restart all Avaya Breeze® platform nodes of Avaya Oceana® Cluster 3.

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 active Omnichannel Database server

About this task

Use this procedure to secure the Cache Mirror on the active Omnichannel Database server using TLS.

Before you begin

- Configure Cache Mirroring on the active Omnichannel Database server.
- Ensure that the certificates for the active and standby servers are signed by the same CA.
- 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. 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**.
4. On the Edit Mirror page, click **Set up SSL/TLS**.
5. On the Edit SSL/TLS Configurations for Mirror page, do the following:
    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 key.
    d. In the **Private key type** field, select the type of key.
    e. In the **Password** field, select **Enter new password**.
    f. In the **Private key password** field, enter the new password.
    g. In the **Private key password (confirm)** field, reenter the password.
    h. In the **Protocols** field, select the appropriate protocol.
    i. Click **Save**.
6. On the Edit Mirror page, do the following:
    a. Click **Verify SSL**.
    b. On the Verification dialog box, click **Okay** after successful verification.
    c. Select the **Use SSL/TLS** check box.
    d. Click **Save**.

Securing the Cache Mirror on the standby Omnichannel Database server

About this task

Use this procedure to secure the Cache Mirror on the standby Omnichannel Database server using TLS.

Before you begin

Configure Cache Mirroring on 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** > **Edit Async**.
4. On the Edit Async page, click **Set up SSL/TLS**.
5. On the Edit SSL/TLS Configurations for Mirror page, do the following:
   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 key.
   d. In the **Private key type** field, select the type of key.
   e. In the **Password** field, select **Enter new password**.
   f. In the **Private key password** field, enter the new password.
   g. In the **Private key password (confirm)** field, reenter the password.
   h. In the **Protocols** field, select the appropriate protocol.
   i. Click **Save**.
6. On the Edit Async page, do the following:
   a. Click **Verify SSL**.
   b. On the Verification dialog box, click **Okay** after successful verification.
   c. Select the **Use SSL/TLS** check box.
   d. Click **Save**.

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. On the server, right-click the **Cache** icon, and then click **Stop Cache**.
6. Click **Restart**.

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**.

   After removing the Cache Mirroring configuration, you must take a backup of the database on the primary server, so that you can restore the database after uninstallation and reinstallation of Avaya Oceana® Solution.

Post upgrade tasks for Omnichannel Database

The following is a list of tasks that you must perform after upgrading and restoring Omnichannel Database:

- If security was configured on Omnichannel Database before the upgrade, reconfigure the security.
- If Cache Mirroring was configured on Omnichannel Database before the upgrade, reconfigure Cache Mirroring.
- If any Cache user passwords were changed before the upgrade, change them again.

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.

Chapter 41: 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 2012 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 2012 server.
9. 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.

Procedure

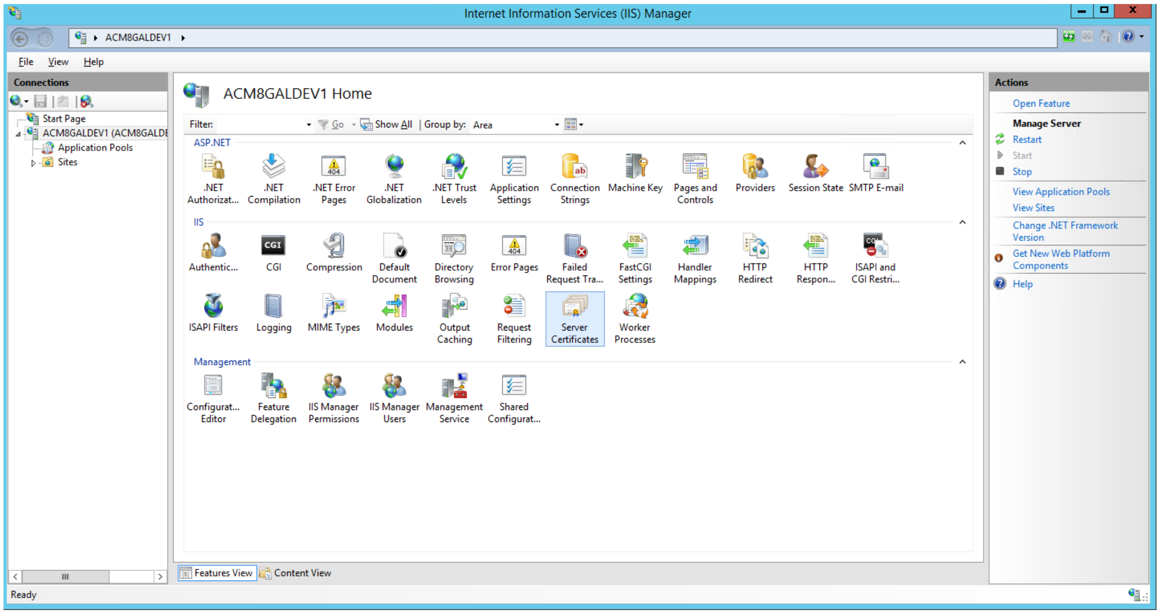
1. Log on to Avaya Control Manager.
2. Navigate to **Configuration** > **Avaya Oceana™** > **Server Details**.
3. On the Avaya Oceana Server List page, do one of the following:
   - Double-click the **UCAServer** instance.
   - Select the check box for the **UCAServer** instance and click **Edit**.
4. Click the **System Properties** tab.
5. Expand **Omni Channel**.
6. In the Omni Channel Database area, do the following:
   a. In the **Omni Channel Database Server** field, enter the FQDN of the Omnichannel Windows 2012 server.
   b. In the **Omni Channel Database Server Port Number** field, enter 443.
   c. Select the **Https** check box to have a secure communication between Avaya Control Manager and your Omnichannel Windows 2012 server.
7. Click **Save**.

