Avaya Oceana® and Avaya Analytics™ Disaster Recovery

Release 3.8.1
Issue 3
November 2021

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

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

License types

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

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

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya

including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are 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 Inc.

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

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


Java
POWERED

Contents

Chapter 1: Introduction

Purpose

This document provides information about how to configure Disaster Recovery functionality of Avaya Oceana® and recover after a partial or complete data center outage.

This document is intended for anyone who administers Avaya Oceana®.

Important:

The procedures in this document are applicable to Avaya Oceana® 3.7.x and 3.8.1 with Avaya Analytics™ 3.x. For instructions on Avaya Analytics™ 4.x Disaster Recovery, see *Deploying Avaya Analytics™*.

Change history

Issue	Date	Summary of changes
3	November 2021	Minor updates throughout the guide.
2	April 2021	Minor updates throughout the guide.
1	April 2021	Initial issue for Avaya Oceana® Release 3.8.1.

New in this release

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

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

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

Chapter 2: Overview

Disaster recovery overview

Avaya Oceana® disaster recovery provides a planned approach to re-establish a critical service at a secondary data center when a complete outage occurs at the primary data center. The primary and secondary data centers are installed in the same way. The two data centers are linked for replication such that one becomes the primary and the other becomes the disaster recovery site.

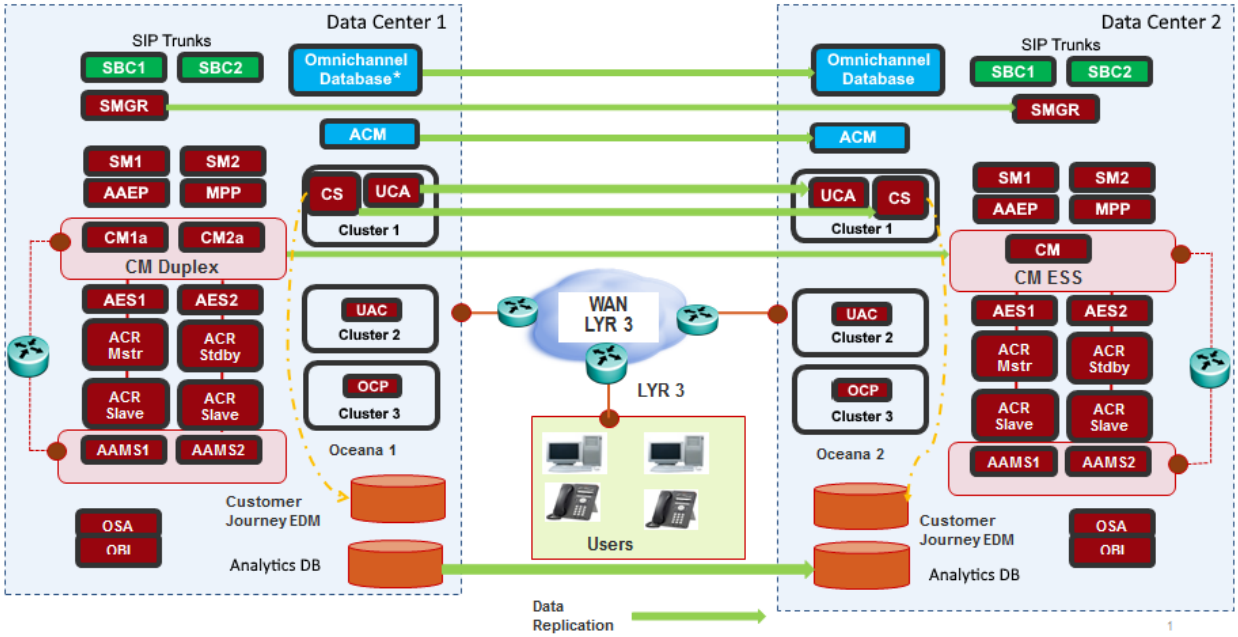
This document provides information about how to configure a geographically redundant Avaya Oceana® so that when a primary data center outage occurs, the redundant site can be made operational. The secondary site has an updated copy of the required administration and reporting data so that operations are not affected.

Note:

This document refers to the primary data center as Data Center 1 and the secondary data center as Data Center 2.

System architecture

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



* Data Center 1 can also have two Omnichannel Databases if you configure it for High Availability.

Chapter 3: Failure modes

Failure modes

Failure mode	Description
Unplanned total outage of Data Center 1	This failure mode involves the failure of Avaya Oceana® Contact Center components and Avaya Aura® Communication Manager telephony infrastructure. This failure mode results in unavoidable system downtime and the loss of all alerting, queued, and in progress contacts.
Planned total outage of Data Center 1	This failure mode involves the controlled manual shutdown of Data Center 1 and switchover to Data Center 2. In this failure mode, Avaya Oceana® supports a maintenance mode. In the maintenance mode, Avaya Oceana® does not add any new contacts to the queue, so that agents can handle the existing queued contacts before the shutdown.
Unplanned total outage of Avaya Oceana® or Avaya Analytics™ components only at Data Center 1. Avaya Aura®, Communication Manager, and other applications remain operational.	This partial disaster recovery failure mode involves the failure of Avaya Oceana® components at Data Center 1 only. In this failure mode, you can switch the Contact Center functionality to Data Center 2 if the Avaya Aura® infrastructure functionality and all other applications remain operational in Data Center 1. Communication Manager and Application Enablement Services components continue to be operational in Data Center 1. This failure mode requires you to reconfigure Avaya Oceana® components at Data Center 2, and ensure that Avaya Oceana® components point to Application Enablement Services at Data Center 2. You must also re-configure Application Enablement Services at Data Center 2 to communicate with Communication Manager at Data Center 1. **Important:** • Do not make any administration changes while Data Center 2 is functioning. If you make any changes, Avaya Oceana® handles the changes in the same manner as if there was an ESS switchover. • This failure mode does not support Avaya WebRTC Connect voice and video calls.

Table continues…

Failure mode	Description
Unplanned total outage of Communication Manager at Data Center 1	This failure mode involves the failure of Communication Manager at Data Center 1. If the failure of Communication Manager results in a switchover to the ESS at Data Center 2, you must manually switch over Avaya Oceana® components to Data Center 2. When you identify the failure of Communication Manager, you must immediately commence the manual switchover of all Avaya Oceana® channels to ensure that Avaya Oceana® voice routing is operational without a delay.
Unplanned partial outage of Avaya Oceana® components at Data Center 1	This failure mode involves the failure of one or more Avaya Oceana® components at Data Center 1. When you identify the failure of an Avaya Oceana® component, you must either recover the component at Data Center 1 or perform one of the following actions: • Partial disaster recovery to Data Center 2. • Full switchover to Data Center 2. When a partial failure occurs, you must determine whether the downtime to recover the components is preferable, or the disruption caused by a partial or full switchover is preferable.
Split WAN	This failure mode involves a WAN outage. Avaya Oceana® does not support an active-active mode of operation. Therefore, if a split WAN occurs, Data Center 1 continues to operate in isolation from Data Center 2. The data replication for Avaya Aura® System Manager, Avaya Control Manager, Unified Collaboration Administration (UCA), and Omnichannel Provider (OCP) breaks temporarily. After the WAN connection is restored, Avaya Oceana® components synchronize data from Data Center 1 to Data Center 2. The synchronization depends on the WAN outage time. Avaya Oceana® components can buffer only a limited number of changes that Data Center 2 synchronizes after recovery. After reaching the buffer limit, Avaya Oceana® components start to overwrite oldest changed records. When an extended WAN outage occurs, you must manually synchronize data from Data Center 1 to Data Center 2.

Limitations

Avaya Oceana® disaster recovery does not support the following:

- Automatic switchover: If a disaster occurs in Data Center 1, you must manually move all operations to Data Center 2. Disaster recovery does not support automatic switchover from Data Center 1 to Data Center 2.
- Call preservation: For planned and un-panned switchovers, not all active voice contacts move with Oceana during the switchover. All existing voice contacts are anchored on the Avaya Communication Manager, these calls follow the existing fallback to Elite mechanism as standard Elite calls.
- Partial switchover: Avaya Oceana® supports only sharing of the following applications between both data centers for partial disaster recovery switchover:
  - Avaya Aura® System Manager primary
  - Avaya Aura® Communication Manager primary
  - Avaya Control Manager primary
  - Application Enablement Services servers in Data Center 2
- Avaya Aura® Communication Manager switchover to ESS: Because it requires corresponding Avaya Oceana® switchover.
- Cross-WAN Application Enablement Services link to ESS: No Device, Media, and Call Control (DMCC) over WAN. Application Enablement Services servers in Data Center 1 must connect to Communication Manager only.

  Note:

  Application Enablement Services servers in Data Center 2 can temporarily connect to the main site Avaya Aura® Communication Manager in a partial disaster recovery failover. For more information, see later sections of this document for setup details and Application Enablement Services network requirements.
- WAN outage scenario: Active-Active mode not available.
- Avaya Aura® Communication Manager: Communication Manager configuration changes while the disaster recovery site is active.

Avaya Oceana® disaster recovery supports a single disaster recovery site, that is, a single ESS. Disaster recovery requires some down time while activating the secondary site. It also mandates that the WAN delay is less than 50 milliseconds for Avaya Control Manager. Some loss of historical reporting data occurs because of the down time.

Chapter 4: Disaster recovery deployment across Data Center 1 and Data Center 2

Introduction

A disaster recovery deployment is the deployment of Avaya Oceana® in two geographically separated data centers, Data Center 1 (DC1) and Data Center 2 (DC2). Avaya Oceana® and Avaya Analytics™ components are installed in each data center with replication of data between a number of elements from DC1 to DC2.

For information about installation instructions of Avaya Oceana® and Avaya Analytics™ components, see:

- *Deploying Avaya Oceana®*
- *Deploying Avaya Analytics™ for Avaya Oceana®*

This document provides procedures and instructions to enable the disaster recovery capabilities from DC1 to DC2.

Deploying Avaya Oceana® components in Data Center 1

Installing Avaya Aura® System Manager in Data Center 1

You must install and configure System Manager in Data Center 1 and enable System Manager replication with the Data Center 2 System Manager. For more information, see *Deploying Avaya Oceana®* and the supporting suite of *Deploying System Manager* documents.

Note:

You must configure trust certificates between System Manager and the customer's LDAP provider on the System Manager in each site.

Configuring Communication Manager, ESS, and Application Enablement Services

You can configure Communication Manager according to the standalone deployment of Avaya Oceana®. For more information, see *Deploying Avaya Oceana®*.

Application Enablement Services servers at Data Center 1 (DC1) communicate only with Communication Manager. Application Enablement Services servers at Data Center 2 (DC2) communicate with the ESS system in non-failover mode.

In a partial DR switchover, Oceana now supports the Application Enablement Services feature called Survivable Hierarchy. This feature allows the DC2 AES Server(s) to be configured with the primary CM as its main CM link and the ESS CM as its failover link. After Survivable Hierarchy is enabled in the DC2 AES, there is no need to manually re-configure the DC2 AES during a partial switchover. This feature allows the DC2 AES to remain in communication with the Communication Manager in DC1. If the DC1 site fails and a full switchover is required, the DC2 AES will automatically failover to the ESS.

Do not use any components from DC2 when DC1 is operational.

- For more information on how to configure Communication Manager and ESS, see Communication Manager documentation.
- For more information on how to configure a standalone Application Enablement Services, see Application Enablement Services documentation.

If Avaya Oceana® is unavailable to process incoming voice calls, you can configure the fallback VDN and vector to provide fallback for voice handling capabilities. For these additional configurations, you must create additional VDNs, vectors, and skills, which you can use when the adjunct route to Avaya Oceana® fails. For more information about fallback configuration, see *Deploying Avaya Oceana®*.

Note:

Avaya Oceana® does not support Application Enablement Services (AES) Geo Redundant High Availability (GRHA).

Installing Omnichannel database server

You can install Omnichannel Windows server in Data Center 1 as a standalone server. For more information about the installation instructions, see *Deploying Avaya Oceana®*.

For the disaster recovery deployment of Avaya Oceana®, database mirroring between the Omnichannel servers in mandatory. For more information, see Omnichannel database mirroring configurations on page 36.

Installing Avaya Control Manager

You can install Avaya Control Manager in Data Center 1 and Data Center 2 and choose an appropriate High Availability (HA) option for your customer deployment. The installation wizard requires specific parameters while installing Avaya Control Manager for an HA deployment. For more information, see *Installing Avaya Control Manager for Enterprise - Legacy High Availability*.

Enabling the Toggle button in Avaya Control Manager

About this task

Use this procedure to enable the Toggle button in the Locations area of Avaya Control Manager on each server.

Before you begin

You must configure the details on the primary Avaya Control Manager server in Data Center 1. The Avaya Control Manager HA replication provides these details into the Avaya Control Manager database in Data Center 2. Ensure that you have access to Avaya Control Manager servers in Data Center 1 and Data Center 2.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **General** > **System Parameters**.
2. Scroll to the bottom and select the **Enable Oceana Disaster Recovery Support** check box.
3. Click **Save**.
4. On the Avaya Control Manager webpage, click **Configuration** > **Locations**.
5. Select the location of your Avaya Oceana® and click **Edit**.
6. On the Location Edit page, click the **Systems** tab.
7. Verify that the **Toggle** button is available next to the **Delete** button on the tool bar.

   This toggle button is used for switching Avaya Control Manager from Data Center 1 to Data Center 2 and vice versa.
8. Expand the width of the browser window and verify that there is a **Switched Over** column to the right-hand side of the browser.

Configuring Data Center 2 application details in the UCA server in Data Center 1

About this task

Use this procedure to configure Data Center 2 application details in the UCA server in Data Center 1.

Before you begin

Enable the Toggle button in Avaya Control Manager on each server to make the Avaya Control Manager 9.x Toggle Button visible in the Locations area of Avaya Control Manager.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Server Details**.
2. Double-click the UCA Server instance of Data Center 1.

   You can view the following details for Data Center 2 by clicking on the tabs on the Avaya Oceana Server Edit page:

   - **Alias**
   - **APU URL**
   - **Avaya Oceana Workspaces Welcome Page URL**
   - **Workspaces Library URL**
   - **Omni Channel Database Server**

   Note:

   Enter the hostname of the VIP if using Omnichannel database mirroring. Otherwise, enter the name of the Omnichannel Database server as administered in the HTTPS certificate installed on the Omnichannel Database server. However, for lab deployments customers you can use IP address.

   To see how to retrieve details of each tab, see *Configuring Avaya Oceana Solution components* chapter in *Configuring Avaya Control Manager* guide.
3. Enter the value for each Data Center 2 applications.
4. Click **Save**.

Configuring Data Center 2 application details in the Analytics server in Data Center 1

About this task

Use this procedure to configure the Data Center 2 application details in the Avaya Analytics™ server.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Customer Engagement** > **Avaya Analytics™**.
2. On the Avaya Analytics Server List page, double-click the Avaya Analytics™ server.

   You can view the following details for Data Center 2 by clicking on the tabs on the Avaya Analytics Server Edit page:

   - **Alias**

- **API URL**
- **Version**
- **Enable Authorization**

3. Enter the value for each Data Center 2 application.
4. Click **Save**.
5. Click the **Streams Servers** tab to add additional details for the stream server.
6. On the Streams Servers page, double-click the **Analytics** row to enter the DR details for the failover server.
7. Enter appropriate values in each of the following fields for the failover server:
   - **Name**
   - **FQDN**
   - **Port**
   - **Alternate FQDN**
   - **TLS Flag**
8. Click **Save**.

Enabling authorization in the Avaya Analytics™ server

About this task

Use this procedure to enable Authorization in the Avaya Analytics™ server if customers have enabled token-based access.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Customer Engagement** > **Avaya Analytics™**.
2. On the Avaya Analytics Server List page, double-click the Avaya Analytics™ server.

   You can view the following details for Data Center 2 by clicking on the tabs on the Avaya Analytics Server Edit page:

   - **Alias**
   - **API URL**
   - **Version**
   - **Enable Authorization**
3. Select **Enable Authorization**.
4. In the **Authorization Service URL** field, enter the appropriate value.
5. In the **ACM instance on Breeeze** field, enter the appropriate value.
6. Click **Save**.

Installing Avaya Oceana® services in Data Center 1

About this task

You must install the following at Data Center 1:

- In Data Center 1, install all required Avaya Oceana® snap-ins.
- In Data Center 1, install all required Engagement Designer tasks and workflows.

Enabling SSL connection for Context Store replication from Data Center 1 to Data Center 2

About this task

Use this procedure to enable Context Store replication from Data Center 1 to the geo-redundant Context Store in Data Center 2.

Note:

Context Store replication functions only when Data Center 1 has the security certificate.

Procedure

1. Download the Root CA certificate to a location from where you can import it to Avaya Oceana® Cluster 1 nodes in Data Center 2.
2. Create a new identity certificate or keystore certificate file signed by your Root CA for the Avaya Oceana® Cluster 1 FQDN and Avaya Breeze® platform nodes in Data Center 2.
3. Log on as a root user and copy the Root CA certificate and generated keystore file to all Avaya Oceana® Cluster 1 nodes in Data Center 2.

   If you use Avaya Aura® System Manager as a CA function, you can retrieve the Root CA certificate as a `.pem` file from the primary System Manager in Data Center 1.

   If you use a third-party CA, consult the CA documentation and procedures for methods to retrieve the CA certificate.

   Context Store replication only functions in one direction from primary Data Center 1 to disaster recovery Data Center 2. Therefore, there is no requirement to repeat this procedure for Avaya Oceana® Cluster 1 nodes in Data Center 1.

Retrieving the System Manager root certificate

About this task

Use this procedure to retrieve the System Manager root certificate.

Before you begin

You must have access to the System Manager console.

Procedure

1. Log in to the Avaya Aura® System Manager web console in Data Center 1.
2. On the System Manager web console, click **Services** > **Security** > **Certificate** > **Authority**.
3. In the navigation pane, click **CA Structures & CRLs**.

   System Manager displays information of your primary System Manager CA certificate.
4. Click **Download PEM file** link to save a copy of System Manager CA certificate to your browser `Downloads` folder.
5. Go to `Downloads` folder and copy the CA certificate to a location that is accessible to Data Center 2 applications.

   You must add the CA certificate file to all Avaya Oceana® Cluster 1nodes in Data Center 2.

Creating a new keystore certificate file

Use this procedure to create a new keystore certificate to enable Context Store replication from Data Center 1 to Data Center 2. This section provides a worked example on how to create a new identity certificate (keystore file) that contains the DC1 Avaya Oceana® Cluster 1 FQDN and all the nodes Management FQDNs, which are used to setup a secure SSL encrypted link between Context Store in Data Center 1 and Data Center 2.

The certificate enforces SSL encryption on the replication channel. For more information on the certificate-based authentication and creation of the keystore certificate, see *Avaya Context Store Snap-in Developer Guide*.

Important:

You must enable SSL encryption for Context Store replication from Data Center 1 to Data Center 2 to work.

There are multiple ways of generating identity certificates for Avaya Oceana® entities. This procedure describes a simple method for creating an identity certificate for Data Center 1 Avaya Oceana® Cluster 1 and its nodes.

The new identity certificate for Data Center 1 Avaya Oceana® Cluster 1 must include the following in the Subject Alternative Name (SAN) fields:

- SAN DNS Name = DC1 Avaya Oceana® Cluster 1 FQDN
- SAN DNS Name = Avaya Oceana® Cluster 1 Node 1 Management FQDN
- SAN DNS Name = Avaya Oceana® Cluster 1 Node 2 Management FQDN
- SAN DNS Name = Avaya Oceana® Cluster 1 Node 3 Management FQDN

Entities that access Avaya Breeze® platform through HTTPS must resolve the Common Name (CN) and SAN fields in the certificate with the FQDNs of the Avaya Breeze® platform node.

To resolve the certificate CN or SAN fields, you must enter the Management FQDN of each Avaya Breeze® platform node in your DNS server. You must also enter DC1 Avaya Oceana® Cluster 1 FQDN in your DNS server.

Modifying end entity profile

About this task

Use this procedure to modify end entity profile to support multiple SAN fields. Avaya Oceana® certificates require more DNS entries than the entries supported by the default settings in System Manager. You can edit the end entity profile to allow additional DNS entries. Alternatively, you can create a new profile with the appropriate number of DNS entries for this certificate.

Procedure

1. On the primary System Manager web console, click **Services** > **Security** > **Certificates** > **Authority**.
2. In the navigation pane, in the RA Functions area, click **End Entity Profiles**.
3. In the **List of End Entity Profiles** field, select the profile that you want to modify and click **Edit End Entity Profile**.

   You can also create a new profile and use it for Avaya Oceana®.
4. Scroll down to the Other subject attributes area.
5. In the **Subject Alternative Names** field, select **DNS Name**.
6. Click **Add**.

   You can continue to add additional DNS name fields to SAN until you add one Avaya Oceana® Cluster 1 FQDN and three node management FQDNs.
7. Click **Save**.

Creating a new keystore certificate file for Data Center 1 of Avaya Oceana® Cluster 1

Procedure

1. On the primary System Manager web console, click **Services** > **Security** > **Certificates** > **Authority**.
2. In the navigation pane, in the RA Functions area, click **Add End Entity**.
3. In the **End Entity Profile** field, select the profile that you modified or created earlier.
4. In the **Username** field, type a user name.
5. In the **Password** field, type a password.

   You must use the user name and password while creating the certificate.
6. In the **CN Common Name** field, enter the full FQDN of DC1 Avaya Oceana® Cluster 1.

7. In the Subject Alternative Name area, in the first **DNS Name** field, enter the FQDN of DC1 Avaya Oceana® Cluster 1.
8. In the next **DNS Name** field, enter the Avaya Oceana® Cluster 1 Node 1 Management full FQDN.
9. In the next **DNS Name** field, enter the Avaya Oceana® Cluster 1 Node 2 Management full FQDN.
10. In the next **DNS Name** field, enter the Avaya Oceana® Cluster 1 Node 3 Management full FQDN.
11. In the **Token** field, select `P12 file`.
12. Click **Add**.
13. Open System Manager public web portal.
14. On the left panel, click **Public Web**.

    System Manager displays the public web portal for CA functionality.
15. In the web portal, on the **Enroll** menu, click **Create Keystore**.
16. Enter the **Username** and **Password** for the end entity certificate that you created.
17. From the **Key Length** list, select `2048` or `4096`.
18. Click **Enroll**.

