Avaya Oceana® and Avaya Analytics™ Disaster Recovery

Release 3.10.0.1
Issue 1
February 2025

Notices

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

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

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

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

License types

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, or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

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

Third Party Components

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

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.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 to comply with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

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

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

Contents

Chapter 1: Introduction

Purpose

This document provides information on configuring the Disaster Recovery (DR) functionality of Avaya Oceana®, Avaya Analytics™ for Avaya Oceana®, and recovering after a partial or complete data center outage.

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

Important:

- This document is based on the assumption that you have deployed Avaya Oceana®, Avaya Analytics™ for Avaya Oceana®, and the required components and services on Data Centers 1 and 2.

  You have to deploy Avaya Oceana® Data Center 1 and Avaya Oceana® Data Center 2 on the same System Manager.
- This document refers to the primary data center as Data Center (DC) 1 and the secondary data center as Data Center (DC) 2.

Chapter 2: System Architecture

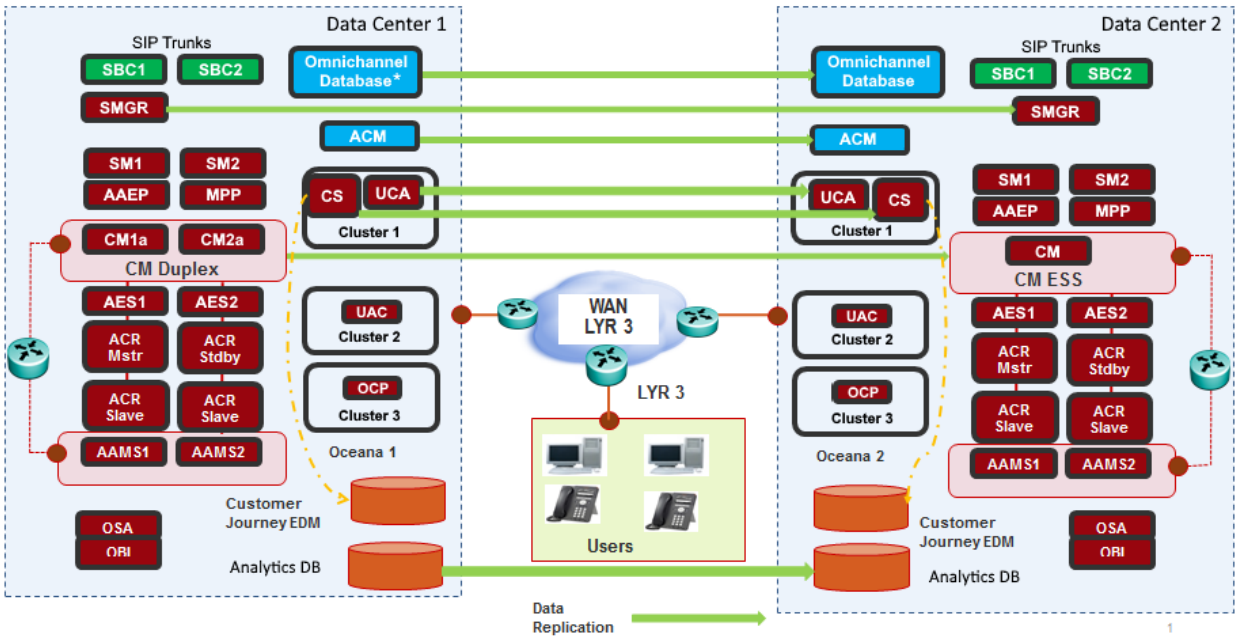
Overview

Disaster Recovery provides a planned approach to setting up redundancy capabilities at Data Center 2 (DC2) when a complete outage occurs at Data Center 1 (DC1). The deployment process for DC1 and DC2 is identical. The two data centers are linked for replication. Post replication, one is the primary site designated as DC1, and the other is the secondary or disaster recovery site set as DC2.

This document provides information about configuring geographically redundant Avaya Oceana® and Avaya Analytics™ so when an outage occurs at DC1, DC2 can be operational. DC2 has replicated the data required for administration and reporting, facilitating regular operations.

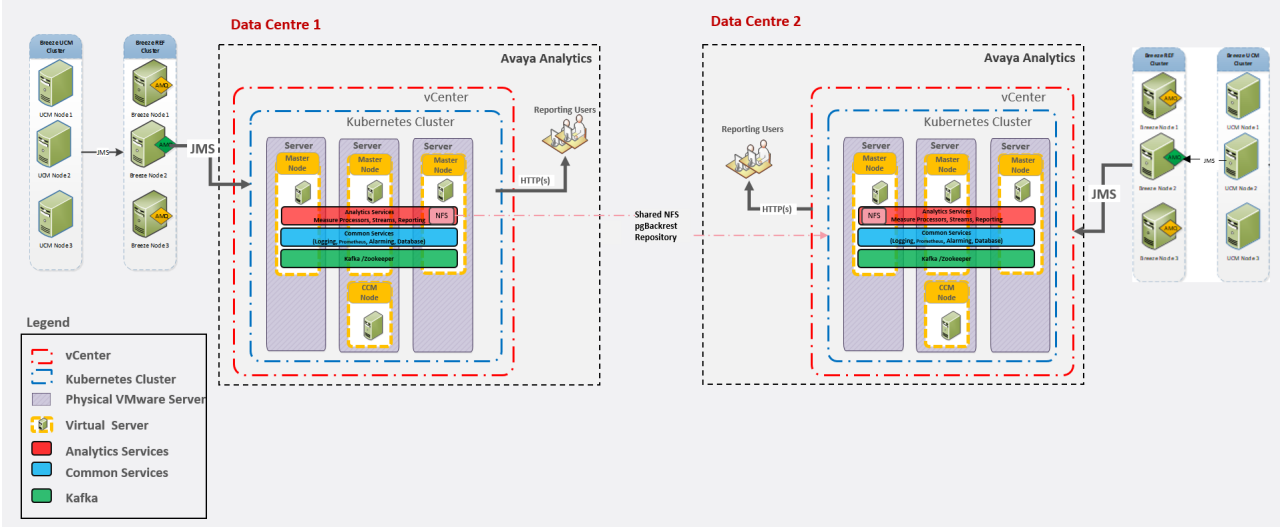
System architecture

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.

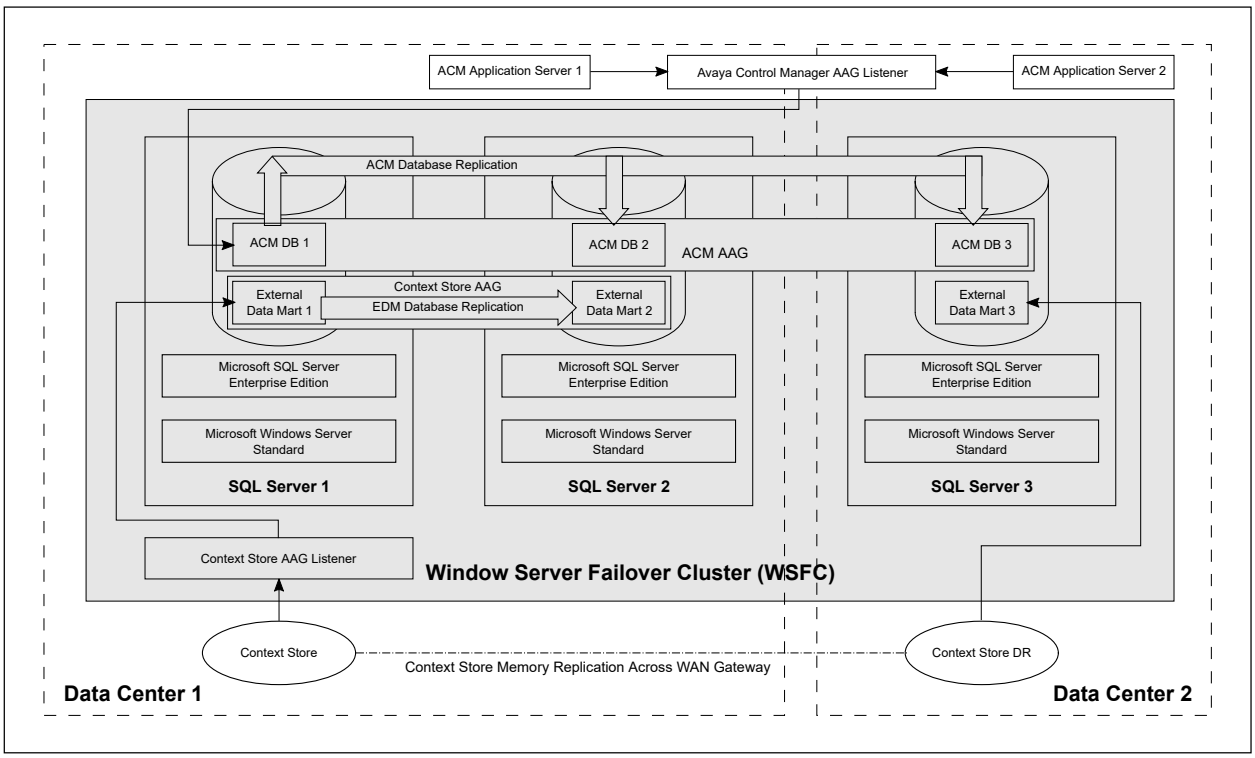
The following diagram depicts the high-level architecture of Avaya Analytics™ disaster recovery:



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

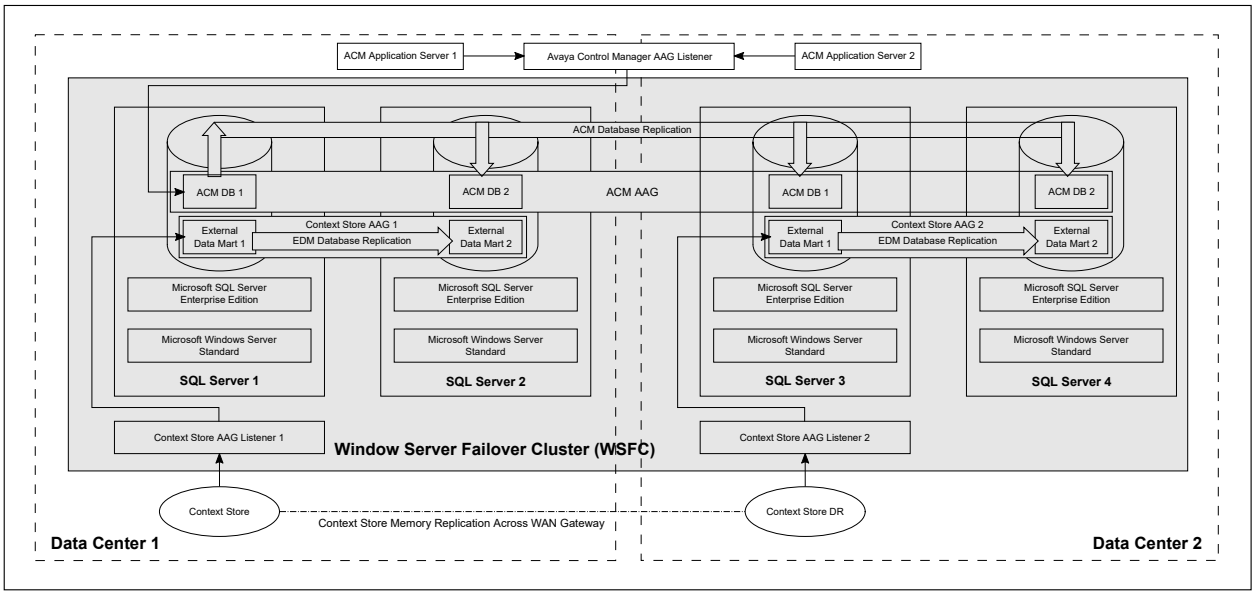
Configuration with three SQL Server replicas

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.

Chapter 3: Failover scenarios

Failover scenarios

Scenarios	Description
Unplanned total outage of DC1	Failure of Avaya Oceana® 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 DC1	The controlled manual shutdown of DC1 and switchover to DC2. Avaya Oceana® supports a maintenance mode. Avaya Oceana® does not add any new contacts to the queue in the maintenance mode so that agents can handle the existing queued contacts before the shutdown.
Unplanned total outage of Avaya Oceana® or Avaya Analytics™ components only at DC1. Avaya Aura®, Communication Manager, and other applications remain operational.	Partial disaster recovery failure of Avaya Oceana® components at DC1 only. You can switch the Contact Center functionality to DC2 if the Avaya Aura® infrastructure functionality and all other applications remain operational in DC1. The Communication Manager and Application Enablement Services components continue to be operational in DC1. You must re-configure Avaya Oceana® components at DC2 and ensure that Avaya Oceana® components point to Application Enablement Services at DC2. You must also re-configure Application Enablement Services at DC2 to communicate with the Communication Manager at DC1. **Important:** • Retain the same administration settings while DC2 is functioning. If you make any changes, Avaya Oceana® handles the changes similar to an ESS switchover. • This failure mode does not support Avaya WebRTC Connect voice and video calls.

Table continues…

Scenarios	Description
Unplanned total outage of Communication Manager at DC1	Failure of the Communication Manager at DC1. If failure of the Communication Manager results in a switchover to the ESS at DC2, you must manually switchover Avaya Oceana® components to DC2. 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 delay.
Unplanned partial outage of Avaya Oceana® components at DC1	The failure of one or more Avaya Oceana® components at DC1. When you identify the failure of an Avaya Oceana® component, you must recover the component at DC1 or perform one of the following actions: • Partial disaster recovery to DC2. • Full switchover to DC2. When a partial failure occurs, you must determine whether the downtime to recover the components or the disruption caused by a partial or full switchover is preferable.
Split WAN	WAN outage. Avaya Oceana® does not support an active-active mode of operation; therefore, if a split WAN occurs, DC1 operates in isolation from DC2. 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 DC1 to DC2. The synchronization depends on the WAN outage time. Avaya Oceana® components can buffer only a limited number of changes that DC2 synchronizes after recovery. After reaching the buffer limit, Avaya Oceana® components start to overwrite the oldest changed records. When an extended WAN outage occurs, you must manually synchronize data from DC1 to DC2.

Limitations

The Disaster Recovery (DR) limitations are as follows:

- **Automatic switchover**: If a disaster occurs in DC1, you must manually move all operations to DC2. Disaster recovery does not support automatic switchover from DC1 to DC2.
- **Call preservation**: For planned and unplanned switchovers, not all active voice contacts move with Avaya Oceana® during the switchover. All existing voice contacts are anchored in the Avaya Aura® Communication Manager. The calls use the same fallback mechanism to the 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**: Requires a 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 DC1 must connect to the Communication Manager only.

  Note:

  Application Enablement Services (AES) servers in DC2 can temporarily connect to the main site Avaya Aura® Communication Manager in a partial disaster recovery failover.
- **WAN outage scenario**: Active-Active mode is not available.
- **Avaya Aura® Communication Manager**: The Communication Manager configuration changes while the DC2 is active.

Avaya Oceana® disaster recovery supports a single disaster recovery site, a single ESS. Disaster recovery requires downtime while activating the DC2. It also mandates that the WAN delay is less than 50 milliseconds for Avaya Control Manager. In addition, the downtime may result in the loss of historical reporting data.

Chapter 4: Disaster Recovery Configuration

Overview

Assuming that you have deployed Avaya Oceana®, Avaya Analytics™ for Avaya Oceana®, and the required components and services on DC1 and DC2, this chapter provides the procedures to configure DC1 and DC2 for DR.

Important:

For detailed deployment instructions of Avaya Oceana®, Avaya Analytics™ for Avaya Oceana®, and Avaya Aura® components for the Data Centers 1 and 2, refer to the following documentation:

Component	Deployment documentation
Avaya Oceana®	Deploying Avaya Oceana®
Avaya Analytics™ for Avaya Oceana®	Deploying Avaya Analytics™ for Avaya Oceana®
Avaya Aura® System Manager	Deploying Avaya Aura® System Manager in Virtualized Environment
Avaya Control Manager	Planning for an Avaya Control Manager Deployment
Avaya Aura® Communication Manager	Deploying Avaya Aura® Communication Manager in Virtualized Environment Deploying Avaya Aura® Communication Manager in Software-Only and Infrastructure as a Service Environments
Application Enablement Services	Deploying Avaya Aura® Application Enablement Services in Virtualized Environment Deploying Avaya Aura® AE Services on Infrastructure as a Service Environment Deploying Avaya Aura® Application Enablement Services in a Software-Only Environment

Note:

The Compatibility Matrix provides compatibility information for the Avaya products that are supported with the various releases of Avaya Oceana®.

Configuring Avaya Aura® System Manager for Disaster Recovery

Configuration Checklist

No.	Task	Description	✔
Geographic Redundancy configuration			
1.	Prerequisites for the Geographic Redundancy setup	Prerequisites for the Geographic Redundancy setup on page 18	
2.	Prerequisites for System Manager on VMware in the Geographic Redundancy setup	Prerequisites for System Manager on VMware in the Geographic Redundancy setup on page 19	
3.	Key tasks for Geographic Redundancy	Key tasks for Geographic Redundancy on page 20	
Prerequisites before configuring Geographic Redundancy			
4.	Geographic Redundancy prerequisites overview	Geographic Redundancy prerequisites overview on page 22	
5.	Copy the CRL URL	Copying the CRL URL on page 23	
6.	Configure CRL download on the secondary System Manager server	Configuring CRL download on the secondary System Manager server on page 24	
7.	Add the trusted certificate of primary server to the secondary System Manager server	Adding the trusted certificate of primary server to the secondary System Manager server on page 25	
Configuration			
8.	Configure Geographic Redundancy	Configuring Geographic Redundancy on page 25	
9.	Enable the Geographic Redundancy replication	Enabling the Geographic Redundancy replication on page 27	
10.	Scenarios of auto-disable for the Geographic Redundancy system	Scenarios of auto-disable for the Geographic Redundancy system on page 28	
11.	Geographic Redundancy field descriptions	Geographic Redundancy field descriptions on page 28	
12.	Geographic Redundancy Health field descriptions	GR Health field descriptions on page 30	

Prerequisites for the Geographic Redundancy setup

In a Geographic Redundancy setup, the two standalone System Manager servers that you designate as primary and secondary servers must meet the following requirements:

- Contain the same version of the software that includes software packs.

- Contain the same profile for primary and secondary System Manager Geographic Redundancy virtual machines. For example, if the primary System Manager contains Profile 2, the secondary System Manager must also contain Profile 2.
- Contain the same version of the System Manager software that includes service pack and software patches.
- Contain the same parent domain names for two System Manager systems. For example, smgr.abc.com and smgr.xyz.com are invalid domain names because the parent domain names abc and xyz are different.
- Communicate with each other over the network by using the IP address and FQDN.
- In the Geographic Redundancy setup, the primary and secondary System Manager must use the same VFQDN.
- Have a synchronized network time.
- Use DNS to ensure that the name resolution is automatic. Otherwise, you must resolve the IP address and the host name in the `/etc/hosts` file on the primary and secondary System Manager servers.
- Have open required ports to support the Geographic Redundancy feature. For port usage information, see *Avaya Port Matrix: Avaya Aura® System Manager* on the Avaya Support website at http://support.avaya.com/.
- Have T1 as the minimum data pipe between the primary and the secondary System Manager server. T1 provides 1.544 Mbps.
- Have network latency that is less than 500 ms.
- In the Geographic Redundancy setup, if you need to configure the outbound firewall rules, then you need to add the peer IP addresses on the primary and secondary System Manager servers.

Prerequisites for System Manager on VMware in the Geographic Redundancy setup

In a Geographic Redundancy-enabled system running on VMware, ensure that System Manager that you designate as primary and secondary systems meet the following requirements:

- Contain the same profile for primary and secondary System Manager Geographic Redundancy virtual machines. For example, if the primary System Manager contains Profile 2, the secondary System Manager must also contain Profile 2.
- Contain the same version of the System Manager software that includes service pack and software patches.
- Contain the same parent domain names for two System Manager systems. For example, smgr.abc.com and smgr.xyz.com are invalid domain names because the parent domain names abc and xyz are different.
- Communicate with each other over the network by using the IP address and FQDN.

- Have a synchronized network time.
- Use DNS to ensure that the name resolution is automatic. Otherwise, you must resolve the IP address and the host name in the `/etc/hosts` file on the primary and secondary System Manager servers.
- Have open required ports to support the Geographic Redundancy feature. For port usage information, see *Avaya Port Matrix: Avaya Aura® System Manager* on the Avaya Support website at http://support.avaya.com/.
- Have network latency that is less than 500 ms.
- Have T1 as the minimum data pipe between the primary and the secondary System Manager server. T1 provides 1.544 Mbps.

Key tasks for Geographic Redundancy

Prerequisites

Ensure that the two System Manager servers meet the requirements that are defined in Prerequisites for the Geographic Redundancy setup on page 18.

Key tasks

Only the system administrator can perform Geographic Redundancy-related operations.

- Configure Geographic Redundancy.

  Configure Geographic Redundancy to handle the situation when the primary System Manager server fails or when the managed element loses connectivity to the primary System Manager server.

  Important:

  During the configuration of Geographic Redundancy, the primary System Manager replicates the data between the primary and the secondary System Manager servers. Therefore, ensure that the system maintenance activities such as backup, restore, and shutdown are not in progress.

- Enable the Geographic Redundancy replication between the two servers.

  Enable the replication in the following scenarios:

  - After you configure the two standalone System Manager servers for Geographic Redundancy, you must enable the Geographic Redundancy replication between the two servers to ensure that the secondary System Manager server contains the latest copy of the data from the primary System Manager server.
  - During system maintenance or upgrades, Geographic Redundancy replication must be disabled. After the maintenance activity is complete, you must enable Geographic Redundancy replication if it was manually or automatically disabled due to the maintenance activity.

    Note:

    If the heartbeat between the two System Manager servers on which the Geographic Redundancy replication is enabled stops due to network connectivity failure or server

failure, the system automatically disables the Geographic Redundancy replication within a preconfigured time. The default is 5 minutes. If the primary and secondary System Manager servers are running and if the network connectivity between the two servers fails, the system triggers auto-disable on both servers. If one of the two servers becomes nonoperational, the system triggers auto-disable on the server that is operational.

Enable Geographic Redundancy replication after network connectivity has been restored. For information about the network latency and bandwidth, see Prerequisites for the Geographic Redundancy setup on page 18.

For information about the auto-disable scenarios, see Scenarios of auto-disable for the Geographic Redundancy system on page 28.

- After the primary System Manager server recovers from failure.

Important:

During bulk activities such as import, export, and full synchronization of Communication Manager, the system might disable the Geographic Redundancy replication for reasons, such as the size of the data involved in the bulk activity and the bandwidth between the primary and secondary System Manager servers. After you complete the bulk activity, enable the Geographic Redundancy replication if the replication is disabled.

- Disable the Geographic Redundancy replication between the two servers.

  Disable the Geographic Redundancy replication before you start the maintenance activities, such as upgrades, the installation of software patches, or hot fixes. If the primary and secondary System Manager servers disconnect from each other for longer than the threshold period, the system automatically disables the Geographic Redundancy replication. The default threshold period is 5 minutes.

- Activate the secondary System Manager server.

  Activate the secondary System Manager server in the following scenarios:

  - The primary System Manager becomes nonoperational.
  - The enterprise network splits.

- Deactivate the secondary System Manager server.

  Deactivate the secondary System Manager server in the following situations:

  - The primary System Manager server becomes available.
  - The element network restores from the split.

- Restore the primary System Manager server.

  After you activate the secondary System Manager server, to return to active-standby mode, you must restore the primary System Manager server. You can choose to restore from the primary System Manager server or the secondary System Manager server.

  Note:

  The system does not merge the data from the primary and secondary server.

- Reconfigure Geographic Redundancy.

You can reconfigure Geographic Redundancy when the secondary System Manager is in standby mode or active mode. The reconfiguration process copies the data from the primary System Manager server to the secondary System Manager server.

- Convert the primary System Manager server to the standalone server.

  Perform this procedure to convert the primary System Manager server in the Geographic Redundancy-enabled system to a standalone server or if you have to configure a new secondary server.

For detailed instructions to complete each task, see the appropriate section in this document.

Prerequisites before configuring Geographic Redundancy

Geographic Redundancy prerequisites overview

Before enabling and configuring Geographic Redundancy, do the following:

1. Configure CRL download on the secondary System Manager server.

   Note:

   By default, CRL is valid only for 7 days. Therefore, you must configure Geographic Redundancy before the expiry date of CRL.