Enabling SSL for secure browser access

Procedure

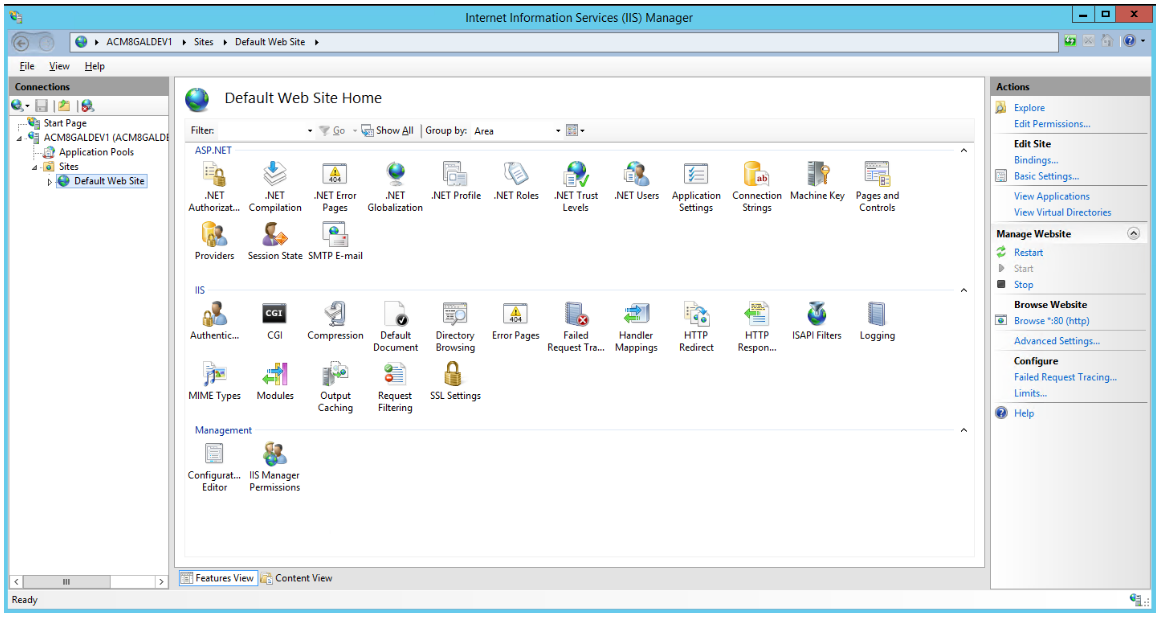
1. Log on to Windows as administrator on the primary application server (ACM-APP-1).
2. Open the Microsoft IIS Manager tool.
3. Click on the Control Manager primary application server (ACM-APP-1) server as shown in the **Connections** tree.

   The system displays a screen similar to the following example:



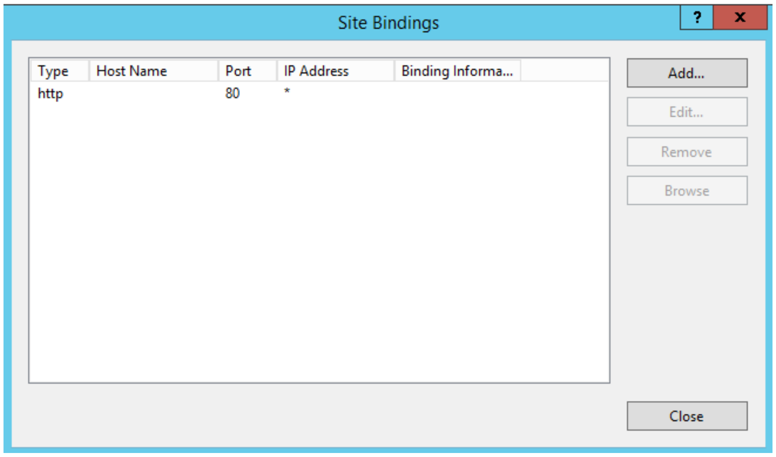
4. Expand the **Sites** folder and select **Default Web Site**.

   See the following example:



5. Select **Bindings** from the **Actions** menu on the right side of the screen.

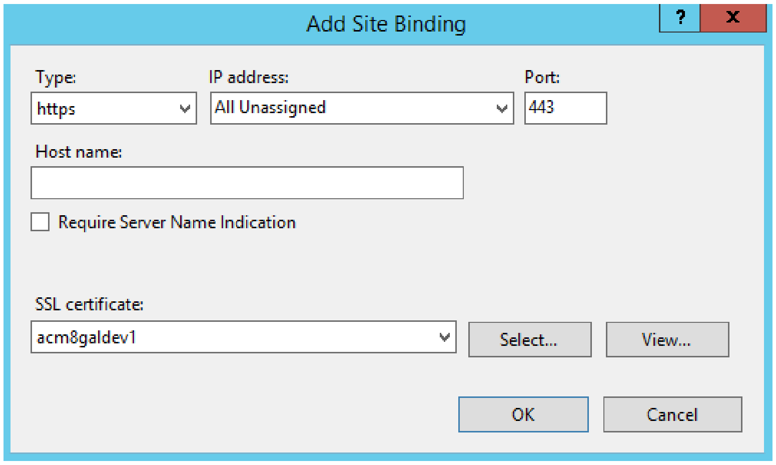
   The system displays the Site Bindings screen.



Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	

6. Click **Add**.

   The system displays the Add Site Binding screen:



Add Site Binding

Type: https

IP address: All Unassigned

Port: 443

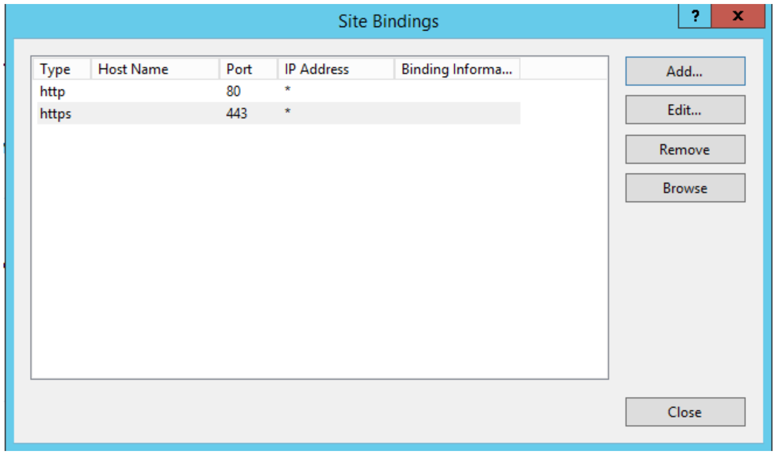
Host name:

□ Require Server Name Indication

SSL certificate: acm8galdev1

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 again showing the HTTPS type:

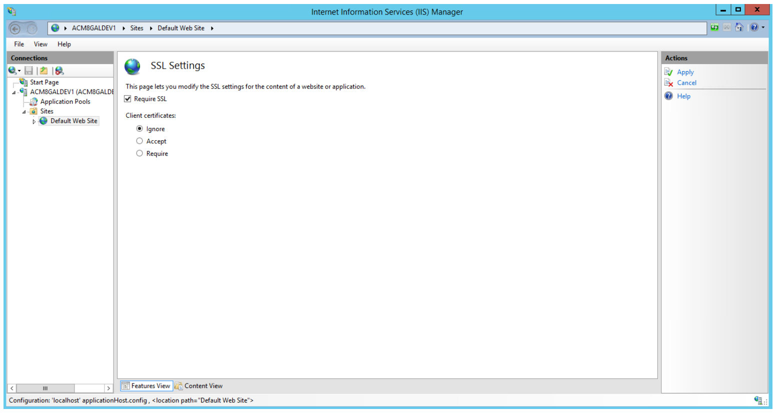


Site Bindings

Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	
https		443	*	

9. Click **Close**.
10. On the Default Web Site Home page, double-click the **SSL Settings** option.

    The system displays the SSL Settings screen:



SSL Settings

This page lets you modify the SSL settings for the content of a website or application.

☑ Require SSL

Client certificates:

● Ignore
○ Accept
○ Require

Configuration: 'localhost' applicationHost.config , <location path="Default Web Site">

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. Ensure that you open the Oceana Customer Management Tool using Microsoft Internet Explorer or Microsoft Edge browsers.