    The p12 certificate (keystore file) is downloaded to the `Downloads` folder in your browser.
19. Save the p12 and CA root certificates to a location that is accessible from Data Center 2. These files are copied to all Avaya Oceana® Cluster 1 nodes in Data Center 1.

Adding CA root certificate and keystore certificate files to Data Center 2 Cluster 1 nodes

About this task

Use this procedure to copy the CA Root certificate and the newly created keystore file to all Avaya Breeze® platform nodes in Data Center 2 Cluster 1.

Procedure

1. Log in to the Avaya Oceana® Cluster 1 Node 1 as the `cust` user and change to the root user.
2. As a root user, go to `/opt/Avaya/dcm/gigaspace/security/` folder and copy the following:
   - CA Root Certificate
   - Newly generated Keystore certificate file for the Avaya Oceana® Cluster 1 nodes in DC1.

3. Repeat Step 1 and Step 2 for the other two nodes in Data Center 2 Avaya Oceana® Cluster 1.

Enabling Context Store integration to External Data Mart in Data Center 1

About this task

Use this procedure to enable Context Store integration to External Data Mart (EDM) in Data Center 1.

Before you begin

Create database tables in the EDM database. For more information, see *Avaya Context Store Snap-in Reference*.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. In the **Cluster** field, click Avaya Oceana® Cluster 1.
   b. In the **Service** field, click **ContextStoreManager**.
   c. Scroll down to the External Data Mart Configuration area.
   d. In the **EDM: Enable Persistence to database** field, type `true`.
   e. Configure the other EDM attributes.

      For more information, see *Avaya Context Store Snap-in Reference*.
   f. Enter an appropriate value in each of the following fields:
      - **ContextStore ManagerSpace DataGrid Settings**
      - **ContextStoreSpace DataGrid Settings**
      - **EDM: Mirror Service container size**
3. Click **Commit**.

Setting cluster activity status for clusters in Data Center 1

Before you begin

You must install OceanaMonitorService on the clusters in Data Center 1 as a troubleshooting tool to validate Avaya Oceana® health state of the snapins and PU's.

Procedure

1. Enter the following URL `https://<DataCenter1_AvayaOceanaCluster1_FQDN>/services/OceanaMonitorService/manager.html?affinity=)` in your web browser to open the Oceana Manager page.

   Important:

   You can create a bookmark of this URL in your web browser, so that you can open the Oceana Manager page when System Manager is unavailable.

   To change the global status of the Avaya Oceana® and Avaya Breeze® platform Clusters in Data Center 1 or Data Center 2, you need to access the Oceana Manager page.

2. **(Optional)** To open the Oceana Manager page through System Manager, do the following:
   a. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
   b. On the Cluster Administration page, in the **Service URL** column for Avaya Oceana® Cluster 1, select **Oceana Manager**.
3. Log in to Oceana Manager using an Admin account.
4. On the Oceana Manager page, do the following:
   a. Check the status of the clusters.
   b. If the status of the clusters is `STANDBY`, click **Set Cluster Group to Active** to change the status to `ACTIVE`.
   c. On the confirmation message box, click **OK**.
   d. **(Optional)** If the Oceana Manager page does not display the updated status after some time, click **Refresh**.

Configuring Oceana Monitor authorization

About this task

Use this procedure to configure Oceana Monitor Authorization so that you can use Oceana Manager to switch between Data Center 1 and Data Center 2.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. In the **Cluster** field, click DC1 Avaya Oceana® Cluster 1.
   b. In the **Service** field, click **OceanaMonitorService**.

3. In the Run-time Service Configuration area, in the **Authorization Required to access Oceana Manager** field, do the following:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, select `true`.
4. Identify **Oceana Authorization Cluster IP** and do the following:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, enter the FQDN or IP address of the cluster that hosts the AuthorizationService snap-in in Data Center 1.
5. Click **Commit**.

Setting disaster recovery attributes in OceanaConfiguration snap-in for Data Center 1 UCAStoreService and Context Store

About this task

Use this procedure to centrally configure the disaster recovery attributes for the UCAStoreService and Context Store snap-ins from the OceanaConfiguration snap-in. In the previous versions of Avaya Oceana®, these attributes were set on the individual snap-ins.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. In the **Cluster** field, click DC1 Provisioning Cluster.
   b. In the **Service** field, click **OceanaConfiguration**.
3. In the Geo-Redundancy area, in the **Disaster Recovery Mode** field, do the following:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, select `GEO Primary`.
4. Identify **Geo-Redundant Common Cluster** and do the following:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, select Avaya Oceana® Cluster 1 that you created in DC2, which is hosting the DR (DC2) UCAStoreService and Context Store snap-ins.
5. Identify the attribute **Keystore File Name** and do the following:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, enter the name of the keystore file required for Context Store replication.

For more information, see Creating a new keystore certificate file on page 22 and Enabling SSL connection for Context Store replication from Data Center 1 to Data Center 2 on page 21.

6. Identify the attribute **Keystore Password** and do the following:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, enter the password that you used when creating the keystore file containing the security certificate for DC2 Avaya Oceana® Cluster 1 nodes.
7. Click **Commit**.
8. Reboot Avaya Oceana® Cluster 1 in Data Center 1.

   You can reboot Cluster 1 after configuring Avaya Oceana® components in Data Center 2.

Updating Engagement Designer during disaster recovery

In a disaster recovery deployment, whenever you update an Engagement Designer workflow in Data Center 1, you must export the workflow and import it in Data Center 2 through Engagement Designer console.

Note:

For all operations in Data Center 2, before starting Engagement Designer console, you must temporarily take the Avaya Oceana® Cluster 1 out of the Denying mode.

Deployment of Avaya Oceana® components in Data Center 2

Installing Avaya Aura® System Manager in Data Center 2

You can install and configure System Manager in Data Center 2 as a Geo standby server for the primary System Manager. For more information, see *Deploying Avaya Oceana®* and the supporting suite of *Deploying System Manager* guides.

Note:

You must configure trust certificates between System Manager and the LDAP provider on both instances of System Manager.

Installing services in Data Center 2

Procedure

1. Verify that all the Avaya Breeze® platform nodes in Data Center 2 are in the Denying state.

   For instruction about how to verify the status of Avaya Breeze® platform nodes, see *Deploying Avaya Oceana®*.

2. In Data Center 2, install the same set and same version of the services that you installed in Data Center 1.
3. In Data Center 2, install the same set of Engagement Designer tasks and flows that you installed in Data Center 1.

   For both data centers, you can verify the services from System Manager in Data Center 1.

Configuring Oceana Monitor authorization

About this task

Use this procedure to configure Oceana Monitor Authorization so that you can use Oceana Manager to switch between Data Center 1 and Data Center 2.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. In the **Cluster** field, click DC2 Avaya Oceana® Cluster 1.
   b. In the **Service** field, click **OceanaMonitorService**.
3. In the Run-time Service Configuration area, in the **Authorization Required to access Oceana Manager** field, do the following:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, select `true`.
4. Identify **Oceana Authorization Cluster IP** and do the following:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, enter the FQDN or IP address of the cluster that hosts the AuthorizationService snap-in in Data Center 2.
5. Click **Commit**.

Setting disaster recovery attributes

About this task

Use this procedure to set disaster recovery attributes in OceanaConfiguration snap-in for Data Center 2 UCAStoreService and Context Store.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. In the **Cluster** field, click DC2 Provisioning Cluster.
   b. In the **Service** field, click **OceanaConfiguration**.
3. In the Geo-Redundancy area, in the **Disaster Recovery Mode** field, do the following:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, select `GEO Secondary`.
4. Identify **Geo-Redundant Common Cluster** and do the following:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, select Avaya Oceana® Cluster 1 that you created in Data Center 1, which is hosting the primary UCAStoreService and Context Store snap-ins.
5. Identify the attribute **Keystore File Name** and do the following:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, enter the name of the keystore file.

      CA signed certificate for the DR Cluster 1 and its nodes required for Context Store replication.

      For more information, see Creating a new keystore certificate file on page 22 and Enabling SSL connection for Context Store replication from Data Center 1 to Data Center 2 on page 21.
6. Identify the attribute **Keystore Password**, and do the following:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, enter the password that you used when creating the keystore file containing the security certificate for DC2 Avaya Oceana® Cluster 1 nodes.
7. Click **Commit**.
8. Reboot Avaya Oceana® Cluster in Data Center 1.

   You can reboot Cluster 1 after configuring Avaya Oceana® components in Data Center 2.

Setting the cluster activity status for the clusters in Data Center 2

Before you begin

You must install OceanaMonitorService on the clusters in Data Center 2.

Procedure

1. Open the Oceana Manager page by entering the following URL in your web browser:

   `https://<DataCenter2_AvayaOceanaCluster1_FQDN>/services/OceanaMonitorService/manager.html?affinity=)`

   Important:

   You can create a bookmark of this URL in your web browser, so that you can open the Oceana Manager page even when System Manager is unavailable.

2. **(Optional)** To open the Oceana Manager page through System Manager, do the following:
   a. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
   b. On the Cluster Administration page, in the **Service URL** column for Avaya Oceana® Cluster 1, select **Oceana Manager**.
3. Log in to Oceana Manager using an Admin account.
4. On the Oceana Manager page, do the following:
   a. Check the status of the clusters.
   b. If the status of the clusters is `ACTIVE`, click **Set Cluster Group to Standby** to change the status to `STANDBY`.
   c. On the confirmation message box, click **OK**.
   d. **(Optional)** If the Oceana Manager page does not display the updated status after some time, click **Refresh**.
   e. Verify that all clusters and nodes in Data Center 2 are now in the `Deny` state.

Unified Collaboration Administration data synchronization

Unified Collaboration Administration (UCA) data replication handles data added after the replication is enabled. If the UCA instance in Data Center 1 contains data, you must perform a manual backup and restore to restore the data from Data Center 1 to Data Center 2. After the backup and restore is done, ensure that the two UCA instances are in an initial synchronized state.

Preparing Data Center 2 for UCA restore from Data Center 1

About this task

Use this procedure to prepare the Avaya Oceana® deployment in Data Center 2 for the UCAStoreService database restore from Data Center 1. The UCAStoreService database contains all the information related to users, accounts, attributes, providers, and resources that is common to Data Center 1 and Data Center 2 in Avaya Oceana® disaster recovery deployment.

Note:

You can perform the following procedure at any time before enabling UCAStoreService replication and it does not affect the operation of the systems in Data Center 1.

Procedure

1. On the DC1 System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
2. Select the check box for **UCAStoreService** and click **Uninstall**.
3. In the pop-up window, select the **Oceana Cluster 1 in the DC2** site (DR location).

   Do not uninstall UCAStoreService from the Data Center 1 (primary site).
4. Click **Yes** to the confirmation dialog box.

   You can use the System Manager web console to monitor progress of uninstallation of UCAStoreService from DC2 Avaya Oceana® Cluster 1.
5. After complete uninstallation, reboot DC2 Avaya Oceana® Cluster 1 to ensure that the UCAStoreService PUs are completely removed.
6. After reboot, verify that all Avaya Oceana® services in DC2 are deployed and ready for the UCAStoreService database restore procedure.

Taking a backup of UCAStoreService on Data Center 1

About this task

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

Note:

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

Procedure

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

2. From the **Backup and Restore** field, select **Configure**.

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

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

```
SSH connection ok.
Backup directory ok.
File transfer test ok.
File remove test ok.
```

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

    Note:

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

    System Manager displays the Cluster DB Backup page.
15. Select the **UCAStoreService** check box.
16. In the **Backup Password** field, enter a password for the backup.

    Important:

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

Restoring the UCAStoreService data

About this task

Use this procedure to restore the UCAStoreService data from DC1 to the Avaya Oceana® Cluster 1 in DC2.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
2. On the Services page, click the UCAStoreService to verify that the service is not in the `Installed` state in the DR cluster.
3. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
4. From the **Backup and Restore** field, select **Restore**.
5. On the Backup and Restore Status page, in the Backup and Restore Jobs section, select the check box of the latest backup file and click **Restore**.
6. In the Cluster Database Restore Confirmation dialog box, select Avaya Oceana® Cluster 1 and click **Continue**.
7. On the Backup and Restore Status page, ensure that the **Status** column for the restore operation displays the value `Completed`.
8. Reboot Avaya Oceana® Cluster 1 in DC2.

Installing UCAStoreService

About this task

Use this procedure to install UCAStoreService on Avaya Oceana® Cluster 1 in DC2.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
2. On the Services page, select the check box of UCAStoreService and click **Install**.
3. In the Confirm Install service: UCAStoreService dialog box, select the check box of Avaya Oceana® Cluster 1 and click **Commit**.
4. On the Services page, verify that the state of the service is `Installing`.

   The state changes to `Installed` when the installation is complete.
5. Restart the Avaya Breeze® platform nodes of Avaya Oceana® Cluster 1.

   Ensure that you select Cluster 1 on the DR site.

Installing the Omnichannel database server in Data Center 2

You must install Omnichannel Windows Server in Data Center 2 as a standalone server. For details, see *Deploying Avaya Oceana®*.

Installing Avaya Control Manager in Data Center 2

The installation of Avaya Control Manager is customized for High Availability (HA). The installation wizard requires specific parameters while installing Avaya Control Manager for an HA deployment. For more information, see *Installing Avaya Control Manager in an Enterprise Solution*.

You must install an instance of Avaya Control Manager in Data Center 2 and enable all the required functionality according to Data Center 1.

Updating Engagement Designer during disaster recovery

In a disaster recovery deployment, whenever you update an Engagement Designer workflow in Data Center 1, you must export the workflow and import it in Data Center 2 through Engagement Designer console.

Note:

For all operations in Data Center 2, before starting Engagement Designer console, you must temporarily take the Avaya Oceana® Cluster 1 out of the Denying mode.

Web voice and web video requirements

Web voice and video is an optional configuration in Avaya Oceana® deployments. You can skip these procedures if there is no web voice or video required in the solution.

The following are the requirements for web voice and web video:

- Deploy the Web Voice and Web Video solution in Data Center 1 and Data Center 2 and ensure that each data center has its own Disaster Management Zone (DMZ).
- Configure web and mobile clients with the FQDNs of the Authorization token service, AvayaMobileCommunications cluster, and Avaya Aura® Web Gateway server.
- Configure DNS to map the FQDNs to the public addresses exposed on the active data center.

You can switchover a data center by changing the DNS mapping to the alternative data center. For example:

- Initial DNS mapping in Data Center 1:
  - FQDN of the Authorization token service is mapped to the public address of the Authorization token service in Data Center 1.
  - FQDN of the Avaya Aura® Web Gateway server is mapped to the public address of the Avaya Aura® Web Gateway server in Data Center 1.
  - FQDN of the AvayaMobileCommunications cluster is mapped to the public address of the AvayaMobileCommunications cluster in Data Center 1.
- DNS mapping for switchover in Data Center 2:
  - Change the DNS mapping of the Authorization token service FQDN to map to the public address of the Authorization token service in Data Center 2.
  - Change the DNS mapping of the Avaya Aura® Web Gateway server FQDN to map to the public address of the Avaya Aura® Web Gateway server in Data Center 2.
  - Change the DNS mapping of the AvayaMobileCommunications cluster FQDN to map to the public address of the AvayaMobileCommunications cluster in Data Center 2.

Omnichannel database mirroring configurations

Avaya Oceana® supports the following two options for Omnichannel Database:

- Omnichannel Campus HA with DR
- DR deployment

Depending on these options, you can choose the appropriate procedures to enable Omnichannel database mirroring from Data Center 1 to Data Center 2.

Note:

- Ensure full hostname and FQDN resolution between Data Center 1 and Data Center 2.
- Cache Mirroring traffic between Data Center 1 and Data Center 2 is 60 MB per second of journal data at peak. The round trip time between Data Center 1 and Data Center 2 is 50 milliseconds maximum.
- Do not disable Internet Control Message Protocol (ICMP) on any system configured as a mirror member. Cache Mirroring relies on ICMP to detect whether or not members are reachable.

Omnichannel Database mirroring for primary and DR site deployments

Checklist for configuring Cache Mirroring with a backup server

Use the following checklist to configure Cache Mirroring with a backup server in DC1:

No.	Task	Description	✔
1	Configure Cache Mirroring on the active Omnichannel Database server in Data Center 1.	See Configuring Cache Mirroring on the active Omnichannel Database server in Data Center 1 on page 37.	
2	Configure Cache Mirroring on the backup Omnichannel Database server in Data Center 2.	See Configuring Cache Mirroring on the backup Omnichannel Database server in Data Center 2 on page 39.	
3	Secure the Cache Mirror on the active Omnichannel Database server in Data Center 1.	See Securing the Cache Mirror on the Omnichannel Database server in Data Center 1 and Data Center 2 on page 40.	

Configuring Cache Mirroring on the active Omnichannel Database server in Data Center 1

About this task

Omnichannel Database utilizes the Cache Mirroring feature to replicate the Cache data between Data Center 1 and Data Center 2.

Procedure

1. Navigate to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement` folder.
2. Double-click the `OceanaDataManagementTool.exe` file.
3. Navigate to **Configuration** > **Mirror Settings** > **Create Mirror**.
4. Enter the details for **Arbiter address**, **Virtual IP** and **Network Interface**.
5. Select the **Require SSL/TLS** checkbox to **Set up SSL/TLS** .
    a. In the **File containing trusted Certificate Authority X.509 certificate**, field enter the location of your CA.

b. In the **File containing this configuration's X.509 certificate** field, browse and select the server certificate.
c. In the **File containing associated private key** field, browse and select the key.
d. In the **Private key password** field, enter the new password

6. Start the Windows Services application by doing the following:
   a. Click **Start** > **Run**.
   b. In the Run dialog box, type `services.msc`.
   c. Click **OK**.
7. In the Services window, do the following:
   a. Double-click the ISCAgent service.
   b. Click the **Recovery** tab.
   c. In the **First failure**, **Second failure**, and **Subsequent failures** fields, select the **Restart the Service** option.
   d. In the **Reset fail count after** field, type `120`.
   e. In the **Restart service after** field, type `0`.
   f. Click **Apply**.
   g. Click **OK**.
8. In the Oceana Data Management utility, click **Backup And Restore**.
9. In the navigation pane, click **Backup And Restore**
10. In the **Select/create file to backup to** field, click **Browse**.
11. On the Save As screen, do the following:
    a. Select the location where you want to save the backup file.

       Do not save the backup file to the software, journal, or multimedia drive.
    b. Specify a name for the backup file. When naming the file, use English or numeric characters only.
    c. Click **Save**.
12. Click **Backup Database**.

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

Configuring Cache Mirroring on the backup Omnichannel Database server in Data Center 2

Procedure

1. Navigate to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement` folder.
2. Double-click the `OceanaDataManagementTool.exe` file.
3. Navigate to **Configuration** > **Mirror Settings** > **Join Mirror**.
4. In the **Type** attribute, select **Disaster Recovery**.
5. Type the IP address of the agent and select **Virtual address interface**.
6. If SSL is configured on the primary server select the **Require SSL/TLS** checkbox to set up SSL/TLS.
    a. In the **File containing trusted Certificate Authority X.509 certificate**, field enter the location of your CA.
    b. In the **File containing this configuration's X.509 certificate** field, browse and select the server certificate.
    c. In the **File containing associated private key** field, browse and select the key.
    d. In the **Private key password field**, enter the new password.
7. Start the Windows Services application by doing the following:
    a. Click **Start** > **Run**.
    b. In the Run dialog box, type `services.msc`.
    c. Click **OK**.
8. In the Services window, do the following:
    a. Double-click the ISCAgent service.
    b. Click the **Recovery** tab.
    c. In the **First failure**, **Second failure**, and **Subsequent failures** fields, select the **Restart the Service** option.
    d. In the **Reset fail count after** field, type `120`.
    e. In the **Restart service after** field, type `0`.
    f. Click **Apply**.
    g. Click **OK**.
9. Copy the backup file from the active Omnichannel Database server in Data Center 1 to the backup Omnichannel Database server in Data Center 2.
10. In the Oceana Data Management utility, click **Backup And Restore**.
11. In the navigation pane, click **Backup And Restore**
12. In the **Select file to restore from** field, click **Browse**.

13. On the Open dialog box, do the following:
    a. Browse to the location where you stored the backup file.
    b. Select the backup `cbk` file.
    c. Click **Open**.
14. Click **Restore Database**.
15. For **Are you restoring a mirrored backup**, click **Yes**.
16. Click Restore

    Note:

    If data is submitted to the Data Center 1 database after the backup, this data is not lost once the replication starts from Data Center 1 to Data Center 2.

    The system displays the `Restore complete!` message after the restore process is completed.
17. To verify whether the restore was successful, do the following:
    a. On Cache Management Portal, click **System Operation** > **Mirror Monitor**.
    b. Click **Details**.

    Verify both Avaya Oceana® databases in the list.

Securing the Cache Mirror on the Omnichannel Database server in Data Center 1 and Data Center 2

About this task

This procedure is only required if SSL/TLS secure connections are needed to and from the Omnichannel Database servers.

Before you begin

Configure Cache Mirroring on the active Omnichannel Database server in Data Center 1 and Data Center 2.

Procedure

1. On Primary server in DC1 do the following
    a. Navigate to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement` folder.
    b. Double-click the `OceanaDataManagementTool.exe` file.
    c. Navigate to **Configuration** > **Mirror Settings** > **Create Mirror**
    d. Select the **Require SSL/TLS** checkbox.
        - In the **File containing trusted Certificate Authority X.509 certificate** field, enter the location of your CA.

- In the **File containing this configuration's X.509 certificate** field, browse and select the server certificate.
- In the **File containing associated private key** field, browse and select the key.
- In the **Private key password** field, enter the new password.

e. Click **Save** or **Update** button.