2. Add the trusted certificate of primary server to the secondary System Manager server.
3. If certificate is replaced on Primary Server by third-party signed certificate then same certificate type must be replaced on Secondary Server by same third-party CA.

   For example, if the *Management Container TLS Service* is replaced by a third-party CA signed certificate on the primary server, the same type of certificate must be replaced on the secondary server by the same third-party CA.

4. Install a third-party certificate on both servers prior to Geographic Redundancy configuration and post Geographic Redundancy configuration.

   For more information, see “Managing certificates”.

5. Ensure that third-party CA certificate is added into trust store of both System Manager.
6. Replaced certificate must have full chain (id certificate ->inter CA (if present) certificate -> root CA certificate) and also must contain correct FQDN/VFQDN in required places.
7. Configure CRL download is mandatory for Geographic Redundancy.
8. If the CRL URL for a third-party is not accessible from System Manager, then set **Certificate Revocation Validation** from **BEST_EFFORT** to **NONE** on the **Security** > **Configuration** > **Security Configuration** > **Revocation Configuration** page.

   When you click **Commit**, System Manager displays the following message:

   ```
   Changes are updated successfully. An Application server restart is
   required for changes to take effect. Click Ok to restart it now.
   Click Cancel to restart it later. Web Console would be unavailable
   for 10-15 minutes during a restart.
   ```

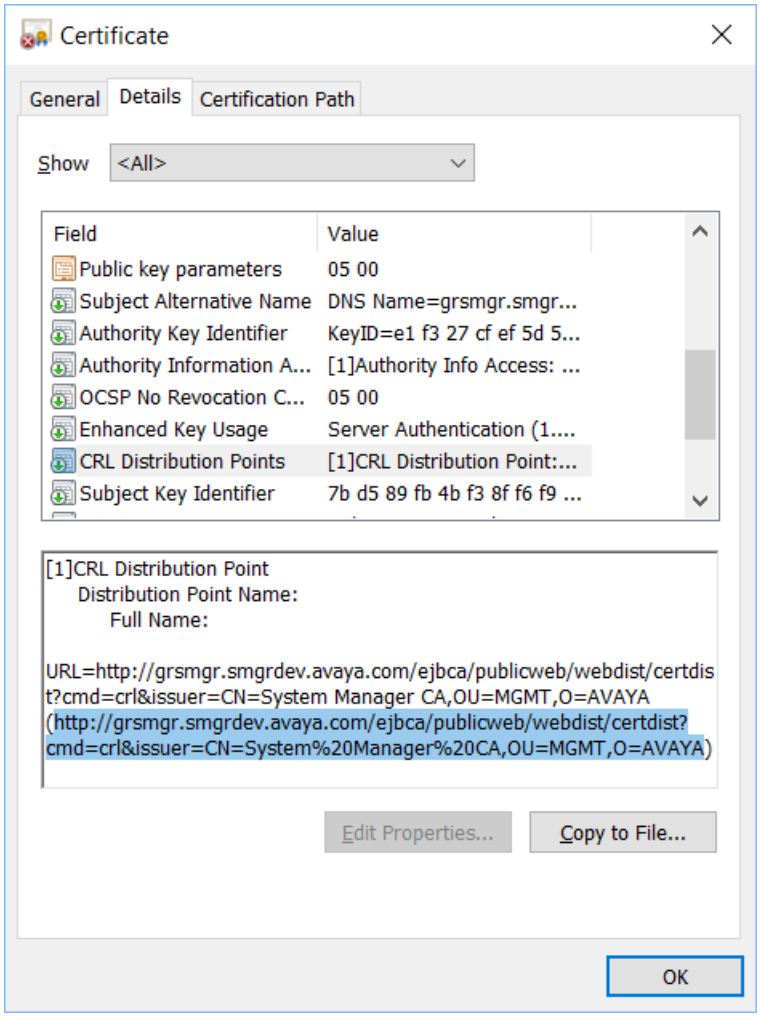
Copying the CRL URL

Procedure

1. On the web browser, type `https://<Fully Qualified Domain Name>/SMGR`, the System Manager URL.
2. On the address bar, click the Lock icon.
3. Click **View certificates**.
4. On the Certificate dialog box, do the following:
   a. Click on the **Details** tab.
   b. Scroll down and click the **CRL Distribution Points** field.

      The system displays the CRL URL in the text box.

      For example: http://<vFQDN>/ejbca/publicweb/webdist/certdist?cmd=crl&issuer=CN=System%20Manager%20CA,OU=MGMT,O=AVAYA



c. Press **Ctrl+C** and copy the URL in Notepad for configuring CRL download in the Geographic Redundancy set up.

d. Click **OK**.

Configuring CRL download on the secondary System Manager server

Procedure

1. Access the login page of the primary System Manager server.
2. Copy the CRL of the browser certificate.

   For information about copying the CRL URL, see “Copying the CRL URL.”
3. Replace the vFQDN in the CRL with the IP address of the primary System Manager server.

   For example, the CRL in the certificate is:

   ```
   http://<vFQDN>/ejbca/publicweb/webdist/certdist?
   cmd=crl&issuer=CN=System%20Manager%20CA,OU=MGMT,O=AVAYA
   ```

   The new CRL for the certificate will be:

   ```
   http://<ip-address>/ejbca/publicweb/webdist/certdist?
   cmd=crl&issuer=CN=System%20Manager%20CA,OU=MGMT,O=AVAYA
   ```

   Where, <*vFQDN*> and <*ip-address*> are the respective vFQDN and IP address.

   Note:

   If you installed a third-party certificate on System Manager servers, this step is not required. If third-party certificate, then configure CRL URL of the third-party certificate for CRL download.
4. Log on to the secondary System Manager web console.
5. On the System Manager web console, click **Services** > **Security**.
6. In the navigation pane, click **Configuration** > **CRL Download**.
7. On the CRL Download Configuration page, click **Add**.

   System Manager displays the Schedule CRL Download page.
8. In **Job Name**, type the job name.
9. In **Job Frequency**, set the frequency and recurrence to schedule the job within a few minutes after the CRL addition.
10. Copy the new CRL URL from Notepad and paste the URL in the **Configure CRL Distribution Point** field.

    For information about copying the CRL URL, see Copying the CRL URL on page 23.

    CRL URL example:

    ```
    http://<ip-address>/ejbca/publicweb/webdist/certdist?
    cmd=crl&issuer=CN=System%20Manager%20CA,OU=MGMT,O=AVAYA
    ```
11. Click **Add**, and then click **Commit**.

Ensure that the job is completed successfully.

Next steps

Add the trusted certificate of the primary server to the secondary System Manager server.

Adding the trusted certificate of primary server to the secondary System Manager server

Procedure

1. Log in to the primary System Manager web console.
2. On the System Manager web console, click **Services** > **Security**.
3. In the navigation pane, click **Certificates** > **Authority**.
4. Click **CA Functions** > **CA Structure & CRLs**.
5. Click **Download PEM file**.
6. Log in to the secondary System Manager web console.
7. On the System Manager web console, click **Services** > **Inventory**.
8. In the navigation pane, click **Manage Elements**.
9. On the Manage Elements page, select the System Manager certificate and click **More Actions** > **Manage Trusted Certificates**.
10. On the Manage Trusted Certificates page, click **Add**.
11. Click **Choose File** and select the previously downloaded PEM file.
12. Click **Retrieve Certificate**, and then click **Commit**.

Configuring Geographic Redundancy

Before you begin

- For the new installation of System Manager, ensure that you change the default password for the system administrator user.
- Ensure that you change CLI passwords on primary and secondary System Manager servers.

  60 days after the System Manager CLI password expires, Geographic Redundancy becomes nonoperational. You must set a new password on primary and secondary System Manager servers for Geographic Redundancy to become operational again.
- Ensure that the two System Manager servers meet the requirements that are defined in Prerequisites for the Geographic Redundancy setup on page 18.

About this task

For resiliency, from the pair of standalone System Manager servers, you can configure Geographic Redundancy.

Important:

- During the configuration of Geographic Redundancy, the primary System Manager replicates the data between the primary and secondary System Manager servers. Therefore, ensure that the system maintenance activities such as backup, restore, and shutdown are not in progress.
- After the Geographic Redundancy configuration is complete, the credentials used for logging in to the secondary System Manager become identical to the login credentials of the primary System Manager.

Procedure

1. Log on to the System Manager web console of the standalone server that you require to designate as the secondary server and perform the following:
   a. On the System Manager web console, click **Services** > **Geographic Redundancy**.
   b. Click **Configure**.
   c. In the dialog box, provide the details of the primary System Manager server in the following fields:
      - **Primary Server Username**

        Enter the system administrator user name that you use to log on to the primary System Manager server.
      - **Primary Server Password**

        Enter the system administrator password that you use to log on to the primary System Manager server.
      - **Primary Server IP**
      - **Primary Server FQDN**
   d. Click **OK**.

      The configuration process takes about 30 minutes. However, the duration might vary depending on the size of the data on the primary System Manager server.

      Note:

      Because the server becomes unavailable, you cannot gain access to the web console. Wait until the process is complete before you continue with the next step.

      The server that you configured becomes the secondary server, and the other standalone server becomes the primary System Manager server.
2. To view the status of the Geographic Redundancy configuration during the restart of the two application servers, perform one of the following:
   - Log on to the web console of the primary System Manager server and perform the following:
     a. On the System Manager web console, click **Services** > **Geographic Redundancy**.

b. Refresh the GR Health page.

If **Enable** is available, the configuration is complete.

Note:

Log off and log on to the primary System Manager server to view the updated status of Geographic Redundancy health.

- Log in to the secondary System Manager server as system administrator by using the command line interface and perform the following:

a. Type `tail -f /home/ucmdeploy/quantum/autoReconfig.log`.

The system displays the progress during the restart of the two application servers. When the second application server restart completes, the system displays the following messages:

```
SMGR  ::  operationStatus=success

SMGR  ::  Quantum has been successfully
configured as a secondary.
```

Next steps

On the web console of the primary System Manager server, enable the Geographic Redundancy replication.

Enabling the Geographic Redundancy replication

Enable the Geographic Redundancy replication between the two servers to ensure that the data gets continuously replicated between the primary and secondary System Manager servers.

Before you begin

- Log on to the System Manager web console of the primary server.
- Ensure that CLI passwords on primary and secondary System Manager servers do not expire.

  60 days after the System Manager CLI password expires, Geographic Redundancy becomes nonoperational. You must set a new password on primary and secondary System Manager servers for Geographic Redundancy to become operational again.

About this task

Important:

During the configuration of Geographic Redundancy, the primary System Manager replicates the data between the primary and the secondary System Manager servers. Therefore, ensure that the system maintenance activities such as backup, restore, and shutdown are not in progress.

Procedure

1. On the System Manager web console, click **Services** > **Geographic Redundancy**.
2. Click **Enable Replication**.

The system displays the progress information in the **Enable GR Status** section.

Note:

Because the server becomes unavailable, you cannot gain access to the web console. Wait until the process is complete before you continue with the next step.

If the enabling process is successful, the system displays the Geographic Redundancy replication status as `Enabled`. If the process fails, the system displays an error message with the replication status as `Failed` on the primary System Manager web console. The primary server remains in the failed state while the secondary server rolls back to the previous state. Verify if the system has raised an alarm for a temporary network connectivity failure. Retry when network connectivity is restored. If the problem persists, contact Avaya service personnel.

Scenarios of auto-disable for the Geographic Redundancy system

System Manager triggers auto-disable and disables the Geographic Redundancy replication within a preconfigured time. The default is 5 minutes.

- If the primary and secondary System Manager servers are running and if the network connectivity between the two servers fails, the system triggers auto-disable on both servers.

  When the network connectivity is restored, enable the Geographic Redundancy replication.

  For information about the network latency and bandwidth, see Prerequisites for the Geographic Redundancy setup on page 18.
- If one of the two servers becomes non-operational, the system triggers auto-disable on the server that is operational.
- If the PostgreSQL database disk partition utilization reaches the threshold limit of 75%, System Manager generates a Warning alarm.

  If the PostgreSQL database disk partition utilization reaches the threshold limit of 85%, System Manager triggers auto-disable and generates a Critical alarm.

  Note:

  If auto-disable is due to a PostgreSQL database disk space issue, contact Avaya Support. Do not enable the Geographic Redundancy until the database disk partition space issue is resolved.

Geographic Redundancy field descriptions

The Geographic Redundancy and the GR Health pages remain blank on a standalone server or until you configure a secondary System Manager.

Primary Server Details

The system displays the IP address and the FQDN of the primary System Manager server.

Name	Description
Convert to Standalone	Converts to a standalone server. The system displays the **Convert to Standalone** button only when the replication is disabled.
Configure	Configures Geographic Redundancy. The system displays the **Configure** button only on the standalone System Manager server.
Reconfigure	Configures Geographic Redundancy. The system displays the **Reconfigure** button only on the secondary System Manager server.

Secondary Server Configured

You can use the **Enable Replication**, **Disable Replication**, and **Restore Data** buttons only from the primary System Manager server.

Button	Description
Enable Replication	Continuously replicates the data between the primary and the secondary System Manager server. The system displays the **Enable Replication** button after the following events: • State of Geographic Redundancy is Disable. • Geographic Redundancy configuration. • Restoration of the primary Geographic Redundancy server is complete.
Disable Replication	Stops replicating the data between the primary and the secondary System Manager server. The system displays the **Disable Replication** button when the state of Geographic Redundancy is Enable.
Restore Data	Recovers the server after the failback. The system displays the **Restore Data** button when the secondary System Manager server is deactivated.

Name	Description
IP	Displays the IP address of the secondary System Manager server.
FQDN	Displays FQDN of the secondary System Manager server.
Replication Status	Displays the status of replication. The values are Disabled and Enabled.
Last Action	Displays the last action that you performed on the secondary System Manager server.
Last Action Status	Displays the status of the last action that you performed on the secondary System Manager server.

GR Health field descriptions

The information available on the GR Health page is read-only.

The Geographic Redundancy and the GR Health pages remain blank on a standalone server or until you configure a secondary System Manager.

GR Health

Name	Description
GR Health Status	Displays the health status of the monitored services. The page displays: • ■, if the monitored service stops. • ✔, if the monitored service is running. • ✘, if the monitored service fails to run.
Activate Secondary Server	Click to make the secondary server provide full System Manager functionality when the primary System Manager server fails or the data network splits. **Note:** • The system displays **Activate Secondary Server** only on the secondary System Manager server. • The system displays the **Activate Secondary Server** or the **Deactivate Secondary Server** button on the page.
Deactivate Secondary Server	Click to make the primary System Manager resume operation. You use this option when the primary System Manager server restores operation or recovers from a network failure. **Note:** The system displays **Deactivate Secondary Server** only on the secondary System Manager server.
Service Name	Displays the name of the service for which the system provides the status of the health.
View Detail	Click **View Graph**. • For database and directory replication, the system displays the graph for default interval. If no graph is present for the default interval, using the calendar, you can set the period for which you require to check the health status and click **Generate** to view health details in a graph. For database replication, the system displays graphs for time lag and the size lag. For directory replication, the system displays a graph for time lag only. • For file replication, the system displays the last replication time and the size of the lag.

HeartBeat status

Click **View Heartbeat Status** to view the details. The system displays the GR Heartbeat page.

Name	Description
Service Name	The name of the monitored service. The services are: • **System Health**: The heartbeat status indicates if the primary or secondary System Manager server can communicate with the peer System Manager server over the network. • **Database Replication**: The heartbeat status indicates if the data stored in the System Manager database is getting replicated between the primary and secondary System Manager servers. • **Application System Health**: The heartbeat status indicates if the application server of the primary or secondary System Manager can query the application server of the peer System Manager. • **File Replication**: The heartbeat status indicates if the configuration files are getting replicated between the primary and secondary System Manager servers. • **Directory Replication**: The heartbeat status indicates if the data stored on the internal LDAP server is getting replicated on the respective System Manager server.
Last Successful Heartbeat Time	The last time the heartbeat was successful for the monitored service.
Last Missed Heartbeat Time	The last time when the monitored service missed the heartbeat.
View Details	The **View Graph** link to view the health status of the monitored service over a period of time. To configure the time period, click **Edit Dates**. The graph displays the status in 0 and 1. • 0 indicates that the monitored service is either stopped or failed at that point of time • 1 indicates that the monitored service is running at that point of time.

Configuring Aura Voice Services for Disaster Recovery

Overview

This section describes the procedures to configure Avaya Aura® and Avaya Oceana® components to enable voice functionality in an Avaya Oceana® Disaster Recovery (DR) solution.

The following diagram depicts the main components for voice functionality:

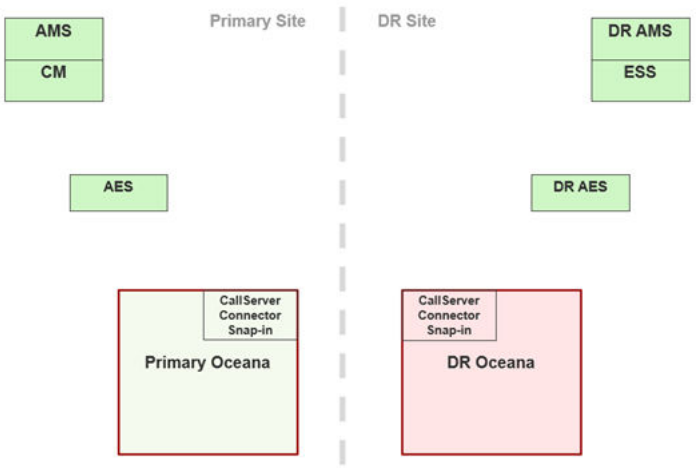


Figure 1: Components for Avaya Oceana® DR voice functionality

Configuration Checklist

No.	Task	Description	✔
Enterprise Survivable Server (ESS) configuration on Communication Manager			
1.	Add a node name for ESS server on Communication Manager	Adding a node name for Enterprise Survivable Server on Communication Manager on page 34	
2.	Add a Survivable Processor on Communication Manager	Adding a Survivable Processor on Communication Manager on page 34	
Communication Manager/ESS configuration for Server Roles and Network Configuration on System Manager Interface (SMI) portal. **Note:** The DC1 Communication Manager is configured for Server Roles, Network Configuration, and Duplication Parameters. Configure the DC2, DR site as follows:			
3.	Configure Communication Manager/ESS server role	Configuring the server role for the Enterprise Survivable Server in DC2 on page 35	
	Configure Communication Manager/ESS Network Configuration	Configuring ESS network on page 36	
	Verify status of Survivable Processor	Verifying the status of Survivable Processor on page 36	
Other Communication Manager Configuration			
4.	Add Computer Telephony Integration (CTI) link to DC2 Application Enablement Services	Adding a CTI link to the DC2 Application Enablement Services on page 37	

Table continues…

No.	Task	Description	✔
5.	Configure IP-services	Configuring IP services on page 38	
6.	View the ESS cluster status	Viewing Enterprise Survivable Server cluster status on page 38	
Application Enablement Services Configuration - The DC1 Application Enablement Services is configured with one switch connection that connects the Application Enablement Services to the DC1 site Communication Manager. DC1 has this configuration for voice for regular operations. The switch connection has a Telephony Server Application Programming Interface (TSAPI) link which maps to CTI link 1 on the Communication Manager. The DC2 Application Enablement Services also has one switch connection that connects it to the DC1 Communication Manager. However, on the DC2 Application Enablement Services, the ESS is added under the switch connection in Survivable Hierarchy. The DC2 Application Enablement Services can connect to both the main Communication Manager and ESS using the same CTI link. When the Communication Manager is functional, the DC2 Application Enablement Services is connected to it through the CTI link <x>, and when the Communication Manager is non-functional, the DC2 Application Enablement Services uses the Survivable Hierarchy to connect to the ESS using the same CTI link <x>.			
10.	Switch connection	The switch connection name configured on the DC2 Application Enablement Services is the same as on the DC1 Application Enablement Services. This allows you to configure the Call Server Connector (CSC) attributes in Avaya Workspaces for Call Center Elite so that the CSC can connect to either Application Enablement Services. Therefore, the Application Enablement Services user for Avaya Workspaces for Call Center Elite must have the same name and password configured on each Application Enablement Services. This switch connection has a TSAPI link which maps to CTI link <x> on the Communication Manager and has the following attributes to be configured: • **Link** • **Switch Connection** • **Switch CTI Link Number** • **ASAI Link version** • **Security**	
11.	Survivability Hierarchy - Steps to add ESS in Survivability Hierarchy	Adding Enterprise Survivable Server in Survivability Hierarchy on page 39	

Table continues…

No.	Task	Description	✔
CallServerConnector Configuration You must configure the CSC snap-in attributes so that the CSC connects to Application Enablement Services. The CSC is configured the same in both DC1 and DC2 Avaya Workspaces for Call Center Elite, except that the DC2 CSC must be configured with two Application Enablement Services IP addresses, one for the DC1 Application Enablement Services and the second for the DC2 Application Enablement Services.			
12.	Configure CSC atts (primary)	Configuring the CallServerConnector attributes for DC1 on page 40	
13.	Configure CSC atts (DR)	Configuring the CallServerConnector attributes for DC2 on page 41	

Adding a node name for Enterprise Survivable Server on Communication Manager

Procedure

1. Log on to Communication Manager System Access Terminal (SAT) as `init` user.
2. Run the command: **`change node-names ip`**
3. In **Name**, enter a name for the Enterprise Survivable Server (ESS) server.
4. In **IP Address**, enter the ESS server IP address.
5. Press **F3** to save the changes.

Adding a Survivable Processor on Communication Manager

About this task

Use this procedure to add a Survivable Processor entry on the Communication Manager for the Enterprise Survivable Server using the node name created. For more information, refer Adding a node name for Enterprise Survivable Server on Communication Manager on page 34.

Procedure

1. Log on to Communication Manager System Access Terminal (SAT) as `init` user.
2. Run the command: **`add survivable processor <node name>`**
3. On the configuration page 1, enter the following:
   a. In **Type**, enter `simplex-ess`.
   b. In **Cluster ID/MID**, enter the cluster number in use.
   c. In **Enable PE for H.323 Endpoints?**, enter `y`.
   d. In **Enable PE for H.248 Gateways**, enter `y`.

Important:

Retain the other field values as default. **V4 Node Name** and **Address** fields auto populates with details from the node name created earlier.

4. On the configuration page 2, ensure that **AESVCS** is enabled.

   This field is enabled by default.

5. On page 3, in **Priority with respect to Media Servers**, enter `2`.

   Important:

   Further page options open. Available pages change from 3 to 8, where you can configure the Avaya Aura® Media Server that the Enterprise Survivable Server uses.

6. On page 4, enter the Avaya Aura® Media Server number that the Enterprise Survivable Server is using.
7. To view list of available Avaya Aura® Media Servers run the command: **`list media-server`**

   The **Node-Name** field is populated automatically.

8. On configuration pages 5,6,7 and 8, retain the default values.
9. Press **F3** to save the changes.
10. To save translations after the configuration changes, run the command: **`save translations`**

Configuring the server role for the Enterprise Survivable Server in DC2

Procedure

1. Open the Enterprise Survivable Server (ESS) web admin portal using the following URL:

   `https://<ESS_IP_Address>/cgi-bin/common/login/webLogin`

2. Log in as `init` user.
3. Navigate to **Administration** > **Server Maintenance** > **Server Configuration** > **Server Role**.

   The Server Role page opens.

4. In the **Server Settings** area, enter the following details:
   a. In **This Server is**, select **an enterprise survivable server (ESS)**.
   b. In **System ID and Module ID**, for **SID** and **MID**, enter `1` and `3` respectively.

   Note:

   The MID must match the **Cluster ID/MID** set for the Survivable Processor configured earlier.

5. In the **Configure Survivable Data** area, enter the following details for the components:
   a. In **Registration address at the main server (CLAN or PE Address)**, enter the Communication Manager IP address.
   b. In **File Synchronization address at the main cluster (PE Address)**, enter the Communication Manager IP address and the duplicate server if in use.
   c. In **File Synchronization address at the alternate** main cluster (PE Address)**, enter.
6. In the **Configure Memory** area, configure the server memory settings as required.
7. Click **Save** to save the changes.

Configuring ESS network

Procedure

1. Open the Enterprise Survivable Server (ESS) web admin portal using the following URL:

   `https://<ESS_IP_Address>/cgi-bin/common/login/webLogin`
2. Log in as `init` user.
3. Navigate to **Administration** > **Server Maintenance** > **Server Configuration** > **Network Configuration**.

