Upgrading Avaya Oceana®

Release 3.8.1
Issue 4
February 2022

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 as indicated in the order, Documentation, or as authorized by Avaya in writing. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions

Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at 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

Contents

Chapter 1: Introduction

Purpose

This document contains checklists, descriptions, and procedures for upgrading and migrating Avaya Oceana®. Administrators and other personnel who perform Avaya Oceana® upgrades and migrations can use this document.

Change history

Issue	Date	Summary of changes
4	February 2022	• Updated Chapter “Upgrading the Omnichannel server”. • Minor updates.
3	November 2021	Minor updates.
2	April 2021	Updated the following: • Added a new section “Upgrading the Oceana Pluggable Data Connector plugin”. • Updated chapter “Upgrading the Omnichannel server”. • Minor updates.
1	April 2021	Initial release.

New in this release

Avaya Oceana® Release 3.8.1 includes the following features and enhancements:

Support for integration of Avaya Workspaces for Avaya Oceana® and Avaya Workplace Client

As a SIP-based Avaya Aura Unified Communications endpoint, you can deploy Avaya Workplace Client for all Avaya Oceana® and Avaya Analytics™ registered users. Avaya Oceana® users can use Avaya Workplace Client as a softphone with Avaya Workspaces for handling Oceana® routed and non-Oceana® routed voice contacts. Additionally, customers can now deploy remote Avaya Oceana® users (Supervisors and agents) on the Internet using Avaya Workplace Client as the Avaya Aura Unified Communications endpoint for Oceana® routed voice contacts and direct non-Oceana® routed voice contacts.

Avaya Analytics™ generates reports on Avaya Oceana® with the Avaya Workplace Client in the same manner as non-Avaya Workplace Client users.

Support for approval of outbound emails

Avaya Oceana® introduces support for approval of outbound agent email replies. For customer satisfaction and to avoid escalations, an agent's email responses can now be routed through an approval process.

Avaya Analytics™ supports the ability to generate custom reports on the approval or rejection of the outbound emails for both real-time and historical operations.

Support for integrating social messaging platforms with Avaya Oceana®

You can integrate social messaging platforms with Avaya Oceana® through the Avaya Digital Connection. The Avaya Digital Connection is a software platform that enables businesses to communicate with their customers across several popular messaging apps.

Avaya Oceana® supports messaging with the following social platforms:

- WhatsApp
- Facebook Messenger
- Twitter Direct Message

Support for enhancement of timed After Contact Work

Avaya Oceana® introduces support for enhancement of timed after contact work by allowing a system administrator to configure After Contact Work (ACW) timer values on a per-service and per-channel basis.

Support for OAuth for Avaya Oceana® email - Office 365

Avaya Oceana® supports OAuth to allow our customers to continue to operate their email channels after Microsoft announced the end of support for basic authentication of POP3 and IMAP in Office 365.

Support for upscaling Avaya Analytics™ cluster

Avaya Analytics™ supports upscaling the cluster by accommodating the changes in the existing configuration. The upscaling process involves increasing the VMware node resources for the Avaya Common Services cluster by allocating additional CPU, memory, and disk storage.

Support for Avaya Analytics™ full database backup on remote server

You can schedule to run an automatic full backup of the Avaya Analytics™ historical reporting database to a remote server, which is located outside of the cluster. You can also run an immediate full backup manually.

Support for reset Historical Reporting local users password

Avaya Analytics™ 4.1.1.0 introduces the ability for users to reset their login password in one of two ways:

- The Supervisor and Administrator reporting user can reset their own password once they have logged into Avaya Analytics™.
- The Historical Reporting administrator can use the Analytics Administration script on the Cluster Control Manager (CCM) to reset the password of Historical Reporting local users (including supervisors) accounts.

Support to view or delete Historical Reporting local users

The Historical Reporting administrator can use the Analytics Administration script on the Cluster Control Manager (CCM) to view the list and delete Historical Reporting local user accounts.

Support for Private key storage

You must input a password for encrypting the key during the CSR file creation and input that same password during the importing procedure of the certificate.

The private key is displayed in an encrypted format on Cluster Control Manager (CCM).

Support for VMware ESXi 7.0

Avaya Oceana® 3.8.1 and Avaya Analytics™ 4.1.1 supports the following VMware versions:

- VMware ESXi 6.5, 6.7, and 7.0
- Citrix/Xenapp 7.6

Support for Avaya Analytics™ Disaster Recovery Monitoring Tool for replication and failovers

Avaya Analytics™ offers DR monitoring tool that allows you to understand the current status of your replication environment between the active and standby.

Enhancement in deployment spreadsheet

You can see the status of the Macros as `enabled` or `disabled` on the Instructions worksheet of the deployment spreadsheet.

If the macros are disabled, then other worksheets are not visible. Therefore you must enable the macros to proceed.

Support for upgrading to Avaya Analytics™ Release 4.1.1.0

You can use online and offline modes to upgrade Avaya Analytics™. You can archive, export, and save custom reports during an upgrade. Avaya Analytics™ 4.1.1.0 release supports the following upgrade paths:

- Avaya Analytics™ 4.0.0.1 Patch 7 to Avaya Analytics™ 4.1.1.0
- Avaya Analytics™ 4.1.0.0 Patch 1 to Avaya Analytics™ 4.1.1.0
- Avaya Analytics™ 4.1.0.1 to Avaya Analytics™ 4.1.1.0

Note:

You can upgrade the Avaya Analytics™ component before upgrading the Avaya Oceana® component.

Support for Avaya Analytics™ migration from Release 3.7.0.2 to Release 4.1.1.0

Avaya Analytics™ supports data migration, data retention, and legacy data roll up from Release 3.7.0.2 to Release 4.1.1.0.

Support for Routing Service Groups in Avaya Analytics™ Historical Reporting

You can configure Routing Service Groups for Historical Reporting in Avaya Analytics™. You can select the routing services within a routing service group for reporting and track the historical performance of the channel. You can only view routing services and routing service measures associated with the routing service group to which you are assigned.

Support for Call Profile reports in Avaya Analytics™

You can use the Call Profile historical reporting feature in Avaya Analytics™ to view information about the call performance of your routing services for a selected duration. You can view this information for the routing services in the Routing Service Groups to which you are assigned.

Call Profile reports display information such as whether a call was answered, the duration of a call, the duration for which a call was waiting in a queue, or whether a call was abandoned. The following Call Profile reports are available in Avaya Analytics™:

- Call Profile Abandoned
- Call Profile Active Time Duration
- Call Profile Answered
- Call Profile Waiting in Queue

Support for EASG-based Authentication in Avaya Oceana® and Avaya Analytics™

Avaya Oceana® and Avaya Analytics™ provide support for Enhanced Access Security Gateway (EASG) based authentication. Using a challenge-response mechanism, EASG allows support engineers and remote users to log in to the Web administrative interfaces of Avaya Oceana® and Avaya Analytics™, without using credentials such as username and password.

Support for CSV file enhancement for WFO integration

You can configure Avaya Analytics™ to generate `CSV` files for Agent By Account and Routing Service historical reports. For the Agent by Account historical report, you can enable daily or interval CSV Producers. For the Routing Service historical report, you can enable only Interval CSV Producers.

Support for authentication between outbound connector and Omnichannel resource connector

Avaya Oceana® introduces support for establishing authentication between the outbound connector and the Omnichannel resource connector for system security.

Support for Omnichannel Database Server identity certificate expiry alarms

Avaya Oceana® raises an alarm 60 days before the Omnichannel database server identity certificates are due to expire. This alarm is visible in the Avaya Aura® System Manager event viewer.

Support for Oceana Breeze Node Identity certificate expiry alarms

Avaya Breeze® nodes in an Avaya Oceana® solution can be integrated with Avaya Aura® System Manager SNMP listener service to capture all KeyStore identity certificates expiry alarms. The alarms are captured from 60 days to the expiry date and displayed in the event viewer in System Manager. If System Manager is configured with access to a network management application or a simple mail server mailbox, these alarms can be forwarded to an authorized system administrator.

Chapter 2: Upgrade overview and considerations

Upgrade overview

Avaya Oceana® is a next-generation customer engagement solution. Enterprises can use Avaya Oceana® to seamlessly handle Voice, Web and Mobile Chat, Web Voice/Video, Email, Simple Messaging, and Social Media channels. Avaya Oceana® consists of multiple Avaya components such as Avaya Aura® suite, Avaya Control Manager, and the core Omnichannel components deployed on Avaya Breeze® platform. Therefore, when you upgrade Avaya Oceana®, you must also upgrade all components.

Before starting the upgrade process, you must complete the preupgrade tasks to safely shut down Avaya Oceana®.

Note:

If you are upgrading from a version of Oceana earlier than 3.8, then you need to do a database migration from the old External Data Mart (EDM) data.

After taking Avaya Oceana® out of service:

- Shut down all Avaya Oceana® servers which run Avaya Oceana® applications
- Take snapshots using VMware tools and applications.

  For more information about Avaya Oceana® VMware snapshots, see *Deploying Avaya Oceana®*.
- Upgrade Avaya Oceana® and Avaya Breeze® platform and snap-ins using the automated scripted migration tool.
- Upgrade Avaya Control Manager.
- Upgrade the Omnichannel server.

Depending on your release, update the following if required:

- Sample Experience Portal Self Service Application
- Engagement Designer workflows
- Communication Manager vectors
- Sample Chat front ends

- Avaya Workspaces Widget SDK
- Any custom applications customers may have built with the Generic Channel API

  Recompile your custom widgets if required.

After upgrading the components, you must complete the postupgrade tasks to start the operations of Avaya Oceana®.

Important:

The Avaya Oceana® Release Notes contain the known issues, patches, procedures, and workarounds specific to a release and patch line-up of Avaya Oceana®. It is important to download and read the Release Notes for additional instructions to successfully upgrade Avaya Oceana®. For more information about the Avaya Oceana® Release Notes, see https://support.avaya.com.

Supported upgrade paths

The following table lists the supported upgrade paths for Avaya Oceana®:

From release	To release
3.5.x	3.8.1
3.6.x	3.8.1
3.7.x	3.8.1
3.8.0.0/3.8.0.1	3.8.1

Important:

- Avaya Oceana® does not support direct upgrade from 3.4.x to 3.8.1. To upgrade Avaya Oceana® from 3.4.x, you must perform a manual upgrade to 3.5.x.
- Before upgrading to a later Avaya Oceana® Release, you must review the target release hardware requirements to ensure that your hardware meets the minimum specifications. For more information about Avaya Oceana® hardware requirements, see *Avaya Oceana® Solution Description*.
- Before upgrading to a later Avaya Oceana® Release, you must review the component interoperability requirements for the target release to ensure the versions used in your solution are supported. The Compatibility Matrix provides compatibility information for the Avaya products that are supported with the various releases of Avaya Oceana®. Access the Compatibility Matrix page at https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml.

Upgrade process for single site solutions

Avaya Oceana® single site solutions do not include a Disaster Recovery (DR) site. When you upgrade to Avaya Oceana® Release 3.8.1, you must migrate your software. Avaya recommends that you perform your Avaya Oceana® Release 3.8.1 during two maintenance windows:

- Maintenance Window 0: Avaya Aura® System Manager migration. This maintenance window is not service impacting, and you can schedule this maintenance window before upgrading the remaining solution components at a later time. For more information about Avaya Aura® System Manager migration, refer to the Avaya Aura® System Manager documentation, available on the Avaya Support website at https://support.avaya.com.
- Maintenance Window 1: Avaya Oceana® components software upgrade. This maintenance window is service impacting, Avaya Oceana® cannot be in production during this time.

Upgrade process for Disaster Recovery solutions

Avaya Oceana® Disaster Recovery (DR) solutions typically include a primary datacenter location (DC1) and a DR datacenter location (DC2). DC2 is geographically separated across a suitably engineered layer 3 data network. For more detailed information about Avaya Oceana® Disaster Recovery, see *Avaya Oceana® and Avaya Analytics™ Disaster Recovery*.

There are two supported migration options for Avaya Oceana® DR solutions. Both migration options require an initial maintenance window to upgrade Avaya Aura® System Manager. This maintenance window is not service impacting, and you can schedule this maintenance window before upgrading the remaining solution components at a later time. For more information about Avaya Aura® System Manager migration, refer to the Avaya Aura® System Manager documentation, available on the Avaya Support website at https://support.avaya.com.

After upgrading Avaya Aura® System Manager, you must upgrade the remaining Avaya Oceana® components using one of the following options:

1. In a single maintenance window, upgrade all of the Avaya Oceana® components at both DC1 and DC2. This maintenance window is service impacting, Avaya Oceana® cannot be in production during this time.
2. In 2 separate maintenance windows, upgrade both datacenters at different times. Upgrade DC1 during the first scheduled window. This maintenance window is service impacting, Avaya Oceana® cannot be in production during this time. After the upgrade is complete and Avaya Oceana® is back in production, upgrade DC2. During the second scheduled maintenance window, you must re-enable data replication and full DR capabilities.

Impacts on the External Data Mart data

For information about how the upgrade of Avaya Oceana® impacts the External Data Mart (EDM) data within Avaya Oceana®, see *Avaya Context Store Release Notes.*

Chapter 3: Preupgrade tasks

Preupgrade tasks overview

This chapter provides information about the tasks that you must perform to gracefully shut down Avaya Oceana® before starting the upgrade process.

Preupgrade tasks are:

- Gracefully shutting down all Avaya Oceana® channels.
- Shutting down all applications and taking snapshots.

  Snapshot is the only supported fallback mechanism when an unrecoverable failure occurs during the migration process of Avaya Aura® System Manager and Avaya Breeze® platform nodes. You can take snapshots only during a maintenance window when Avaya Oceana® is shutdown. You must remove snapshots before placing the Avaya Oceana® in production.
- Upgrading Avaya Aura® System Manager for the new release of Avaya Oceana®.
- Disabling mailboxes to prevent processing of new emails during the upgrade process.
- Configuring Avaya Oceana® to reject contacts so that it stops accepting SMS, Social, Chat, and Generic conversations.
- Configuring Avaya Oceana® to close chatrooms so that it closes any remaining chat sessions.
- Taking Avaya Oceana® out of service for voice so that subsequent voice calls do not route to Avaya Oceana®.
- Taking a backup of UCAStoreService to retain static information of Avaya Oceana®, such as information related to users, accounts, attributes, providers, and resources.
- Taking a backup of UCMService to retain data related to deferred emails.
- Taking a backup of Engagement Designer workflows.

Preupgrade checklist

Use the following checklist for the tasks that you must complete before upgrading Avaya Oceana®:

No.	Task	Notes	✔
1	Take snapshots of all applications.	For information about how to use snapshots in production, see the documentation for the respective application.	
2	Upgrade Avaya Aura® System Manager for the new release of Avaya Oceana®.	See Avaya Aura System Manager upgrade overview on page 21.	
3	Disable all mailboxes.	See Disabling mailbox polling on page 22.	
4	Configure Avaya Oceana® to reject contacts.	See Configuring Avaya Oceana to reject new digital contacts on page 23.	
5	Configure Avaya Oceana® to close chatrooms.	See Configuring Avaya Oceana to close chatrooms on page 23.	
6	Take Avaya Oceana® out of service for voice.	See Taking Avaya Oceana out of service for voice on page 24.	
7	Take a backup of UCAStoreService.	See Taking a backup of UCAStoreService on Data Center 1 on page 24.	
8	Take a backup of Engagement Designer workflows.	See Taking a backup of Engagement Designer workflows on page 26.	
9	Take a backup of UCMService.	See Taking a backup of UCMService on page 27.	

Avaya Aura® System Manager upgrade overview

Avaya Aura® System Manager acts as a central management system for deployments, migrations, upgrades, and updates of Avaya Aura® applications. Before starting the upgrade process of Avaya Oceana®, you must complete the mandatory Avaya Aura® System Manager migration.

Avaya recommends that you complete the Avaya Aura® System Manager migration in a separate window, and do not do it during the maintenance window of the Avaya Oceana® component upgrade.

When you upgrade to Avaya Oceana® Release 3.8.1, you must migrate Avaya Aura® System Manager to Release 8.1.2 using the Avaya Aura® System Manager OVA and the data migration utility. After the migration, you must upgrade to Avaya Aura® System Manager 8.1.3.1 and apply the relevant hotfix for Avaya Oceana® Release 3.8.1.

Ensure that the Avaya Breeze® Element Manager patch 3.8.1.0 is applied for Avaya Oceana® Release 3.8.1.

The high-level tasks of the Avaya Aura® System Manager 8.1.3.1 migration process are:

- Taking a VMWare snapshot of the Avaya Aura® System Manager before attempting the migration or upgrade.

  After the successful migration or upgrade, you must remove the snapshot. Avaya Aura® System Manager and Avaya Oceana® do not support snapshots in production.
- Taking a backup of the Avaya Aura® System Manager database to preserve Avaya Aura® System Manager configuration.
- Deploying Avaya Aura® System Manager 8.1.2 OVA.
- Migrating the backup data to Avaya Aura® System Manager 8.1.3.1.
- Installing the integrated patch, Hotfix patch, and license.
- Installing all previous licenses for all Avaya Oceana® components on the new Avaya Aura® System Manager using the new Host ID.
- Setting the enrollment password.
- Installing the Avaya Aura® System Manager 8.1.3.1 patch and Hotfix patch.

For detailed information about Avaya Aura® System Manager migration, see the Avaya Aura® System Manager documentation available on the Avaya Support website at https://support.avaya.com.

Disabling mailbox polling

About this task

Use this procedure to disable polling of all configured mailboxes to prevent processing of new emails during the upgrade process. When you disable all mailboxes, external tools such as Microsoft Outlook handle live emails. Agents can still process active emails or emails in the Avaya Oceana® queue.

Procedure

1. Log on to Avaya Control Manager.
2. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana®** > **Omnichannel Administration**.
3. Click **Launch OC Database Administration Client**.

   Avaya Control Manager starts Omnichannel Administration Utility.
4. In the navigation pane, click **E-mail** > **Recipient Addresses**.
5. Click **Disable All**.

Configuring Avaya Oceana® to reject new digital contacts

About this task

Use this procedure to configure Avaya Oceana® so that it stops accepting new SMS, Social, Chat, and Generic conversations. With this configuration, Avaya Oceana® stops accepting new conversations. However, it continues processing the currently active conversations.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Attributes Configuration page, click the **Service Clusters** tab.
3. In the **Cluster** field, select Avaya Oceana® Cluster 3.
4. In the **Service** field, select **MessagingService**.
5. For **Shutdown Mode**, select the **Override Default** check box and select `true` in the **Effective Value** field.
6. Click **Commit**.
7. In the **Service** field, select **CustomerControllerService**.
8. For **Shutdown Mode**, select the **Override Default** check box and select `true` in the **Effective Value** field.
9. Click **Commit**.
10. In the **Service** field, select **GenericChannelAPI**.
11. For **Shutdown Mode**, select the **Override Default** check box and select `true` in the **Effective Value** field.
12. Click **Commit**.

Configuring Avaya Oceana® to close chatrooms

About this task

Use this procedure to configure Avaya Oceana® so that it closes any remaining chat sessions. For example, Avaya Oceana® closes the chat sessions that customers or agents leave without closing.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Attributes Configuration page, click the **Service Clusters** tab.
3. In the **Cluster** field, select Avaya Oceana® Cluster 3.
4. In the **Service** field, select **CustomerControllerService**.

5. For **Close all Chatrooms**, select the **Override Default** check box and select `true` in the **Effective Value** field.
6. Wait for at least five minutes so that Avaya Oceana® Cluster 3 closes the chat sessions and stores the chat transcripts in the customer history.
7. Click **Commit**.

Taking Avaya Oceana® out of service for voice

About this task

Use this procedure to take Avaya Oceana® out of service for voice so that subsequent voice calls do not route to Avaya Oceana®. After you take Avaya Oceana® out of service for voice, all subsequent voice calls route to Call Center Elite. However, all in-progress Avaya Oceana® voice calls remain unaffected.

Before you begin

During the deployment of Avaya Oceana®, you must have:

- Configured the out of service Feature Access Code (FAC)
- Configured the dial plan for the FAC
- Enabled the Class of Service permissions

For information about these configurations, see *Deploying Avaya Oceana®*.

Procedure

From any CM station in Avaya Oceana®, dial the following number:

```
<FAC Out of Service Number>0
```

For example, if you configured *59 as the FAC out of service number, then you must dial *590 to take Avaya Oceana® out of service for voice. For information about the FAC out of service number, see *Deploying Avaya Oceana®*.

Taking a backup of UCAStoreService on Data Center 1

About this task

Use this procedure to take a backup of UCAStoreService on Data Center 1. This service stores static information of Avaya Oceana®. For example, the information related to users, accounts, attributes, providers, and resources.

Note:

- This database is maintained during the Avaya Breeze® platform upgrade. However, you must take this backup as a precaution so that you can retrieve the data if any problem occurs.
- Avaya Control Manager, UCA, and the Omnichannel server back up their data independently. Therefore, you must take their backups in synchronization and restore them in synchronization.

Procedure

1. On the System Manager web console of Data Center 1, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. From the **Backup and Restore** field, select **Configure**.

   System Manager displays the Backup Storage Configuration page.
3. In the **FQDN or IP Address** field, enter the FQDN or IP Address of the backup storage server.
4. In the **Login** field, enter the user name that you use to log in to the backup storage server.
5. In the **Password** field, enter the password that you use to log in to the backup storage server.
6. In the **SSH Port** field, enter the port number of the backup storage server.
7. In the **Directory** field, enter the path to a directory in the backup storage server.
8. In the **Retained backup copies per cluster per snap-in DB** field, specify the maximum number of backup file copies that you want to retain on the backup storage server.

   If you do not specify any value, the backup storage server retains all backup files.
9. Click **Test Connection**.
10. On the Test Connection Result dialog box, verify the following messages:

    ```
    SSH connection ok.
    Backup directory ok.
    File transfer test ok.
    File remove test ok.
    ```
11. Click **OK**.
12. Click **Commit**.

    Note:

    This is a one-time configuration. Once you configure the backup location, successive backups reuse the same information.
13. Select the check box for Avaya Oceana® Cluster 1.
14. From the **Backup and Restore** field, select **Backup**.

    System Manager displays the Cluster DB Backup page.

15. Select the **UCAStoreService** check box.
16. In the **Backup Password** field, enter a password for the backup.

    Important:

    Make a note of the password because you require this password to restore UCAStoreService.
17. In the **Schedule Job** field, click **Run immediately**.
18. Click **Backup**.
19. After the backup process is complete, verify that the **Status** column on the Backup and Restore Status page displays the status `Completed`.

Taking a backup of Engagement Designer workflows

About this task

Use this procedure to take a backup of Engagement Designer workflows.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. From the **Backup and Restore** field, select **Configure**.

