Migrating 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 migrating to Avaya Oceana® 3.10.0.2.

Administrators and other personnel who perform Avaya Oceana® 3.10.0.2 migration can use this document.

Chapter 2: Overview

Avaya Oceana® migration overview

The subsequent sections in this document provide tasks that you must perform before, during, and after migrating to Avaya Oceana® 3.10.0.2.

The Avaya Oceana® migration procedure replaces each existing Avaya Breeze® platform server in the cluster with a new server installed from the latest release of Avaya Breeze® platform OVA. The migration procedure impacts service and must be performed only during a maintenance window.

Supported Avaya Oceana® migration paths

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

From release	To release
3.10	3.10.0.2
3.9	3.10.0.2
3.8.2	3.10.0.2
3.8.1.1	3.10.0.2

Important:

- Before migrating 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 migrating 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. 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.

Prerequisite for migration

Avaya Analytics™

Avaya Analytics™ 4.3.1.1 is compatible with Avaya Oceana® 3.10.0.2 release. If you are on Avaya Analytics™ 4.1.x or 4.1.2 release, then you have to migrate the Avaya Analytics™ to 4.3.1.1. If you are on Avaya Analytics™ 4.2 or 4.3 release, then you have to upgrade to Avaya Analytics™ 4.3.1.1. For information about the upgrade, see Avaya Analytics™ 4.3.1.1 release notes.

Other requirements

- Identify hardware resources to deploy Avaya Aura®, Avaya Breeze® platform, and Omnichannel Provider database components.
- Identify if your environment is on the supported migration paths.
- Check for third-party integrated software compatibility.
- Download the Avaya Oceana® 3.10.0.2 software from the Avaya Support website at https://support.avaya.com.
- An additional 2 GB of RAM for each Avaya Breeze® platform node as compared to the older release.
- An additional 5 GB of disk space for each Avaya Breeze® platform node as compared to older release.
- Additional storage is required as the new and old Avaya Breeze® platform nodes co-exist until the migration is completed.
- For more information about hardware requirement for Avaya Analytics™ 4.3.1.1, refer to the *Deploying Avaya Analytics™ for Avaya Oceana®* documentation available on the Avaya Support website at https://support.avaya.com.

Chapter 3: Pre-migration tasks

Avaya Oceana® 3.10.0.2 pre-migration checklist

Use the following checklist for the tasks that you must complete before migrating to Avaya Oceana® 3.10.0.2:

No.	Task	Notes	✔
1	Take a snapshot of all Avaya Breeze® platform servers, Omnichannel Provider database, and Avaya Aura® System Manager before performing any activity.	Perform this step if the customer decides to fall back to the previous release of Avaya Oceana®.	
2	Take a backup of UCAStoreService, UCMService, Engagement Designer Workflows, and Engagement Designer Quartz database on a remote server or location.	Perform this step if the customer decides to fall back to the previous release of Avaya Oceana®. For more information, see Taking a backup of UCAStoreService on page 22, Taking a backup of UCMService on page 24, Taking a backup of Engagement Designer workflows on page 25, Taking a backup of Engagement Designer Quartz on page 26.	
3	Disable all mailboxes.	See Disabling mailbox polling on page 10.	
4	Configure Avaya Oceana® to reject contacts.	See Configuring Avaya Oceana to reject new digital contacts on page 11.	
5	Configure Avaya Oceana® to close chatrooms.	See Configuring Avaya Oceana to close chatrooms on page 11.	
6	Take Avaya Oceana® out of service for voice.	See Taking Avaya Oceana out of service for voice on page 12.	

Table continues…

No.	Task	Notes	✔
7	Record Avaya Breeze® platform identity certificate and third-party certificate information.	Note the information about the following certificates: • Security Module HTTPS • Security Module SIP • Authorization • WebSphere For more information about accessing these certificates, see Chapter *Configure certificates* in the *Deploying Avaya Oceana®* documentation available on the Avaya Support website at https://support.avaya.com.	
8	Delete the reliable eventing group.	See Deleting a Reliable Eventing group for cluster 1 on page 13.	
9	Editing service profiles to remove snap-ins.	See Editing service profiles to remove snap-ins on page 13.	

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®*.

Viewing Avaya Breeze® platform Identity Certificate details

Procedure

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

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

You have to re-apply third-party CA root certificate and p12 files after the upgrade.

5. Ping each DNS entry and verify if it returns the correct IP address to ensure that all the DNS entries are resolvable.
6. Repeat the step 4 and step 5 for Security Module SIP, Authorization, and WebSphere certificates.

   Note:

   WebSphere certificates is required only for Avaya Oceana® Cluster1.
7. Click **Done**.

Deleting a Reliable Eventing group for cluster 1

Before you begin

To delete a Reliable Eventing group configuration, you must set the Avaya Oceana® Cluster 1 status in Avaya Oceana® to `Denying`. For more information, see the *Deploying Avaya Oceana®* document.

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®** > **Reliable Eventing Administration** > **Dashboard**.
2. Select the **Reliable Eventing group** and click **Delete**.
3. In the Confirm Delete window, click **Continue**.

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.

Chapter 4: Migrating to Avaya Oceana® 3.10.0.2

Checklist for Avaya Oceana® 3.10.0.2 migration

Use the following checklist for the tasks that you must perform to migrate to Avaya Oceana® 3.10.0.2:

No.	Task	Notes	✔
1	Upgrade Avaya Aura® System Manager.	Avaya Oceana® 3.10.0.2 is compatible with Avaya Aura® System Manager 10.1.3.6 and later and Avaya Aura® System Manager 10.2.0.1, 10.2.1.0, and 10.2.1.1. Avaya Oceana® 3.10.0.2 requires Avaya Breeze® Element Manager package 3.9.0.3. Apply Avaya Breeze® Element Manager manually using the `upgradeSolution` script to all versions of Avaya Aura® System Manager. For more information about Avaya Aura® System Manager 10.1.x and Avaya Aura® System Manager 10.2.x migrations, see, Avaya Aura® System Manager Release Notes and *Upgrading Avaya Aura® System Manager* documentation available on the Avaya Support website at https://support.avaya.com.	
2	Upgrade Avaya Breeze® Element Manager.	See the topic *Running the upgradeSolution script for System Manager* from the Chapter *Planning and preconfiguration within Deploying Avaya Breeze® platform* of *Deploying Avaya Breeze® platform* documentation available on the Avaya Support website at https://support.avaya.com.	

Table continues…

No.	Task	Notes	✔
3	Install `ClusterDBMigrationService-3.9.0.3` service on all clusters.	See Installing the ClusterDBMigrationService-3.9.0.3 on page 17.	
4	Deploy Avaya Breeze® platform 3.9.0.3.	See Deploying Avaya Breeze platform 3.9.0.3 on page 20.	
5	Set the cluster state of all clusters to Denying.	See Setting Cluster State to Denying on page 22.	
6	Take a backup of UCAStoreService.	See Taking a backup of UCAStoreService on page 22.	
7	Take a backup of UCMService.	See Taking a backup of UCMService on page 24.	
8	(Optional) Take a backup of Engagement Designer Workflows.	Perform this task only if you want to take a backup of the Engagement Designer Workflows. See Taking a backup of Engagement Designer workflows on page 25.	
9	(Optional) Take a backup of Engagement Designer Quartz.	Perform this task only if you want to take a backup of Engagement Designer Quartz. See Taking a backup of Engagement Designer Quartz on page 26.	
10	Edit the cluster and disable load balancer.	See Disabling HTTP load balancing in an Avaya Breeze platform clusters on page 27.	
11	Remove Avaya Breeze® platform nodes from Avaya Oceana® clusters.	See Removing an Avaya Breeze platform server from the cluster on page 28.	
12	Power down the prior release Avaya Breeze® platform nodes.	-	
13	Power on the 3.9.0.3 Avaya Breeze® platform nodes individually.	Provide a gap of 5 minutes or more to power on each node.	
14	Upload Avaya Oceana® 3.10.0.2 snap-in services on System Manager.	See Loading snap-in services on page 29.	
15	Swap Avaya Oceana® services with the latest release.	Remove old services and add Avaya Oceana® 3.10.0.2 service version. To add the new service, see *Loading SVARs in System Manager* topic of the *Deploying Avaya Oceana®* documentation available on the Avaya Support website at https://support.avaya.com.	