   The Network Configuration page opens.
4. Enter all the required details under Network Configuration for the ESS.

   Important:

   Ensure the **Server ID** field matches the **Server ID** value configured for the Survivable Processor on Communication Manager.

Verifying the status of Survivable Processor

About this task

Use this procedure to view the status of Enterprise Survivable Server (ESS) on Communication Manager.

Before you begin

Configure ESS on Communication Manager. After configuring the ESS status is displayed as **Reg** - `y`.

Procedure

1. Log on to Communication Manager System Access Terminal (SAT) as an `init` user.
2. Run the following command: **`list survivable-processor`**

   Reg - `y`

   Act - `n`

When the Communication Manager is offline, the **Act** field displays `y`.

Adding a CTI link to the DC2 Application Enablement Services

About this task

Avaya Workspaces for Call Center Elite DR setup requires two Computer Telephony Integration (CTI) links. Link 1 is connected to DC1 Application Enablement Services, and link 2 is connected to DC2 Application Enablement Services.

Link 1 to the DC1 Application Enablement Services is pre-configured as it is required for regular Avaya Workspaces for Call Center Elite voice.

Use this procedure to add Link 2 to the DC2 DR Application Enablement Services.

Procedure

1. Log on to Communication Manager System Access Terminal (SAT) as an `init` user.
2. Run the following command: **`add cti-link 4`**
3. On configuration page 1, do the following:
   a. In **Extension number**, enter the required extension number.
   b. In **Type**, enter `ADJ-IP`.
   c. In **Name**, enter the required name.
   d. Retain the other field values as default.

   Note:

   Security code can be blank.
4. On configuration page 2, do the following:
   a. In **IC Adjunct Routing?**, enter `y`.
   b. Retain the other field values as default.
5. On configuration page 3, retain the field values as default.
6. Press **F3**.

Adding a second Adjunct Route to vectors

About this task

Vectors are pre-configured in DC1 as they are required for regular Avaya Oceana® voice.

Use this procedure to add a second Adjunct Route to any vectors with an adjunct route configured for the DC2 DR setup.

Procedure

1. Log on to Communication Manager System Access Terminal (SAT) as an `init` user.
2. To add the second Adjunct Route link, run the following command: **`change vector <x>`**

3. On the edit page tab, on the line below the 1st adjunct route link, in **adjunct routing link**, type <y>.

   Where:

   <x> is the vector you change.

   <y> is the Computer Telephony Integration (CTI) link to the DR Application Enablement Services.

4. Repeat the process to update all vectors with an adjunct route link.

Configuring IP services

About this task

You must have **ip-services** entries for DC1 and DC2 Application Enablement Services servers. The **AESVCS** service is pre-configured under **ip-services** as this is required for regular Avaya Workspaces for Call Center Elite voice.

Use this procedure to add the DC2 Application Enablement Services server.

Procedure

1. Log on to Communication Manager System Access Terminal (SAT) as an `init` user.
2. Run the following command: **`change ip-services`**
3. On page 3, enter the DC2 site Application Enablement Services server name and password.

   Note:

   This password is used when configuring the switch connection on Application Enablement Services.

4. Press **F3**.

Viewing Enterprise Survivable Server cluster status

About this task

Use this procedure to view the state of the main server and all administered Survivable Core Servers. Under normal conditions, with full network connectivity, all Survivable Core Servers must register with the main.

Before you begin

Ensure that you have the credentials of an `init` user.

Procedure

1. Log on to Communication Manager System Access Terminal (SAT) as an `init` user.
2. To view the Enabled, Registered, and Translations status of the Enterprise Survivable Server (ESS), run the following command: **`status ess clusters`**

Configuring Avaya Aura® Media Server

About this task

Ensure you have a DC2 site Avaya Media Server (AMS) registered in Communication Manager and the Survivable Processor settings. If the DC2 AMS is not on Communication Manager, add it.

Procedure

1. To add a node name for AMS, do the following:
   a. Run the following command: **`change node-names ip`**
   b. In **Name**, type the AMS name.
   c. In **IP Address**, enter the IP address.
   d. Press **F3**.
2. To add a signaling group that points to the new node, do the following:
   a. Run the following command: `add signaling-group <x>`
   b. In **Group Type**, type `sip`.
   c. In **Peer Detection Enabled**, type `n`.
   d. In **Peer Server**, type `AMS`.
   e. In **Far-end Node Name**, type DC2 AMS node name.
   f. In **Far-end Network Region**, type `1`.
   g. Press **F3**.
3. To add a media server, do the following:
   a. Run the following command: **`add media-server <x>`**
   b. In **Signaling Group**, type the group number you configured in the previous step.
   c. In **Channel limit**, type the required limit.
   d. Press **F3**.
4. After configuring the AMS, run the following command: **`save translations`**

Adding Enterprise Survivable Server in Survivability Hierarchy

About this task

The IP address for the Enterprise Survivable Server (ESS) is configured under Survivability Hierarchy for the switch connection. The ESS connection in the survivable hierarchy becomes `active` if the Communication Manager fails while the Communication Manager switch connection is `In Use` and the ESS connection status is `Idle`.

The **Cluster ID/MID** configured here matches the **Cluster ID** of the ESS or the Survivable Processor configured on Communication Manager.

Procedure

1. Log on to the DC2 Application Enablement Services web admin portal.
2. Navigate to **Communication Manager Interface** > **Switch Connections**.
3. On the **Switch Connection** page, click **Survivability Hierarchy**.
4. Type the ESS Cluster ID/MID value configured earlier and click **Insert**.
5. Click **Edit PE IP** and type the ESS server IP address.
6. Restart the Application Enablement Services server.

   The Application Enablement Services connects to the DC1 Communication Manager using the switch connection and to the ESS using the Survivable Hierarchy functionality when the Communication Manager fails.

Configuring the CallServerConnector attributes for DC1

About this task

The Call Server Connector (CSC) snap-in is a Voice-only Service Provider interface to the underlying switching infrastructure. You must configure the CSC attributes for call control and agent control functions on DC1.

Procedure

1. Log on to Avaya Aura® System Manager.
2. Navigate to **Elements** > **Avaya Breeze** > **Configuration** > **Attributes**.
3. Click the **Service Clusters** tab.
4. Select the **Provisioning Cluster** for DC1.
5. Select the **Oceana Configuration** service.
6. In **Voice Provider Id**, enter the name of your voice provider configured in Avaya Control Manager.
7. In **Application Enablement Services IP address**, enter the IP address of the DC1 Application Enablement Services.
8. In **Communication Manager Connection Name on Application Enablement Services**, enter the name of your switch connection configured in Application Enablement Services.
9. In **AES user**, type the username of the user configured on Application Enablement Services for Avaya Workspaces for Call Center Elite connection.
10. In **AES user password**, type the password of the user.
11. Reboot the common cluster to enable the changes to CallServerConnector attributes.

Configuring the CallServerConnector attributes for DC2

About this task

You must configure the CSC attributes for call control and agent control functions on DC2.

Procedure

1. Log on to Avaya Aura® System Manager.
2. Navigate to **Elements** > **Avaya Breeze** > **Configuration** > **Attributes**.
3. Click the **Service Clusters** tab.
4. Select the **Provisioning Cluster** for DC2.
5. Select the **Oceana Configuration** service.
6. In **Voice Provider Id**, enter the name of your voice provider configured in Avaya Control Manager.
7. In **Application Enablement Services IP address**, enter the IP address of the DC1 and DC2 Application Enablement Services.
8. In **Communication Manager Connection Name on Application Enablement Services**, enter the name of your switch connection configured in Application Enablement Services.
9. In **AES user**, type the username of the user configured on Application Enablement Services for Avaya Workspaces for Call Center Elite connection.
10. In **AES user password**, type the password of the user.
11. Reboot the common cluster to enable the changes to CallServerConnector attributes.

Failover Scenarios

The three failover scenarios for the voice channel in Avaya Oceana® are as follows:

- Primary Active - a system in regular operation.
- Partial switchover - Avaya Oceana® is switched over, but primary Avaya Aura® is active.
- Full switchover - Avaya Oceana® and Avaya Aura® are switched over.

Primary Active

The **Primary Active** state describes the solution in regular operation. The DC2 is prepared for a failover, but all the components are active in the DC1.

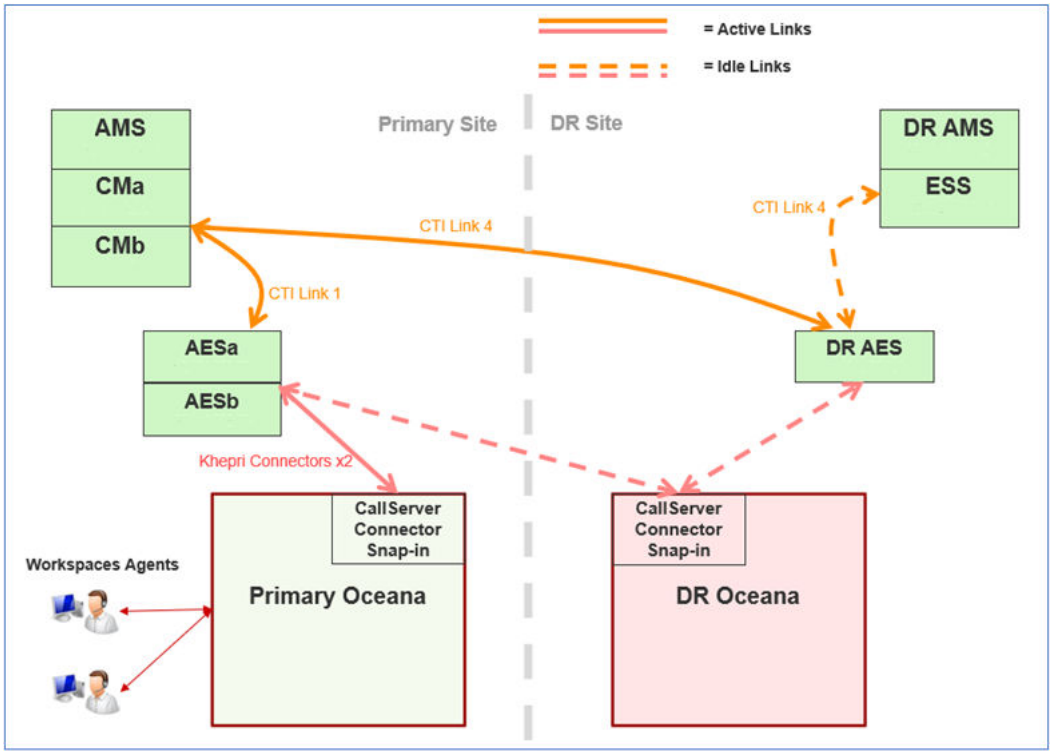


Figure 2: Avaya Oceana® DR Voice - Primary Active state

- DC1 Avaya Oceana® is active.
- The CallServerConnector snap-in connects to the DC1 Application Enablement Services through Khepri connectors (x2).
- The DC1 Application Enablement Services connects to the Communication Manager through Computer Telephony Integration (CTI) Link 1.
- The Communication Manager has an active CTI Link (4) to the DC2 Application Enablement Services because both components are functional, but this link is not used in this scenario.

Partial Switchover

A **Partial Switchover** is a scenario where the Avaya Oceana® components, such as Avaya Breeze® nodes and hosted services, are failed over to the DC2. In this scenario, the DC1 Avaya Aura® components remain active, so the Enterprise Survivable Server (ESS) does not become active.

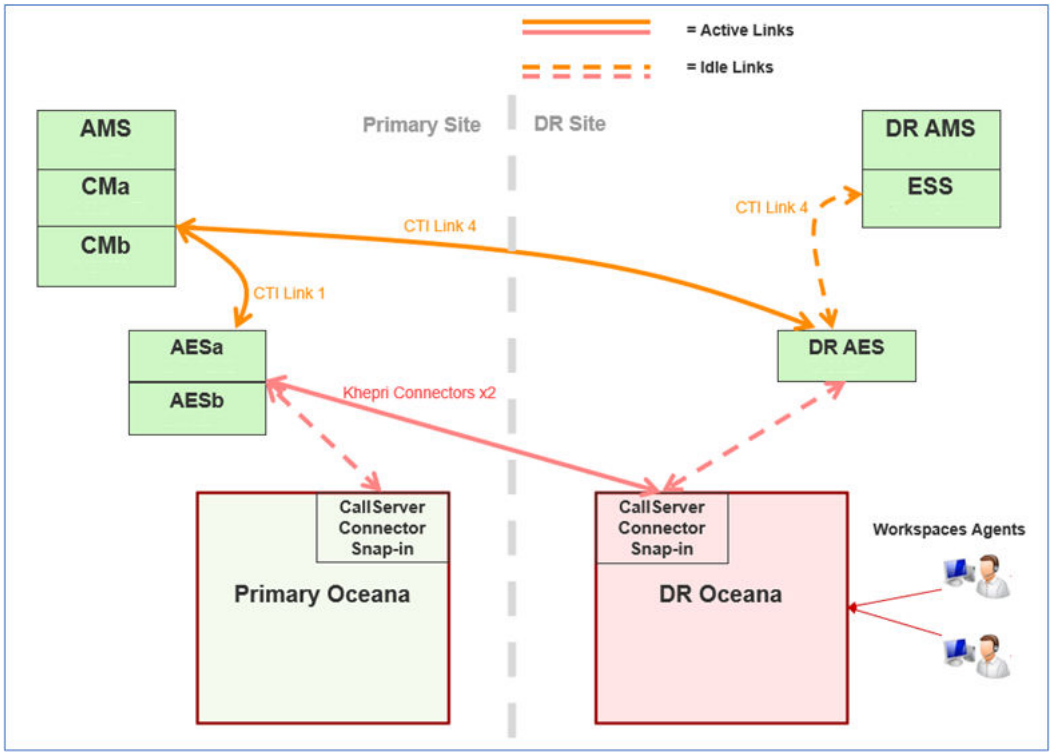


Figure 3: Avaya Oceana® DR Voice - DR Active state (Partial Switchover)

- DC2 Avaya Oceana® is active.
- The DC2 CallServerConnector snap-in connects to the DC1 Application Enablement Services through Khepri connectors (x2).
- The DC1 Application Enablement Services connects to the Communication Manager through Computer Telephony Integration (CTI) Link 1.
- The Communication Manager has an active CTI Link (4) to the DC2 Application Enablement Services because both components are functional, but this link is not used in this scenario.

Full Switchover

In a **Full Switchover** scenario, the DC1 Avaya Aura® components are non-functional, so all the functionality moves to the DC2. The link between the DC2 Application Enablement Services and the Enterprise Survivable Server (ESS) configured under Survivable Hierarchy becomes active because the main switch connection between the DC2 Application Enablement Services and the Communication Manager is not functional. This enables Avaya Oceana® to continue working in the fully switched-over state with voice capability.

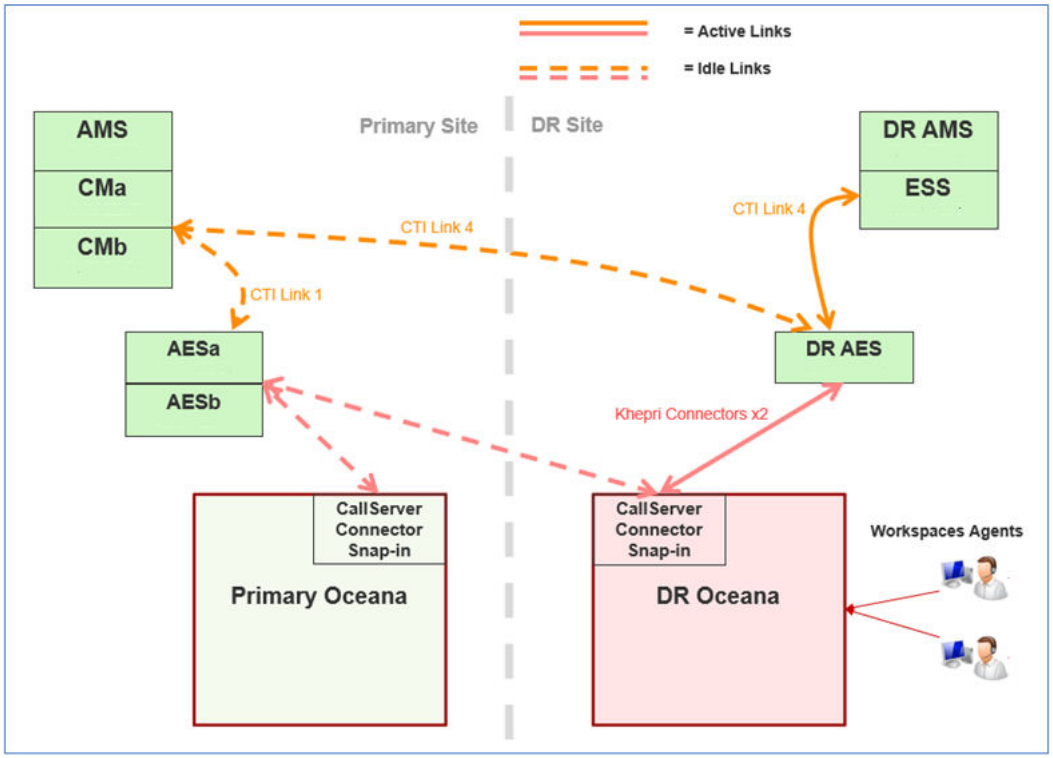


Figure 4: Avaya Oceana® DR Voice - DR Active state (Full Switchover)

- DC2 Avaya Oceana® is active.
- The DC2 CallServerConnector snap-in connects to the DC2 Application Enablement Services through Khepri connectors (x2).
- The DC2 Application Enablement Services connects to the ESS through Computer Telephony Integration (CTI) Link 4.

Configuring ACM for Disaster Recovery

Configuration Checklist

Important:

For detailed information on High Availability (HA) deployment for Avaya Control Manager, refer Installing Avaya Control Manager.

No.	Task	Description	✔
1.	Enable the Toggle button in Avaya Control Manager	Enable Disaster Recovery Support Avaya Control Manager on page 45	

Table continues…

No.	Task	Description	✔
2.	Configuring DC2 application details in the UCA server in DC1	Configuring DC2 application details in the UCA server in DC1 on page 46	
3.	Configure DC2 application details in the Avaya Analytics™ server in DC1	Configuring Data Center 2 application details in the Analytics server in Data Center 1 on page 47	
4. .	Enabling authorization in the Avaya Analytics server	Enabling authorization in the Avaya Analytics server on page 48	

Enable Disaster Recovery Support 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. To disable the Disaster Recovery option, clear the **Disaster Recovery** checkbox.

   If any disaster recovery enabled systems are in a fail-over state, Avaya Control Manager disables the **Disaster Recovery** checkbox. The administrator cannot disable the Disaster Recovery option.
5. On the Avaya Control Manager webpage, click **Configuration** > **Locations**.
6. Select the location of your Avaya Oceana® and click **Edit**.
7. On the Location Edit page, click the **Systems** tab.
8. 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.
9. 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 DC2 application details in the UCA server in DC1

Before you begin

Ensure that you enable the Oceana Disaster Recovery options on the **System Parameters** page.

Procedure

1. Log on to Avaya Control Manager.
2. Navigate to **Configuration** > **Avaya Oceana™** > **Server Details**.
3. On the Oceana Server List page, click **Edit an Oceana Server**.
4. In the Failover Server tab, perform the following steps:
   a. In the **Alias** field, enter an alias name for the Avaya Oceana® failover server.
   b. In the **API URL** field, enter the URL of the Avaya Oceana® UCA REST interface.

      For example: `https:// <AvayaOceanaCluster1_DR_FQDN>/services/UCAStoreService/uca`

      Important:

      If the Avaya Oceana® deployment and the Avaya Analytics™ deployment are using the same UCA server (Common setup), then the URLs configured for the Avaya Oceana® server must use the exact same URL as the Avaya Analytics™ server. That is, the Avaya Oceana® server URL and the Avaya Analytics™ server URL must use either an IP address or an FQDN. You cannot use an IP address on one server and the FQDN on the other server.
   c. From the **Version** drop-down list, select the Avaya Oceana® version.
   d. In the **Avaya Oceana Workspaces Welcome Page URL** field, enter the server URL for Workspaces.
   e. In the **Workspaces Widget Library URL** field, enter the Widget Library for Workspaces.
   f. In the **OMNI Channel Database Server** field, enter the Database Server address for OMNI Channel.
   g. In the **Authorization Service URL** field, enter the URL Server of the service.
   h. From the **Breeze alias** drop-down list, select the alias of the Avaya Breeze® platform instance.
5. Click **Save**.
6. Do one of the following:
   - Navigate to **Configuration** > **Customer Engagement** > .
   - In the **Search** field, type `Avaya Analytics` and click the **Avaya Analytics™ Configuration/Customer Engagement tile** link.
7. On the Avaya Analytics Server List page, click **Edit an Analytics Server**.

8. In the **Failover Server** tab, perform the following steps:
    a. In the **Alias** field, enter an alias name for the Avaya Analytics™ failover server.
    b. In the **API URL** field, enter the URL of the Avaya Analytics™ UCA REST interface.
    c. From the **Version** drop-down list, select the version number of Avaya Analytics™.
    d. From the **Breeze alias** drop-down list, select the alias of the Avaya Breeze® platform instance.
9. 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 Breeze** field, enter the appropriate value.
6. Click **Save**.

Configuring Omnichannel for disaster recovery

Omnichannel database mirroring configurations

Avaya Oceana® supports the following two options for Omnichannel Database Disaster Recovery (DR):

- Omnichannel Campus (active only) with DR
- Omnichannel Campus (active and standby) with DR

Data Center 1 has the Campus installation and Data Center 2 has the DR installation. 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.
- Select **Require SSL/TLS** only for the configurations using SSL/TLS certificates.

Verifying the Omnichannel Database mirroring status

About this task

All planned full and partial DR switchovers require that the Omnichannel DB servers in both locations are functioning properly and that data is mirrored between them. After a planned switchover, mirroring shall initiate from the DR site (DC2) to the original primary site (DC1).

In the event of unplanned switchovers due to Omnichannel failures, you must reinstate the failed servers first, and then reinstate the mirroring. Refer to Clean up Mirror setup on DC1 and DC2 on page 159 for procedure on reinstating a failed Omnichannel server before proceeding with the switchover.

It is important to verify that data from the primary Omnichannel database is actually mirrored across a data link to the DR database before switchback. To do this, log on to the Omnichannel Database server in the DR site and verify the mirroring status from the primary to DR site. This is a necessary step to ensure operational readiness before switchback.

Use the following steps to verify the DB mirroring status using the Oceana Data Management (ODM) tool:

Procedure

1. Connect to the primary Omnichannel database server.
2. Run the Omnichannel server software using an administrator account.
3. On the Omnichannel host, navigate to the application drive and start the ODM tool.

   For example, navigate to `D:\Avaya\Oceana\MMDataManagement\OceanaDataManagementTool application executable` for ODM.
4. Run the ODM tool using the same administrator account.
5. Navigate to **Configuration** > **Mirror Settings**.

   The Mirror Status window shows the current mirroring status for all mirror members, including the primary Omnichannel database and the DR Omnichannel database.

Checklist for configuring Cache Mirroring for Omnichannel Campus (active only) with DR

Use the following checklist to configure Cache Mirroring for Omnichannel Campus (active only) in Data Center 1 and DR in Data Center 2:

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 50.	
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 51.	
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 53.	
4	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 55.	

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. 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**.
2. In the Services window, do the following:
   a. Right-click **ISCAgent service** and select **Start**.
   b. Double-click the **ISCAgent service**.
   c. Click the **General** tab.
   d. In the **Startup type** field, select `Automatic`.
   e. Click the **Recovery** tab.
   f. In the **First failure**, **Second failure**, and **Subsequent failures** fields, select the **Restart the Service** option.

g. In the **Reset fail count after** field, type `120`.

h. In the **Restart service after** field, type `0`.

i. Click **Apply**.

j. Click **OK**.

3. Navigate to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement` folder.
4. Right-click the `OceanaDataManagementTool.exe` file and click **Run as administrator**.
5. Navigate to **Configuration** > **Mirror Settings** > **Create Mirror**.
6. Enter the details for **Arbiter address**, **Virtual IP** and **Network Interface**.
7. 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
8. Click **Save**.
9. In the Oceana Data Management utility, click **Backup And Restore**.
10. In the navigation pane, click **Backup And Restore**
11. In the **Select/create file to backup to** field, click **Browse**.
12. 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**.
13. Click **Backup Database**.