   System Manager displays the Backup Storage Configuration page.
3. In the **FQDN or IP Address** field, enter the FQDN or IP Address of the backup storage server.
4. In the **Login** field, enter the user name that you use to log in to the backup storage server.
5. In the **Password** field, enter the password that you use to log in to the backup storage server.
6. In the **SSH Port** field, enter the port number of the backup storage server.
7. In the **Directory** field, enter the path to a directory in the backup storage server.
8. In the **Retained backup copies per cluster per snap-in DB** field, specify the maximum number of backup file copies that you want to retain on the backup storage server.

   If you do not specify any value, the backup storage server retains all backup files.
9. Click **Test Connection**.
10. On the Test Connection Result dialog box, verify the following messages:

    ```
    SSH connection ok.
    Backup directory ok.
    ```

```
File transfer test ok.
File remove test ok.
```

11. Click **OK**.
12. Click **Commit**.

    Note:

    This is a one-time configuration. Once you configure the backup location, successive backups reuse the same information.

13. Select the check box for Avaya Oceana® Cluster 1.
14. From the **Backup and Restore** field, select **Backup**.

    System Manager displays the Cluster DB Backup page.

15. Select the **engagementdesigner_workflow** database check box.
16. In the **Backup Password** field, enter a password for the backup.

    Important:

    Make a note of the password because you require this password to restore the backup.

17. In the **Schedule Job** field, click **Run immediately**.
18. Click **Backup**.
19. After the backup process is complete, verify that the **Status** column on the Backup and Restore Status page displays the status `Completed`.

Taking a backup of UCMService

About this task

Use this procedure to take a backup of the UCMService database. This service persists metadata related to deferred emails and requires this data to retrieve expired deferred emails and route them back to the appropriate agent. This service is installed on Avaya Oceana® Cluster 1.

Before you begin

Ensure that all agents are logged out of their accounts.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. From the **Backup and Restore** field, select **Configure**.

   System Manager displays the Backup Storage Configuration page.

3. In the **FQDN or IP Address** field, enter the FQDN or IP Address of the backup storage server.
4. In the **Login** field, enter the user name that you use to log in to the backup storage server.
5. In the **Password** field, enter the password that you use to log in to the backup storage server.
6. In the **SSH Port** field, enter the port number of the backup storage server.
7. In the **Directory** field, enter the path to a directory in the backup storage server.
8. In the **Retained backup copies per cluster per snap-in DB** field, specify the maximum number of backup file copies that you want to retain on the backup storage server.

   If you do not specify any value, the backup storage server retains all backup files.
9. Click **Commit**.
10. Select the check box for the Avaya Oceana® Cluster 1.
11. From the **Backup and Restore** field, select **Backup**.
12. On the Cluster Database Backup Confirmation dialog box, select the **UCMService** check box and click **Continue**.
13. In the **Backup Password** field, enter a password for the backup.

    Important:

    Make a note of the password because you require this password to restore UCMService.
14. In the **Schedule Job** field, click **Run immediately**.
15. Click **Backup**.
16. After the backup process is complete, verify that the **Status** column on the Backup and Restore Status page displays the status `Completed`.

Stopping Web Voice and Web Video calls

About this task

Use this procedure to stop Web Voice and Web Video calls being routed to Avaya Oceana® agents during a maintenance window.

Note:

Skip this task if your solution does not use WebRTC Voice or Video.

Procedure

Modify the front-end web portal’s that host the WebRTC voice or video capabilities to indicate to users that the service is temporarily unavailable. Avaya recommends using a flag to toggle between in service and out of service for this purpose.

Stopping Outbound calls

About this task

Use this procedure to stop Outbound calls being routed to Avaya Oceana® agents during a maintenance window.

Note:

Skip this task if your solution does not use POM.

Procedure

Stop all POM campaigns.

Verifying Avaya Oceana® is not running

About this task

Before beginning the Avaya Oceana® upgrade process, you must ensure that all Avaya Oceana® agents are logged out and that no new contacts arrive into Avaya Oceana®. However, you must allow agents time to gracefully close out any queuing or in process contact. You can use Avaya Workspaces to verify this.

Procedure

1. Log on to Avaya Workspaces as a supervisor.
2. Use real-time displays to ensure all new and existing contacts are complete.
3. Use the My Team widget to ensure that all agents are logged out.

Setting Cluster State to Denying

About this task

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

Procedure

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

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

   ✱ **Note:**

   Steps are optional for Avaya Oceana® Cluster 4 and Avaya Oceana® Cluster 5.

Chapter 4: Upgrading Avaya Breeze® platform nodes and Avaya Oceana® snap-ins

Automated upgrade

Automated upgrade overview

This section provides information about the tasks that you must perform before running the automated scripted upgrade of Avaya Breeze® platform nodes and Avaya Oceana® snap-ins.

Note:

The automated upgrade procedure does not make any assumptions about your existing deployment. If your current deployment is configured in a manner that does not align with the current documented procedures, the automated upgrade process can fail. If the automated upgrade process fails, you must perform a manual upgrade to correct your system.

The high-level tasks of the automated upgrade process are:

- Deleting older loaded versions of Oceana services from System Manager to ensure that System Manager is running only one version of each service.

  Important:

  Do not delete the OceanaConfiguration service.
- Editing service profiles in System Manager to remove EngagementDesigner and AvayaMobileCommunications snap-ins from service profiles.
- Uninstalling all third-party .jar files or non-Oceana custom snap-ins from all Oceana clusters. These third party components are deleted from during System Manager the automated upgrade process if they are still installed on the Avaya Oceana® clusters. If this occurs, you must manually upload the files to System Manager after upgrading. However, if you uninstall the files from the cluster before the upgrade and leave them in a Loaded state, the files are retained after the upgrade completes. The non-Oceana custom snap-ins are not supported on Oceana clusters.
- Checking the stability of Avaya Breeze® platform nodes.

- Checking the replication status of Avaya Breeze® platform nodes to ensure that none of the nodes is in the audit state.
- Checking the state of services.
- Upgrading Avaya Breeze® platform nodes and Avaya Oceana® snap-ins by running the automated script.
- Configuring the Enable Tokenless Access attribute of UCAStoreService.
- Removing all Engagement Designer workflows.
- Removing all Engagement Designer tasks.
- Deploying the latest versions of Engagement Designer tasks.
- Deploying the latest versions of Engagement Designer workflows and setting their routing rules and attributes.
- Editing service profiles in System Manager to add EngagementDesigner and AvayaMobileCommunications snap-ins to service profiles.
- Configuring SMSVendorSnapin attributes through the OceanaConfiguration service.

  Important:

  By using a configuration service, you can configure all the SVAR attributes in a single step. However, if you have set individual SVAR attributes outside the configuration service, you must update all those attributes.
- Configuring the POM Server attribute for OBCService.
- Refreshing the certificates on the cluster containing AuthorizationService.

Automated upgrade checklist

Use the following checklist for automated upgrade of Avaya Breeze® platform nodes and Avaya Oceana® snap-ins:

Task	Notes	✔
Delete older loaded versions of Oceana services from System Manager.	This task ensures that System Manager is running only one version of each service.	
Edit service profiles in System Manager to remove EngagementDesigner and AvayaMobileCommunications snap-ins from service profiles.	See Editing service profiles to remove snap-ins on page 34.	
Check the stability of Avaya Breeze® platform nodes.	See Checking the stability of Avaya Breeze platform nodes on page 35.	

Table continues…

Task	Notes	✔
Check the replication status of Avaya Breeze® platform nodes.	See Checking the replication status of Avaya Breeze platform nodes on page 35.	
Check the state of Oceana services.	See Checking the state of services on page 35.	
Verify that there is sufficient free disk space on each Avaya Breeze® platform node.	See Checking free disk space on Avaya Breeze platform nodes on page 36.	
Upgrade all Avaya Breeze® platform nodes and Avaya Oceana® snap-ins.	See Upgrading Avaya Breeze platform on page 36.	
Check the status of Avaya Oceana® Clusters.	Validate if all clusters are in the same state before the migration • If the cluster state before the migration is `Accept`, then the state is set to `Accept` after the migration. • If the cluster state before the migration is `Deny`, then the state is set to `Deny` after the migration.	
Configure the Enable Tokenless Access attribute of UCAStoreService.	Set the **Enable Tokenless Access** attribute of UCAStoreService to `True` to enable requests to access resource end-points without the need of the Authorization token. For more information, see *Deploying Avaya Oceana®*.	
Remove all Engagement Designer workflows.	See Removing Engagement Designer workflows on page 40. **Note:** After a successful upgrade, you must remove all workflows because the automated upgrade leaves the existing flows and tasks in place. You can manually apply the new Engagement Designer flows and tasks after the migration. The tasks are available in the Avaya Oceana® zip file.	
Remove all Engagement Designer tasks.	See Removing Engagement Designer tasks on page 40.	

Table continues…

Task	Notes	✔
Deploy Engagement Designer tasks.	See Deploying Engagement Designer tasks on page 41. **Important:** Deploy the latest versions of Engagement Designer tasks only if you use latest workflows.	
Deploy Engagement Designer workflows.	See Deploying Engagement Designer workflows on page 42.	
Edit service profiles in System Manager to add EngagementDesigner and AvayaMobileCommunications snap-ins to service profiles.	See Editing service profiles to add snap-ins on page 43.	
Configure the attributes and routing rules of Engagement Designer workflows.	See Configuring the attributes and routing rules of Engagement Designer workflows on page 44.	
Configure SMSVendorSnapin attributes through OceanaConfiguration.	See Configuring SMSVendorSnapin attributes through OceanaConfiguration on page 44.	
Configure the POM Server attribute for OBCService.	See Configuring the POM Server attribute on page 45.	
Refresh the certificates on the cluster containing AuthorizationService.	See Refreshing the Authorization Service identity certificates on page 45.	

Note:

If you are using Reliable Eventing Streaming for ACR-A integration then the upgrade script does not include an option to upgrade this automatically. You must manually apply Reliable Eventing Streaming on the cluster it was installed on after the cluster is upgraded.

Editing service profiles to remove snap-ins

About this task

Use this procedure to edit any existing service profiles in System Manager to remove EngagementDesigner and AvayaMobileCommunications snap-ins from service profiles.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Service Profiles**.
2. On the Service Profile Configuration page, select a service profile and click **Edit**.

3. In the Services in this Service Profile area, on the All Services tab, click the cross sign (**X**) on AvayaMobileCommunications and EngagementDesigner services to remove them from the service profile.

   AvayaMobileCommunications and EngagementDesigner services are added to service profiles to support Web Voice, Web Video, and Engagement Designer initiated calls.
4. Click **Commit**.
5. Repeat Step 2 to Step 4 for all service profiles.

Checking the stability of Avaya Breeze® platform nodes

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Server Administration**.
2. On the Server Administration page, verify that all Avaya Breeze® platform nodes are in the stable state.

Checking the replication status of Avaya Breeze® platform nodes

Procedure

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

Checking the state of services

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, in the **Service Install Status** column, verify the check boxes for all clusters to determine that all services in the clusters are in the `Installed` state.

Checking free disk space on Avaya Breeze® platform nodes

About this task

Before you run the automated upgrade script, use this procedure to verify there is enough disk space on each on Avaya Breeze® platform node to run the script.

Procedure

1. Log on to the Avaya Breeze® platform node as cust.
2. Run the following command to check the current space available in the **root** and **var** partitions: `df -h / /var`

   Ensure that each Avaya Breeze® platform node meets the following requirements:

Disk partition	Minimum free space
/ (root partition)	3.5 GB
/var:	4 GB

3. Repeat this procedure on each Avaya Breeze® platform node that you want to upgrade.

Upgrading Avaya Breeze® platform

About this task

Use this procedure to upgrade the existing Avaya Breeze® platform nodes by running the automated upgrade script.

The automated script does the following:

- Uninstalls the older versions of all Avaya Oceana® snap-ins from clusters.
- Deletes Avaya Oceana® snap-ins from System Manager.
- Upgrades all Avaya Breeze® platform nodes.
- Loads the latest versions of all Avaya Oceana® snap-ins in System Manager.
- Installs Avaya Oceana® snap-ins to their relevant clusters.

Important:

Ensure that you deploy all Avaya Oceana® nodes on the same version of VMware ESX.

Before you begin

- Download the `Oceana<Release_number>.zip` artifacts file from PLDS.
- Take a snapshot of System Manager.

  You can use the snapshot to recover the previous working state of System Manager. A snapshot is the only recovery mechanism to recover from catastrophic failures.

  After the successful migration or upgrade, you must remove the snapshot. System Manager and Avaya Oceana® do not support snapshots in production.

- Take a snapshot of the existing Avaya Breeze® platform nodes.

  You can use the snapshot to recover the previous working state of the Avaya Breeze® platform to reattempt the automated or manual upgrade. A snapshot is the only recovery mechanism to recover from catastrophic failures. For information about how to take a snapshot, see *Upgrading Avaya Breeze® platform*.

  After the successful upgrade and post upgrade testing in production for a limited period, you must remove the snapshot. Avaya Breeze® platform and Avaya Oceana® do not support snapshots in production.

  Important:

  Remove all snapshots before placing Avaya Oceana® in production.

Procedure

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

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

   In this command:

   - Replace <*N*> with the Cluster Group number of the Oceana nodes being upgraded.

     There are two cluster group numbers for DR solutions. Ensure that you choose the correct cluster group number when using this command.
   - Replace <*Configuration Package*> with the configuration type to match with the deployment type.

     For example, Combined-4500 for Oceana_Large.
   - Replace <*OPTION*> with space-separated values depending on the required configuration to include non-mandatory snap-ins.

     For example, Chat GenericChannel Social AMC.

   For detailed information about these parameters, see Avaya Breeze platform upgrade script parameters on page 38.

   Important:

   - The current version of the command provides validation of these parameters.
   - Ensure that you carefully type all option values in the **`upgradeSolution`** command.
   - During the upgrade process, the script tries to determine the names of the current Avaya Oceana® Clusters and the current snap-ins installed on them. The script prompts for a confirmation if each cluster name corresponds to a specific cluster.

For example, "Is Cluster 1 name Cluster1_CC (y/n)". If the prompted cluster name is incorrect and you press `n`, the script prompts again until you get the correct cluster name and press `y`.

For these questions, the clusters refer to the naming conventions mentioned in *Deploying Avaya Oceana®*. For example, Cluster 1 refers to Common Cluster, Cluster 2 refers to Unified Agent Cluster, Cluster 3 refers to OCP Cluster, Cluster 4 refers to CoBrowse Cluster, and Cluster 5 refers to Zang and CRM cluster.

- You can view the upgrade logs in the `solution-upgrade.log` file in the `/var/log/Avaya` folder on System Manager.

Avaya Breeze® platform upgrade script parameters

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

Table continues…

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

Note:

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

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

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

SnapInGroup OPTION	Snap-ins included
Messaging	MessagingService
SMS	SMSVendorSnapin
AMC	AvayaMobileCommunications
AvayaChat	BotConnector
Chat	AutomationController
CoBrowse	CoBrowse
GenericChannel	GenericChannelAPI
Social	SocialConnector

Table continues…

SnapInGroup OPTION	Snap-ins included
POM	OBCService
DataView	DataViewer
Logging	Centralized Logger
PacketMetric	Packetbeat and Metricbeat

Note:

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

Postupgrade tasks

Removing Engagement Designer workflows

About this task

Use this procedure to remove Engagement Designer workflows so that you can install latest workflows and take the advantage of performance improvements, new features and capabilities, and bug fixes.

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, select the check boxes for all workflows.
3. Click **Undeploy Workflow**.
4. On the Undeploy workflow dialog box, click **OK**.

Removing Engagement Designer tasks

About this task

Use this procedure to remove Engagement Designer tasks so that you can install latest tasks and take the advantage of performance improvements, new features and capabilities, and bug fixes.

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 Bundles tab, select a task.
3. Click **Undeploy**.

4. On the Undeploy bundle dialog box, click **OK**.
5. Select the undeployed bundle and click **Delete**.
6. Repeat Step 2 to Step 5 to remove all old tasks as follow:
    - EngagementDesignerTasks.svar
    - ContextStoreTasks.svar
    - WATasks.svar
    - OceanaTasks.svar

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 Admin Console of Engagement Designer:

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

2. On the Bundles tab, click **Upload**.
3. On the Choose bundle file to upload dialog box, click **Choose File**.
4. Browse to the `EngagementDesignerTasks.svar` file and click **Upload**.
5. Select the bundle and click **Deploy**.

    After the bundle is deployed successfully, ensure that:

    - The **Deployed** column for the bundle displays the value `Yes`.
    - The **Deployed Nodes** column for the bundle contains all nodes of Avaya Oceana® Cluster 1.

    When you open or refresh the Designer Console of Engagement Designer, the system displays the drawers and tasks associated with the tasks bundle.

6. Repeat steps 2 to 5 to deploy Context Store, Work Assignment, and Oceana tasks.

Deploying Engagement Designer workflows

Before you begin

Download the latest version of the sample workflow from PLDS.

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 a 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**.

   Note:

   You can either configure the workflow attributes while deploying the workflow or at a later time.
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 workflow is available in the list of deployed workflows.
11. Repeat Step 2 to Step 10 to deploy and verify all remaining workflows.

Recreating Engagement Designer rules for Transfer workflows

About this task

Avaya Oceana® supports the Transfer to Service and Transfer to User features. The ROUTE_CONTACT_TRANSFER event was previously named ROUTE_CONTACT_TRANSFER_TO_SERVICE. If you are upgrading from Avaya Oceana® Release 3.6.x or earlier, you must delete any existing Engagement Designer rules applicable to Transfer workflows and re-create the rules using the ROUTE_CONTACT_TRANSFER event.

You can skip this procedure if you are upgrading from Avaya Oceana® Release 3.7.x to 3.8.x.x onwards.

Before you begin

- Import and deploy the most recent Transfer workflows.
- Make a note of the existing routing rules in the Engagement Designer Admin UI.

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 only Transfer workflows are available in the list of deployed workflows.
3. Click the **Routing** tab.
4. Delete all existing Transfer rules applicable for all channels.

   Note:

   You cannot edit these rules if they use the ROUTE_CONTACT_TRANSFER_TO_SERVICE event. You must delete and then re-create them.

5. Recreate the rules using the ROUTE_CONTACT_TRANSFER event. For more information about creating Engagement Designer rules, see *Deploying Avaya Oceana®*.

Editing service profiles to add snap-ins

About this task

Use this procedure to edit any existing service profiles in System Manager to add EngagementDesigner and AvayaMobileCommunications snap-ins to service profiles.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Service Profiles**.
2. On the Service Profile Configuration page, select a service profile and click **Edit**.
3. In the Available Service to Add to this Service Profile area, click the plus sign (**+**) on AvayaMobileCommunications and EngagementDesigner services to add them to the service profile.

   AvayaMobileCommunications and EngagementDesigner services are added to service profiles to support Web Voice, Web Video, and Engagement Designer initiated calls.

4. Click **Commit**.
5. Repeat Step 2 to Step 4 for all service profiles.

Reinstalling third-party .jar files

Ensure that you reinstall all third-party .jar files that were removed at the start of the automated upgrade process. Only `EDM jdbc jar` file is supported on cluster 1.

Configuring the attributes and routing rules of Engagement Designer workflows

Before you begin

Install the Engagement Designer workflow for which you want to configure the attributes and routing rules.

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 check box for the workflow for which you want to configure the attributes.
3. Click **Attributes**.
4. On the Workflow Attributes tab, configure the required attributes and click **Close**.
5. Click the **Routing** tab.
6. Select the appropriate rule from the list of rules and click **Edit**.
7. In the **Select workflows** drop-down list, select the latest workflow and click **Save**.
8. Repeat Step 2 to Step 7 for the other workflows.

Configuring SMSVendorSnapin attributes through OceanaConfiguration

About this task

Use this procedure to configure the SMSVendorSnapin attributes through OceanaConfiguration.

Note:

SMSVendorSnapin is an optional snap-in. If SMS is not deployed in your solution, you must skip configuring SMSVendorSnapin attributes.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Attributes Configuration page, click the **Service Clusters** tab.
3. In the **Cluster** field, select **Provisioning Cluster**.
4. In the **Service** field, select **OceanaConfiguration**.

5. In the SMS Vendor area, do the following:
    a. For **Oceana Messaging Service IP or FQDN**, select the **Override Default** check box and enter the FQDN or IP address of the cluster that hosts MessagingService.
    b. For **Oceana Messaging Service key**, select the **Override Default** check box and enter the name of the snap-in that you provide while configuring the SMS gateway.
6. Click **Commit**.

Configuring the POM Server attribute

About this task

Use this procedure to configure the POM Server attribute through OceanaConfiguration.

Note:

If the Outbound channel is not deployed in your solution, you must skip configuring this attribute.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Attributes Configuration page, click the **Service Clusters** tab.
3. In the **Cluster** field, select **Provisioning Cluster**.
4. In the **Service** field, select **OceanaConfiguration**.
5. Locate the OBCService area.
6. For **POM Server**, select the **Override Default** check box and enter the FQDN or IP address of the POM server to be serviced by the OutboundConnector.
7. Click **Commit**.

Next steps

After configuring all the snap-in attributes in a cluster, you must reboot the cluster.

Refreshing the Authorization Service identity certificates

About this task

Use this procedure to refresh the certificates on the cluster containing AuthorizationService. This is a mandatory procedure.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. Select the check box for the cluster containing AuthorizationService.
3. From the **Certificate Management** field, select **Update/Install Identity Certificate (Authorization Service)**.

Configuring CustomerControllerService attributes for connection to Omnichannel Database

About this task

Use this procedure to configure the CustomerControllerService service attributes for connection to the Omnichannel Database.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Attributes Configuration page, click the **Service Clusters** tab.
3. In the **Cluster** field, select the **OCP Cluster**, usually Cluster 3.
4. In the **Service** field, select **CustomerControllerService**.
5. In the **Advanced** section, in **Password for the Omnichannel Database**, enter the password for Omnichannel Database.
6. In the **Secure Connections to Omnichannel Database** field, select `true`.

   This attribute toggles a secure connection to the Omnichannel Database.
7. Click **Commit**.

Upgrading the Oceana Pluggable Data Connector plugin

About this task

Use this procedure to upgrade the Oceana Pluggable Data Connector (PDC) plugin.

Procedure

1. Start the Orchestration Designer Eclipse application.
2. Select **Window** > **Perspective** > **Open Perspective** > **Speech**.
3. In the Avaya Orchestration Designer navigation window, right-click a **Project** menu, select **Properties**.
4. On the left pane of the Properties window, click the **Orchestration Designer**.
5. On the **Orchestration Designer** pane, click the **Pluggable Connectors** tab.
6. From the **Available Connectors** list, find the **Oceana Services** check box and check if it is enabled.

   If there is no Oceana Services Pluggable Connector in the list, close the Orchestration Designer and proceed to step 10. Copy the Oceana PDC into the eclipse plugin folder.
7. If the Oceana Services Pluggable Connector is enabled, to disable the existing plugins, clear the respective checkbox. Click **Apply** and **Close**.

   Complete this step for each project that is open in Orchestration Designer.