Table continues…

No.	Task	Notes	✔
16	Remove the `ClusterDBMigrationService-3.9.0.3` service.	See Removing the ClusterDBMigrationService-3.9.0.3 service on page 29.	
17	Place Avaya Breeze® platform 3.9.0.3 nodes as a part of Avaya Oceana® cluster.	Ensure that Avaya Oceana® services are installed.	
18	Re-enable HTTP load balancer for all Avaya Oceana® clusters.	See Enabling HTTP load balancing in an Avaya Breeze platform cluster on page 30.	
19	Restore the backup of UCAStoreService.	See *Restoring the UCAStoreService data* topic from the *Maintaining and Troubleshooting Avaya Oceana®* documentation on the Avaya Support website at https://support.avaya.com.	
20	Restore the backup of UCMService.	See *Restoring UCMService data for Avaya Oceana® Cluster 1* topic from the *Maintaining and Troubleshooting Avaya Oceana®* documentation on the Avaya Support website at https://support.avaya.com.	
21	(Optional) Restore the backup of Engagement Designer Workflows.	Perform this task only if you want to restore Engagement Designer Workflows.	
22	(Optional) Restore the backup of Engagement Designer Quartz.	Perform this task only if want to restore Engagement Designer Quartz database.	
23	Replace Avaya Breeze® platform WebSphere, Authorization, and securitymodule_http identity certificates. Import LDAP and third-party certificates.	See Replacing the WebSphere certificate on page 32 and Replace Avaya Breeze platform node identity certificates on page 30.	
24	Upgrade the Omnichannel Provider database server.	See Upgrading the Omnichannel Server on page 37.	
25	Reboot Avaya Oceana® clusters.	See Rebooting Avaya Oceana clusters on page 41.	

For more information about migration steps overview, see Avaya Oceana migration tasks overview on page 20.

Installing the ClusterDBMigrationService-3.9.0.3

About this task

The `ClusterDBMigrationService-3.9.0.3` service is delivered and pre-loaded as a part of Element Manager release 3.9. The `ClusterDBMigrationService-3.9.0.3` service is

versioned as a 3.9 service. However, the snap-in is compatible and intended for installation on 3.8.1.1 Avaya Breeze® platform clusters.

You must install the `ClusterDBMigrationService` on the Avaya Breeze® platform 3.8.x cluster before you backup the Avaya Oceana® databases and migrate to Avaya Breeze® platform 3.9.0.3 with Avaya Oceana® 3.10.0.2. This enables you to restore the existing cluster database backed up from 3.8.x to the cluster following the upgrade of the cluster servers to Avaya Breeze® platform 3.9.

Important:

The `ClusterDBMigrationService` is required for the cluster database backup of snap-ins that need to be restored to Avaya Breeze® platform 3.9.0.3 with Avaya Oceana® 3.10.0.2.

As a precaution, take a remote backup of your cluster databases before installing the `ClusterDBMigrationService`. If a reversion is necessary, you can still use these backups on Avaya Breeze® platform 3.8.x and earlier nodes. When you install `ClusterDBMigrationService` on Avaya Breeze® platform cluster, the postgres compatibility version is permanently changed to postgres 13 and is no longer compatible with Avaya Breeze® platform 3.8.1.1 and before releases.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
2. Select the **ClusterDBMigrationService-3.9.0.3** service and click **Install**.
3. Select the clusters on which you want to install the ClusterDBMigrationService-3.9.0.3 service and click **Commit**.
4. To see the status of the service installation, click **Refresh**.
   - Installed: A green check mark indicates that the snap-in has completed installation on all the Avaya Breeze® platform servers in the cluster.
   - Installing: A yellow exclamation mark enclosed in a triangle indicates that the snap-in has not completed installation on all the servers.

   Perform this step only for Cluster 1.

Related links

Taking a backup of cluster database after installing the clusterDBMigrationService on page 18

Taking a backup of cluster database after installing the clusterDBMigrationService

About this task

The backup feature enables you to take a backup of the databases in the cluster database. The cluster database contains different databases defined by the snap-ins that are installed on the cluster.

Before you begin

- If you take a back up of a cluster from an earlier release of Avaya Breeze® platform (for example 3.8.1.1 or earlier) before an upgrade to Avaya Breeze® platform 3.9, you must verify the that you install the `clusterDBMigrationService-3.9.0.3` service on the cluster before proceeding.
- Windows servers are incompatible with the cluster backup and restore feature and do not use as an archive server.

Procedure

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

   Note:

   You can store the backup on a remote linux server. Windows is not supported for Avaya Breeze® platform backups.
4. Click **Test Connection** to verify the connection of the backup server.
5. Click **Commit**.
6. Select the cluster to backup and click **Backup and Restore** > **Backup**.

   The web console displays the Cluster DB Backup page.
7. In the **Backup** section, select the services to back up.
8. In the **Job schedule** section, enter the following details:
   a. In the **Backup password** field, enter a password.
   b. In the **Schedule Job** field, to run an immediate backup, select **Run immediately**. Otherwise, select **Schedule later** and enter the required details in the **Task Time**, **Recurrence**, and **Range** fields.
9. Click **Backup**.
   a. To monitor the status of the backup, click **Backup and Restore** > **Job Status**.
   b. To cancel a backup operation, click **Backup and Restore Cancel**.

Related links

Installing the ClusterDBMigrationService-3.9.0.3 on page 17

Deploying Avaya Breeze® platform 3.9.0.3

About this task

Moving to Avaya Breeze® platform 3.9.0.3 from the releases 3.8.1, 3.8.1.1 and before requires a migration as mentioned in the chapter *Method 1: Upgrading using OVA reinstallation* of the *Upgrading Avaya Breeze® platform* documentation available on the Avaya Support website at https://support.avaya.com.

Procedure

Deploy the Avaya Breeze® platform 3.9.0.3 OVA in vCenter to replace each node in the targeted cluster, using same IP, FQDN of current node.

Modify the memory, disk, and vCPU requirements for each component of Avaya Oceana® in addition to 2 GB RAM and 5 GB hard disk for each node. For information about the requirements, see *Avaya Oceana® hardware requirements* topic in the *Deploying Avaya Oceana®* documentation available on Avaya Support website at https://support.avaya.com.

Do not power on the virtual machines after deploying the OVA, until the previous virtual machines running the older versions of Avaya Breeze® platform are removed from their clusters and powered down. This is mandatory to avoid duplicate IP addresses running in your production network.

Avaya Oceana® migration tasks overview

About this task

Avaya Oceana® 3.10.0.2 requires an OVA reinstallation of each Avaya Breeze® platform cluster node within the solution.

See *Method 1: Upgrading using OVA reinstallation* chapter in the *Upgrading Avaya Breeze® platform* documentation available on the Avaya Support website at https://support.avaya.com.

Before you begin

Perform the pre-migration tasks before you begin with the migration. For more information, see Avaya Oceana 3.10.0.2 pre-migration checklist on page 9. Avaya Oceana® 3.10.0.2 migration requires an addition of 2 GB RAM and 5 GB hard disk for each node. Avaya Breeze® platform supports VMware/ESXi 7.x and VMware/ESXi 8.x.

Procedure

1. Install the Avaya Breeze® platform 3.9.0.3 `ClusterDBMigrationService` on Avaya Oceana® cluster 1 while your nodes are still on Avaya Breeze® platform 3.8.x.
2. Set the cluster state to **Deny New Service** for all Avaya Oceana® clusters.
3. Take a cluster DB backup of Avaya Oceana® cluster1:
   - Taking a backup of UCAStoreService

- Taking a backup of UCMService
- (Optional) Taking a backup of Engagement Designer Workflows
- (Optional) Taking a backup of Engagement Designer Quartz

4. Edit the cluster and disable load balancer.
5. Remove previous release Avaya Breeze® platform nodes from all clusters by removing the node marked as Idle, Standby, and Active for the cluster DB roles.
6. Click **Commit**.