    The utility displays the `Backup complete!` message when the backup process is complete.
14. 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. 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**.

2. In the Services window, do the following:
   a. Right-click **ISCAgent service** and select **Start**.
   b. Double-click the **ISCAgent service**.
   c. Click the **General** tab.
   d. In the **Startup type** field, select `Automatic`.
   e. Click the **Recovery** tab.
   f. In the **First failure**, **Second failure**, and **Subsequent failures** fields, select the **Restart the Service** option.
   g. In the **Reset fail count after** field, type `120`.
   h. In the **Restart service after** field, type `0`.
   i. Click **Apply**.
   j. Click **OK**.
3. Navigate to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement` folder.
4. Right-click the `OceanaDataManagementTool.exe` file and click **Run as administrator**.
5. Navigate to **Configuration** > **Mirror Settings** > **Join Mirror**.
6. In the **Type** attribute, select **Disaster Recovery**.
7. Type the IP address of the agent and select **Virtual address interface**.
8. 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.
9. Click **Save**.
10. Copy the backup file from the active Omnichannel Database server in Data Center 1 to the backup Omnichannel Database server in Data Center 2.
11. In the Oceana Data Management utility, click **Backup And Restore**.
12. In the navigation pane, click **Backup And Restore**
13. In the **Select file to restore from** field, click **Browse**.

14. On the Open dialog box, do the following:
    a. Browse to the location where you stored the backup file.
    b. Select the backup `cbk` file.
    c. Click **Open**.
15. Click **Restore Database**.
16. For **Are you restoring a mirrored backup**, click **Yes**.
17. 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.
18. To verify whether the restore was successful, do the following:
    a. On Cache Management Portal, click **System Operation** > **Mirror Monitor**.
    b. Click **Details**.

       Verify both Avaya Oceana® 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. This is applicable for both DR options.

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. Right-click the `OceanaDataManagementTool.exe` file and click **Run as administrator**.
    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. Right-click the `OceanaDataManagementTool.exe` file and click **Run as administrator**.
   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

      Where, <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 for Omnichannel Campus (active and standby) with DR

Use the following checklist to configure Cache Mirroring for Omnichannel Campus (active and standby) in Data Center 1 and DR in Data Center 2:

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	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 51.	
3	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 53.	
4	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 55.	

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. This is applicable for both DR options.

Before you begin

- Securing the Cache Mirror on the Omnichannel Database server in Data Center 1 and Data Center 2 on page 53

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**.

Configuring Context Store for Disaster Recovery

Configuration Checklist

No.	Task	Description	✔
1.	Enable SSL connection for Avaya Context Store replication from DC1 to DC2.	See Enabling SSL connection for Context Store replication from DC1 to DC2 on page 57.	
2.	Retrieve the System Manager root certificate.	See Retrieving the System Manager root certificate on page 57.	
3.	Create a new keystore certificate file.	See, • Creating a new keystore certificate file on page 58. • Modifying end entity profile on page 58. • Creating a new keystore certificate file for Data Center 1 of Avaya Oceana Cluster 1 on page 59.	
4.	Add CA root certificate and keystore certificate files to DC2 Cluster 1 nodes.	Adding CA root certificate and keystore certificate files to Data Center 2 Cluster 1 nodes on page 60.	
5.	Enable Context Store integration to External Data Mart in DC1.	Enabling Context Store integration to External Data Mart in Data Center 1 on page 60.	

Enabling SSL connection for Context Store replication from DC1 to DC2

About this task

Use this procedure to enable Context Store replication from DC1 to the geo-redundant Context Store in DC2.

Note:

Context Store replication functions only when DC1 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 DC2.
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 DC2.
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 DC2.

   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 DC1.

   On the System Manager host, verify that the file ownerships are set to `wsuser:susers` and the permissions are set to `775`, similar to the other files in the Gigaspaces security folder.

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

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**.

Configuring Avaya Oceana® for Disaster Recovery

Configuration Checklist

Important:

You must install the following at DC1 and DC2.

- Ensure the deployment is complete for DC1 and DC2.
- Install required Avaya Oceana® snap-ins.
- Install all required Engagement Designer tasks and workflows.

  For detailed information on installation procedures, see Deploying Avaya Oceana®.

No.	Task	Description	✔
1.	Set cluster activity status for clusters in DC1	Setting cluster activity status for clusters in DC1 on page 62	
2.	Configure Oceana Monitor authorization for DC1	Configuring Oceana Monitor authorization for DC1 on page 63	

Table continues…

No.	Task	Description	✔
3.	Set disaster recovery attributes in OceanaConfiguration snap-in for DC1 UCAStoreService and Context Store	Setting disaster recovery attributes in OceanaConfiguration snap-in for Data Center 1 UCAStoreService and Context Store on page 64	
4.	Configure Oceana Monitor authorization for DC2	Configuring Oceana Monitor authorization for DC2 on page 65	
5.	Set disaster recovery attributes	Setting disaster recovery attributes in OceanaConfiguration snap-in for Data Center 2 UCAStoreService and Context Store on page 65	
6.	Set the cluster activity status for the clusters in DC2	Setting the cluster activity status for the clusters in DC2 on page 66	
7.	Unified Collaboration Administration data synchronization	Schedule database backups UCMServer and UCAStoreService on page 67 • Preparing DC2 for UCA restore from DC1 on page 68 • Taking a backup of UCAStoreService on page 69 • Restoring UCAStoreService data on DC2 on page 70 • Installing UCAStoreService on DC2 on page 71	
8.	Web voice and web video requirements	Web voice and web video requirements on page 73	
9.	Reboot DC1 and DC2 Avaya Oceana® clusters	Rebooting DC1 and DC2 Avaya Oceana clusters on page 71	
10.	Verify replication status for all disaster recovery components	• Verifying the UCA replication status on page 71 • Verifying Context Store replication status on page 73 • Verifying the Omnichannel Database mirroring status on page 49	

Setting cluster activity status for clusters in DC1

Before you begin

Ensure that the OceanaMonitorService is installed on the clusters in DC1 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 DC1 or DC2, 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 Primary and Backup DC clusters and also check Data Replication and Service Install status have green check marks.
   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 for DC1

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® Configuration Cluster**.
   b. In the **Service** field, click **Authorization Service Address**.

3. 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.
4. 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 **Cluster**, click DC1 Provisioning Cluster.
    b. In **Service**, click **OceanaConfiguration**.
3. In the Geo-Redundancy area, in **Disaster Recovery Mode**, do the following:
    a. Select the **Override Default** check box.
    b. In **Effective Value**, select `GEO Primary`.
4. Identify **Geo-Redundant Common Cluster** and do the following:
    a. Select the **Override Default** check box.
    b. In **Effective Value**, select Avaya Oceana® Cluster 1 that you created in DC2, which hosts 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 **Effective Value**, enter the name of the keystore file required for Context Store replication.

    For more information, see Creating a new keystore certificate file on page 58 and Enabling SSL connection for Context Store replication from DC1 to DC2 on page 57.
6. Identify the attribute **Keystore Password** and do the following:
    a. Select the **Override Default** check box.
    b. In **Effective Value**, 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.

Configuring Oceana Monitor authorization for DC2

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® Configuration Cluster**.
   b. In the **Service** field, click **Authorization Service Address**.
3. 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.
4. Click **Commit**.

Setting disaster recovery attributes in OceanaConfiguration snap-in for Data Center 2 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.

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 58 and Enabling SSL connection for Context Store replication from DC1 to DC2 on page 57.
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 2.

Setting the cluster activity status for the clusters in DC2

Before you begin

You must install OceanaMonitorService on the clusters in DC2.

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 2, 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 Primary and Backup DC clusters and also check Data Replication and Service Install status have green check marks.
    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 DC2 are now in the `Deny` state.

Schedule database backups UCMServer and UCAStoreService

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.

Scheduling Database Backups UCMServer and UCAStoreService

About this task

Use this procedure to schedule automatic backups of the UCAStoreService/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 required service check box and click **Continue**.

    Select the **UCMService** and **UCAStoreService database** check boxes to be included in the backup.
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 time zone 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`.

Preparing DC2 for UCA restore from DC1

About this task

In the event scheduled backups have not been configured or completed recently, use this procedure to manually backup UCAStoreService in preparation to restore this data in Avaya Oceana® deployment in Data Center 2. The UCAStoreService database contains all the information related to users, accounts, attributes, providers, and resources that are 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.

Taking a backup of UCAStoreService

About this task

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

Procedure

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

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

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

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

12. Click **OK**.
13. Click **Commit**.

Note:

The backup location is a one-time configuration, after which the successive backups reuse the same information.

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

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

    Important:

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

    After the backup process is complete, verify that the **Status** column on the Backup and Restore Status page displays the status `Completed`.

Restoring UCAStoreService data on DC2

About this task

If the Unified Collaboration Administration (UCA) instance in DC1 contains data, you must create a manual backup and restore the UCAStoreService data from DC1 to the Avaya Oceana® Cluster 1 on DC2.

Procedure

1. Log in to System Manager.
2. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
3. On the Services page, click **UCAStoreService**.
4. Verify that the UCAStoreService is not in the `Installed` state in the DR cluster.

   Important:

   You cannot restore the UCAStoreService data backup if the service is in the `Installed` state in the DR cluster. Therefore, to uninstall the service, select the **UCAStoreService** check box and click **Uninstall**.
5. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
6. In the **Backup and Restore** field, select **Restore**.
7. On the Backup and Restore Status page, in the Backup and Restore Jobs area, select the check box of the latest backup file.
8. Click **Restore**.
9. In the Cluster Database Restore Confirmation dialog box, select Avaya Oceana® Cluster 1.
10. Click **Continue**.

On the Backup and Restore Status page, ensure that the **Status** column for the restore operation displays the value `Completed`.

Installing UCAStoreService on DC2

About this task

After restoring the UCAStoreService data to the Avaya Oceana® Cluster 1 on DC2, you must install the UCAStoreService on Avaya Oceana® Cluster 1 on DC2.

Procedure

1. Log in to System Manager.
2. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
3. On the Services page, select the **UCAStoreService** check box.
4. Click **Install**.
5. In the **Confirm Install service: UCAStoreService** dialog box, select the Avaya Oceana® Cluster 1 check box on the DC2.
6. Click **Commit**.
7. On the Services page, verify that the state of the service is `Installing`.

   After the installation is complete, the service state changes to `Installed`.

Rebooting DC1 and DC2 Avaya Oceana® clusters

For a disaster recovery deployment, you must reboot all the Avaya Oceana® clusters in DC1 and DC2.

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.

Verify replication status for all disaster recovery components

Verifying the UCA replication status

About this task

Important:

- The UCA replication check does not work with the token-based access turned on.

  To disable the token access from Avaya Aura® System Manager, select `Cluster 1` then select `UCAStoreService` and set *Enable Tokenless Access* to `true`.
- To verify if the UCA replication is functioning between primary and disaster recovery (DR) sites, you must make an administrative change in the Avaya Control Manager application and then submit the change to the primary UCA instance. The system replicates this

change from the primary UCA to the DR UCA. You must add a new test attribute to Avaya Oceana® and verify that this is replicated across the DR UCA instance.

- When verification is complete revert `UCAStoreService` and set *Enable Tokenless Access* to `false`.
- 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. From 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 the PU status of **uca-gateway-pu** and **uca-store-space** PUs are `INTACT`.

   If it is not present or has a status `Scheduled` or `Broken`, then the system indicates that the UCA replication is not operational. You must resolve this issue before proceeding with the switchover.
5. On the primary site, go to the **Show Cluster Messages** tab, select the **UCAStoreService** PU.
6. Verify that the `HEARTBEAT` message for the replication channel state is `ACTIVE`.
7. Repeat steps 1 through 6 for Avaya Oceana® Cluster 1 in Data Center 2.

   Note:

   On the **Cluster Messages** tab, in the **UCAStoreService** messages, check the last Cluster DB updated message time on all nodes on both the primary and DR sites.

   Perform the subsequent steps only after successfully completing up to step 6.
8. Log on to the primary Avaya Control Manager server instance.
9. Add a new test attribute and save the attribute to the primary UCA instance.
10. Reload the cluster message, select **UCAStoreService**, and check the new time of the Cluster DB updated message.

    The time of the updated message must coincide with the newly added attribute.
11. To check for any replication errors alarmed on System Manager, do the following.
    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 investigate the issue to ensure replication is operational before a switchover.

If the replication to DR gives an error, you can back up the replication and synchronize the updates manually. Ensure the replication is working.

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.

Optionally, you must also create a context to verify that the 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.

Configuring Web Voice Web Video

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.

Configuring Avaya Analytics™ Disaster Recovery

Overview

Avaya Analytics™ disaster recovery provides a planned approach to re-establish critical services at a secondary data center when a complete outage occurs at the primary data center.

This section provides information on how to configure a geographically redundant Avaya Oceana®, so that when a primary data center outage occurs, the redundant site can be made operational.

In this configuration, two instances of Avaya Analytics™ are deployed in two separate data centers with Write Ahead Log (WAL) streaming between the operational reporting databases. With WAL streaming, the primary data center database continuously streams updates to the secondary data center.

Avaya Analytics™ also provides support for disaster recovery scenarios where you might lose the primary DB node in DC1 for an extended period of time and you want to configure your DC2 system to stream from the failed over replica node on DC1 instead of the default primary node.

Analytics Geo Enhancements

The Analytics Geo solution is enhanced for Historical Reporting so that the custom reports and local users in the metadata are replicated from a primary DC to a secondary DC.

- Replication of Historical Reporting Local users in metadata to DC2.
- Replication of Historical Reporting custom reports in metadata to DC2.

Note:

In this configuration where two instances of Avaya Analytics™ are deployed the Historical Reporting Administrator credentials must be identical as this is replicated between both DC1 and DC2.

Warning:

If Geo Primary performs a full backup during a network outage and Geo Standby cannot access the NFS server on Geo Primary, Geo Standby loses the WAL archive sequence to catch up after the network outage is resolved.

Losing the WAL archive sequence to catch up causes the Geo alarm to trigger as the last update received on Standby exceeds the time limit.

Consequently, it is necessary to run the CCM analytics script on Geo Standby to recreate the standby system based on the new backup and WAL archives.

Disaster Recovery Configuration Checklist

Complete the following processes to prepare the solution for a future disaster recovery scenario.

No.	Task	Description	✔
1.	Configure Avaya Analytics™ for Disaster Recovery.	See Configuring Avaya Analytics for Disaster Recovery on page 75.	
2.	Configure Avaya Analytics™ server details for real-time reporting.	See Configuring Avaya Analytics™ 4.x server details for real-time reporting on page 78	

Configuring Avaya Analytics™ for Disaster Recovery

About this task

Use this procedure to configure geo-redundancy at the primary (Data Center1) and the standby site (Data Center2).

Before you begin

Complete the Avaya Analytics™ deployment on Avaya Common Services.

During Avaya Analytics™ deployment on Avaya Common Services for DC1 and DC2 sites, ensure that the same passwords are employed for Postgres user, Measure Processor user, and Historical Reporting user in the spreadsheet as below:

- Postgres user:

  `ORCA tab – crunchydb:password`

- Measure Processor user:

  `ORCA tab – crunchydb:encodedMpuserPassword`

- Historical Reporting user:

  `MSTR tab – dbLogin:loginPW`

  `ORCA tab – crunchydb:encodedMstuserPassword`

Geo configuration synchronizes the passwords in the database. Therefore, if the implementation passwords do not match, the internal connection strings become invalid on DC2 after the Geo configuration.

Warning:

When you configure Geo, you can take a backup. Restoring this backup later onto the Geo Primary system interferes with the Geo Standby functionality. Therefore, if you are restoring a full backup or incremental backup on Geo Primary, reconfigure Geo Standby to sync with the restored Geo Primary system.

Procedure

1. To configure the primary data center, do the following:
   a. Log in to the Cluster Control Manager (CCM) console in the DC1 cluster as the cust user.
   b. To switch to the root user, enter `su`.
   c. To run the `Analytics Administration` script as root user, use the following command:

      `ccm release orca analytics`

   d. To select the **Geo/High Availability** option, enter the corresponding number.
   e. To select the **Geo Options** option, enter the corresponding number.
   f. To configure the primary cluster, select **Configure Primary Geo cluster** by entering the corresponding number.
   g. In the **Proceed to Primary Geo cluster config** field, enter `y`.
   h. Enter CCM **IP address** of the Geo Standby cluster.
   i. Enter the Username to login to ccm of the Geo Standby cluster(DC2).
   j. Enter the password to login to ccm of the Geo Standby cluster(DC2) and click enter.

Note:

The script will take few minutes to run, meanwhile it returns **IP address** and **PV name**, make a note of it.

You must use this IP address and PV name for configuring the standby data center.

2. Return to the previous page by entering `b`.
3. Quit the current page by entering `q`.
4. Return to the main menu by entering `m`.
5. Log in to the Cluster Control Manager (CCM) console in the DC2 cluster as the cust user.
6. To switch to the root user, enter `su`.
7. To disable firewall on DC2(Standby), do the following:
   a. Run **`cluster_ssh`**.

      It displays the available nodes on the system. For example;

      a. node164182.puneccq.avaya.com
      b. node164183.puneccq.avaya.com
      c. node164184.puneccq.avaya.com

   b. Run the firewall config command for each node and exit.

      Note:

      The IP Address argument is the same IP provided as output from Geo Primary config.

   c. For example; Select [1].

```
Last login: Tue May 31 21:10:27 2022 from 135.27.164.178
DeployType=Cluster Node
[ccmuser@node164182 ~]$ sudo firewall-cmd --permanent --direct --add-rule
ipv4 filter OUTPUT 0 -o eth0 -d IP_Address -j ACCEPT
[ccmuser@node164182 ~]$ sudo systemctl restart firewalld
[ccmuser@node164182 ~]$ exit
```

8. To configure the standby data center, do the following:
   a. Log in to the Cluster Control Manager (CCM) console in the DC2 cluster as the cust user.
   b. To switch to the root user, enter `su`.
   c. To run the `Analytics Administration` script as root user, use the following command:

      `ccm release orca analytics`

   d. To select the **Geo/High Availability** option, enter the corresponding number.
   e. To select the **Geo Options** option, enter the corresponding number.

f. To configure the standby cluster, select **Configure Standby Geo cluster** option by entering the corresponding number.

g. In the **Proceed to Standby Geo cluster config** field, enter `y`.

Entering `n` cancels the operation.

h. At the prompt for IP address, enter the IP address and at the prompt of PV name, enter PV name that you noted while configuring the primary data center.

Note:

The script will take few minutes to run.

9. Return to the previous page by entering `b`.
10. Quit the current page by entering `q`.
11. To return to the main menu, type `m` and press **Enter**.

Note:

Once the above steps are completed successfully the Analytics database and MicroStrategy database will start to sync.

The MSTR will not be accessible for standby data center.

Configuring Avaya Analytics™ 4.x server details for real-time reporting

About this task

Avaya Analytics™ provides producers and measures to Avaya Workspaces for use in real-time reporting dashboards. Using Avaya Workspaces, users can view real-time reporting dashboards to monitor up-to-date statistics for your contact center and resources.

You configure the Avaya Analytics™ 4.x server details in Avaya Control Manager so that Avaya Workspaces can receive data from Avaya Analytics™.

Important:

Use this procedure only if your solution uses Avaya Analytics™ 4.x.

Procedure

1. Log on to the Avaya Control Manager interface with administrator credentials.
2. On the Avaya Control Manager web page, click **Configuration** > **Customer Engagement** > **Avaya Analytics™**.
3. On the **Avaya Analytics Server List** page, click **Add**.
4. In the **Alias** field, type an alias name for the Avaya Analytics™ 4.x server.
5. In the **API URL** field, type the URL that the Avaya Analytics™ 4.x server communicates with. For example, type `https://<AvayaOceanaCluster1_FQDN>/services/UCAStoreService/uca`.

Important:

- This URL must match the **API URL** configured on the Avaya Oceana® server. Verify that by navigating to **Configuration** > **Avaya Oceana** > **Server Details**.

Important:

- If the Avaya Oceana® and Avaya Analytics™ server use the same UCA server (Common setup), the **API URL** configured on both must match, including using matching address formats. For example, you must not use an IP address on one and FQDN on the other.

6. From the **Version** field, select the appropriate version for your release of Avaya Oceana®.
7. Select the **Enable Authorization** option.
8. Click **Save**.
9. On the Avaya Control Manager web page, click **Configuration** > **Locations**.
10. On the Location List page, select the location where you want to add the Avaya Analytics™ server.
11. Click **Edit**, or double-click the location.
12. On the Location Edit page, select the **Systems** tab.
13. Click the **+** sign.
14. In the **System Type** field, select **Avaya Analytics**.

    The **System Name** field populates the name of the newly created Avaya Analytics™ server.
15. Click **Save**.
16. Click **Confirm** on the Warning message dialog box.
17. On the Avaya Control Manager web page, click **Configuration** > **Customer Engagement** > **Avaya Analytics™**.
18. Select the check box for the Avaya Analytics™ 4.x server and click **Edit**.
19. Select the **Stream Servers** tab.
20. On the **Avaya Analytics Stream Server Add** page, click **Add**.
21. In the **Name** field, type a name for the Avaya Analytics™ 4.x server.
22. In the **FQDN** field, type the FQDN of the Avaya Analytics™ 4.x server. This is the cluster FQDN configured during deployment.
23. In the **Port** field, type `443/orca-streams-rest`.
24. Select the **TLS Flag** check box.
25. Click **Save**.

Disaster Recovery Process Checklist

On a solution that has been prepared for disaster recovery (see Disaster Recovery Configuration Checklist on page 75), the following processes can be used for disaster recovery.

No.	Task	Description	✔
1.	Switch over from primary to secondary data center	See Switching over from the primary to the secondary data center on page 80.	
2.	Resolve the cause of the primary data center failure. Then apply the following processes to return it to being the primary.		
3.	Reverse replication direction after switching from primary to secondary role	See Reversing data replication when the DC2 is the primary on page 81.	
4.	Switch back from the secondary data center to the primary.	Use the same process as previous used for switching but with the data centers reversed. See Switching over from the primary to the secondary data center on page 80.	

Related links

Switching over from the primary to the secondary data center on page 80
Reversing data replication when the DC2 is the primary on page 81

Switching over from the primary to the secondary data center

About this task

Use this procedure to promote the secondary DC2 to the primary role after a DC1 failure.

Note:

- If testing, you must only perform this process during a maintenance window.
- The entire data center must fail over in this case. For example, it is not supported to run Avaya Oceana® on DC1 against Avaya Analytics™ on DC2.

Before you begin

- Check that the secondary DC2 data center is in standby mode.

Procedure

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

   `ccm release orca analytics`
4. Select **Geo/High Availability** by pressing the corresponding number.
5. Select **Geo options** by pressing the corresponding number.

6. Select **Switch over: Promote secondary data center database to primary** by pressing the corresponding number.
7. In the **Proceed to Geo switchover** field, enter `y`. Entering `n` cancels the operation.
8. In the **Continuing will switch over this data center to Primary data center** field, enter `y`.
9. Return to the previous page by entering `b`.
10. Quit the current page by entering `q`.
11. Return to the main menu by entering `m`.
12. Restart the following services using post install scripts, do the following:
    a. Run `Analytics Administration` script, use the following command:

       `ccm release orca analytics`.
    b. Select **Troubleshooting** > **General** > **Restart Measure Processors** and wait until all the measure processors are up.
    c. Restart orca-scheduler and orca-admin-data-service.
    d. Restart pod orca-database-rest.
13. Return to the previous page by entering `b`.
14. Quit the current page by entering `q`.
15. Return to the main menu by entering `m`.

Next steps

- Once the cause of the DC1 failure has been resolved and fixed, you can switch back from DC2 as the primary to DC1. To start that process, DC1 first needs to receive data replication from DC2. See Reversing data replication when the DC2 is the primary on page 81.

Related links

Disaster Recovery Process Checklist on page 80

Reversing data replication when the DC2 is the primary

About this task

Once the cause of the DC1 failure has been resolved and fixed, you can switch back from DC2 as the primary to DC1. However, before doing that, DC1 first needs to receive data replication from DC2.

Note:

- If testing, you must only perform this process during a maintenance window.