8. Close the Orchestration Designer Eclipse application.
9. Open the eclipse plugin folder and delete the existing Oceana PDC plugin jar file.

   Eclipse plugin folder is generally located at `C:\ AAOD\eclipse\plugins`.

   Note:

   If an Oceana PDC is there in the list of Pluggable Connectors but not enabled on any open project, the existing plugin must still be deleted from the plugins folder.
10. Copy the new Oceana PDC plugin jar file into the plugin folder `C:\ AAOD\eclipse\plugins`.
11. Start the Orchestration Designer Eclipse application.
12. To deploy the Oceana PDC plugin, repeat steps 3 to 6.
13. Click **Apply** and **Close**.

Next steps

For information on upgrading the Context Store Pluggable Data Connector (PDC) plugin, see *Avaya Context Store Snap-in Developer Guide*.

Manual upgrade

Manual upgrade overview

This section provides information about the tasks that you must perform for manual upgrade of Avaya Breeze® platform nodes and Avaya Oceana® snap-ins.

Note:

- This is the standard method of upgrading Avaya Breeze® platform nodes and Avaya Oceana® snap-ins if the automated upgrade method is not used.
- If you have already performed a successful automated upgrade, you do not need to do the manual upgrade.

The high-level tasks of the manual upgrade process are:

- Replacing Engagement Designer workflows and tasks to take the advantage of performance improvements, new features and capabilities, and bug fixes.
- Setting the cluster state of all clusters to Denying so that the clusters do not serve any service requests.
- Uninstalling the older versions of all services from clusters so that you can install their latest versions.

- Manually recording the current OceanaConfiguration service attributes.

  Important:

  By using a configuration service, you can configure all the SVAR attributes in a single step. However, if you have set individual SVAR attributes outside the configuration service, you must update all those attributes.

- Editing service profiles in System Manager to remove EngagementDesigner and AvayaMobileCommunications snap-ins from service profiles.
- Deleting the older versions of all services from System Manager so that System Manager does not display their older versions.
- Upgrading all Avaya Breeze® platform nodes.
- Loading the latest versions of all services of Avaya Oceana® in System Manager.
- Installing the OceanaConfiguration service to Provisioning Cluster.
- Installing all services to their relevant clusters.
- Setting the attributes of the services.
- Editing service profiles in System Manager to add EngagementDesigner and AvayaMobileCommunications snap-ins to service profiles.
- Setting the cluster state of all clusters to Accepting so that the clusters start serving the service requests.
- Deploying the latest versions of Engagement Designer tasks.
- Deploying the latest versions of Engagement Designer workflows and setting their routing rules and attributes.

Manual upgrade checklist

Use the following checklist for manual upgrade of Avaya Breeze® platform nodes and Avaya Oceana® snap-ins:

No.	Task	Notes	✔
1	Remove all Engagement Designer workflows.	See Removing Engagement Designer workflows on page 40.	
2	Remove all Engagement Designer tasks.	See Removing Engagement Designer tasks on page 40.	
3	Set the cluster state of all clusters to Denying.	See Setting Cluster State to Denying on page 29.	
4	Uninstall the older versions of all services from clusters.	See Uninstalling all services from the clusters on page 52.	

Table continues…

No.	Task	Notes	✔
5	Manually record the current OceanaConfiguration service attributes.	-	
6	Edit service profiles in System Manager to remove EngagementDesigner and AvayaMobileCommunications snap-ins from service profiles.	See Editing service profiles to remove snap-ins on page 34.	
7	Delete the older versions of all services from System Manager.	See Deleting all services from System Manager on page 53.	
8	Upgrade all Avaya Breeze® platform nodes.	See Upgrading Avaya Breeze platform nodes using the ISO file on page 54.	
9	Apply the Avaya Breeze® platform patch.	See Applying the Avaya Breeze platform patch on page 54.	
10	Load the latest versions of all services in System Manager.	See *Deploying Avaya Oceana®*.	
11	Install the OceanaConfiguration service to Provisioning Cluster.	See Installing the OceanaConfiguration service to Provisioning Cluster on page 55.	
12	Install services to their relevant clusters.	See Installing services to the clusters on page 55.	
13	Set the attributes of the services.	In addition to OceanaConfiguration attributes, you must manually configure the following attributes: • Attributes of SMSVendorSnapin • **Site ID** attribute of BotConnector • **Messaging Snapin Key** attribute of MessagingService • **Enable Tokenless Access** attribute of UCAStoreService For information about how to configure these attributes, see *Deploying Avaya Oceana®*.	
14	Edit service profiles in System Manager to add EngagementDesigner and AvayaMobileCommunications snap-ins to service profiles.	See Editing service profiles to add snap-ins on page 43.	
15	Set the cluster state of all clusters to Accepting.	See Setting Cluster State to Accepting on page 57.	

Table continues…

No.	Task	Notes	✔
16	Deploy Engagement Designer tasks.	See Deploying Engagement Designer tasks on page 41. **Important:** Deploy the latest versions of Engagement Designer tasks only if you use latest workflows	
17	Deploy Engagement Designer workflows.	See Deploying Engagement Designer workflows on page 42.	
18	Configuring the attributes and routing rules of Engagement Designer workflows.	See Configuring the attributes and routing rules of Engagement Designer workflows on page 44.	

Removing Engagement Designer workflows

About this task

Use this procedure to remove Engagement Designer workflows so that you can install latest workflows and take the advantage of performance improvements, new features and capabilities, and bug fixes.

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, select the check boxes for all workflows.
3. Click **Undeploy Workflow**.
4. On the Undeploy workflow dialog box, click **OK**.

Removing Engagement Designer tasks

About this task

Use this procedure to remove Engagement Designer tasks so that you can install latest tasks and take the advantage of performance improvements, new features and capabilities, and bug fixes.

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 Bundles tab, select a task.
3. Click **Undeploy**.
4. On the Undeploy bundle dialog box, click **OK**.
5. Select the undeployed bundle and click **Delete**.
6. Repeat Step 2 to Step 5 to remove all old tasks as follow:
    - EngagementDesignerTasks.svar
    - ContextStoreTasks.svar
    - WATasks.svar
    - OceanaTasks.svar

Setting Cluster State to Denying

About this task

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

Procedure

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

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

    Note:

    Steps are optional for Avaya Oceana® Cluster 4 and Avaya Oceana® Cluster 5.

Uninstalling all services from the clusters

About this task

Use this procedure to uninstall the older versions of all services from Avaya Oceana® Cluster 1, Avaya Oceana® Cluster 2, Avaya Oceana® Cluster 3, Avaya Oceana® Cluster 4, Avaya Oceana® Cluster 5, and Provisioning Cluster.

Before you begin

Record the current attributes values of the OceanaConfiguration service so that you can configure attributes after installing the latest version of the service.

⚠ **Warning:**

> It is necessary to manually record all the current OceanaConfiguration service attribute settings because of the changes in the core attributes of OceanaConfiguration. For implementation of the new changes, it is necessary to delete the old version of OceanaConfiguration before loading the new version. When you delete the old version, all the current OceanaConfiguration attributes are lost and need to be reconfigured after you install the latest version.

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 Avaya Oceana® Cluster 1.
3. Click **Edit**.
4. On the Cluster Editor page, click the **Services** tab.
5. Select the **Uninstall / Force Uninstall** check box for each service, except EventingConnector and CallEventControl.

   When you select the check box for a service, you can select the check box for the next service only after a wait period of 10-15 seconds.
6. Click **Commit**.
7. Repeat Step 2 to Step 6 to uninstall the services from Avaya Oceana® Cluster 2, Avaya Oceana® Cluster 3, Avaya Oceana® Cluster 4, Avaya Oceana® Cluster 5, and Provisioning Cluster.

   Note:

   Uninstall the OceanaConfiguration service last.

Editing service profiles to remove snap-ins

About this task

Use this procedure to edit any existing service profiles in System Manager to remove EngagementDesigner and AvayaMobileCommunications snap-ins from service profiles.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Service Profiles**.
2. On the Service Profile Configuration page, select a service profile and click **Edit**.
3. In the Services in this Service Profile area, on the All Services tab, click the cross sign (**X**) on AvayaMobileCommunications and EngagementDesigner services to remove them from the service profile.

   AvayaMobileCommunications and EngagementDesigner services are added to service profiles to support Web Voice, Web Video, and Engagement Designer initiated calls.
4. Click **Commit**.
5. Repeat Step 2 to Step 4 for all service profiles.

Deleting all services from System Manager

About this task

Use this procedure to delete the older versions of all services from System Manager.

Important:

Do not delete the older version of OceanaConfiguration until you record the current OceanaConfiguration attributes.

Before you begin

Uninstall the older versions of all services from clusters.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
2. On the Services page, select the check boxes for the services that you want to delete.

   Ensure that the services that you want to delete are in the `Loaded` state.
3. Click **Delete**.
4. In the Delete Service Confirmation dialog box, click **Delete**.

Upgrading Avaya Breeze® platform nodes using the ISO file

About this task

Use this procedure to upgrade the existing Avaya Breeze® platform nodes using the Avaya Breeze® platform ISO file.

Before you begin

Take a snapshot of the existing Avaya Breeze® platform nodes. For more information, see *Upgrading Avaya Breeze® platform*.

After the successful upgrade, you must remove the snapshot. Avaya Breeze® platform and Avaya Oceana® do not support snapshots in production.

Procedure

1. Log in to Avaya Breeze® platform nodes using an SSH client application, such as PuTTy.
2. Copy the Avaya Breeze® platform ISO file to each node.
3. Run the following command:

   ```
   upgradeCE <Avaya_Breeze_version_installer>.iso
   ```

   All nodes reboot after the installation is complete.
4. After the reboot, wait until the new nodes replicate successfully with System Manager and pass the maintenance tests.

Applying the Avaya Breeze® platform patch

About this task

Use this procedure to apply the Avaya Breeze® platform patch. This procedure is optional, check the latest release notes to see if a new patch is available.

Procedure

1. Log in to Avaya Breeze® platform nodes using an SSH client application, such as PuTTy.
2. Copy the Avaya Breeze® platform patch to each node.
3. Run the following command:

   ```
   patchCE -i <path>/<patch binary>
   ```

   All nodes reboot after the installation is complete.
4. After the reboot, wait until the new nodes replicate successfully with System Manager and pass the maintenance tests.

Installing the OceanaConfiguration service to Provisioning Cluster

About this task

Use this procedure to install the OceanaConfiguration service to Provisioning Cluster.

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 Provisioning Cluster.
3. Click **Edit**.
4. On the Cluster Editor page, click the **Services** tab.
5. In the Available Services list, click the plus sign **(+)** on the OceanaConfiguration service to install the service to Provisioning Cluster.
6. Click **Commit**.
7. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
8. On the Services page, verify that the state of the OceanaConfiguration service is `Installing`.

   The state changes to `Installed` when the installation is complete.
9. Wait until the service is installed.
10. Set OceanaConfiguration attributes according to the attribute values that you recorded while uninstalling the older version of the OceanaConfiguration service.

    For information about the latest attributes of OceanaConfiguration, see *Deploying Avaya Oceana®*.

Installing services to the clusters

About this task

Use this procedure to install the snap-ins to their relevant clusters. For the list of services or snap-ins of each cluster, see *Deploying Avaya Oceana®*.

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 Avaya Oceana® Cluster 1.
3. Click **Edit**.

4. On the Cluster Editor page, click the **Services** tab.
5. In the Available Services list, click the plus sign **(+)** on each service of Avaya Oceana® Cluster 1.

   When you click the plus sign **(+)** on a service, System Manager moves the service from the Available Services list to the Assigned Services list. After the service moves to the Assigned Services list, you can click the plus sign **(+)** on the next service.
6. In the Available Services list, click the plus sign **(+)** on the latest versions of the CallEventControl and EventingConnector services.
7. In the Assigned Services list, click **Uninstall** for the older installed versions of CallEventControl and EventingConnector services.
8. Click **Commit**.
9. On the Cluster Administration page, select the check box for Avaya Oceana® Cluster 2.
10. Click **Edit**.
11. On the Cluster Editor page, click the **Services** tab.
12. In the Available Services list, click the plus sign **(+)** on each service of Avaya Oceana® Cluster 2.

    When you click the plus sign **(+)** on a service, System Manager moves the service from the Available Services list to the Assigned Services list. After the service moves to the Assigned Services list, you can click the plus sign **(+)** on the next service.
13. In the Available Services list, click the plus sign **(+)** on the latest versions of the CallEventControl, EventingConnector, and AuthorizationService services.
14. In the Assigned Services list, click **Uninstall** for the older installed versions of CallEventControl, EventingConnector, and AuthorizationService services.
15. Click **Commit**.
16. On the Cluster Administration page, select the check box for Avaya Oceana® Cluster 3.
17. Click **Edit**.
18. On the Cluster Editor page, click the **Services** tab.
19. In the Available Services list, click the plus sign **(+)** on each service of Avaya Oceana® Cluster 3.

    When you click the plus sign **(+)** on a service, System Manager moves the service from the Available Services list to the Assigned Services list. After the service moves to the Assigned Services list, you can click the plus sign **(+)** on the next service.
20. In the Available Services list, click the plus sign **(+)** on the latest versions of the CallEventControl and EventingConnector services.
21. In the Assigned Services list, click **Uninstall** for the older installed versions of CallEventControl and EventingConnector services.
22. Click **Commit**.

23. Repeat Step 16 to Step 22 for Avaya Oceana® Cluster 4 and Avaya Oceana® Cluster 5.
24. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
25. On the Services page, verify that the state of all services is `Installing`.

    The state changes to `Installed` when the installation is complete.
26. Wait until all services are installed.
27. Restart the Avaya Breeze® platform nodes of Avaya Oceana® Cluster 2, Avaya Oceana® Cluster 3, Avaya Oceana® Cluster 4, and Avaya Oceana® Cluster 5.

Editing service profiles to add snap-ins

About this task

Use this procedure to edit any existing service profiles in System Manager to add EngagementDesigner and AvayaMobileCommunications snap-ins to service profiles.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Service Profiles**.
2. On the Service Profile Configuration page, select a service profile and click **Edit**.
3. In the Available Service to Add to this Service Profile area, click the plus sign (**+**) on AvayaMobileCommunications and EngagementDesigner services to add them to the service profile.

    AvayaMobileCommunications and EngagementDesigner services are added to service profiles to support Web Voice, Web Video, and Engagement Designer initiated calls.
4. Click **Commit**.
5. Repeat Step 2 to Step 4 for all service profiles.

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.

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 Admin Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`
2. On the Bundles tab, click **Upload**.
3. On the Choose bundle file to upload dialog box, click **Choose File**.
4. Browse to the `EngagementDesignerTasks.svar` file and click **Upload**.
5. Select the bundle and click **Deploy**.

   After the bundle is deployed successfully, ensure that:

   - The **Deployed** column for the bundle displays the value `Yes`.
   - The **Deployed Nodes** column for the bundle contains all nodes of Avaya Oceana® Cluster 1.

   When you open or refresh the Designer Console of Engagement Designer, the system displays the drawers and tasks associated with the tasks bundle.

6. Repeat steps 2 to 5 to deploy Context Store, Work Assignment, and Oceana tasks.

Deploying Engagement Designer workflows

Before you begin

Download the latest version of the sample workflow from PLDS.

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 a 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**.

   Note:

   You can either configure the workflow attributes while deploying the workflow or at a later time.

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 workflow is available in the list of deployed workflows.
11. Repeat Step 2 to Step 10 to deploy and verify all remaining workflows.

Recreating Engagement Designer rules for Transfer workflows

About this task

Avaya Oceana® supports the Transfer to Service and Transfer to User features. The ROUTE_CONTACT_TRANSFER event was previously named ROUTE_CONTACT_TRANSFER_TO_SERVICE. If you are upgrading from Avaya Oceana® Release 3.6.x or earlier, you must delete any existing Engagement Designer rules applicable to Transfer workflows and re-create the rules using the ROUTE_CONTACT_TRANSFER event.

You can skip this procedure if you are upgrading from Avaya Oceana® Release 3.7.x to 3.8.x.x onwards.

Before you begin

- Import and deploy the most recent Transfer workflows.
- Make a note of the existing routing rules in the Engagement Designer Admin UI.

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 only Transfer workflows are available in the list of deployed workflows.
3. Click the **Routing** tab.
4. Delete all existing Transfer rules applicable for all channels.

   Note:

   You cannot edit these rules if they use the ROUTE_CONTACT_TRANSFER_TO_SERVICE event. You must delete and then re-create them.

5. Recreate the rules using the ROUTE_CONTACT_TRANSFER event. For more information about creating Engagement Designer rules, see *Deploying Avaya Oceana®*.

Configuring the attributes and routing rules of Engagement Designer workflows

Before you begin

Install the Engagement Designer workflow for which you want to configure the attributes and routing rules.

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 check box for the workflow for which you want to configure the attributes.
3. Click **Attributes**.
4. On the Workflow Attributes tab, configure the required attributes and click **Close**.
5. Click the **Routing** tab.
6. Select the appropriate rule from the list of rules and click **Edit**.
7. In the **Select workflows** drop-down list, select the latest workflow and click **Save**.
8. Repeat Step 2 to Step 7 for the other workflows.

Configuring CustomerControllerService attributes for connection to Omnichannel Database

About this task

Use this procedure to configure the CustomerControllerService service attributes for connection to the Omnichannel Database.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Attributes Configuration page, click the **Service Clusters** tab.
3. In the **Cluster** field, select the **OCP Cluster**, usually Cluster 3.
4. In the **Service** field, select **CustomerControllerService**.
5. In the **Advanced** section, in **Password for the Omnichannel Database**, enter the password for Omnichannel Database.
6. In the **Secure Connections to Omnichannel Database** field, select `true`.

   This attribute toggles a secure connection to the Omnichannel Database.
7. Click **Commit**.

CylancePROTECT upgrade

Disabling CylancePROTECT before the upgrade

Before you begin

Ensure to run the following commands on every node.

Procedure

1. To disable CylancePROTECT, run the following commands:

   ```
   systemctl stop cylancesvc.service
   systemctl disable cylancesvc.service
   systemctl is-enabled cylancesvc.service
   systemctl status cylancesvc.service
   ```

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

   ```
   systemctl --type=service | grep Cy
   ```

Re-enabling CylancePROTECT post upgrade

Procedure

To re-enable CylancePROTECT, run the following commands:

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

Chapter 5: Upgrading Avaya Control Manager

Avaya Control Manager upgrade overview

This chapter provides information about the tasks that you must perform to upgrade Avaya Control Manager, which acts as the centralized administration interface for Avaya Oceana®.

The high-level tasks of the Avaya Control Manager upgrade process are:

- Taking a backup of Avaya Control Manager databases to preserve information such as Avaya Control Manager system configuration.
- Uninstalling the Arbiter service from the Avaya Control Manager server.
- Upgrading Avaya Control Manager from 8.0.4, 8.1 or 8.1.0.1 to 9.x.

  Ensure that you stop the services on the Avaya Control Manager server before upgrading.
- Installing the latest version of the Arbiter service on the Avaya Control Manager server.

Important:

- After upgrading Avaya Control Manager and the Omnichannel server, do not use them until the Avaya Oceana® and Avaya Breeze® platform upgrade is complete.
- When you upgrade to Avaya Control Manager 9.x, you must obtain a new license.

Avaya Control Manager upgrade checklist

Use the following checklist to upgrade Avaya Control Manager:

No.	Task	Notes	✔
1	Download the Avaya Control Manager 9.x installer on the Avaya Control Manager server.	You can download the Avaya Control Manager 9.x installer from Avaya PLDS at http://plds.avaya.com/.	

Table continues…

No.	Task	Notes	✔
2	Stop the following services on the Avaya Control Manager server: • All Avaya Control Manager services • Apache Tomcat • IIS Admin Service	See Stopping the services on the Avaya Control Manager server on page 64.	
3	Take a backup of the following Avaya Control Manager databases: • ACCCM • ACCCMAVP • ACCCMONEXDB • ACCCMCMSYSLOG • ACCCMSYNC	See Taking a backup of Avaya Control Manager databases on page 65.	
4	Uninstall the Arbiter service from the Avaya Control Manager server (optional).	See Uninstalling the Arbiter service on page 66.	
5	Upgrade Avaya Control Manager to Release 9.x.	See Upgrading Avaya Control Manager on page 66.	
6	Install the latest version of the Arbiter service on the Avaya Control Manager server (optional).	See Installing the Arbiter service on page 67.	

Stopping the services on the Avaya Control Manager server

About this task

Use this procedure to stop the services on the Avaya Control Manager server before upgrading Avaya Control Manager. Alternatively, you can also use the Avaya Control Manager Update Manager tool to stop and start the services.

Procedure

1. Log in to the Avaya Control Manager server as an administrator.
2. Click **Start** > **Run**.
3. In the Run dialog box, type `services.msc` and click **OK**.

   The Avaya Control Manager server displays the Services window.
4. Right-click each Avaya Control Manager service and click **Stop**.

5. Right-click **Apache Tomcat** and click **Stop**.
6. Right-click **IIS Admin Service** and click **Stop**.

Taking a backup of Avaya Control Manager databases

About this task

Use this procedure to take a backup of the following databases before upgrading Avaya Control Manager:

- ACCCM
- ACCCMAVP
- ACCCMONEXDB
- ACCCMCMSYSLOG
- ACCCMSYNC

Procedure

1. On the SQL server used for Avaya Control Manager, open the SQL Management Studio application.
2. In the Connect to Server window, enter the following information:
    - Server type
    - Server name
    - Authentication
    - User name
    - Password
3. Click **Connect**.
4. In the Object Explorer pane, expand the Databases navigation tree and select the ACCCM database.
5. Right-click the database and click **Tasks** > **Back Up**.

    The SQL server displays the Back Up Database window.
6. In the Select a page pane, click **General**.
7. In the **Backup type** field, click **Full**.
8. In the Destination area, click **Add**.
9. In the **File name** field, browse and select the directory where you want to store the backup file.

    You must store the file in the `.bak` format.

10. Click **OK**.
11. Repeat Step 4 to Step 9 to take a backup of the remaining databases.

Uninstalling the Arbiter service

About this task

Use this procedure to uninstall the Arbiter service from the Avaya Control Manager server.

Note:

If the latest version of the Arbiter service is already installed on the server, you do not need to uninstall and reinstall the Arbiter service. This procedure is also required only if your solution uses Omnichannel server campus High Availability.

Procedure

1. Log in to the Avaya Control Manager server as an administrator.
2. Click **Start** > **Control Panel** > **Programs** > **Programs and Features**.

   The Avaya Control Manager server displays the Uninstall or change a program page.
3. In the list of programs, select **Caché instance [CACHE]**.
4. Click **Uninstall/Change**.
5. In the Confirmation message box, click **Yes**.

Upgrading Avaya Control Manager

For information about how to upgrade Avaya Control Manager to 9.0, see *Avaya Control Manager 9.0 Release Notes* at http://support.avaya.com.