   Wait for all services to be uninstalled from the Avaya Breeze® platform nodes.
7. Repeat step 4 to step 6 for all the remaining Avaya Oceana® clusters.
8. Power down the previous release Avaya Breeze® platform nodes.
9. Power on the Avaya Breeze® platform 3.9.0.3 nodes individually.

   Provide a gap of 5 minutes or more to power on each node.
10. Upload Avaya Oceana® 3.10.0.2 services on Avaya Aura® System Manager.
11. Edit the cluster and remove the `ClusterDBMigrationService`. Remove old services and add Avaya Oceana® 3.10.0.2 services.

    You can edit the cluster and exchange versioned services.
12. Place Avaya Breeze® platform 3.9.0.3 nodes as part of all Avaya Oceana® clusters.
13. Edit the cluster and place all Avaya Breeze® platform nodes in the cluster and re-enable load balancer.
14. Wait for green check mark to display on the Cluster Administration dashboard.
15. From the **Backup and Restore** field, select **Restore** to restore cluster DB backup on Avaya Oceana® cluster1:
    - Restore the backup of UCAStoreService
    - Restore the backup of UCMService
    - (Optional) Restore the backup of Engagement Designer Workflows
    - (Optional) Restore the backup of Engagement Designer Quartz
16. Wait for cluster to be up and the Cluster Administration dashboard reports all green.
17. Deploy Avaya Oceana® 3.10.0.2 Engagement Designer workflow.

    Note:

    You can skip this step, if you are migrating from Avaya Oceana® 3.10 and can use the Avaya Oceana® 3.10 workflow.
18. Deploy Avaya Oceana® 3.10.0.2 Engagement Designer tasks.
19. Reconfigure and import third-party certificates on Avaya Breeze® platform servers.

20. Upgrade the Omnichannel Provider database server.
21. Reboot Avaya Oceana® clusters.

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.

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 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`.

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 Engagement Designer Quartz

About this task

Use this procedure to take a backup of Engagement Designer quartz. Taking a backup of quartz database 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_quartz** 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`.

Disabling HTTP load balancing in an Avaya Breeze® platform clusters

About this task

Use this procedure to disable HTTP load balancing in an Avaya Breeze® platform clusters.

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. To disable load balancing for an existing cluster, on the Cluster Administration page, do the following:
   a. Select the check box in front of the cluster 1.
   b. In the **Cluster State** field, click **Deny New Service**.
   c. Verify that the **Cluster State** column for the cluster is changed to **Denying**.
   d. Click **Edit**.
3. In the Cluster Attributes section, unselect the **Is Load Balancer enabled** check box to disable load balancing.
4. Click **Commit**.
5. Repeat the steps for clusters 2, 3, 4, and 5 based on the requirement.

Removing an Avaya Breeze® platform server from the cluster

About this task

Use this procedure to remove an Avaya Breeze® platform server from the cluster. Note that this procedure is service impacting.

Remove Avaya Breeze® platform from all the clusters by removing the node marked as Idle, Standby, and Active for the cluster DB roles.

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®**.
2. In the navigation pane, click **Cluster Administration**.
3. Select the targeted cluster and click **Cluster State**.
   a. Click **Deny New Service**.
   b. Click **Continue** when prompted.

   You can remove a server from the cluster only if all reachable nodes in the cluster are in the **Deny New Service** mode.
4. Select the cluster, and click **Edit**.
5. On the Cluster Editor page, click the **Servers** tab.
6. In the **Assigned Servers** table, click the cross sign (**x**) next to the **Name** column.

   Note:

   The cluster database roles are assigned to the nodes within the cluster. You must remove clusters in the following order of states; Idle, Standby, and Active.

   The action of removing one or more servers from the cluster will restart the respective servers being removed from the cluster and the remaining servers in the cluster. Therefore, a service outage for this cluster should be expected.
7. Click **Commit** to remove the server from the cluster you selected.

   Note:

   When you remove either the primary or the secondary Lookup server from a cluster, all the other servers in the cluster restart due to the configuration change. The system displays the Lookup server icon  against the Lookup server on the **Server Administration** and **Cluster Administration** pages.
8. Confirm the warnings presented.
9. Wait until all services have been uninstalled successfully.

Loading snap-in services

About this task

Download the snap-in services and SDK. Extract the `Oceana<Release_number>.zip` file and then upload the appropriate snap-in services on the System Manager.

Procedure

1. On the System Manager web console, click **Home** > **Elements** > **Avaya Breeze™** > **Service Management** > **Services**.
2. Click **Load**.
3. On the Load Service window, click **Choose File**.
4. Select the snap-in service files to load.
5. Click **Load**.
6. In the Accept End User License Agreement dialog box, click **Accept**.

Removing the ClusterDBMigrationService-3.9.0.3 service

About this task

Use this procedure to uninstall the ClusterDBMigrationService-3.9.0.3 service from each cluster. Perform this procedure before placing the 3.9.0.3 Avaya Breeze® platform nodes back into the cluster. This service is incompatible with 3.9.0.x Avaya Breeze® platform nodes and higher.

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®**.
2. In the navigation pane, click **Service Management** > **Services**.
3. On the Service Management page, select the clusterDBMigrationService-3.9.0.3 service.
4. Click **Uninstall**.
5. From the Confirm Uninstall Service pop-up dialog box, select the cluster or clusters from which you want to remove the service.

   The snap-in status shown on the Service Management page is an aggregated status of snap-in installation across all clusters. Therefore, the status remains **Installed** if you have the snap-in still installed on another cluster.
6. Check that the ClusterDBMigrationService-3.9.0.3 state shows as **Loaded**.

Enabling HTTP load balancing in an Avaya Breeze® platform cluster

About this task

Use this procedure to re-enable load balancer.

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. To enable load balancing for an existing cluster, on the Cluster Administration page, do the following:
   a. Select the check box in front of the cluster.
   b. In the **Cluster State** field, click **Deny New Service**.
   c. Verify that the **Cluster State** column for the cluster is changed to **Denying**.
   d. Click **Edit**.
3. In the Cluster Attributes section, select the **Is Load Balancer enabled** check box to enable load balancing.
4. Click **Commit**.

Replace Avaya Breeze® platform node identity certificates

Avaya Oceana® runs as applications within the Avaya Breeze® platform. For enhanced security, Avaya provides the ability to add or replace Trust and Identity Certificates. Identity Certificates are administered individually for Avaya clusters. Five default Identity Certificates are generated as part of the Avaya OVA deployment process. You can replace a default certificate with a certificate from a well-known Certificate Authority (CA).

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

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

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

Avaya Oceana® Cluster 1 – Identity Certificate Request

Note:

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

The Avaya Oceana® Cluster 1 certificate includes the following:

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

Avaya Oceana® Cluster 2 – Identity Certificate Request

Note:

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

The Avaya Oceana® Cluster 2 certificate includes the following:

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

Avaya Oceana® Cluster 3 – Identity Certificate Request

Note:

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

The Avaya Oceana® Cluster 3 certificate includes the following:

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

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

Replacing the WebSphere certificate

About this task

Use this procedure to replace the WebSphere certificate for Avaya Oceana® cluster 1.