Procedure

1. On the DC2, do the following on the Cluster Control Manager (CCM) console:
   a. Run the `Analytics Administration` script as root user, use the following command:

`ccm release orca analytics`

b. Select **Geo/High Availability** by pressing the corresponding number.

c. Select **Geo options** by pressing the corresponding number.

d. Select **Configure Primary Geo cluster** by pressing the corresponding number.

e. Make a note of the **IP address** and **PV name** that you receive at the end of this process. You need these values later in this process. The script takes a few minutes to run.

2. On the DC1 to make it a standby, do the following on the Cluster Control Manager (CCM) console:

a. Log in to the Cluster Control Manager (CCM) console of the DC1 cluster as the cust user.

b. Switch to the root user by entering `su`.

c. Run **`cluster_ssh`**. This displays the available nodes, for example:

a. `node164182.puneccq.avaya.com`

b. `node164183.puneccq.avaya.com`

c. `node164184.puneccq.avaya.com`

d. Run the firewall config command for each node and exit. For example; Select [1].

Note:

The IP Address argument is the same IP address output from the Geo Primary config.

```
Last login: Tue May 31 21:10:27 2022 from 135.27.164.178
DeployType=Cluster Node
[ccmuser@node164182 ~]$ sudo firewall-cmd --permanent --direct --add-rule
ipv4 filter OUTPUT 0 -o eth0 -d IP_Address -j ACCEPT
[ccmuser@node164182 ~]$ sudo systemctl restart firewalld
[ccmuser@node164182 ~]$ exit
```

3. Quit the current page by entering `q`.
4. To run the `Analytics Administration` script as root user, use the following command:
5. Select **Geo/High Availability** by pressing the corresponding number.
6. Select **Geo options** by pressing the corresponding number.
7. Select **Configure Standby Geo cluster** by pressing the corresponding number.
8. In the **Proceed to Standby Geo cluster config** field, enter `y`.
9. At the prompt for IP address, enter the IP address and PV names that you noted from the secondary data center.

Note:

The script will take few minutes to run.

10. Return to the previous page by entering `b`.
11. Quit the current page by entering `q`.
12. Return to the main menu by entering `m`.

Note:

- Once the above steps are completed successfully, the Analytics database and MicroStrategy database will start to sync.
- The MSTR will not be accessible for the standby data center.

Next steps

- At this stage, DC2 is still the primary but now with data being replicated to DC1. To return the DC1 to the primary role, repeat the switch over process (Switching over from the primary to the secondary data center on page 80) but with the data centers reversed. That is, promote DC1 to be the primary and configure DC2 to be the Standby Geo for DC1.

Related links

Disaster Recovery Process Checklist on page 80
Switching over Avaya Analytics from DC1 to DC2 on page 108
Switching over Avaya Analytics from DC1 to DC2 on page 128

Chapter 5: Planned Partial and Full Switchovers

Planned switchover from DC1 to DC2

This chapter provides information and instructions to take DC1 out of production and into a shutdown or standby mode to perform a switchover to DC2.

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

- Planned full switchover of all Disaster Recovery (DR) components of the solution - All components with a DR capability undergo a switchover.
- Planned partial switchover of Avaya Oceana® (Avaya Breeze® platform nodes and Omnichannel Database) - Customers do not have to switchover any of the following surrounding applications 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.

Planned full or partial switchover

You can perform a planned full or partial switchover even when there are no failures in any part of the solution. You can perform this activity in the following scenarios:

- To test the DR configuration and capabilities in the event of unexpected partial or full failures. Preventive testing enables failover and maintenance timeframes to be recorded based on individual customer configurations.
- Partial switchovers may be required to perform software and patch upgrades. Testing the DR capabilities of the Avaya Oceana® and Avaya Analytics™ components, supports the planning of scheduled maintenance times required to perform these activities.

Advantages of performing a planned switchover

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

There are several advantages of performing a planned switchover of Avaya Oceana® and Avaya Analytics™ DR solution:

- Existing contacts can be processed in a controlled manner.

- New contacts cannot enter into the system queue after the switchover procedures start.
- Logged-in agents can access the currently queued contacts.
- Active contacts can be cleared before the shutdown or failover in both primary and failover scenarios.
- Supervisor users logged in using Avaya Workspaces can view real-time reports and displays to ensure a graceful shutdown of all existing contacts.

Partial and Full Switchover - Preparation and Validation

Checklist for full or partial controlled switchover

The following is a checklist of lists the preparation and validation steps before you perform a full or partial controlled switchover:

Note:

The following preparation and validation steps are mandatory for full and partial controlled switchovers.

No.	Task	Description	✔
1	Prepare for switchover: Before starting any switchover operations on a production Avaya Oceana® and Avaya Analytics™ DR system, you must refer to several key documents.	See the following documents: • Administering Avaya Aura® System Manager • Installing Avaya Control Manager • Administering Avaya Aura® Communication Manager • Administering Avaya Aura® Application Enablement Services	
2	Plan and agree on maintenance window times and durations.	See Planned maintenance windows time and duration on page 88.	

Table continues…

No.	Task	Description	✔
3	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	See Validate identical software levels on page 88.	
4	Validate Avaya Oceana® solution replication before switchover.	See Validate Avaya Oceana components replication on page 88.	
5	Validate Avaya Aura® System Manager primary to DR replication status and health status from DC1 to DC2 is fully operational.	Validate the System Manager primary to DR replication status on page 89.	
6	Validate Avaya Aura® System Manager and Avaya Breeze® platform replication status to all Avaya Breeze® platform nodes in DC1 and DC2.	See Validate the System Manager and Avaya Breeze platform replication status on page 90.	
7	Validate the Avaya Control Manager database HA deployment	See Validating the Avaya Control Manager database HA deployment on page 90.	
8	Verify the Context Store replication status from DC1 to DC2.	See Verify the Context Store replication status on page 90.	
9	Verify the Omnichannel database mirroring status from DC1 to DC2.	See Verifying the Omnichannel database mirroring status on page 91.	
10	Verify Avaya Aura® Communication Manager to ESS data replications.	See Verifying Avaya Aura Communication Manager to ESS data replications on page 91.	
11	Verify the Avaya Analytics™ DB Replication from DC1 to DC2.	See Verifying the Avaya Analytics DB replication from DC1 to DC2 on page 91.	
12	Validate snap-in shutdown or deployment status in the DR site.	See Validate Avaya Oceana snap-in shutdown or deployment status in DC1 and DC2 on page 92.	

Table continues…

No.	Task	Description	✔
13	Verify UCA replication status from DC1 to DC2.	See Verifying the UCA replication status on page 92.	
14	Verify the deployment status of EmailService in DC2.	See Verifying the deployment status of EmailService in DC2 on page 93.	
15	Verify the shutdown status of CustomerControllerService in DC2.	See Verifying the shutdown status of CustomerControllerService in DC2 on page 94.	
16	Verify the shutdown status of MessagingService in DC2.	See Verifying the shutdown status of MessagingService in DC2 on page 94.	
17	Verify the shutdown status of GenericChannelAPI in DC2.	See Verifying the shutdown status of GenericChannelAPI in DC2 on page 95.	
18	Verify the deployment status of the AMC snap-in for Avaya WebRTC Connect.	See Verifying the deployment status of the AMC snap-in for Avaya WebRTC Connect on page 95.	
19	Verify the CSC deployment status in DC1 and DC2.	See the following: • Verifying the CSC deployment status in DC1 on page 96 • Verifying the CSC deployment status in DC2 on page 96 .	
20	Launch Oceana Monitor for DC1 and DC2 locations and verify there are no un-deployed PUs across all Oceana clusters.	See the following: • Launch Oceana Monitor for DC1 and DC2 locations and verify PUs on page 96 • Viewing Oceana Monitor Service pages on page 97 • Oceana Services Overview page on page 97 • Monitor Service page on page 97	

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 some time. Times for switchover and switchback vary depending on whether a partial or full DR switchover or switchback is implemented.

Validate identical software levels

The software versions and levels on primary and DR sites must be identical for planned switchover and switchback testing.

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
  - Snap-in versions on primary and DR must be identical before starting a switchover.

There may be different software versions during the upgrade process for software upgrade maintenance windows. Ensure that DC1 and DC2 applications are at the same software release version before you re-enable solution replication from each application in DC1 to DC2. The software versions of the applications in DC1 and DC2 must be the same for replication to work between the two applications.

Create a table to record the software versions of each application for primary and DR sites. This step is unnecessary for unplanned maintenance windows due to application failures.

Validate Avaya Oceana® components replication

Before any planned switchover from a primary to a Disaster Recovery (DR) site, you must verify that the health status of the applications replicating 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:

- Unified Collaboration Administration (UCA)
- System Manager and Avaya Breeze® platform replication
- Avaya Context Store Snap-in (CS)
- Omnichannel database using CACHE mirroring

The following surrounding applications in 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:

Validate the replicating function of all these replicating applications before a partial DR switchover. If you do not validate, it leads to issues during the switchback process.

Validate the System Manager primary to DR replication status

About this task

For any planned partial DR switchover and switchback, you must verify the health status 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, in the **Application State** widget, verify the following states:
   - GR Server Role is `PRIMARY`
   - GR Server Mode is `ACTIVE`
   - GR Replication is `ENABLED`
2. Click **Services** > **Geographic Redundancy** > **GR Health**.

   Verify the following elements are in a Successful state and in green:
   - Database Replication
   - File Replication
   - Directory Replication

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

Validate the System Manager and Avaya Breeze® platform replication status

About this task

For a planned switchover and switchback testing, you must check replication between System Manager and Avaya Breeze® platform components.

Procedure

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

   System Manager displays the word **Synchronized** in green.
3. Click **Avaya Breeze replica group**.
4. Check if the **Breeze Node Synchronization** status is in the **Synchronized** state and that 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**, 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 the Avaya Control Manager database HA deployment

For all switchovers, you must verify that the Avaya Control Manager database HA feature is operational before proceeding with the switchover.

Note:

Avaya Control Manager offers many multiplex high-availability configuration features. The configurations include load balancing and database-enabled features. For more information on multiplex high availability configuration features, see Multiplex high availability configuration.

Verify the 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.

Optionally, you must also create a context to verify that the 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`, 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 that can be used for all context operations, such as creating and retrieving contexts from Context Store. You can download the Postman collection from **Products** > **Avaya Oceana Solution** > **Context Store Snapin** > **Select Release** > **Downloads** at www.devconnectprogram.com.
7. Verify that the context is present in DC1 Context Store and in DC2 Context Store.

Verifying the Omnichannel database mirroring status

About this task

To verify that data from the primary Omnichannel database is mirrored to the DR site, you must use the Oceana Data Management (ODM) tool to check the mirroring status.

Use this procedure to verify the database mirroring status using the ODM tool.

Procedure

1. Connect to the primary Omnichannel database server.
2. Launch the Oceana Data Management (ODM) tool.
3. Log in as an administrator.
4. Navigate to **Configuration** > **Mirror Settings**.

   The Mirror Status window shows the current mirroring status for all mirror members, including the primary Omnichannel database and the DR Omnichannel database.

Verifying Avaya Aura® Communication Manager to ESS data replications

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. Run a save translation command, login to the ESS server, and verify if the change is available on the ESS system.

For more information on administration configurations on Avaya Aura® Communication Manager, see the *Avaya Communication Manager Administrator* document.

Verifying the Avaya Analytics DB replication from DC1 to DC2

About this task

Use this procedure to verify the replication status 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. Switch to being the root user by entering the command `su`.
3. To run the `Analytics Administration` script, use the following command:

   `ccm release orca analytics`
4. Select **Troubleshooting** by pressing the corresponding number.
5. Select **Database** by pressing the corresponding number.
6. To check the status of Crunchy pod replication, enter the corresponding number.

   Verify that the output shows a successful connection to the remote cluster and there are no warnings about a time lag in replication.

Validate Avaya Oceana® snap-in shutdown or deployment status in DC1 and DC2

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 where 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. Validating the attribute values also requires an additional restart of the Avaya Oceana® clusters to complete the switchover.

Verifying the UCA replication status

About this task

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

When you make an administrative change using the primary Avaya Control Manager, the changes are replicated from the primary UCA to the DR UCA.

Important:

Ensure that there are no active UCA alarms. If there are any active UCA alarms, resolve them before the switchover.

Procedure

1. Log on to the System Manager.
2. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration** > **Primary Cluster**.
3. In the **Cluster** field, select **Oceana Monitor**.
4. To view the PU status of all the snap-ins, select **Cluster 1** > **Grid Info**.
5. Verify if the PU status of **ucaStoreSpace-GATEWAY** is `INTACT`.

   If the status is `Scheduled` or `Broken`, UCA replication is not operational.

You must correct the issue before proceeding with the switchover.

6. On the primary site, in the **Show Cluster Messages** tab, select the **UCAStoreService** PU.
7. Verify that the `HEARTBEAT` message for the replication channel state is `ACTIVE`.
8. Repeat steps 1 to 6 for Avaya Oceana® Cluster 1 in Data Center 2.

   Note:

   On the **Cluster Messages** tab, in **UCAStoreService** messages, check the time of the last cluster DB updated message on all nodes on the Primary and the DR site.

   Important:

   Perform the subsequent steps after successfully completing steps 1 to 6.
9. Log on to the Avaya Control Manager on DC1.
10. 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®*.

    Note:

    If the test attribute does not appear, UCA replication is not operational from primary to DR or the request to save a new attribute to the primary UCA server is not successful. Ensure that you correct these issues before proceeding with the switchover.
11. Reload the cluster message, select **UCAStoreService**, and check the new time of the cluster DB updated message.

    The time of the updated message must coincide with the newly added attribute.

Verifying the deployment status of EmailService in DC2

About this task

The EmailService snap-in handles email contacts within the Avaya Oceana® solution.

Before the switchover to the DR site, use this procedure to ensure that the deployment status attribute in the DR site for the EmailService snap-in is set as `false`.

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

Procedure

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

4. In the **Deployment status of emailmanager** attribute, verify if the value is set to `false`.

   If this field is set to `true`, set it to `false` and commit the change.

   If you change this value to `true`, there is no need to reboot Avaya Oceana® Cluster 3.

Verifying the shutdown status of CustomerControllerService in DC2

About this task

The CustomerControllerService snap-in handles chat contacts within the Avaya Oceana® solution.

Before the switchover to the DR site, use this procedure to ensure that the shutdown mode status attribute in the DR site for the CustomerControllerService snap-in is set as `true`.

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

Procedure

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

   If you change this value to `true`, there is no need to reboot Avaya Oceana® Cluster 3.

Verifying the shutdown status of MessagingService in DC2

About this task

The MessagingService snap-in handles Avaya Oceana® channel snap-ins like the SMS, Social, or Async channels.

Before the switchover to the DR site, use this procedure to ensure that the shutdown mode status attribute in the DR site for the MessagingService snap-in is set as `true`.

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

Procedure

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

4. In the **Shutdown Mode** attribute field, verify if the value is set to `true`.

   If you change this value to `true`, there is no need to reboot Avaya Oceana® Cluster 3.

Verifying the shutdown status of GenericChannelAPI in DC2

About this task

The GenericChannelAPIService snap-in injects generic contacts into Avaya Oceana®.

Before the switchover to the DR site, use this procedure to ensure that the shutdown mode status attribute in the DR site for this snap-in is set 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. Log on to System Manager.
2. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
3. On the Service Clusters tab, do the following:
   a. **Cluster**: Select DR Avaya Oceana® Cluster 3.
   b. **Service**: Select **GenericChannelAPIService**.
4. In the **Shutdown Mode** attribute field, verify if the value is set to `true`.

   If you change this value to `true`, there is no need to reboot Avaya Oceana® Cluster 3.

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

About this task

The Avaya Mobile Communications (AMC) snap-in enables WebRTC Connect voice and video contacts to enter Avaya Oceana®.

Before the switchover to the DR site, use this procedure to verify that the deployment status of the AMC snap-in Processing Unit (PU) is active and operational.

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

Procedure

1. Log on to System Manager.
2. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration** > **DR Cluster 1**.
3. In the **Cluster** field, select **Oceana Monitor**.
4. To view the PU status of all the snap-ins, select **Cluster 2** > **Grid Info**.
5. Verify that the PU status is `Intact`.

If the status is `Scheduled` or `Broken`, the AMC snap-in is not operational. You must resolve the issue before proceeding with the switchover. Otherwise, when the switchover is complete, WebRTC Connect voice or video contacts will not be routed in Avaya Oceana®.

6. Click **Show Cluster Messages** and click the AMC snap-in.
7. Verify that there are no alarms or errors.

Verifying the CSC deployment status in DC1

About this task

Use this procedure to verify the deployment status for the CallServerConnector (CSC) PU on DC1.

Procedure

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

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

2. On the Monitor Service page, click **Cluster 1** > **Show cluster Messages**.

   The page displays all the PUs in Cluster 1.

3. From the **Filters** column, select the **CallServerConnector** PU.
4. Verify that the `HEARTBEAT` message for the **CallServerConnector** PU is `INTACT`.

Verifying the CSC deployment status in DC2

About this task

Use this procedure to verify the deployment status for the CallServerConnector (CSC) PU on DC2.

Procedure

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

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

2. On the Monitor Service page, click **Cluster 1** > **Show cluster Messages**.

   The page displays all the PUs in Cluster 1 (DR site).

3. From the **Filters** column, select the **CallServerConnector** PU.
4. Verify that the `HEARTBEAT` message for the **CallServerConnector** PU is `ACTIVE`.

Launch Oceana Monitor for DC1 and DC2 locations and verify PUs

Launch Oceana Monitor for DC1 and DC2 locations and verify there are no un-deployed PU's across all Oceana clusters.

Viewing Oceana Monitor Service pages

Procedure

1. To view the Oceana Services Overview page, enter the following URL in your web browser:

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

2. To view the Monitor Service page, enter the following URL in your web browser:

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

   On the Monitor Service page, click the cluster node to view the information about the cluster.

Oceana Services Overview page

The Oceana Services Overview page provides the following information about each snap-in of Avaya Oceana®:

- Name of the snap-in.
- Symbol specifying whether Oceana Monitor Service has detected the snap-in:
  - ✔ indicates that Oceana Monitor Service has detected the snap-in.
  - ✖ indicates that Oceana Monitor Service has not detected the snap-in.
- Version of the snap-in.
- Name of the cluster where the snap-in is installed.
- Latest Heartbeat message of the snap-in.

  The Heartbeat message includes the node reporting the Heartbeat, the status level of the Heartbeat (OK, WARN, ERROR), and the time since the last update. The Heartbeat background indicates the status of the Heartbeat.

Monitor Service page

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

- Name of the cluster.
- IP address of the cluster.
- Number of nodes in the cluster.
- IP address of each node of the cluster.
- Cluster view of the snap-ins installed.
- View of snap-in lifecycle messages.

Monitor Service page field descriptions

When you click the cluster node, the Monitor Service page displays the following buttons:

Button name	Description
Show Node Details	Displays information about the nodes of the cluster.
Show Grid Info	Displays the following information about the processing units of the cluster: • Name of the processing unit • Embedded space of the processing unit • Number of instances • Type of the processing unit • Status of the processing unit
Show Cluster Messages	Displays the service messages for all the snap-ins installed on the cluster.
Show Service Details	Displays the following information about each of the snap-ins installed on the cluster: • Name of the snap-in • Version of the snap-in • Service messages of the snap-in

Partial controlled switchover

Checklist for partial controlled switchover

The following is a checklist of steps to perform a partial controlled switchover.

No.	Task	Description	✔
1	Configure the primary site voice channel shutdown.	See Configuring the primary site voice channel shutdown on page 99.	
2	Configure the primary site email channel shutdown.	See Configuring the primary site EmailService shutdown on page 100.	
3	Configure the primary site chat channel shutdown.	See Configure the primary site chat shutdown on page 100.	
4	Configure the primary site messaging channel shutdown.	See Configuring the primary site MessagingService shutdown on page 101.	
5	Configure the primary site generic channel shutdown.	See Configuring the primary site GenericChannelAPI service shutdown on page 101.	

Table continues…

No.	Task	Description	✔
6	Take a backup of the UCMService deferred email data.	See Backing up the UCMService database during planned switchover and switchback on page 102.	
7	Set the maintenance mode for front-end web voice and web video.	See Setting the maintenance mode for front end web voice and web video on page 104.	
8	Stop running campaigns on the primary site POM server and switch to the DR site Oceana and POM system.	See Oceana POM switchover on page 104.	
9	Validate contacts in DC1.	See Validating contacts on page 104.	
10	Log out supervisors and agents from DC1.	See Logging out supervisors and agents on page 105.	
11	Change the cluster activity status for clusters in DC1.	See Changing the Cluster Activity status for the clusters in Data Center 1 on page 105.	
12	Switch over the Omnichannel database server in the primary site (DC1) to the Omnichannel database server in the DR site (DC2).	See the following: • Omnichannel database switchover on page 106. • Promoting Omnichannel server in DC2 on page 106. • Pointing ACM to the new Omnichannel database server in DC2 on page 107.	
13	Switch over Avaya Analytics™ from DC1 to DC2.	See the following: • Switching over Avaya Analytics from DC1 to DC2 on page 108. • Reversing data replication when the DC2 is the primary on page 81.	

Configuring the primary site voice channel shutdown

About this task

Use this procedure to set incoming voice calls to an Avaya Oceana® DR system from the front-end application running on Avaya Experience Portal.

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

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 appropriate application and click **Configurable Application Variables**.

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

Configuring the primary site EmailService shutdown

About this task

Use this procedure to set the primary site EmailService on Avaya Oceana® Cluster 3 to false.

If the email 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 primary site Service Clusters tab, do the following:
   a. **Cluster**: Select primary Avaya Oceana® Cluster 3.
   b. **Service**: Select **EmailService**.
3. In the **Deployment status of emailmanager** 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**.

Configure the primary site chat shutdown

About this task

Use this procedure to set the primary site CustomerControllerService on Avaya Oceana® Cluster 3 to true.

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

Note:

You must configure the customer-deployed chat front-end application to point to the Oceana DR system. The deployment instructions are beyond the scope of this guide, as each deployment utilizes different methods to integrate into the Oceana back-end systems. For more information on the various disaster recovery configurations, see *Disaster Recovery Configuration* chapter in *Avaya Oceana® and Avaya Analytics™ Disaster Recovery* document.

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 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 `false` to `true`.
4. Click **Commit**.

Configuring the primary site MessagingService shutdown

About this task

Use this procedure to set the primary site MessagingService on Avaya Oceana® Cluster 3 to true.

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

Note:

You must configure the customer-deployed SMS, Social, or Async front-end applications to point to the Oceana DR system. The deployment instructions are beyond the scope of this guide, as each deployment utilizes different methods to integrate into the Oceana back-end systems. For more information on the various disaster recovery configurations, see *Disaster Recovery Configuration* chapter in *Avaya Oceana® and Avaya Analytics™ Disaster Recovery* document.

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 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 `false` to `true`.
4. Click **Commit**.

Configuring the primary site GenericChannelAPI service shutdown

About this task

Use this procedure to set the primary site GenericChannelAPI service on Avaya Oceana® Cluster 3 to true.

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 primary site Service Clusters tab, do the following:
   a. **Cluster**: Select primary 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 `false` to `true`.
4. Click **Commit**.

Note:

You must configure the customer-deployed generic channel front-end application to point to the Oceana DR system. The instructions to complete the task are beyond the scope of this guide as each generic channel deployment can utilize different methods to integrate to the Oceana back-end systems.

UCMService Backup and Restore Procedures

Backing up the UCMService database during planned switchover and switchback

About this task

UCMService stores the metadata related to deferred emails. UCMService requires this data to retrieve expired deferred emails and route them back to the appropriate agent. The information is updated in real-time.

You must take backups during the following events:

- Planned switchover and recovery
- Unplanned switchover and recovery

Note:

You can skip the procedure 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 do not keep new UCM data post switch back to the primary site.
- You are not restoring the UCM DB from the DR site.

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 **Backup and Restore**, 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 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 Avaya Oceana® Cluster 1.
11. From **Backup and Restore**, select **Backup**.

    System Manager displays the Cluster DB Backup page.
12. On the **Cluster Database Backup** confirmation dialog box, select the **UCMService** check box, and click **Continue**.
13. In **Backup Password**, enter a password for the backup.

    Important:

    Note the password entered. You will require this password to restore the UCMService.
14. In **Schedule Job**, click **Run immediately**.
15. Click **Backup**.
16. After the backup process is complete, verify the **Status** column on the **Backup and Restore Status** page. The status must display `Completed`.

