Upgrading Avaya Oceana®

Release 3.10.0.2
Issue 1
March 2026

Notices

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, your modifications, additions or deletions to the publications.

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

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

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

License types

Copyright

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

Virtualization

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

Third Party Components

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

Service Provider

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

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

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

Contents

Chapter 1: Introduction

Purpose

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

New in this release

Avaya Oceana® 3.10.0.2 supports the following:

- Avaya Oceana® Release 3.10.0.2 supports migration from 3.10 and previous releases. For more information and procedure to migrate, refer to the following documents:
  - Migrating Avaya Oceana®
  - Avaya Oceana® Disaster Recovery and Migration
- Avaya Oceana® Release 3.10.0.2 supports:
  - Support for upgrade from 3.10.0.1 to 3.10.0.2
  - Breeze Release 3.9.0.3
  - VMWare Release 8.0
  - Windows Server 2022 for Omnichannel Server.

Chapter 2: Upgrade 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®.

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. VMware ESXi 8.0 is supported.

  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

Avaya Oceana® supports upgrade from release 3.10.0.1 to release 3.10.0.2.

Important:

- 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. Avaya recommends that you perform your Avaya Oceana® Release 3.10.0.2 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 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 upgrade options for Avaya Oceana® DR solutions. Both upgrade 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 upgrade, 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:

- 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.
- In two 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.

Impact 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.*

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

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

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

Important:

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

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

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

Chapter 3: Preupgrade tasks

Preupgrade tasks overview

This chapter provides information about the tasks that you must perform before starting the Avaya Oceana® migration process.

The following are the preupgrade tasks:

- Shutting down all applications and taking snapshots.
- Disabling mailboxes to prevent processing of new emails during the migration 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 Engagement Designer workflows.
- Taking a backup of UCMService to retain data related to deferred emails.
- Taking a backup of MMDB.
- Upgrading Avaya Aura® System Manager for the new release of Avaya Oceana®.
- Setting the cluster state of all clusters to Denying.

Preupgrade checklist

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

No.	Task	Notes	✔
1	Take snapshots of all applications.	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. For information about how to use snapshots in production, see the documentation for the respective application.	
2	Disable all mailboxes.	See Disabling mailbox polling on page 13.	
3	Configure Avaya Oceana® to reject contacts.	See Configuring Avaya Oceana to reject new digital contacts on page 14.	
4	Configure Avaya Oceana® to close chatrooms.	See Configuring Avaya Oceana to close chatrooms on page 15.	
5	Take Avaya Oceana® out of service for voice.	See Taking Avaya Oceana out of service for voice on page 15.	
6	Take a backup of UCAStoreService.	See Taking a backup of UCAStoreService on page 16.	
7	Take a backup of Engagement Designer workflows.	See Taking a backup of Engagement Designer workflows on page 17.	
8	Take a backup of UCMService.	See Taking a backup of UCMService on page 18.	
9	Set the cluster state of all clusters to Denying.	See Setting Cluster State to Denying on page 20.	

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 Avaya Oceana® Cluster 3 to close the chat sessions, and store 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 are handled on the Avaya Aura® system. 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

About this task

UCAStoreService stores information related to users, accounts, attributes, providers, and resources. You must create a backup to retain the data. Avaya Control Manager, Unified Collaboration Administration (UCA), and the Omnichannel server backup the data independently. Therefore, you must create the backups and restore them in coordination.

Procedure

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

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

   If you do not specify any value, the backup storage server retains all backup files.
10. Click **Test Connection**.
11. In the Test Connection Result dialog box, the System Manager must display the following messages:

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

    Note:

    The backup location is a one-time configuration, after which the successive backups reuse the same information.
14. Select the check box for Avaya Oceana® Cluster 1.
15. In the **Backup and Restore** field, select **Backup**.

System Manager displays the Cluster DB Backup page.

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

    Important:

    Note the password, as it is required to restore the UCAStoreService database.
18. In the **Schedule Job** field, click **Run immediately**.
19. Click **Backup**.

    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. Taking a backup of workflows is optional and depends on your requirement.

Procedure

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

   The 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 you use to log in to the backup storage server.
5. In the **Password** field, enter the password 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 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. After 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:

    Note 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 you use to log in to the backup storage server.
5. In the **Password** field, enter the password 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 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:

    Note 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 and Avaya Oceana® Cluster 3.

Chapter 4: Upgrading Avaya Oceana

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:

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.
- 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 Oceana services.
- Verify that there is sufficient free disk space on each Avaya Breeze® platform node.
- Upgrading Avaya Breeze® platform nodes and Avaya Oceana® snap-ins by running the automated script.
- Check the status of Avaya Oceana® clusters.
- Removing all Engagement Designer tasks.
- Deploying the latest versions of Engagement Designer tasks.
- **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.