Note:

After you upgrade Avaya Control Manager, log on to Avaya Control Manager and navigate to **Configuration** > **Avaya Oceana™** > **Server Details**. Verify that the correct version of Avaya Oceana® is set.

Installing the Arbiter service

About this task

Use this procedure to install the Arbiter service, which controls the Omnichannel Database failover. If the primary Avaya Control Manager server is unreachable, the automatic Omnichannel Database failover does not occur until the primary Avaya Control Manager application server is recovered.

The configuration of the Arbiter service involves minimal software installation and does not require the installation of Cache.

Note:

This procedure is required only if your solution uses Omnichannel server campus High Availability.

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\Cache2018` 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 the **Startup type** field, 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**.

Chapter 6: Upgrading the Omnichannel server

Enabling or disabling a scheduled computer maintenance in Windows 2016

About this task

Windows Server 2016 provides a centralized mechanism called Computer Maintenance, for maintaining the operating system, to perform hard disk defragmentation, and Microsoft Windows updates. Computer Maintenance can interfere with the deployment of Contact Center software, resulting in failed installations. You can turn on or off, the scheduled computer maintenance during the software installation.

Procedure

1. Open Windows Control Panel.
2. Navigate to **Troubleshooting** > **Change Settings**.
3. Before an installation Omni Channel Provider (OCP) begins, on the Change troubleshooting settings page, select **Off**.
4. Click **OK**.
5. After the installation process completes, on the Change troubleshooting settings page, select **On (Recommended)**.
6. Click **OK**.

Upgrading from Avaya Oceana® 3.7 and earlier versions to Avaya Oceana® 3.8.1 version

This chapter provides information about the tasks that you must perform to upgrade the Omnichannel server software.

Note:

Refer to this section for upgrading from Avaya Oceana® 3.7 and earlier versions to Avaya Oceana® 3.8.1 version. To upgrade from Avaya Oceana® 3.7.0.1 and later versions to Avaya

Oceana® 3.8.1 version, see Upgrading from Avaya Oceana 3.7.0.1 and later versions to Avaya Oceana 3.8.1 version on page 85.

The high-level tasks of the Omnichannel server upgrade process are:

- Removing Omnichannel Database Mirrorring from Omnichannel databases.

  This task is applicable for the following configurations:

  - Mirroring configuration with a backup server. For example, a DR 1+1 deployment.
  - Mirroring configuration with failover and backup servers. For example, a campus HA and DR 2+1 deployment.
- Taking a backup of the active Omnichannel database.
- Deploying a new Microsoft Windows Server 2016 virtual machine with the latest software updates. If you have a HA or DR solution, deploy additional Microsoft Windows Server 2016 virtual machines to replace your existing servers.
- Installing the latest version of the Omnichannel server software.
- Restoring the Omnichannel database for migrations from earlier releases to Avaya Oceana® 3.8.

Important:

- From Avaya Oceana® 3.7, Omnichannel server is supported only on Microsoft Windows Server 2016 (Desktop Experience).
- You must install, run, and patch the Omnichannel server software using a Windows Administrator account with full Administrator privileges. You must run the Oceana Data Management Tool using this same account.
- After upgrading Avaya Control Manager and the Omnichannel server, do not use them until you upgrade Avaya Breeze® platform.

Reducing the maintenance window downtime

If you are upgrading a live production solution, you can reduce the maintenance window downtime by preparing Windows 2016 servers before the start of the maintenance window. There are two options you can use, which are summarized here:

Option 1 — using a new hostname and IP address for the new Windows Server 2016 Omnichannel server:

1. Before the maintenance window:
   a. Build the Windows Server 2016 Virtual Machine.
   b. Install Windows Server 2016 updates, IIS, and add the server to a domain.
   c. Install the Omnichannel server software.
2. During the Maintenance Window:
   a. Take a database backup of the Windows Server 2012 Omnichannel database.
   b. Take the existing Windows Server 2012 Omnichannel server off line and power it off.

   c. Restore the Omnichannel database on the Windows Server 2016 Omnichannel server.
   d. Log on to SMGR and reconfigure the Omnichannel Database Address attribute to reference the IP address or FQDN of the new Windows Server 2016 Omnichannel server.

Option 2 — reuse the same hostname and IP address for the new Windows Server 2016 Omnichannel server:

1. Before the maintenance window:
   a. Build the Windows Server 2016 Virtual Machine.
   b. Install Windows Server 2016 updates, IIS, and add the server to a domain.
   c. Install the Omnichannel server software.
2. During the Maintenance Window:
   a. Take a database backup of the Windows Server 2012 Omnichannel database.
   b. Take the existing Windows Server 2012 Omnichannel server off line and power it off.
   c. Rename the new Windows Server 2016 Omnichannel server to reuse the existing IP address and host name of the Windows Server 2012 Omnichannel server.
   d. On the new Windows Server 2016 Omnichannel server, delete this file: `<install drive>\Avaya\Cache\Cachesys\mgr\cache.ids`. After you delete this file, Caché creates a new file with the new hostname details.

      Important:

      Do not edit this file, you must delete it.
   e. Restore the Omnichannel database on the Windows Server 2016 Omnichannel server.

Related links

Omnichannel server upgrade checklist on page 71
Installing Microsoft Windows Server 2016 on page 76
Installing the most recent supported operating system service packs on page 77
Adding the server to a domain on page 78
Disabling unused network adapters on page 79
Enabling Microsoft Remote Desktop connection on page 80

Omnichannel server upgrade checklist

Use the following checklist to upgrade the Omnichannel server:

For upgrading from the releases earlier than Avaya Oceana® 3.7 to 3.8.1 version:

No.	Task	Notes	✔
1	Download the latest version of the Omnichannel server software on the Omnichannel server.	You can download the latest version of the Omnichannel server software from http://support.avaya.com. The format of the file is `OCEANA_x.x.xxx.iso`.	
2	Remove the current Cache Mirroring configuration.	See Remove the current Omnichannel Database Mirroring configuration on page 73.	
3	Take a backup of the Omnichannel database.	See Taking a backup of the Omnichannel database on page 74.	
4	Install a new Microsoft Windows Server 2016 virtual machine with the latest software updates.	See Installing Microsoft Windows Server 2016 on page 76 and the accompanying procedures.	

For upgrading from Avaya Oceana® 3.7 to 3.8.1 version:

No.	Task	Notes	✔
1	Download the latest version of the Omnichannel server software on the Omnichannel server.	You can download the latest version of the Omnichannel server software from http://support.avaya.com. The format of the file is `OCEANA_x.x.xxx.iso`.	
2	Install the latest version of the Omnichannel server software on the Omnichannel server.	See Installing the Omnichannel server software on page 81.	
3	Restore the Omnichannel database for migrations from earlier releases to Avaya Oceana® 3.8.1.	See Restoring the Omnichannel database on page 82.	
4	Configuring Cache Mirroring.	See the following documents: • *Deploying Avaya Oceana®* • *Avaya Oceana® and Avaya Analytics™ Disaster Recovery*	
5	Patching the Omnichannel server software.	See Patching the Omnichannel server software on page 83.	
6	Upgrading from Avaya Oceana® 3.7 to 3.8.1.	See Upgrading from Avaya Oceana® 3.7 to 3.8.1 on page 85.	

Related links

Upgrading from Avaya Oceana 3.7 and earlier versions to Avaya Oceana 3.8.1 version on page 69

Remove the current Omnichannel Database Mirroring configuration

If the Omnichannel servers in your solution have any of the following Omnichannel Database Mirroring configurations, then you must remove the configuration before starting the upgrade process:

- Mirroring configuration with a backup server
- Mirroring configuration with failover and backup servers

In the Mirroring configuration with a backup server (DR 1+1), remove the Omnichannel Database Mirroring in the following order:

1. Remove Omnichannel Database Mirroring from the backup server in Data Center 2
2. Remove Omnichannel Database Mirroring from the active server in Data Center 1

In the Mirroring configuration with failover and backup servers (Campus HA and DR, 2+1), remove the Omnichannel Database Mirroring in the following order:

1. Remove Omnichannel Database Mirroring from the backup server in Data Center 2
2. Remove Omnichannel Database Mirroring from the standby server in Data Center 1
3. Remove Omnichannel Database Mirroring from the active server in Data Center 1

Removing Cache Mirroring from the backup Omnichannel server

Procedure

1. In your web browser, enter the following URL to open Cache Management Portal:

   `http://<BackupOmnichannelServerIP>:57772/csp/sys/UtilHome.csp`

   <BackupOmnichannelServerIP> is the IP address of the backup Omnichannel server in Data Center 2.
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. Click **Yes** and then click **Remove** to remove the mirrored attribute.

Removing Cache Mirroring from the standby Omnichannel 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 standby Omnichannel server in Data Center 1.

2. On the Cache Management Portal login page, do the following:
   1. In the **User Name** field, type `_admin`.
   2. In the **Password** field, type `Oceana16`.
   3. Click **LOGIN**.
3. On Cache Management Portal, click **System Administration** > **Configuration** > **Mirror Settings** > **Edit Mirror** > **Remove Mirror Configuration**.
4. Click **Yes** and then click **Remove** to remove the mirrored attribute.
5. Restart the Windows Omnichannel Database server.

Removing Cache Mirroring from the active Omnichannel 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 active Omnichannel server in Data Center 1.
2. On the Cache Management Portal login page, do the following:
   1. In the **User Name** field, type `_admin`.
   2. In the **Password** field, type `Oceana16`.
   3. 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. Log in to Cache Management Portal.
8. On Cache Management Portal, click **System Administration** > **Configuration** > **Mirror Settings** > **Edit Mirror** > **Remove Mirror Configuration**.
9. Click **Yes** and then click **Remove** to remove the mirrored attribute.

Taking a backup of the Omnichannel database

About this task

Use this procedure to take a backup of the Omnichannel database. This procedure is applicable for a standalone Omnichannel database that does not have a cache mirror.

For information about how to take a backup of the Omnichannel database that has a cache mirror, see *Avaya Oceana® and Avaya Analytics™ Disaster Recovery*.

Note:

- Ensure that you take backups of the Omnichannel database at regular intervals.
- The backup is taken from the active database if it was previously in an HA mirrored configuration on Data Center 1.

Procedure

1. Log in to the Omnichannel server.
2. Do one of the following:
    - For Avaya Oceana® 3.5.x or 3.6, go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\Oceana\BackupAndRestore` folder.
    - For Avaya Oceana® 3.7 or higher version, go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement` folder.
3. Do one of the following:
    - For Avaya Oceana® 3.5.x or 3.6, right-click the `BackupAndRestore.exe` file and select **Run as Administrator**.
    - For Avaya Oceana® 3.7 or higher version, double-click the `OceanaDataManagementTool.exe` file.
4. In the Oceana Data Management utility, click **Backup and Restore**.
5. In the navigation pane, click **Backup and Restore**.
6. In the **Select/create file to backup to** field, click **Browse**.
7. 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**.
8. Click **Backup Database**.

   The utility displays the `Backup complete!` message when the backup process is complete.
9. Verify that the backup file is created at the specified location.

Installing Microsoft Windows Server 2016

About this task

Install the Microsoft Windows Server 2016 (Desktop Experience) Standard or Datacenter edition and configure it to support the Omnichannel software.

Before you begin

- Ensure that you have a newly formatted server that meets the specifications for installing Microsoft Windows Server 2016 (Desktop Experience) Standard or Datacenter edition.
- Ensure that you have a DVD of the Microsoft Windows Server 2016 (Desktop Experience) Standard or Datacenter edition.
- Ensure that you have a product key for Microsoft Windows Server 2016 (Desktop Experience) Standard or Datacenter edition.
- Obtain the IP addresses for the Omnichannel subnet.

Procedure

1. Insert the Microsoft Windows Server 2016 (Desktop Experience) DVD into the DVD drive.
2. Turn on the power to the server.

   The server begins to boot up.
3. On the Windows Setup screen, in the **Language to install** field, select the appropriate language.
4. In 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 2016 that includes a Desktop Experience.
9. Click **Next**.
10. On the Enter the product key to activate Windows screen, enter the operating system product key.
11. Click **Next**.
12. On the Applicable notices and license terms screen, read the notices and terms, and select **I accept the license terms**.
13. Click **Next**.
14. Select **Custom: Install Windows only (advanced)** for a new installation.
15. Click **Next**.
16. Select the disk partition where you want to install Windows Server 2016 (Desktop Experience) Standard or Datacenter edition.

Important:

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

17. Click **Next**.

    The installation proceeds and automatically restarts the server several times.

18. After completing the installation, log on to the server as an administrator by entering and confirming the administrator password.
19. Select **Set time zone** and complete the information as required for your system.
20. Select **Configure Networking** and complete the information for your Network Interface Card (NIC) with the server IP address.
21. Select **Provide computer name and domain** and complete the information for your server name and network settings.
22. Change the DVD drive letter to **E:** and ensure that the correct drive letters are free for the Omnichannel application and database hard disk drives and partitions.
23. Configure the hard disk drives and partitions for this server using the Windows Server 2016 (Desktop Experience) Standard or Datacenter edition.
24. Install other required drivers for your hardware configuration.

Related links

Upgrading from Avaya Oceana 3.7 and earlier versions to Avaya Oceana 3.8.1 version on page 69

Installing the most recent supported operating system service packs

About this task

Avaya recommends installing Operating System Service Packs and Security Hotfixes in a controlled manner during the initial deployment. Installing subsequent Operating System updates must be carefully controlled and tested within a planned Maintenance Window.

Avaya tests the Omnichannel software on Windows servers using the most recent Operating System updates of the time. However, because Microsoft publishes new Operating System updates every month, some precautions are necessary to ensure that Operating System updates published after the Omnichannel software is released do not break Oceana features or functions.

Note:

- Install and test the Operating System updates in the Preproduction solution before installing them in the Production solution.
- In Omnichannel Database HA solutions, to minimize number of server switchovers needed, perform this procedure first on the current backup server and then on the other Omnichannel server.

Before you begin

- Install and configure Microsoft Windows Server 2016 (Desktop Experience) Standard or Datacenter edition on your server.
- Disable Operating System Automatic Updates.

Procedure

1. Review the published Microsoft updates to determine the most recent patches or service packs for the Windows Server 2016 (Desktop Experience) Standard or Datacenter OS.
2. Download the appropriate Windows Server 2016 updates for the Omnichannel software installed on this server.
3. Plan a Maintenance Window.
    a. At the start of the Maintenance Window, take a VMware snapshot of the Omnichannel server.
    b. Install the most recent Windows Server 2016 Operating System Updates, following the Microsoft Installation instructions.
    c. Some of the OS updates and hotfixes may require a reboot of the Omnichannel server.
    d. Sanity test Oceana to ensure the OS updates and hotfixes have not broken any Oceana feature and function.
    e. If the OS updates and hotfixes break any feature and function, revert to the VM snapshot taken before applying the updates and notify Avaya of the issue.
    f. If the OS updates and hotfixes do not break any feature and function, delete the VM snapshot.
    g. For Omnichannel Database HA solutions, ensure Cache DB Mirroring is working before returning the solution to Production.
4. End the Maintenance Window.

Related links

Upgrading from Avaya Oceana 3.7 and earlier versions to Avaya Oceana 3.8.1 version on page 69

Adding the server to a domain

About this task

Before installing the Omnichannel software, you must add the server to the domain.

Before you begin

- Ensure that the server time and domain controller time are synchronized.
- On the server, configure a preferred Domain Name System (DNS) server on the Network Interface Card (NIC).

- Ask your System Administrator to add a Domain Name System (DNS) static entry for this server.

  Each Omnichannel server in a domain requires a DNS static entry.

Procedure

1. Log on to the server.
2. Click **Start** > **Server Manager**.
3. In the navigation pane, click **Local Server**.
4. In the content pane, in the PROPERTIES section, double-click the **Domain** value.
5. In the System Properties dialog box, click the **Computer Name** tab.
6. Click **Change**.
7. In the Member of dialog box, click **Domain** to add the server to a domain.
8. In the **Domain** field, 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.

Related links

Upgrading from Avaya Oceana 3.7 and earlier versions to Avaya Oceana 3.8.1 version on page 69

Disabling unused network adapters

About this task

Use this procedure to disable all unused network adapters or Network Interface Cards (NICs) to improve network communications and prevent the erroneous configuration of unused NICs during the Omnichannel server commissioning.

Procedure

1. Log on to the server.
2. Click **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center**.
3. In the navigation pane, click **Change adapter settings**
4. Right-click the unused network adapter and click **Disable**.
5. Repeat Step 4 to disable all unused network adapters.

Related links

Upgrading from Avaya Oceana 3.7 and earlier versions to Avaya Oceana 3.8.1 version on page 69

Enabling Microsoft Remote Desktop connection

About this task

Use this procedure to enable Microsoft Remote Desktop connection as your remote access tool. Microsoft Remote Desktop provides remote access for support on the server.

Important:

This procedure is optional. System administrators must determine whether to enable Microsoft Remote Desktop connection.

Procedure

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

Related links

Upgrading from Avaya Oceana 3.7 and earlier versions to Avaya Oceana 3.8.1 version on page 69

Installing Microsoft IIS on Omnichannel Windows Server

About this task

Before installing the Omnichannel server software, you must install Microsoft Internet Information Services (IIS) on Omnichannel Windows Server.

Procedure

1. Log in to the Omnichannel server.
2. Click **Start** > **Server Manager**.
3. On the Server Manager screen, in the QUICK START section, click **Add roles and features**.
4. On the Before you begin screen, click **Next**.

5. On the Select installation type screen, click **Next**.
6. On the Select destination server screen, click **Next**.
7. On the Select server roles screen, select **Web Server (IIS)** and click **Next**.
8. Complete the remaining steps and click **Finish**.

Installing the Omnichannel server software

About this task

Use this procedure to install the Omnichannel server software.

When you install the Omnichannel server software, the installer disables SSL 3.0, TLS 1.0, and TLS 1.1 on the Omnichannel server. Therefore, you must enable them after the installation is complete.

Important:

You must install, run, and patch the Omnichannel server software using a Windows Administrator account with full Administrator privileges. You must run the Oceana Data Management Tool using this same account.

Procedure

1. Log in to the Omnichannel server.
2. Right-click the `OCEANA_x.x.xxx.iso` file and click **Mount**.
3. Double-click the `Setup.exe` file.
4. Click **Accept** to install the Microsoft .NET Framework on the Omnichannel server.

   You must install Microsoft .NET Framework 4.7.2.
5. If the installer prompts you to accept the Microsoft .NET Framework license agreement, click **Accept**.
6. If the installer prompts you to restart the server, click **Yes** and repeat Step 4.

   The installer runs the operating system and hardware checks on the server. If the software installation fails, you must review the logs of System Readiness Check and resolve the problems that caused the failure. You can ignore the warnings that do not impact the operation of the contact center.

   The installer displays the Omnichannel Server Select Destination Drive screen.
7. In the **Product Install Drive** field, select the hard disk partition for the main application.
8. In the **Journal Database Drive** field, select the hard disk partition for the Journal database.
9. In the **Oceana Database Drive** field, select the hard disk partition for the Omnichannel database.
10. Click **Next**.

11. On the AVAYA GLOBAL SOFTWARE LICENSE TERMS screen, click **I ACCEPT THE LICENSE TERMS**.
12. After the installation is complete, click **Restart**.

Restoring the Omnichannel database

About this task

Use this procedure to restore the Omnichannel database onto your Microsoft Windows Server 2016 (Desktop Experience) Omnichannel server. This procedure is applicable for a standalone Omnichannel database that does not have a database mirror. For information about how to restore the Omnichannel database that has a database mirror, see *Avaya Oceana® and Avaya Analytics™ Disaster Recovery*.

Important:

You must install, run, and patch the Omnichannel server software using a Windows Administrator account with full Administrator privileges. You must run the Oceana Data Management Tool using this same account.

Procedure

1. Log in to the Omnichannel server as an administrator.
2. Do one of the following:
   - For Avaya Oceana® 3.5.x or 3.6, go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\Oceana\BackupAndRestore` folder.
   - For Avaya Oceana® 3.7 or higher version, go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement` folder.
3. Do one of the following:
   - For Avaya Oceana® 3.5.x or 3.6, right-click the `BackupAndRestore.exe` file and select **Run as Administrator**.
   - For Avaya Oceana® 3.7 or higher version, double-click the `OceanaDataManagementTool.exe` file.
4. In the Oceana Data Management utility, click **Backup and Restore**.
5. In the navigation pane, click **Backup and Restore**.
6. Navigate to the **Select file to restore from** section.
7. The **Allow Restore if user file is missing** option is checked by default. This ensures that the restore continues without error even if a user file is missing while the Restore file is present on a folder .
8. Click **Browse**.
9. Select the backup file and click **Open**.
10. Click **Restore Database**.

The application displays the Drive restore screen.

11. In the **Select your database drive letter** field, select the drive that you specified for the Omnichannel database when installing the Omnichannel server software.
12. In the **Are you restoring a mirrored backup** field, select one of the following options:
    - Select **Yes** if you are taking the backup from the server with mirroring configured.
    - Select **No** if you are taking the backup from a system with no mirroring configured.
13. Click **Restore**.

    Important:

    If the Omnichannel server displays the Cache Post Restore Script terminal window, keep the window open until the process in the window is completed.

    Note:

    If the **Allow Restore if user file is missing** option is unchecked and a user file is missing, then the restore is not completed and a message box appears. To complete the restore, you must check the **Allow Restore if user file is missing** option and restart the restore process.

    The utility displays the `Restore complete!` message when the restore process is complete.
14. **(Optional)** If you modified the default passwords of the Omnichannel database, modify the passwords again after the restore process because the backup does not contain the previously modified passwords.
15. **(Optional)** If you configured the Omnichannel server for secure connections, reconfigure the server for secure connections after the restore process.

Patching the Omnichannel server software

About this task

Use this procedure to patch the Omnichannel server software to ensure that the most current application updates are installed.

Before you begin

- Download the most recent Avaya Oceana® Omnichannel patch.
- Take a backup of the Omnichannel database.
- Uninstall an existing Avaya Oceana® Omnichannel patch.

Procedure

1. Log in to the Omnichannel server.

2. Double-click the `Avaya_OCP_x.x.x.x.xxx.x.msi` patch file.

   The installer displays the details of the patch.
3. Click **Next**.

   The installer displays the License Agreement screen.
4. Click **Next** to accept the license agreement.
5. Click **Install** to start the installation of the patch.

   The installer displays the progress of the installation and presents the Oceana Omnichannel Installer Completed screen on completion.
6. Click **Finish** to complete the patch installation.
7. If the installer prompts you to restart the server, click **Yes** to finalize the patch installation.

Uninstalling an Omnichannel server software patch

About this task

Use this procedure to uninstall an existing Avaya Oceana® Omnichannel patch.

Before you begin

Take a backup of the Omnichannel database.

Procedure

1. Log in to the Omnichannel server.
2. Click **Start** > **Settings** > **Apps & features** > **Apps & features** to start the **Add or Remove Programs** application.