2. Go to async server in DC2 and do the following:
   a. Navigate to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement` folder.
   b. Double-click the `OceanaDataManagementTool.exe` configuration file.
   c. Navigate to **Configuration** > **Mirror Settings** > **Join Mirror**
   d. Select the **Require SSL/TLS** checkbox.
      - In the **File containing trusted Certificate Authority X.509 certificate** field, enter the location of your CA.
      - In the **File containing this configuration's X.509 certificate** field, browse and select the server certificate.
      - In the **File containing associated private key** field, browse and select the key.
      - In the **Private key password** field, enter the new password.

   e. Click **Save** or **Update** button.
3. Go back to primary server on DC1.
   a. In your web browser, enter the following URL to open Cache Management Portal:

      http://<DC1OmnichannelServerIP>:57772/csp/sys/UtilHome.csp

      <DC1OmnichannelServerIP> is the IP address of the active Omnichannel Database server

      in Data Center 1.
   b. On the Cache Management Portal login page, do the following:
      - In the **User Name** field, type the user name.
      - In the **Password** field, enter the password.
      - Click **Login**.

   c. On Cache Management Portal, click **System Administration** > **Configuration** > **Mirror Settings** > **Edit Mirror**.
   d. On the Edit Mirror page, look for **Pending New Members** section.
   e. Tick the async server and select **Authorize**.
   f. Select **Ok**.

Checklist for configuring Cache Mirroring with failover and backup servers

Use the following checklist to configure Cache Mirroring with failover and backup servers:

No.	Task	Description	✔
1	Configure Omnichannel Database High Availability (HA) with active and standby Omnichannel Database servers within Data Center 1.	See *Deploying Avaya Oceana®*.	
2	Secure the Cache Mirror on the active Omnichannel Database server in Data Center 1 and Data Center 2.	See Securing the Cache Mirror on the Omnichannel Database server in Data Center 1 and Data Center 2 on page 40.	
3	Authorize the backup Cache Mirror on the active Omnichannel Database servers in Data Center 1.	See Authorizing the backup Cache Mirror on the active Omnichannel Database server in Data Center 1 on page 42.	

Authorizing the backup Cache Mirror on the active Omnichannel Database server in Data Center 1

About this task

Use this procedure to authorize the other Cache Mirror(s) on the active Omnichannel Database server in Data Center 1. This procedure is only required if SSL/TLS secure connections are configured between the Omnichannel Database servers.

Before you begin

- Securing the Cache Mirror on the Omnichannel Database server in Data Center 1 and Data Center 2 on page 40

Procedure

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

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

   <ActiveOmnichannelServerIP> is the IP address of the server containing the active Omnichannel Database.

2. On the Cache Management Portal login page, do the following:

   a. In the **User Name** field, type `_admin`.

b. In the **Password** field, type `Oceana16`.

c. Click **LOGIN**.

3. On Cache Management Portal, click **System Operations** > **Mirror Monitor**.
4. Under the Authorized Async Members section, click **Add**.
5. Specify the backup Cache Mirror name and the distinguished name in the fields

   You can get these values in one of the following locations from the Cache Management Portal on the other Omnichannel Database servers depending on mirror type:

   System Administration > **Configuration** > **Mirror Settings** > **Edit Async**.

   System Administration > **Configuration** > **Mirror Settings** > **Edit Mirror**.
6. Click **Save**.

Restarting Data Center 1 Avaya Oceana® clusters

For a disaster recovery deployment, you must reboot all the Avaya Oceana® clusters in Data Center 1.

Use Oceana Monitor and other System Manager web console indicators to determine when the system is fully operational.

After the reboot, you can verify the replication status of UCAStoreService and Context Store.

Verifying the UCA replication status

About this task

Use this procedure to verify that the UCA replication is operational.

Note:

The UCA replication check does not work with the Token-based access turned on. To perform the check, you must temporarily turn off the Token-based authorization using Avaya Control Manager. After verifying the UCA replication status, you can re-enable the Token-based authorization access to UCA.

To verify UCA replication is functioning between primary and disaster recovery (DR) sites, you must make an administrative change in the primary Avaya Control Manager application and submit the change to the primary UCA instance. This change is then replicated from the primary UCA to the DR UCA. Using a browse http/https request, you can verify the change in each UCA instance. You must add a new test attribute to Avaya Oceana® and verify that this is replicated across the DR UCA instance.

Important:

You must ensure that there are no active UCA alarms. If there are any active UCA alarms, you must resolve them before the switchover.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. In the drop-down list next to Primary Avaya Oceana® Cluster 1, select **Oceana Monitor**.
3. On the Monitor Service page, click **Cluster 1** > **Grid Info** and wait for the pop up to display the status of all snap-in PUs.
4. Verify that the PU **ucaStoreSpace-GATEWAY** is present with status `INTACT`.

   If it is not present or has a status `Scheduled` or `Broken`, then it indicates that the UCA replication is not operational. You must resolve this issue before proceeding with the switchover.
5. Repeat steps 1 to 4 for Avaya Oceana® Cluster 1 in Data Center 2.

   Perform the subsequent steps only after successfully completing until step 5.
6. Log on to the primary Avaya Control Manager server instance.
7. Add a new test attribute and save it to the primary UCA instance.
8. Using the following URL, verify that the new attribute appears in the response from the URL request: `http(https)://<<primary cluster 1 FQDN>/services/UCAStoreService/uca/attributes`
9. Repeat this URL test for the Avaya Oceana® DR system using a similar request:

   `http(https)://<<DR cluster 1 FQDN>/services/UCAStoreService/uca/attributes`

   If your test attribute does not appear in the responses from both URL UCA requests, this indicates that the UCA replication is not operational from primary to DR or the request to save a new attribute to the primary UCA server is not operational. Troubleshoot any of these issues before proceeding with the switchover.
10. Check for any replication errors alarmed on System Manager.
    a. Go to **Services** > **Events** > **Alarms**.
    b. Click **Advanced Search**.
    c. In the Criteria section, select **Description contains Replication**.
    d. Click **Search**.

    Important:

    You must ensure that there are no active alarms. If there are any recent alarms, then you must investigated the issue to ensure replication is operational before a switchover.

Verifying Context Store replication status

About this task

To verify if Context Store replication is functioning between primary and DR sites, you can use Oceana Monitor to validate the presence of the Context Store replication gateway PU.

You must check if there are any EDM Replication error alarms in System Manager Alarm Viewer. You must also create a context to verify that replication is working.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. In the drop-down list next to the Primary Avaya Oceana® Cluster 1, select **Oceana Monitor**.
3. On the Monitor Service page, click **Cluster 1** > **Grid Info** and wait for the pop-up to display the status of all snap-in PUs.
4. Verify that the PU **cs-gateway** is present with status `INTACT`.

   If it is not present or has a status `Scheduled` or `Broken`, then it indicates that the Context Store replication is not operational. You must resolve this issue before proceeding with the switchover.
5. Repeat steps 1 to 4 for Avaya Oceana® Cluster 1 in Data Center 2.
6. Create a context in DC1 Context Store.

   Context Store provides a Postman collection of API calls which can be used for all context operations such as creating and retrieving contexts from Context Store. You can download the Postman collection from **Products & Resources** > **Context Store** > **Context Store Snapin** > **Select Release** > **Downloads** at www.devconnectprogram.com.
7. Verify that the context is present in DC 1 Context Store and in DC2 Context Store.

Verifying Omnichannel Database mirroring status

About this task

To verify that data from the primary omnichannel database is mirrored across a data link to the disaster recovery (DR) omnichannel database, you must log on to the Omnichannel Database server in the DR site and verify mirroring status from primary to DR site.

Procedure

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

   http(https)://*<DC2OmnichannelServerIP>*:57772/csp/sys/UtilHome.csp

<DC2OmnichannelServerIP> is the IP address of the Omnichannel Database server in the DR site.

2. On the Cache Management Portal login page, do the following:
   a. In the **User Name** field, type `_admin`.
   b. In the **Password** field, type `Oceana16`.
   c. Click **LOGIN**.
3. On Cache Management Portal, click **System Operation** > **Mirror Monitor**.
   a. Verify the following details:
      - Primary server Member Type = Failover
      - Primary server Status = Primary
      - Disaster recovery server Member Type = Disaster Recovery
      - Disaster recovery server Status = Connected
      - Disaster recovery server Journal Transfer = Caught up
   b. Verify that Multimedia_DATA, Multimedia_Offline, and Cobrowse_Data databases are in the Mirrored databases for AOCMIRROR list.
4. **(Optional)** Repeat step 1 to step 3 on the primary Omnichannel Database.

Note:

In a deployment with both Omnichannel Campus HA (two Omnichannel Database servers) and DR (2+1), it is only required to verify replication status on the DR server.

Chapter 5: Procedures for planned switchover

Planned maintenance of Avaya Oceana® components

Overview

This chapter provides information and instructions for planned maintenance windows of a production Avaya Oceana® and Avaya Analytics™ Disaster Recovery (DR) solution.

Planned maintenance windows are defined as customer agreed time periods where the deployed solution is taken out of the production and put into a shutdown or standby mode to perform a switchover and a switchback between the two parts of the DR solution.

Avaya Oceana® supports the following options for full and partial switchover and switchback operations during planned maintenance windows:

- Performing a planned full switchover and switchback of all DR components of the solution. For this option, all components with a DR capability undergo a switchover and switchback as documented in this guide.
- Performing a planned partial switchover and switchback of Avaya Oceana® (Avaya Breeze® platform nodes and Omnichannel Database), which means that the customers do not have to switchover and switchback any of following surrounding applications that are deployed with DR capabilities in an Avaya Oceana® and Avaya Analytics™ DR solution provided they are fully operational.
  - Avaya Aura® Communication Manager with ESS.
  - Avaya Control Manager with any of its supported HA or DR deployments.
  - Avaya Aura® Session Manager with a Geo-Redundant System Manager deployment.

Some reasons for performing either a planned full or partial switchover and switchback are as follows where there are no current failures in any part of the solution.

- Testing the full DR capabilities of the entire solution for an unexpected full site outage of the primary site. Maintenance times required to perform a full DR switchover and switchback must be planned based on customer experience of a DR solution.
- Testing the DR capabilities of the Avaya Oceana® and Avaya Analytics™ components only thereby reducing the scheduled maintenance times required to perform the activity. You must perform this partial switchover and switchback activity post a software upgrade or update that is patch to validate the DR capabilities while the other parts of the full DR solution have not undergone any updates.

The partial DR switchover and switchback option is also supported for unplanned failures of individual components where there are unplanned failures in the solution, the customer must decide to perform either a full DR switchover or a partial DR switchover after assessment of the failures.

If a switchover is required, for an unplanned failure there can only be a full DR switchover or a partial DR switchover. It is not supported to mix procedures from either option. When you decide for a full or partial DR switchover, complete all the procedures described in this guide. It is not supported to attempt a full DR switchover after a partial DR switchover without performing a switchback. It is recommended to address the failures and revert the solution back to normal primary operation before undertaking additional switchover or switchback attempts of either option.

Advantages of performing a planned switchover and switchback

There are several advantages to perform a planned switchover and switchback of Avaya Oceana® and Avaya Analytics™ DR solution using the procedures documented in this guide.

- Planned procedures allow existing contacts to be processed out of the system in a controlled manner.
- New Contacts are not allowed into the system to queue, after the switchover procedures starts.
- The procedures allow existing logged in agents to the currently queued contacts.
- All contacts can be cleared before the shutdown of either side of the DR system; primary or DR.
- Supervisor users logged in using Avaya Workspaces, can view real-time reports and displays to ensure a graceful shutdown of all existing contacts in the system.

Additional or different switchover procedures is required for unplanned outages and these are discussed in chapter *Additional switchover procedures post unplanned failures in Data Center 1* of this guide. A customer has to combine the procedures in this chapter with the additional procedures in chapter *Additional Switchover Procedures post unplanned failures in DC1* to switchover to the DR site following partial or total failures of the primary site.

Summary checklist for full and partial DR switchover and switchback

The summary checklist provides information on the procedures for both full and partial DR switchover from the primary site (Data Center 1) to a deployed DR site (Data Center 2). The subsequent sections list out the detailed steps for each of the summary items listed in the table. The switchover procedures are listed in the order of a switchover from the primary system to the DR system. The switchback procedures are listed in the order of a switchback from the DR system to the primary system. Here, the primary system is referred as Data Center 1 (DC1), DR system as Data Center 2(DC2), and Data Center as DC. Avaya Oceana® and Avaya Analytics™ are deployed across two data centers – DC1 and DC2.

Note:

Each customer deployment has different Avaya Oceana® channels enabled. Yes or No in the table only applies if the channel or capability is deployed in the customer solution.

Functional area	Procedure high level description	Mandatory for partial DR switchover	Mandatory for full DR switchover
Preparation for Switchover	Download Avaya Oceana® and Avaya Analytics™ DR Guide.	Yes	Yes
	Download Avaya Aura® System Manager Administration Guide.	Yes	Yes
	Download Avaya Control Manager HA Guide.	Yes	Yes
	Download Administration Guides for AES and Avaya Aura® Communication Manager.	Yes	Yes
	Agree maintenance windows with customers for the date, time, and duration as Avaya Oceana® and Avaya Analytics™ will be out of production.	Yes	Yes
Validation of Avaya Oceana® and Avaya Analytics™ DR health prior to switchovers			
Validation of DC2 functionality prior to switchover to DC2.	Validate identical software levels on the following applications across DC1 and DC2: • Avaya Aura® System Manager • Avaya Control Manager • Avaya Aura® Communication Manager • AES • Avaya Oceana® • Avaya Analytics™ • Avaya Breeze® platform • Omnichannel	Yes	Yes

Table continues…

Functional area	Procedure high level description	Mandatory for partial DR switchover	Mandatory for full DR switchover
	Validate Avaya Aura® System Manager replication and health status from DC1 to DC2 is fully operational.	Yes	Yes
	Validate Avaya Control Manager database replication from DC1 to DC2.	Yes	Yes
	Validate Avaya Aura® System Manager primary replication and synchronization to all Avaya Breeze® platform nodes in DC1 and DC2.	Yes	Yes
	Validate UCA replication from DC1 to DC2.	Yes	Yes
	Validate Context Store replication from DC1 to DC2.	Yes	Yes
	Validate Omnichannel database mirroring from DC1 to DC2.	Yes	Yes
	Validate Avaya Aura® Communication Manager and ESS replication.	Yes	Yes
	Validate Analytics database replication from DC1 to DC2.	Yes	Yes
Validation of Avaya Oceana® Snapin Status in DC2 prior to switchover.	Validate Email Snapin deployment status in DC2, if email channel is deployed.	Yes	Yes
	Validate Customer Controller Snapin shutdown status in DC2, if chat channel is deployed.	Yes	Yes

Table continues…

Functional area	Procedure high level description	Mandatory for partial DR switchover	Mandatory for full DR switchover
	Validate Messaging Snapin shutdown status in DC2, if either Social or SMS or Async channels are deployed.	Yes	Yes
	Validate Generic Snapin status in DC2, if generic channel is deployed.	Yes	Yes
	Validate Avaya WebRTC Connect AMC Snapin PU status in DC2, if WebRTC Connect is deployed.	Yes	Yes
	Validate CSC Snapin PU Deployment status.	Yes	Yes
	Launch Oceana Monitor for DR location, and verify there are no un-deployed PU's across all Oceana clusters.	Yes	Yes
Avaya Oceana® & Avaya Analytics™ primary site graceful shutdown starts.			
Controlled shutdown of DC1 deployed channels and operation.	Graceful shutdown incoming Voice Contacts to DC1.	Yes	Yes
	Graceful shutdown of Email channel in DC1.	Yes	Yes
	Graceful shutdown of Chat channel in DC1.	Yes	Yes
	Graceful shutdown of Messaging service in DC1, if SMS or Social is deployed.	Yes	Yes
	Graceful shutdown of Social channel in DC1.	Yes	Yes
	Graceful shutdown of Generic channel in DC1.	Yes	Yes
	Graceful shutdown of incoming WebRTC Connect contacts to DC1.	Yes	Yes

Table continues…

Functional area	Procedure high level description	Mandatory for partial DR switchover	Mandatory for full DR switchover
	Shutdown of incoming Proactive Outreach Manager contacts to DC1 if Proactive Outreach Manager is deployed.	Yes	Yes
	Graceful shutdown of ASYNC channel contacts to DC1.	Yes	Yes
	Validate no active or queued contacts in DC1.	Yes	Yes
	Validate all agents logged out of DC1.	Yes	Yes
	Set DC1 all cluster status to Standby using Oceana Manager.	Yes	Yes
Avaya Oceana® & Avaya Analytics™ primary site shutdown complete, switchover starts.			
Switchover Operations from DC1 to DC2.	Switchover Communication Manager from DC1 to ESS in DC2.	No	Yes
	Switchover PSTN Voice Channels from Avaya Oceana® DC1 to Avaya Oceana® DC2.	Yes	Yes
	Switchover System Manager from DC1 to DC2 Geo System Manager.	No	Yes
	Set DC2 Oceana Cluster Status to Accepting using Oceana Manager	Yes	Yes
	Switchover Avaya Control Manager and Avaya Control Manager database operations from DC1 to DC2.	No	Yes

Table continues…

Functional area	Procedure high level description	Mandatory for partial DR switchover	Mandatory for full DR switchover
	Validate all Avaya Oceana® Avaya Breeze® platform nodes replicating and managed by System Manager in DC2. Only required in full DR where System Manager switchover is performed.	No	Yes
	Perform Avaya Analytics™ switchover from DC1 to DC2.	Yes	Yes
Put Avaya Oceana® in DC2 into full operation	Verify CSC deployment status in DC2.	Yes	Yes
	Enable DC2 Email Snapin deployment status.	Yes	Yes
	Switchover Optional WebRTC Connect Voice and Video to DC2.	Yes	Yes
	Verify DC2 Analytics connections to Avaya Oceana® in DC2.	Yes	Yes
	Reconfigure Avaya Control Manager in DC1 to connect to Avaya Oceana® and Avaya Analytics™ applications in DC2 for Partial DR switchovers using Avaya Control Manager Toggle button feature.	Yes	No

Table continues…

Functional area	Procedure high level description	Mandatory for partial DR switchover	Mandatory for full DR switchover
	Optionally, switchover to DC2 Avaya Control Manager and reconfigure Avaya Control Manager in DC2 to connect to Avaya Oceana® and Avaya Analytics™ and ESS applications in DC2 for full DR switchovers using Avaya Control Manager Toggle button feature.	No	Yes
	Startup optional Chat channel in DC2	Yes	Yes
	Startup optional Messaging based channels in DC2 – Social/SMS/ASYNC	Yes	Yes
	Startup optional POM channel in DC2	Yes	Yes
	Startup optional Generic channel in DC2	Yes	Yes
	Login Agents using DC2 Workspaces and Test deployed Channel Routing.	Yes	Yes
	Turn on all incoming channels to DC2 if disabled at the front end.	Yes	Yes
	Validate all Avaya Oceana® and Avaya Analytics™ functionality by launching Oceana Dashboard and verifying all deployed channels are in the Green status.	Yes	Yes
	Launch Oceana Workspaces Supervisor and verify all required Analytics Real Time Displays operational.	Yes	Yes
Avaya Oceana® & Avaya Analytics™ Switchover Complete. Avaya Oceana® & Avaya Analytics™ DR in service.			

After you complete these procedures, operations can start using infrastructure in the DR site (DC2).

Download reference documentation

Before doing any switchover or switchback operations on a production Avaya Oceana® and Avaya Analytics™ DR system, you have to refer several key documents. The following documents available on Avaya support site are recommended for all switchover and switchback procedures:

- Avaya Aura® System Manager Administration
- Avaya Control Manager High Availability
- Avaya Aura® Communication Manager
- Avaya Aura® Application Enablement Services

Agree planned maintenance windows time and duration

Planned maintenance windows require planning and scheduling. During the planned maintenance window, the solution is out of operation for a period of time. Times for switchover and switchback vary depending on whether a partial or full DR switchover or switchback is implemented. For all planned maintenance windows of an Avaya Oceana® and Avaya Analytics™ DR solution, it is recommended to plan for a minimum of four hours, but the tasks might take longer that the minimum recommended time.

Validate identical software levels

For a planned switchover and switchback testing, software versions and levels on both primary and DR sites must be identical.

You must validate the following applications and platforms:

- Avaya Aura® System Manager
- Avaya Control Manager
- Avaya Breeze® platform
- Avaya Aura® Communication Manager and ESS
- Avaya Aura® Application Enablement Services
- Avaya Analytics™
- Avaya Oceana® Snap-ins
  - Snapin versions on primary and DR must be identical prior to starting an upgrade

For software upgrade maintenance windows, you have different software versions during the upgrade process. Both DC1 and DC2 applications must be at the same software release version before you can re-enable solution replication from each application in DC1 to DC2. You cannot

upgrade an application in only DC1, and not upgrade its equivalent application in DC2, and expect replication to work between the two applications.

It is recommended to create a table to record the software versions of each application for primary and SR sites. For unplanned maintenance windows due to application failures, this step is not necessary.

Validating System Manager primary to DR replication status

About this task

For any planned partial or full DR switchover and switchback, you must verify the health of the System Manager replication state between the primary System Manager and the DR System Manager.

Procedure

1. On the primary System Manager web console, navigate to **Application State** widget. Verify the following states:
   - Geographic Redundancy (GR) Server Role is Primary
   - GR Server Mode is Active
   - GR Replication is Enabled
2. Click **Services** > **Geographic Redundancy** > **GR Health**. Verify that Database Replication, File Replication, and Directory Replication are in green color and is Successful.

   If any element is in red color and is in Failure or Stopped state, then do not proceed with the switchover and contact the system administrator to correct any problems.
3. On the DR System Manager web console, in the **Application State** widget, verify the following states:
   - GR Server Role is Secondary
   - GR Server Mode is Standby
   - GR Replication is Enabled
4. Verify the status of elements in **GR Health**.

   If any element is in red color and is in Failure or Stopped state, then do not proceed with the switchover and contact the system administrator to correct any problems.

Validating System Manager and Avaya Breeze® platform replication status

About this task

For a planned switchover and switchback testing, you must synchronize Avaya Workspaces for Call Center Elite and Avaya Breeze® platform and replicate System Manager before starting the switchover and switchback procedures.

Procedure

1. On the System Manager web console, click **Services** > **Replication**.
2. Validate that all replica groups synchronization status is **Synchronized**.

   System Manager displays the word **Synchronized** in green color.
3. Click **Avaya Breeze replica group**.
4. Verify that **Breeze Node Synchronization** status is in the **Synchronized** state and the synchronization date is one month or less from the current date.