- Refreshing the certificates on the cluster containing AuthorizationService.

Automated upgrade

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

Sno	Task	Notes	✔
1	Delete older loaded versions of Oceana services from System Manager.	This task ensures that System Manager is running only one version of each service.	
2	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 24.	
3	Check the stability of Avaya Breeze® platform nodes.	See Checking the stability of Avaya Breeze platform nodes on page 25.	
4	Check the replication status of Avaya Breeze® platform nodes.	See Checking the replication status of Avaya Breeze platform nodes on page 25.	
5	Check the state of Oceana services.	See Checking the state of services on page 25.	
6	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 26.	
7	Upgrade all Avaya Breeze® platform nodes and Avaya Oceana® snap-ins.	See Upgrading Avaya Breeze platform nodes and Avaya Oceana snap-ins on page 26.	
8	Check the status of Avaya Oceana® clusters.	See Checking the status of Avaya Oceana clusters on page 30.	
9	Upgrade the Oceana Pluggable Data Connector plugin. **Note:** This step is optional.	See Upgrading the Oceana Pluggable Data Connector plugin on page 37.	
Post upgrade tasks:			
10	Remove all Engagement Designer tasks.	See Removing Engagement Designer tasks on page 31.	

Table continues…

Sno	Task	Notes	✔
11	Deploy Engagement Designer tasks.	See Deploying Engagement Designer tasks on page 31. **Important:** Deploy the latest versions of Engagement Designer tasks only if you use latest workflows.	
12	Recreate Engagement Designer rules for Transfer workflows.	See Recreating Engagement Designer rules for Transfer workflows on page 33	
13	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 34.	
14	Re-install third-party .jar files.	See Reinstalling third-party .jar files on page 34	
15	Refresh the certificates on the cluster containing AuthorizationService.	See Refreshing the Authorization Service identity certificates on page 36.	
16	Configure the CustomerControllerService attributes to connect to the Omnichannel database.	See Configuring CustomerControllerService attributes to connect to Omnichannel Database on page 36.	

Note:

If you are using Reliable Eventing Streaming for ACR-A integration, 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 that there is enough disk space on each of the Avaya Breeze® platform nodes 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 nodes and Avaya Oceana® snap-ins

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 ESXi.

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 28.

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

Table continues…

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

Note:

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

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

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

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

Note:

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

Checking the status of Avaya Oceana® clusters

You must validate if all Avaya Oceana® 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.

Configuring the Enable Tokenless Access attribute of UCAStoreService

About this task

Configure the Enable Tokenless Access attribute of UCAStoreService to enable requests to access resource end-points without the need of the Authorization token.

For more information, see *Deploying Avaya Oceana®*.

Procedure

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.

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.

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 can skip this step, if you have already configured the DNS correctly, and the Windows desktop uses the same DNS as Avaya Breeze® platform nodes.

Procedure

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

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

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

   After the bundle is deployed successfully, ensure that:

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

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

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

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. The Routing Rules will be needed in the further procedure.

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 service profiles in System Manager. You can add EngagementDesigner and AvayaMobileCommunications snap-ins to the 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

About this task

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 to connect 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**.
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 check box. 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 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, you must delete the existing plugin 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.
- 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 tasks.	See Removing Engagement Designer tasks on page 31.	
2	Set the cluster state of all clusters to Denying.	See Setting Cluster State to Denying on page 20.	
3	Uninstall the older versions of all services from clusters.	See Uninstalling all services from the clusters on page 41.	
4	Manually record the current OceanaConfiguration service attributes.	-	
5	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 24.	
6	Delete the older versions of all services from System Manager.	See Deleting all services from System Manager on page 43.	
7	Upgrade all Avaya Breeze® platform nodes.	See Upgrading Avaya Breeze platform nodes using the ISO file on page 43.	
8	Apply the Avaya Breeze® platform patch.	See Applying the Avaya Breeze platform patch on page 44.	
9	Load the latest versions of all services in System Manager.	See *Deploying Avaya Oceana®*.	
10	Install the OceanaConfiguration service to Provisioning Cluster.	See Installing the OceanaConfiguration service to Provisioning Cluster on page 44.	
11	Install services to their relevant clusters.	See Installing services to the clusters on page 45.	

Table continues…

No.	Task	Notes	✔
12	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®*.	
13	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 34.	
14	Set the cluster state of all clusters to Accepting.	See Setting Cluster State to Accepting on page 47.	
15	Deploy Engagement Designer tasks.	See Deploying Engagement Designer tasks on page 31. **Important:** Deploy the latest versions of Engagement Designer tasks only if you use latest workflows	
16	Deploy Engagement Designer workflows.	See Deploying Engagement Designer workflows on page 32.	
17	Configuring the attributes and routing rules of Engagement Designer workflows.	See Configuring the attributes and routing rules of Engagement Designer workflows on page 34.	