Procedure

1. On the Avaya Aura® System Manager web console, click **Home** > **Services** > **Inventory** > **Manage Elements**.
2. On the **Manage Elements** page, select the check box for the Avaya Breeze® platform node, and click **More Actions** > **Manage Identity Certificates**.
3. On the **Manage Identity Certificates** page, select **WebSphere** and click **Replace**.
4. On the **Replace Identity Certificate** page, do the following:
   a. Select the **Replace this Certificate with Internal CA Signed Certificate** option.
   b. In the **Key Algorithm and Key Size** fields, select the appropriate values. For example, RSA, 2048.
   c. In the **Common Name (CN)** field, use **Avaya Breeze Node Management FQDN**.
   d. In the **Subject Alternative Name** field, select the **DNS Name**.
   e. In the **DNS Name** field, enter the Management FQDN, SIP (SM-100) FQDN of the Avaya Breeze® platform node.
   f. In the **Subject Alternative Name** field, select the IP Address.
   g. In the **IP Address** field, enter the Management, SIP (SM-100) IP address of the Avaya Breeze® platform node.
   h. Click **Commit**.
5. Repeat these steps for all 3 Nodes of Cluster 1.

   WebSphere certificate is only applicable for Cluster1.

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

Procedure

1. On the Avaya Aura® System Manager web console, click **Home** > **Services** > **Security**.

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

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

    The p12 certificate downloads to your **Downloads** folder.
21. On the Avaya Aura® System Manager Web console, click **Services** > **Inventory**.
22. In the left navigation pane, click **Manage Elements**.
23. On the **Manage Elements** page, select an Avaya Oceana® Cluster 1 server/node and click **More Actions** > **Configure Identity Certificates**.
24. On the **Identity Certificates** page, select the **Security Module HTTPS** certificate.
25. Click **Replace**.
26. On the **Replace Identity Certificate** page, select **Import third party certificate**.
27. Click **Choose File**.
28. In the **Password** field, enter the Avaya Oceana® Cluster 1 password used earlier.

29. Click **Retrieve Certificate**.

    The certificate is loaded.

30. Click **Commit**.
31. Replace the Identity Certificate for the other two nodes in Avaya Oceana® Cluster 1 using this same **P12 file**.
32. Reboot the cluster.
33. Wait for the cluster to start before setting to **Acceptance** state.

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

Procedure

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

   Note the user name and password. These are required when creating the certificate.

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

18. Click **Enroll**.

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

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

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

Procedure

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

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

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

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

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

Upgrading the Omnichannel server

Using Windows server 2022 for Omnichannel database

Avaya Oceana® 3.10.0.2 supports Windows server 2022 for Omnichannel database. For upgrading to Windows server 2022, refer to *Upgrading Avaya Oceana®* document.

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**.

Upgrading Standalone Omnichannel server from Avaya Oceana® 3.8.1.1 and later versions to Avaya Oceana® 3.10.0.2 version

Checklist for Omnichannel server upgrade

Use this checklist to upgrade standalone Omnichannel server from Avaya Oceana® 3.8.1.1 and later versions to Avaya Oceana® 3.10.0.2 version.

No.	Task	Notes	✔
1	Download the latest version of the Omnichannel server software on the Omnichannel server.	You can download the latest version of the Omnichannel server software from https://support.avaya.com. The format of the file is `OCEANA_x.x.xxx.iso`.	

Table continues…

No.	Task	Notes	✔
2	Take a backup of the Omnichannel database for failure upgrade.	See Taking a backup of the Omnichannel database on page 38.	
3	Upgrade to the latest version of the Omnichannel server software on the Omnichannel server.	See Upgrading Standalone Omnidatabase on page 38.	

Taking a backup of the Omnichannel database

About this task

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

Procedure

1. Log in to the Omnichannel server.
2. For Avaya Oceana® 3.7 or higher version, go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement` folder.
3. 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.

Upgrading Standalone Omnidatabase

Before you begin

Do the following:

- Take a backup of the Omnichannel database. See Taking a backup of the Omnichannel database on page 38.

- 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 server Campus HA from Avaya Oceana® 3.8.1.1 and later versions to Avaya Oceana® 3.10.0.2 version

Checklist for upgrading Omnichannel server Campus HA

Use this checklist for upgrading Omnichannel server Campus HA from Avaya Oceana® 3.8.1.1 and later versions to Avaya Oceana® 3.10.0.2 version.

No.	Task	Notes	✔
1	Download the latest version of the Omnichannel server software on the Omnichannel server.	You can download the latest version of the Omnichannel server software from https://support.avaya.com. The format of the file is `OCEANA_x.x.xxx.iso`.	
2	Take a snapshot of primary server on vCenter for failure upgrading.	-	
3	Upgrade to the latest version of the Omnichannel server software on the Omnichannel server Campus HA solution.	Upgrading the Omnichannel server software on the Campus HA on page 39.	

Upgrading the Omnichannel server software on the Campus HA

About this task

Use this procedure to upgrade the latest version of the Omnichannel server software on the Omnichannel server Campus HA solution.

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

1. Upgrade Standby server.

2. Perform Switchover.
3. Upgrade Standby server (previously the Primary server).
4. Perform Switchover.

Before you begin

Ensure that the High Availability servers are operational.

Procedure

1. Log in to the Omnichannel standby server and do the following:
   a. Right-click the `OCEANA_x.x.xxx.iso` file.
   b. Click **Mount**.
   c. Run the `AvayaReleasePackInstaller.exe` file.
   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 in to the Omnichannel standby server and 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 in to the Omnichannel Primary Server and 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` file.
   c. Click **Mount**.
   d. Run the `AvayaReleasePackInstaller.exe` file.
   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 in to the Omnichannel Primary server (running as a Standby server now) and 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 in to the Omnichannel DR server.
   b. Right-click the `OCEANA_x.x.xxx.iso` file.
   c. Click **Mount**.
   d. Run the `AvayaReleasePackInstaller.exe` file.
   e. If the installer prompts for server restart, click **Yes** and repeat step (a) though step (d).
   f. Click **Next**.
   g. Click **Accept** on license agreement.
   h. Click **Restart**.

Rebooting Avaya Oceana® clusters

About this task

Use this procedure to reboot Avaya Oceana® clusters.

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®**.
2. In the navigation pane, click **Cluster Administration**.
3. Select the cluster and click **Cluster State** > **Deny New Service**.

4. When the system prompts, click **Continue**.
5. Select the cluster and click **Reboot**.
6. Click **Continue** when the system prompts.

Chapter 5: Post migration tasks

Checklist for Avaya Oceana® 3.10.0.2 post migration

Use the following checklist for the tasks that you must complete after migrating to Avaya Oceana® 3.10.0.2:

No.	Task	Notes	✔
1	Remove all Engagement Designer tasks.	See Removing Engagement Designer tasks on page 44.	
2	Deploy Engagement Designer tasks.	See Deploying Engagement Designer tasks on page 45.	
3	Remove all Engagement Designer workflows.	You can skip this task, if you are migrating from Avaya Oceana® 3.10 and can use the Avaya Oceana® 3.10 workflow. See Removing Engagement Designer workflows on page 46.	
4	Deploy Engagement Designer workflows.	You can skip this task, if you are migrating from Avaya Oceana® 3.10 and can use the Avaya Oceana® 3.10 workflow. See Deploying Engagement Designer workflows on page 46.	
5	Configure the attributes and routing rules of Engagement Designer workflows.	See Configuring the attributes and routing rules of Engagement Designer workflows on page 47.	
6	Upgrade Avaya Control Manager.	Check the product compatibility matrix before the upgrade. Avaya Control Manager 9.1 is compatible with Avaya Oceana® 3.10.0.2. See *Upgrading Avaya Control Manager* documentation on the Avaya Support website at https://support.avaya.com.	

Table continues…

No.	Task	Notes	✔
7	Editing service profiles to add snap-ins.	See Editing service profiles to add snap-ins on page 48.	
8	Configure the reliable eventing group for Avaya Oceana®.	See Creating a Reliable Eventing group on page 48.	
9	Enable Avaya Oceana® to monitor all configured mailboxes.	See Enabling mailboxes on page 49.	
10	Configure Avaya Oceana® to accept contacts.	See Configuring Avaya Oceana to accept contacts on page 50.	
11	Configure Avaya Oceana® to open chatrooms.	Configuring Avaya Oceana to open chatrooms on page 50.	
12	Enable Avaya Oceana® for voice calls.	Enabling Avaya Oceana for voice calls on page 51.	

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.

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**.