   If any Avaya Breeze® platform element displays the status as **Synchronizing** or **Repairing**, you must wait until the process completes and the status is **Synchronized**. If any Avaya Breeze® platform node is not synchronized, do not proceed with the switchover process until you address the issue.

Validating Avaya Control Manager database HA replication status

About this task

For all switchovers, you must verify Avaya Control Manager database HA feature as operational before proceeding with the procedure.

Important:

Instructions on how to perform this validation are beyond the scope of this document and you can refer Avaya Control Manager HA deployment guides available on Avaya support site.

Validating Avaya Oceana® components replication operation before switchover

Before any planned switchover from a primary to a Disaster Recovery (DR) site, you must verify the health status of the applications that replicate data from the primary to the DR site is completely operational. The following Avaya Oceana® core applications replicate data from the primary site to the DR site.

Replication is:

- Unified Collaboration Administration (UCA) using Gigaspaces DataGrid replication.
- Avaya Context Store Snap-in (CS) using Gigaspaces DataGrid replication.
- Omnichannel database using cache mirroring.

The following surrounding applications in the Avaya Oceana® replicate data from the primary to the DR site:

- Avaya Aura® System Manager primary to System Manager Geo in the DR location.
- Avaya Control Manager database replication from primary to DR location.
- Avaya Aura® Communication Manager from primary to DR ESS.

Important:

You must validate the replicating function of all these replicating applications before a partial or a full DR switchover. If you do not perform this validation, it leads to issues during the switchback process.

Verifying UCA replication status

About this task

When you make an administrative change using the primary Avaya Control Manager, the changes are replicated from the primary UCA to the DR UCA. Using a browser request, you can verify the change in each UCA instance. You must add a new test attribute and verify that this is replicated across to the DR UCA instance.

Use this procedure to check that UCA replication is operational, and then verify that the test attribute is replicated to the DR instance.

Important:

You must ensure that there are no active UCA alarms. If there are any active UCA alarms, you must resolve them before the switchover.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration** > **Primary Cluster**.
2. In the **Cluster** field, select **Oceana Monitor**.
3. Select **Cluster 1** > **Grid Info** to view the PU status of all the snap-ins.

   Verify if the PU status of ucaStoreSpace-GATEWAY is Intact. If the status is Scheduled or Broken, then UCA replication is not operational and you must correct the issue before proceeding with the switchover.
4. Repeat steps 1 to step 3 for Cluster 1 in the DR site.
5. Log on to the primary Avaya Control Manager.

6. Add a new test attribute and save the attribute to the primary UCA instance.

   For more information on creating a new test attribute, see the *Adding Attributes to Avaya Control Manager* section in *Deploying Avaya Oceana®*.

7. Using the following URL, verify that the new attribute appears in the response from the URL request.

   ```
   https://<<primary cluster 1 FQDN>/services/UCAStoreService/uca/
   attributes
   ```

8. Repeat the URL test for DR system using a similar request:

   ```
   https://<<DR cluster 1 FQDN>/services/UCAStoreService/uca/
   attributes URL
   ```

   Note:

   If the test attribute does not appear in both responses, UCA replication is not operational from primary to DR or the request to save a new attribute to the primary UCA server was not successful. You must correct the issues before proceeding with the switchover.

Verifying Context Store replication status

About this task

Use Oceana Monitor to verify Avaya Context Store Snap-in replication functioning between primary and DR sites. You must validate the presence of the Avaya Context Store Snap-in replication gateway PU. You must also create a context to verify that replication is working.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration** > **Primary Cluster 1**.
2. In the **Cluster** field, select **Oceana Monitor**.
3. Select **Cluster 1** > **Grid Info** to view the PU status of all the snap-ins.

   Verify if the PU status of cs-gateway is Intact. If the status `Scheduled` or `Broken`, then it indicates that the Context Store replication is not operational. You must correct the issue before proceeding with the switchover.

4. Repeat steps 1 to step 3 for Cluster 1 in the DR site.
5. Create a context in DC1 Context Store.

   Context Store provides a Postman collection of API calls which can be used for all context operations such as creating and retrieving contexts from Context Store. You can download the Postman collection from **Products & Resources** > **Context Store** > **Context Store Snapin** > **Select Release** > **Downloads** at www.devconnectprogram.com.

6. Verify that the context is present in DC 1 Context Store and in DC2 Context Store.

Verifying Omnichannel database mirroring status

About this task

You must check the mirroring status from primary to DR site to verify that data from the primary Omnichannel database is mirrored across a data link to the DR Omnichannel database.

Procedure

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

   http(https)://<*DC2OmnichannelServerIP*>:57772/csp/sys/UtilHome.csp

   <*DC2OmnichannelServerIP*> is the IP address of the Omnichannel Database server in the DR site.

2. On the Cache Management Portal login page, do the following:
   a. In the **User Name** field, type `_admin`.
   b. In the **Password** field, type `Oceana16`.
   c. Click **LOGIN**.
3. On Cache Management Portal, click **System Operation** > **Mirror Monitor**.
   a. Verify the following details:
      - Primary server Member Type = Failover
      - Primary server Status = Primary
      - Disaster recovery server Member Type = Disaster Recovery
      - Disaster recovery server Status = Connected
      - Disaster recovery server Journal Transfer = Caught up
   b. Verify that Multimedia_DATA, Multimedia_Offline, and Cobrowse_Data databases are in the Mirrored databases for AOCMIRROR list.
4. **(Optional)** Repeat steps 1 to 3 on the primary Omnichannel Database, if required.

   Note:

   In a deployment with both Omnichannel Campus HA (2 Omnichannel Database servers) and DR (2+1), it is only required to verify replication status on the DR server.

Verifying Avaya Aura® Communication Manager to ESS data replication integration

You must perform administration configurations on the primary Avaya Aura® Communication Manager to verify that any data from the primary communication manager is replicated to the ESS in the DR site. You must then run a save translation command and then login to the ESS server

and verify the change is available on the ESS system. For more information, see *Avaya Communication Manager Administrator* guide.

Verifying Avaya Analytics DB Replication from DC1 to DC2

About this task

Use this procedure to verify the status of replication between primary and replica pods on DC1 and between DC1 and DC2.

Procedure

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

   `ccm release orca analytics`
4. To select the **Troubleshooting** option, enter the corresponding number.
5. To select the **Database** option, enter the corresponding number.
6. To check Crunchy pod replication status, enter the corresponding number.

   The output from the script shows different information for each pod depending on whether a pod is a primary, a standby replica, or a Geo replica. The expectations are as follows:

   - The primary pod **crunchy-primary-service-orca-dbmgr-0** must be listed as `master list` of replicas.
   - The `master list` displays a list of replica pods listening to the primary pod.
   - The **state** column must be `streaming`. It indicates whether the replication is currently running. It also displays if there is any lag in writing data on the target pod.

Validating Avaya Oceana® snap-in shutdown or deployment status in DR site before switchover

Before any planned switchover from a primary to a Disaster Recovery (DR) site, you must validate the deployment status of Avaya Oceana® snap-ins and the configured attribute values. There can be previous switchovers and switchbacks performed on the system where many attributes are modified as part of these processes. It is important to validate these attribute values for channel snap-ins. Otherwise, this impacts a successful switchover process and requires manual intervention to correct any issues. This also requires additional restart of the Avaya Oceana® clusters to complete the switchover.

Verifying the deployment mode status of EmailService in the DR site

About this task

The Email snapin deployment status attribute in the DR site must be validated as `false`.

If you do not have email channel deployed on Avaya Oceana®, you can skip this procedure.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the DR site Service Clusters tab, do the following:
   a. **Cluster**: Select DR Avaya Oceana® Cluster 3.
   b. **Service**: Select **EmailService**.
3. In the **Deployment status of emailmanager** attribute, validate if the value of this field is set to `false`.

   If this field is set to `true`, set it to `false` and commit the change. There is no need to reboot Cluster 3.

Verifying the shutdown mode status of CustomerControllerService in the DR site

About this task

The CustomerControllerService snapin is responsible for allowing chat contacts to enter the Oceana ecosystem.

Before the switchover to the DR site, the shutdown mode status attribute in the DR site for this snapin must be validated as `true`, while the primary site is in production.

If the chat channel is not deployed on Avaya Oceana®, you can skip this procedure.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the DR site Service Clusters tab, do the following:
   a. **Cluster**: Select DR Avaya Oceana® Cluster 3.
   b. **Service**: Select **CustomerControllerService**.
3. In the **Shutdown Mode** attribute field, validate if the value of this field is set to `true`.

There is no need to reboot Avaya Oceana® Cluster 3 if you have to change this value to `true`.

Verifying the shutdown mode status of MessagingService in the DR site

About this task

The MessagingService snapin is responsible on the front-end for a number of Avaya Oceana® channel snapins such as the SMS, Social, or Async channels. Before the switchover to the DR site, the shutdown mode status attribute in the DR site for this snapin must be validated as `true` while the primary site is in production.

If SMS, Social, or Async channels are not deployed on Avaya Oceana®, you can skip this procedure.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the DR site Service Clusters tab, do the following:
   a. **Cluster**: Select DR Avaya Oceana® Cluster 3.
   b. **Service**: Select **MessagingService**.
3. Ensure that the **Shutdown Mode** attribute value is set to `True`.

   There is no need to reboot Avaya Oceana® Cluster 3 if you have to change this value.

Verifying the shutdown mode status of GenericChannelAPI in the DR site

About this task

The GenericChannelAPIService snapin is responsible for injecting generic contacts into the Oceana ecosystem.

Before the switchover to the DR site, the shutdown mode status attribute in the DR site for this snapin must be validated as `true` while the primary site is in production.

If the Generic channel is not deployed on Avaya Oceana®, you can skip this procedure.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the DR site Service Clusters tab, do the following:
   a. **Cluster**: Select DR Avaya Oceana® Cluster 3.

b. **Service**: Select **GenericChannelAPIService**.

3. Ensure that the **Shutdown Mode** attribute value is set to `True`.

   There is no need to reboot Avaya Oceana® Cluster 3 if you have to change this value.

Verifying the deployment status of the AMC snap-in PU for Avaya WebRTC Connect contacts

About this task

The AMC snap-in allows all WebRTC Connect voice and video contacts to enter Avaya Oceana®. You must validate the deployment status of the AMC snap-in Processing Unit (PU) using Oceana Monitor to ensure if the snap-in is active and operational before the switchover.

If the WebRTC Connect channel is not deployed on Avaya Oceana®, you can skip this procedure.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration** > **DR Cluster 1**.
2. In the **Cluster** field, select **Oceana Monitor**.
3. Select **Cluster 2** > **Grid Info** to view the PU status of all the snap-ins.

   Verify if the PU status is Intact. If the status is Scheduled or Broken, then the AMC snap-in is not operational and you must correct the issue before proceeding with the switchover. Otherwise, when the switchover is complete, WebRTC Connect voice or video contacts are not routed in Avaya Oceana®.
4. Click **Show Cluster Messages** and click the AMC snap-in and verify that there are no alarms or errors.

Switchover from primary to DR for Avaya Oceana® and Avaya Analytics™ operations

Part 1 and Part 2 are the actual switchover procedures to switch production operations from the primary site to the DR site. A full or partial DR switchover is performed at this point depending on the current requirements. The following is the summary of high level function steps that you must perform to complete the switchover:

Part1- Shutdown Primary Production Operations:

- Shutdown the PSTN Voice channel.
- Shutdown all deployed digital channels such as Chat, SMS, Social, Generic, and Async.
- Shutdown the WebRTC Connect channel.
- Shutdown the POM outbound.

- Validate if all contacts are cleared from Avaya Oceana® queue.
- Ensure that all agents are logged out.
- Set primary Avaya Oceana® Clusters to Deny state.

Part 2 - Switchover Production to DR Site

- Switchover System Manager – Full DR switchover only.
- Switchover Avaya Control Manager – Full DR switchover only.
- Switchover Omnichannel primary to DR – Partial or Full.
- Switchover Avaya Analytics™ primary to DR – Partial or Full.
- Set Oceana Cluster state to Accept in DR.
- Switchover Web Voice to DR.
- Login Avaya Oceana® agents to DR site and test all deployed channels functionality.
- Enable all Channels before performing switchover.

Configuring primary site voice channel shutdown

About this task

For a planned shutdown of the PSTN voice channel, the following are the two methods to shutdown incoming voice contacts from the front-end options supported in Avaya Oceana®.

- For Avaya Oceana® deployments with a front-end application running on Avaya Experience Portal, a flag is used at the start of the workflow for startup or shutdown operations. Using this flag, the administrator can redirect incoming voice calls to an automated response. The automated response rejects the incoming call or transfers the calls to an alternate call handling mechanism. The Avaya Oceana® 3. x Avaya Experience Portal based sample voice application contains sample code to implement this using Call Application Variables (CAVs) which specify which data center is operational at any given time. Setting this flag to any of the data center ensures incoming PSTN voice contacts are only routed to that data center. This is a simple and effective method to turn on or turn off incoming voice to an Avaya Oceana® DR system.
- For Avaya Oceana® deployments with Call Center Elite as front end, a CM variable indicating Avaya Oceana® in service or out of service is configured and checked on new incoming voice contacts. If the flag is set to indicate out of service, then new incoming voice contacts are routed to alternate fallback options until the switchover to the DR infrastructure is complete.

  You can skip these instructions if you do not have PSTN channel deployed on Avaya Oceana®.

Procedure

1. Log in to the Avaya Experience Portal web portal with the Administrator user role.
2. In the navigation pane, click **System Configuration** > **Applications**.
3. Select the application you want to modify, and click **Configurable Application Variables**.

4. In the **Active Data Center** field, click **DataCenter2**.
5. Click **Save**.

   New incoming voice contacts arriving at the application in the Avaya Experience Portal, are routed to the Avaya Oceana® system in the DR location.

Configuring primary site email shutdown

About this task

For a planned switchover of EmailService, you must change the deployment status. An Avaya Oceana® administrator with access to System Manager can change the status. Failure to shut down the email service in the primary site means that all incoming emails to Avaya Oceana® monitored mailboxes are queued by the primary email service after switchover is complete.

For a planned switchover of EmailService, an administrator must shut down EmailService on primary site by using a flag in Avaya Oceana® Cluster 3. When the administrator shuts down the EmailService:

- New emails are not retrieved from the email server.
- Outgoing emails are queued within the Cache database.

After completing the switchover process, EmailService processes all emails in the DR site and sends the outgoing emails from the DR site.

If you do not have email channel deployed on Avaya Oceana®, you can skip this procedure.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the primary site Service Clusters tab, do the following:
   a. **Cluster**: Select primary Avaya Oceana® Cluster 3.
   b. **Service**: Select **EmailService**.
3. In **Deployment status of emailmanager**, do the following:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, change the value from `true` to `false`.
4. Click **Commit**.

Configuring primary site chat shutdown

About this task

For a planned switchover, the administrator can manually stop chat contacts from entering the Avaya Oceana® and allow existing contacts to get processed out of the system.

If you do not have chat channel deployed on Avaya Oceana®, you can skip this procedure.

Procedure

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

2. On the primary site Service Clusters tab, do the following:
   a. **Cluster**: Select primary Avaya Oceana® Cluster 3.
   b. **Service**: Select **CustomerControllerService**.
3. In **Shutdown Mode**, do the following:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, change the value from `false` to `true`.
4. Click **Commit**.

Note:

The customer deployed chat front-end application now needs to be configured to point to the Oceana DR system. The instructions to complete that task are beyond the scope of this DR guide as each chat deployment can utilize different methods to integrate to the Oceana back-end systems.

Configuring primary site MessagingService shutdown

About this task

For a planned switchover, the administrator can manually stop SMS and Social contacts from entering the Avaya Oceana® and allow existing contact to get processed out of the system.

If you do not have SMS, Social, and Async channels deployed on Avaya Oceana®, you can skip this procedure.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the primary site Service Clusters tab, do the following:
   a. **Cluster**: Select primary Avaya Oceana® Cluster 3.
   b. **Service**: Select **MessagingService**.
3. In **Shutdown Mode**, do the following:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, change the value from `false` to `true`.
4. Click **Commit**.

Note:

The customer deployed Social Media, SMS, or Async front-end applications now need to be configured to point to the Oceana DR system. The instructions to complete that task are beyond the scope of this DR guide as each deployment can utilize different methods to integrate to the Oceana back-end systems.

Configuring primary site GenericChannelAPI service shutdown

About this task

For a planned switchover, the administrator can manually stop new generic contacts from entering the Avaya Oceana® and allow existing contacts to get processed out of the system.

An administrator must set the primary site GenericChannelAPI service on Avaya Oceana® Cluster 3 to True.

If you do not have generic channel deployed on Avaya Oceana®, you can skip this procedure.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the primary site Service Clusters tab, do the following:
   a. **Cluster**: Select primary Avaya Oceana® Cluster 3.
   b. **Service**: Select **GenericChannelAPI**.
3. In **Shutdown Mode**, do the following:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, change the value from `false` to `true`.
4. Click **Commit**.

Note:

The customer deployed Generic Channel front-end application now needs to be configured to point to the Oceana DR system. The instructions to complete that task are beyond the scope of this DR guide as each generic channel deployment can utilize different methods to integrate to the Oceana back-end systems.

Setting the maintenance mode for front end web voice and web video

For a planned switchover, you must modify the front-end web portals that host the Avaya WebRTC Connect voice or video capabilities to indicate to the end users that the service is temporarily unavailable. Use a flag to toggle between in service and out of service.

Oceana POM switchover

The Oceana POM Outbound solution does not support disaster recovery. Therefore, you must stop all running campaigns on the primary Proactive Outreach Manager server before switching over to the DR site Oceana and POM system.

Validating contacts

For a planned switchover, you must ensure that new contacts do not arrive into the primary Avaya Oceana® once the shutdown process starts. You must also close any Queued or In Progress contacts which an agent is processing. To check if the status of all the current contacts for all channels are Processed and Closed, log in as an Avaya Oceana® supervisor and use Avaya Analytics™ real time displays. For more information, refer Avaya Oceana® and Avaya Analytics™ documentation suite.

Logging out supervisors and agents

For a planned switchover, ensure that all Avaya Oceana® agents are logged out. Supervisors can verify using **My team** widget. Supervisors must co-ordinate locally to ensure that the agents are logged out.

Put primary Avaya Oceana clusters into Deny mode – Complete shutdown of DC1 operations

Changing the Cluster Activity status for the clusters in Data Center 1

Before you begin

OceanaMonitorService must be installed on the clusters in Data Center 1.

Procedure

1. Open the Oceana Manager page by entering the following URL in your web browser:

   `https://<DataCenter1_AvayaOceanaCluster1_FQDN>/services/OceanaMonitorService/manager.html?affinity=)`

   Important:

   Create a bookmark of this URL in your web browser, so that you can open the Oceana Manager page even when System Manager is unavailable.

2. **(Optional)** To open the Oceana Manager page through System Manager, do the following:

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

b. On the Cluster Administration page, in the **Service URL** column for Avaya Oceana® Cluster 1, select **Oceana Manager**.

3. Log in to Oceana Manager using an Admin account.
4. On the Oceana Manager page, do the following:
   a. Verify that the status of the clusters is `ACTIVE`.
   b. Click **Set Cluster Group to Standby** to change the status to `STANDBY` and place all nodes in the Deny New Service mode.
   c. On the confirmation message box, click **OK**.
   d. Wait for 5-10 minutes for the Oceana Manager page to display the updated status.
   e. **(Optional)** If the Oceana Manager page does not display the updated status after some time, click **Refresh**.
   f. Refresh the Clusters page in Avaya Breeze® platform and validate that all the clusters in the primary site are in Deny state.

Configuring switchover operations to Data Center 2

This section provides the actual switchover procedures to move production to the applications and systems in the DR Location.

Switchover from Avaya Aura® Communication Manager to ESS in DR site

For full DR switchover, you must shutdown the Communication Manager in Data Center 1 so that the ESS in Data Center 2 can come into operation. The phonesets and gateways re-register with the ESS. Once the registration is complete, the agents can start handling voice contacts that are routed through Avaya Aura® Call Center Elite while Avaya Oceana® and Avaya Analytics™ are switched over to the DR site

For partial DR switchovers, you do not have to shut down the Communication Manager in Data Center 1 if the Avaya Aura® applications are fully functional.

System Manager switchover

Checklist for Avaya Aura® System Manager switchover

Note:

For partial switchover of Avaya Oceana® and Avaya Analytics™ applications, do not perform System Manager switchover. System Manager switchover is required only for a full DR switchover or a failure of the actual primary System Manager.

Note:

The procedure to bring the DR System Manager into production involves disabling operational geographic redundancy replication and shutting down the primary System Manager. There is no switchover from the primary System Manager application to the DR System Manager application.

No.	Task	Description	Notes	✔
1	Disable the Geographic Redundancy replication.	Disable Avaya Aura® System Manager Geographic Replication at Data Center 1.	For more information, see Administering Avaya Aura® System Manager.	
2	Shut down System Manager at Data Center 1.	You must shut down Avaya Aura® System Manager to trigger the Avaya Breeze® platform snap-ins to switch to the System Manager instance at Data Center 2.	For more information, see Administering Avaya Aura® System Manager.	
3	Activate System Manager at Data Center 2.	Activate Avaya Aura® System Manager at Data Center 2.	For more information, see Administering Avaya Aura® System Manager.	
4	Verify the Avaya Breeze® platform node controller.	Confirm that the Avaya Breeze® platform nodes are switched from System Manager in Data Center 1 to System Manager in Data Center 2.	For more information, see Verifying Breeze node controller on page 92.	

Verifying Avaya Breeze® platform node controller for Data Center 2

About this task

Use this procedure:

- To verify that the Avaya Breeze® platform nodes are switched from System Manager in Data Center 1 to System Manager in Data Center 2 after System Manager switchover.
- If a full DR switchover is in progress.

This procedure is not required in a partial DR switchover because the Avaya Breeze® platform nodes are managed by the primary System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. In the **Managed by** field, verify that system displays **Secondary** for the Avaya Breeze® platform nodes.

Omnichannel database switchover

You can manually switchover the Omnichannel database server in the primary site Data Center 1 to the Omnichannel database server in the DR site Data Center 2 in partial or full DR switchover scenarios.