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.

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 and Avaya Oceana® Cluster 3.

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:

   The OceanaConfiguration service must be the last service to be uninstalled.

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. 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 service profiles in System Manager. You can add EngagementDesigner and AvayaMobileCommunications snap-ins to the 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 can skip this step, if you have already configured the DNS correctly, and the Windows desktop uses the same DNS as Avaya Breeze® platform nodes.

Procedure

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

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`
2. On the Bundles tab, click **Upload**.
3. On the Choose bundle file to upload dialog box, click **Choose File**.

4. Browse to the `EngagementDesignerTasks.svar` file and click **Upload**.
5. Select the bundle and click **Deploy**.

   After the bundle is deployed successfully, ensure that:

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

   When you open or refresh the Designer Console of Engagement Designer, the system displays the drawers and tasks associated with the tasks bundle.
6. Repeat steps 2 to 5 to deploy Context Store, Work Assignment, and Oceana tasks.

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. The Routing Rules will be needed in the further procedure.

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 to connect 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**.
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**.

Chapter 5: Upgrading the Omnichannel server

Enabling or disabling a scheduled computer maintenance in Windows 2019

About this task

Windows Server 2019 provides a centralized mechanism called Computer Maintenance, for maintaining the operating system, to perform hard disk defragmentation, and Microsoft Windows updates. Computer Maintenance can interfere with the deployment of Contact Center software, resulting in failed installations. You can turn on or off, the scheduled computer maintenance during the software installation.

Procedure

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

Migrating from Avaya Oceana® 3.10.0.1 on Windows Server 2019 to Avaya Oceana® 3.10.0.2 on Windows Server 2022

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

Refer to this section for upgrading from Avaya Oceana® 3.7 and earlier versions to Avaya Oceana® 3.10.0.2 version.

To upgrade from Avaya Oceana® 3.10.0.1 to Avaya Oceana® 3.10.0.2 on the same Windows Server 2019, see Upgrading Standalone Omnidatabase on page 66.

Important:

- From Avaya Oceana® 3.10.0.2, Omnichannel server is supported only on Microsoft Windows Server versions 2019 and 2022 (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 the 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 2022 servers before the start of the maintenance window. You can use the following options:

Option 1 — using a new hostname and IP address for the new Windows Server 2022 Omnichannel server:

- Before the maintenance window:
  - Build the Windows Server 2022 Virtual Machine.
  - Install Windows Server 2022 updates, IIS, and add the server to a domain.
  - Install the Omnichannel server software.
- During the Maintenance Window:
  - Take a database backup of the Windows Server 2022 Omnichannel database.
  - Take the existing Windows Server 2022 Omnichannel server offline and power it off.
  - Restore the Omnichannel database on the Windows Server 2022 Omnichannel server.
  - Log on to SMGR and reconfigure the Omnichannel Database Address attribute to reference the IP address or FQDN of the new Windows Server 2022 Omnichannel server.

Option 2 — reuse the same hostname and IP address for the new Windows Server 2022 Omnichannel server:

- Before the maintenance window:
  - Build the Windows Server 2022 Virtual Machine.
  - Install Windows Server 2022 updates, IIS, and add the server to a domain.
  - Install the Omnichannel server software.
- During the Maintenance Window:
  - Take a database backup of the Windows Server 2022 Omnichannel database.

- Take the existing Windows Server 2022 Omnichannel server off line and power it off.
- Rename the new Windows Server 2022 Omnichannel server to reuse the existing IP address and host name of the Windows Server 2022 Omnichannel server.
- On the new Windows Server 2022 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.
- Do not edit this file, you must delete it.
- Restore the Omnichannel database on the Windows Server 2022 Omnichannel server.

Checklist for upgrading the Omnichannel server

Use the following checklists to upgrade the Omnichannel server:

Checklist for preparing for the upgrade:

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 54.	
3	Take a backup of the Omnichannel database.	See Taking a backup of the Omnichannel database on page 56.	
4	Install a new Microsoft Windows Server 2022 virtual machine with the latest software updates.	See Installing Microsoft Windows Server 2022 on page 57 and the accompanying procedures.	
5	Install the most recent supported operating system service packs.	See Installing the most recent supported operating system service packs on page 59.	
6	Add the server to a domain.	See Adding the server to a domain on page 60.	
7	Disable unused network adapters.	See Disabling unused network adapters on page 60.	
8	Enable Microsoft Remote Desktop connection.	See Enabling Microsoft Remote Desktop connection on page 61.	
9	Install Microsoft IIS on Omnichannel Windows Server.	See Installing Microsoft IIS on Omnichannel Windows Server on page 61.	