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.

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.

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.

Creating a Reliable Eventing group

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Reliable Eventing Administration** > **Dashboard**.
2. On the Reliable Eventing Groups page, click **New**.
3. On the Reliable Eventing Group Editor page, enter the following details:
   - **Cluster**: Select Avaya Oceana® Cluster 1.
   - **Group Name**: Assign a name to the Reliable Eventing group.
   - **Description**: Enter a brief description.
   - **Type**: Select **HA** or **Standalone**.
     - If you select **HA**, you must select at least three Avaya Breeze® platform nodes or brokers. For example, the three Avaya Breeze® platform nodes of Avaya Oceana® Cluster 1.
     - If you select **Standalone**, you must select at least one Avaya Breeze® platform node or broker.
4. In the **Unassigned Brokers** table, click **+** to assign the Avaya Breeze® platform nodes or brokers to the Reliable Eventing group.

5. Click the Associated clusters tab:
   a. In the **Unassigned associated clusters** table, click the **+** icon to add an associated cluster.
   b. In the **Assigned associated clusters** table, click the **X** icon to remove an associated cluster.
6. Click **Commit**.

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

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.

Chapter 6: Fallback procedure

Avaya Oceana® fallback procedure

You can revert to a previous version of Avaya Oceana® if you face any issues with the current version. Before proceeding with the fallback procedure, perform the tasks mentioned in Avaya Oceana 3.10.0.2 pre-migration checklist on page 9.

The following are the ways to perform Avaya Oceana® fallback to the previous release:

Option 1 - Restore cluster1 database backup on previous release and existing Avaya Breeze® platform servers.

- Revert the snapshot to prior to start of migration stage.
- Take Avaya Breeze® platform server, Omnichannel Provider (OCP) database, and Avaya Aura® System Manager snapshots prior to the start of the migration activity.
- Revert the snapshots to prior to start of Avaya Oceana® 3.10.0.2 migration activity.
- Power on the Avaya Aura® System Manager , OCP database and Avaya Breeze® platform servers.
- Restore UCAStoreService, UCMService, Engagement Designer workflow and Quartz database on cluster1.
- Restart the Avaya Oceana® clusters.

Option 2 - Restore cluster1 database backup on fresh install and previous release of Avaya Breeze® platform servers.

- Install the previous release Avaya Breeze® platform servers freshly.
- Revert OCP database to previous release.
- Place Avaya Breeze® platform servers to cluster.
- Restore UCAStoreService, UCMService, Engagement Designer workflow, and Quartz database.
- Restart the Avaya Oceana® clusters.

Chapter 7: Migrating from Avaya Analytics™ 4.x to 4.3.1.1

Avaya Analytics™ migration overview

In Avaya Analytics™, you can migrate data from Avaya Analytics™ Release 4.x to Avaya Analytics™ Release 4.3.1.1.

For information about upgrading Geo lab to Avaya Analytics™ 4.3.1.1, refer to *Avaya Oceana® and Avaya Analytics™ Disaster Recovery and Migration* document.

Note:

If you are on Avaya Analytics™ 4.2 or 4.3 release, then refer *Deploying Avaya Analytics™* document to upgrade your Avaya Analytics™ to Avaya Analytics™ 4.3.1.1.

Avaya Analytics™ version 4.3.1.1 is supported with Avaya Oceana® 3.10.0.2. Hence, you must perform upgrade or migrate with Avaya Analytics™ versions 4.3.1.1.

The migration from Avaya Analytics™ release 3.7.0.2 to Avaya Analytics™ release 4.3.1.1 is not supported. You must migrate Avaya Analytics™ release 3.7.0.2 to release 4.2 Patch 2, then upgrade Avaya Analytics™ release 4.2 Patch 2 to release 4.3.1.1.

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

Supported migration paths

From	To	Considerations
Avaya Analytics™ Release 3.7.0.2 patch 2	Do the following steps: 1. Migrate to Avaya Analytics™ release 4.2 Patch2 2. Upgrade to release 4.3.1.1	You can find patch-related information on the Avaya Support site. For upgrading from Avaya Analytics™ Release 4.2 to Release versions 4.3.1.1, refer to *Upgrading Avaya Analytics™* chapter in *Deploying Avaya Analytics™ for Avaya Oceana®* guide.
Avaya Analytics™ Release 4.0.0.1 latest patch	Do the following steps: 1. Migrate to Avaya Analytics™ release 4.2 Patch 2 2. Upgrade to release 4.3.1.1	
Avaya Analytics™ Release 4.1.0.1 latest patch	Do the following steps: 1. Migrate to Avaya Analytics™ release 4.2 Patch 2 2. Upgrade to release 4.3.1.1	
Avaya Analytics™ Release 4.1.1.0 latest patch	Migrate to Avaya Analytics™ Release 4.3.1.1	
Avaya Analytics™ Release 4.1.2.0 latest patch	Migrate to Avaya Analytics™ Release 4.3.1.1	
Avaya Analytics™ Release 4.2 Patch 2	Upgrade Avaya Analytics™ Release 4.3.1.1	

Migrating from Avaya Analytics™ 4.x to Avaya Analytics™ 4.3.1.1

Avaya Analytics™ 4.x Migration process checklist

Use the following checklist to prepare for the migration of Avaya Analytics™ 4.x to Avaya Analytics™ Release versions 4.3.1.1:

Action	Reference/Notes	✔
Review the prerequisites and optional HA audit requirements.	See the following sections in the *Deploying Avaya Analytics™ for Avaya Oceana®* guide: • VMware requirements for Avaya Common Services Platform • Minimum solution resource requirements for Avaya Common Services Platform • IP address requirements • HA audit requirements	
Download the Avaya Common Services license file and solution license file from PLDS.		
Download the Cluster Control Manager OVA, Cluster Node OVA, and Avaya Analytics™ deployment spreadsheet from the Avaya Support website.		
Gather key configuration information for the deployment.	See the following sections in the *Deploying Avaya Analytics™ for Avaya Oceana®* guide: • Before deploying Cluster Control Manager, see section required information for *Cluster Control Manager deployment.* • Before deploying the Avaya Analytics™, see Required information for *Preparing the deployment spreadsheet* section.	
Install the Avaya Common Services and solution license files.	See section *Installing the license file on System Manager or Avaya WebLM* in the *Deploying Avaya Analytics™ for Avaya Oceana®* guide.	
Prepare Avaya Analytics™ deployment spreadsheet for the single-node migration.	Use a modified deployment spreadsheet for the single-node migration step. See section *Preparing the solution spreadsheet for migration* in this guide.	
Deploy Cluster Control Manager.	See section *Deploying Cluster Control Manager* in the *Deploying Avaya Analytics™ for Avaya Oceana®* guide.	
Deploy the Cluster Node OVA for the single-node cluster.	Deploy a single-node cluster for solution migration. See section *Deploying cluster nodes* in the *Deploying Avaya Analytics™ for Avaya Oceana®* guide.	
Install the single-node migration cluster.		

Table continues…

Action	Reference/Notes	✔
Migrate the Crunchy 2 database to Crunchy 5 on the single-node cluster.	On Cluster Control Manager for the single-node cluster, convert the solution database to the required format.	
Adjust CPU, memory, and SDS disk resources.	If your solution requires, resize the SDS disk on the single-node cluster and edit the VM CPU and memory settings. This process includes gracefully shutting down the solution databases (original and migrated) and powering off the single-node cluster. See section *Adding cluster resources during migration*.	
Take a VMware VM snapshot.	When the cluster node is powered off, take a VMware VM snapshot of Cluster Control Manager and the cluster node. This step is optional.	
Install two more nodes.	See section *Deploying Cluster Nodes* in the *Deploying Avaya Analytics™ for Avaya Oceana®* guide.	
Power on the single-node cluster and Cluster Control Manager.	Ensure that all pods are running as expected before you proceed. Also, ensure that the solution database remains shut down during the entire migration process.	
Migrate from the single-node cluster to a multinode (HA) cluster.	See section *Migrating from the single-node cluster to a multinode (HA) cluster*.	
Enable the HA audit for the migrated cluster.	To configure the HA audit to run on the cluster nodes, run the `ccm infra update-vcenter-creds` command.	
Remove the VMware VM snapshot.	Remove the snapshot you took of the cluster before you migrated it from single-node to multinode (HA). This step is required only if VM snapshot is taken. VMware VM snapshots are supported for cluster nodes only when the nodes are powered off. Keep snapshots for a maximum of 72 hours. Over longer periods, snapshot files increase in size and can degrade performance of the virtual machine and the ESXi host.	