Note:

Do not restart the cluster. You can perform switchover from:

- A single active server in Data Center 1 to the async Omnichannel server in Data Center 2.
- An active or standby server in Data Center 1 to the async server in Data Center 2.

Promoting async server when active and async servers are available

About this task

Use this procedure to promote the async server in the DR site when the active server in primary and async server in DR location are available and mirroring operational for planned maintenance windows. This procedure can be used whether a dual server pair is deployed in primary site or not.

Procedure

Deploy Omnichannel Server C as the async member in the primary site.

On Server C in the DR site, do the following:

1. Navigate to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement` folder.
2. Double-click `OceanaDataManagementTool.exe`.
3. In the Oceana Data Management utility, click **Backup And Restore**.
4. In the navigation pane, expand the **Backup And Restore** node, and then click **Backup And Restore**.
5. Click **Mirror Configuration**.
6. In the **Select Mirror Scenario** field, select `Switchover Cache up on both servers - DR server`.
7. Click **Execute**.
8. Set up ACM to point to the new Omnichannel database primary server. For more information on setting up the ACM to point to the new Omnichannel database, see Setting ACM to point to the new Omnichannel database primary server on page 73.

Setting ACM to point to the new Omnichannel database primary server

About this task

Use this procedure to set up Avaya Control Manager to point to the new Omnichannel database primary server.

Procedure

1. Log on to Avaya Control Manager.
2. Navigate to **Configuration** > **Avaya Oceana™** > **Server Details**.
3. Double-click the administered Avaya Oceana® server or select the administered Avaya Oceana® server and click **Edit**.
4. Click the **System Properties** tab.
5. Expand **Omni Channel**.
6. In **Omni Channel Database Server**, enter the name of the Omnichannel Database server (Server C) as administered in the HTTPS certificate installed on the Omnichannel Database server. The name must match the name on the certificate and the certificate must also be trusted to avoid any certificate errors.

Enable Avaya Oceana® components in DR site

System Manager user interface – Primary or DR location

If you are performing a partial DR switchover, then you must perform the following procedures using the interface of the primary System Manager. If you are performing a full DR switchover, System Manager Geo switchover is completed and the following procedures are implemented using the interface of the Geo System Manager in the DR location.

Changing cluster activity status for clusters in Data Center 2

Before you begin

You must install OceanaMonitorService on the clusters in Data Center 2.

Procedure

1. Open the Oceana Manager page in the DR location by entering the following URL in your web browser:

   `https://<DataCenter2_AvayaOceanaCluster1_FQDN>/services/OceanaMonitorService/manager.html?affinity=)`

   Important:

   Create a bookmark of this URL in your web browser, so that you can open the Oceana Manager page even when System Manager is unavailable.

2. **(Optional)** To open the Oceana Manager page through System Manager, do the following:
   a. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
   b. On the Cluster Administration page, in the **Service URL** column for Avaya Oceana® Cluster 1, select **Oceana Manager**.
3. Log in to Oceana Manager using an Admin account.
4. On the Oceana Manager page, do the following:
   a. Verify that the status of the clusters is `STANDBY`.
   b. Click **Set Cluster Group to Active** to change the status to `ACTIVE` and place all nodes in the Accept New Service mode.
   c. On the confirmation message box, click **OK**.
   d. Wait for 5-10 minutes for the Oceana Manager page to display the updated status.
   e. **(Optional)** If the Oceana Manager page does not display the updated status after some time, click **Refresh**.

5. In System Manager, select DR Cluster 1 drop-down menu and start Oceana Monitor.

   On Cluster 1, verify the PUs deployed and status is **Intact** including CSC. CSC PU do not deploy if the Communication Manager configuration is not configured and validated. On Cluster 3, verify the PUs deployed and status is **Intact** including the Email PU. Verify that all nodes and clusters in the DR location are set to status **Accept**. If any clusters or nodes are in **Deny** state, then re-do the above steps or manually set them to **Accept** state using the Avaya Breeze® platform EM cluster overview page.

Configuring DR site EmailService startup

About this task

Use this procedure to enable the email channel in the DR site.

If the email channel is not deployed on Avaya Oceana® Cluster 3, you can skip this procedure.

Procedure

1. On the System Manager web console of Data Center 2, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. **Cluster**: Select Avaya Oceana® Cluster 3.
   b. **Service**: Select **EmailService**.
3. In **Deployment status of emailmanager**, do the following:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, change the value from `false` to `true`.
4. Click **Commit**.

Configuring DR site Chat startup

About this task

Use this procedure to enable the Chat channel in the DR site.

If the Chat channel is not deployed on Avaya Oceana®, you can skip this procedure.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Oceana Primary Service Clusters tab, do the following:
   a. **Cluster**: Select Avaya Oceana® Cluster 3.
   b. **Service**: Select **CustomerControllerService**.

3. In the **Shutdown Mode** attribute field, do the following:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, change the value from `true` to `false`.
4. Click **Commit**.

Note:

The customer deployed chat front-end application now needs to be configured to point to the Oceana DR system. The instructions to complete that task are beyond the scope of this DR guide as each chat deployment can utilize different methods to integrate to the Oceana back-end systems.

Configuring DR site MessagingService for Social or SMS startup

About this task

Use this procedure to enable the Social or SMS channel in the DR site.

If the Social or SMS channel is not deployed on Avaya Oceana®, you can skip this procedure.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. **Cluster**: Select Avaya Oceana® Cluster 3.
   b. **Service**: Select **MessagingSevice**.
3. In the **Shutdown Mode** attribute field, do the following:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, change the value from `true` to `false`.
4. Click **Commit**.

Note:

The customer deployed Social, Async, or SMS channel front-end application now needs to be configured to point to the Oceana DR system. The instructions to complete that task are beyond the scope of this DR guide as each Social or SMS channel deployment can utilize different methods to integrate to the Oceana back-end systems.

Configuring DR site GenericChannelAPI Service startup

About this task

Use this procedure to enable the Generic channel in the DR site.

If the Generic channel is not deployed on Avaya Oceana®, you can skip this procedure.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. **Cluster**: Select Avaya Oceana® Cluster 3.
   b. **Service**: Select **GenericChannelAPI**.
3. In the **Shutdown Mode** attribute field, do the following:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, change the value from `true` to `false`.
4. Click **Commit**.

Note:

The customer deployed Generic channel front-end application now needs to be configured to point to the Oceana DR system. The instructions to complete that task are beyond the scope of this DR guide as each Generic channel deployment can utilize different methods to integrate to the Oceana back-end systems.

Verifying DR Application Enablement Services server to enable Switch Connection to primary site Communication Manager

About this task

In the setup instructions for Avaya Oceana® disaster recovery solution, there are two switch connections configured from Application Enablement Services in the DR location:

- Switch Connection 1 is the primary Communication Manager.
- Switch Connection 2 is the ESS configured under the survivable hierarchy features in AES.

For a partial DR switchover, Switch Connection 1 remains in the **online** state and Switch Connection 2 remains in the **offline** state even after the Avaya Oceana® Clusters in the DR location are set to an Accept Mode. This proves that the AES survivable hierarchy feature is working as expected.

Procedure

1. Log in to the DR Application Enablement Services web portal, and go to **Communication Manager Interface** > **Switch Connections**.

The Switch Connection tab displays the following two entries configured from Application Enablement Services:

- Switch Connection 1
- Switch Connection 2

If there are no connections, then contact the system administrator to add the required number of switch connections.

2. On the Application Enablement Services administration portal, go to **Status** > **Status and Control** > **Switch Connection Summary**.

   The two switch connections are displayed in this menu.

3. Verify the Switch Connection entry for the ESS server is set to **offline**.
4. Verify the Switch Connection entry for the main Communication Manager in the primary location is set to **online**.
5. Close the AES window after verification.

Avaya Control Manager switchover from primary to DR site

This section provides information on the options available on switchover from a primary set of Avaya Control Manager servers in the primary site to the alternate set of servers in the DR site. For a planned maintenance window and a partial DR switchover, it is not required to switchover Avaya Control Manager servers. Enable the Avaya Control Manager 9.x Toggle feature to switch Avaya Control Manager to use the Avaya Oceana® and Avaya Analytics™ components in the DR site.

For a planned maintenance window and a full DR switchover, you must perform switchover of Avaya Control Manager application and database server. Enable the Avaya Control Manager 9.x Toggle feature to switch Avaya Control Manager DR to use the Avaya Oceana®, Avaya Analytics™, and ESS components in the DR site. Due to failures of the Avaya Oceana® applications where Avaya Control Manager is operational, Avaya Control Manager switchover is not required to use the Avaya Oceana® and Avaya Analytics™ applications in the DR location.

For more information on unplanned maintenance windows due to failures, see the respective chapters in this document. Avaya Control Manager supports several HA and DR models that is beyond the scope of this Avaya Oceana® Disaster recovery guide. These models are independent of the Avaya Oceana® DR deployment. For more information on how to setup Avaya Control Manager HA and DR, see Avaya Control Manager documentation suite.

For more information see, *Installing Avaya Control Manager for Enterprise - Multiplex High Availability* and *Installing Avaya Control Manager for Enterprise - Legacy High Availability* documents.

Avaya Control Manager Toggle Button utility for switchover and switchback

Avaya Control Manager provides the Toggle button feature to avoid manual intervention of the administrator to make configuration changes post switchover to Avaya Oceana® DR applications. The toggle button configures Avaya Control Manager to use the Avaya Oceana® UCA server instance in the DR location after the switchover is complete. On a switchback, the toggle button reverts the Avaya Control Manager application to use the Avaya Oceana® UCA server instance at the primary site. However, on a switchback, the administrator must manually re-configure Avaya Control Manager to use the primary Avaya Oceana® and Avaya Analytics™ applications as the toggle back feature does not preserve these settings.

Reconfiguring Avaya Control Manager in full and partial DR switchover scenarios

Overview

With the Toggle feature of Avaya Control Manager, an administrator can toggle a flag to configure Avaya Control Manager with the settings required for Avaya Oceana® in the primary or DR locations. This toggle feature allows the Avaya Control Manager application server to identify which Avaya Oceana® UCA instance to administer Avaya Oceana® configuration data. The toggle button can also be used when performing a switchover or a switchback. In releases prior to Avaya Oceana® 3.7, after the Avaya Oceana® and Avaya Control Manager switchover to the DR location, an Avaya Control Manager administrator must manually re-configure the settings for the following applications in the Avaya Oceana® UCA instance in the DR site. The administrator performs these update tasks using the Avaya Control Manager web application. These settings are added at deployment time and when a switchover or switchback is required, the toggle button is used in Avaya Control Manager.

- Omnichannel DB IP/FQDN
- Workspaces Widget Server IP/FQDN
- Workspaces Home Page URL
- Avaya Analytics Server (Streams Server)

For both the partial and full DR switchover scenarios, the toggle button can be used on the ACM application server in the DR location to adjust to values suitable to the Avaya Oceana® deployment at the DR site.

Using Toggle button to switch Avaya Control Manager in Data Center 1 to use Avaya Oceana® applications in Data Center 2

Before you begin

You must have access to the Data Center 1 and Data Center 2 Avaya Control Manager servers.

Procedure

1. On the Avaya Control Manager webpage in DC1, go to Locations tab.
2. Select Data Center 1 location and click **Edit**.
3. Select the applications that you want to switchover to the set of applications in the DR site.

   For a partial DR switchover, select Avaya Oceana® and Avaya Analytics™.
4. Click **Toggle** to use the applications from Avaya Oceana® in DC2

   Verify switched over status in the Switched Over Column for Avaya Oceana® and Avaya Analytics™ servers.

   For a full DR switchover, perform this procedure on Avaya Control Manager in Data Center 2 after the Avaya Control Manager switchover from Data Center 1 to Data Center 2. Select the Communication Manager server entry for switchover.

Configuring the Web Voice and Web Video switchover

About this task

Use this procedure to re-configure a deployed customer web voice and video capabilities after completing the switchover to Avaya Oceana® in the DR site.

Procedure

1. Change the DNS mapping of the Authorization token service FQDN to map to the public address of the Authorization token service in the DR site
2. Change the DNS mapping of the Avaya Aura® Web Gateway server FQDN to map to the public address of the Avaya Aura® Web Gateway server in the DR site.
3. Change the DNS mapping of the AvayaMobileCommunications cluster FQDN to map to the public address of the AvayaMobileCommunications cluster in the DR site

   After the DNS changes take effect, all new call requests from web and mobile clients go to the DR site.
4. Ensure WebRTC Connect on the DR site is configured with suitable WebRTC routing numbers and implicit user details for the DR site operation.

Avaya Workspaces Agent switchover

Agents must re-login to Avaya Oceana® after a switchover. The agents need Avaya Workspaces URL for Data Center 2.

The default Avaya Workspaces URL for both locations are:

- Primary Site:

  ```
  http(s)://<UAC Cluster IP/FQDN/services/UnifiedAgentController/
  workspaces/exit.html
  ```

- DR Site:

  ```
  http(s)://<DR Cluster 2 IP/FQDN/services/UnifiedAgentController/
  workspaces/exit.html
  ```

Ensure all Oceana and Analytics users have the required Security Certificates installed in their client PC trust store to successfully access Workspaces and Analytics functionality when the DR site is in operation.

Validate and test deployed channels

After switchover, verify if the elements in the DR location are active. You must also validate routing of the deployed channels.

Chapter 6: Procedures for planned and unplanned recovery and switchback

Recovery to primary Data Center from DR operations

Switchback from unplanned maintenance windows

A switchback is always a planned maintenance window regardless of how the system underwent a switchover. After failures and switchover to the DR site, after the primary site failure is corrected and the primary site is functional and ready to resume contact processing, you must re-instate the primary site as the operational data center. The disaster recovery at the DR site only functions only for a limited time period due to the licensing restrictions with ESS.

When you re-instate Data Center 1 (DC1), ensure that the data in Avaya Aura® System Manager and Avaya Control Manager is aligned with the data on Avaya Aura® Communication Manager. The administrative changes from Data Center 2 (DC2) are not present on Avaya Aura® Communication Manager in Data Center 1, so Avaya Aura® System Manager and Avaya Control Manager must have data corresponding to Avaya Aura® Communication Manager prior to the switchover to Data Center 2.

Note:

You must perform the recovery operations in a planned maintenance window. During this maintenance window, Avaya Oceana® cannot process any contacts. If the contact center needs to process voice contacts during the maintenance window, it is recommended to use the fallback to Elite feature that can be automatically invoked once Avaya Oceana® is out of service. There is no fallback alternative for Digital Contacts.

Switchback from planned maintenance windows

After planned switchovers to the DR site either partial or full, implement a planned switchback to re-instate the primary site as the operational data center. The disaster recovery at the DR site functions only for a limited time period due to the licensing restrictions with ESS.

Switchback from Full DR Switchover

When you re-instate DC1, ensure that the data in Avaya Aura® System Manager and Avaya Control Manager is aligned with the data on Avaya Aura® Communication Manager. The administrative changes from DC2 are not present on Avaya Aura® Communication Manager in DC1, so Avaya Aura® System Manager and Avaya Control Manager must have data corresponding to Avaya Aura® Communication Manager prior to the switcback to DC1.

Switchback from Partial DR Switchover

In a partial switchover, Avaya Aura® System Manager, Avaya Aura® Communication Manager, and Avaya Control Manager are not switched from the primary site to the DR site.

When you re-instate the primary site, the Avaya Aura® System Manager and Avaya Control Manager are aligned with the data on Avaya Aura® Communication Manager.

Note:

You need a maintenance window to perform the recovery regardless of the switchover option performed. During this maintenance window, Avaya Oceana® cannot process any contacts. If the contact center needs to process voice contacts during the maintenance window, it is recommended to use the fallback to Elite feature that can be automatically invoked once Avaya Oceana® is out of service. There is no fallback alternative for Digital Contacts.

The following table provides a checklist of the procedures to perform for switchback operations to the primary site following a planned or unplanned switchover to the DR site.

The switchback procedures are listed in the order of a switchback from the DR system to the primary system.

Note:

Each customer deployment has different Avaya Oceana® channels enabled. You can xxecute procedures only on channels that are deployed in each solution. A Yes or No in the following table only applies if the customer solution deploys the channel or capability.

Ensure DC1 is fully re-instated and all failures caused by the initial unplanned switchover to DC2 are corrected. For planned switchovers, it is assumed that there were no failures and DC1 was simply put into standby mode.

Functional Area	Procedure High Level Description	Mandatory for Partial DR Switchback	Mandatory for Full DR Switchback
Preparation for Switchback	Download Avaya Oceana® and Avaya Analytics™ Disaster Recovery guide.	Yes	Yes
	Download Avaya Aura® System Manager Administration guide.	Yes	Yes
	Download Avaya Control Manager HA guide.	Yes	Yes
	Download administration guides for AES and CM.	Yes	Yes
	Agree Maintenance Windows Date, Time and Duration as Avaya Oceana® and Avaya Analytics™ are out of Production.	Yes	Yes

Table continues…

Functional Area	Procedure High Level Description	Mandatory for Partial DR Switchback	Mandatory for Full DR Switchback
Validation of DC1 status prior to Switchback			
Validation of DC1 functionality prior to switchback from DC2	Validate identical software levels on following applications across DC1 and DC2. • System Manager • Avaya Control Manager • Communication Manager • Application Enablement Services • Avaya Oceana® • Avaya Analytics™ • Avaya Breeze® platform • Omnichannel	Yes	Yes
	Re-Instate System Manager replication to DC2 System Manager and validate successful replication to System Manager DR. Do not proceed if you cannot enable System Manager replication.	Yes	No
	Validate System Manager primary replication and synchronization to all Avaya Breeze® platform nodes in DC1 and DC2.	Yes	Yes
	Validate that System Manager primary manages all Avaya Breeze® platform nodes in primary and DR sites.	Yes	Yes

Table continues…

Functional Area	Procedure High Level Description	Mandatory for Partial DR Switchback	Mandatory for Full DR Switchback
	Validation of Avaya Control Manager Application and Database Status in DC1 and DC2.	Yes	Yes
	Validation of Omnichannel Database mirroring from DC2 to DC1.	Yes	Yes
Validation of Avaya Oceana® Snapin Status in DC1 prior to switchback	Validation of Email Snapin Deployment status in DC1, if Email is deployed.	Yes	Yes
	Validation of CustomerController snapin status in DC1, if Chat is deployed.	Yes	Yes
	Validation of Messaging Service snapin status in DC1, if either Social or SMS is deployed.	Yes	Yes
	Validation of Generic snapin status in DC1, if Generic is deployed.	Yes	Yes
	Validation of Avaya WebRTC Connect snap-in status in DC1, if WebRTC Connect is deployed.	Yes	Yes
DC1 Only	On DC1 Avaya Oceana®, reset UCA Geo Attributes to default settings (replication off) and reboot Avaya Oceana® Cluster 1 in DC1. Validate that Avaya Oceana® Cluster 1 is fully up and set to Deny Mode and UCAStore Gateway PU is not displayed in Oceana Monitor.	Yes	Yes
Commence Graceful Shutdown of DR Applications			

Table continues…

Functional Area	Procedure High Level Description	Mandatory for Partial DR Switchback	Mandatory for Full DR Switchback
Controlled Shutdown of all DC2 deployed channels	Graceful Shutdown incoming Voice Contacts to DC2.	Yes	Yes
	Graceful Shutdown of Email channel in DC2.	Yes	Yes
	Graceful Shutdown of Chat channel in DC2.	Yes	Yes
	Graceful Shutdown of Messaging Service Snapin in DC2 if SMS or Social is deployed.	Yes	Yes
	Graceful Shutdown of Generic channel in DC2.	Yes	Yes
	Graceful Shutdown of incoming WebRTC Connect contacts to DC2.	Yes	Yes
	Validate that there are no active or queued contacts in DC2.	Yes	Yes
	Validate that all agents are logged out of DC2.	Yes	Yes
	Set DC2 Cluster Status to Standby using Oceana Manager.	Yes	Yes
DR Applications Shutdown, Begin Switchback to Primary Site DC1			
Switchback Operations from DC2 to DC1	Switchback Communication Manager from DC2 ESS back to Communication Manager DC1.	No	Yes
	Switchback PSTN Voice Channels from Avaya Oceana® DC2 to Avaya Oceana® DC1.	Yes	Yes
	Validate that all Avaya Breeze® platform nodes replicating and Managed by primary System Manager in DC1.	No	Yes

Table continues…

Functional Area	Procedure High Level Description	Mandatory for Partial DR Switchback	Mandatory for Full DR Switchback
	Perform process to restore UCAStore DB from DC2 to DC1. This involves UCA DB backup and restore to UCA primary.	Yes	Yes
	Perform process to restore UCM DB from DC2 to DC1. This involves UCM DB backup and restore to UCM DB primary. UCM DB is required to preserve deferred emails.	Yes	Yes
	Perform procedures to ensure EDM DB from DC2 is identical to EDM DB on DC2 post switchback.	Yes	Yes
	Perform Omnichannel switchback from DC2 to DC1. Re-enable Mirroring if required.	Yes	Yes
	Perform Avaya Analytics™ switchback from DC2 to DC1.	Yes	Yes
	Enable Avaya Oceana® in DC1 using Oceana Manager to set DC1 to Active and DC2 to Standby.	Yes	Yes
	Switchback Avaya Control Manager and Avaya Control Manager database from DC2 to DC1.	No	Yes
	Switchback optional WebRTC Connect Voice and Video from DC2 to DC1.	Yes	Yes

Table continues…

Functional Area	Procedure High Level Description	Mandatory for Partial DR Switchback	Mandatory for Full DR Switchback
	Use Avaya Control Manager Toggle button switch Avaya Control Manager point to Avaya Oceana® UCA DC1.	Yes	Yes
	Reconfigure Avaya Control Manager in DC1 to connect to primary Communication Manager.	No	Yes
	Set Email snap-in deployment attribute to false in DC2.	Yes	Yes
	Reconfigure Avaya Control Manager UCA in DC1 to connect to Omnichannel, Widget Server, Avaya Workspaces Home Page URL and Avaya Analytics™ Server in DC1.	Yes	No
	Reboot Avaya Oceana® Cluster 1, Avaya Oceana® Cluster 2, and Avaya Oceana® Cluster 3 in DC1.	Yes	Yes
	Validate that all Avaya Oceana® services and PU's active in DC1 including UCAStore Gateway and CSManager Gateway for UCA and Context Store replications.	Yes	Yes
	Log in agents using DC1 Workspaces and Test deployed Channel Routing.	Yes	Yes
Avaya Oceana® Primary in Production; DR Site in Standby			

After you complete these procedures, operations can commence using infrastructure in the primary site (DC1).