Checklist for upgrading:

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 62.	
3	Restore the Omnichannel database for migrations from earlier releases to Avaya Oceana® 3.10.0.2.	See Restoring the Omnichannel database on page 63.	
4	Configure Cache Mirroring.	See the following documents: • *Deploying Avaya Oceana®* • *Avaya Oceana® and Avaya Analytics™ Disaster Recovery*	
5	Patch the Omnichannel server software.	See the following: • Patching the Omnichannel server software on page 64. • Uninstalling an Omnichannel server software patch on page 65	

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 **User Name**, type `_admin`.
   b. In **Password**, 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:
   a. In **User Name**, type `_admin`.
   b. In **Password**, 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.
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:
   a. In **User Name**, type `_admin`.
   b. In **Password**, type `Oceana16`.
   c. Click **LOGIN**.
3. On Cache Management Portal, click **System Administration** > **Configuration** > **Mirror Settings** > **Edit Mirror** > **Remove Mirror Configuration**.
4. On the Remove Mirror Configuration page, click **Clear JoinMirror Flag**.
5. On the server, right-click the **Cache** icon on the toolbar and click **Stop Cache**.
6. Click **Restart**.
7. 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 applies to 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 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 2022

About this task

Install the Microsoft Windows Server 2022 (Desktop Experience) Standard or Datacenter edition and configure it to support the Omnichannel software.

Before you begin

- Ensure that you have a newly formatted server that meets the specifications for installing Microsoft Windows Server 2022 (Desktop Experience) Standard or Datacenter edition.
- Ensure that you have a DVD of the Microsoft Windows Server 2022 (Desktop Experience) Standard or Datacenter edition.
- Ensure that you have a product key for Microsoft Windows Server 2022 (Desktop Experience) Standard or Datacenter edition.
- Obtain the IP addresses for the Omnichannel subnet.

Procedure

1. Insert the Microsoft Windows Server 2022 (Desktop Experience) DVD into the DVD drive.
2. Turn on the power to the server.

   The server begins to boot up.
3. On the Windows Setup screen, in the **Language to install** field, select the appropriate language.
4. In **Time and currency format**, select the appropriate time and currency.

5. In **Keyboard or input method**, select an appropriate value.
6. Click **Next**.
7. Click **Install now**.
8. Select a version of Windows Server 2022 that includes a Desktop Experience.
9. Click **Next**.
10. On the Enter the product key to activate Windows screen, enter the operating system product key.
11. Click **Next**.
12. On the Applicable notices and license terms screen, read the notices and terms, and select **I accept the license terms**.
13. Click **Next**.
14. Select **Custom: Install Windows only (advanced)** for a new installation.
15. Click **Next**.
16. Select the disk partition where you want to install Windows Server 2022 (Desktop Experience) Standard or Datacenter edition.

    Important:

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

    The installation proceeds and automatically restarts the server several times.
18. After completing the installation, log on to the server as an administrator by entering and confirming the administrator password.
19. Select **Set time zone** and complete the information as required for your system.
20. Select **Configure Networking** and complete the information for your Network Interface Card (NIC) with the server IP address.
21. Select **Provide computer name and domain** and complete the information for your server name and network settings.
22. Change the DVD drive letter to **E:** and ensure that the correct drive letters are free for the Omnichannel application and database hard disk drives and partitions.
23. Configure the hard disk drives and partitions for this server using the Windows Server 2022 (Desktop Experience) Standard or Datacenter edition.
24. Install other required drivers for your hardware configuration.

Installing the most recent supported operating system service packs

About this task

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

Avaya tests the Omnichannel software on Windows servers using the most recent updates to the operating system. However, as Microsoft publishes new Operating System updates monthly, some precautions are necessary to ensure that updates published after the Omnichannel software releasedo not break Oceana features or functions.

Note:

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

Before you begin

- Install and configure Microsoft Windows Server 2019 (Desktop Experience) Standard or Datacenter edition on your server.
- Disable Operating System Automatic updates.

Procedure

1. Review the published Microsoft updates to determine the most recent patches or service packs for the Windows Server 2019 (Desktop Experience) Standard or Datacenter OS.
2. Download the appropriate Windows Server 2019 updates for the Omnichannel software installed on this server.
3. Plan a Maintenance Window.
    a. At the start of the Maintenance Window, take a VMware snapshot of the Omnichannel server.
    b. Install the most recent Windows Server 2019 Operating System Updates, following the Microsoft Installation instructions.
    c. Some OS updates and hotfixes might require a reboot of the Omnichannel server.
    d. Do a Sanity test of Oceana to ensure the OS updates and hotfixes have not broken any Oceana feature and function.
    e. If the OS updates and hotfixes break any feature and function, revert to the VM snapshot taken before applying the updates and notify Avaya of the issue.
    f. If the OS updates and hotfixes do not break any feature or function, delete the VM snapshot.
    g. For Omnichannel Database HA solutions, ensure Cache DB Mirroring is working before returning the solution to Production.