   The server displays the currently installed Oceana Omnichannel patches with patch number.
3. Select the `Avaya_OCP_x.x.x.x.xxx.x` patch to be uninstalled.
4. Click **Uninstall**.
5. Click **Uninstall** to start the actual removal of the patch.
6. If the installer prompts you to restart the server, click **Yes**.

Upgrading from Avaya Oceana® 3.7.0.1 and later versions to Avaya Oceana® 3.8.1 version

About this task

Use this procedure to upgrade from Avaya Oceana® 3.7.0.1 and later versions to Avaya Oceana® 3.8.1 version.

You need to update HA and DR Omnichannel Database servers in the following order:

1. Upgrade Standby server
2. Perform Switchover
3. Upgrade Standby server (previously the Primary server)
4. Perform Switchover
5. Upgrade the DR server if installed. This step is optional.

Before you begin

Ensure that the High Availability servers are operational.

Procedure

1. Log on to the Omnichannel standby server, do the following:
    a. Right-click the `OCEANA_x.x.xxx.iso`.
    b. Click **Mount**.
    c. Run `AvayaReleasePackInstaller.exe`.
    d. If the installer prompts for server restart, click **Yes** and repeat step (a) though step (c).
    e. Click **Next**.
    f. Click **Accept** on license agreement.
    g. Click **Restart**.
2. Log on to the Omnichannel standby server, do the following:
    a. Start **Oceana Data Management Tool**.
    b. Go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDatamanagement` folder.
    c. Double click the `OceanaDataManagementTool.exe` file.
    d. In the Oceana Data Management Tool, click **Backup and Restore**.
    e. In the navigation pane, click **Backup and Restore**
    f. In the content pane, click **Mirror Configuration**.
    g. Select the **Switchover Cache up on both servers – Backup server**.
    h. Click **Execute** and wait for the script to complete.
    i. Click **Ok**.

3. Log on to the Omnichannel Primary Server, do the following:

   ✱ **Note:**

   This server is now running as a Standby server.

   a. Using the Cache Cube in the system tray start **Cache**.
   b. Right-click the `OCEANA_x.x.xxx.iso`.
   c. Click **Mount**.
   d. Run `AvayaReleasePackInstaller.exe`.
   e. If the installer prompts for server restart, click **Yes** and repeat step (c) though step (e).
   f. Click **Next**.
   g. Click **Accept** on license agreement.
   h. Click **Restart**.
4. Log on to the Omnichannel Primary server (running as standby server now), do the following:
   a. Start **Oceana Data Management Tool**.
   b. Go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDatamanagement` folder.
   c. Double click the `OceanaDataManagementTool.exe` file.
   d. In the Oceana Data Management Tool, click **Backup and Restore**.
   e. In the navigation pane, click **Backup and Restore**.
   f. In the content pane, click **Mirror Configuration**.
   g. Select the **Switchover Cache up on both servers – Backup server**.
   h. Click **Execute** and wait for the script to complete.
   i. Click **Ok**.
5. Upgrade the DR Omnichannel server if installed.
   a. Log on to the Omnichannel DR server.
   b. Right-click the `OCEANA_x.x.xxx.iso`.
   c. Click **Mount**.
   d. Run `AvayaReleasePackInstaller.exe`.
   e. If the installer prompts for server restart, click **Yes** and repeat step (a) though step (g).
   f. Click **Next**.
   g. Click **Accept** on license agreement.
   h. Click **Restart**.

Chapter 7: Post upgrade tasks

Post upgrade tasks overview

Note:

Post upgrade tasks are only applicable if you have updated from a release prior to Avaya Oceana® 3.7.0.0 version to Avaya Oceana® 3.8.1 version.

This chapter provides information about the tasks that you must perform to start Avaya Oceana® after completing the upgrade process.

Postupgrade tasks are:

- Enabling mailboxes to start processing of new emails after the upgrade.
- Configuring Avaya Oceana® to accept contacts so that it starts accepting SMS, Social, Chat, and Generic conversations.
- Configuring Avaya Oceana® to open chatrooms.
- Enabling Avaya Oceana® for voice calls so that all voice calls route to Avaya Oceana®.

Post upgrade checklist

Use the following checklist for the tasks that you must complete after upgrading Avaya Oceana®:

No.	Task	Notes	✔
1	Configure TLS for the Cache database, if you use a secure connection.	See *Deploying Avaya Oceana®*.	
2	Configure Omnichannel Database Mirroring on the active Omnichannel database servers for campus HA and DR solutions.	See *Deploying Avaya Oceana®* and *Avaya Oceana® and Avaya Analytics™ Disaster Recovery*.	
3	Configure Cache Mirroring on the standby Omnichannel database servers.	See *Deploying Avaya Oceana®* and *Avaya Oceana® and Avaya Analytics™ Disaster Recovery*.	

Table continues…

No.	Task	Notes	✔
4	Change the Omnichannel database password.	See *Deploying Avaya Oceana®*.	
5	If you are upgrading to Avaya Oceana® 3.8.x release, then do the following: Update the Avaya Analytics™ input adaptor configuration from **FORWARD_NOTIFICATION** to **SEND_NOTIFICATION**.	See *Maintenance and Troubleshooting Avaya Analytics™*.	
6	Verify that Avaya Oceana® and Avaya Analytics™ can communicate.	See Verifying Avaya Oceana Cluster 1 and Avaya Analytics communication on page 88.	
7	Enable Avaya Oceana® to monitor all configured mailboxes.	See Enabling mailboxes on page 91.	
8	Configure Avaya Oceana® to accept contacts.	See Configuring Avaya Oceana to accept contacts on page 91.	
9	Configure Avaya Oceana® to open chatrooms.	See Configuring Avaya Oceana to open chatrooms on page 92.	
10	Enable Avaya Oceana® for voice calls.	See Enabling Avaya Oceana for voice calls on page 93.	
11	Place Avaya Oceana® in production and validate all in-production functionality.	-	
12	Remove all snapshots before placing Avaya Oceana® in production.	-	
13	Configure AgentControllerService to have authenticated access to UnifiedAgentController.	See Configuring AgentControllerService to have authenticated access to UnifiedAgentController on page 97.	

Verifying Avaya Oceana® Cluster 1 and Avaya Analytics™ communication

About this task

After upgrading, you must ensure that Avaya Oceana® Cluster 1 is communicating with Avaya Analytics™ by checking the status of the cluster and the Avaya Breeze® platform Reliable Eventing Framework groups.

Procedure

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

   System Manager displays the Cluster Administration page.

2. Verify that a green check mark (✓) appears in the **TestsPass** column. If a green check mark does not appear, continue with the rest of this procedure.
3. On System Manager, click **Elements** > **Avaya Breeze®** > **System Tools and Monitoring** > **Maintenance Tests**.
4. In the **Select Avaya Breeze to test** field, click the Avaya Breeze® platform instance that you want to test.
5. Select the **Test Reliable Eventing Framework** check box.
6. Click **Execute Selected Tests**.

   Avaya Breeze® platform displays one of the following statuses:

   - `Failure` when Reliable Eventing is down. That is, publishing and receiving messages by Reliable Eventing is failing.
   - `Success` when Reliable Eventing is functional. That is, publishing and receiving messages by Reliable Eventing is working.

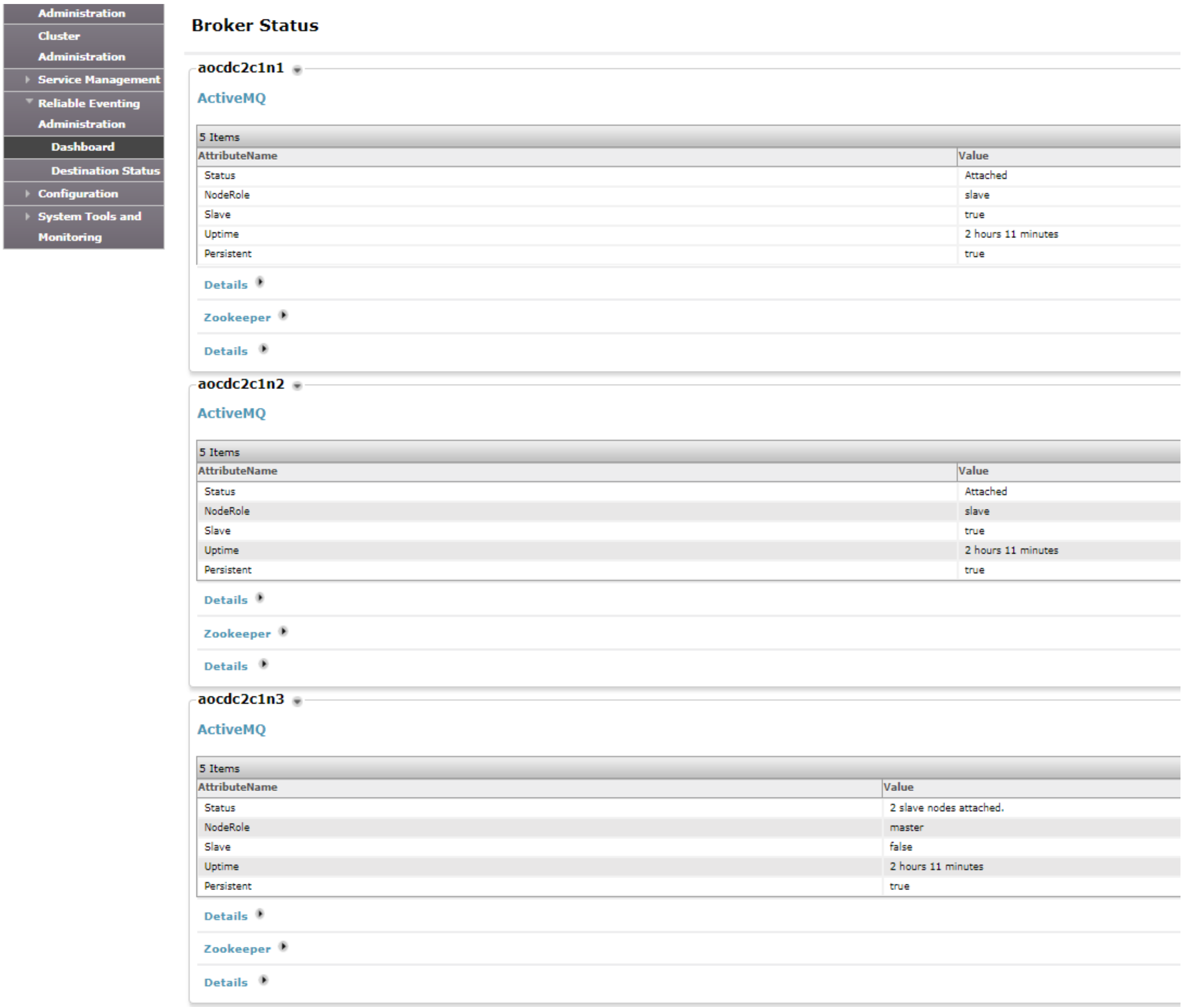
7. Repeat steps 4–6 for the remaining Avaya Breeze® platform nodes.
8. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.

   System Manager displays the Cluster Administration page.

9. Verify that a green check mark (✓) appears in the **TestsPass** column. If a green check mark does not appear, continue with the rest of this procedure.
10. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Reliable Eventing Administration** > **Dashboard**.
11. The **Status** column shows one of the following:

    - Green check mark (✓) : Indicates that the status of the broker is up and running for subscription and event transfers.
    - Red cross mark (✖): Indicates that the status of the broker is down.

12. To view the status of the brokers, click the green check mark.



aocdc2c1n1

ActiveMQ

5 Items

AttributeName	Value
Status	Attached
NodeRole	slave
Slave	true
Uptime	2 hours 11 minutes
Persistent	true

Details

Zookeeper

Details

aocdc2c1n2

ActiveMQ

5 Items

AttributeName	Value
Status	Attached
NodeRole	slave
Slave	true
Uptime	2 hours 11 minutes
Persistent	true

Details

Zookeeper

Details

aocdc2c1n3

ActiveMQ

5 Items

AttributeName	Value
Status	2 slave nodes attached.
NodeRole	master
Slave	false
Uptime	2 hours 11 minutes
Persistent	true

Details

Zookeeper

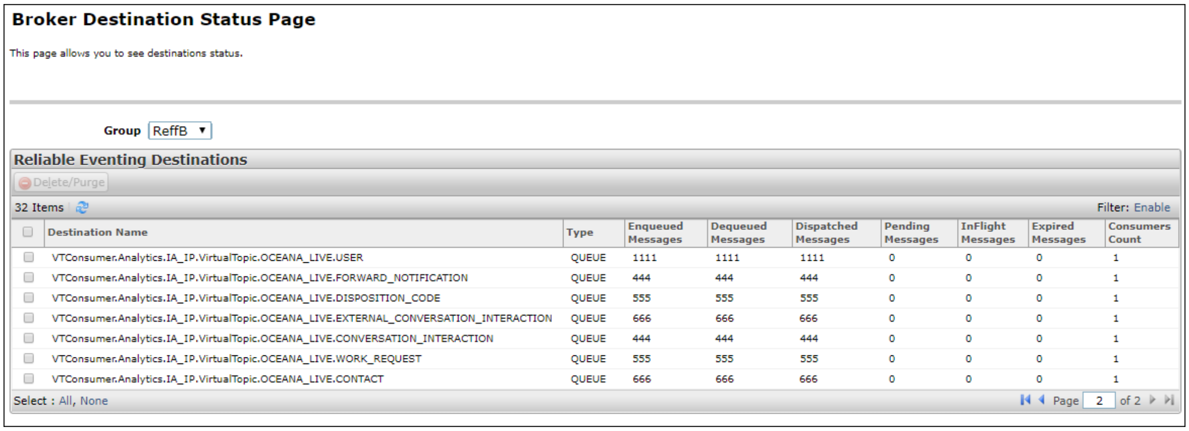
Details

13. On System Manager, click **Elements** > **Avaya Breeze®** > **Reliable Eventing Administration** > **Destination Status**.

    The system displays Broker Destination Status Page.

14. In the **Group** field, select the **Reliable Eventing group**.

    The system displays the destination status.



Broker Destination Status Page
This page allows you to see destinations status.
Group ReffB ▾
Reliable Eventing Destinations
Delete/Purge
32 Items
Filter: Enable

☐	Destination Name	Type	Enqueued Messages	Dequeued Messages	Dispatched Messages	Pending Messages	InFlight Messages	Expired Messages	Consumers Count
☐	VTConsumer.Analytics.IA_IP.VirtualTopic.OCEANA_LIVE.USER	QUEUE	1111	1111	1111	0	0	0	1
☐	VTConsumer.Analytics.IA_IP.VirtualTopic.OCEANA_LIVE.FORWARD_NOTIFICATION	QUEUE	444	444	444	0	0	0	1
☐	VTConsumer.Analytics.IA_IP.VirtualTopic.OCEANA_LIVE.DISPOSITION_CODE	QUEUE	555	555	555	0	0	0	1
☐	VTConsumer.Analytics.IA_IP.VirtualTopic.OCEANA_LIVE.EXTERNAL_CONVERSATION_INTERACTION	QUEUE	666	666	666	0	0	0	1
☐	VTConsumer.Analytics.IA_IP.VirtualTopic.OCEANA_LIVE.CONVERSATION_INTERACTION	QUEUE	444	444	444	0	0	0	1
☐	VTConsumer.Analytics.IA_IP.VirtualTopic.OCEANA_LIVE.WORK_REQUEST	QUEUE	555	555	555	0	0	0	1
☐	VTConsumer.Analytics.IA_IP.VirtualTopic.OCEANA_LIVE.CONTACT	QUEUE	666	666	666	0	0	0	1

Enabling mailboxes

About this task

Use this procedure to enable all mailboxes after the upgrade process is complete.

Procedure

1. Log on to Avaya Control Manager.
2. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana®** > **Omnichannel Administration**.
3. Click **Launch OC Database Administration Client**.

   Avaya Control Manager starts Omnichannel Administration Utility.
4. In the navigation pane, click **E-mail** > **Recipient Addresses**.
5. Click **Enable All**.

   Important:

   After Avaya Oceana® system restart, to preserve the order of the emails, you must wait until the existing emails are re-queued before re-enable polling. For contact centres with 25000 emails in queue, Avaya recommends to wait approximately 25 minutes after all the clusters have been set to an **Accepting** state after the restart.

Configuring Avaya Oceana® to accept contacts

About this task

Use this procedure to configure Avaya Oceana® so that it starts accepting SMS, Social, Chat, and Generic conversations.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Attributes Configuration page, click the **Service Clusters** tab.
3. In the **Cluster** field, select Avaya Oceana® Cluster 3.
4. In the **Service** field, select **MessagingService**.
5. For **Shutdown Mode**, select the **Override Default** check box and select `false` in the **Effective Value** field.
6. Click **Commit**.
7. In the **Service** field, select **CustomerControllerService**.
8. For **Shutdown Mode**, select the **Override Default** check box and select `false` in the **Effective Value** field.
9. Click **Commit**.
10. In the **Service** field, select **GenericChannelAPI**.
11. For **Shutdown Mode**, select the **Override Default** check box and select `false` in the **Effective Value** field.
12. Click **Commit**.

Configuring Avaya Oceana® to open chatrooms

About this task

Use this procedure to configure Avaya Oceana® so that it opens all chatrooms.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Attributes Configuration page, click the **Service Clusters** tab.
3. In the **Cluster** field, select Avaya Oceana® Cluster 3.
4. In the **Service** field, select **CustomerControllerService**.
5. For **Close all Chatrooms**, select the **Override Default** check box and select `false` in the **Effective Value** field.
6. Click **Commit**.

Enabling Avaya Oceana® for voice calls

About this task

Use this procedure to enable Avaya Oceana® for voice calls so that all voice calls route to Avaya Oceana®.

Procedure

From any CM station in Avaya Oceana®, dial the following number:

`<FAC Out of Service Number>1`

For example, if you configured *59 as the FAC out of service number, then you must dial *591 to enable Avaya Oceana® for voice calls.

Migration of Engagement Designer workflows

Engagement Designer workflows in Avaya Oceana® contain the following:

- Core logic for the contact center to operate properly
- Customizable branches and tasks for customers to tailor Avaya Oceana® to their needs

With the new release of Avaya Oceana®, the installation of new core logic is important to take the advantage of performance improvements, new features and capabilities, and bug fixes. Therefore, when you upgrade Avaya Oceana®, you must install the latest out-of-the-box workflows and verify the basic functionality of Avaya Oceana®.

After you verify that Avaya Oceana® is working as expected, you can migrate the customizations of the earlier workflows to the latest workflows.

Important:

Migration of workflow is needed only if you want the new core logic of the latest workflow and customizations of the earlier workflows.

Engagement Designer Diff Tool

Engagement Designer Designer Console provides Diff Tool. With this tool, you can compare two Engagement Designer workflows and identify the differences between them.

When you install the latest out-of-the-box workflows as part of Avaya Oceana® upgrade, the workflows only contain the new core logic but do not contain the customizations that you made in the earlier workflows.

To migrate the customizations to the latest workflows, you must first compare the out-of-the-box and customized versions of the earlier workflows by using Engagement Designer Diff Tool. From the output of the tool, you can identify the customizations and migrate them to the latest workflows.

Migrating a customized workflow

About this task

When you install the latest out-of-the-box workflow as part of Avaya Oceana® upgrade, the workflow does not contain the customizations of the earlier workflow. With this procedure, you can migrate the customizations of the earlier workflow to the latest workflow.

Before you begin

- Download the earlier out-of-the-box workflow from PLDS and save it to a server or local machine.
- Save the earlier customized workflow to a server or local machine.

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. In the top right corner, click the **Settings** icon and then click **Diff Tool**.

   Engagement Designer displays the Diff Tool page.

3. To open the earlier out-of-the-box workflow, do the following:

   a. Click the left arrow icon.

   b. Click **Open from server** or **Choose file** based on the location where you saved the earlier out-of-the-box workflow.

   c. Browse and select the workflow.

   d. Click **Open**.

      The tool displays the workflow in the left.

4. To open the earlier customized workflow, do the following:

   a. Click the right arrow icon.

   b. Click **Open from server** or **Choose file** based on the location where you saved the earlier customized workflow.

   c. Browse and select the workflow.

   d. Click **Open**.

      The tool displays the workflow in the right.

5. Click **Show Diff**.

The tool displays the List Changes tab highlighting the following types of changes:

- **Modified**: Specifies that the node is available in both workflows with some modification in properties.
- **New Task**: Specifies that the task is available in one workflow but is missing from the other workflow.

6. On the List Changes tab, click the link of the change to view the respective node or task in the workflows.

   The annotation tool displays the differences and traces them on the workflow.
7. Select and copy the nodes and connections to be moved to the latest out-of-the-box workflow.
8. Open the latest out-of-the-box workflow in Engagement Designer Designer Console.
9. Paste the copied nodes and connections to the latest out-of-the-box workflow.
10. Save the workflow.

    Note:

    If you already know the customizations of the earlier workflow, you can open the earlier customized workflow in Engagement Designer Designer Console, select and copy the differences, and paste them to the latest out-of-the-box workflow.

Comparing workflows

About this task

With Engagement Designer Diff Tool, you can view the changes made in the nodes of a workflow.

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. In the top right corner, click the **Settings** icon and then click **Diff Tool**.

   Engagement Designer displays the Diff Tool page.
3. To open the earlier version of the workflow, do the following:
   a. Click the left arrow icon.
   b. Click **Open from server** or **Choose file** based on the location where you saved the workflow.
   c. Browse and select the workflow.
   d. Click **Open**.

      The tool displays the workflow in the left.

4. To open the newer version of the workflow, do the following:
    1. Click the right arrow icon.
    2. Click **Open from server** or **Choose file** based on the location where you saved the workflow.
    3. Browse and select the workflow.
    4. Click **Open**.

       The tool displays the workflow in the right.
5. Click **Show Diff**.

   The tool displays the List Changes tab highlighting the following types of changes:

   - **Modified**: Specifies that the node is available in both workflows with changes in properties.

     You can view the differences between the nodes in the workflow. The Ⓜ, Ⓟ, and Ⓛ icons indicate the changes made to the Input or Output Mapping, Properties, and Label attributes respectively. The **Changes** column displays the corresponding icon next to the **Modified** button.
   - **New Task**: Specifies that the task is available in one workflow but is missing from the other workflow.

   The **Type** column displays the gold stamp Ⓐ and gold stamp broken icons if there are changes in the nodes of gold stamped workflows. The gold stamp broken icon indicates changes made to the standard workflow.
6. To view the differences between the nodes in the workflow, do the following:
    1. Click **Modified**.
    2. In the Task properties difference dialog box, expand the **Properties**, **Input Mapping**, **Output Mapping**, and **Boundary attachment** sections to view the differences highlighted in red.
    3. To view the differences in the functions in data mappings, move the cursor to the fx icon.
    4. To view the differences in the templates in data mappings, move the cursor to the ts icon.