Validating DC1 Status prior to Switchback

Agree for switchback for planned maintenance window time and duration

Planned maintenance windows for switchback require planning and scheduling for the switchback. During the maintenance window, the solution is out of operation. Times for switchback varies depending on whether a partial or full DR switchover was initially implemented.

For all planned maintenance windows of a DR solution, it is recommended to plan for a minimum of eight hours, but the tasks takes considerably longer that this minimum recommended time.

The other major difference between a switchback and a switchover is that you must reinstate all failed elements that caused a switchover in Data Center 1 before the switchback can take place and restore normal disaster recovery functionality.

Validate identical software levels on Data Center 1 and Data Center 2

For a planned switchover and switchback testing, software versions and levels on both Data Center 1 and Data Center 2 must be identical.

You must validate the following applications and platforms:

- Avaya Aura® System Manager
- Avaya Control Manager
- Avaya Breeze® platform
- Avaya Aura® Communication Manager and ESS
- Avaya Aura® Application Enablement Services
- Avaya Analytics™
- Avaya Oceana® Snap-ins
  - Snapin versions on primary and DR must be identical prior to starting an upgrade

For software upgrade maintenance windows, it is acceptable to have different software versions during the upgrade process. For unplanned maintenance windows due to application failures, there is no difference in software versions. You can create a checklist to record the software versions of each application for Data Center 1 and Data Center 2.

Re-Instate Avaya Aura® System Manager

Re-instate Avaya Aura® System Manager primary in Data Center 1 replication to Geo Standby in Data Center 2

Before any switchback, re-establish original System Manager primary and System Manager disaster recovery with replication from Data Center 1 (DC1) to Data Center 2 (DC2) regardless of the current state of the system post switchover. You must also verify the health of System Manager DC1 and DC2 replication state. You must have a healthy replication state between System Manager in DC1 and the System Manager in DC2.

At this point in the process, a partial or full switchover can occur. It can occur due to a failure or a planned maintenance window for testing the disaster recovery capabilities. Regardless of the current state of the two System Manager, reinstate their original deployed state before proceeding any further with the switchback. This means that you must have a primary System Manager in DC1 replicating to a standby System Manager in DC2.

If the switchover was caused by the failure or loss of the primary System Manager, you must first reinstate the failed System Manager and replication before attempting a switchback.

If the switchover was a planned full DR switchover, then the role of the primary is taken over by System Manager in DC2. Reverse with a System Manager switchback.

If a planned partial DR switchover occurred, then the roles of the System Manager is not changed from their original deployed state and further action is not required.

Checklist for Avaya Aura® System Manager switchback

No.	Task	Description	Notes	✔
1	For full DR switchbacks, deactivate the secondary System Manager server	Deactivate the secondary System Manager server.	For more information, see *Administering Avaya Aura® System Manager*.	
2	For full DR switchback, restore the primary System Manager server	After you deactivate the secondary System Manager server, restore the Primary System Manager server.	For more information, see *Administering Avaya Aura® System Manager*.	

Verifying Avaya Aura® System Manager from Data Center 1 to Data Center 2

About this task

When Data Center 1 (DC1) contains the primary Avaya Aura® System Manager and DC2 contains the Geo or standby Avaya Aura® System Manager, you must check Avaya Aura® System Manager replication status from DC1 to DC2.

Procedure

1. On the primary System Manager web console, navigate to **Application State** widget. Verify the following states:
   - GR Server Role is Active
   - GR Server Mode is Active
   - GR Replication is Active
2. Click **Services** > **Geographic Redundancy** > **GR Health**. Verify that Database Replication, File Replication, and Directory Replication are in green color and is Successful.

   If any of the element is in red color and is in Failure or Stopped state, then do not proceed with the switchover and contact the system administrator to correct any problems.
3. On DC2 System Manager web console, in the **Application State** widget, verify the following states:
   - GR Server Role is Standby
   - GR Server Mode is Active
   - GR Replication is Active
4. Verify the status of elements in **GR Health**.

   If any of the element is in red color and is in Failure or Stopped state, then do not proceed with the switchover and contact the system administrator to correct any problems.

Validating Avaya Aura® System Manager and Avaya Breeze® replication status

About this task

Before starting switchover or switchback procedures, you must synchronize Avaya Oceana® and Avaya Breeze® platform nodes and replicate with either primary or DR System Manager.

Procedure

1. After a partial DR switchover, log in to the primary System Manager web console.

2. Click **Services** > **Replication**.
3. After a full DR switchover, log in to the DR System Manager web console.
4. Click **Services** > **Replication**.
5. Validate the replica groups synchronization status is `synchronized` and displays the word `Synchronized in green color`.
    a. Click **Avaya Breeze replica group**.
    b. Verify that **Breeze Node Synchronization** status is `Synchronized`.
    c. Verify that the synchronization dates are not greater than 1 month from the current date.
    d. If any Breeze element is displaying a status Synchronizing, or Repairing, wait until the process completes and verify the status is Synchronized.
    e. If any Breeze Node is not Synchronized, do not proceed any further with the switchover process until the issue is addressed and corrected.

Verifying Avaya Breeze® platform node controller

About this task

Use this procedure to verify, that the Avaya Breeze® platform nodes managed by the primary System Manager.

This procedure is not required in a partial DR switchover because all the Avaya Breeze® platform nodes is managed by the primary System Manager.

You can perform this procedure if a full DR switchback is in progress.

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. In the **Managed by** field, verify that system displays **Primary** for the Avaya Breeze® platform nodes. If not, consult the system administrator to correct this issue before proceeding with the switchback.

Validate Avaya Control Manager Database HA Replication Status

About this task

For all switchback operations, verify the Avaya Control Manager Database HA feature as operational before proceeding with either of the procedures. For instructions on how to perform this validation, see *Avaya Control Manager HA* guides available on Avaya support site.

Validating Avaya Oceana® core components replication operational before switchback

About this task

Before any planned switchback to the re-instated DC1, verify that the health status of the application that replicate data from the DC2 to DC1 is fully operational.

Using Cache Mirroring from DR to primary, Omnichannel Database replicate data from the DC2 to DC1 after a planned switchover. If this was an unplanned switchover due to failures, then Omnichannel Database does not replicate any data and you must reinstate its replication capabilities after completing the switchback to DC1.

Omnichannel DB must have its replicating function validated before attempting a switchback. Failure to perform this validation can lead to issues during the switchback process.

Verifying Omnichannel database mirroring status

About this task

For all planned full and partial DR switchovers, the Omnichannel DB servers in both locations are not failed and data is mirrored between each other. Post a planned switchover, mirroring is from the DR (DC2) site to the original primary (DC1) site.

For unplanned switchovers due to Omnichannel failures, reinstate the failed servers first, and then reinstate mirroring. Refer the later chapters in this document for procedures to reinstate a failed Omnichannel server before proceeding with the switchover.

Assuming that mirroring is enabled from the DR to Primary servers, you need to verify that is the actual situation before switchback. This is the baseline require to be operational before switchback.

For more information, see procedure in Verifying Omnichannel Database mirroring status on page 45.

Validating Avaya Oceana® snap-in shutdown or deployment status in primary site before switchback

About this task

Before any planned switchback from the newly prompted DR site DR site, you must validate the deployment status of Avaya Oceana® snap-ins and the configured attribute values. There can be previous switchovers and switchbacks performed on the system where many attributes are modified as part of these processes. It is important to validate these attribute values for channel snap-ins. Otherwise, this impacts a successful switchback process and requires manual intervention to correct any issues. This also requires additional restart of the Avaya Oceana® clusters to complete the switchback.

Note:

You must perform all operations in this section using the reinstated primary site System Manager.

Verifying deployment mode status of primary site email snapin

About this task

The email snapin deployment mode status attribute in the primary site must be validated as false post a switchback.

If you do not have email channel deployed on Avaya Oceana®, you can skip this procedure.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the primary site Service Clusters tab, do the following:
   a. **Cluster**: Select primary Cluster 3.
   b. **Service**: Select `EmailService`.
3. In the **Advanced** area, in the **Deployment status of emailmanager** field, ensure that the field value is set to `true`.

   Note:

   Setting the field value to `true` triggers the deployment. The default value is `true`.
4. Click **Commit**.
5. Reboot the Avaya Oceana® Cluster 3.

Verifying shutdown mode status of primary site CustomerController chat snap-in

About this task

The CustomerController snap-in is responsible for allowing chat contacts to enter Avaya Oceana® ecosystem. Before switchback from the DR site, validate the shutdown mode status attribute in the primary site for this snapin as false.

If you do not have chat channel deployed on Avaya Oceana®, you can skip this procedure.

Procedure

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

2. On the primary Site Service Clusters tab, do the following:
   a. **Cluster**: Select `primary Cluster 3`.
   b. **Service**: Select `CustomerControllerService`.
3. In **Shutdown Mode** status, validate that the field value is set to false. If it is set to true, then set to false and Commit the change.

   You do not need to reboot Avaya Oceana® Cluster 3.

Verifying shutdown mode status of primary site MessagingService snapin

About this task

The MessagingService snap-in is responsible on the front-end for a number of Avaya Oceana® channel snap-ins such as SMS, Social, or Async. To ensure a smooth switchback, it is required, to validate the shutdown mode attribute status for this snap-in in the primary site prior to the switchback.

If you do not have SMS, Social, or Async channel deployed on Avaya Oceana®, you can skip this procedure.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the primary Site Service Clusters tab, do the following:
   a. **Cluster**: Select `primary Cluster 3`.
   b. **Service**: Select `MessagingService`.
3. In **Shutdown Mode** status, validate that the field value is set to false. If it is set to true, then set to false and Commit the change.

   You do not need to reboot Avaya Oceana® Cluster 3.

Verifying shutdown mode status of primary site GenericChannelAPI snap-in

About this task

The GenericChannelAPI snap-in is responsible for getting generic contacts into the Avaya Oceana®. To ensure a smooth switchback, you must validate the shutdown mode attribute status for this snap-in in the primary site prior to the switchback.

If you do not have generic channel deployed on Avaya Oceana®, you can skip this procedure.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the primary Site Service Clusters tab, do the following:
   a. **Cluster**: Select `primary Cluster 3`.
   b. **Service**: Select `GenericChannelAPI`.
3. In **Shutdown Mode** status, validate that the field value is set to `false`.

   If this value is set to true, then set it to false and commit the change.

   You do not need to reboot Avaya Oceana® Cluster 3.

Verifying deployment status of AMC snap-in for Avaya WebRTC Connect contacts

About this task

The AMC snap-in allows all WebRTC Connect voice and video contacts to enter Avaya Oceana®. To ensure a smooth switchback, you must validate the deployment status of the AMC snap-in PU using Oceana Monitor to ensure if the snap-in is active and operational before the switchback.

If you do not have WebRTC Connect channel deployed on Avaya Oceana®, you can skip this procedure.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration** > **Primary Cluster 1**.
2. In the **Cluster** field, select **Oceana Monitor**.
3. Select **Cluster 2** > **Grid Info** to view the PU status of all the snap-ins.

   Verify if the PU status of amcSpace is Intact. If the status is Scheduled or Broken, then AMC snap-in is not operational and you must correct the issue before proceeding with the switchover. Otherwise, when a switchover is complete, WebRTC Connect voice or video contacts are not routed in Avaya Oceana®.

Prepare primary DC1 Avaya Oceana® for potential UCA and UCM DB restore

About this task

Use this procedure to prepare primary DC1 for potential UCA and UCM database restore.

In the switchback procedures, it is required to restore the data for both UCA and UCM post a partial or full DR switchover.

Procedure

1. Reconfigure UCAStoreService Geo and disaster recovery attributes.
2. Uninstall UCAStore Service and UCM service.
3. Perform a reboot of primary Cluster 1 before restoring either database data.

Configuring primary site UCA as standalone in Data Center 1

About this task

Before switchback to the primary UCA, re-configure manually to be a standalone UCA with the attribute settings to enable replication to the DR UCA temporarily removed. After completing the UCA DB back and restore steps, enable UCA replication again from the primary to the DR site. This does not impact on the current DR production operations.

The following procedure implements two important steps:

- Resets the primary site UCAStoreService geo and disaster recover replication settings to Off.
- Uninstalls the UCA service from the primary Cluster 1 in DC1 so that the UCA database restore from DC2 is picked up by UCA in DC1.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. **Cluster**: Select Avaya Oceana® Cluster 1.
   b. **Service**: Select **UCAStoreService**.
3. For the **Oceana disaster recovery role** option, clear **Override Default**.
4. Click **Commit**.

   Do not reboot any Clusters in the primary at this stage of the procedures.
5. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
6. On the Services page, select the check box of **UCAStoreService** and click **Uninstall**.
7. In the **Confirm Uninstall service: UCAStoreService** dialog box, select the check box of **primary Cluster 1** and click **Commit**.
8. On the Services page, verify that the state of the service is `Uninstalling`.

   The state changes to `Uninstalled` when the process is complete.

Configuring primary site UCMService as standalone in Data Center 1

About this task

Use this procedure to uninstall the UCMService from primary Cluster 1 so that it is ready for any UCM DB restores later in the procedures. This does not impact on the current Avaya Oceana® DR operations.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
2. On the Services page, select the check box of **UCMService** and click **Uninstall**.
3. In the **Confirm Uninstall service: UCMService** dialog box, select the check box of **primary Cluster 1** and click **Commit**.
4. On the Services page, verify that the state of the service is `Uninstalling`.

   The state changes to `Uninstalled` when the process is complete.

Reboot Oceana Cluster 1 in the Primary DC1 site

About this task

Use this procedure to reboot cluster 1 nodes in the primary site. This reboot can happen outside of the maintenance window allocated for the actual switch back to the primary site DC1.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. Select **Primary cluster 1** and reboot.
3. Wait until the reboot of all nodes is complete, and the nodes are back in service in deny mode.

Shutdown DR and switchback to primary for Avaya Oceana® and Avaya Analytics™ operations

This is the actual switchback procedure to switch production operations from the DR site to the original primary site. You can perform a full or partial DR switchback at this point depending on the current requirements.

If a failure in the original primary caused either a partial or full DR switchover, then correct all failures, all failed applications, and resources reinstated before proceeding with the switchback procedures.

The following is the summary of high level functional steps that you must perform to complete the switchback:

Part 1- Shutdown DR Production Operations:

- Shutdown the PSTN Voice channel.
- Shutdown all deployed digital channels such as Chat, SMS, Social, and Generic.
- Shutdown the WebRTC Connect channel.
- Shutdown the POM outbound.
- Validate if all contacts are cleared from Avaya Oceana® queue.
- Ensure that all agents are logged out.
- Re-configure DR AES to connect to ESS.
- Set DR Avaya Oceana® Clusters to Deny state.

Part 2 - Switchback Production to Primary Site:

- Switchback Avaya Communication Manager from ESS.
- Perform Optional UCA Database Restore from DR site.
- Perform Optional UCM Database Restore from DR site.
- Switchback Avaya Control Manager.
- Switchback Omnistore primary to Primary.
- Switchback Avaya Analytics™ primary to Primary.
- Set Oceana Cluster state to Accept in primary site.
- Switchback Web Voice to primary site.
- Set Primary Oceana Clusters to Accept State.
- Login Avaya Oceana® agents to DR site and test all deployed channels functionality.
- Enable all Channels if disabled whilst before performing switchback.

Part 1 – DR site voice channel shutdown and switchback to primary site

About this task

You can omit these instructions if the PSTN channel is not deployed in the solution.

Before switching back to the primary, you must shut down the existing PSTN Voice channel in a graceful manner. The following are some recommendations to shut down incoming voice contacts for the two front end options supported in Avaya Oceana® 3.x.

- For Avaya Oceana® deployments with a front-end application running on Avaya Experience Portal, it is recommended to have a flag is used at the start of the workflow for startup or shutdown operations. Using this flag, the administrator can redirect incoming voice calls to an automated response. The automated response rejects the incoming call or transfers the calls to an alternate call handling mechanism. The Avaya Oceana® 3.x solution uses Avaya Experience Portal voice application, which contains sample code to implement this using Call Application Variables (CAVs). Also, specifies the data center that is operational at a given time. Setting this flag to any of the data center ensures incoming PSTN voice contacts are only routed to that data center. This is a simple and effective method to turn on or turn off incoming voice to an Avaya Oceana® DR system.
- For Avaya Oceana® deployments with Call Center Elite as front end, a CM variable indicating Avaya Oceana® in service or out of service is configured and checked on new incoming voice contacts. If the flag is set to indicate out of service, then new incoming voice contacts are routed to alternate fallback options until the switchback to the DR infrastructure is complete.

Procedure

1. Log in to the Avaya Experience Portal web portal with the Administrator user role.
2. In the navigation pane, click **System Configuration** > **Applications**.
3. Select the application you want to modify, and click **Configurable Application Variables**.
4. In the **Active Data Center** field, click **DataCenter1**.
5. Click **Save**.

   New incoming voice contacts arriving at the application in the Avaya Experience Portal, are routed to the Avaya Oceana® system in the primary location DC1.

Configuring DR site email shutdown

About this task

For switchback, you must change the shutdown status of the EmailService snap-in (if email is deployed) from false to true. An Avaya Oceana® administrator with access to System Manager can change the status. Failure to shut down the email service in the DR site means that all incoming emails to the Avaya Oceana® monitored mailboxes are pulled in by the primary email service after switchback is complete.

If the email channel is not deployed on Avaya Oceana®, you can skip this procedure.

When the administrator shuts down the EmailService using the shutdown mode flag:

- New emails are not retrieved from the email server.
- Outgoing emails are queued within the Cache database.

After completing the switchback process, the EmailService snap-in processes all mails in the DR site and sends all outgoing emails from the DR site.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the primary site Service Clusters tab, do the following:
   a. **Cluster**: Select primary Avaya Oceana® Cluster 3.
   b. **Service**: Select **EmailService**.
3. In the **Deployment Mode** status, do the following:
   a. Select the **Override Default** check box
   b. In the **Effective Value** field, change the value from `true` to `false`.
4. Click **Commit**.

Configuring DR site MessagingService shutdown

About this task

For a planned switchover, an administrator can manually stop new incoming SMS and/or Social contacts from entering the Avaya Oceana® and allow existing contacts to gracefully be processed out of the system. An administrator must set the primary site MessagingService on Avaya Oceana® Cluster 3 to True.

This procedure is required only if the SMS or Social channels are deployed.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the primary Site Service Clusters tab, do the following:
   a. **Cluster**: Select primary Avaya Oceana® Cluster 3.
   b. **Service**: Select **MessagingService**.
3. In **Shutdown Mode** status, do the following:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, change the value from `false` to `true`.
4. Click **Commit**.

Configuring DR site chat shutdown

About this task

For a planned switchover, an administrator can manually stop new incoming chat contacts from entering Avaya Oceana® and allow existing contacts to gracefully be processed out of the system.

An administrator must set the primary site CustomerControllerService on Avaya Oceana® Cluster 3 to True.

This procedure is required only if the chat channel is deployed on Avaya Oceana®.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the primary Site Service Clusters tab, do the following:
   a. **Cluster**: Select primary Avaya Oceana® Cluster 3.
   b. **Service**: Select **CustomerControllerService**.
3. In **Shutdown Mode** status, do the following:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, change the value from `false` to `true`.
4. Click **Commit**.

Configuring DR site GenericChannelAPI Service shutdown

About this task

For a planned switchover, an administrator can manually stop new incoming Generic contacts from entering Avaya Oceana® and allow existing contacts to gracefully get processed out of the system. An administrator must set the primary site GenericChannelAPI on Avaya Oceana® Cluster 3 to True.

This procedure is required only if the Generic channel is deployed on Avaya Oceana®.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the primary site Service Clusters tab, do the following:
   a. **Cluster**: Select primary Avaya Oceana® Cluster 3.
   b. **Service**: Select **GenericChannelAPI**.
3. In **Shutdown Mode** status, do the following:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, change the value from `false` to `true`.
4. Click **Commit**.

Setting the maintenance mode for web voice and web video

For a planned switchback, you must modify the front-end web portals that host the Avaya WebRTC Connect voice or video capabilities to indicate to the end users that the service is temporarily unavailable. Avaya recommends a simple flag to toggle between in service and out of service is utilized for this purpose. There are no configuration flags available in the web voice components.

DR outbound shutdown

The Outbound channel does not support disaster recovery. Therefore, you must stop the running campaigns on the Proactive Outreach Manager server before shutting down Avaya Oceana®.

Validating contacts

For a planned switchback, you must ensure that new contacts do not arrive into the DR Avaya Oceana® once the shutdown process starts. You must also close any Queued or In Progress contacts which an agent is processing. To check if the status of all the current contacts for all channels are Processed and Closed, log in as an Avaya Oceana® supervisor and use Avaya Analytics™ real time displays. For more information, refer Avaya Oceana® and Avaya Analytics™ documentation suite.

Note:

Queued contacts are lost if they are not processed before the switchback to Data Center 1.

Logging out supervisors and agents from the DR site

For a planned switchback, ensure that all Avaya Oceana® agents are logged out. Supervisors can verify agent status using the **My Agents** widget. Supervisors must co-ordinate locally to ensure that the agents are logged out. It is also suggested that supervisors view the Analytics real time dashboard to validate if all users are logged out.

Configuring DR Application Enablement Services server to enable Switch Connection back to ESS

About this task

In the setup instructions for Avaya Oceana® disaster recovery solution, there are two switch connections configured from Application Enablement Services in the DR location. Switch

Connection 1 is the primary Communication Manager and Switch Connection 2 is the ESS. During the switchback procedures, you must reset the active Communication Manager link to the original configured ESS link on the DR Application Enablement Services server or servers.

Procedure

1. On the Application Enablement Services web portal of the DR location, go to **Communication Manager Interface** > **Switch Connections**.