Preparing Avaya Analytics™ deployment spreadsheet for migration

About this task

Use this procedure to prepare a modified version of the Avaya Analytics™ deployment spreadsheet for deploying a single-node cluster for initial migration.

Before you begin

Download the Cluster Control Manager OVA, Cluster Node OVA, and Avaya Analytics™ deployment spreadsheet from the Avaya Support website.

Procedure

1. Select appropriate values in the **Async Messaging** and **Customize Processors to Install** fields.

   Note:

   If the **Async Messaging** and **Customize processors to install** fields are set to `True`, note the updated CPU, memory, and SDS disk size. This information will be used to configure two additional nodes.

2. In the Deployment properties worksheet, in the **Select your install option** field, select `Data Migration`.
3. In the `cluster_config` tab of the deployment spreadsheet, add a single cluster node FQDN for `cluster_fqdn`.
4. Complete the remaining fields as required.

   Note:

   Ensure that all the new passwords match the old ones in the deployment spreadsheet.

Deploying single node cluster

About this task

The steps in this procedure use the vSphere web client connected to vCenter.

Before you begin

- Deploy the Cluster Control Manager. See chapter *Deploying Cluster Control Manager* in the *Deploying Avaya Analytics™ for the Avaya Oceana®* guide.
- Collect the required node information needed for deployment.

Procedure

1. To log in to vCenter, use an account that has deployment permissions.
2. Access the target folder to deploy the cluster node virtual machines.
3. Use the Cluster Node OVA to deploy one VM for a single-node deployment.

Use the values from the table of required node information that you collected.

A centralized storage array with thin provisioning and no encryption is required.

4. Update the CPU, Memory, and SDS disk resource values in deployment properties worksheet in the `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` spreadsheet.
5. Power on cluster node VM.

   Wait for the cluster node to come up.
6. Copy the Avaya Analytics™ deployment spreadsheet on the CCM server.

Next steps

Perform the *Install Avaya Analytics™* procedure in chapter *Deploying Avaya Analytics™ online* under *Deploying Avaya Analytics™ for Avaya Oceana® guide*.

Migrating Avaya Analytics 4.x Crunchy 2 data to Avaya Analytics 4.3.x.x Crunchy 5 data

Setting Source Crunchy 2 Environment

About this task

The data is migrated from the source system that is Avaya Analytics™ 4.x to the target system that is Avaya Analytics™ 4.3.x.x

Using this procedure, you can set up the Crunchy 2 environment in the source system.

Before you begin

A single node cluster is deployed.

Procedure

1. Log in to the Cluster Control Manager (CCM) console of the target system as a customer user.
2. Switch to being the root user by entering the command `su`.
3. Copy the script in the following location from the target system Avaya Analytics™ 4.3.x.x installation to the Source CCM system:

   `/opt/avaya/flex/clusters/<cluster_name>/staging/orca-dbmgr-x.0.x/orca-dbmgr/avaya-flex/bin/release/HAsourcemigrate2to5.sh`

   Here, <cluster_name> is the name of the cluster as defined in the Cluster Properties sheet in the Avaya Analytics™ deployment excel.

   In `orca-dbmgr-x.0.x`, substitute x for the version of orca-dbmgr running in the environment.
4. Log in to the Cluster Control Manager (CCM) console of the source system as the customer user.

5. Switch to being the root user by entering the command `su`.
6. Go to the directory where the script file is copied in the source system. The script file must have required permission.
7. Run the following command:

   `./HAsourcemigrate2to5.sh`

   The IP address and port of warehouse analytics_db and microstrategy database are displayed. Copy this information and store at a secure location, as it can be used in the next steps when required.

   The script takes up to 10 minutes to run after the checks for read-only and master pod status pass, and the script returns the message `Process Complete`.

Setting up target Crunchy 5 environment and migrating the data

About this task

Using this procedure, you can set up a Crunchy 5 environment on the target system that is Avaya Analytics™ version 4.3.1.1. You can perform migration from the source system Crunchy 2 to the target system Crunchy 5.

Before you begin

A single node cluster must be deployed.

A Source system with Crunchy 2 environment must be configured.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Switch to being the root user by entering the command `su`.
3. Run the following script:

   `ccm release orca-dbmgr migration2to5.sh`

4. When prompted, provide the **IP address** and **Port** for the source warehouse **analytics_db**.

   Note:

   Here, you need to enter the IP address and port number which you noted after running **`HAsourcemigrate2to5.sh`** script on the source system.

5. Enter the postgres password for the source database.

   There is a prompt to enter **mstr db password**. Ignore it as the script will not work with mstr db as a source.

6. Select the **Migrate source to target** option, enter the corresponding number.

   This option starts migration from the source system to the target system.

Note:

The migration process on the target system can fail if the script on the source system does not finish its process. If the migration process fails on the target system, go to the source system and ensure that the script **`./HAsourcemigrate2to5.sh`** has successfully completed and shows status as `Process complete`.

In Avaya Analytics™ 4.0.0.1 and 4.1.0.1 releases, while the migration replication process is in progress, the Engagement and Messaging reports are blocked from working on the source system. If the migration process is aborted or completed, these reports will be functional again.

Once the migration process is completed, there is a prompt to enter next option. The data keeps syncing from source system to target system until you run the option **Break link to source make target independent**.

If any errors occur, you need to run option **Cleanup failed attempt** and then run option **Migrate source to target** again.

7. Select **Cleanup failed attempt**, enter the corresponding number.

   This option rolls back all the migration steps in the event of a failure at any point in the process. In the event of a failure in the migration process, you must perform cleanup before running **Migrate source to target** option again.

   Note:

   If you see error on selecting **Cleanup failed attempt** option, it can be because the migration did not complete all the steps. For example,

   If migration process fails at step **Break link to source make target independent** and you run the cleanup, you will see errors trying to clean up next steps because these steps are not completed. You can ignore such an error.

8. Select **Break link to source make target independent**, enter the corresponding number.

   This option notifies the target system to stop copying from source system. It disconnects the source database, which means data coming on the source system will not be synced with the target system.

   You must run this option when you want to move to the target system Avaya Analytics™ version 4.3.1.1. You must ensure that the target system is usable, and a final switchover is needed. You must check the following conditions.

   Before disconnecting the source system, verify that the data is matching in the source system and the target system. You can verify this by running option **Check Migration Status** in another console. Before running **Check Migration Status** in another console, run command **`ccm release orca-dbmgr migration2to5.sh`**.

   Note:

   After running option **Break link to source make target independent**, the new data that comes in the source system is not available in the target system.

9. Select **Check Migration Status**, enter the corresponding number.

   This option performs row counts and database object counts to compare the source system and the target system. Run this option only after the **Migrate source to target** step is completed successfully.

10. Select **Quit**, enter the corresponding number.

    This option is to exit the script.

Migrating the Microstrategy Database

About this task

Using this procedure, you can migrate the Microstrategy database (mstr db) from the source system Crunchy 2 to the target system Crunchy 5.

Perform this procedure on the target DC1.

Before you begin

Source system with Crunchy 2 environment must be configured.

Target system with Crunchy 5 environment must be configured.