Configuring AgentControllerService to have authenticated access to UnifiedAgentController

About this task

Starting from Avaya Oceana® Release 3.8.0.0 UnifiedAgentController requires all the requests to its internal endpoints to be authenticated using AuthorizationService token. Use this procedure to configure AgentControllerService to access UnifiedAgentController.

You can also configure AgentControllerService using the OceanaConfiguration service. For more information, see *Deploying Avaya Oceana®*.

Note:

This procedure is mandatory for Avaya Oceana® to handle contacts properly.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
    a. In 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**.

Chapter 8: Upgrading WebRTC components

WebRTC components upgrade overview

This chapter provides information about the tasks that you must perform to upgrade WebRTC components if your solution has WebRTC agents or accepts incoming WebRTC calls from remote clients applications.

This chapter describes the upgrade process of WebRTC components when you upgrade from Avaya Oceana® 3.5.x to 3.8.1.

Preupgrade tasks for WebRTC components

Before upgrading WebRTC components as part of Avaya Oceana® upgrade from 3.5.x to 3.8.1:

- Verify that the Oceana Elite Voice solution is upgraded and is routing voice calls to Avaya Workspaces agents.

WebRTC components upgrade checklists

Use the following checklist to upgrade WebRTC components as part of Avaya Oceana® upgrade from 3.5.x to 3.8.1:

No.	Task	Notes	✔
1	Upgrade or install Avaya Aura® Web Gateway.	• If Avaya Aura® Web Gateway is already installed, then upgrade to Avaya Aura® Web Gateway 3.9. For upgrade instructions, see *Administering the Avaya Aura® Web Gateway*. • If Avaya Aura® Web Gateway is not installed, then install Avaya Aura® Web Gateway 3.9. For installation instructions, see *Deploying Avaya Oceana®*.	
2	Upgrade or install Avaya Aura® Device Services.	• If Avaya Aura® Device Services is already installed, then upgrade to Avaya Aura® Device Services 8.1.3. For upgrade instructions, see *Deploying Avaya Aura® Device Services*. • If Avaya Aura® Device Services is not installed, then install Avaya Aura® Device Services 8.1.3. For installation instructions, see *Deploying Avaya Oceana®*.	
3	Upgrade or install Avaya Aura® Media Server for Web Voice/Video.	• If Avaya Aura® Web Gateway-controlled Avaya Aura® Media Server is already installed, then upgrade to Avaya Aura® Media Server 8.0.2. For upgrade instructions, see *Deploying and Updating Avaya Aura® Media Server Appliance*. • If Avaya Aura® Web Gateway-controlled Avaya Aura® Media Server is not installed, then install Avaya Aura® Media Server 8.0.2. For installation instructions, see *Deploying Avaya Oceana®*.	

Table continues…

No.	Task	Notes	✔
4	Upgrade or install Avaya Aura® Media Server for Avaya Breeze® platform.	• If Avaya Breeze® platform-controlled Avaya Aura® Media Server is already installed, then upgrade to Avaya Aura® Media Server 8.0.2. For upgrade instructions, see *Deploying and Updating Avaya Aura® Media Server Appliance*. • If Avaya Breeze® platform-controlled Avaya Aura® Media Server is not installed, then install Avaya Aura® Media Server 8.0.2. For installation instructions, see *Deploying Avaya Oceana®*.	
5	Upgrade Avaya Aura® Session Border Controller.	For instructions about how to upgrade to Avaya Aura® Session Border Controller 8.1.1, see *Upgrading Avaya Session Border Controller for Enterprise*.	
6	Rebuild customer web and mobile applications.	After upgrading WebRTC components, you must rebuild customer web and mobile applications. For more information, see *Avaya Oceana™ Web Voice and Video Software Development Guide*.	

Chapter 9: Upgrading the Disaster Recovery solution

Disaster Recovery solution upgrade overview

A Disaster Recovery deployment of Avaya Oceana® involves two deployments at two geographically separated data centers, Data Center 1 (DC1) and Data Center 2 (DC2). On each data center, you install Avaya Oceana® and Avaya Analytics™ components with replication of data between a number of elements from DC1 to DC2.

During migration of a Disaster Recovery solution to the latest release, you must consider the hours of operation of the contact center when choosing the appropriate software migration strategy. Each Avaya Oceana® deployment allows downtime during migration. All Avaya Oceana® software migrations require downtime when the system is out of service. Alternate fallback options are available as standard for PSTN voice channels. However, no alternate fallback mechanism is available for digital and WebRTC channels within Avaya Oceana®.

The following table summarizes the supported software migration strategies for migration of Avaya Oceana® from earlier releases to Release 3.8.1:

Option	Migration strategy	Maintenance window	Description	Impact to contact center operations
Option A	Simultaneous migration of primary and Disaster Recovery sites	Maintenance window 1	Migrate primary and Disaster Recovery sites in a single maintenance window.	Avaya Oceana® contact center is unavailable during the maintenance window.

Table continues…

Option	Migration strategy	Maintenance window	Description	Impact to contact center operations
Option B	Two-step migration of primary and Disaster Recovery sites	Maintenance window 1	Migrate primary Avaya Oceana® and Avaya Analytics™, and backup Avaya Analytics™ in a single maintenance window 1, place the upgraded primary site back in production, and then proceed to migrate the Disaster Recovery site.	Avaya Oceana® contact center is unavailable during the maintenance windows.
		Maintenance window 2	1. Migrate Avaya Oceana® including Omnichannel Database in the Disaster Recovery site. 2. Re-enable Disaster Recovery capabilities in the maintenance window 2.	

The maintenance window in Option B is shorter than the single maintenance window of Option A, because it is a two-step software migration process.

The migration steps in Option A and Option B are same for each application in the solution that requires the software update. For software migration, you can choose Option A or Option B but not both.

In both strategies, you must migrate Avaya Aura® System Manager to the latest software version required for Avaya Oceana® Release 3.8.1 and Avaya Breeze® platform Release 3.8.

Before the actual Avaya Oceana® and Avaya Analytics™ disaster recovery migration, do the following in a separate maintenance window:

- Migrate to System Manager 8.1
- Apply latest System Manager patch and hotfix

Simultaneous migration of primary and Disaster Recovery sites

Option A migrates the complete Avaya Oceana® including primary and Disaster Recovery (DR) sites to the latest Avaya Oceana® 3.8.1 software in a single maintenance window.

Ensure that you complete the following pre-upgrade procedures and tasks:

- Migrate Avaya Aura® System Manager to the latest software release.
- Migrate Avaya Aura® applications, such as Control Manager, AES, Avaya Experience Portal, and Avaya Aura® System Manager, to a minimum release compatible with Avaya Oceana® 3.8.1.
- Download the Avaya Oceana® 3.8.1 software from PLDS.
- Download the Avaya Control Manager 9.x software from PLDS.

The following table lists the tasks to migrate Avaya Oceana® from 3.5.x, 3.6.x, 3.7.x, or 3.8 to 3.8.1:

Note:

This table lists the tasks in a sequential order assuming that one person is performing the migration.

Table 1: Primary and DR sites migration

Task	Description	Reference	Expected outcome
Validation of System Manager geo-replication	Validate that the System Manager geo-replication is operational.	See *Avaya Oceana® and Avaya Analytics™ Disaster Recovery*.	System Manager geo-replication is completely functional.

Table continues…

Task	**Description**	**Reference**	**Expected outcome**
Graceful shutdown of active channels in primary and DR sites	Graceful shutdown of all voice and digital channels deployed on the primary site. The system must be operating using the primary and not the DR site. Ensure that no active or queueing contacts are left on the system. Avaya Oceana® is in the Deny state across both sites.	See *Avaya Oceana® and Avaya Analytics™ Disaster Recovery*.	Avaya Oceana® is in the shutdown mode.
Power down	Power down the following applications across both sites: • All Avaya Breeze® platform nodes in clusters. • Avaya Control Manager servers. • Omnichannel Database servers. • Avaya Analytics™ servers including the database server.	You must power off these applications before taking snapshots.	Avaya Oceana® and Avaya Analytics™ are powered off.

Table continues…

Task	Description	Reference	Expected outcome
Snapshots	Take snapshots of the following applications while they are powered off because this is the only recovery mechanism: • All Avaya Breeze® platform nodes in clusters. • Avaya Control Manager servers. • Omnichannel Database servers. • Avaya Analytics™ servers.	Snapshots are mandatory for recovery in event of catastrophic failures during migration.	Suite of snapshots is taken.
Power on	Power on the following applications to perform the software migration and wait for the system to come back online. However, ensure that you do not enable Avaya Oceana® in production. • All Avaya Breeze® platform nodes in clusters. • Avaya Control Manager servers. • Omnichannel Database servers. • Avaya Analytics™ servers including the database server.	-	Avaya Oceana® and Avaya Analytics™ are powered on but not enabled to process any contacts.

Table continues…

Task	Description	Reference	Expected outcome
Start Avaya Oceana® migration for the primary site	Summary of high-level steps: • Copy the `Oceana<Release_number>.zip` file to the primary System Manager. • Run the **`upgradeSolution`** command on primary cluster group 1 to upgrade the primary Avaya Oceana®. • Verify successful Avaya Oceana® migration. • Undeploy the current Avaya Engagement Designer tasks and flows. • Migrate to latest tasks and Avaya Engagement Designer flows.	See Upgrading Avaya Breeze platform on page 36.	The Avaya Oceana® primary site is migrated to Avaya Oceana® 3.8.1.

Table continues…

Task	Description	Reference	Expected outcome
Start Avaya Oceana® migration for the DR site	Summary of high-level steps: • Run the **`upgradeSolution`** command on the primary cluster group 2 to upgrade the DR Avaya Oceana®. • Verify successful Avaya Oceana® migration. • Undeploy the current Avaya Engagement Designer tasks and flows. • Migrate to latest tasks and Avaya Engagement Designer flows.	See Upgrading Avaya Breeze platform on page 36.	The Avaya Oceana® DR site is migrated to Avaya Oceana® 3.8.1.
Start Avaya Control Manager and database migration for primary and DR sites	Migrate the primary and DR Avaya Control Manager servers to the latest release required for Avaya Oceana® 3.8.1.	See the Avaya Control Manager upgrade documentation.	The Avaya Control Manager primary and DR sites are migrated to Avaya Oceana® 3.8.1.

Table continues…

Task	Description	Reference	Expected outcome
Start Omnichannel Database migration for primary and DR sites **Note:** This procedure is not required if you are upgrading from Avaya Oceana® release 3.7 or later versions. In this case you just need to run an upgrade as Windows 2016 server is already deployed.	You must perform the following steps to remove Omnichannel Database mirroring prior to software migration: • Remove database mirroring to return servers to standalone role. • Create backups of primary and DR databases. • Deploy the new operating system Windows 2016 Server required for Avaya Oceana® 3.8.1 and apply appropriate Microsoft hotfixes. • Install the latest Omnichannel software on primary and DR servers. • Restore the database backup to the primary server. • Enable Database mirroring again from the primary server to DR server.	See *Avaya Oceana® and Avaya Analytics™ Disaster Recovery*.	Omnichannel Database primary and DR sites are migrated to Avaya Oceana® 3.8.1.

Table continues…

Task	Description	Reference	Expected outcome
Update Avaya Oceana® custom applications and interfaces	The following items are migrated to the latest release with each Avaya Oceana® update. • Self-Service sample application. • Customer front-end sample chat application. • All custom widgets deployed to Avaya Oceana® users.	-	
Commission and instate the newly upgraded solution	Do the following: • Set the primary Avaya Oceana® in the Active mode. • Set the DR Avaya Oceana® in the Deny or Standby mode. • Validate that the replication is operational from the primary to DR site for UCA, Context Store, Omnichannel Database, Avaya Control Manager, and System Manager. • Validate Avaya Oceana® user login and operation of all deployed voice and/or digital channels. • Validate reporting. • Set the primary Avaya Oceana®.	See *Avaya Oceana® and Avaya Analytics™ Disaster Recovery*.	Avaya Oceana® 3.8.1 and Avaya Analytics™ 4.1.1 are completely upgraded, and the solution is back in production.

Two-step migration of primary and Disaster Recovery sites

Option B migrates the complete Avaya Oceana® in two separate maintenance windows. Between the maintenance windows, the primary site is placed back into production with Disaster Recovery (DR) capabilities while the Avaya Oceana® in the DR site is upgraded. After the DR Avaya Oceana® is migrated completely to the latest release, a second maintenance window is required to enable replication and DR functionality from the primary to the DR site.

Avaya recommends that you upgrade the DR site immediately after the primary is re-established in production.

Ensure that you complete the following pre-upgrade procedures and tasks:

- Migrate Avaya Aura® System Manager to the latest software release.
- Migrate Avaya Aura® applications, such as Control Manager, AES, Avaya Experience Portal, and Avaya Aura® System Manager, to a minimum release compatible with Avaya Oceana® 3.8.1.
- Download the Avaya Oceana® 3.8.1 software from PLDS.
- Download the Avaya Control Manager 9.x software from PLDS.

The following tables list the tasks to migrate Avaya Oceana® from 3.5.x, 3.6.x, 3.7.x, or 3.8 to 3.8.1:

Note:

This tables list the tasks in a sequential order assuming that one person is performing the migration.

Table 2: Primary migration

Task	Description	Reference	Expected outcome
Validation of System Manager geo-replication	Validate that the System Manager geo-replication is operational.	See *Avaya Oceana® and Avaya Analytics™ Disaster Recovery*.	System Manager geo-replication is completely functional.
Maintenance window 1 begins			

Table continues…

Task	Description	Reference	Expected outcome
Graceful shutdown of active channels in the primary site	Graceful shutdown of all voice and digital channels deployed on the primary site. The system must be operating using the primary and not the DR site. Ensure that no active or queueing contacts are left on the system. Avaya Oceana® is in the Deny state across both sites.	See *Avaya Oceana® and Avaya Analytics™ Disaster Recovery*.	Avaya Oceana® is in the shutdown mode.
Power down	Power down the following applications in the primary site: • All Avaya Breeze® platform nodes in clusters. • Avaya Control Manager servers. • Omnichannel Database servers. • Avaya Analytics™ servers including the database server.	You must power off these applications before taking snapshots.	Avaya Oceana® and Avaya Analytics™ are powered off.
Snapshots	Take snapshots of the following applications while they are powered off because this is the only recovery mechanism. • All Avaya Breeze® platform nodes in clusters. • Avaya Control Manager servers. • Omnichannel database servers. • Avaya Analytics™ servers.	Snapshots are mandatory for recovery in event of catastrophic failures during migration.	Suite of snapshots taken.

Table continues…

Task	Description	Reference	Expected outcome
Power on	Power on the following applications to perform the software migration and wait for the system to come back online. However, ensure that you do not enable Avaya Oceana® to process any contacts. - All Avaya Breeze® platform nodes in clusters. - Avaya Control Manager servers. - Omnichannel Database servers. - Avaya Analytics™ servers including the database server.	-	Avaya Oceana® and Avaya Analytics™ are powered on but not enabled to process any contacts.
Start Avaya Oceana® migration for the primary site.	Summary of high-level steps: - Copy the `Oceana<Release_number>.zip` file to the primary System Manager. - Run the **`upgradeSolution`** command on the primary cluster group 1 to upgrade the primary Avaya Oceana® only. - Verify successful Avaya Oceana® migration. - Undeploy the current Avaya Engagement Designer tasks and flows. - Migrate to latest tasks and Avaya Engagement Designer flows.	See Upgrading Avaya Breeze platform on page 36.	The Avaya Oceana® primary site is migrated to Avaya Oceana® 3.8.1.

Table continues…

Task	Description	Reference	Expected outcome
Start Avaya Control Manager and database migration for primary and DR sites.	Migrate the primary and DR Avaya Control Manager servers to the latest release required for Avaya Oceana® 3.8.1.	See the Avaya Control Manager upgrade documentation.	The Avaya Control Manager primary and DR sites are migrated to Avaya Oceana® 3.8.1.
Start Omnichannel Database migration for the primary site only. ✱ **Note:** This procedure is not required if you are upgrading from Avaya Oceana® release 3.7 or later versions. In this case you just need to run an upgrade as Windows 2016 server is already deployed.	You must perform the following steps to remove Omnichannel Database mirroring prior to software migration: • Remove database mirroring to return primary and DR servers to standalone role. • Create backup of the primary databases. • Deploy the new operating system Windows 2016 Server required for Avaya Oceana® 3.8.1 and apply appropriate Microsoft hotfixes. • Install the latest Omnichannel software on the primary server. • Restore the database backup to primary.	See *Avaya Oceana® and Avaya Analytics™ Disaster Recovery*.	Omnichannel database primary and DR is migrated to Avaya Oceana® 3.8.1.
Update Avaya Oceana® custom applications and interfaces.	The following items are migrated to the latest release with each Avaya Oceana® update. • Self-Service sample application. • Customer front-end sample chat application. • All custom widgets deployed to Avaya Oceana® users.	-	-

Table continues…

Task	Description	Reference	Expected outcome
Commission and Instate the newly upgraded primary.	Do the following: • Set the primary Avaya Oceana® in the Active mode. • Set the DR Avaya Oceana® in the Deny or Standby mode. • Validate that the replication is operational from the primary to DR site for UCA, Context Store, Omnichannel Database, Avaya Control Manager, and System Manager. • Validate Avaya Oceana® user login and operation of all deployed voice and/or digital channels. • Validate reporting. • Set the primary Avaya Oceana®.	See *Avaya Oceana® and Avaya Analytics™ Disaster Recovery* for instructions about how to enable the Avaya Oceana® DR solution with data mirroring.	Avaya Oceana® and Avaya Analytics™ 3.8.1 solution are completely upgraded, and the solution is back in production.
Enable the primary Avaya Oceana® to process contacts.	Enable primary Avaya Oceana® and Avaya Analytics™ to process and report on contacts. Avaya Analytics™ replication from the primary to DR is enabled. System Manager and Avaya Control Manager database replication from the primary to DR is enabled.	-	-
Maintenance window 1 ends			

Table 3: DR Migration

Functional Area	Summary of Tasks	Where to find the detailed step by step procedures	Expected Outcomes
Validation of System Manager geo-replication	Validate that the System Manager geo-replication is operational.	See *Avaya Oceana® and Avaya Analytics™ Disaster Recovery*.	System Manager geo-replication is completely functional.
Power down	Power down all Avaya Breeze® platform nodes in the clusters in the DR site. It is essential to power off before taking snapshots.	-	Avaya Oceana® is in the shutdown mode.
Snapshots	Take a snapshot of all Avaya Breeze® platform nodes while they are powered off because this is the only recovery mechanism.	Snapshots are mandatory for recovery in event of catastrophic failures during migration.	Suite of snapshots is taken.
Power on	Power on all Avaya Breeze® platform nodes in the clusters in the DR site to perform the software migration and wait for the system to come back online. However, ensure that you do not enable Avaya Oceana® to process any contacts.	-	Avaya Oceana® DR is powered on.

Table continues…

Functional Area	Summary of Tasks	Where to find the detailed step by step procedures	Expected Outcomes
Start Avaya Oceana® software migration for the DR site.	Summary of high-level steps: • Run **`upgradeSolution`** command on the primary cluster Group 2 which upgrades the primary Avaya Oceana® system. • Verify successful Avaya Oceana® migration. • Undeploy the current Avaya Engagement Designer tasks and flows. • Migrate to latest tasks and Avaya Engagement Designer flows.	See Upgrading Avaya Breeze platform on page 36.	The Avaya Oceana® DR site is migrated to Avaya Oceana® 3.8.1.
Start Omnichannel database migration for the DR site. **Note:** This procedure is not required if you are upgrading from Avaya Oceana® release 3.7 or later versions. In this case you just need to run an upgrade as Windows 2016 server is already deployed.	Do the following: • Deploy the new operating system Windows 2016 Server required for Avaya Oceana® 3.8.1 and apply appropriate Microsoft hotfixes. • Install the latest Omnichannel software on the DR server. • Validate that the Omnichannel DR server software is fully installed and ready for mirroring setup from primary.	-	Omnichannel Database DR is migrated to Avaya Oceana® 3.8.1.

Table continues…

Functional Area	Summary of Tasks	Where to find the detailed step by step procedures	Expected Outcomes
Update Avaya Oceana® custom applications and interfaces for the DR site if you are using a different set than the primary site.	The following items are migrated to the latest release with each Avaya Oceana® update. • Self-Service sample application. • Customer front-end sample chat application. • All custom widgets deployed to Avaya Oceana® users.	-	-
Maintenance window 2 begins			
Commission and reinstate the DR functionality.	Do the following: • Enable UCA and CS replication from the primary to DR. • Enable Omnichannel database mirroring from the primary to DR site. It involves database backup from the primary to DR site. • Reboot Avaya Oceana® primary clusters. • Validate that the replication is operational from the primary to DR site for UCA, Context Store, Omnichannel Database, Avaya Control Manager, and System Manager.	See *Avaya Oceana® and Avaya Analytics™ Disaster Recovery* for instructions about how to enable the Avaya Oceana® DR solution with data mirroring.	Avaya Oceana® 3.8.1 and Avaya Analytics™ 4.1.1 are completely upgraded, and the solution is back in production.

Table continues…

Functional Area	Summary of Tasks	Where to find the detailed step by step procedures	Expected Outcomes
Enable the primary Avaya Oceana® in production and keep the DR Avaya Oceana® in standby.	Primary Avaya Oceana® and Avaya Analytics™ are back in production with DR functionality. UCA and CS replication is re-established.	-	-
Maintenance window 2 ends			

Checklist for upgrading Omnichannel Database

Use the following checklist to upgrade the mirrored Omnichannel Database.

No.	Task	Description	✔
1	Remove Cache Mirroring from all Omnichannel Database servers.	See the following: • Removing Cache Mirroring from the backup Omnichannel server on page 73 • Removing Cache Mirroring from the active Omnichannel server on page 74	
2	Take a backup of the primary Omnichannel Database server on Data Center 1, and store the backup file at a preferred location.	See *Deploying Avaya Oceana®*.	
3	Uninstall the Omnichannel Server software.	-	
4	Install the Omnichannel Server software.	See *Deploying Avaya Oceana®*.	
5	Restore the backup on the primary Omnichannel Database server.	See *Deploying Avaya Oceana®*.	

Table continues…

No.	Task	Description	✔
6	Configure Cache Mirroring on the primary Omnichannel Database server.	See *Avaya Oceana® and Avaya Analytics™ Disaster Recovery*.	
7	Take a backup of the mirrored primary Omnichannel Database server.	See *Deploying Avaya Oceana®*.	
8	Configure Cache Mirroring on the standby and backup Omnichannel Database servers.	See *Avaya Oceana® and Avaya Analytics™ Disaster Recovery*	
9	Restore the mirrored backup on the standby and backup Omnichannel Database servers.	See *Deploying Avaya Oceana®*.	

Chapter 10: Migrating to Microsoft SQL Server

Microsoft SQL server migration overview

Avaya Oceana® no longer supports Oracle as the database for External Data Mart (EDM). If you are currently using Oracle, you must migrate to Microsoft SQL (MS SQL) server.