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.

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® Solution 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.

Table continues…

Fields	Description
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.
#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.
#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.

Table continues…

Fields	Description
#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.
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 filed.
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.
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.

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® Solution.

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® Solution. 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® Solution. These measures are taken to ensure that OCMT does not impact the normal operation of Avaya Oceana® Solution 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

Support for customer entered account data

Avaya Oceana® Solution provides support for customer entered account data to enhance management of customer accounts. A customer account consists of the following components:

- Account type: The type of 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 Oceana®.
- Account value: The value that the end customer supplies during the customer's interaction with the Oceana® contact center.

Currently, Oceana® supports accounts for voice and generic channels only.

- In voice channel, two methods of orchestrating front-end IVR are Avaya Aura® Experience Portal and Avaya Aura® Call Center Elite.

  Note:

  The Oceana® 3.6.x 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 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 Designertasks. The updated information is then retrieved and updated through the sample Engagement Designer workflows that enable the customer journey to display the account of current customer interaction with the previous interactions of the customer inOceana®.

- In generic channel support, for each generic contact entered in 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® Solution does not validate any customer entered account value or CRM identifier value against data stored in the Oceana Omnistore database. For more details on validation caveats, see *Avaya Oceana® Solution 3.6 Release Notes*.

Adding new account types to Oceana®

About this task

Use this procedure to create a display name that is associated with a new account type in 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 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® Solution

Importing customer data into Avaya Oceana® Solution

About this task

Use this procedure to import customer data into Avaya Oceana® Solution.

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.

Chapter 42: Configure Avaya CRMGateway snap-in

Avaya CRMGateway snap-in overview

The Avaya CRMGateway snap-in provides a normalized access layer between 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 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 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 Oceana® Serviceability API to send messages and heartbeats
- Registers on the 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
- 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.
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 for the connection establishment.
Server User-Name	The user name of the CRM server that has permission to access the CRM server database. This is a mandatory attribute for the connection establishment.
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.

Table continues…

Name	Description
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 for the connection establishment. 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 The is a mandatory attribute for connection establishment. 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 from establishing 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 from establishing 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.