Procedure

1. Log in to the Cluster Control Manager (CCM) console in target system as the customer user.
2. Switch to being the root user by entering the command `su`.
3. To find the name of the Crunchy 5 primary pod, run the following command:

   ```
   kubectl get pod -l postgres-operator.crunchydata.com/cluster=analyticsdb,postgres-operator.crunchydata.com/role=master -o name | cut -c 5-
   ```

4. Run the following command into Crunchy 5 primary pod:

   ```
   kubectl exec -it POD_NAME -- /bin/bash
   ```

   Here, replace **`POD_NAME`** with the name of the Crunchy 5 primary pod found in above step.

5. Run the following commands in the primary pod:

   ```
   bash-4.4$ cd pgdata
   bash-4.4$ pg_dump -U postgres -W -f mstr.sql avaya_analytics_md  --if-exists --clean --create -h Microstrategy_HOST -p Microstrategy_PORT
   bash-4.4$ psql -f mstr.sql
   bash-4.4$\l (This lists current databases on the cluster. Verify that avaya_analytics_md is in the list of databases.)
   bash-4.4$ exit
   ```

   Note:

   The second command pg_dump will request a password for mstr postgres db.

   This lists current databases on the cluster. Verify that avaya_analytics_md is in the list of databases.

6. When prompted, enter the Microstrategy host, and port values noted from the output of running the **HAsourcemigrate2to5.sh** script on the source CCM in the Setting Source Crunchy 2 Environment on page 58 section.
7. Run the command **exit** to exit from pod and return to CCM.

Renaming the database

About this task

After the source link is broken on the target system, the analytics_db must be renamed to analyticsdb for Avaya Analytics™ release version 4.3.x.x usage and grant global access permissions.

Before you begin

- Complete Migrating the Microstrategy Database on page 61.
- Ensure to log into the CCM with root user.

Procedure

1. To find the name of the Crunchy 5 primary pod, run the following command:

```
kubectl get pod -l postgres-operator.crunchydata.com/cluster=analyticsdb,postgres-
operator.crunchydata.com/role=master -o name | cut -c 5-
```

2. Run the following command into Crunchy 5 primary pod:

```
kubectl exec -it POD_NAME -- /bin/bash
```

   Here, replace **POD_NAME** with the name of the Crunchy 5 primary pod found in above step.

3. Open the database command prompt with the following psql command:

```
bash-4.4$ psql
psql (11.13)
Type "help" for help.
postgres=#
```

4. Run the following commands to rename the DB and grant permissions:

```
UPDATE pg_database SET datallowconn = false WHERE datname = 'analyticsdb';
UPDATE pg_database SET datallowconn = false WHERE datname = 'analytics_db';
SELECT pg_terminate_backend(pid) FROM pg_stat_activity WHERE datname is not null
AND pid <> pg_backend_pid();
DROP database analyticsdb;
ALTER DATABASE analytics_db RENAME TO analyticsdb;
UPDATE pg_database SET datallowconn = true WHERE datname = 'analyticsdb';
grant temporary, connect on database analyticsdb to public;
grant ALL on database analyticsdb to dbwriterservice;
grant ALL on database analyticsdb to mstruser;
```

5. Run the command **\q** to exit psql.
6. Run the command **exit** to exit the pod and return to CCM.

Preparing Avaya Analytics™ deployment spreadsheet for upscaling single-node cluster

About this task

Use this procedure to prepare the Avaya Analytics™ deployment spreadsheet for increasing footprint resources for migration of single-node cluster (target system) to multinode cluster (HA).

Before you begin

- Deploy single-node cluster for migration.
- Migrate the Avaya Analytics™ Crunchy 2 to Crunchy 5 environment.

Procedure

1. In the Avaya Analytics™ deployment spreadsheet used for single node deployment, in the Deployment Properties worksheet, set the **Select your install options** field to **Upscale single node**.

   The above step enables a migration option that the platform uses to pull the correct software for the upgrade.

   Two more nodes are added to the Deployment Spreadsheet for configuration.
2. In the Deployment Properties worksheet, add **FQDN** and **IP address** for nodes 2 and 3.

Gracefully power off the single-node cluster

About this task

Use this procedure to gracefully power off the single-node cluster (target system).

Before you begin

- Deploy single-node cluster for migration.
- Migrate the Avaya Analytics™ Crunchy 2 to Crunchy 5 environment.
- Prepare Avaya Analytics™ deployment spreadsheet to upscale single-node.

Procedure

1. Log in to the Cluster Control Manager(CCM) as the customer user.
2. Gracefully shutdown the Avaya Common Services database resource and run the following command:

   ```
   pre-infra-upgrade
   ```

   Wait for the command to complete before continuing.
3. Log in to vCenter as an administrator or with the account used to deploy the single-node cluster.
4. Click the **VMs and Templates** tab.
5. Locate and right-click the single-node cluster VM in the folder you designated during your cluster deployment.

6. Right-click the node and click **Power** > **Shut Down Guest OS**.

Next steps

When the cluster node is powered off, take a VMware VM snapshot of Cluster Control Manager and all the cluster nodes. This step is optional.

Increasing resources in single-node cluster

About this task

Use this procedure to increase the CPU, memory, and SDS disk resources in the single-node cluster (target system) during the Avaya Analytics™ migration process.

Before you begin

- Deploy single-node cluster for migration.
- Migrate the Avaya Analytics™ Crunchy 2 to Crunchy 5 environment.
- Prepare Avaya Analytics™ deployment spreadsheet to upscale single-node.
- Power off the single-node cluster.

Procedure

1. To increase CPU and Memory, perform the following steps:
   a. Log in to the vCenter as an administrator or with the account used to deploy the cluster.
   b. Click the **VMs and Templates** tab.
   c. Locate and right-click the single-node cluster VM in the folder you designated during your cluster deployment.
   d. Click the, **Edit** settings.
   e. Increase the CPU/Memory resources as required based on the Footprint Summary table on the **Deployment Properties** sheet in the Avaya Analytics™ deployment spreadsheet.
   f. Click **Ok** to save.
2. To increase SOS disk size, perform the following steps:

   Perform this step if the SDS disk size is different than the Footprint Summary table on the **Deployment Properties** sheet in the Avaya Analytics™ deployment spreadsheet.

   a. Log in to the vCenter as an administrator or with the account used to deploy the cluster.
   b. Click the **VMs and Templates** tab.
   c. Locate and right-click the single-node cluster VM in the folder you designated during your cluster deployment.
   d. Click the, **Edit** settings.
   e. Expand Hard disks.

f. Select **Hard Disk 2**.

g. Enter the virtual hard disk size based on **Disk Storage Requirements** in the Footprint Summary table present in the Deployment Properties sheet.

h. Click **Ok** to save.

Gracefully power on single-node cluster

About this task

Use this procedure to gracefully power on the single-node cluster.

Before you begin

- Deploy single-node cluster for migration.
- Migrate the Avaya Analytics™ Crunchy 2 to Crunchy 5 environment.
- Prepare Avaya Analytics™ deployment spreadsheet to upscale single-node.
- Gracefully power off the single-node cluster.
- Increase the footprint resources in the single-node cluster.

Procedure

1. Log in to the vCenter as an administrator or with the account used to deploy the cluster.
2. Click the **VMs and Templates** tab.
3. Locate and right-click the single-node cluster VM in the folder you designated during your cluster deployment.
4. Right-click the node and click **Power** > **Power On**.
5. Wait for approximately 10 minutes, and then on the CCM, run command **`post-infra-upgrade`** to bring up the database resources.
6. Wait for approximately 7 minutes for pods to come up and storage to sync.
7. To verify all pods are in a Running or Completed state, perform the following steps:
   a. Log in to the Cluster Control Manager (CCM) console as the customer user.
   b. Switch to root user.
   c. Run command **`k get pods`**.

Deploy two cluster nodes

About this task

Deploy two more cluster nodes. For procedure, see chapter *Deploying cluster nodes* in *Deploying Avaya Analytics™ for Avaya Oceana®* guide.

Before you begin

- Deploy single-node cluster for migration.
- Migrate the Avaya Analytics™ Crunchy 2 to Crunchy 5 environment.