From Release 3.8 onwards, Avaya Oceana® also supports EDM co-resident with Avaya Control Manager on MS SQL server for both existing and new users.

For existing users, Avaya Oceana® continues to support PostgreSQL and MS SQL server as standalone databases.

For new Avaya Oceana® deployments, Avaya Context Store Snap-in supports only MS SQL server as the EDM.

The migration from Oracle or PostgreSQL to MS SQL server is a five-step process:

1. Creating new schema
2. Migrating data from old database
3. Migrating to new resurrect schema
4. Migrating to a new journey schema
5. Removing old schema data

Note:

The migration process is incremental, and you can resume from where you stop the process. You can re-run any of these steps to migrate data that is modified or added after you run the last migration step.

Creating new schema

This step involves creating the database schema for Context Store on the target MS SQL server.

Migrating data from old database

This step involves copying the old audit trail data from the existing database server to the new MS SQL server database. You can skip this step if the data in the old schema is already on the MS SQL server.

Migrating to new resurrect schema

This step involves parsing the audit trail data and loading Avaya Oceana® routing context data into the new schema for Context Store resurrection. It migrates all data for the currently open work requests.

You can also migrate data for work requests that are closed recently if these are required for external software, such as Callback Assist and Survey Assist. By default, this migration step migrates contacts that are closed for 30 days or less. You can set the time limit to any number of days of your choice.

Migrating to a new journey schema

This step involves parsing the audit trail data and loading the Customer Journey data into the new schema for Customer Journey.

Customer Journey also stores routing information, which was used to route an interaction through the contact center. To speed up the migration process, you can choose to skip this information. However, the information will then not be available for old contacts in Customer Journey.

Removing old schema data

After you complete the migration, you can remove the old audit trail data from the MS SQL server database. This data is not required after Avaya Oceana® starts using the new Customer Journey schema.

⚠ **Warning:**

This step cannot be undone, and the data gets permanently deleted.

Use the procedures in this chapter to migrate from an Oracle or a PostgreSQL server to MS SQL server.

Pre-migration checklist

Use the following checklist for the tasks that you must complete before migrating to Microsoft SQL Server for External Data Mart (EDM):

No.	Task	Notes	✔
1	Take a backup of the database.	The backup steps are different for different databases.	
2	Clean the data.	This step speeds up the migration process. **Note:** This step is optional.	

Table continues…

No.	Task	Notes	✔
3	Remote desktop to the Windows server running the MS SQL server.		
4	Create a new Microsoft SQL Server database using Microsoft SQL Server Management Studio.	See, *Creating a new database* in this chapter.	
5	Copy and extract the script and its configuration file to a new folder on the server running the MS SQL Server.	See *Downloading the migration script* in this chapter.	
6	Edit the `config.properties` file in a text editor.	See *Editing the configuration file for the migration* in this chapter. **Note:** This procedure describes a worked example using Notepad. You can use any text editor.	

Creating a new database

About this task

You must create a new database by using Microsoft SQL Server Management Studio. You must also set the appropriate collation type for the desired language while creating the database, such as Cyrillic for Russian.

Important:

If you select a collation type that does not support the Unicode characters for the desired language, then Context Store EDM does not store those Unicode characters. For example, if you want to store Russian characters, and set the Collation Type to Cyrillic_General_CI_AI, then it stores only the ASCII and Cyrillic characters, and not other Unicode characters, such as Arabic.

Before you begin

You must have:

- A Windows server with MS SQL server installed on it.
- A valid database administrator credential.

Procedure

1. Remote desktop to the Windows server running SQL Server.
2. Open Microsoft SQL Server Management Studio.
3. Connect to the database engine using your administrator credentials.
4. Expand the server node.
5. Right-click **Databases** and select **New Database**.
6. Enter a database name and click **OK**.

   The left navigation pane displays the new database.
7. To set the collation type, click **Options**.
8. In the **Collation** field, select the required collation type for the desired language.
9. Click **OK**.

Downloading the migration script

About this task

Use this procedure to download the migration script and extract the `config.properties` file.

Before you begin

Create a new database.

Procedure

1. Download the migration script from the Avaya Support website at https://support.avaya.com. The name of the archive that contains migration script is `ContextStoreDataMigrationScripts.zip`.
2. Extract the script and the `config.properties` configuration file to a new folder on your Windows server running the MS SQL server.

Next steps

Edit the `config.properties` configuration file for the migration.

Editing the configuration file for the migration

About this task

Use this procedure to edit the `config.properties` file extracted with the migration script. You can edit the file in a text editor to suit your migration requirements.

In this procedure, the source database refers to an Oracle or a PostgreSQL server and destination refers to the MS SQL server.

Note:

This procedure describes a worked example using Notepad. You can use any text editor.

Before you begin

Extract the script and its configuration file to a new folder on your Windows server.

Procedure

1. Open the Windows start menu and type `notepad` into the search bar.
2. Click the **Notepad** icon.
3. Click **File** > **Open** and navigate to the location of the configuration file.
4. Select the file from the list of files and click **Open**.

   The file you select opens in Notepad and is ready for you to edit.
5. Depending on your requirements, set the **sourceDbType** attribute to **oracle**, **postgres**, or **mssql**.
6. Enter the details in the following fields for the source database:
   - In the **sourceServer** field, enter the IP address of the source server.
   - In the **sourcePort** field, enter the port for Oracle, PostgreSQL, or MS SQL.
   - In the **sourceDatabase** field, enter the source server database name.
   - In the **sourceSchema** field, enter the source server database schema name.

     Enter the value for this field only for Oracle servers.
   - In the **sourceUser** field, enter the source server username.
7. Enter the details in the following fields for the destination database:
   - In the **sqlServer** field, enter the MS SQL server IP address.
   - In the **sqlPort** field, enter the MS SQL server port.
   - In the **sqlDatabase** field, enter the MS SQL server database name.
   - In the **sqlUser** field, enter the MS SQL server username.
8. **(Optional)** Enter the details in the following fields for both the source and destination databases
   - In the **sourcePassword** field, enter the password of the source server.
   - In the **sqlPassword** field, enter the password of the MS SQL server.

   Note:

   If you do not enter the details during pre-migration, then you must provide the passwords while running the migration script.

9. When you are ready to save the configuration file, click **File** > **Save**.

Creating a new schema

About this task

Complete the following steps to create a new schema:

Procedure

1. When the Windows PowerShell screen displays that the testing is done, press **Enter** for the **Create new schema** step.
    - If you enter incorrect details in the configuration properties file, then the test result displays errors. Fix the issue and start the migration process again.
    - The status of all the migration steps displays as `Not started` before you start this operation.
2. In the **would you like to continue with the schema creation** field enter `y`.

    Entering `n` takes you to the previous menu.

    The creation of the new schema is complete.
3. Press **Enter** after the completion of the migration step and wait for the migration to continue.

    The Windows PowerShell screen displays the next step for migration.

    The output is logged in the `logs` folder every time you run the script.

Next steps

Migrate data from the old database.

Migrating data from the old database

About this task

Use this procedure to migrate the Context Store data from version 3.7 to version 3.8

Important:

You can skip this procedure if the data in the old schema is already on the MS SQL server.

Depending on your configuration, use these steps to migrate from:

- Oracle to MS SQL server
- PostgreSQL to MS SQL server

- An MS SQL server to another MS SQL server

You can use the upward and downward arrow keys on your keyboard to move to the required migration step while running the migration process.

Before you begin

- Create a database.
- Create a new schema.

Procedure

1. On the Windows PowerShell screen, ensure that the **Create new schema** step displays `Completed`.
2. Select **Migrate data from old database**, then press **Enter**.

   This step starts running a database connection test and analyzes the data for the migration.
3. After the test is complete, in the **Would you like to continue with the database test** field, enter `y`.

   Entering `n` takes you back to the previous menu.

   The screen displays the details of the data, total space required, and the estimated time for the migration.
4. To continue, in the **Would you like to start the data migration now**, enter **y**.

   Entering `n` takes you to the main menu.

   Wait for the migration process to continue.
5. When the screen displays that the migration is complete, press **Enter** to continue to the next migration step.
6. **(Optional)** To interrupt the migration process, press `Ctrl+C`.

   To resume the migration, you can rerun the script.

   Note:

   Rollback is not required for resuming the migration.

Next steps

Migrate to new resurrect schema.

Migrating to a new resurrect schema

About this task

Use this procedure to migrate the data for open and recently closed contacts to the new resurrect schema. Details of recently closed contacts can be used by external software such as Callback Assist and Survey assist.

You can use the upward and downward arrow keys on your keyboard to move to the required migration step while running the migration process.

Before you begin

- Create a new schema.
- Migrate data from the old database to the MS SQL server.

Procedure

1. Ensure that the Windows PowerShell screen displays `Completed` for the following migrations steps:
    - Create a new schema
    - Migrate data from old database
2. Select **Migrate to new resurrect schema**, then press **Enter**.

    This step starts running a database connection test and analyzes the data for the migration.
3. After the test is complete, in the **Would you like to continue with the database test** field, enter `y`.

    Entering `n` takes you to the previous menu.

    The screen displays the details of the data, total space required, and the estimated time for the migration.
4. To migrate contacts data that is closed, in the **Would you like to migrate additional data** field, enter `y`.

    Entering `n` skips step 5 and goes directly to step 6.
5. To select the number of days for which you want to migrate closed contacts data, in the **How many days of closed contacts should be migrated** field, enter the required number.

    The default is 30 days, with no maximum limit for the number of days you can enter.

    The screen displays the details of the data to be migrated, the disk space required, and the estimated time for the migration.
6. To continue, in the **Would you like to start the data migration now**, enter `y`.

    Entering `n` takes you to the main menu.

    Wait for the migration process to continue.

7. Press `Enter` after each migration step is complete and wait for the migration to continue.

   ⚠ **Warning:**

   To avoid data loss, use the target database for Context Store only after the migration is complete.

   The output is logged in the `logs` folder every time you run the script.

8. **(Optional)** To interrupt the migration process, press `Ctrl+C`.

   To resume the migration, you can rerun the script.

   Note:

   Rollback is not required for resuming the migration.

Next steps

Migrate to a new journey schema.

Migrating to a new journey schema

About this task

Use this procedure to migrate the journey data to the new Customer Journey schema. You can also migrate routing information data in this migration step.

You can use to the upward and downward arrow keys on your keyboard to move to the required migration step while running the migration process.

Before you begin

- Create a new schema.
- Migrate data from the old database to the MS SQL server.
- Migrate to a new resurrect schema for contacts data.

Procedure

1. Ensure that the Windows PowerShell screen displays `Completed` for the following migrations steps:
   - Create a new schema
   - Migrate data from old database
   - Migrate to a new resurrect schema
2. Select **Migrate to new journey schema**, then press **Enter**.

   This step starts running a database connection test and analyzes the data for the migration.

3. After the test is complete, in the **Would you like to continue with the database test** field, enter `y`.

Entering `n` takes you back to the previous menu.

The screen displays the details of the data, total space required, and the estimated time for the migration.

4. To migrate routing information data, in the **Would you like to copy routing information** field, enter `y`.

   Entering `n` continues without copying routing information data.

   Note:

   Migrating the routing information data requires extra disk space and can slow down the migration process.

5. To continue, in the **Would you like to start the data migration now**, enter `y`.

   Entering `n` takes you back to the main menu.

   Wait for the migration process to continue.

6. Press `Enter` after each migration step is complete and wait for the migration to continue.

   Warning:

   To avoid data loss, use the target database for Context Store only after the migration is complete.

   - All the steps in the scripts display the status as `Completed`.
   - The output is logged in the `logs` folder every time you run the script.

7. **(Optional)** To interrupt the migration process, press `CtrlC`.

   To resume the migration, you can rerun the script.

   Note:

   Rollback is not required for resuming the migration.

Next steps

Remove or delete old schema data.

Removing old schema data

About this task

When the migration to the MS SQL server is complete, the script prompts you to delete the old schema data. Use this procedure to remove the old audit trail data from the MS SQL server database. This migration step is optional.

Note:

The original database, from which you are migrating the old Context Store data, is not affected by this step.

Warning:

This step cannot be undone, and the data gets permanently deleted.

Before you begin

- Create a new schema.
- Migrate data from the old database to the MS SQL server.
- Migrate to a new resurrect schema for contacts data.
- Migrate to a new journey schema.

Procedure

1. Ensure that the Windows PowerShell screen displays `Completed` for the following migrations steps:
    - Create a new schema
    - Migrate data from old database
    - Migrate to new resurrect schema
    - Migrate to new journey schema
2. Ensure that the required data is migrated to the new database.
3. Ensure if the Customer Journey feature is working with the new schema and the new customer journey processing unit (PU).
4. Select **Remove old schema data**, then press **Enter**.

    The screen displays the following messages:

    - `Analysing tables`
    - Database summary

      Ensure that all the steps display the status as `YES`.
5. To delete the data, in the **Would you like to start the deletion now?,** type `Y`.

    Typing `N` stops the operation.
6. Press `Enter` and wait for the deletion to continue.

    Warning:

    To avoid data loss, use the target database for Context Store only after the migration is complete.

    - All the steps in the scripts display the status as `Completed`.
    - The output is logged in the `logs` folder every time you run the script.

7. To exit from the migration process, press **Enter** for the **Exit** option.

Post migration tasks

Setting service attributes in System 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 **ProvisioningCluster**.
    b. In the **Service** field, select **OceanaConfiguration**.
3. Configure the following attributes of the External Data Mart configuration:
    - In the **EDM: Persistence type** field, change persistence type from **Audit** to **Journey**.
    - In the **EDM: Database type** field, enter `Microsoft SQL Server`.
    - In the **EDM: TLS version** field, enter the TL version for the connection to the EDM database.
    - In the **EDM: Database host** field, enter the host name of the EDM database.
    - In the **EDM: Database port** field, enter the port number of the EDM database.
    - In the **EDM: Database name** field, enter the name of the EDM database.
    - In the **EDM: Database username** field, enter the user name of the EDM database.
    - In the **EDM: Database password** field, enter the password of the EDM database.
4. Click **Commit**.

Shrinking the database

About this task

After you remove the data from the old schema, the Microsoft SQL (MS SQL) server does not make the free space available on the disk. The space remains allocated to MS SQL server so that the database can reuse the space later. To make the space available, you must shrink the database. This procedure is optional.

Procedure

1. On MS SQL Management Studio, navigate to the new database you create for the migration to the MS SQL server.

2. Right-click the database.
3. Click **Tasks** > **Shrink** > **Database**.
4. Click **OK**.

Chapter 11: Migrating from Avaya Analytics™ 3.7.0.2 to Avaya Analytics™ 4.1.1

Migration overview

In Avaya Analytics™, you can migrate data from:

- Avaya Analytics™ Release 3.7.0.2 to Avaya Analytics™ Release 4.1.1

Note:

For the migration, you must first upgrade from Avaya Analytics™ 3.x to Avaya Analytics™ Release 3.7.0.2.

During the migration process, the source Avaya Analytics™ system can continue to run and process events from Avaya Oceana® in the production mode with no data loss. However, all data collected during the process in the target Avaya Analytics™ system is discarded when the post-migration steps are complete.

See the following sections for the data migration process details:

Data Migration components

For data migration, you must upgrade the source Avaya Analytics™ system to Release 3.7.0.2, patch 2. The target Avaya Analytics™ must be Release 4.1.1. No patch is required for the target system.

- Data migration is built on scenarios running in Oracle Data Integrator (DI). These scenarios query data from the source database (DB), transform it if required, and then insert into the target DB.
- Source DB stores data to be migrated, data migration parameters, and migration progress or logs to enable the migration process to stop or resume at any time.
- The source system contains a set of scripts that enable configuration of the source system; start, stop, or reset of the migration, and monitoring of the progress.

The target database has a set of scripts for the pre-migration and post-migration configurations of the target system.

Data migration process

Data migration process consists of one or more iterations. The process is incremental, a new session starts where the previous one is complete. For example, if you stop the first session at

10%, the new session continues from where you stopped the previous one. However, incremental migration is not possible after you complete the post-migration steps on the target system. You can also enable the Extract, Transform, Load (ETL) process between sessions to load or migrate new production data.

Interval data migration algorithm

The migration of the interval data is done in increments. Data migration for each table is done from the oldest data to the recent. If it is the first migration session for a table, the algorithm uses the interval data migration start date parameter that you configure. Otherwise, the algorithm finds the next interval after the last migrated one, and starts migration from that interval.

Data migration algorithm for non-interval tables

The data migration algorithm for the non-interval table is similar to the one used for interval data migration. The key difference is that the non-interval data that is already migrated can be changed between migration sessions. For example, you can move an agent or a supervisor to a different group.

When you restart the migration, the migration algorithm takes up the data that has updates to the migrated items in the source database. Then, the process updates the data before continuing with the data that is to be migrated.

CDR data migration

The migration of the Call Record Detail (CDR) tables take place in the following order:

- OCEANA_DATAMART. FCT_CDR_CUSTOMER_ENGAGEMENT
- OCEANA_DATAMARTFCT_CDR_CUSTOMER_CONTACT
- OCEANA_DATAMART. FCT_CDR_AGENT_SEGMENT

All contacts and segments linked to migrated engagements are migrated.

Migration iteration or session

If you start a new migration session after a previous migration is stopped, complete, or failed, the migration process starts migrating all the tables again. The new process migrates data that is added or modified in the previous iteration, and then migrates data that is not migrated.

Data migration and retention

The data retention feature is applicable in the following two scenarios:

- Rolling up the Avaya Analytics™ Release 4.0.0.1 data during an upgrade to Avaya Analytics™ Release 4.1.1.0.

This chapter describes the procedures for data migration from preparing the Avaya Analytics™ solution to completing roll-up of legacy data.

Note:

- The data migration procedures in this chapter are same for the High Availability (HA), non-HA, and disaster recovery Avaya Analytics™ solutions.
- For troubleshooting Avaya Analytics™ migration issues, see the relevant section in the *Maintaining and Troubleshooting Avaya Analytics™ for Avaya Oceana®* document.

Supported migration paths

From	To	Considerations
Avaya Analytics™ Release 3.7.0.2 patch 2	Avaya Analytics™ Release 4.1.1.0	You can find patch related information on the Avaya Support site.

Migration scenarios

The migration process can consist of one or more migration sessions.

The possible sessions are:

- Single migration session: You can migrate all data in one session. After the migration is complete, you must set the Avaya Analytics™ Release 4.1.1 system in production mode.
- Planned multiple migration sessions: You can migrate the data in a phased manner. In the first session, you can migrate the data partially or fully. After more than a day, you can start the migration process to migrate data from the time of the first migration session to the current one. This data includes data that was not migrated earlier, is new, or was modified during that duration. You can repeat the sessions multiple times. During the duration of the two sessions, Avaya Analytics™ Release 3.7.0.2 remains in production mode.

  Warning:

  Change the Avaya Analytics™ Release 4.1.1 to production mode only after you migrate all the required data.

- Unplanned multiple migration sessions: You can resume a migration session if the process fails. Before resuming the session, you must resolve the issue that caused the migration failure. To troubleshoot migration-related errors, see the *Maintaining and Troubleshooting Avaya Analytics™ for Avaya Oceana®* document. When the migration is complete, you can set Avaya Analytics™ Release 4.1.1 to production mode. You can no longer use the Avaya Analytics™ Release 3.7.0.2 to collect data.

Migration limitations

Migration from Avaya Analytics™ Release 3.7.0.2 to Avaya Analytics™ Release 4.1.1 does not support the following:

- If CDR data is redacted in the source database by data privacy procedures, automatic or by request after migration, the redaction changes do not get reflected in the target database. Here, the migration procedure applies automatic redaction on the data in the Avaya Analytics™ Release 4.1.1 database according to the gdpr_enabled and gdpr_auto_redaction_timeout parameters that are configured in the Release 4.1.1 database.

- Migration of individual tables.
- Partial migration from any date of dimension, Agent Logon data, and GDPR audit logs.
- Migration of custom columns or tables. Only the default Avaya Analytics™ schema is migrated.

Pre-migration checklist

Use this checklist to prepare for the migration from Avaya Analytics™ Release 3.7.0.2 to Avaya Analytics™ Release 4.1.1.

No.	Task	Notes	✔
1	Take a backup of: • Avaya Analytics™ Release 3.7.0.2. • Avaya Analytics™ Release 4.1.1.		
2	Configure migration parameters.	You must configure the migration parameters before starting the first migration session. This step is not required for the subsequent migration sessions. See, Configuring migration parameters on page 136.	

Configuring migration parameters

About this task

Use this procedure after upgrading to Avaya Analytics™ Release 3.7.0.2 to configure the migration parameters before starting the first migration session. You do not need to perform these steps for the subsequent migration sessions.

Procedure

1. Open an SSH session to the Avaya Analytics™ Oracle Business Intelligence Enterprise Edition Plus (OBIEE) server as oracle user.
2. Navigate to the directory specified during the Oracle Data Integrator (ODI) installation.

   For example, `cd /home/oracle/DataMigration`
3. Update the `migration_parameters.conf` file. Use vi, vim, or other text editor to modify the following parameters:

Parameter	Description	Example or To Do
POSTGRES_DB_IP_ADDRESS	IP address of PostgreSQL DB.	Check the Avaya Analytics™ Release 4.1.1 configuration to get this IP address.
POSTGRES_DB_IP_PORT	The external PostgreSQL DB port that Kubernetes exposes. Running the pre-migration script on the Avaya Analytics™ Release 4.1.1 system opens this port.	Check the script output to get the port number. For more information, see *Preparing the target system for the migration* in this document.
STATUS_REFRESH_INTERVAL	Migration status or progress refresh interval in seconds. The `./status.sh` script uses this parameter.	Set this parameter to a higher value because a smaller value impacts the status querying time and can affect the DB or migration performance.
INTERVAL_DATA_MIGRATION_PERIOD_MONTHS	Specifies the number of full months for which interval the data is migrated. Use this parameter to calculate the interval data migration start date. The calculation ignores the current day, and rounds start date to the first day of a month. For example; If the day when migration starts is June 27, then INTERVAL_DATA_MIGRATION_PERIOD_MONTHS =3. The interval data migration start date is set to the 1st of March, which gives March+April+May = 3 full months. Plus, the current month that is always included in the migration. **Note:** The migration start date is calculated in UTC. In this example, the start date is March 1st 00:00:00 UTC.	Maximum value is 36 months. **Important:** You can set this parameter only once for a migration process. If it is changed after one or more migration sessions, the value is ignored. You can set to a new value only after resetting the migration progress and starting the migration from scratch.