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":"11-0
3-2019 14:53:12"}
```

If the adapter is not installed correctly, the browser displays an error message.

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 services

About this task

When you uninstall the Avaya CRMGateway snap-in, the service attributes from the Avaya Breeze®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. On the Confirm uninstall service window, do the following:

   a. Select the required cluster.

   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 43: Resources

Documentation

Title	Use this document to:	Audience
Overview		
Avaya Aura® Communication Manager Overview and Specification	Know about 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
Avaya Aura® Session Manager Overview and Specification	Know about 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
Avaya Aura® System Manager Overview and Specification	Know about 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
Avaya Aura® Call Center Elite Overview and Specification	Know about 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

Table continues…

Title	Use this document to:	Audience
Avaya Control Manager Overview and Specification	Know about 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
Avaya Aura® Experience Portal Overview and Specification	Know about 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
Avaya Aura® Application Enablement Services Overview and Specification	Know about 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
Avaya Oceana® Solution Description	Know about 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
Avaya Oceana® Solution Disaster Recovery	Know about how to restore Avaya Oceana® Solution when a complete outage at the primary data center.	• Sales Engineers • Business Partners • Solution Architects • Implementation Engineers
Implementing		
Avaya Co-Browsing Snap-in Reference	Install, configure, and administer Avaya Co-Browsing Snap-in.	• Solution Architects • Implementation Engineers
Avaya Context Store Snap-in Reference	Install, configure, and administer Avaya Context Store Snap-in.	• Solution Architects • Implementation Engineers
Avaya Engagement Designer Reference	Install, configure, and administer Avaya Engagement Designer Snap-in.	• Solution Architects • Implementation Engineers
Avaya BotConnector Snap-in Reference	Install, configure, and administer Avaya BotConnector Snap-in.	• Solution Architects • Implementation Engineers

Table continues…

Title	Use this document to:	Audience
Avaya Aura® Presence Services Snap-in Reference	Install, configure, and administer Avaya Aura® Presence Services snap-in.	- Solution Architects - Implementation Engineers
Configuring Avaya Control Manager	Configure Avaya Control Manager to work with other products	- Solution Architects - Implementation Engineers
Installing Avaya Control Manager	Install Avaya Control Manager.	- Solution Architects - Implementation Engineers
Deploying Avaya Oceana® Solution on Amazon Web Services	Deploy and configure Avaya Oceana® Solution and Avaya Analytics™ in an Amazon Web Services (AWS) environment.	- Solution Architects - Implementation Engineers
Deploying Avaya Control Manager in an Avaya Customer Experience Virtualized Environment	Deploy and configure Avaya Control Manager in an Avaya Customer Experience Virtualized Environment.	- Solution Architects - Implementation Engineers
Deploying Avaya Aura® System Manager on VMWare® in Virtualized Environment	Deploy and configure Avaya Aura® System Manager in virtualized environment.	- Solution Architects - Implementation Engineers
Deploying Avaya Aura® Session Manager	Deploy and configure Avaya Aura® Session Manager.	- Solution Architects - Implementation Engineers
Deploying Avaya Aura® System Manager on System Platform	Deploy and configure Avaya Aura® System Manager.	- Solution Architects - Implementation Engineers
Deploying Avaya Aura® Experience Portal in an Avaya Customer Experience Virtualized Environment	Deploy and configure Avaya Aura® Experience Portal in an Avaya Aura® Virtualized Environment.	- Solution Architects - Implementation Engineers
Deploying Avaya Aura® Communication Manager	Deploy and configure Avaya Aura® Communication Manager.	- Solution Architects - Implementation Engineers
Deploying Avaya Aura® Application Enablement Services	Deploy and configure Avaya Aura® Application Enablement Services	- Solution Architects - Implementation Engineers
Deploying and Updating Avaya Aura® Media Server Appliance	Deploy and configure Avaya Aura® Media Server.	- Solution Architects - Implementation Engineers
Deploying Avaya Workspaces for Oceana®	Deploy and configure Avaya Workspaces.	- Solution Architects - Implementation Engineers

Table continues…

Title	Use this document to:	Audience
Deploying Avaya Workforce Optimization Select with Avaya Aura® Communication Manager and Avaya Oceana® Solution	Deploy and configure Avaya Workforce Optimization Select with Avaya Oceana® Solution.	• Solution Architects • Implementation Engineers
Deploying the Avaya Aura® Web Gateway	Deploy and configure Avaya Aura® Web Gateway.	• Solution Architects • Implementation Engineers
Deploying Avaya Aura® Device Services	Deploy and configure Avaya Aura® Device Services	• Solution Architects • Implementation Engineers
Administering		
Administering Avaya Workspaces	Administer Avaya Workspaces	• Solution Architects • Implementation Engineers • System Administrators
Administering Avaya Aura® System Manager for Release 7.0.1	Administer Avaya Aura® System Manager	• Solution Architects • Implementation Engineers • System Administrators
Administering Avaya Aura® Communication Manager	Administer Avaya Aura® Communication Manager	• Solution Architects • Implementation Engineers • System Administrators
Administering Avaya Aura® Call Center Elite	Administer Avaya Aura® Call Center Elite	• Solution Architects • Implementation Engineers • System Administrators
Administering Avaya Aura® Session Manager	Administer Avaya Aura® Session Manager	• Solution Architects • Implementation Engineers • System Administrators
Using		
Using Avaya Workspaces	Use Avaya Workspaces	• Solution Architects • Implementation Engineers
Using Avaya Analytics™ reports	Use Avaya Analytics™ reports	• Solution Architects • Implementation Engineers
Avaya Context Store Snap-in Developer Guide	Use Context Store services and SDKs	Developers

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.
7. Click **Enter**.

Avaya Documentation Portal navigation

Customer documentation for some programs is now available on the Avaya Documentation Portal at https://documentation.avaya.com.

Important:

For documents that are not available on the Avaya Documentation Portal, click **Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Portal, you can:

- Search for content in one of the following ways:
  - Type a keyword in the **Search** field.
  - Type a keyword in **Search**, and click **Filters** to search for content by product, release, and document type.
  - Select a product or solution and then select the appropriate document from the list.
- Find a document from the **Publications** menu.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** (☆).

  Navigate to the **My Content** > **My Docs** menu, and do any of the following:
  - Create, rename, and delete a collection.

  - Add content from various documents to a collection.
  - Save a PDF of selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive content that others have shared with you.
- Add yourself as a watcher by using the **Watch** icon (👁).

  Navigate to the **My Content** > **Watch list** menu, and do the following:

  - Set how frequently you want to be notified, starting from every day to every 60 days.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

  As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the portal.
- Share a section on social media platforms, such as Facebook, LinkedIn, Twitter, and Google +.
- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log in to the portal. The available functionality depends on the role with which you are logged in.

Training

The following courses are available for the Avaya Oceana® Solution program.

Course code	Course title	Delivery Type
Fundamental - Technical Delta Courses		
21160W	Avaya Oceana® Fundamentals	Web-based Training
21140W	Avaya Oceana® and Avaya Analytics™ R 3.6 Technical Delta	Web-based Training
Implementation Courses		
74150V	Integrating Avaya Oceana®	Virtual Instructor-Led Training
74550V	Supporting Avaya Oceana®	Virtual Instructor-Led Training
74350V	Integrating and Supporting Avaya Analytics™ for Avaya Oceana®	Virtual Instructor-Led Training
Administration Courses		
24320W	Administering Avaya Oceana® Basics	Web-based Training
24300V	Administering Avaya Oceana® Channels	Virtual Instructor-Led Training

Table continues…

Course code	Course title	Delivery Type
24310W	Administering Avaya Analytics™ for Avaya Oceana®	Web-based Training
	End User Courses	
24020W	Using Avaya Oceana® Workspaces for Agents	Web-based Training
24040W	Using Avaya Oceana® Workspaces for Supervisors	Web-based Training
	Developer Courses	
24100W	Developing Customer Applications for Avaya Oceana®	Web-based Training
24150W	24150W - Customizing the Avaya Workspaces® Framework	Web-based Training
	Design Courses	
34200W	Avaya Oceana® Solutions Design Fundamentals	Web-based Training
34800W	Designing the Avaya Oceana® Solution	Web-based Training
	Sales Courses	
41410W	Selling Avaya Oceana®	Web-based Training
41490W	What's New for Sales: Avaya Oceana®	Web-based Training
41480W	The Basics of Cost Justification and Selling Oceana Using the Oceana ROI Tool	Web-based Training
41400W	Selling Avaya Analytics™ Strategy and Positioning Overview	Web-based Training
41020W	Avaya Oceana and Analytics Solutions Product Information Documents (Sales)	Web-based Training
4785W	Avaya Oceana Remote Agent Solution	Web-based Training
4789W	Avaya Oceana: The Customer Experience	Web-based Training
4794W	Avaya Oceana: The Agent Experience	Web-based Training
4795W	Avaya Oceana: The Management Experience	Web-based Training
4877W	Avaya Oceana Solution for Financial Services: Car Loan Use Case	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

This section describes how to set the attributes of a service and explains the attributes of the services that you install on Avaya Oceana® Solution 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® Solution, select `Oceana`.
Number of Communication Managers	The number of Communication Managers that your solution supports. For Avaya Oceana® Solution, select `1`.

Table continues…

Name	Description
Deployment type	The deployment type that determines the memory size of processing units. • For an Avaya Oceana® Solution deployment that supports up to 4500 active agents, select `OCEANA_3XLARGE`. • For an Avaya Oceana® Solution deployment that supports up to 2000 active agents, select `OCEANA_XLARGE`. • For an Avaya Oceana® Solution deployment that supports up to 1000, 500, or 250 active agents, select `OCEANA_LARGE`. • For an Avaya Oceana® Solution 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.

Table continues…

Name	Description
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.
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® Solution deployment that supports up to 4500 active agents, select `OCEANA_3XLARGE`. • For an Avaya Oceana® Solution deployment that supports up to 2000 active agents, select `OCEANA_XLARGE`. • For an Avaya Oceana® Solution deployment that supports up to 1000, 500, or 250 active agents, select `OCEANA_LARGE`. • For an Avaya Oceana® Solution deployment that supports up to 100 active agents, select `OCEANA_SMALL`.

Table continues…

Name	Description
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.
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® Solution 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.