- Prepare Avaya Analytics™ deployment spreadsheet to upscale single-node.
- Gracefully power off the single-node cluster.
- Increase the CPU, memory, and SDS disk resources in the single-node cluster.
- Power on the single-node cluster.

Migrating from a single-node cluster to a multinode (HA) cluster

About this task

Use this procedure to complete the Avaya Analytics™ migration from a single-node to a multinode (HA) cluster.

Before you begin

- Single-node cluster is deployed for migration.
- Avaya Analytics™ Crunchy 2 is migrated to the Crunchy 5 environment.
- Avaya Analytics™ deployment spreadsheet is configured to upscale single-node.
- Gracefully powered off the single-node cluster.
- Increased the CPU, memory, and SDS disk resources in single-node cluster.
- Powered on the single-node cluster.
- Deployed two more cluster nodes.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Copy the Avaya Analytics™ deployment spreadsheet on the CCM server.
3. From the directory on CCM that contains the excel file, enter the following command:
   `screen`

   The screen utility enables installation to run in the background.

   Warning:

   Do not skip this step.
4. Power on all cluster node VMs.
5. To perform the infrastructure migration upgrade to HA, run the following command:

   ```
   ccm upgrade spec <Analytics_Excel> --infra --force
   ```

   The `ccm smoke-test` command will not pass after the infra upgrade for the single-node deployment. It will pass after you complete the migration to the full solution when `kube-keepalive-vip` is defined as part of the product upgrade.
6. To verify the status of all the cluster pods and nodes, perform the following steps:
   a. Log in to the Cluster Control Manager (CCM) console as the customer user.
   b. Switch to the root user.

c. To check the current status of all cluster nodes, run the command: **`k get nodes`**. The status should be `Ready`.

d. To check the current status of all cluster pods, run the command: **`k get pods`**. The status should be `Running` or `Completed`.

7. If you are reusing the same FQDN as your original (pre-migration) installation, shut down the original cluster before you proceed to the next step.
8. Initialize any databases that you shut down at the beginning of the migration process.

   Wait until the database resources are available before you proceed to the next step.
9. To perform the product migration upgrade, use the following command:

   ```
   ccm upgrade spec <Analytics_Excel> --products --force
   ```

   Note:

   A product upgrade can take 3 hours to complete. Wait for the upgrade to complete before the next step.
10. **(Optional)** To enable HA audit for the migrated cluster, run the `ccm infra update-vcenter-creds` command.

    This command causes the HA audit to run on the cluster nodes.
11. Remove the VMware VM snapshot that you took before you began this procedure.

    VMware VM snapshots are supported for cluster nodes only when the nodes are powered off. Keep snapshots for a maximum of 72 hours. Over longer periods, snapshot files increase in size and can degrade performance of the virtual machine and the ESXi host.
12. To upscale the Avaya Analytics™ database, run the following command:

    ```
    ccm release orca-dbmgr patch_scaling.py
    ```

    The analyticsdb replica pod (analyticsdb-node-1) should get scheduled on node 2. Both database pods should be in the `Running` state.
13. To verify that the pods are in `Running` state, run the following command:

    ```
    k get pods | grep node
    ```

Restarting orca-dbmgr pod

About this task

Use this procedure to restart the orca-dbmgr pod.

Before you begin

Single-node to multinode cluster migration must be completed.

Upscaling of Avaya Analytics™ database must be completed.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Switch to being the root user by entering the command `su`.
3. To restart the **orca-dbmgr**, use the post install script and do the following steps:
   a. Run the command: `ccm release orca analytics`
   b. Select the option **Troubleshooting** by entering the corresponding number.
   c. Select the option **General** by entering the corresponding number.
   d. Choose the option **Restart Database Manager** by entering the corresponding number.

Note:

It can take a long time for the orca-dbmgr job to complete, depending on the database size. Historical reports may not work if the orca-dbmgr job is not completed.

Restarting mstr-srv pod

About this task

Use this procedure to restart the mstr-srv pod.

Before you begin

Single-node to multinode cluster migration must be completed.

Upscaling of Avaya Analytics™ database must be completed.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Switch to being the root user by entering the command `su`.
3. To update the **MSTR_DEF_ADMIN_PW** to match with **MSTR_ADMIN_PW** in mstr-srv secret, run the following command:

   ```
   k edit secret -n mstr srv-secret
   ```

   Both passwords must be the same.
4. To stop the mstr-srv pod, run the following command:

   ```
   k scale deployment mstr-srv --replicas=0 -n mstr
   ```
5. Wait till complete and then run the following command:

   ```
   k scale deployment mstr-web --replicas=0 -n mstr
   ```

Note:

Ensure that the pods are not shown when executing the command:

```
k get pods -n mstr
```

6. To start the mstr-srv pod, run the following command:

```
k scale deployment mstr-srv --replicas=1 -n mstr
```

7. Wait till complete and then run the following command:

```
k scale deployment mstr-web --replicas=1 -n mstr
```

8. To check if pods are up, run the following command:

```
k get pods -n mstr
```

Note:

mstr-srv pod takes 25 - 30 minutes to get to **Ready (1/1)** state.

Next steps

For more information about certificate creation procedure, see *Post installation tasks* chapter in *Deploying Avaya Analytics™ for Avaya Oceana®* guide.

Verify that all the pods are in a `Running` state.

Chapter 8: Resources

Documentation

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

Table continues…

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

Finding documents on the Avaya Support website

Procedure

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

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

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

8. Click to display the search results.

Avaya Documentation Center navigation

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

Important:

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

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

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

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

You can do the following:

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

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

  You can do the following:

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

Training

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

Table 1: Sales Credentials

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

Table 2: Pre-Sales Design

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

Table 3: Technical Services Partner Credentials

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

Table 4: Pre-requisite Courseware

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

Table 5: End User, Programmer, Administration

Avaya Learning Center				
Course code	**Course title**	**Course duration in hours**	**Delivery type**	**Vanity Link for Attachment**
ALEU-5002 Avaya Oceana® End-User Training				
24020W	Using Avaya Workspaces for Avaya Oceana® - Agent	1.0	Web-based Training	https://www.avaya.com/oceana-agent
24040W	Using Avaya Workspaces for Avaya Oceana® - Supervisor	1.0	Web-based Training	https://www.avaya.com/oceana-supervisor
ALUC-4001 Avaya Breeze® Client SDK				
2410W	Customer Communications and Apps with Oceana® for Developers	3.0	Web-based Training	
ASDC-0010 Avaya Workspaces® Framework				
24150W	Customizing the Avaya Workspaces® Framework	3.0	Web-based Training	
24150T	Avaya Workspaces® Framework R3 Test	1.0	Online Test	
ASAC-0005 Avaya Oceana® Administration				
21160W	Avaya Oceana® Fundamentals	0.5	Web-based Training	
24300V	Administering Avaya Oceana® R3 Omnichannel	40.0	Virtual Instructor-Led Training	Attached with the sale
2430T	Administering Avaya Oceana® R3 Online Test	1.0	Online Test	

Table continues…

Avaya Learning Center				
Course code	**Course title**	**Course duration in hours**	**Delivery type**	**Vanity Link for Attachment**
24320W	Administering Avaya Oceana® - Basic	2.5	Web-based Training	https://www.avaya.com/Oceana-admin
ASAC-0031 Avaya Analytics™ R4 for Oceana® Administrator				
24380T	Administering Avaya Analytics1M R4 for Oceana8 Specialized Test	1.0	Online Test	

Table 6: Other Miscellaneous Courseware

Course code	Course title	Course duration in hours	Delivery type	Vanity Link for Attachment
ALCC-0001 Avaya Workforce Optimization Select Integration with Avaya Oceana® Workspaces				
7014W	Integrating Avaya Workforce Optimization Select with Avaya Oceana® Workspaces	3.0	Web-based Training	
7014A	Avaya Workforce Optimization Select with Avaya Oceana® Workspaces Integration Assessment	1.0	Assessment	
71610W	Integrating POM with Avaya Oceana®	1.0	Web-based Training	

Support

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

Index

N

O

P

R

S

T

U

V

W