   The Switch Connection tab displays the entries configured from Application Enablement Services. If there are no connections, then contact the system administrator to add the required number of switch connections.
2. On the Application Enablement Services administration portal, go to **Status** > **Status and Control** > **Switch Connection Summary**
3. Set the Switch Connection entry for Communication Manager in the primary location to **offline**.
4. Set the Switch Connection entry for ESS server in the DR location to **online**.
5. On the Application Enablement Services administration portal, go to **Status** > **Status and Control** > **TSAPI Service Summary**.
6. Set the Switch Connection entry for ESS server to `online`.
7. Set the Switch Connection entry for the Communication Manager in the primary location to `offline`.

Put DR Oceana Clusters into Deny Mode – Complete Shutdown of DC2 operations

Changing the Cluster Activity status for the clusters in Data Center 2

Before you begin

You must install OceanaMonitorService on the clusters in Data Center 2.

Procedure

1. Open the Oceana Manager page by entering the following URL in your web browser:

   `https://<DataCenter1_AvayaOceanaCluster1_FQDN>/services/OceanaMonitorService/manager.html?affinity=)`

Important:

Create a bookmark of this URL in your web browser, so that you can open the Oceana Manager page even when System Manager is unavailable.

2. **(Optional)** To open the DR Oceana Manager page through System Manager, do the following:
   a. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
   b. On the Cluster Administration page, in the **Service URL** column for Avaya Oceana® Cluster 1, select **Oceana Manager**.
3. Log in to Oceana Manager using an Admin account.
4. On the Oceana Manager page, do the following:
   a. Verify that the status of the clusters is `ACTIVE`.
   b. Click **Set Cluster Group to Standby** to change the status to `STANDBY` and place all nodes in the Deny New Service mode.
   c. On the confirmation message box, click **OK**.
   d. **(Optional)** If the Oceana Manager page does not display the updated status after some time, click **Refresh**.
   e. Refresh the Clusters page in Avaya Breeze® platform EM and validate that all the clusters in the DR site are not in Deny state.

Part 2 – Switchback Avaya Oceana® and Avaya Analytics™ operations to primary site

This section provides the actual switchback procedures to move production to Avaya Oceana® and Avaya Analytics™ applications and systems back to the reinstated primary location.

Switchback from ESS to Avaya Aura® Communication Manager after full DR switchovers

The ESS to Avaya Aura® Communication Manager recovery is dependent on customer deployment of media servers or gateways. For more information, see White Paper - Communication Manager Survivability in an Environment with Media Servers.

Re-establishing UCA replication from primary UCA to DR UCA

Use the procedures in this section to synchronize the UCAStoreSevice database on both the primary and DR sites. After the databases are synchronized, you can re-establish UCA replication from the primary to the DR site The UCAStoreService database stores static information of Avaya Oceana®. Static information such as users, accounts, attributes, providers, and resources.

Any new updates applied using Avaya Control Manager are stored in the UCA database in the DR site. If you want to save these updates even after switchback to the primary site, then you must implement the following procedures as part of the switchback. For planned partial or full DR switchovers, the customer can decide if they want to retain any new administration data from the UCAStoreService database in the DR site.

If you do not want to retain the data, follow the UCM restore procedure.

Note:

Avaya Control Manager, UCA, and Multimedia Server back up their data independently. Therefore, you must take backups in synchronization and restore them in synchronization.

Taking a backup of UCAStoreService in Data Center 2

About this task

Use this procedure to take a backup of UCAStoreService.

Procedure

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

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

   If you do not specify any value, the backup storage server retains all backup files.

9. Click **Commit**.
10. Select the check box for the DR Avaya Oceana® Cluster 1.
11. From the **Backup and Restore** field, select **Backup**.
12. On the Cluster Database Backup Confirmation dialog box, select the **ucastoreservice** check box and click **Continue**.
13. On Backup and Restore Status page, ensure that the **Status** column for the backup operation displays the value as `Completed`.

Restoring the UCAStoreService data in Data Center 1

Before you begin

Uninstall UCAStoreService from Avaya Oceana® Cluster 1 in Data Center 1 and restart the nodes of the Avaya Oceana® Cluster 1 to delete UCAStoreSpace.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
2. On the Services page, verify that UCAStoreService is not in the `Installed` state.

   UCAStoreService is shown as installed on DR Cluster 1 but not on Primary Cluster 1.
3. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
4. From the **Backup and Restore** field, select **Restore**.
5. On the Backup and Restore Status page, in the Backup and Restore Jobs section, select the check box for the latest backup file and click **Restore**.
6. On the Cluster Database Restore Confirmation dialog box, select Data Center 1 Avaya Oceana® Cluster 1 and click **Continue**.
7. On the Backup and Restore Status page, ensure that the **Status** column for the restore operation displays the value `Completed`.

Installing UCAStoreService in Data Center 1

About this task

Use this procedure to install UCAStoreService on Avaya Oceana® Cluster 1 in Data Center 1.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
2. On the Services page, select the check box of UCAStoreService and click **Install**.

3. In the Confirm Install service: UCAStoreService dialog box, select the check box of Avaya Oceana® Cluster 1 and click **Commit**.
4. On the Services page, verify that the state of the service is `Installing`.

   The state changes to `Installed` when the installation is complete.
5. Restart the Avaya Breeze® platform nodes of Avaya Oceana® Cluster 1.

   If you are planning to perform a UCM DB restore, then do not restart the primary Cluster 1 in the switchback process. However, perform instructions on how to restore UCM database from the DR site. If you are not planning to perform a UCM DB restore, then restart primary cluster 1 to become fully operational.

Restoring UCM

UCMService defer data backup

UCMService persists metadata related to deferred emails. UCMService requires this data to retrieve expired deferred emails and route them back to the appropriate agent.

This information is updated in real-time. Therefore, you must take backups during the following events:

- Planned switchover and recovery
- Unplanned switchover and recovery

Note:

You can skip the procedures for the following:

- The email channel is not deployed at this installation and therefore there are no deferred email capabilities
- The partial or full DR switchover is for test purposes and you do not want to keep new UCM data post switchback to the primary site.

Taking a backup of UCMService during planned switchback and recovery

About this task

Use this procedure to take a manual backup of the UCMService database during planned switchover and switchback.

Before you begin

Ensure that all agents are logged out of their accounts.

Procedure

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

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

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

    Important:

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

Taking a backup of UCMService during unplanned switchover and recovery

About this task

Use this procedure to schedule automatic backups of the UCMService database to maintain a reasonably up to date data set in the event of an unplanned switchover and recovery from Data Center 1 to Data Center 2.

Procedure

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

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

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

    Important:

    Make a note of the password because you require this password to restore UCMService.
14. In the **Schedule Job** field, click **Schedule later**.
15. In the **Task Time** field, specify the date, time, and timezone for the first backup.
16. In the **Recurrence** field, select the **Tasks are repeated** option and specify the recurring backup schedule.
17. In the **Range** field, specify a range for the recurring backup schedule.
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`.

Restoring the UCMService data for Avaya Oceana® Cluster 1 in Data Center 1

About this task

Use this procedure to restore a UCMService database backup to the primary Avaya Oceana®.

If the email channel is not deployed on Avaya Oceana®, you can skip this procedure.

Before you begin

- Ensure that all agents are logged out of their accounts.
- Ensure that the state of Avaya Oceana® Cluster 1 and Avaya Oceana® Cluster 3 is `Deny New Service`.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
2. On the Services page, verify that UCMService is not in the `Installed` state.
3. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
4. From the **Backup and Restore** field, select **Restore**.
5. On the Backup and Restore Status page, in the Backup and Restore Jobs section, select the check box for the latest backup file and click **Restore**.
6. On the Cluster Database Restore Confirmation dialog box, select Avaya Oceana® Cluster 1 and click **Continue**.
7. On the Backup and Restore Status page, ensure that the **Status** column for the restore operation displays the value `Completed`.
8. Install UCMService on Avaya Oceana® Cluster 1.
9. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
10. On the Services page, select the **UCMService** check box and click **Install**.
11. In the Confirm Install service: UCMService dialog box, select the primary Avaya Oceana® Cluster 1 check box and click **Commit**.
12. On the Services page, verify that UCMService is in the `Installed` state.
13. Restart the Avaya Breeze® platform nodes of Avaya Oceana® Cluster 3.

    Reboot of the Avaya Breeze® platform nodes of Avaya Oceana® Cluster 3 is necessary for an unplanned restore, so that any deferred emails that are not included in the backup file are presented as new emails.
14. Restart the Avaya Breeze® platform nodes of Avaya Oceana® Cluster 1.

If you are planning to perform a UCM DB restore, then do not restart the primary Cluster 1 in the switchback process. However, perform instructions on how to restore UCM database from the DR site. If you are not planning to perform a UCM DB restore, then restart primary cluster 1 to become fully operational.

Restoring Avaya Control Manager

You must restore Avaya Control Manager in DC1 to the same level of data as Avaya Aura® Communication Manager and System Manager. Avaya Control Manager is restored from a backup prior to the failure. In a planned switchover, there is no requirement to restore Avaya Control Manager.

Avaya Control Manager switchback from DR to primary site

This section provides information on the options available on switchback from the Avaya Control Manager servers in the DR site to the set of servers in the primary site. For a planned maintenance window and a partial DR switchover, it is not required to switchback Avaya Control Manager servers.

For a planned maintenance window and a full DR switchover, you must perform switchback of Avaya Control Manager application and database server. Due to failures of the Avaya Oceana® applications where Avaya Control Manager is operational in primary site, Avaya Control Manager switchback is not required. Avaya Control Manager supports several HA and DR models that are beyond the scope of this document. These models are independent of the Avaya Oceana® DR deployment. The information about the models and how to setup Avaya Control Manager HA and DR is covered in the Avaya Control Manager documentation suite.

For more information, see *Installing Avaya Control Manager for Enterprise - Multiplex High Availability* and *Installing Avaya Control Manager for Enterprise - Legacy High Availability* documents.

ACM Toggle Button Utility after switchback to primary

Reconfiguring Avaya Control Manager in switchback scenarios

Overview

With the Toggle feature of Avaya Control Manager, an administrator can toggle a flag to configure Avaya Control Manager with the settings required for Avaya Oceana® in the primary or DR locations.

This toggle feature allows the Avaya Control Manager application server to identify which Avaya Oceana® UCA instance to administer Avaya Oceana® configuration data. The toggle button can also be used when performing a switchover or a switchback.

The procedures in this section are applicable following a successful switchback to the primary Avaya Control Manager applications. In Avaya Control Manager 9.x, you must manually update the following parameters when doing a switchback to the primary Avaya Control Manager application using the toggle button.

- Omnichannel DB IP/FQDN
- Workspaces Widget Server IP/FQDN
- Workspaces Home Page URL
- Avaya Analytics Server (Streams Server)

Using the Toggle button to switch back Avaya Control Manager in Data Center 1

About this task

With this procedure, you can use the Toggle button to switch back Avaya Control Manager in Data Center 1 so that you can use Avaya Oceana® applications in Data Center 1.

Before you begin

You must have access to the Data Center 1 and Data Center 2 Avaya Control Manager servers.

Procedure

1. Log in to Avaya Control Manager.
2. On the Avaya Control Manager webpage, click **Configuration** > **Locations**.
3. On the Location List page, Select the Data Center 1 location and click **Edit**.
4. Select the applications that you want to switch back to the applications in the restored primary site.
5. For a partial DR switchover, select Avaya Oceana® and Avaya Analytics™.
6. Click **Toggle** to use the applications from Avaya Oceana® in DC2.
7. Verify the switched back status in the **Switched Over** column for Avaya Oceana® and Avaya Analytics™ servers.

Reconfiguring Avaya Oceana® addresses to DC1

About this task

Use this procedure to restore and reconfigure multiple fields in Avaya Control Manager to point to local hostnames or IP addresses at Data center 1.

Procedure

1. Log on to Avaya Control Manager with an administrator user role.
2. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Server Details**.
3. Double-click the **UCAServer** instance.
4. Select the **System Properties** tab.

5. Expand **Omni Channel**.
6. In the **Omni Channel Database Server** field, update the hostname or IP address pointing to the Omnichannel server in Data center 1.

   Note:

   Enter the hostname of the VIP if using Omnichannel database mirroring. Otherwise, enter the name of the Omnichannel Database server as administered in the HTTPS certificate installed on the Omnichannel Database server. However, for lab deployments customers you can use IP address.
7. In the **Workspaces** field, enter the Welcome Page URL for Data Center 1 operations.
8. In the **Workspaces** field, enter the Widget Web Server URL link for Data Center 1 operations.
9. Click **Save**.

Configuring the UCA URL to point to Data Center 1

About this task

Use this procedure to update the Oceana Server Details and Avaya Analytics™ Streams server details in Avaya Control Manager to point to the Avaya Oceana® Cluster 1 address in Data Center 1.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Server Details**.
2. On the Avaya Oceana Server List page, double-click the UCAServer server.
3. On the Avaya Oceana Server Edit page, in the **API URL** field, update the URL to point to the Avaya Oceana® Cluster 1 address in Data Center 1.
4. Click **Save**.
5. On the Avaya Control Manager webpage, click **Configuration** > **Customer Engagement** > **Avaya Analytics™**.
6. On the Avaya Analytics Server List page, double-click the Avaya Analytics™ Streams server.
7. In the **API URL** field, update the URL to point to the Avaya Oceana® Cluster 1 address in Data Center 1.
8. Click **Save**.

Clean up and reconfigure Mirror setup on DC1 and DC2

For switchback to Cache server DC1 site, you must manually remove mirroring configuration and re-setup. Perform the procedure only when all Cache servers in DC1 and DC2 are available.

Important:

For both planned maintenance and un-planned switchovers, mirroring must be re-configured as part of the switchback procedure.

Before performing the procedures, ensure that you have deployed the following Omnichannel Database servers:

- Omnichannel Server A as the original primary member on DC1
- Omnichannel Server B as the original standby member on DC1 if you have dual server pair setup on DC1
- Omnichannel Server C as the original async member on DC1 which is now the primary member after switchover

Note:

If you do not have dual server setup on DC1, you can ignore Removing mirroring configuration on Omnichannel Server B on page 116.

Removing mirroring configuration on Omnichannel Server A

Procedure

On the Omnichannel Server A in the primary site, do the following:

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

   `http://<DC1OmnichannelServerIP>:57772/csp/sys/UtilHome.csp`

   <DC1OmnichannelServerIP> is the IP address of the active Omnichannel Database server in Data Center 1.

2. On the Cache Management Portal login page, do the following:
   a. In the **User Name** field, type `_admin`.
   b. In the **Password** field, type `Oceana16`.
   c. Click **LOGIN**.
3. Go to **System Administration** > **Configuration** > **Mirror Settings** > **Edit async**.
4. Select **Remove mirror configuration**.
5. For Remove mirror attribute, select `Yes`.
6. Click **Remove**.
7. Remove any Journal files beginning with MIRROR in `E:\AVAYA\OCEANA\DATABASES\JOURNAL` where E represents the Journal drive.

Removing mirroring configuration on Omnichannel Server B

Procedure

On the Omnichannel Server B in the primary site, do the following:

1. In system management tray, right-click the greyed out Cache cube icon.
2. Select **Start Cache**.
3. Navigate to the Cache Management Portal.
4. Navigate to **System Administration** > **Configuration** > **Mirror Settings** > **Edit mirror**.
5. Select **Remove mirror configuration**.
6. For Remove mirror attribute, select `Yes`.
7. Click **Remove**.
8. Remove any Journal files beginning with MIRROR in `E:\AVAYA\OCEANA\DATABASES\JOURNAL` where E represents the Journal drive.

Removing mirroring configuration on Omnichannel Server C

Procedure

On the Omnichannel Server C in the DR site, do the following:

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

   `http://<DC1OmnichannelServerIP>:57772/csp/sys/UtilHome.csp`

   where <DC1OmnichannelServerIP> is the IP address of the active Omnichannel Database server in Data Center 1.
2. On the Cache Management Portal login page, do the following:
   a. In the **User Name** field, type `_admin`.
   b. In the **Password** field, type `Oceana16`.
   c. Click **LOGIN**.
3. Navigate to **System Administration** > **Configuration** > **Mirror Settings** > **Edit mirror**.
4. Select **Remove mirror configuration**.
5. Select **Clear mirror flag**.
6. In system management tray, right-click the greyed out Cache cube icon.
7. Select **Stop Cache**.
8. Select **Restart**.
9. Navigate to the Cache Management Portal.

10. Navigate to **System Administration** > **Configuration** > **Mirror Settings** > **Edit mirror**.
11. Select **Remove mirror configuration**.
12. For Remove mirror attribute, select `Yes`.
13. Click **Remove**.
14. Remove any Journal files beginning with MIRROR in `E:\AVAYA\OCEANA\DATABASES\JOURNAL` where E represents the Journal drive.

Creating a data backup on Server C

Procedure

1. Navigate to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement folder`.
2. Double-click the `OceanaDataManagementTool.exe` file.
3. In the Oceana Data Management utility, click **Backup And Restore**.
4. In the navigation pane, click **Backup And Restore**.
5. In the **Select/create file to backup to** field, click **Browse**.
6. On the Save As screen, select the location where you want to save the backup file.

   Important:

   Do not save the backup file to the software, journal, or multimedia drive.
7. Specify a name for the backup file.

   Note:

   When naming the file, use English or numeric characters only.
8. Click **Save**.
9. Click **Backup Database**.

   The application displays the `Backup complete!` message when the backup process is complete.

Next steps

Verify that the backup file is created at the specified location.

Restoring data on Server A

Procedure

1. Copy the backup file from Server C to Server A.

2. Navigate to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement` folder.
3. 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 file to restore from** field, click **Browse**.
7. On the Open dialog box, browse to the location where you stored the backup file.
8. Select the backup `.cbk` file.
9. Click **Open**.
10. Click **Restore Database**.
11. For **Are you restoring a mirrored backup**, click **Yes**.
12. Click **Restore**.

    The application displays the `Restore complete!` message after the restore process is completed.

Configuring Omnichannel database mirroring between DC1 and DC2

To re-establish configuration between DC1 and DC2, see Omnichannel database mirroring configurations on page 36.

Configuring CallServerConnector attributes on Data Center 2

About this task

On recovery of Data Center 1, you must undeploy the CallServerConnector service on Data Center 2.

Procedure

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

3. In **Deploy CSC**, do the following:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, change the value from `true` to `false`.
4. Click **Commit**.

Restoring Context Store External Data Mart server

Context Store External Data Mart (EDM) is an external component of the Avaya Oceana®. When you restore back to Data Center 1, you must copy the EDM contents from Data Center 2 to the EDM in the Data Center 1. Ensure that you backup and restore the database to complete the restoring of Context Store EDM.

Changing the Cluster Activity status of Data Center 1 components

Before you begin

You must install OceanaMonitorService on the clusters in the primary site as it is required later in the procedure to verify the deployment of the CSC PU.

Procedure

1. Open the primary Oceana Manager page by entering the following URL in your web browser:

   ```
   https://<DR_AvayaOceanaCluster1_FQDN>/services/
   OceanaMonitorService/manager.html?affinity=)
   ```

   Important:

   Create a bookmark of this URL in your web browser, so that you can open the Oceana Manager page even when System Manager is unavailable.

2. To open the Oceana Manager page through System Manager, do the following:
   a. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
   b. On the Cluster Administration page, in the **Service URL** column for primary Cluster 1, select **Oceana Manager**.
3. Log in to Oceana Manager using an Admin account.
4. In your web browser, open the Oceana Manager page by clicking the bookmark that you created while deploying Data Center 1
   a. Check the status of Avaya Oceana® Cluster 1
   b. If the status of the clusters is `STANDBY`, click **Set Cluster Group to Active** to change the status to `ACTIVE`

This action is applied to all the nodes in all the clusters on the primary Avaya Oceana®.

c. On the confirmation message box, click **OK**

d. If the Oceana Manager page does not display the updated status after some time, click **Refresh**

5. Open Oceana Monitor and verify that all the PU's in primary Cluster 1 are set to status INTACT including the CSC PU.
6. Using System Manager, select `primary Cluster 1` and start Oceana Monitor.
7. Verify on Avaya Oceana® Cluster 1 that all PUs are deployed and INTACT including CSC.

   CSC PU is not deployed if the **Oceana** > **CSC** > **AES** > **CM** configuration is not done and validated.
8. On Avaya Oceana® Cluster 3, verify the Email PU and all PUs are deployed and INTACT.
9. Verify that all the nodes and clusters in the primary location are set to status `Accept`.

   If any clusters or nodes are in Deny state, either repeat the Oceana Manager step or manually set them to Accept State using the Breeze EM cluster overview page.

Configuring the Web Voice and Web Video after Switchback

About this task

Use this procedure to re-configure any deployed Customer Web Voice and Video capabilities once the switchback to the Oceana in the primary site is complete.

Procedure

1. Change the DNS mapping of the Authorization token service FQDN to map to the public address of the Authorization token service in the primary site.
2. Change the DNS mapping of the Avaya Aura® Web Gateway server FQDN to map to the public address of the Avaya Aura® Web Gateway server in the primary site.
3. Change the DNS mapping of the AvayaMobileCommunications cluster FQDN to map to the public address of the AvayaMobileCommunications cluster in the primary site.

   After the DNS changes take effect, all new call requests from web and mobile clients go to the primary site.

Avaya Workspaces agent switchover

When all the elements in the restored primary location are active, then the Avaya Workspaces agents must re-login to the primary Avaya Oceana® after a switchback. The agents requires access to the Avaya Workspaces URL for the primary location.

The default Avaya Workspaces URL for both locations are:

Primary Site: `http(s)://<Primary Cluster 2 IP/FQDN/services/UnifiedAgentController/workspaces/exit.html`

DR Site: `http(s)://<DR Cluster 2 IP/FQDN/services/UnifiedAgentController/workspaces/exit.html`

Validate and test deployed channels

After a partial or full switchover, verify if the elements in the primary location are active. You must also validate routing of the deployed channels.

Chapter 7: Additional switchover procedures post unplanned failures in Data Center 1

Additional switchover procedures

This section provides information on additional switchover procedures to the disaster recovery systems as a result of partial or complete primary site failures. The Avaya Oceana® and Avaya Analytics™ solution are designed to cater for a full primary site outage. From Avaya Oceana® 3.7 onwards, it can also cater for partial failures of some of the core application in the solution, which means a switchover to the applications in the DR site can be performed for just the failed applications instead of a total site.

During catastrophic failures of the following applications in the primary site, a partial switchover is performed as per instructions in earlier chapters.