Table continues…

Name	Description
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.
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

Startup Configuration

Name	Description
ContextStore DataGrid type	The type of Context Store DataGrid. For Avaya Oceana® Solution, select `STANDARD`.
ContextStore ManagerSpace DataGrid Settings	The comma-separated values of memoryCapacityPerContainer, maximumMemoryCapacity, and maximumRelocationsPerMachine for ContextStore ManagerSpace DataGrid. For example, `128m,256m,1`. The system interprets the numeric-only values as GB. To specify the values in MB, you must add the letter “m” after the number. For example, `128m`.

Table continues…

Name	Description
ContextStoreSpace DataGrid Settings	The comma-separated values of memoryCapacityPerContainer, maximumMemoryCapacity, and maximumRelocationsPerMachine for ContextStoreSpace DataGrid. For example, `512m,10240m,1`. The system interprets the numeric-only values as GB. To specify the values in MB, you must add the letter “m” after the number. For example, `128m`.

External Data Mart Configuration

Name	Description
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® Solution, select `true`.
EDM: Enable Provisioning from database	The attribute that enables or disables the provisioning of Context data to EDM. For Avaya Oceana® Solution, keep the default value `false`.
EDM: Database type	The type of the EDM database. The available values are: • PostgreSQL • Microsoft SQL Server • Oracle 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® Solution 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® Solution, enter the value as `50`.
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*.
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*.

Table continues…

Name	Description
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.
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*.

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*.

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*.

The Customer Journey view in Avaya Workspaces requests the journey data from the EDM database when the interaction is present on the client. The system only retrieves the data which is available at this time. There is no refresh or notification mechanism.

External Data Mart Configuration

Name	Description
EDM: Database username	The user name of the EDM database.
EDM: Database password	The password of the EDM database.

ContextStoreRest attributes

Advanced Configuration

Name	Description
Authorization Service Address	The FQDN or IP address of the cluster that hosts AuthorizationService.

Table continues…

Name	Description
Enable Breeze Authorization Service	The attribute that enables or disables authentication for Breeze authorization service. • To disable authentication, keep the default value `false`. • To enable authentication, select `true`.
Require user for Breeze Authorization Service	The attribute that enables or disables user authentication for Breeze authorization service. • To disable user authentication, keep the default value `false`. • To enable user authentication, 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 expired in Context Store Space. • To disable centralized logging, select `false`. • To enable centralized logging, keep the default value `true`.

CustomerJourneyService attributes

Startup Configuration

Name	Description
Context Store Cluster Address	The cluster that hosts Context Store services. To set this attribute, select Avaya Oceana® Cluster 1.

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 applications connections through HTTPS. Therefore, you must configure Avaya Oceana® Solution 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.
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® Solution deployment that supports up to 100 active agents, enter the FQDN or IP address of Avaya Oceana® Cluster 1. • For an Avaya Oceana® Solution 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 CustomerJourneyService.

CustomerManagement attributes

Startup Configuration

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® Solution 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.

Table continues…

Name	Description
Retrieve customer information from CRM	The attribute that enables or disables merging of CRM data into the Oceana customer database.
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® Solution 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.

EngagementDesigner attributes

DEFAULT_GROUP

Name	Description
ChatBot Cluster(s)	The cluster that hosts the BotConnector service. • For an Avaya Oceana® Solution deployment that supports up to 100 active agents, select Avaya Oceana® Cluster 1. • For an Avaya Oceana® Solution deployment that supports up to 4500, 2000, 1000, 500, or 250 active agents, select Avaya Oceana® Cluster 2.
Completed instance to be deleted or not	The attribute that enables or disables the deletion of completed instances.
Context Store Cluster(s)	The cluster that hosts Context Store services. To set this attribute, select Avaya Oceana® Cluster 1.

Table continues…

Name	Description
Customer Management Cluster(s)	The cluster that hosts the CustomerManagement service. To set this attribute, select Avaya Oceana® Cluster 1.
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.
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® Solution 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 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
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.

OceanaCoreDataService attributes

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.

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® Solution deployment that supports up to 100 active agents, enter the FQDN or IP address of Avaya Oceana® Cluster 1. • For an Avaya Oceana® Solution 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.

OceanaMonitorService attributes

Startup Configuration

Name	Description
Cluster 1	To set this attribute, select Avaya Oceana® Cluster 1.
Cluster 2	• For an Avaya Oceana® Solution deployment that supports up to 100 active agents, select Avaya Oceana® Cluster 1. • For an Avaya Oceana® Solution 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.

Table continues…

Name	Description
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`.

Run-time Service Configuration

Name	Description
Authorization Required to view Monitor output	The attribute that enables or disables user authentication for viewing Oceana Monitor Service pages. • To disable user authentication, keep the default value `false`. • To enable user authentication, select `true`.
Oceana Authorization cluster IP	The FQDN or IP address of the cluster that hosts AuthorizationService. • For an Avaya Oceana® Solution deployment that supports up to 100 active agents, enter the FQDN or IP address of Avaya Oceana® Cluster 1. • For an Avaya Oceana® Solution 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.

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® Solution deployment that supports up to 4500 active agents, select `OCEANA_3XLARGE`. • For an Avaya Oceana® Solution deployment that supports up to 2000 active agents, select `OCEANA_XLARGE`. • For an Avaya Oceana® Solution deployment that supports up to 1000, 500, or 250 active agents, select `OCEANA_LARGE`. • For an Avaya Oceana® Solution deployment that supports up to 100 active agents, select `OCEANA_SMALL`.

Table continues…

Name	Description
Persistence configuration	The attribute that ensures the persistence of the data to the local cluster database. For Avaya Oceana® Solution, select `OCEANA_DATABASE`.
Disaster recovery role	For information about this attribute, see *Avaya Oceana® Solution Disaster Recovery*.
OCPDataServices Cluster	The cluster that hosts OCPDataServices. To set this attribute, select Avaya Oceana® Cluster 3.

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® Solution deployment that supports up to 4500 active agents, select `OCEANA_3XLARGE`. • For an Avaya Oceana® Solution deployment that supports up to 2000 active agents, select `OCEANA_XLARGE`. • For an Avaya Oceana® Solution deployment that supports up to 1000, 500, or 250 active agents, select `OCEANA_LARGE`. • For an Avaya Oceana® Solution deployment that supports up to 100 active agents, select `OCEANA_SMALL`.

Table continues…

Name	Description
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® Solution deployment that supports up to 1000, 500, or 250 active agents, enter the value `1024,6144,0,1`. • For an Avaya Oceana® Solution deployment that supports up to 100 active agents, enter the value `256,1536,0,1`.
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® Solution deployment that supports up to 4500 active agents, select `OCEANA_3XLARGE`. • For an Avaya Oceana® Solution deployment that supports up to 2000 active agents, select `OCEANA_XLARGE`. • For an Avaya Oceana® Solution deployment that supports up to 1000, 500, or 250 active agents, select `OCEANA_LARGE`. • For an Avaya Oceana® Solution 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™.
DC ADAPTOR: Lookup Locator	The FQDN lookup locators of Unified Collaboration Model Data Collector Adaptor Space. **Note:** You must set this attribute 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® Solution deployment that supports up to 4500 active agents, select `OCEANA_3XLARGE`. • For an Avaya Oceana® Solution deployment that supports up to 2000 active agents, select `OCEANA_XLARGE`. • For an Avaya Oceana® Solution deployment that supports up to 1000, 500, or 250 active agents, select `OCEANA_LARGE`. • For an Avaya Oceana® Solution deployment that supports up to 100 active agents, select `OCEANA_SMALL`.

Table continues…

Name	Description
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 the 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. **Note:** Set this attribute only if you deploy Avaya Analytics™.

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, then 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	The attribute that 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 Email timeout in milliseconds	The timeout of the Email WorkItem Queued state in milliseconds. The default value of this attribute is 604800000. You must set the limit above the maximum number of days for which you expect the emails to be in queue, considering the holiday periods where email responses can be delayed.
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 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® Solution deployment that supports up to 4500 active agents, select `OCEANA_3XLARGE`. • For an Avaya Oceana® Solution deployment that supports up to 2000 active agents, select `OCEANA_XLARGE`. • For an Avaya Oceana® Solution deployment that supports up to 1000, 500, or 250 active agents, select `OCEANA_LARGE`. • For an Avaya Oceana® Solution 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

Avaya Automated Chat

Name	Description
Automated Chat Base URL	The base URL of the Avaya Automated Chat system starting with http or https.
Automated Chat default Site-id	The Site ID of the BotConnector service followed by :FriendlyName. This is used as the Site Code of the Automated Chat System if a site code is not provided while starting the chat session. For example, `iasljety4so7`.

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`.

UnifiedAgentContextService attributes

Startup Configuration

Name	Description
Deployment Type	The deployment type that determines the memory size of processing units. • For an Avaya Oceana® Solution deployment that supports up to 4500 active agents, select `OCEANA_3XLARGE`. • For an Avaya Oceana® Solution deployment that supports up to 2000 active agents, select `OCEANA_XLARGE`. • For an Avaya Oceana® Solution deployment that supports up to 1000, 500, or 250 active agents, select `OCEANA_LARGE`. • For an Avaya Oceana® Solution 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® Solution 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.