Restoring the UCMService data for Avaya Oceana® Cluster 1 in Data Center 2

About this task

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

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®** > **Cluster Administration**.
2. From **Backup and Restore**, select **Restore**.
3. 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**.
4. On the Cluster Database Restore Confirmation dialog box, select Avaya Oceana® Cluster 1 and click **Continue**.
5. On the Backup and Restore Status page, ensure that the **Status** column for the restore operation displays the value `Completed`.
6. Install UCMService on Avaya Oceana® Cluster 1.
7. Reboot Avaya Oceana® Cluster 1 and then Avaya Oceana® Cluster 3.

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 to the DR site Oceana and POM system.

For more information about switching over and restarting Proactive Outreach Manager, see *Implementing Avaya Proactive Outreach Manager*.

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. Supervisors must then logout.

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

Before you begin

Ensure OceanaMonitorService is 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**.

      The cluster status changes to `STANDBY` and all nodes are placed in the Deny New Service mode.
   c. Click **OK** on the confirmation message box.
   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.

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.

OCP DB switchover with Campus HA 2+1

Removing cache mirroring from Campus Standby

About this task

Use this procedure to remove cache mirroring from Campus Standby.

Procedure

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

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

   <IP> is the IP address of the standby Omnichannel server in Data Center 1.
2. On the Cache Management Portal login page, do the following:
   a. In 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 Mirror** > **Remove Mirror Configuration**.
4. To remove the mirrored attribute, click **Yes** and then click **Remove**.

Switching over DR server

Promoting Omnichannel server in DC2

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 is available, and mirroring is operational for planned maintenance windows. You can use this procedure irrespective of whether a dual server pair is deployed on the primary site.

Procedure

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 Avaya Control Manager (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 Pointing ACM to the new Omnichannel database server in DC2 on page 107.

Demoting primary to async

About this task

Use this procedure to demote the primary server to async.

Procedure

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

1. Navigate to **CCDINSTANCE** and click **Start Caché**.
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 node** > **Backup And Restore**.
6. Click **Mirror Configuration**.
7. In the **Select Mirror Scenario** field, select **Demote** to **Async**.
8. Click **Execute**.

Pointing ACM to the new Omnichannel database server in DC2

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, host name, or IP address of the Omnichannel Database DR 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.

   For more information on configuring the Omnichannel certificate, refer to the *Retrieve certificate files* section in the *Deploying Avaya Oceana®* document.

Switching over Avaya Analytics™ from DC1 to DC2

About this task

Using the following steps you can promote DC2 to primary role after a fail over. DC1 does not synchronize data after this operation until a rebuild from DC2 is available.

Note:

You must perform this switch over only during a maintenance window.

Before you begin

Ensure that the secondary data center is on standby mode.

Procedure

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

   `ccm release orca analytics`
4. To select the **Geo/High Availability** option, enter the corresponding number.
5. To select the **Geo options** option, enter the corresponding number.
6. To select the **Switch over: Promote secondary data center database to primary** option, enter the corresponding number.

   Warning:

   You must use this option only on the secondary data center.
7. In the **Proceed to Geo switchover**, enter `y`.

   Entering `n` cancels the operation.
8. In the **Continuing will switch over this data center to Primary data center** field, type `y` and press **Enter**.

This operation is successful only when a server is available on standby mode.

9. Return to the previous page by entering `b`.
10. Quit the current page by entering `q`.
11. Return to the main menu by entering `m`.

Related links

Reversing data replication when the DC2 is the primary on page 81

Reversing data replication when the DC2 is the primary

About this task

Once the cause of the DC1 failure has been resolved and fixed, you can switch back from DC2 as the primary to DC1. However, before doing that, DC1 first needs to receive data replication from DC2.

Note:

- If testing, you must only perform this process during a maintenance window.

Procedure

1. On the DC2, do the following on the Cluster Control Manager (CCM) console:
   a. Run the `Analytics Administration` script as root user, use the following command:

      `ccm release orca analytics`

   b. Select **Geo/High Availability** by pressing the corresponding number.
   c. Select **Geo options** by pressing the corresponding number.
   d. Select **Configure Primary Geo cluster** by pressing the corresponding number.
   e. Make a note of the **IP address** and **PV name** that you receive at the end of this process. You need these values later in this process. The script takes a few minutes to run.
2. On the DC1 to make it a standby, do the following on the Cluster Control Manager (CCM) console:
   a. Log in to the Cluster Control Manager (CCM) console of the DC1 cluster as the cust user.
   b. Switch to the root user by entering `su`.
   c. Run **`cluster_ssh`**. This displays the available nodes, for example:
      a. `node164182.puneccq.avaya.com`
      b. `node164183.puneccq.avaya.com`
      c. `node164184.puneccq.avaya.com`
   d. Run the firewall config command for each node and exit. For example; Select [1].

Note:

The IP Address argument is the same IP address output from the Geo Primary config.

```
Last login: Tue May 31 21:10:27 2022 from 135.27.164.178
DeployType=Cluster Node
[ccmuser@node164182 ~]$ sudo firewall-cmd --permanent --direct --add-rule
ipv4 filter OUTPUT 0 -o eth0 -d IP_Address -j ACCEPT
[ccmuser@node164182 ~]$ sudo systemctl restart firewalld
[ccmuser@node164182 ~]$ exit
```

3. Quit the current page by entering `q`.
4. To run the `Analytics Administration` script as root user, use the following command:
5. Select **Geo/High Availability** by pressing the corresponding number.
6. Select **Geo options** by pressing the corresponding number.
7. Select **Configure Standby Geo cluster** by pressing the corresponding number.
8. In the **Proceed to Standby Geo cluster config** field, enter `y`.
9. At the prompt for IP address, enter the IP address and PV names that you noted from the secondary data center.

   Note:

   The script will take few minutes to run.
10. Return to the previous page by entering `b`.
11. Quit the current page by entering `q`.
12. Return to the main menu by entering `m`.

    Note:

    - Once the above steps are completed successfully, the Analytics database and MicroStrategy database will start to sync.
    - The MSTR will not be accessible for the standby data center.

Next steps

- At this stage, DC2 is still the primary but now with data being replicated to DC1. To return the DC1 to the primary role, repeat the switch over process (Switching over from the primary to the secondary data center on page 80) but with the data centers reversed. That is, promote DC1 to be the primary and configure DC2 to be the Standby Geo for DC1.

Related links

Disaster Recovery Process Checklist on page 80
Switching over Avaya Analytics from DC1 to DC2 on page 108
Switching over Avaya Analytics from DC1 to DC2 on page 128

Full controlled switchover

Checklist for Full Controlled Switchover

The following checklist provides the list of steps to perform a Full Controlled Switchover.

No.	Task	Description	✔
1	Shut down and switchover to DR site voice channel.	See Shut down and switch back DR site voice channel to primary site on page 112.	
2	Switch over from Avaya Aura® Communication Manager to ESS in the DR site.	See Switchover from Avaya Aura Communication Manager to ESS in DR site on page 113.	
3	Configure the primary site voice channel shutdown.	See Configure the primary site voice channel shutdown on page 113.	
4	Switch over voice channels from DC1 to DC2.	See Switching over Voice Channels from Avaya Workspaces for Call Center Elite DC1 to Avaya Workspaces for Call Center Elite DC2 on page 114.	
5	Configure the primary site email shutdown.	See Configure the primary site email shutdown on page 117.	
6	Configure the primary site chat shutdown.	See Configure the primary site chat shutdown on page 117.	
7	Configure the primary site MessagingService shutdown.	See Configure the primary site MessagingService shutdown on page 118.	
8	Configure the primary site GenericChannelAPI service shutdown.	See Configure the primary site GenericChannelAPI service shutdown on page 118.	
9	Back up the UCMService database.	See Backing up the UCMService database during planned switchover and switchback on page 119	
10	Set the maintenance mode for front end web voice and web video.	See Setting the maintenance mode for front end web voice and web video on page 121.	
11	Switch over Oceana and POM system to the DR site.	See Oceana POM switchover on page 121.	
12	Validate contacts in DC1.	See Validating contacts on page 121.	
13	Log out supervisors and agents from DC1.	See Logging out supervisors and agents on page 121.	

Table continues…

No.	Task	Description	✔
14	Change the cluster activity status for clusters in DC1.	See Changing the Cluster Activity status for the clusters in Data Center 1 on page 105	
15	Switch over System Manager from DC1 to DC2 Geo System Manager.	See Switchover System Manager from DC1 to DC2 Geo System Manager on page 121.	
16	Verify Avaya Breeze® platform node controller for Data Center 2.	See Verifying Avaya Breeze platform node controller for Data Center 2 on page 125.	
17	Switch over the Omnichannel database server in the primary site DC1 to the Omnichannel database server in the DR site DC2.	See the following: • Omnichannel database switchover on page 125. • Promoting Omnichannel server in DC2 on page 126. • Pointing ACM to the new Omnichannel database server in DC2 on page 127.	
18	Switch over Avaya Analytics™ from DC1 to DC2.	See the following: • Switching over Avaya Analytics from DC1 to DC2 on page 128. • Reversing data replication when the DC2 is the primary on page 81.	
19	Switch over Avaya Control Manager from primary to DR site.	See Avaya Control Manager switchover from primary to DR site on page 130.	
20	Avaya Control Manager Toggle Button utility for switchover and switchback	Avaya Control Manager Toggle Button utility for switchover and switchback on page 131	
21	Reconfigure Avaya Control Manager in full and partial DR switchover scenarios.	See Overview on page 131.	
22	Configure the Web Voice and Web Video switchover.	See Configure the Web Voice and Web Video switchover on page 132.	

Shut down and switch back DR site voice channel 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**.

   When new incoming voice contacts come in through the Avaya Experience Portal application, they are routed to the Avaya Oceana® system in the primary location DC1.

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 phone sets 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.

Configure the primary site voice channel shutdown

About this task

Use this procedure to set incoming voice calls to an Avaya Oceana® DR system from the front-end application running on Avaya Experience Portal.

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

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 appropriate application and click **Configurable Application Variables**.
4. In the **Active Data Center** field, click **DataCenter2**.
5. Click **Save**.

Switching over Voice Channels from Avaya Workspaces for Call Center Elite DC1 to Avaya Workspaces for Call Center Elite DC2

Use the following procedure to test and verify the complete DR voice capabilities for Avaya Workspaces for Call Center Elite. This is a complete switchover scenario.

Pre-requisites:

1. Deploy and configure a Avaya Workspaces for Call Center Elite DR solution.
2. Add the settings described in this document to enable DR for voice.
3. Verify Avaya Workspaces for Call Center Elite voice channel in the regular primary active state.

No.	Task	Description	✔
1.	Verify Enterprise Survivable Server (ESS) is registered with Communication Manager	Verifying the status of Survivable Processor on page 36	
2.	Verify Computer Telephony Integration (CTI) link status	In the regular primary active state, there must be two active CTI links: • **Link 1** - Connecting the Communication Manager and the DC1 Application Enablement Services. • **Link 2** - Connecting the Communication Manager and the DC2 Application Enablement Services. When the Communication Manager is offline, the **Link 1** becomes inactive. The **Link 2** is active, but it is now between the ESS and the DC2 Application Enablement Services with the Survivable Hierarchy.	
3.	Verify the Call Server Connector (CSC) to Application Enablement Services connection	Verifying the Call Server Connector (CSC) to Application Enablement Services connection on page 116	
4.	Turn the DC1 Communication Manager and Application Enablement Services offline to make ESS active	Power off the Communication Manager or make it non-reachable so that the ESS becomes active.	

Table continues…

No.	Task	Description	✔
5.	Verify that the ESS is active	Verifying the status of Survivable Processor on page 36	
6.	Verify station login using the ESS IP address	When ESS is active, you must be able to log a station in using the ESS IP address. Station login details are the same on ESS as they are on Communication Manager because all the configuration data is copied from the Communication Manager to ESS, when you run the **`save translations`** command. Verifying a station login using Enterprise Survivable Server IP address on page 116	
7.	Verify CTI Link status	When the Communication Manager is offline, the CTI **Link 2** must be the only active link. Verifying the Computer Telephony Integration (CTI) Link status on page 116	
8.	Verify that the DC1 Application Enablement Services Khepri connectors are inactive	When the Communication Manager is offline, the **DMCC Service Summary** page on the DC1 Application Enablement Services must display that the two Khepri connectors are no longer active. Verifying that the DC1 Application Enablement Services Khepri connectors are inactive on page 116	
9.	Switch over Avaya Workspaces for Call Center Elite	The DC1 Avaya Workspaces for Call Center Elite working with the DC2 ESS, is not a supported DR scenario. Therefore, you must switch Avaya Workspaces for Call Center Elite over to the DC2 to test ESS functionality with Avaya Workspaces for Call Center Elite for voice channel.	
10.	Verify CTI Link status	Verify that the CTI **Link 2** is active, as in step 7 above. This is the connection between the ESS and DC2 Application Enablement Services.	
11.	Verify DC2 Application Enablement Services Khepri connectors are active	The solution is completely switched over and the two Khepri connectors between the DC2 Application Enablement Services and Avaya Workspaces for Call Center Elite are active. Verifying that the DC2 Application Enablement Services Khepri connectors are active on page 117	

Table continues…

No.	Task	Description	✔
12.	Log an agent configured to handle voice contacts into Avaya Workspaces.	Log the agent's station into a softphone using the ESS IP address. Then log the agent into Avaya Workspaces and make a call to the Avaya Workspaces for Call Center Elite Vector Directory Number (VDN). The agent must be able to login without any errors and the call must be presented to the logged in agent.	

Verifying the Call Server Connector (CSC) to Application Enablement Services connection

Procedure

1. Log on to the DC1 Application Enablement Services web admin portal.
2. Navigate to **Status** > **Status and Control** > **DMCC Service Summary**.

   There must be two Khepri Call Server Connector entries with two common cluster node SIPs as the **Far-end Identifier**s.

Verifying a station login using Enterprise Survivable Server IP address

Procedure

1. Open a softphone application.
2. Log in using the Enterprise Survivable Server (ESS) IP address for call server.

   You must be able to log in successfully.

Verifying the Computer Telephony Integration (CTI) Link status

Procedure

1. Log on to the Enterprise Survivable Server (ESS) System Access Terminal (SAT).
2. Run the command: **`status aesvcs cti-link`**
3. Verify that the **Service State** is `Established`.

Verifying that the DC1 Application Enablement Services Khepri connectors are inactive

Procedure

1. Log on to the DC1 Application Enablement Services web admin portal.
2. Navigate to **Status** > **Status and Control** > **DMCC Service Summary**.

   The Khepri Call Server Connector entries are not displayed.

Verifying that the DC2 Application Enablement Services Khepri connectors are active

Procedure

1. Log on to the DC2 Application Enablement Services web admin portal.
2. Navigate to **Status** > **Status and Control** > **DMCC Service Summary**.

   There must be two Khepri Call Server Connector entries with two DC2 common cluster node SIPs as the **Far-end Identifier**s.

Configure the primary site email shutdown

About this task

Use this procedure to set the primary site EmailService on Avaya Oceana® Cluster 3 to false.

If the email 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 primary site Service Clusters tab, do the following:
   a. **Cluster**: Select primary Avaya Oceana® Cluster 3.
   b. **Service**: Select **EmailService**.
3. In the **Deployment status of emailmanager** 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**.

Configure the primary site chat shutdown

About this task

Use this procedure to set the primary site CustomerControllerService on Avaya Oceana® Cluster 3 to true.

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

Note:

You must configure the customer-deployed chat front-end application to point to the Oceana DR system. The deployment instructions are beyond the scope of this guide, as each deployment utilizes different methods to integrate into the Oceana back-end systems. For more information on the various disaster recovery configurations, see Overview on page 17.

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 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 `false` to `true`.
4. Click **Commit**.

Configure the primary site MessagingService shutdown

About this task

Use this procedure to set the primary site MessagingService on Avaya Oceana® Cluster 3 to true.

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

Note:

You must configure the customer-deployed SMS, Social, or Async front-end applications to point to the Oceana DR system. The deployment instructions are beyond the scope of this guide, as each deployment utilizes different methods to integrate into the Oceana back-end systems. For more information on the various disaster recovery configurations, see Overview on page 17.

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 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 `false` to `true`.
4. Click **Commit**.

Configure the primary site GenericChannelAPI service shutdown

About this task

Use this procedure to set the primary site GenericChannelAPI service on Avaya Oceana® Cluster 3 to true.

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 primary site Service Clusters tab, do the following:
   a. **Cluster**: Select primary 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 `false` to `true`.
4. Click **Commit**.

Note:

You must configure the customer-deployed generic channel front-end application to point to the Oceana DR system. The instructions to complete the task are beyond the scope of this guide as each generic channel deployment can utilize different methods to integrate to the Oceana back-end systems.

UCMService Backup and Restore Procedures

Backing up the UCMService database during planned switchover and switchback

About this task

UCMService stores the metadata related to deferred emails. UCMService requires this data to retrieve expired deferred emails and route them back to the appropriate agent. The information is updated in real-time.

You must take backups during the following events:

- Planned switchover and recovery
- Unplanned switchover and recovery

Note:

You can skip the procedure 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 do not keep new UCM data post switch back to the primary site.
- You are not restoring the UCM DB from the DR site.

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 **Backup and Restore**, 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 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 Avaya Oceana® Cluster 1.
11. From **Backup and Restore**, select **Backup**.

    System Manager displays the Cluster DB Backup page.
12. On the **Cluster Database Backup** confirmation dialog box, select the **UCMService** check box, and click **Continue**.
13. In **Backup Password**, enter a password for the backup.

    Important:

    Note the password entered. You will require this password to restore the UCMService.
14. In **Schedule Job**, click **Run immediately**.
15. Click **Backup**.
16. After the backup process is complete, verify the **Status** column on the **Backup and Restore Status** page. The status must display `Completed`.

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 to the DR site Oceana and POM system.

For more information about switching over and restarting Proactive Outreach Manager, see *Implementing Avaya Proactive Outreach Manager*.

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. Supervisors must then logout.

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	✔
1	Disable the Geographic Redundancy replication.	Disable Avaya Aura® System Manager Geographic Replication at Data Center 1. Disabling the Geographic Redundancy replication on page 122	
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. Shutting down System Manager from the web console on page 123	
3	Activate System Manager at Data Center 2.	Activate Avaya Aura® System Manager at Data Center 2. Activating the secondary System Manager server on page 124	
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. Verifying Breeze node controller on page 179	

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.

Disabling the Geographic Redundancy replication

Before you begin

Log on to the System Manager web console of the primary server.

Procedure

1. On the System Manager web console, click **Services** > **Geographic Redundancy**.
2. Click **Disable Replication**.
3. In the dialog box, click **Yes**.

   The system displays the progress information in the **Disable GR Status** section.

If the disabling process is successful, the system displays the Geographic Redundancy replication status as `Disabled`. The system stops replicating the data from the primary and secondary System Manager server. If the disabling process fails, the system displays an error message on the web console of the primary System Manager.

Shutting down System Manager from the web console

About this task

When you start the shutdown process, you cannot access the System Manager web console.

Before you begin

Log on to the System Manager web console of the active server.

Procedure

1. On the System Manager web console, click **Services** > **Shutdown** > **Shutdown System Manager**.
2. In the Running and Pending Scheduled Jobs section, view the running and pending scheduled jobs.
3. In the Active User Sessions section, view the active user sessions.
4. On the System Manager web console, click **Services** > **Shutdown** > **Shutdown History**.
5. In Initiate Shutdown, click **Shutdown System Manager**.

   System Manager displays the Shutdown System Manager dialog box with the following message.

   ```
   The system initiates System Manager shut down after the grace
   period of 10 minutes, and stops all running jobs. Once you click
   Yes, you cannot abort this operation.

   The system notifies all the users who logged in before System
   Manager shuts down is initiated.

   Are you sure you want to shutdown System Manager?
   ```

6. To start the shutdown process, click **Yes**.

Shutdown System Manager field descriptions

Initiate Shutdown

Button	Description
Shutdown System Manager	Displays the Shutdown System Manager dialog box to select an option to start the shutdown process.

Initiate Reboot

Button	Description
Reboot System Manager	Displays the Reboot System Manager dialog box to select an option to start the reboot process.

Running and Pending Scheduled Jobs

Name	Description
Job Name	The job name as displayed on the Scheduler page.
Job Type	The job type as displayed on the Scheduler page.
Job Status	The status of the job.
Scheduled By	The name of the user who created the job
Start Time	The date and time the job is scheduled to start.

Active User Sessions

Name	Description
User Name	The user name who is currently active.
Session Duration	The session duration since when the user is active.
Is Current Session Status	The status of the current session. The status can be: • **true** • **false**

Activating the secondary System Manager server

About this task

- When you activate the secondary System Manager server, the system stops replicating the data from the primary System Manager server to the secondary System Manager server. During activation, you cannot gain access to the web console of the secondary System Manager server for some time.
- In the same browser instance, do not open the primary and secondary System Manager server in different tabs. The system might display an unknown error after the activation, deactivation, or recovery is complete. You can ignore this error message.

Before you begin

Log on to the System Manager web console of the secondary server.

Procedure

1. On the System Manager web console, click **Services** > **Geographic Redundancy** > **GR Health**.
2. Click **Activate Secondary Server**.

   The system displays the Geographic Redundancy (GR) Health Current status dialog box.
3. In the Select the reason for activation, choose one of the following options:
   - **Primary Down**: When the primary System Manager server becomes nonoperational, the server hardware is faulty and unusable, or the application server fails to recover.
   - **Network Split**: When the enterprise network splits and servers fail to communicate with each other.

- **Maintenance**: When the maintenance activities such as backup, restore, upgrade, and shutdown are in progress.
- **Other**: Any other reason where the primary System Manager server becomes unusable and needs the secondary System Manager server to become operational.

4. Click **Yes**.

   The system displays the initialization of the activation process.

5. Click **Yes**.

   The activation process takes about 15–20 minutes to complete.

   If the activation process fails, the system displays an error message on the secondary System Manager web console and rolls back to the previous state. If the activation process is successful, the secondary System Manager server changes to the active mode and provides complete System Manager functionality.

   Because the server becomes unavailable, you cannot gain access to the web console. Wait until the process is complete before you continue with the next step.

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.

OCP DB switchover with Campus HA 2+1

Removing cache mirroring from Campus Standby

About this task

Use this procedure to remove cache mirroring from Campus Standby.

Procedure

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

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

   <IP> is the IP address of the standby Omnichannel server in Data Center 1.
2. On the Cache Management Portal login page, do the following:
   a. In 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 Mirror** > **Remove Mirror Configuration**.
4. To remove the mirrored attribute, click **Yes** and then click **Remove**.

Switching over DR server

Promoting Omnichannel server in DC2

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 is available, and mirroring is operational for planned maintenance windows. You can use this procedure irrespective of whether a dual server pair is deployed on the primary site.

Procedure

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 Avaya Control Manager (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 Pointing ACM to the new Omnichannel database server in DC2 on page 107.

Demoting primary to async

About this task

Use this procedure to demote the primary server to async.

Procedure

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

1. Navigate to **CCDINSTANCE** and click **Start Caché**.
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 node** > **Backup And Restore**.
6. Click **Mirror Configuration**.
7. In the **Select Mirror Scenario** field, select **Demote** to **Async**.
8. Click **Execute**.

Pointing ACM to the new Omnichannel database server in DC2

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, host name, or IP address of the Omnichannel Database DR 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.

For more information on configuring the Omnichannel certificate, refer to the *Retrieve certificate files* section in the *Deploying Avaya Oceana®* document.

Switching over Avaya Analytics™ from DC1 to DC2

About this task

Using the following steps you can promote DC2 to primary role after a fail over. DC1 does not synchronize data after this operation until a rebuild from DC2 is available.

Note:

You must perform this switch over only during a maintenance window.

Before you begin

Ensure that the secondary data center is on standby mode.

Procedure

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

   `ccm release orca analytics`
4. To select the **Geo/High Availability** option, enter the corresponding number.
5. To select the **Geo options** option, enter the corresponding number.
6. To select the **Switch over: Promote secondary data center database to primary** option, enter the corresponding number.

   Warning:

   You must use this option only on the secondary data center.
7. In the **Proceed to Geo switchover**, enter `y`.

   Entering `n` cancels the operation.
8. In the **Continuing will switch over this data center to Primary data center** field, type `y` and press **Enter**.

   This operation is successful only when a server is available on standby mode.
9. Return to the previous page by entering `b`.
10. Quit the current page by entering `q`.
11. Return to the main menu by entering `m`.