4. End the Maintenance Window.

Adding the server to a domain

About this task

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

Before you begin

- Ensure that the server time and domain controller time are synchronized.
- On the server, configure a preferred Domain Name System (DNS) server on the Network Interface Card (NIC).
- Ask your System Administrator to add a Domain Name System (DNS) static entry for this server.

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

Procedure

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

   Provide the fully qualified domain name with the prefix and suffix.
9. Click **OK**.
10. Type the domain administrator username and password.
11. Click **OK**.
12. Restart the server when you are prompted.

Disabling unused network adapters

About this task

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

Procedure

1. Log on to the server.
2. Click **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center**.

3. In the navigation pane, click **Change adapter settings**
4. Right-click the unused network adapter and click **Disable**.
5. Repeat Step 4 to disable all unused network adapters.

Enabling Microsoft Remote Desktop connection

About this task

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

Important:

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

Procedure

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

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 2019 (Desktop Experience) Omnichannel server. This procedure applies to a standalone Omnichannel database that does not have a database mirror. For more information on 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 the 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 later, 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 later, 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.

   Note:

   The **Allow Restore if user file is missing** option 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 take the backup from the server with mirroring configured.
    - Select **No** if you take 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 cleared and a user file is missing, the restore is not completed, and a message box appears. To complete the restore, you must select 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)** Modify the passwords again after the restore process because the backup does not contain the previously modified passwords.

    Note:

    Perform this step if you had modified the default passwords of the Omnichannel database previously.
15. **(Optional)** Reconfigure the server for secure connections after the restore process.

    Note:

    Perform this step if you had previously configured the Omnichannel server for secure connections.

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 Omnichannel database

Upgrading Standalone Omnidatabase

Before you begin

Do the following:

- Take a backup of the Omnichannel database. See BROKEN LINK: Taking a backup of the Omnichannel database.
- 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`.

Procedure

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**.

Upgrading Omnichannel HA Servers

About this task

You must update HA and Omnichannel Database servers in the following order:

1. Take a snapshot of primary server on vCenter for failure upgrading.
2. Upgrade Standby server
3. Perform Switchover
4. Upgrade Standby server (previously the Primary server)
5. Perform Switchover

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 6: 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. You can contact Avaya support for obtaining 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 70.	
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 71.	
4	Uninstall the Arbiter service from the Avaya Control Manager server (optional).	See Uninstalling the Arbiter service on page 72.	
5	Upgrade Avaya Control Manager to Release 9.x.	See Upgrading Avaya Control Manager on page 72.	
6	Install the latest version of the Arbiter service on the Avaya Control Manager server (optional).	See Installing the Arbiter service on page 73.	

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, see *Avaya Control Manager 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 7: Post upgrade tasks

Post upgrade tasks overview

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

The following Postupgrade tasks are applicable for all upgrade paths:

- 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®.
- Migration of Engagement designer workflows.
- Configuring AgentControllerService to have authenticated access to UnifiedAgentController.

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 or later, 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 76.	
7	Enable Avaya Oceana® to monitor all configured mailboxes.	See Enabling mailboxes on page 79.	
8	Configure Avaya Oceana® to accept contacts.	See Configuring Avaya Oceana to accept contacts on page 79.	
9	Configure Avaya Oceana® to open chatrooms.	See Configuring Avaya Oceana to open chatrooms on page 80.	
10	Enable Avaya Oceana® for voice calls.	See Enabling Avaya Oceana for voice calls on page 80.	
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 84.	

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. In 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.

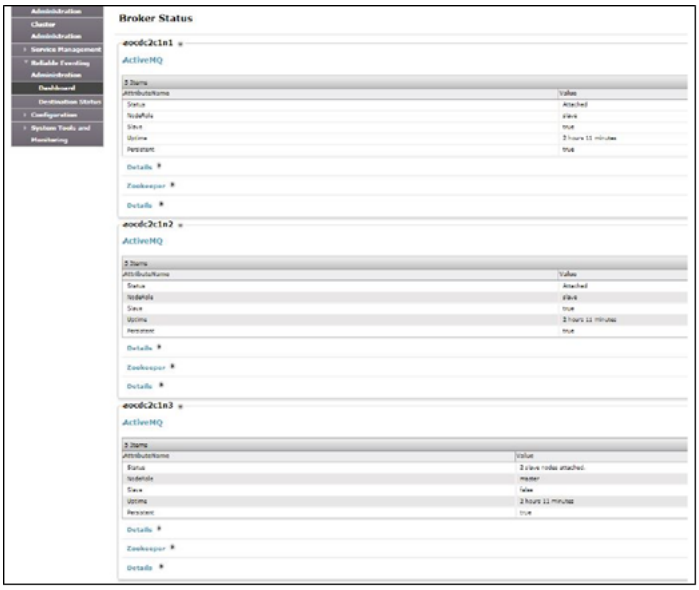
7. Repeat steps 4–6 for the remaining Avaya Breeze® platform nodes.
8. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.