Table continues…

Parameter	Description	Example or To Do
CDR_MIGRATION_PERIOD_MONTHS	Specifies the number of full months for which the Call Detail Record (CDR) data is migrated. It is used to calculate the CDR data migration start date. The calculation ignores the current day and rounds start date to the first day of a month. For example; If the day when migration starts is June 27, then CDR_MIGRATION_PERIOD_MONTHS =3. The interval data migration start date is set to the 1st of March, which gives March+April+May = 3 full months. Plus the current month that is always included in the migration. **Note:** The migration start date is calculated in UTC. In this example, the start date is March 1st 00:00:00 UTC.	Maximum value is 12 months. **Important:** You can set this parameter only once for a migration process. If it is changed after one or more migration sessions, the value is ignored. You can set to a new value after resetting the migration progress and starting the migration from scratch.
MIGRATE_ZERO_ROWS	Applied in interval data migration.	When this parameter is set to false, the migration does not include rows with values of all measures columns equal to 0. The default value is false.
Other parameters	The remaining parameters are set by the Oracle Data Integrator installer.	Do not modify these parameters.

Preparing for the migration

Preparing the target system for the migration

About this task

Use this procedure to migrate to Avaya Analytics™ Release 4.1.1. You must use these steps only if you are migrating from scratch. You can use these steps once, regardless of the number of migration sessions you have planned.

Note:

- Take a back up of Avaya Analytics™ Release 4.1.1 to revert or roll back to the previous state if you want at a later stage.
- Do not restore backups taken before the migration on Avaya Analytics™ Release 4.1.1 system after the migration is complete.
- These steps delete all data from the target database and disable the Extract, Transform, Load (ETL) process.
- The Avaya Analytics™ Release 4.1.1 database can continue to run and process events from Avaya Oceana® during the migration process. However, all data gets discarded when the migration is complete.
- You can use the Avaya Analytics™ Release 4.1.1 database to collect production data only after the post migration is complete.

Before you begin

- Take a backup of the Avaya Analytics™ Release 4.1.1 system.
- Test the Avaya Analytics™ Release 4.1.1 system.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. To switch to the root user, type `su` and press **Enter**.
3. To run the `Analytics Administration` script, use the following command:

   ```
   ccm release orca analytics
   ```
4. To select the **Database** option, enter the corresponding number.
5. To select the **Data Migration** option, enter the corresponding number.
6. To start the pre-migration procedure, select the **Pre-Migration** option by clicking the corresponding number.
7. In the **Proceed to pre-migration config** field, enter `y`.

   The CCM console displays that:

   - The process for installing the schemas is in progress.
   - The database port, which users must use when configuring the POSTGRES_DB_PORT parameter in the `migration_parameters.conf` file.

   Note:

   The entire process takes up to 15 minutes to complete.
8. To return to the previous page, type `b` and press **Enter**.
9. To quit from the current page, type `q` and press **Enter**.
10. To return to the main menu, type `m` and press **Enter**.

Preparing the source system for the migration

About this task

Use this procedure to disable the regular Oracle Data Integrator (ODI) tasks in the Avaya Analytics™ Release 3.7.0.2 system. You must run the post migraton steps to enable the ODI tasks.

Note:

These steps are required for the first migration session or if the post-migration steps were run after a previous migration session. You can also run these steps before starting every migration session.

Before you begin

Take a backup of the Avaya Analytics™ Release 3.7.0.2 system.

Procedure

1. Navigate to the directory that you specified during the ODI installation.

   For example, `cd /home/oracle/DataMigration`

2. Run the following command:

   ```
   ./pre_migration.sh
   ```

   This step disables the Extract, Transform, Load (ETL) process in the source system.

Starting the migration in the source system

About this task

Use this procedure to start the migration in the Avaya Analytics™ Release 3.7.0.2 system.

Before you begin

Complete the pre-migration steps for the source database.

Procedure

1. Open an ssh session to Avaya Analytics™ Release 3.7.0.2 OBIEE server with your Oracle user credentials.

2. Navigate to the directory specified during the installation.

   For example, `cd /home/oracle/DataMigration`.

3. To modify the migration parameters configuration details, go to `modify migration_parameters.conf`.

Note:

You can set the migration start interval once.

4. To start the migration, run the following command:

   `./start.sh`

Checking the migration status in the source system

About this task

You can use this procedure to monitor the migration status in multiple SSH sessions with different monitoring options in the Avaya Analytics™ Release 3.7.0.2 system.

The status displays the following:

- Status of the last migration iteration
- The overall migration progress
- Access to errors

To understand what each status indicates, see the *Maintaining and Troubleshooting Avaya Analytics™* document.

Procedure

1. Open an ssh session to Avaya Analytics™ Release 3.7.0.2 OBIEE server with your Oracle user credentials.
2. Navigate to the directory specified during the installation.

   For example, `cd /home/oracle/DataMigration`
3. To check the migration status, run the following command:

   `./status.sh`
4. To return to the main menu, press `CTRL+C`.

Restarting the migration from scratch

Resetting the migration in the target system

About this task

You can reset the progress of a migration session that is already complete and start the migration again from scratch. You can use these steps in situations when you decide to change the migration start date for interval or the Call Detail Record (CDR) data migration. You can also reset the migration process when the target system or the database displays any errors.

In this case, the migrated data is deleted from the target system. Use this procedure to restart the migration from scratch in the target Avaya Analytics™ Release 4.1.1 system.

Note:

- You must reset the migration process in Avaya Analytics™ Release 4.1.1.0 and Avaya Analytics™ Release 3.7.0.2. You cannot do a partial reset.
- You must restart the migration process from the pre-migration steps after the reset. You can also change the parameters.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. To switch to the root user, type `su` and press **Enter**.
3. To run the `Analytics Administration` script, use the following command:

   ```
   ccm release orca analytics
   ```
4. To select the **Database** option, enter the corresponding number.
5. To select the **Data Migration** option, enter the corresponding number.
6. To select the **Reset Migration** option, enter the corresponding number.
7. In the **Proceed to migration reset** field, enter `y`.

   The CCM console displays the prompt to close the node port that was opened as a part of the pre-migration procedure.
8. In the **Would you like to close this node port**, enter `y`.

   Entering `n` cancels the operation.

   The step removes the exposed port.
9. To return to the previous page, type `b` and press **Enter**.
10. To quit from the current page, type `q` and press **Enter**.
11. To return to the main menu, type `m` and press **Enter**.

Resetting the migration in the source system

About this task

You can reset the progress of a migration session that is already complete and start the migration again from the beginning. You can use these steps when you decide to change the migration start date for interval or the Call Detail Record (CDR) data migration. You can also reset the migration process when the target system or the database displays any errors.

In this case, the migrated data is deleted from the source system. Use this procedure to restart the migration from scratch in the source Avaya Analytics™ Release 3.7.0.2 database.

Note:

- You must reset the migration process in Avaya Analytics™ Release 4.1.1.0 and Avaya Analytics™ Release 3.7.0.2. You cannot do a partial reset.
- You must restart the migration process from the pre-migration steps after the reset. You can also change the parameters.

Procedure

1. Open an ssh session to Avaya Analytics™ Release 3.7.0.2 OBIEE server with your Oracle user credentials.
2. Navigate to the directory that was specified during the installation.

   For example, `cd /home/oracle/DataMigration`.
3. In the `./reset_migration_progress.sh` file, specify the password of the SYS user for the Oracle database.

   SYS is the inbuilt user ID in the database.
4. To start the migration process, run the following command:

   ```
   ./start.sh
   ```

Stopping or pausing the migration

About this task

You can stop or pause a migration for planned multiple migration sessions, or when you have to stop a session to save time.

Procedure

1. Open a ssh session to Avaya Analytics™ Release 3.7.0.2 OBIEE server with your Oracle user credentials.
2. Navigate to the directory that was specified during the installation.

   For example, `cd /home/oracle/DataMigration`.
3. To stop or pause the migration process, run the following command:

   ```
   ./stop.sh
   ```
4. Specify the password of the SYS user for the Oracle database.

   SYS is the inbuilt user ID in the database.

Resuming the migration process

About this task

Use this procedure to resume the migration process after a migration failure or after a planned break in the migration process.

Note:

You cannot resume the migration process after you complete the post migration steps in the Avaya Analytics™ Release 4.1.1 database.

Procedure

1. Open an ssh session to Avaya Analytics™ Release 3.7.0.2 OBIEE server with your Oracle user credentials.
2. Navigate to the directory that was specified during the installation.

   For example, `cd /home/oracle/DataMigration`.
3. To resume the migration, run the following command:

   ```
   ./start.sh
   ```
4. Specify the password of the SYS user for the Oracle database.

   SYS is the inbuilt user ID in the database.

Accessing or retrieving the migration logs

About this task

Use this procedure to access or retrieve the migration logs from the source Avaya Analytics™ Release 3.7.0.2 system.

Procedure

1. In the Avaya Analytics™ Release 3.7.0.2 OBIEE server, navigate to `/home/oracle/DataMigration/logs`.
2. To access the commands that the user ran, locate the `migration.log` file.
3. To access the ODI debug logs, locate the `migration_session_debug_<date>.log` file, where <date> is the current date.

Post migration procedures

Completing the post migration steps in the source system

About this task

Use this procedure to re-enable ETL in the source Avaya Analytics™ Release 3.7.0.2 system.

You can use the post migration steps for the source system after each migration session.

Note:

After the post migration steps are complete, the source Avaya Analytics™ Release 3.7.0.2 database and the Avaya Analytics™ Release 4.1.1.0 database display different records in the respective databases.

Before you begin

Complete the pre-migration and migration steps.

Procedure

1. Open an ssh session to Avaya Analytics™ Release 3.7.0.2 OBIEE server with your Oracle user credentials.
2. Navigate to the directory that was specified during the installation.

   For example, `cd /home/oracle/DataMigration`.
3. Run the following command:

   ```
   ./post_migration.sh
   ```

   The step enables the regular ODI tasks on the source system for the OBIEE reports to display actual data.

Completing the post migration steps in the target system

About this task

Use this procedure to complete the following tasks in the Avaya Analytics™ Release 4.1.1.0:

- Update target database (DB) to recreate unique indexes for dimension tables, update sequences, clean up import tables at stage schema.
- Re-enable the Extract, Transform, Load (ETL) process for processing new data, such as historical data processing, data retention, and partition management.
- Delete the data from the Avaya Analytics™ Release 4.1.1 database that are generated after the pre-migration steps are completed on the database.
- Close database port for external connections.

✱ **Note:**

After the post migration steps are complete, the source Avaya Analytics™ Release 3.7.0.2 database and the Avaya Analytics™ Release 4.1.1.0 database display different records in the respective databases.

Before you begin

Complete the pre-migration and migration steps.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. To switch to the root user, type `su` and press **Enter**.
3. To run the `Analytics Administration` script, use the following command:

   ```
   ccm release orca analytics
   ```
4. To select the **Database** option, enter the corresponding number.
5. To select the **Data Migration** option, enter the corresponding number.
6. To select the **Post-Migration** option, enter the corresponding number.
7. In the **Proceed with post migration config** field, enter `y`.

   Entering `n` cancels the operation.

   The CCM console displays the prompt to close the node port that was opened as a part of the migration.
8. In the **Would you like to close this node port** field, enter `y`.

   Entering `n` cancels the operation.

   The CCM console displays the message that the exposed port is removed and the Avaya Analytics™ scheduler pod is getting restarted. This process can take up to 15 minutes to complete.
9. To return to the previous page, type `b` and press **Enter**.
10. To quit from the current page, type `q` and press **Enter**.
11. To return to the main menu, type `m` and press **Enter**.

Rolling up legacy data

About this task

Use this procedure to roll up legacy data for interval-based data. By default, the roll up data gets generated for the previous month from the moment the Extract, Transform, Load (ETL) process starts the data roll up.

You must use these steps in the following scenarios:

- Installation of Avaya Analytics™ Release 4.1.1.0, where data migration from Avaya Analytics™ Release 3.7.0.2 is complete.

Before you begin

Complete whichever is applicable:

- The pre-upgrade, upgrade, and post upgrade steps.
- The pre-migration, migration, and post migration steps.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. To switch to the root user, type `su` and press **Enter**.
3. To run the `Analytics Administration` script, use the following command:

   ```
   ccm release orca analytics
   ```
4. To select the **Database** option, enter the corresponding number.
5. To select the **Roll-Up Legacy Data** option, enter the corresponding number.
6. To start the legacy data roll up, select the **Start legacy data rollup** option by entering the corresponding number.

   The ETL process starts running in the background. Depending on the amount of data, this process can take from several minutes to hours to complete.

   Note:

   This step disables the daily, and monthly data roll-up and obsolete data deletion procedures.
7. To return to the previous page, type `b` and press **Enter**.
8. To view the status of the roll up data, select the **Legacy data rollup status** option by entering the corresponding number.

   When the CCM console displays 0 for all the days_remaining and months_remaining rows, it indicates that the data roll up process is complete for all interval-based data.
9. To return to the previous page, type `b` and press **Enter**.
10. To quit from the current page, type `q` and press **Enter**.
11. To return to the main menu, type `m` and press **Enter**.

Managing post legacy data roll up operations

About this task

This procedure enables the regular roll up of daily and monthly data and the deletion of obsolete data on Extract, Transform, Load (ETL). Use this procedure to set the data retention period of the following data:

- Interval-based data
- Non-interval based data
- Call Detail Record (CDR) data
- Monthly roll up data

Before you begin

- Start legacy data roll up.
- Check legacy data roll up status. Ensure that the status displays that the roll up of all legacy data is complete.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. To switch to the root user, type `su` and press **Enter**.
3. To run the `Analytics Administration` script, use the following command:

   ```
   ccm release orca analytics
   ```

4. To select the **Database** option, enter the corresponding number.
5. To select the **Roll-Up Legacy Data** option, enter the corresponding number.
6. To start the legacy data roll up, select the **Post legacy data rollup operations** option by entering the corresponding number.
7. To set the retention period for the interval-based data, in the **Enter the new limit value** field, enter the required value.

   The maximum limit is 12 months.

8. To set the retention period for the non-interval based data, in the **Enter the new limit value** field, enter the required value.

   The maximum limit is 12 months.

9. To set the retention period for the Call Detail Record (CDR) data, in the **Enter the new limit value** field, enter the required value.

   The maximum limit is 365 days.

10. To set the retention period for the monthly roll up data, in the **Enter the new limit value** field, enter the required value.

    The maximum limit is 9999 months.

11. To set the data retention period for the daily roll up data, in the **Enter the new limit value** field, enter the required value.

    The maximum limit is 60 months.
12. To return to the previous page, type `b` and press **Enter**.
13. To quit from the current page, type `q` and press **Enter**.
14. To return to the main menu, type `m` and press **Enter**.

Chapter 12: Resources

Documentation

Title	Use this document to:	Audience
Overview		
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
Implementing		
Deploying Avaya Oceana®	Deploy Avaya Oceana®.	• Sales engineers • Business partners • Solution architects • Implementation engineers
Avaya Oceana® and Avaya Analytics™ Disaster Recovery	Know about how to restore Avaya Oceana® when a complete outage at the primary data center.	• Sales engineers • Business partners • Solution architects • Implementation engineers
Upgrading Avaya Oceana®	Upgrade Avaya Oceana®.	• Sales engineers • Business partners • Solution architects • Implementation engineers
Deploying Avaya Analytics™	Deploy Avaya Analytics™.	• Sales engineers • Business partners • Solution architects • Implementation engineers
Administering		

Table continues…

Title	Use this document to:	Audience
Administering Avaya Oceana®	Administer Avaya Oceana®.	• System administrators • Supervisors
Using		
Using Avaya Workspaces for Avaya Oceana®	Use Avaya Workspaces for Avaya Oceana®.	• Agents • Supervisors
Using Avaya Analytics™	Use the features and capabilities of Avaya Analytics™.	• Supervisors • Administrators • Report designers
Avaya Analytics™ Data Dictionary	Use historical and real-time measures in custom reports.	• Administrators • Report designer
Maintaining and Troubleshooting		
Maintaining and Troubleshooting Avaya Oceana®	Perform maintenance and troubleshooting procedures for routine maintenance and troubleshooting of Avaya Oceana®.	• Support personnel • Implementation engineers • Administrators
Maintaining and Troubleshooting Avaya Analytics™	Perform common maintenance functions of Avaya Analytics™ and use tools and utilities for troubleshooting of Avaya Analytics™.	• Support personnel • Implementation engineers • Administrators
Avaya Oceana® Alarms	View details about Avaya Oceana® alarms.	• Support personnel • Administrators

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. 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 the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.
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 only displays the documents for the selected category.

7. Click **Enter**.

Avaya Documentation Center navigation

For some programs, the latest customer documentation is now available on the Avaya Documentation Center website at https://documentation.avaya.com.

Important:

For documents that are not available on Avaya Documentation Center, click **More Sites** > **Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Center, you can:

- Search for keywords.

  To filter by product, click **Filters** and select a product.

- Search for documents.

  From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.

- Sort documents on the search results page.
- Click **Languages** (🌐) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection using **My Docs** (☆).

  Navigate to the **Manage Content** > **My Docs** menu, and do any of the following:

  - Create, rename, and delete a collection.
  - Add topics from various documents to a collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collection that others have shared with you.

- Add yourself as a watcher using the **Watch** icon (👁).

  Navigate to the **Manage Content** > **Watchlist** menu, and do the following:

  - Enable **Include in email notification** to receive email alerts.
  - 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 website.

- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log in to the website. The available functionality depends on your role.

Training

The following courses are available for the Avaya Oceana® program.

Table 4: Sales Credentials

Course code	Course title	Course duration in hours	Delivery type
APSS – 1202 Avaya IX™ Contact Center Solutions for Sales			
41510W	Avaya IX™ Contact Center Portfolio Overview (for Sales)	0.75	Web-based Training
41550T	APSS Avaya IX™ Contact Center Solutions	1.0	Web-based Training
ALCC –2005 Avaya IX™ Voice and Digital Solutions for Sales			
41710W	The Avaya IX™ Contact Center Automated Story	0.50	Web-based Training
41410W	Selling Avaya Oceana®	0.75	Web-based Training
41400W	Selling Avaya Analytics™	0.50	Web-based Training
41480W	The Basics of Cost Justification and Selling Avaya Oceana® Using the ROI Tool	0.50	Web-based Training
41770W	Avaya Experience Portal and Proactive Outreach Manager (POM) for Sales	0.25	Web-based Training

Table 5: Pre-Sales Design

Course code	Course title	Course duration in hours	Delivery type
ACDS – 3480 Avaya Oceana® Design			
34210W	Avaya Oceana® Overview for Design	1.0	Web-based Training
34810W	Designing the Avaya Oceana® Part 1 of 3	1.0	Web-based Training

Table continues…

Course code	Course title	Course duration in hours	Delivery type
34820W	Designing the Avaya Oceana® Part 2 of 3	1.50	Web-based Training
34830W	Designing the Avaya Oceana® Part 3 of 3	1.50	Web-based Training
34800X	Avaya Oceana® Design Exam	1.50	Exam
ALRI-7001 Avaya Oceana® Product Release Information Collection			
39000W	Avaya Oceana® Release 3.8 Details for Pre-Sales	1.0	Portable Document Format (PDF)
39010W	Avaya Analytics™ Release 3.8 and 4.1 Details for Pre-Sales	1.0	PDF
39020W	Avaya Breeze® Snap-Ins for Avaya Oceana® R3.8 Details for Pre-Sales	1.0	PDF

Table 6: Technical Services Partner Credentials

Course code	Course title	Course duration in hours	Delivery type
ACIS – 7495 Avaya Oceana®			
74150V	Integrating Avaya Oceana® Core and Workspaces	40.0	Virtual Instructor-Led Training
7495X	Avaya Oceana® Integration Exam	1.50	Exam
ACSS-7497 Avaya Oceana®			
74550V	Supporting Avaya Oceana®	24	Virtual Instructor-Led Training
7497X	Avaya Oceana® Support Exam	1.75	Exam
ACSS-7498 Avaya Analytics ™ Insights			
74360V	Integrating and Supporting Avaya Analytics™ R4	40.0	Virtual Instructor-Led Training
74980X	Avaya Analytics™ Insights Integration and Support Exam	1.75	Exam

Table 7: Pre-requisite Courseware

Course code	Course title	Course duration in hours	Delivery type
77900W	Avaya Control Manager Training Bundle (5 courses 21900W, 77910W, 77920W, 77930W, 77940W)	5.50	Web-based Training
70160W	Avaya Breeze® Implementation and Support	30.0	Web-based Training

Table 8: End User, Programmer, Administration

Avaya Learning Center				
Course code	**Course title**	**Course duration in hours**	**Delivery type**	**Vanity Link for Attachment**
ALEU-5002 Avaya Oceana® End-User Training				
24020W	Using Avaya Workspaces for Avaya Oceana® - Agent	1.0	Web-based Training	https://www.avaya.com/oceana-agent
24040W	Using Avaya Workspaces for Avaya Oceana® - Supervisor	1.0	Web-based Training	https://www.avaya.com/oceana-supervisor
ALUC-4001 Avaya Breeze® Client SDK				
2410W	Customer Communications and Apps with Oceana® for Developers	3.0	Web-based Training	
ASDC-0010 Avaya Workspaces® Framework				
24150W	Creating Avaya Oceana® Workspaces Framework for Developers	2.0	Web-based Training	
24150W	Avaya Workspaces Framework R3 Test	1.0	Online Test	
ASAC-0010 Avaya Oceana® Administration				
21160W	Avaya Oceana® Fundamentals	0.5	Web-based Training	
24300V	Avaya Oceana® Administration Training	40.0	Virtual Instructor-Led Training	Attached with the sale
24300T	Administering Avaya Oceana® R3 Online Test	1.0	Online Test	
24320W	Administering Avaya Oceana® - Basic	2.5	Web-based Training	https://www.avaya.com/Oceana-admin
ASAC-0022 Administering Avaya Analytic™ for Avaya Oceana®				
24380W	Administering Avaya Analytics™ for Oceana®	1.5	Web-based Training	https://www.avaya.com/Oceana-analyticsadmin
24310T	Administering Avaya Analytics™ R3 for Oceana® Basic Online Teat	1.0	Web-based Training	

Table 9: Other Miscellaneous Courseware

Course code	Course title	Course duration in hours	Delivery type	Vanity Link for Attachment
ALCC-0001 Avaya Workforce Optimization Select Integration with Avaya Oceana® Workspaces				
7014W	Integrating Avaya Workforce Optimization Select with Avaya Oceana® Workspaces	3.0	Web-based Training	
7014A	Avaya Workforce Optimization Select with Avaya Oceana® Workspaces Integration Assessment	1.0	Assessment	
70170W	Integrating Avaya Workspaces with Avaya Aura Call Center Elite	1.0	Web-based Training	
70170T	Avaya Workspaces for Elite Integration Online Test	1.0	Online Test	
71610W	Integrating POM with Avaya Oceana®	1.0	Web-based Training	
71610T	Proactive Outreach Manager with Avaya Oceana® Integration Online Test	1.0	Online Test	
ALEU-5005 Avaya Workspaces for Elite End User				
24120W	Using Avaya Workspaces for Elite – Agents	0.75	Web-based Training	https://www.avaya.com/elite-workspaces-agent
24140W	Using Avaya Workspaces for Elite – Supervisor	0.50	Web-based Training	https://www.avaya.com/elite-workspaces-supervisor

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.

Index