Related links

Reversing data replication when the DC2 is the primary on page 81

Reversing data replication when the DC2 is the primary

About this task

Once the cause of the DC1 failure has been resolved and fixed, you can switch back from DC2 as the primary to DC1. However, before doing that, DC1 first needs to receive data replication from DC2.

Note:

- If testing, you must only perform this process during a maintenance window.

Procedure

1. On the DC2, do the following on the Cluster Control Manager (CCM) console:
   a. Run the `Analytics Administration` script as root user, use the following command:

      `ccm release orca analytics`

   b. Select **Geo/High Availability** by pressing the corresponding number.
   c. Select **Geo options** by pressing the corresponding number.
   d. Select **Configure Primary Geo cluster** by pressing the corresponding number.
   e. Make a note of the **IP address** and **PV name** that you receive at the end of this process. You need these values later in this process. The script takes a few minutes to run.
2. On the DC1 to make it a standby, do the following on the Cluster Control Manager (CCM) console:
   a. Log in to the Cluster Control Manager (CCM) console of the DC1 cluster as the cust user.
   b. Switch to the root user by entering `su`.
   c. Run **`cluster_ssh`**. This displays the available nodes, for example:
      a. `node164182.puneccq.avaya.com`
      b. `node164183.puneccq.avaya.com`
      c. `node164184.puneccq.avaya.com`
   d. Run the firewall config command for each node and exit. For example; Select [1].

      Note:

      The IP Address argument is the same IP address output from the Geo Primary config.

```
Last login: Tue May 31 21:10:27 2022 from 135.27.164.178
DeployType=Cluster Node
[ccmuser@node164182 ~]$ sudo firewall-cmd --permanent --direct --add-rule
ipv4 filter OUTPUT 0 -o eth0 -d IP_Address -j ACCEPT
[ccmuser@node164182 ~]$ sudo systemctl restart firewalld
[ccmuser@node164182 ~]$ exit
```

3. Quit the current page by entering `q`.
4. To run the `Analytics Administration` script as root user, use the following command:
5. Select **Geo/High Availability** by pressing the corresponding number.
6. Select **Geo options** by pressing the corresponding number.
7. Select **Configure Standby Geo cluster** by pressing the corresponding number.
8. In the **Proceed to Standby Geo cluster config** field, enter `y`.
9. At the prompt for IP address, enter the IP address and PV names that you noted from the secondary data center.

   Note:

   The script will take few minutes to run.
10. Return to the previous page by entering `b`.
11. Quit the current page by entering `q`.
12. Return to the main menu by entering `m`.

    Note:

    - Once the above steps are completed successfully, the Analytics database and MicroStrategy database will start to sync.
    - The MSTR will not be accessible for the standby data center.

Next steps

- At this stage, DC2 is still the primary but now with data being replicated to DC1. To return the DC1 to the primary role, repeat the switch over process (Switching over from the primary to the secondary data center on page 80) but with the data centers reversed. That is, promote DC1 to be the primary and configure DC2 to be the Standby Geo for DC1.

Related links

Disaster Recovery Process Checklist on page 80
Switching over Avaya Analytics from DC1 to DC2 on page 108
Switching over Avaya Analytics from DC1 to DC2 on page 128

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 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

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.

Configure 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.

Partial and Full Switchover - Configuration and Validation

Checklist for full or partial controlled switchover

The following checklist lists the configuration and validation steps after you perform a full or partial controlled switchover.

Note:

The configuration and validation steps listed here are mandatory for both full or partial controlled switchovers.

No.	Task	Description	✔
1	Verify CSC deployment status in DC2.	See Verifying the CSC deployment status in DC2 on page 133.	

Table continues…

No.	Task	Description	✔
2	Restore the UCMService data for Avaya Oceana® cluster 1 in Data Center 2.	See • Preparing UCMService in DC2 for database restore on page 134 • Restoring the UCMService data for Avaya Oceana Cluster 1 in Data Center 2 on page 134	
3	Configure the DR site EmailService startup.	See Configure the DR site EmailService startup on page 135.	
4	Configure the DR site Chat startup.	See Configure the DR site Chat startup on page 135.	
5	Configure the DR site MessagingService for Social or SMS startup.	See Configure the DR site MessagingService for Social, SMS or Async startup on page 136.	
6	Configure the DR site GenericChannelAPI Service startup.	See Configure the DR site GenericChannelAPI Service startup on page 136.	
7	Verify DR Application Enablement Services server to enable switch connection.	See Verify the DR Application Enablement Services on page 137.	
8	Change the cluster activity status for clusters in DC2	See Changing cluster activity status for clusters in Data Center 2 on page 138	
9	Avaya Workspaces Agent switchover: Login Agents using DC2 Workspaces and test deployed Channel Routing.	See Avaya Workspaces Agent switchover on page 139.	
10	Use the Toggle button to switch ACM in DC 1 to use Avaya Oceana® applications in DC2.	See Using Toggle button to switch Avaya Control Manager in Data Center 1 to use Avaya Oceana applications in Data Center 2 on page 139	
11	Validate and test deployed channels: Launch Oceana Dashboard and verify all deployed channels are in the Green status.	See Validate and test deployed channels on page 140.	

Verifying the CSC deployment status in DC2

About this task

Use this procedure to verify the deployment status for the CallServerConnector (CSC) PU on DC2.

Procedure

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

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

2. On the Monitor Service page, click **Cluster 2** > **Show cluster Messages**.

   The page displays all the PUs in Cluster 2 (DR Cluster).
3. From the **Filters** column, select the **CallServerConnector** PU.
4. Verify that the `HEARTBEAT` message for the **CallServerConnector** PU is `ACTIVE`.

Preparing UCMService in DC2 for database restore

About this task

Use this procedure to uninstall UCMService from secondary Cluster 1 for the Unified Collaboration Model (UCM) database restore. Uninstalling UCMService does not impact the ongoing Avaya Oceana® disaster recovery operations.

Procedure

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

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

Restoring the UCMService data for Avaya Oceana® Cluster 1 in Data Center 2

About this task

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

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®** > **Cluster Administration**.
2. From **Backup and Restore**, select **Restore**.
3. 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**.

4. On the Cluster Database Restore Confirmation dialog box, select Avaya Oceana® Cluster 1 and click **Continue**.
5. On the Backup and Restore Status page, ensure that the **Status** column for the restore operation displays the value `Completed`.
6. Install UCMService on Avaya Oceana® Cluster 1.
7. Reboot Avaya Oceana® Cluster 1 and then Avaya Oceana® Cluster 3.

Configure the 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 DR site Service Clusters tab, do the following:
   a. **Cluster**: Select DR site 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 **Effective Value**, change the value from `false` to `true`.
4. Click **Commit**.

Configure the 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 DR site Service Clusters tab, do the following:
   a. **Cluster**: Select DR site Avaya Oceana® Cluster 3.
   b. **Service**: Select **CustomerControllerService**.
3. In **Shutdown Mode** attribute, do the following:
   a. Select the **Override Default** check box.

b. In **Effective Value**, change the value from `true` to `false`.

4. Click **Commit**.

Note:

You must configure the customer deployed chat front-end application to point to the Oceana DR system. The instructions to complete the 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.

Configure the DR site MessagingService for Social, SMS or Async 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 DR site Service Clusters tab, do the following:
   a. **Cluster**: Select DR site Avaya Oceana® Cluster 3.
   b. **Service**: Select **MessagingService**.
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:

You must configure the customer deployed Social, Async, or SMS channel front-end application to point to the Oceana DR system. The instructions to complete the 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.

Configure the 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 DR site Service Clusters tab, do the following:
   a. **Cluster**: Select DR site 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:

You must configure the customer deployed Generic channel front-end application to point to the Oceana DR system. The instructions to complete the 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.

Verify the DR Application Enablement Services

About this task

In the setup instructions for Avaya Workspaces for Call Center Elite 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 Workspaces for Call Center Elite 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.

Changing cluster activity status for clusters in Data Center 2

Before you begin

Ensure that the OceanaMonitorService is installed 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**.

      The cluster status changes to `ACTIVE` and all nodes are placed in the Accept New Service mode.

   c. Click **OK** on the confirmation message box.
   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 is not deployed if the **Oceana** > **CSC** > **AES** > **CM** configuration is not done 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 **Accepting**. If any clusters or nodes are in **Deny** state, then re-do the above steps or manually set them to **Accepting** state using the Avaya Breeze® platform EM cluster overview page.

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:

  ```
  https://<UAC Cluster IP/FQDN DC1>/services/UnifiedAgentController/
  workspaces/#/login
  ```

- DR Site:

  ```
  https://<UAC Cluster IP/FQDN DC2>/services/UnifiedAgentController/
  workspaces/#/login
  ```

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.

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.

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: Planned Partial and Full Recovery and Switchback

Planned switchback from DC2 to DC1

This chapter provides information and instructions to take DC2 out of production and into a shutdown or standby mode to perform a switchback to DC1.

Switchback from planned maintenance windows

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

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 in 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 before the switchback 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. During this maintenance window, Avaya Oceana® cannot process any contacts. For example, if the contact center needs to process voice contacts during the maintenance window, it is recommended to use the fallback to Elite feature that gets automatically invoked once Avaya Oceana® is out of service. There is no fallback alternative for Digital Contacts.

Advantages of performing a planned switchback

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

There are several advantages of performing a planned switchback of Avaya Oceana® and Avaya Analytics™ DR solution.

- Existing contacts can be processed in a controlled manner.
- New contacts cannot enter into the system queue after the switchover procedures start.
- Logged-in agents can access 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.

Switchback from Partial and Full switchover - Preparation and Validation

Checklist for full or partial controlled switchback

The following is a checklist of the preparation and validation steps before you perform a full or partial controlled switchback:

Note:

The preparation and validation steps listed here are mandatory for a full or partial controlled switchback.

No.	Task	Description	✔
1	Prepare for switchback: Before starting any switchback operations on a production Avaya Oceana® and Avaya Analytics™ DR system, you must refer several key documents.	See the following documents: • Administering Avaya Aura® System Manager • Installing Avaya Control Manager • Administering Avaya Aura® Communication Manager • Administering Avaya Aura® Application Enablement Services	
2	Agree on a date, time, and duration for planned maintenance windows with customers as Avaya Oceana® and Avaya Analytics™ will be unavailable.	See Planned maintenance window for Switchback on page 144.	

Table continues…

No.	Task	Description	✔
3	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	See Validate identical software levels on following applications across DC1 and DC2. on page 144.	
4	Validate Avaya Control Manager database HA replication status.	Validate Avaya Control Manager Database HA Replication Status on page 145.	
5	Verify the Omnichannel database mirroring status from DC2 to DC1.	See Validation of Omnichannel Database mirroring from DC2 to DC1 on page 145.	
6	Validate Avaya Oceana® core components replication operational before switchback.	See Validating Avaya Oceana core components replication operational before switchback on page 146.	
7	Verify the CallServerConnector component in the primary site.	See Verifying the CallServerConnector component in the primary site on page 146.	
8	Verify the deployment mode status of the primary site email snap-in.	See Verifying deployment mode status of primary site email snap-in on page 146.	
9	Verify the shutdown mode status of the primary site CustomerController chat snap-in.	See Verifying the shutdown mode status of primary site CustomerController chat snap-in on page 147.	
10	Verify the shutdown mode status of the primary site MessaginService snap-in.	See Verifying the shutdown mode status of primary site MessagingService snap-in on page 147.	
11	Verify the shutdown mode status of the primary site GenericChannelAPI snap-in.	See Verifying the shutdown mode status of primary site GenericChannelAPI snap-in on page 148.	

Table continues…

No.	Task	Description	✔
12	Verify deployment status of AMC snap-in for Avaya WebRTC Connect contacts.	See Verifying deployment status of AMC snap-in for Avaya WebRTC Connect contacts on page 148.	
13	Prepare primary DC1 Avaya Oceana® for potential UCA and UCM DB restore.	See the following: • Preparing DC1 for UCA and UCM database restore on page 149 • Preparing UCAStoreservice in DC1 for database restore on page 149 • Preparing UCMService in DC1 for database restore on page 150	
14	Reboot Avaya Oceana® Cluster 1 in the Primary DC1 site.	See Rebooting Avaya Oceana Cluster 1 on DC1 on page 150.	
15	Log supervisors and agents out of DC2.	See Logging out supervisors and agents from the DR site on page 150.	
16	Validate contacts in DC2.	See Validating contacts on page 151.	

Planned maintenance window for Switchback

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

The other major difference between a switchback and a switchover is that you must reinstate all failed elements that caused a switchover in DC1 before the switchback can take place and restore normal disaster recovery functionality.

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

The software versions and levels on Data Center 1 and Data Center 2 must be identical for a planned switchover and switchback testing,

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 before 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. Instead, you can create a checklist to record the software versions of each application for DC1 and DC2.

Validate Avaya Control Manager Database HA Replication Status

About this task

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

Verifying Omnichannel database mirroring status

About this task

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

For unplanned switchbacks due to Omnichannel failures, reinstate the failed servers first and then reinstate mirroring. Before starting the switchback, read the later chapters of this document to find out how to reinstate a failed Omnichannel server.

Verify that mirroring is enabled from the DR to primary servers before a switchback. This is a baseline requirement before starting a switchback.

The Omnichannel database replicates data from DC2 to DC1 after a planned switchover using Cache Mirroring from DR to the primary. 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.

For more information, see procedure in Verifying the Omnichannel Database mirroring status on page 49.

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 replicating data from the DC2 to DC1 is fully operational.

The Omnichannel database replicates data from DC2 to DC1 after a planned switchover using Cache Mirroring from DR to primary. 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 the CallServerConnector component in the primary site

About this task

Before switchback, you must verify the CallServerConnector component in the primary site as the CallServerConnector attributes handle the call control and the agent control functions on DC1.

Procedure

1. On the Monitor Service page, click **Cluster 1** > **Show cluster Messages**.

   You can see all the PUs in Cluster 1.
2. From the **Filters** column, select **CallServerConnector** PU.
3. Verify that the `HEARTBEAT` message for **CallServerConnector** PU is `INTACT`.

Verifying deployment mode status of primary site email snap-in

About this task

Before a switchback, validate that the email snap-in deployment mode status attribute in the primary site is `true`.

If you do not have an 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 as it is the default value.

4. Click **Commit**.

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

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

About this task

The CustomerController snap-in enables the chat contacts to enter the Avaya Oceana® ecosystem. Before a switchback from the DR site, validate that the shutdown mode status attribute in the primary site for this snap-in is `false`.

If you do not have a 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 the **Advanced** area, in the **Shutdown mode status** field, ensure that the field value is set to `false`.
4. Click **Commit**.

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

Verifying the shutdown mode status of primary site MessagingService snap-in

About this task

The MessagingService snap-in works on the front-end of many Avaya Oceana® channel snap-ins such as SMS, Social, or Async. Before a switchback, you must check the status of the shutdown mode attribute for this snap-in in the primary site. This will help make sure that the switchback goes smoothly.

If you do not have an 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 the **Advanced** area, in the **Shutdown Mode status** field, ensure that the field value is set to `false`.
4. Click **Commit**.

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

Verifying the shutdown mode status of primary site GenericChannelAPI snap-in

About this task

The GenericChannelAPI snap-in gets the generic contacts into the Avaya Oceana®. Before a switchback, you must check the status of the shutdown mode attribute for this snap-in in the primary site. This will help make sure that the switchback goes smoothly.

If you do not have a 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 the Advanced area, in the **Shutdown Mode** status field, validate that the field value is set to `false`.
4. Click **Commit**.

   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 Avaya Mobile Communications (AMC) snap-in enables WebRTC Connect voice and video contacts to enter Avaya Oceana®. Before a switchback.

You must verify the deployment status of the AMC snap-in Processing Unit (PU) using Oceana Monitor to ensure if the snap-in is active and operational. This will help make sure that the switchback goes smoothly.

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 is `Intact`. If the status is `Scheduled` or `Broken`, the AMC snap-in is not operational. You must resolve the issue before proceeding with the switchover. Otherwise, when the switchover is complete, WebRTC Connect voice or video contacts will not be routed in Avaya Oceana®.

Preparing DC1 for UCA and UCM database restore

About this task

After a partial or full DR switchover, when there are additions and changes to the databases, restore Unified Collaboration Administration (UCA) and Unified Collaboration Model (UCM) data. If the customer does not require any data from DC2 to be restored, do not uninstall or reboot the cluster.

Procedure

1. Log on to Avaya Aura® System Manager.
2. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
3. On the Service Clusters tab, select **UCAStoreService**.
4. In the Startup Configuration group, set the **Disaster recovery role** attribute to `GEO_MASTER` on DC1 and `GEO_SLAVE` on DC2.

   Important:

   Disaster recovery role is a mandatory attribute if you require geographical disaster recovery. After configuration, if you change the **Disaster recovery role** attribute, you must reboot the cluster for the changes to take effect.
5. Click **Commit**.

Preparing UCAStoreservice in DC1 for database restore

About this task

You must uninstall the Unified Collaboration Administration (UCA) service from the primary Cluster 1 in DC1 so that the UCA in DC1 picks up the UCA database restore from DC2.

Procedure

1. Log on to Avaya Aura® System Manager.
2. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.

3. On the Services page, select the **UCAStoreService** check box and click **Uninstall**.
4. In the **Confirm Uninstall service: UCAStoreService** dialog box, select the **primary Cluster 1** check box and click **Commit**.
5. On the Services page, verify that the state of the service is `Uninstalling`.

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

Preparing UCMService in DC1 for database restore

About this task

Use this procedure to uninstall UCMService from primary Cluster 1 for the Unified Collaboration Model (UCM) database restore. Uninstalling UCMService does not impact the ongoing Avaya Oceana® disaster recovery operations.

Procedure

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

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

Rebooting Avaya Oceana® Cluster 1 on DC1

About this task

You can reboot outside the maintenance window allocated for the actual switchback to DC1.

Procedure

1. Log on to Avaya Aura® System Manager.
2. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
3. Select the **Primary cluster 1** check box and reboot.

   Wait until the reboot of all nodes is complete, and the nodes are back in service in `Deny` mode.

Logging out supervisors and agents from the DR site

For a planned switchback, ensure that all Avaya Workspaces for Call Center Elite agents are logged out. Supervisors can verify agent status using the **My team** widget. Supervisors must co-ordinate locally to ensure that the agents are logged out. Supervisors must then logout.

Validating contacts

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

Note:

Queued contacts are lost if not processed before the switchback to DC1.

Switchback - Partial controlled failover

Checklist for Partial Controlled Switchback

The following checklist provides the list of steps to perform a Partial Controlled Switchback.

No.	Task	Description	✔
1	Shut down and switch back the DR site voice channel to the primary site.	See Shut down and switchover to DR site voice channel on page 152.	
2	Configure the DR site email shutdown.	See Configuring DR site email shutdown on page 153.	
3	Configure the DR site MessagingService shutdown.	See Configuring DR site MessagingService shutdown on page 154.	
4	Configure the DR site chat shutdown.	See Configuring DR site chat shutdown on page 154.	
5	Configure the primary site GenericChannelAPI service shutdown.	See Configuring DR site GenericChannelAPI Service shutdown on page 155.	
6	Set the maintenance mode for web voice and web video.	See Setting the maintenance mode for web voice and web video on page 155.	
7	Shut down the DR outbound channel.	See Oceana POM switchback on page 155.	
8	Change the cluster activity status for clusters in DC2.	See Changing the Cluster Activity status for the clusters in Data Center 2 on page 156.	

Table continues…

No.	Task	Description	✔
9	Switchback Avaya Analytics™ from DC2 to DC1.	See Switching over from the primary to the secondary data center on page 80.	
10	Reconfigure Avaya Oceana® addresses to DC1.	See Reconfiguring Avaya Oceana addresses to DC1 on page 158.	
11	Point ACM to the Omnichannel database server in DC1.	See Pointing ACM to the new Omnichannel database server in DC2 on page 158.	
12	Clean up and reconfigure the Mirror setup on DC1 and DC2.	See Clean up Mirror setup on DC1 and DC2 on page 159.	
13	Configure Omnichannel database mirroring between DC1 and DC2.	See the following: • Configuring Omnichannel database mirroring between DC1 and DC2 on page 162. • Prompting OCP DB Server A to primary server on page 162. • Demoting OCP DB server C to async member (DR Server) on page 163. • Joining mirror for OCP DB server B as failover member (Standby Server) on page 164.	
14	Configure the Web Voice and Web Video after Switchback.	See Configuring the Web Voice and Web Video after Switchback on page 165.	
15	Change the cluster activity status for clusters in DC1.	See Changing cluster activity status from Standby to Active for clusters in Data Center 1 on page 165.	
16	Use the Toggle button to switch ACM in DC2 to use Avaya Oceana® applications in DC1.	See Using the Toggle button to switch back Avaya Control Manager in Data Center 1 on page 192.	
17	Avaya Workspaces Agent switchover.	See Avaya Workspaces agent switchover on page 166.	
18	Validate and test deployed channels.	See Validate and test deployed channels on page 166.	

Shut down and switchover to DR site voice channel

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 **DataCenter2**.
5. Click **Save**.

   When new incoming voice contacts come in through the Avaya Experience Portal application, they are routed to the Avaya Oceana® system in the primary location DC1.

Configuring DR site email shutdown

About this task

For switchbacks, if email is deployed, you must change the deployment mode status of the EmailService snap-in from true to false. An Avaya Oceana® administrator with access to System Manager can change the status.

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.

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 DR site 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 switchback, an administrator can manually stop new incoming SMS, Social and Async contacts from entering the Avaya Oceana® and allow existing contacts to be processed gracefully out of the system.

If you do not have SMS, Social, or 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 Service Clusters tab, do the following:
    a. **Cluster**: Select DR site 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 switchback, an administrator can manually stop new incoming chat contacts from entering Avaya Oceana® and allow existing contacts to be processed gracefully out of the system.

If you do not have the 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 Service Clusters tab, do the following:
    a. **Cluster**: Select DR site 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 switchback, an administrator can manually stop new incoming Generic contacts from entering Avaya Oceana® and allow existing contacts to be processed gracefully out of the system.

If you do not have the 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 Service Clusters tab, do the following:
    a. **Cluster**: Select DR site 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 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 switchback

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

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

Before you begin

Ensure that you install OceanaMonitorService on the clusters in Data Center 2.

Procedure

1. To open the Oceana Manager page, enter the following URL in your web browser:

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

   Important:

   Create a bookmark for this URL in your web browser to 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 administrator 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. In 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 in the Deny state.

Switching over from the primary to the secondary data center

About this task

Use this procedure to promote the secondary DC2 to the primary role after a DC1 failure.

Note:

- If testing, you must only perform this process during a maintenance window.
- The entire data center must fail over in this case. For example, it is not supported to run Avaya Oceana® on DC1 against Avaya Analytics™ on DC2.

Before you begin

- Check that the secondary DC2 data center is in standby mode.

Procedure

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

   `ccm release orca analytics`
4. Select **Geo/High Availability** by pressing the corresponding number.
5. Select **Geo options** by pressing the corresponding number.
6. Select **Switch over: Promote secondary data center database to primary** by pressing the corresponding number.
7. In the **Proceed to Geo switchover** field, enter `y`. Entering `n` cancels the operation.
8. In the **Continuing will switch over this data center to Primary data center** field, enter `y`.
9. Return to the previous page by entering `b`.
10. Quit the current page by entering `q`.
11. Return to the main menu by entering `m`.
12. Restart the following services using post install scripts, do the following:
    a. Run `Analytics Administration` script, use the following command:

       `ccm release orca analytics`.
    b. Select **Troubleshooting** > **General** > **Restart Measure Processors** and wait until all the measure processors are up.
    c. Restart orca-scheduler and orca-admin-data-service.
    d. Restart pod orca-database-rest.
13. Return to the previous page by entering `b`.
14. Quit the current page by entering `q`.
15. Return to the main menu by entering `m`.

Next steps

- Once the cause of the DC1 failure has been resolved and fixed, you can switch back from DC2 as the primary to DC1. To start that process, DC1 first needs to receive data replication from DC2. See Reversing data replication when the DC2 is the primary on page 81.

Related links

Disaster Recovery Process Checklist on page 80

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 in 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, type 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, type the Welcome Page URL for Data Center 1 operations.
8. In the **Workspaces** field, type the Widget Web Server URL link for Data Center 1 operations.
9. Click **Save**.