   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.

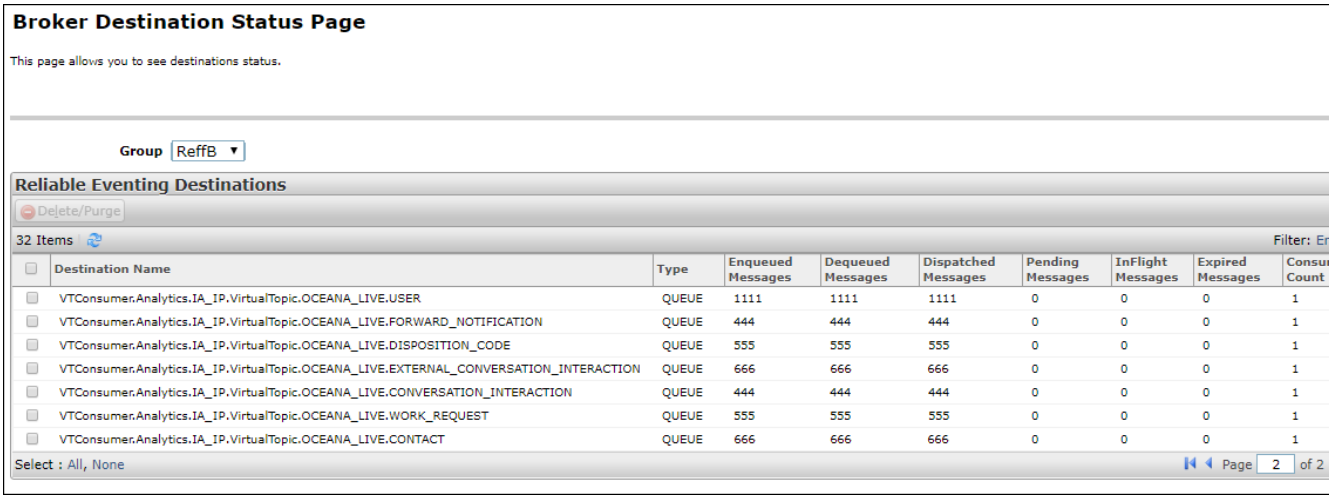


13. On System Manager, click **Elements** > **Avaya Breeze®** > **Reliable Eventing Administration** > **Destination Status**.

    The system displays Broker Destination Status Page.

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

    The system displays the destination status.



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® to open 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 every new release of Avaya Oceana®, the installation of the updates is important for performance improvements and to use the new features and capabilities. 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:

- Workflows are not changed in Avaya Oceana® 3.10.0.2. Skip this section if you are upgrading from Avaya Oceana® 3.10.0.1.
- 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 a Differential 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:
   a. Click the right 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 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 M, P, and L 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:
   a. Click **Modified**.
   b. 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.
   c. To view the differences in the functions in data mappings, move the cursor to the fx icon.
   d. 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 handling Avaya Oceana® contacts.

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 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 3.10.0.2:

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.

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

- Migrate to the latest System Manager release
- Apply latest System Manager patch and hotfix

Simultaneous upgrade of primary and Disaster Recovery sites

Option A upgrades the complete Avaya Oceana® including primary and Disaster Recovery (DR) sites to the latest Avaya Oceana® 3.10.0.2 software in a single maintenance window.

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

- Upgrade Avaya Aura® System Manager to the latest software release.
- Upgrade Avaya Aura® applications, such as Control Manager, AES, Avaya Experience Portal, and Avaya Aura® System Manager, to a minimum release compatible with Avaya Oceana® 3.10.0.2
- Download the Avaya Oceana® 3.10.0.2 software from PLDS.
- Download the Avaya Control Manager 9.x software from PLDS.

The following table lists the tasks to upgrade Avaya Oceana® from 3.10.0.1 to 3.10.0.2:

Note:

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

Table 1: Primary and DR sites upgrade

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.
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.

Table continues…

Task	Description	Reference	Expected outcome
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.
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 upgrade.	Suite of snapshots is taken.

Table continues…

Task	Description	Reference	Expected outcome
Power on	Power on the following applications to perform the software upgrade 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® upgrade 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® upgrade. • Undeploy the current Avaya Engagement Designer tasks and flows. • Upgrade to latest tasks and Avaya Engagement Designer flows.	See Upgrading Avaya Breeze platform nodes and Avaya Oceana snap-ins on page 26.	The Avaya Oceana® primary site is upgraded to Avaya Oceana® 3.10.0.2.