Table continues…

Name	Description
Co-Browse Cluster	The cluster that hosts the CoBrowse service. To set this attribute, select Avaya Oceana® Cluster 4.
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® Solution deployment that supports up to 4500 active agents, select `OCEANA_3XLARGE`. • For an Avaya Oceana® Solution deployment that supports up to 2000 active agents, select `OCEANA_XLARGE`. • For an Avaya Oceana® Solution deployment that supports up to 1000, 500, or 250 active agents, select `OCEANA_LARGE`. • For an Avaya Oceana® Solution 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® Solution 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.
OCDS Cluster	The cluster that hosts OceanaCoreDataService. To set this attribute, select Avaya Oceana® Cluster 1.

Table continues…

Name	Description
OCP Api Cluster	The cluster that hosts Omnichannel Provider services. To set this attribute, select Avaya Oceana® Cluster 3.
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.
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.

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**.

AgentControllerService attributes

Startup

Name	Description
Omnichannel Database Address	The IP address or FQDN of Omnichannel Database.

Table continues…

Name	Description
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® Solution deployment that supports up to 4500, 2000, 1000, 500, or 250 active agents, select Avaya Oceana® Cluster 2. • For an Avaya Oceana® Solution 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 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.
Deployment status of ChatMonitorPu	The value that sets the deployment process.
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`.
Thread pool size for the Omnichannel Database	The number of concurrent connections to the Omnichannel Database. You can 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.

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 the **Clusters** field, click Avaya Oceana® Cluster 3.
    b. In the **Service** field, click **AgentControllerService**.
3. For **Authorization Service Address**:
    a. Select the **Override Default** check box.
    b. In the **Effective Value** field, enter the IP address or FQDN of the cluster that hosts AuthorizationService.
4. Click **Commit**.
5. On the Service Clusters tab, do the following:
    a. In the **Clusters** field, click **Avaya Oceana® Cluster 3**.
    b. In the **Service** field, click **OCPDataService**.
6. For **Authorization Service Address**:
    a. Select the **Override Default** check box.
    b. In the **Effective Value** field, enter the IP address or FQDN of the cluster that hosts AuthorizationService.
7. For **Enable Tokenless Access**:
    a. Select the **Override Default** check box.
    b. In the **Effective Value** field, select **false**.

8. Click **Commit**.
9. Restart Avaya Oceana® Cluster 3.

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.
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.

Table continues…

Name	Description
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.

Table continues…

Name	Description
Deployment Type	The deployment type that determines the memory size of processing units. • For an Avaya Oceana® Solution deployment that supports up to 4500 active agents, select `OCEANA_3XLARGE`. • For an Avaya Oceana® Solution deployment that supports up to 2000 active agents, select `OCEANA_XLARGE`. • For an Avaya Oceana® Solution deployment that supports up to 1000, 500, or 250 active agents, select `OCEANA_LARGE`. • For an Avaya Oceana® Solution deployment that supports up to 100 active agents, select `OCEANA_SMALL`.
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`.

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`.
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.

Table continues…

Name	Description
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`.
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

Startup

Name	Description
Authorization Service Address	The IP address or FQDN of that hosts AuthorizationService. • For an Avaya Oceana® Solution 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® Solution 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`.
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. For example, if you set this attribute for Social Media, you must enter the name of the snap-in that you create while configuring Social Media for Avaya Messaging Automation.
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.
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.

Table continues…

Name	Description
Deployment Type	The deployment type that determines the memory size of MessagingSpace to be deployed. • For an Avaya Oceana® Solution deployment that supports up to 4500 active agents, select `OCEANA_3XLARGE`. • For an Avaya Oceana® Solution deployment that supports up to 2000 active agents, select `OCEANA_XLARGE`. • For an Avaya Oceana® Solution deployment that supports up to 1000, 500, or 250 active agents, select `OCEANA_LARGE`. • For an Avaya Oceana® Solution deployment that supports up to 100 active agents, select `OCEANA_SMALL`.
Toggle Secure Mode	The attribute that toggles all secure connections, except the connection to Omnichannel Database. To set this attribute, select `true`.

Authorization Service

Name	Description
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.

OBCService attributes

Startup Configuration

Name	Description
Deployment type	The deployment type that determines the memory size of processing units. • For an Avaya Oceana® Solution deployment that supports up to 4500 active agents, select `OCEANA_3XLARGE`. • For an Avaya Oceana® Solution deployment that supports up to 2000 active agents, select `OCEANA_XLARGE`. • For an Avaya Oceana® Solution deployment that supports up to 1000, 500, or 250 active agents, select `OCEANA_LARGE`. • For an Avaya Oceana® Solution deployment that supports up to 100 active agents, select `OCEANA_SMALL`.
POM Server	The IP address or FQDN of the POM server that is to be serviced by Outbound Connector.
UAC Cluster	The cluster that hosts the Unified Agent Controller services. • For an Avaya Oceana® Solution deployment that supports up to 100 active agents, select Avaya Oceana® Cluster 1. • For an Avaya Oceana® Solution 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
Secure Connection	The attribute that enables or disables the secure connection to UAC. • To enable secure connection, select `TRUE`. • To disable secure connection, select `FALSE`.
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`.

Table continues…

Name	Description
Username for the Omnichannel Database	The user name for Omnichannel Database.
Enable Centralized Logging	The value that enables centralized logging when a snap-in is installed.

ORCRestService attributes

Startup

Name	Description
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.
ContextStore Cluster	The cluster that hosts Context Store services. To set this attribute, select Avaya Oceana® Cluster 1.
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.
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.

Table continues…

Name	Description
UCA Lookup Locators	The cluster that hosts the Unified Collaboration Administrator (UCA) service. To set this attribute, select Avaya Oceana® Cluster 1.
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® Solution deployment that supports up to 4500 active agents, select `OCEANA_3XLARGE`. • For an Avaya Oceana® Solution deployment that supports up to 2000 active agents, select `OCEANA_XLARGE`. • For an Avaya Oceana® Solution deployment that supports up to 1000, 500, or 250 active agents, select `OCEANA_LARGE`. • For an Avaya Oceana® Solution deployment that supports up to 100 active agents, select `OCEANA_SMALL`.
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.

OceanaDataViewer attributes

Startup

Name	Description
Authorization Service Address	The IP address or FQDN of the cluster that hosts AuthorizationService.
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
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.
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.

SocialConnector attributes

Startup Configuration

Name	Description
Oceana Messaging Snapin IP	The FQDN or IP address of the cluster that hosts MessagingService.

Table continues…

Name	Description
Oceana Messaging Snapin key	The name of the snap-in that you create while configuring the Social Media gateway. The same name is 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 that enables or disables this snap-in's heartbeat and lifecycle messages to be shown on System Manager Monitoring Service page.
Maintenance Mode	The attribute that determines whether or not to fetch or accept any request from Social Media Gateway • If you want Social Media Snap-in to not fetch or accept any request from Social Media Gateway, select `true`. • If you want Social Media Snap-in to fetch or accept requests from Social Media Gateway, select `false`.
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`.

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.

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® Solution, 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® Solution, 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.

Table continues…

Name	Description
Connection URL	The FQDN or IP address of the CRM server. This is a mandatory attribute for the connection establishment.
Server User-Name	The user name of the CRM server that has permission to access the CRM server database. This is a mandatory attribute for the connection establishment.
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 for the connection establishment. Changing this attribute during runtime needs a service restart or cluster reboot.

Table continues…

Name	Description
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 The is a mandatory attribute for connection establishment. 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 from establishing 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 from establishing 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.

Appendix B: Take Avaya Oceana® Solution out of service for voice

This section describes the configuration required to take Avaya Oceana® Solution out of service for voice. Using this feature, you can avoid service interruption for voice if you need to take Avaya Oceana® Solution out of service. For example, if you need to perform an upgrade or routine maintenance of hardware, you can take the Avaya Oceana® Solution out of service and automatically route all subsequent calls to Call Center Elite. Any Avaya Oceana® Solution voice calls already in progress are not affected. Agents can complete all Avaya Oceana® Solution voice calls before the start of the maintenance window.

You take Avaya Oceana® Solution out of service for voice by dialing a Feature Access Code (FAC) from any station used by Avaya Oceana® Solution.

Configuring the out of service FAC

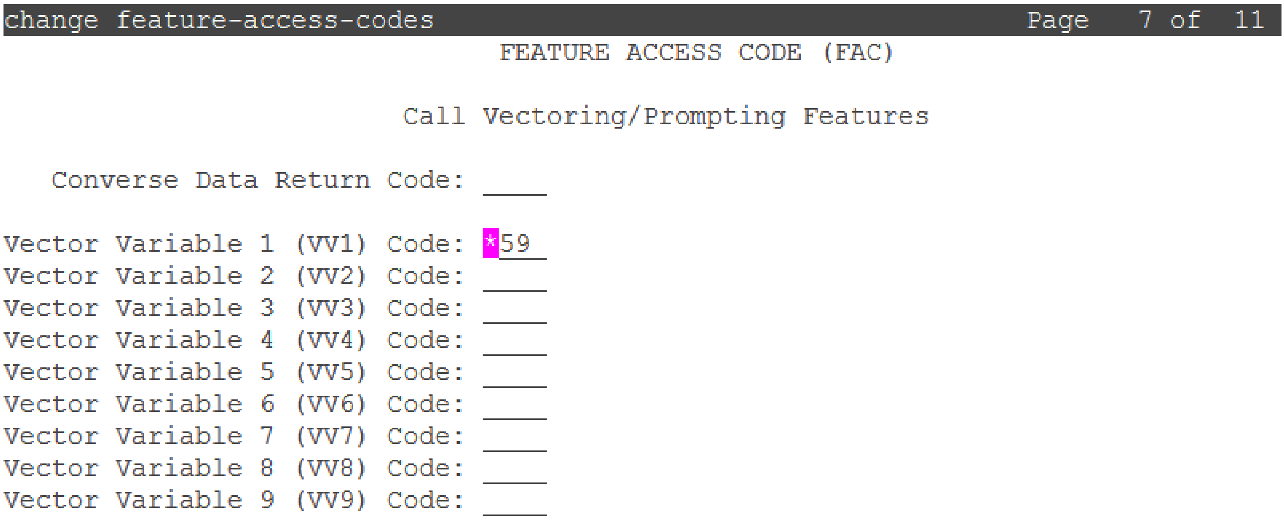
About this task

You can dial a Feature Access Code (FAC) from any station used by Avaya Oceana® Solution to take the system out of service of voice. Use the following procedure to configure the FAC out of service number. Configure the FAC using a code that is not in use in your solution.

Procedure

1. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Use the **`change feature-access-codes`** command.
3. On page 7 of the Feature Access Code screen, in the **Vector Variable 1 Code** field, enter the value `*59`.
4. Save the settings.

Example