Pointing ACM to the new Omnichannel database server in DC2

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, host name, or IP address of the Omnichannel Database DR 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.

   For more information on configuring the Omnichannel certificate, refer to the *Retrieve certificate files* section in the *Deploying Avaya Oceana®* document.

Clean up 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 160.

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 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. Go to **System Administration** > **Configuration** > **Mirror Settings** > **Edit mirror**.
4. Select **Remove mirror configuration**.
5. Select **Clear mirror flag**.
6. In the 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. Go 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.

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 48.

Switchback with OCP DB server - planned switchback

Prompting OCP DB Server A to primary server

About this task

Use this procedure to prompt the OCP DB Server A to primary server.

Procedure

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

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 node** > **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**. Verify the message when execution is complete.
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 page, do the following:
    a. Select the location where you want to save the backup file.

       Note:

       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.
    c. Click **Save**.
12. Click **Backup Database**.

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

Demoting OCP DB server C to async member (DR Server)

About this task

Use this procedure to demote the OCP DB server C to async member.

Procedure

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

1. Navigate to **CCDSINSTANCE** and click **Start Caché**.
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 node** > **Backup And Restore**.

6. Click **Mirror Configuration**.
7. In the **Select Mirror Scenario** field, select **Demote** to **Async**.
8. Click **Execute**. Verify the message when execution is complete.

Joining mirror for OCP DB server B as failover member (Standby Server)

About this task

Use this procedure to join mirror for the OCP DP Server B as failover member.

Procedure

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

1. Navigate to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement` folder.
2. Right-click the `OceanaDataManagementTool.exe` file and click **Run as administrator**.
3. In the navigation pane, click **Configuration** > **Mirror Settings** > **Join Mirror** .
4. In the **Type** attribute, select **Failover**.
5. Enter 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** check box 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, select the server certificate from the list.
    c. In the **File containing associated private key** field, select the key from the list.
    d. In the **Private key password** field, enter the new password.
7. Click **Save**.
8. Copy the backup file from the active Omnichannel Database server to the standby Omnichannel Database server in Data Center 1.
9. In the Oceana Data Management utility, click **Backup And Restore**.
10. In the navigation pane, click **Backup And Restore**.
11. In the **Select file to restore from** field, click **Browse**.
12. On the Open window, do the following:
    a. Browse to the location where you stored the backup file.
    b. Select the backup cbk file.
    c. Click **Open**.
13. Click **Restore Database**.

    The system displays the message:`Are you restoring a mirrored backup?`

14. Click **Yes**.
15. Click **Restore**.

    The utility displays the Restore complete! message when the restore process is complete.

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 the web and mobile clients go to the primary site.

Changing cluster activity status from Standby to Active for clusters in Data Center 1

Before you begin

Ensure that the OceanaMonitorService is installed on the clusters in Data Center 1.

Procedure

1. Open the Oceana Manager page in the DR location 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. 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**.

      The cluster status changes to `ACTIVE` and all nodes are placed in the Accept New Service mode.
   c. Click **OK** on the confirmation message box.
   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 primary Cluster 1 drop-down menu and start Oceana Monitor.

   On Cluster 1, verify the PUs deployed and status is **Intact** including CSC. CSC PU is not deployed if the **Oceana** > **CSC** > **AES** > **CM** configuration is not done 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 **Accepting**. If any clusters or nodes are in **Deny** state, then re-do the above steps or manually set them to **Accepting** state using the Avaya Breeze® platform EM cluster overview page.

Avaya Workspaces agent switchover

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

The default Avaya Workspaces URL for both locations are:

Primary Site: `https://<UAC Cluster IP/FQDN DC1>/services/UnifiedAgentController/workspaces/#/login`

DR Site: `https://<UAC Cluster IP/FQDN DC2>/services/UnifiedAgentController/workspaces/#/login`

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 the routing of the deployed channels.

Switchback - Full controlled failover

Checklist for Full Controlled Switchback

The following checklist provides the list of steps to perform a Full Controlled Switchback.

No.	Task	Description	✔
1	Shut down and switch back DR site voice channel to primary site.	See Shut down and switchover to DR site voice channel on page 169.	
2	Configure Application Enablement Services (AES) for switchback.	See Configuring Application Enablement Services (AES) for switchback on page 170.	
3	Switch back from ESS to Avaya Aura® Communication Manager after full DR switchovers.	See Switchback from ESS to Avaya Aura Communication Manager after full DR switchovers on page 171.	
4	Configure the DR site email shutdown.	See Configuring DR site email shutdown on page 171.	
5	Configure the DR site MessagingService shutdown.	See Configuring DR site MessagingService shutdown on page 171.	
6	Configure the DR site chat shutdown.	See Configuring DR site chat shutdown on page 172.	
7	Configure the DR site GenericChannelAPI service shutdown.	See Configuring DR site GenericChannelAPI Service shutdown on page 172.	
8	Set the maintenance mode for front end web voice and web video.	See Setting the maintenance mode for web voice and web video on page 173.	
9	Shut down DR outbound channel.	See Oceana POM switchback on page 173.	
10	Change the cluster activity status for clusters in DC2.	See Changing cluster activity status from Active to Standby for clusters in Data Center 2 on page 173.	
11	Re-instate System Manager as Primary on DC1.	See the following topics: • Re-Instate System Manager replication to DC2 System Manager on page 174. • Checklist for Avaya Aura System Manager switchback on page 174.	
11	Verify Avaya Aura® System Manager replication status between DC1 to DC2.	See Verifying replication status between DC1 to DC2 on page 178.	
12	Validate Avaya Aura® System Manager and Avaya Breeze® platform replication status to all Avaya Breeze® platform nodes in DC1 and DC2.	See Validating Avaya Aura® System Manager and Avaya Breeze® replication status on page 178.	
13	Verify Avaya Breeze® platform node controller.	See Verifying Avaya Breeze platform node controller on page 179.	

Table continues…

No.	Task	Description	✔
14	Change the cluster activity status for clusters in DC1.	See Changing cluster activity status from Standby to Active for clusters in Data Center 1 on page 179.	
15	Reconfigure Avaya Oceana® addresses to DC1.	See Reconfiguring Avaya Oceana addresses to DC1 on page 180.	
16	Re-establish UCA replication from primary UCA to DR UCA.	See the following: • Re-establishing UCA replication from primary UCA to DR UCA on page 181. • Taking a backup of UCAStoreService in Data Center 1 on page 181. • Scheduling Database Backups UCMServer and UCAStoreService on page 182. • Restoring UCAStoreService data in DC1 on page 183. • Installing UCAStoreService in DC1 on page 184.	
17	Restore UCMService after switchback.	See the following: • Backing up UCMService in DC2 on page 184. • Restoring UCMService data in DC1 on page 186.	
18	Point ACM to the Omnichannel database server in DC1.	See Pointing ACM to the new Omnichannel database server in DC2 on page 186.	
19	Clean up and reconfigure Mirror setup on DC1 and DC2.	See the following: • Clean up and reconfigure Mirror setup on DC1 and DC2 on page 187. • Prompting OCP DB Server A to primary server on page 162. • Demoting OCP DB server C to async member (DR Server) on page 163. • Joining mirror for OCP DB server B as failover member (Standby Server) on page 164.	

Table continues…

No.	Task	Description	✔
20	Switchback Avaya Analytics™ from DC2 to DC1	See Switching over from the primary to the secondary data center on page 80.	
20	Restore Avaya Control Manager.	See the following: • Restoring Avaya Control Manager on page 191. • Reconfiguring Avaya Control Manager in switchback scenarios on page 191. • Using the Toggle button to switch back Avaya Control Manager in Data Center 1 on page 192.	
21	Restore the External Data Mart server.	See Restoring the External Data Mart server on page 192.	
22	Avaya Workspaces agent switchover.	See Avaya Workspaces agent switchover on page 195.	
23	Validate and test deployed channels.	See Validate and test deployed channels on page 195.	

Shut down and switchover to DR site voice channel

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 **DataCenter2**.
5. Click **Save**.

   When new incoming voice contacts come in through the Avaya Experience Portal application, they are routed to the Avaya Oceana® system in the primary location DC1.

Configuring Application Enablement Services (AES) for switchback

About this task

In the setup instructions for Avaya Workspaces for Call Center Elite 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`.

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.

Configuring DR site email shutdown

About this task

For switchbacks, if email is deployed, you must change the deployment mode status of the EmailService snap-in from true to false. An Avaya Oceana® administrator with access to System Manager can change the status.

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.

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 DR site 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 switchback, an administrator can manually stop new incoming SMS, Social and Async contacts from entering the Avaya Oceana® and allow existing contacts to be processed gracefully out of the system.

If you do not have SMS, Social, or 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 Service Clusters tab, do the following:
    a. **Cluster**: Select DR site 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 switchback, an administrator can manually stop new incoming chat contacts from entering Avaya Oceana® and allow existing contacts to be processed gracefully out of the system.

If you do not have the 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 Service Clusters tab, do the following:
    a. **Cluster**: Select DR site 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 switchback, an administrator can manually stop new incoming Generic contacts from entering Avaya Oceana® and allow existing contacts to be processed gracefully out of the system.

If you do not have the 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 Service Clusters tab, do the following:
    a. **Cluster**: Select DR site 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 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 switchback

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

Changing cluster activity status from Active to Standby for clusters in Data Center 2

Before you begin

Ensure OceanaMonitorService is installed 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:

   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 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**.

The cluster status changes to `STANDBY` and all nodes are placed in the Deny New Service mode.

c. Click **OK** on the confirmation message box.

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.

Re-Instate Avaya Aura® System Manager

Re-instate Avaya Aura® System Manager as Primary on DC1

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

The following is a checklist of Avaya Aura® System Manager procedures for full DR switchbacks.

No.	Task	Description	Notes	✔
1	Deactivate the secondary System Manager server.	Deactivate the secondary System Manager server. See Deactivating the secondary System Manager server on page 175.	For more information, see *Administering Avaya Aura® System Manager*.	

Table continues…

No.	Task	Description	Notes	✔
2	Restore the primary System Manager server.	After you deactivate the secondary System Manager server, restore the Primary System Manager server. See Restoring the primary System Manager server on page 175.	For more information, see *Administering Avaya Aura® System Manager*.	

Deactivating the secondary System Manager server

Before you begin

Log on to the System Manager web console of the secondary server.

Procedure

1. On the System Manager web console, click **Services** > **Geographic Redundancy** > **GR Health**.
2. Click **Deactivate Secondary Server**.

   The system displays the Deactivate Secondary Server dialog box and the progress while performing the deactivation process.
3. Click **OK**.

   If the deactivation process is complete, the secondary System Manager server goes to the standby mode. If the deactivation process fails, the system displays an error message on the secondary System Manager web console and the server remains in the active mode.

Next steps

Restore primary System Manager. For information, see “Restoring the primary System Manager server”.

Restoring the primary System Manager server

Before you begin

- Create the snapshot of the primary and secondary System Manager servers.

  Note:

  Delete the snapshot after the data is successfully restored.
- Log on to the System Manager web console of the primary server.

About this task

You can restore the data when the secondary System Manager server is active or in the standby mode. However, for minimum system nonfunctional time during data restoration or an emergency or both, you can restore the data when the secondary System Manager server is active.

Note:

It is recommended to first deactivate secondary System Manager server and then start the **Restore Data** operation. If the Geo Data Restore operation is performed using Secondary Data while Secondary is in active state, then there could be data loss or inconsistency if changes are made on the secondary System Manager server while the Geo Data Restore operation is in progress.

If you choose to retain the primary System Manager database as part of Geo Data Restore then this note does not apply to you.

Important:

After you restore the system with the secondary System Manager data, if you want to revert to the primary System Manager data, you can restore to the primary System Manager data using the procedure in Step 4. However, you must restore to the primary System Manager data, before you enable the Geographic Redundancy replication. After you enable the Geographic Redundancy replication, you cannot restore to the primary System Manager server data.

Procedure

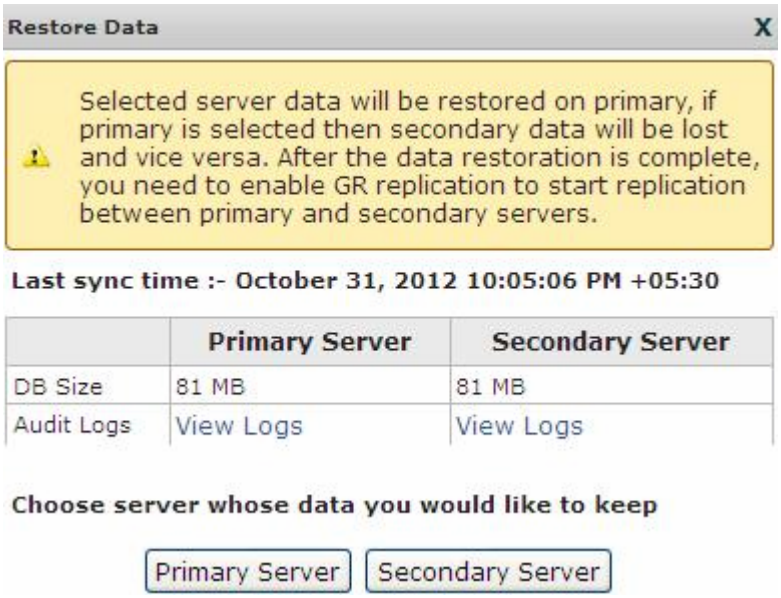
1. On the System Manager web console, click **Services** > **Geographic Redundancy**.
2. Click **Restore Data**.
3. On the Restore GR dialog box, select a server whose data you want to retain:
   - **Primary Server**

     The system keeps the primary System Manager server data. The data on the secondary System Manager server is lost.

     Select the secondary System Manager server if the secondary System Manager server data changes significantly during the interval between activation and deactivation and the administrator wants to retain those changes even after restoring the data using **Restore Data**.
   - **Secondary Server**

     The system restores the data from the secondary server on the primary System Manager server. the System Manager web console is unavailable for some time. The time that the system takes to restore depends on the network speed and the size of the data that the system must restore.

     After the system recovery, select the secondary System Manager server if the secondary System Manager server data changes significantly during the interval between the system recovery and the deactivation and if you want to retain the changes from the secondary System Manager server after restoring the data by using **Restore Data**.



System Manager displays the Restore Status dialog box.

System Manager displays the restore operation status and the status of the primary and the secondary System Manager server.

Important:

After you restore the data, all changes that you make on the secondary System Manager server that is active will not be available on the primary System Manager server.

4. If you later decide to revert to the database of the primary System Manager server, perform the following steps after the restore is complete:
   a. Using the command line interface, log in to System Manager of the primary server with administrator privilege CLI user credentials.
   b. Change to the `$MGMT_HOME/geo/bin` directory.
   c. Type `sh backupandrestore.sh recovery secondaryIP secondaryFQDN`.

      When the script completes, System Manager restarts and contains the data from the primary System Manager server that was available before you restored with the secondary System Manager data.

      Note:

      - To restore with the secondary System Manager server data again, activate and deactivate the secondary System Manager server.
      - Because the server becomes unavailable, you cannot gain access to the web console. Wait until the process is complete before you continue with the next step.

Next steps

Verify the data and deactivate the secondary System Manager server if the server is active during the restoration process.

Enable the Geographic Redundancy replication to synchronize the primary and secondary System Manager servers.

Verifying replication status between DC1 to DC2

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, in the **Application State** widget, verify the following states:
   - 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 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 `SECONDARY`
   - GR Server Mode is `STANDBY`
   - GR Replication is `ENABLED`
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 Workspaces for Call Center Elite 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 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.

Changing cluster activity status from Standby to Active for clusters in Data Center 1

Before you begin

Ensure that the OceanaMonitorService is installed on the clusters in Data Center 1.

Procedure

1. Open the Oceana Manager page in the DR location 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. 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**.

      The cluster status changes to `ACTIVE` and all nodes are placed in the Accept New Service mode.
   c. Click **OK** on the confirmation message box.
   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 primary Cluster 1 drop-down menu and start Oceana Monitor.

   On Cluster 1, verify the PUs deployed and status is **Intact** including CSC. CSC PU is not deployed if the **Oceana** > **CSC** > **AES** > **CM** configuration is not done 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 **Accepting**. If any clusters or nodes are in **Deny** state, then re-do the above steps or manually set them to **Accepting** state using the Avaya Breeze® platform EM cluster overview page.

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**.

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, skip the section on UCA DB restore.

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 1

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 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`.

Scheduling Database Backups UCMServer and UCAStoreService

About this task

Use this procedure to schedule automatic backups of the UCAStoreService/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 required service check box and click **Continue**.

    Select the **UCMService** and **UCAStoreService database** check boxes to be included in the backup.

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 time zone 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 UCAStoreService data in DC1

Before you begin

Uninstall UCAStoreService from 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, 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 DC1

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. Reboot 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.

Restore UCMService after Switchback

Backing up UCMService in DC2

About this task

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 switchback
- Unplanned switchover and switchback

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.
- You are not restoring the UCM DB from the DR site.

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 the Avaya Oceana® Cluster 1.
11. From the **Backup and Restore** field, select **Backup**.
12. On the Cluster Database Backup Confirmation dialog box, select the **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 UCMService data in DC1

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.
- Uninstall UCMService data from Avaya Oceana® Cluster 1 in Data Center 1.
- 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. Reboot Avaya Oceana® Cluster 1 and then Avaya Oceana® Cluster 3.

Pointing ACM to the new Omnichannel database server in DC2

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, host name, or IP address of the Omnichannel Database DR 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.

   For more information on configuring the Omnichannel certificate, refer to the *Retrieve certificate files* section in the *Deploying Avaya Oceana®* document.

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 160.

Switchback with OCP DB server - planned switchback

Prompting OCP DB Server A to primary server

About this task

Use this procedure to prompt the OCP DB Server A to primary server.

Procedure

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

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 node** > **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**. Verify the message when execution is complete.
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 page, do the following:
    a. Select the location where you want to save the backup file.

       Note:

       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.
    c. Click **Save**.
12. Click **Backup Database**.

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

Demoting OCP DB server C to async member (DR Server)

About this task

Use this procedure to demote the OCP DB server C to async member.

Procedure

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

1. Navigate to **CCDSINSTANCE** and click **Start Caché**.
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 node** > **Backup And Restore**.
6. Click **Mirror Configuration**.
7. In the **Select Mirror Scenario** field, select **Demote** to **Async**.

8. Click **Execute**. Verify the message when execution is complete.

Joining mirror for OCP DB server B as failover member (Standby Server)

About this task

Use this procedure to join mirror for the OCP DP Server B as failover member.

Procedure

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

1. Navigate to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement` folder.
2. Right-click the `OceanaDataManagementTool.exe` file and click **Run as administrator**.
3. In the navigation pane, click **Configuration** > **Mirror Settings** > **Join Mirror** .
4. In the **Type** attribute, select **Failover**.
5. Enter 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** check box 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, select the server certificate from the list.
    c. In the **File containing associated private key** field, select the key from the list.
    d. In the **Private key password** field, enter the new password.
7. Click **Save**.
8. Copy the backup file from the active Omnichannel Database server to the standby Omnichannel Database server in Data Center 1.
9. In the Oceana Data Management utility, click **Backup And Restore**.
10. In the navigation pane, click **Backup And Restore**.
11. In the **Select file to restore from** field, click **Browse**.
12. On the Open window, do the following:
    a. Browse to the location where you stored the backup file.
    b. Select the backup cbk file.
    c. Click **Open**.
13. Click **Restore Database**.

    The system displays the message:`Are you restoring a mirrored backup?`
14. Click **Yes**.
15. Click **Restore**.

    The utility displays the Restore complete! message when the restore process is complete.

Switching over from the primary to the secondary data center

About this task

Use this procedure to promote the secondary DC2 to the primary role after a DC1 failure.

Note:

- If testing, you must only perform this process during a maintenance window.
- The entire data center must fail over in this case. For example, it is not supported to run Avaya Oceana® on DC1 against Avaya Analytics™ on DC2.

Before you begin

- Check that the secondary DC2 data center is in standby mode.

Procedure

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

   `ccm release orca analytics`
4. Select **Geo/High Availability** by pressing the corresponding number.
5. Select **Geo options** by pressing the corresponding number.
6. Select **Switch over: Promote secondary data center database to primary** by pressing the corresponding number.
7. In the **Proceed to Geo switchover** field, enter `y`. Entering `n` cancels the operation.
8. In the **Continuing will switch over this data center to Primary data center** field, enter `y`.
9. Return to the previous page by entering `b`.
10. Quit the current page by entering `q`.
11. Return to the main menu by entering `m`.
12. Restart the following services using post install scripts, do the following:
    a. Run `Analytics Administration` script, use the following command:

       `ccm release orca analytics`.
    b. Select **Troubleshooting** > **General** > **Restart Measure Processors** and wait until all the measure processors are up.
    c. Restart orca-scheduler and orca-admin-data-service.
    d. Restart pod orca-database-rest.
13. Return to the previous page by entering `b`.
14. Quit the current page by entering `q`.

15. Return to the main menu by entering `m`.

Next steps

- Once the cause of the DC1 failure has been resolved and fixed, you can switch back from DC2 as the primary to DC1. To start that process, DC1 first needs to receive data replication from DC2. See Reversing data replication when the DC2 is the primary on page 81.

Related links

Disaster Recovery Process Checklist on page 80

Restoring Avaya Control Manager

You must restore Avaya Control Manager in DC1 after an unplanned switchover. Avaya Control Manager is restored from a backup before the failure. In a planned switchover or for a maintenance window, 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.

When there are failures of Avaya Oceana® applications, and 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.

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

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.

Restoring the External Data Mart server

About this task

Context Store External Data Mart (EDM) is an external component of Avaya Oceana®.

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 restore to Data Center 1, copy the EDM contents from Data Center 2 to the EDM in Data Center 1. Ensure that you backup and restore the database to complete the restoring of Context Store EDM.

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 the SQL Server domain user credentials with administrative right to all SQL Server(s) hosting the EDM on DC2.

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 the SQL Server domain user credentials with administrative right to all SQL Server(s) hosting the EDM on DC1.
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 CSEDM;
    GO
    sp_change_users_login @Action='update_one', @UserNamePattern='csEDMLogin',
    ```

```
@LoginName='csEDMLogin';
GO
```

Avaya Workspaces agent switchover

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

The default Avaya Workspaces URL for both locations are:

Primary Site: `https://<UAC Cluster IP/FQDN DC1>/services/UnifiedAgentController/workspaces/#/login`

DR Site: `https://<UAC Cluster IP/FQDN DC2>/services/UnifiedAgentController/workspaces/#/login`

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 the routing of the deployed channels.

Chapter 7: Resources

Documentation

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

Table continues…

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

Finding documents on the Avaya Support website

Procedure

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

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

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

8. Click to display the search results.

Avaya Documentation Center navigation

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

Important:

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

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

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

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

You can do the following:

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

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

  You can do the following:

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

Training

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

Table 1: Sales Credentials

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

Table 2: Pre-Sales Design

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

Table 3: Technical Services Partner Credentials

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

Table 4: Pre-requisite Courseware

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

Table 5: End User, Programmer, Administration

Avaya Learning Center				
Course code	**Course title**	**Course duration in hours**	**Delivery type**	**Vanity Link for Attachment**
ALEU-5002 Avaya Oceana® End-User Training				
24020W	Using Avaya Workspaces for Avaya Oceana® - Agent	1.0	Web-based Training	https://www.avaya.com/oceana-agent
24040W	Using Avaya Workspaces for Avaya Oceana® - Supervisor	1.0	Web-based Training	https://www.avaya.com/oceana-supervisor
ALUC-4001 Avaya Breeze® Client SDK				
2410W	Customer Communications and Apps with Oceana® for Developers	3.0	Web-based Training	
ASDC-0010 Avaya Workspaces® Framework				
24150W	Customizing the Avaya Workspaces® Framework	3.0	Web-based Training	
24150T	Avaya Workspaces® Framework R3 Test	1.0	Online Test	
ASAC-0005 Avaya Oceana® Administration				
21160W	Avaya Oceana® Fundamentals	0.5	Web-based Training	
24300V	Administering Avaya Oceana® R3 Omnichannel	40.0	Virtual Instructor-Led Training	Attached with the sale
2430T	Administering Avaya Oceana® R3 Online Test	1.0	Online Test	
24320W	Administering Avaya Oceana® - Basic	2.5	Web-based Training	https://www.avaya.com/Oceana-admin

Table continues…

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

Table 6: Other Miscellaneous Courseware

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

Support

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

Index

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W