Table continues…

Task	Description	Reference	Expected outcome
Start Avaya Oceana® upgrade 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® upgrade. • Undeploy the current Avaya Engagement Designer tasks and flows. • Upgrade to latest tasks and Avaya Engagement Designer flows.	See Upgrading Avaya Breeze platform nodes and Avaya Oceana snap-ins on page 26.	The Avaya Oceana® DR site is upgraded to Avaya Oceana® 3.10.0.2.
Start Avaya Control Manager and database upgrade for primary and DR sites	Upgrade the primary and DR Avaya Control Manager servers to the latest release required for Avaya Oceana® 3.10.0.2.	See the Avaya Control Manager upgrade documentation.	The Avaya Control Manager primary and DR sites are upgraded to Avaya Oceana® 3.10.0.2.

Table continues…

Task	Description	Reference	Expected outcome
Start Omnichannel Database upgrade for primary and DR sites	You must perform the following steps to remove Omnichannel Database mirroring prior to software upgrade: • Remove database mirroring to return servers to standalone role. • Create backups of primary and DR databases. • 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 upgraded to Avaya Oceana® 3.10.0.2.
Update Avaya Oceana® custom applications and interfaces	The following items are upgraded 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 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® 3.10.0.2 is completely upgraded, and the solution is back in production.

Two-step upgrade of primary and Disaster Recovery sites

Option B upgrades 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 upgraded 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:

- Upgrade Avaya Aura® System Manager to the latest software release.

- Upgrade Avaya Aura® applications, such as Control Manager, AES, Avaya Experience Portal, and Avaya Aura® System Manager, to a minimum release compatible with Avaya Oceana® 3.10.0.2.
- Download the Avaya Oceana® 3.10.0.2 software from PLDS.
- Download the Avaya Control Manager 9.x software from PLDS.

The following tables list the tasks to upgrade Avaya Oceana® from 3.10.0.1 to 3.10.0.2:

Note:

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

Table 2: Primary upgrade

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			
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.

Table continues…

Task	Description	Reference	Expected outcome
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 upgrade.	Suite of snapshots taken.

Table continues…

Task	Description	Reference	Expected outcome
Power on	Power on the following applications to perform the software upgrade 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® upgrade 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® upgrade. • Undeploy the current Avaya Engagement Designer tasks and flows. • Upgrade to latest tasks and Avaya Engagement Designer flows.	See Upgrading Avaya Breeze platform nodes and Avaya Oceana snap-ins on page 26.	The Avaya Oceana® primary site is upgraded to Avaya Oceana® 3.10.0.2.

Table continues…

Task	Description	Reference	Expected outcome
Start Avaya Control Manager and database upgrade for primary and DR sites.	Upgrade the primary and DR Avaya Control Manager servers to the latest release required for Avaya Oceana® 3.10.0.2.	See the Avaya Control Manager upgrade documentation.	The Avaya Control Manager primary and DR sites are upgraded to Avaya Oceana® 3.10.0.2.
Start Omnichannel Database upgrade for the primary site only.	You must perform the following steps to remove Omnichannel Database mirroring prior to software upgrade: • Remove database mirroring to return primary and DR servers to standalone role. • Create backup of the primary databases. • 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 upgraded to Avaya Oceana® 3.10.0.2.
Update Avaya Oceana® custom applications and interfaces.	The following items are upgraded 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™ 3.10.0.2 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 upgrade

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 upgrade.	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 upgrade 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 upgrade 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® upgrade. • Undeploy the current Avaya Engagement Designer tasks and flows. • Upgrade to latest tasks and Avaya Engagement Designer flows.	See Upgrading Avaya Breeze platform nodes and Avaya Oceana snap-ins on page 26.	The Avaya Oceana® DR site is upgraded to Avaya Oceana® 3.10.0.2.
Start Omnichannel database upgrade for the DR site.	Do the following: • 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 upgraded to Avaya Oceana® 3.10.0.2.

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 upgraded 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® 3.10.0.2 and Avaya Analytics™ 4.1.2 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 55 • Removing Cache Mirroring from the active Omnichannel server on page 55	
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 9: Upgrading from Analytics 4.3 P3 or 4.3.1.0 to 4.3.1.1

For information on upgrading to Avaya Analytics™ 4.3.1.1, see *Deploying Avaya Analytics™ for Avaya Oceana® document*.

Chapter 10: Resources

Documentation

Title	Use this document to:	Audience
Overview		
Avaya Oceana® Solution Description	Use this guide to know about the tested product characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements.	• Sales engineers • Business partners • Solution architects • Implementation engineers
Implementing		
Deploying Avaya Oceana®	Use this guide to know how to deploy Avaya Oceana® Solution on the customer environment.	• Sales engineers • Business partners • Solution architects • Implementation engineers
Avaya Oceana® and Avaya Analytics™ Disaster Recovery	Use this guide to know how to restore Avaya Oceana®, solution when there is a complete outage at the primary data center.	• Sales engineers • Business partners • Solution architects • Implementation engineers
Migrating Avaya Oceana®	Use this guide to know how to migrate Avaya Oceana® solution from the existing version.	• Sales engineers • Business partners • Solution architects • Implementation engineers
Deploying Avaya Analytics™	Deploy Avaya Analytics™.	• Sales engineers • Business partners • Solution architects • Implementation engineers
Administering		

Table continues…

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

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.