```
change feature-access-codes                                     Page   7 of  11
                               FEATURE ACCESS CODE (FAC)

                          Call Vectoring/Prompting Features

   Converse Data Return Code: ____

Vector Variable 1 (VV1) Code: *59_
Vector Variable 2 (VV2) Code: ____
Vector Variable 3 (VV3) Code: ____
Vector Variable 4 (VV4) Code: ____
Vector Variable 5 (VV5) Code: ____
Vector Variable 6 (VV6) Code: ____
Vector Variable 7 (VV7) Code: ____
Vector Variable 8 (VV8) Code: ____
Vector Variable 9 (VV9) Code: ____
```

Configuring the dial plan for the FAC

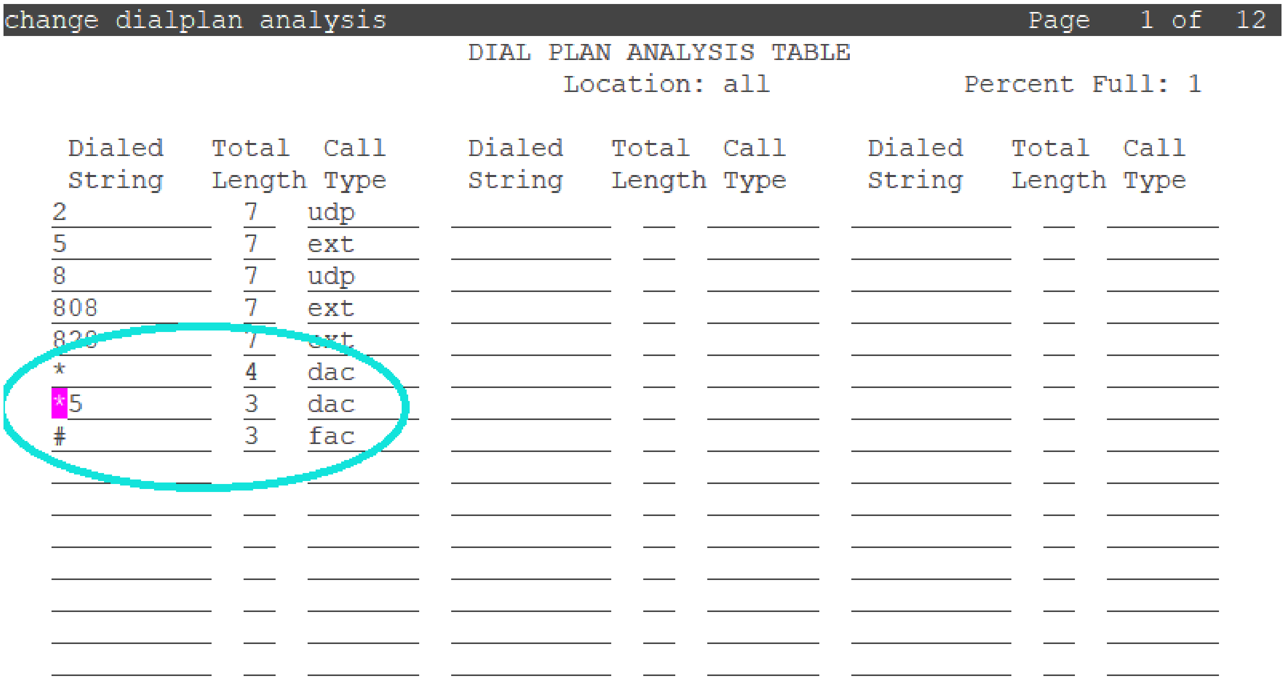
About this task

Communication Manager uses dial plans to define how dialed digits are interpreted, and how many digits to expect for each call. Edit the dial plan so that Communication Manager recognizes that FAC out of service number.

Procedure

1. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Use the **`change dialplan analysis`** command.
3. On page 7 of the Dial Plan Analysis Table screen, in the **Dialed String** field, enter the value `*5`.
4. In the **Total Length** field, enter `3`.
5. In the **Call Type** field, enter `dac`.
6. Save the settings.

Example