- Failure of the core Avaya Oceana® cluster and Avaya Breeze® platform nodes.
- Failure of one or more of the Omnichannel DB servers.
- Failure of one or more of the Avaya Analytics™ servers.

A full site failure requires a full DR switchover. Full site failures can occur due to power outages or disasters such as fire or flood.

The following table provides a potential resolution option for a number of failures in the primary location:

Primary location failure condition	Impacts to solution	Option 1: Address failure without switchover	Option 2: Partial** DR switchover available	Option 3: Full DR switchover available
Complete loss of IT network DNS capabilities	Avaya Oceana® and Avaya Breeze® platform outage	N/A	No	Yes

Table continues…

Complete outage of primary Avaya Aura® System Manager	Avaya Aura Management no longer available. No impact on Avaya Oceana® Operations: Routing/Login	Reinstate new Avaya Aura® System Manager using backup. Recreate Replication to DR System Manager	No	Yes
Complete outage of primary Avaya Aura® Communication ManagerDuplex Pair	Site wide telephony outage	N/A	No	Yes
Complete outage of primary Avaya Aura® Application Enablement ServicesStandalone Pair	Site wide CTI outage affecting all telephony uses	N/A	No	Yes
Complete outage of Avaya Aura® Session Manager	External and Internal Voice Routing Outage	N/A	No	Yes
Complete outage of Avaya Control Manager application or Database Servers	Aura and Oceana Management Outage	Rebuild ACM application or DB server and reinstate ACM Replication	No	Yes
Complete outage of any of the Avaya Oceana® and Avaya Breeze® platform cluster 1, cluster 2, or cluster 3.	Complete loss of Avaya Oceana® core functionality	N/A	Yes	Yes
Complete outage of Avaya Oceana® Omnichannel DB servers	Complete loss of Avaya Oceana® channel routing	N/A	Yes	Yes
Complete outage of any of the Avaya Analytics™ OSA, BI, Streams, or DB servers	Complete loss of Avaya Oceana® Reporting functionality	N/A	Yes	Yes
Complete outage of Avaya Experience Portal Applications (EP and MPP)	Loss of incoming voice routing	Failover to basic CC Elite voice prompting	No	Yes

Table continues…

Complete outage of WFO/WFM applications	Loss of voice recording and/or workforce management capabilities	N/A	No	Yes
Complete Loss of LDAP Instances	New Avaya Oceana® users cannot login if they have not yet performed a first login	Rebuild LDAP Instances	No	Yes
Complete Loss of Customer Provided Widget Web Server hosting custom widgets				

Note:

**A partial DR switchover means that customers have the option to switchover the following 3 sets of applications Avaya Oceana®, Avaya Analytics™ and Omnichannel DB server to the DR site per instructions in chapter *Switchover* of this document. All the three applications must switchover in the maintenance window.

Unplanned failures of a few primary site Oceana applications require special switchover instructions to activate the DR equivalent application. These are as follows:

- Omnichannel DB deployed as a 2+1 or a 1+1
- Avaya Analytics™ Database Server

Switchover from a single active server in Data Center 1 to the async server in Data Center 2

Promoting the async server

About this task

Use this procedure to promote async server when the primary Omnichannel database server is offline due to unplanned failures. Also, to promote the async server in Data Center 2 when the active server in Data Center 1 is not available. That can be due to loss of the server itself, loss of network connectivity to the site, or complete loss of the primary site.

Note:

Disaster Recover switchovers during unplanned outages are meant for extreme scenarios, where Data Center 1 is down and is considered unrecoverable. Switchovers here should not be done as a temporary solution on an outage as it involves risk. Manual Failover to a DR member when the original failover members are not reachable comes with the risk of both loss

of data and global updates. The mirror members on DC1 need to be rebuilt once they are available again.

On the DR Omnichannel database server, do the following:

Procedure

1. Log on to the server.
2. If you are deploying Oceana 3.5.x or 3.6.x, do the following:
   a. Navigate to the `OCEANA_INSTALL_DIR\Avaya\Oceana\Oceana\BackupAndRestore` folder.
   b. Right-click the `BackupAndRestore.exe` file, and click **Run as Administrator**.
3. If you are deploying Oceana 3.7 or higher version, do the following:
   a. Navigate to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement` folder.
   b. Double-click the `OceanaDataManagementTool.exe`.
4. In the Oceana Data Management utility, click **Backup And Restore**.
5. In the navigation pane, expand the **Backup And Restore** node, and then click **Backup And Restore**.
6. Click **Mirror Configuration**.
7. In the **Select Mirror Scenario** field, select **Switchover Primary Server Down**.
8. Click **Execute**.

Switchover from the active or standby server in Data Center 1 to the async server in Data Center 2

Promoting the async server on Data Center 2

About this task

Use this procedure to promote the async server in Data Center 2 when the active and standby servers in Data Center 1 are no longer available. This procedure promotes the async Omnichannel DB server in Data Center 2 when Data Center 1 is either offline or the servers have failed completely.

On the Omnichannel DB server in the DR site, do the following:

Note:

Disaster Recovery switchovers during unplanned outages are for extreme scenarios, where Data Center 1 is down and is considered unrecoverable. Switchovers should not be done as a temporary solution on an outage as it involves risk. Manual Failover to a disaster recovery member when the original failover members are not reachable, may result in loss of both.

Procedure

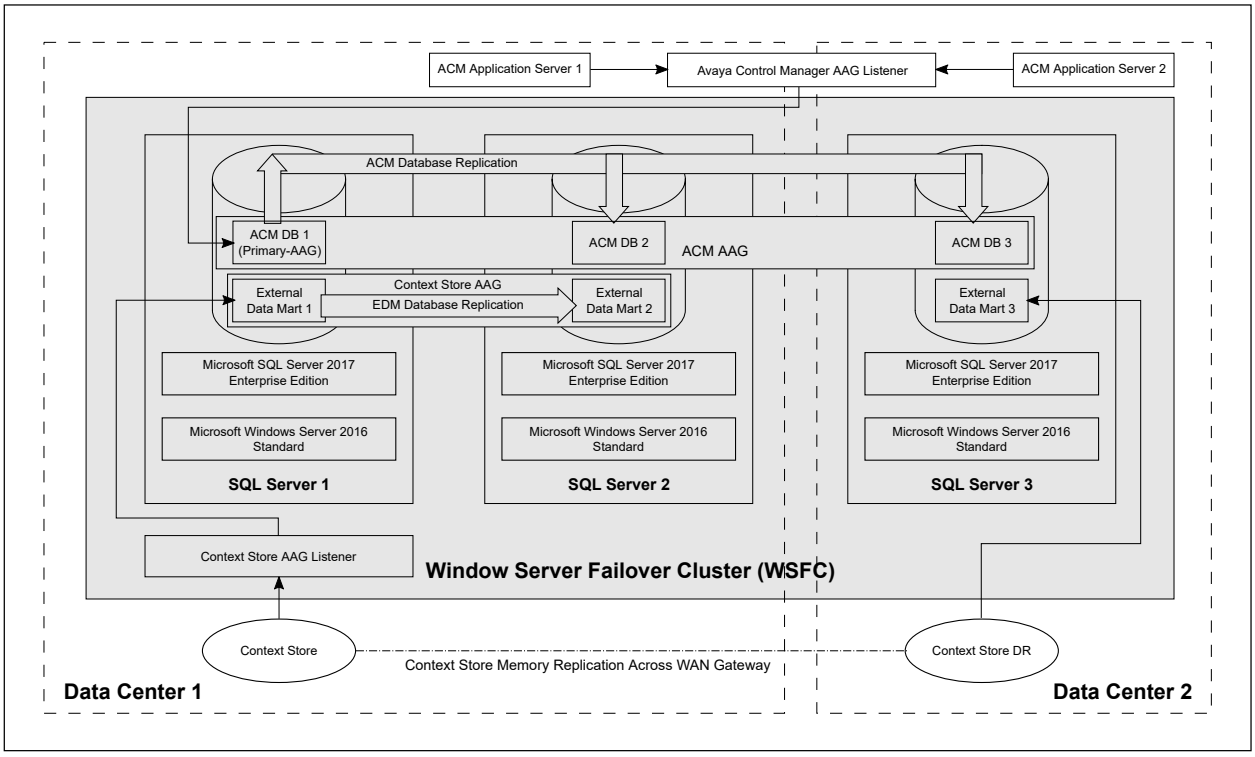
1. Log on to the server.
2. If you are deploying Oceana 3.5.x or 3.6.x, do the following:
   a. Navigate to the `OCEANA_INSTALL_DIR\Avaya\Oceana\Oceana \BackupAndRestore` folder.
   b. Right-click the `BackupAndRestore.exe` file, and click **Run as Administrator**.
3. If you are deploying Oceana 3.7 or higher version, do the following:
   a. Navigate to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement` folder.
   b. Double-click the `OceanaDataManagementTool.exe`.
4. In the Oceana Data Management utility, click **Backup And Restore**.
5. In the navigation pane, expand the **Backup And Restore** node, and then click **Backup And Restore**.
6. Click **Mirror Configuration**.
7. In the **Select Mirror Scenario** field, select **Switchover Primary Server Down**.
8. Click **Execute**.
9. Click **Cache cube** and select **Terminal**.
   a. Enter the username and password.
   b. Type: **`zn "%SYS`**
   c. Type: **`Do ^MIRROR`**
   d. Select option 2.
   e. Select option 9.
   f. Types `Yes` for the command **`Do you want to continue?`**.
   g. On seeing the **`Success`** message, exit the terminal.
10. On the **Edit Mirror** page, select **Remove other mirror member** to remove both the servers.
11. Unselect **Use Virtual IP** option.

Chapter 8: Avaya Control Manager-External Data Mart co-resident deployment in Disaster Recovery

Supported configurations for Avaya Control Manager and External Data Mart in Disaster Recovery

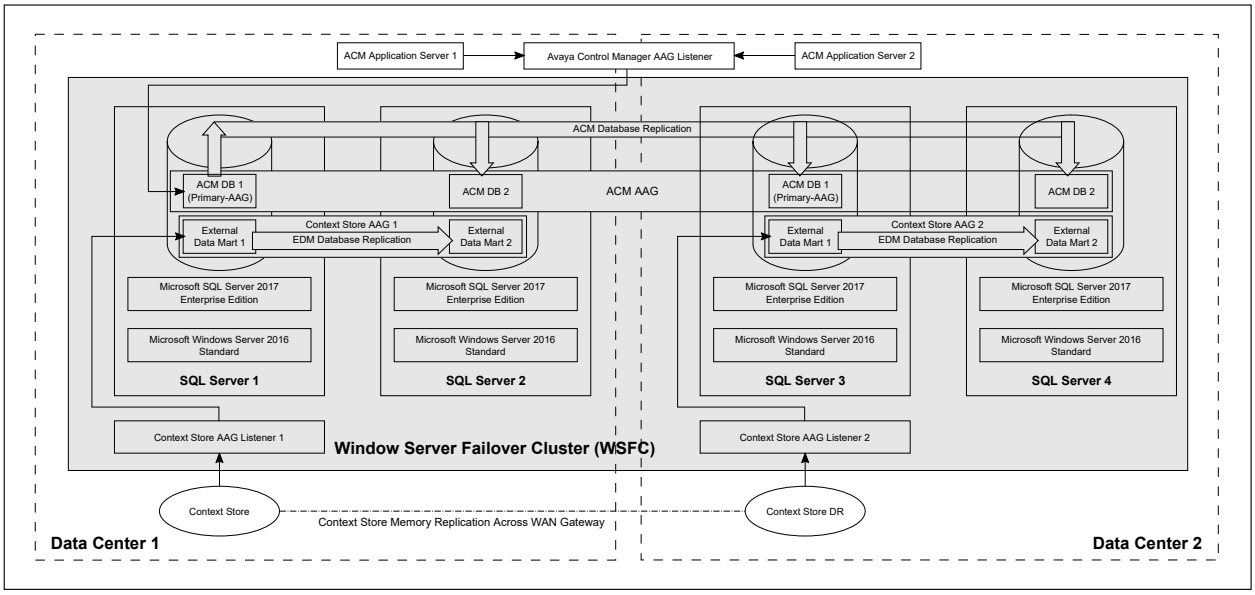
Configuration with three SQL Server replicas

The following diagram depicts the deployment architecture with three SQL Server replicas:



Configuration with four SQL Server replicas

The following diagram depicts the deployment architecture with four SQL Server replicas:



Deployment considerations

- Create a Windows Server Failover Cluster that spans the two datacenters.
- Configure an Avaya Control Manager Advanced Availability Group (AAG) that includes all SQL Server replicas.
- Create a separate Context Store EDM AAG on Data Center 1 for both SQL Server replicas.
- Create a separate Context Store EDM AAG on Data Center 2 for both SQL Server replicas, if you have four SQL replicas.
- If you have three SQL Server replicas, the SQL Server in Data Center 2 is used as Data Center 2 EDM. This EDM is accessed through the FQDN of the SQL Server, and not through an AAG Listener.
- For information about how to create the EDM AAG on SQL Server, see *Deploying Avaya Oceana®*.
- Replication of Context Store data from Data Center 1 to Data Center 2 occurs through WAN Gateway.
- No replication of EDM data occurs from Data Center 1 to Data Center 2 at the database layer.

Setting the OceanaConfiguration attribute to enable unidirectional replication of the Context Store data

About this task

Use this procedure to configure the **Disaster Recovery Mode** attribute in the OceanaConfiguration service in System Manager to enable unidirectional replication of the Context Store data across the WAN Gateway from Data Center 1 to Data Center 2. The attribute configuration prevents data replication from Data Center 2 to Data Center 1.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. In the **Cluster** field, select **ProvisioningCluster**.
   b. In the **Service** field, select **OceanaConfiguration**.
3. For **Disaster Recovery Mode**, do the following:
   a. Select **Override Default**.
   b. In the **Effective Value** field, select **Geo Primary**.
4. Click **Commit**.
5. Reboot the cluster.
6. Repeat Steps 1 to 5 and set the **Disaster Recovery Mode** to **Geo Secondary** for the secondary site.

Restoring the External Data Mart server

About this task

Use this procedure to restore the Context Store External Data Mart (EDM) server before switching back from Data Center 2 to Data Center 1.

When you switch back to Data Center 1, copy the EDM data from Data Center 2 to the EDM in the Data Center 1. Ensure that you backup and restore the database to complete EDM restoration.

Before you begin

- On Data Center 1 and Data Center 2, set the **Cluster State** of Avaya Oceana® Cluster 1 to **Deny New Service**. For instructions about how to change the cluster state, see *Deploying Avaya Oceana®*.
- Configure the **Disaster Recovery Mode** attribute in the OceanaConfiguration service in System Manager.

Procedure

1. Log in to the primary SQL Server hosting the EDM database in Data Center 2.

   You must log in with credentials of the SQL Server domain user who with administrative rights for all machines in the Avaya Control Manager database cluster.
2. Open SQL Server Management Studio.
3. In the Object Explorer pane, click **Connect** > **Database Engine**.

   SQL Server Management Studio displays the Connect to Server dialog box.
4. In the **Server name** field, select the local instance of SQL Server.

5. In the **Authentication** field, select **SQL Server Authentication**.
6. In the **Login** and **Password** fields, enter the system administrator credentials.

   The system administrator is usually the default sa user created during SQL Server installation.
7. Click **Connect**.
8. In the Object Explorer pane, click **Databases** > ***<EDM Database>***.
9. Right-click the EDM database and click **Tasks** > **Back Up**.

   SQL Server Management Studio displays the Back Up Database dialog box.
10. In the navigation pane, click **General**.
11. In the **Backup type** field, select **Full**.
12. In the **Destination** area, click **Add**.
13. In the Select Backup Destination dialog box, select the backup folder location, specify the backup file name with the `.bak` extension, and click **OK**.

    Ensure that the SQLService User login (services.msc) has full permissions on the backup folder.
14. To provide full permissions to the SQLService User login, do the following:
    a. Go to the backup folder location.
    b. Right-click the backup folder and click **Properties**.
    c. On the Security tab, select the SQLService User login and click **Edit**.
    d. In the **Permissions** area, select the **Full control** check box.
    e. Click **OK**.
15. In the navigation pane, click **Media Options**.
16. In the **Overwrite media** area, select **Overwrite all existing backup sets**.
17. In the **Reliability** area, select the **Verify backup when finished** check box.
18. In the navigation pane, click **Backup Options**.
19. In the **Description** field, type a description for the backup.
20. In the **Set backup compression** field, select **Compress backup**.
21. Click **OK**.
22. Log in to the primary SQL Server hosting the EDM database in Data Center 1.

    You must log in with credentials of the SQL Server domain user with administrative rights for all machines in the Avaya Control Manager database cluster.
23. Open SQL Server Management Studio.
24. In the Object Explorer pane, click **Connect** > **Database Engine**.

    SQL Server Management Studio displays the Connect to Server dialog box.

25. In the **Server name** field, select the local instance of SQL Server.
26. In the **Authentication** field, select **SQL Server Authentication**.
27. In the **Login** and **Password** fields, enter the credentials of the system administrator.

    The system administrator is usually the default sa user created during SQL Server installation.
28. Click **Connect**.
29. In the Object Explorer pane, click **Databases** > ***<EDM Database>***.
30. Right-click the EDM database and click **Tasks** > **Restore** > **Database**.

    SQL Server Management Studio displays the Restore Database dialog box.
31. In the navigation pane, click **General**.
32. In the **Device** field, browse and select the backup file location that you create in Data Center 2.
33. In the navigation pane, click **Options**.
34. In the **Restore options** area, select the **Overwrite the existing databases (WITH REPLACE)** check box.
35. In the **Server Connections** area, select the **Close existing connections to destination database** check box.
36. Click **OK**.
37. In the Object Explorer pane, right-click the master database and click **New Query**.
38. In the content pane, run the following command to re-enable the optional non-system administrator user on the primary SQL Server in Data Center 1:

```
USE <database_name>;
GO
sp_change_users_login @Action='update_one', @UserNamePattern='<database_user>',
   @LoginName='<login_name>';
GO
```

For example:

```
USE [master]
GO
sp_change_users_login @Action='update_one', @UserNamePattern= csEDMLogin,
   @LoginName= csEDMLogin;
```

Chapter 9: Resources

Documentation

Title	Use this document to:	Audience
Overview		
Avaya Oceana® Solution Description	Know about tested product characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements.	• Sales engineers • Business partners • Solution architects • Implementation engineers
Implementing		
Deploying Avaya Oceana®	Deploy Avaya Oceana®.	• Sales engineers • Business partners • Solution architects • Implementation engineers
Avaya Oceana® and Avaya Analytics™ Disaster Recovery	Know about how to restore Avaya Oceana® when a complete outage at the primary data center.	• Sales engineers • Business partners • Solution architects • Implementation engineers
Upgrading Avaya Oceana®	Upgrade Avaya Oceana®.	• Sales engineers • Business partners • Solution architects • Implementation engineers
Deploying Avaya Analytics™	Deploy Avaya Analytics™.	• Sales engineers • Business partners • Solution architects • Implementation engineers
Administering		

Table continues…

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

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.

7. Click **Enter**.

Avaya Documentation Center navigation

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

Important:

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

Using the Avaya Documentation Center, you can:

- Search for keywords.

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

- Search for documents.

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

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

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

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

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

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

  - Enable **Include in email notification** to receive email alerts.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

  As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.

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

Note:

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

Training

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

Table 1: Sales Credentials

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

Table 2: Pre-Sales Design

Course code	Course title	Course duration in hours	Delivery type
ACDS – 3480 Avaya Oceana® Design			
34210W	Avaya Oceana® Overview for Design	1.0	Web-based Training

Table continues…

Course code	Course title	Course duration in hours	Delivery type
34810W	Designing the Avaya Oceana® Part 1 of 3	1.0	Web-based Training
34820W	Designing the Avaya Oceana® Part 2 of 3	1.50	Web-based Training
34830W	Designing the Avaya Oceana® Part 3 of 3	1.50	Web-based Training
34800X	Avaya Oceana® Design Exam	1.50	Exam
ALRI-7001 Avaya Oceana® Product Release Information Collection			
39000W	Avaya Oceana® Release 3.8 Details for Pre-Sales	1.0	Portable Document Format (PDF)
39010W	Avaya Analytics™ Release 3.8 and 4.1 Details for Pre-Sales	1.0	PDF
39020W	Avaya Breeze® Snap-Ins for Avaya Oceana® R3.8 Details for Pre-Sales	1.0	PDF

Table 3: Technical Services Partner Credentials

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

Table 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	Creating Avaya Oceana® Workspaces Framework for Developers	2.0	Web-based Training	
24150W	Avaya Workspaces Framework R3 Test	1.0	Online Test	
ASAC-0010 Avaya Oceana® Administration				
21160W	Avaya Oceana® Fundamentals	0.5	Web-based Training	
24300V	Avaya Oceana® Administration Training	40.0	Virtual Instructor-Led Training	Attached with the sale
24300T	Administering Avaya Oceana® R3 Online Test	1.0	Online Test	

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-0022 Administering Avaya Analytic™ for Avaya Oceana®				
24380W	Administering Avaya Analytics™ for Oceana®	1.5	Web-based Training	https://www.avaya.com/Oceana-analyticsadmin
24310T	Administering Avaya Analytics™ R3 for Oceana® Basic Online Teat	1.0	Web-based Training	

Table 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	
70170W	Integrating Avaya Workspaces with Avaya Aura Call Center Elite	1.0	Web-based Training	
70170T	Avaya Workspaces for Elite Integration Online Test	1.0	Online Test	
71610W	Integrating POM with Avaya Oceana®	1.0	Web-based Training	
71610T	Proactive Outreach Manager with Avaya Oceana® Integration Online Test	1.0	Online Test	
ALEU-5005 Avaya Workspaces for Elite End User				
24120W	Using Avaya Workspaces for Elite – Agents	0.75	Web-based Training	https://www.avaya.com/elite-workspaces-agent

Table continues…

Course code	Course title	Course duration in hours	Delivery type	Vanity Link for Attachment
24140W	Using Avaya Workspaces for Elite – Supervisor	0.50	Web-based Training	https://www.avaya.com/elite-workspaces-supervisor

Support

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

Index

I

K

L

M

N

O

P

R

S

T

U

V

W