For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.

8. Click to display the search results.

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at https://documentation.avaya.com. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the Avaya Support website.

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.
- Click **Languages** ( ) in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.

  You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click **<** or **>** next to the document title to navigate to the previous topic or the next topic.
- Click **Share** ( ) to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** ( ). You can add the topic and its subtopics or add the entire publication.
- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

You can do the following:

- Create, rename, and delete a collection.
- Set a collection as the default or favorite collection.
- Save a PDF of the selected content in a collection and download it to your computer.
- Share content in a collection with others through email.
- Receive collections that others have shared with you.

- Click **Watch** ( ) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

  You can do the following:

  - Enable **Email notifications** to receive email alerts.
  - Unwatch the selected content or all topics.
- Send feedback for a topic.

Training

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

Table 4: Sales Credentials

Course code	Course title	Course duration in hours	Delivery type
APSS – 1202 Avaya OneCloud™ CCaaS Sales			
41511W	Selling Avaya OneCloud™ CCaaS Solutions	0.75	Web-based Training
41551T	Avaya OneCloud™ CCaaS Sales Specialized Test	1.0	Web-based Training
ALCC –2005 Avaya Multiexperience Solutions Sales (ALCC-2005)			
41710W	The Avaya OneCloud™ Contact Center Automated Story	0.50	Web-based Training
41411W	Selling Avaya Oceana®	0.75	Web-based Training
41401W	Selling Avaya Analytics™	0.50	Web-based Training
41481W	Avaya Oceana® ROI for Sales	0.50	Web-based Training
41770W	Avaya Experience Portal and Proactive Outreach Manager (POM) for Sales	0.25	Web-based Training

Table 5: Pre-Sales Design

Course code	Course title	Course duration in hours	Delivery type
ACDS – 3480 Avaya Oceana® Solution Design			
34211W	Avaya Oceana® Overview for Design	0.75	Web-based Training
34811W	Designing the Avaya Oceana Solution Part 1 of 3	1.0	Web-based Training
34821W	Designing the Avaya Oceana Solution Part 2 of 3	1.0	Web-based Training
34831W	Designing the Avaya Oceana Solution Part 3 of 3	1.0	Web-based Training
34801X	Avaya Oceana® Solution Design Exam	1.50	Exam
ALRI-7001 Avaya Oceana® Product Release Information Collection			
39001W	Avaya Oceana® R3.8 with Breeze Snap-ins Details for Pre-Sales	1.0	Portable Document Format (PDF)
39020W	Avaya Breeze® Snap-ins for Avaya Oceana Details for Pre-Sales	1.0	PDF

Table 6: Technical Services Partner Credentials

Course code	Course title	Course duration in hours	Delivery type
ACIS – 7495 Avaya Oceana® Solution Implement			
74150V	Integrating Avaya Oceana® Core and Workspaces	40.0	Virtual Instructor-Led Training
74950X	Avaya Oceana® Solution Integration Exam	1.50	Exam
ACSS-7497 Avaya Oceana®			
74550V	Supporting Avaya Oceana®	24	Virtual Instructor-Led Training
7497X	Avaya Oceana® Support Exam	1.75	Exam
74360W	Installing Avaya Analytics™ for Oceana®	1.5	Web-based Training

Table 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	Customizing the Avaya Workspaces® Framework	3.0	Web-based Training	
24150T	Avaya Workspaces® Framework R3 Test	1.0	Online Test	
ASAC-0005 Avaya Oceana® Administration				
21160W	Avaya Oceana® Fundamentals	0.5	Web-based Training	
24300V	Administering Avaya Oceana® R3 Omnichannel	40.0	Virtual Instructor-Led Training	Attached with the sale
2430T	Administering Avaya Oceana® R3 Online Test	1.0	Online Test	
24320W	Administering Avaya Oceana® - Basic	2.5	Web-based Training	https://www.avaya.com/Oceana-admin

Table continues…

Avaya Learning Center				
Course code	**Course title**	**Course duration in hours**	**Delivery type**	**Vanity Link for Attachment**
ASAC-0031 Avaya Analytics™ R4 for Oceana® Administrator				
24380T	Administering Avaya Analytics1M R4 for Oceana8 Specialized Test	1.0	Online Test	

Table 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	
71610W	Integrating POM with Avaya Oceana®	1.0	Web-based Training	

Support

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

Index

N

O

P

R

S

T

U

V

W