```
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
   2            7   udp
   5            7   ext
   8            7   udp
   808          7   ext
   828          7   ext
   *            4   dac
   *5           3   dac
   #            3   fac
```

Enabling the Class of Service permissions

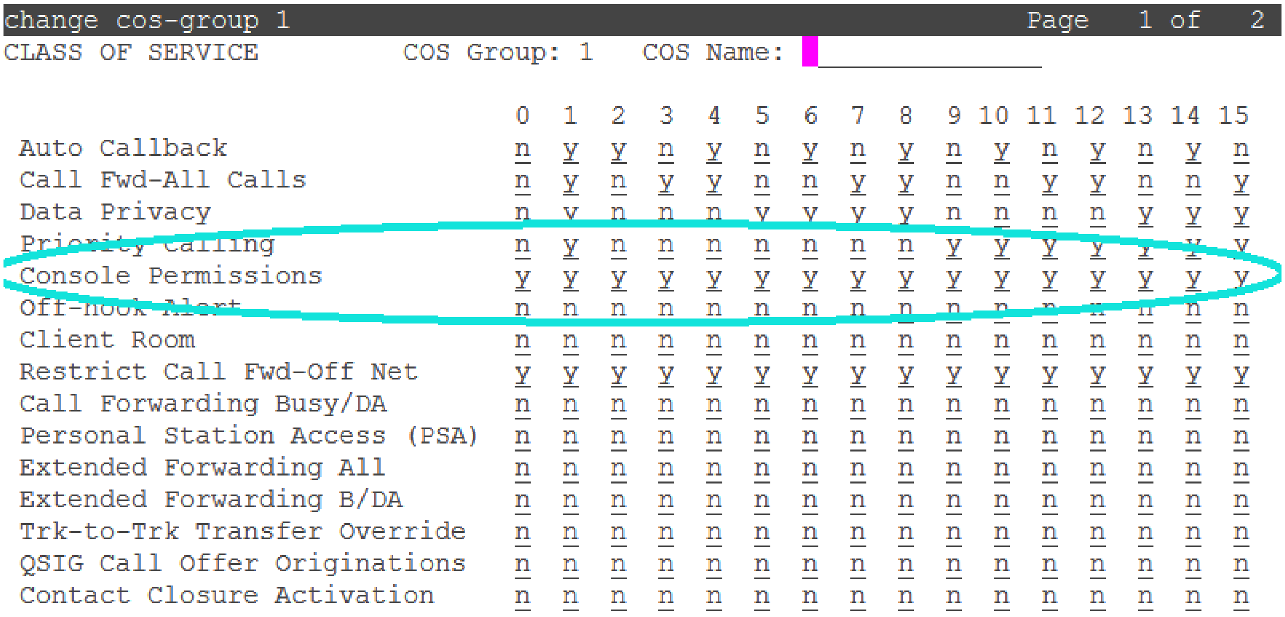
About this task

Use the Class of Service (COS) feature to allow or deny user access to some system features, such as Automatic Callback, Call Forwarding, Data Privacy, Contact Closure Activation, and Console Permissions. The Avaya Oceana® Solution out of service feature requires Console Permissions to be enabled.

Procedure

1. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Use the **`change cos-group n`** command, where *n* is the number of the group to edit.
3. On page 1 of the Class Of Service screen, enable the **Console Permissions** feature.
4. Save the settings.

Example



```
change cos-group 1                                            Page   1 of   2
CLASS OF SERVICE         COS Group: 1   COS Name: 

                                0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15
 Auto Callback                  n  y  y  n  y  n  y  n  y  n  y  n  y  n  y  n
 Call Fwd-All Calls             n  y  n  y  y  n  n  y  y  n  n  y  y  n  n  y
 Data Privacy                   n  y  n  n  n  y  y  y  y  n  n  n  n  y  y  y
 Priority Calling               n  y  n  n  n  n  n  n  n  y  y  y  y  y  y  y
 Console Permissions            y  y  y  y  y  y  y  y  y  y  y  y  y  y  y  y
 Off-hook Alert                 n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Client Room                    n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Restrict Call Fwd-Off Net      y  y  y  y  y  y  y  y  y  y  y  y  y  y  y  y
 Call Forwarding Busy/DA        n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Personal Station Access (PSA)  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Extended Forwarding All        n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Extended Forwarding B/DA       n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Trk-to-Trk Transfer Override   n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 QSIG Call Offer Originations   n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Contact Closure Activation     n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
```

Taking Avaya Oceana® Solution out of service for voice

About this task

Use this procedure to take Avaya Oceana® Solution out of service for voice. Using this feature, you can avoid service interruption for voice if you need to take Avaya Oceana® Solution out of service. For example, if you need to perform an upgrade or routine maintenance of hardware, you can take Avaya Oceana® Solution out of service and automatically route all subsequent calls to Call Center Elite. Any Avaya Oceana® Solution voice calls already in progress are not affected. Agents can complete all Avaya Oceana® Solution voice calls before the start of the maintenance window.

Before you begin

- Complete the FAC, dial plan, and COS configuration required to take Avaya Oceana® Solution out of service for voice. You must also ensure that the `Oceana In Service` variable exists.

Procedure

1. From any CM station used by Avaya Oceana® Solution, dial `*590`.

   This sets the `Oceana In Service` variable to “0”. No further voice calls route to Avaya Oceana® Solution, and fall back to Elite skills-based routing.

2. To re-enable Avaya Oceana® Solution for voice calls, dial `*591` from any CM station used by Avaya Oceana® Solution.

   This sets the `Oceana In Service` variable to “1”.

Index