Avaya Oceana® Solution Disaster Recovery

Release 3.5
Issue 1.1
November 2018

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

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.

Licenses

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

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

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located

at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, 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 G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its

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

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

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

Contents

Chapter 1: Introduction

Purpose

This document provides information about how to configure the disaster recovery functionality of Avaya Oceana® Solution and recover after a complete data center outage.

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

Changes in this release

Avaya Oceana® Solution Release 3.5 includes the following enhancements:

Avaya Analytics™ naming

In Avaya Analytics™ Release 3.5, Avaya Oceanalytics™ Insights has been renamed Avaya Analytics™.

WebRTC enhancements

Avaya Oceana® Solution 3.5 provides the following WebRTC enhancements:

- Voice call handling by Avaya Workspaces WebRTC agents
- WebRTC voice and video on the customer call leg
- WebRTC voice and video on the agent call leg
- Support for a maximum of 500 WebRTC agents
- Replacement of Avaya Mobile Video WebRTC components with Avaya Aura® Web Gateway

  The Avaya Aura® Web Gateway WebRTC solution:

  - Reduces footprint
  - Adds WebRTC component High Availability

  From this release, Avaya Oceana® Solution does not support Avaya Mobile Video WebRTC components.

Note:

In Avaya Oceana® Solution 3.5, WebRTC does not support transfer and conference.

Oracle Restricted Use License

Avaya Analytics™ uses certain embedded Oracle programs. The Oracle programs included in Avaya Analytics™ are subject to a restricted use license and can be used solely in conjunction with Avaya Analytics™.

In Customer environments with administrative practices for functions such as: backup, security, authentication and similar operational aspects, the Customer's administrator may access an Oracle database embedded in Avaya Analytics™ for the sole purpose of configuring the embedded database for use solely with Avaya Analytics™. Customer (or its administrator) may not add or make changes to the Oracle database schemas, metadata or data models other than through and/or as an extension of the functionality of Avaya Analytics™, including but not limited to: incorporating implementation reference data, dimensional and fact tables.

With regards to visual tools, including but not limited to Data Visualization and Stream Analytics, Customer will be permitted to access and administer the tools solely within the scope of Avaya Analytics™. The foregoing is meant to allow Customer access to metadata for visual tools; however, in the case of Avaya Analytics™ that distributes Oracle Database Enterprise Edition, Customer may not access or change the database schema other than through and/or as an extension of the functionality of Avaya Analytics™, including but not limited to: incorporating implementation reference data, dimensional and fact tables solely related to Avaya Analytics™.

Customer is fully responsible and liable to Avaya, its affiliates, and Oracle for any damages or losses caused by any unauthorized use of any of the Oracle programs embedded in Avaya Analytics™.

Chapter 2: Avaya Oceana® Solution disaster recovery overview

Avaya Oceana® Solution disaster recovery provides a planned approach to re-establish a critical service at a secondary data center when a complete outage occurs at the primary data center.

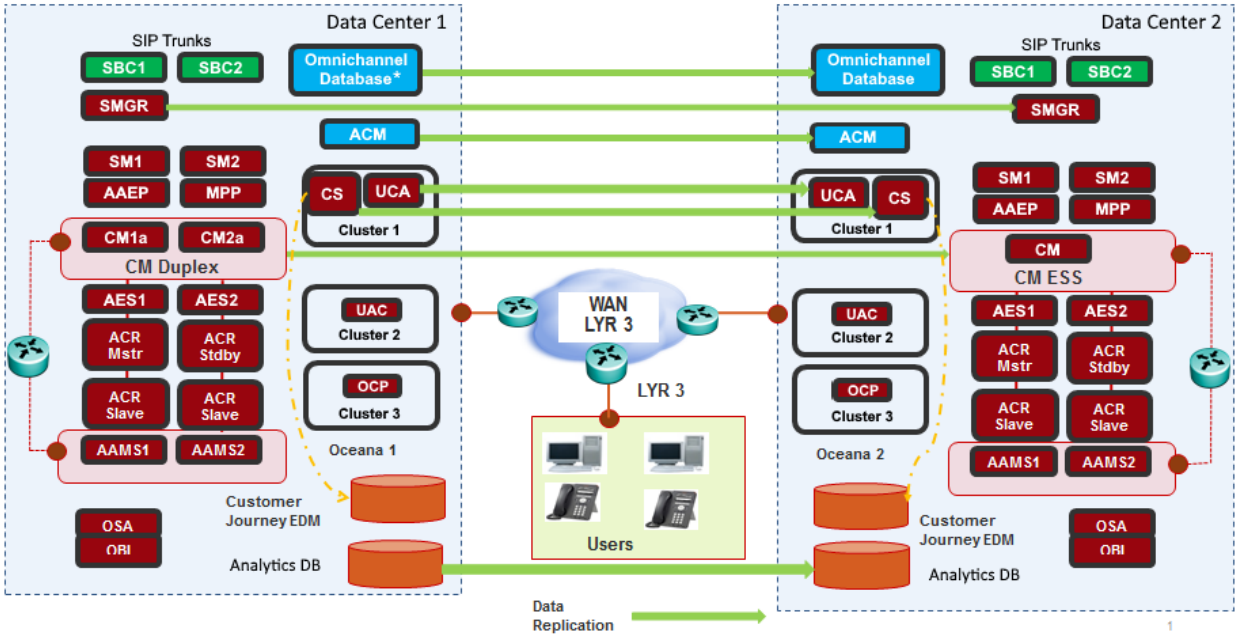
This document provides information on how to configure a geographically redundant Avaya Oceana® Solution so that when a primary data center outage occurs, the redundant site can be made operational. The secondary site has an updated copy of the required administration and reporting data so that the operations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

Note:

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

System architecture

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



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

Chapter 3: Failure modes

Failure modes

Failure mode	Description
Unplanned total outage of Data Center 1	This failure mode involves the failure of Avaya Oceana® Solution Contact Center components and Avaya Aura® Communication Manager telephony infrastructure. This failure mode results in an unavoidable system downtime and the loss of all alerting, queued, and in progress contacts. **Note:** This is the primary failure mode. Therefore, all disaster recovery procedures in this document describe how to address this failure mode.
Planned total outage of Data Center 1	This failure mode involves manual shutdown of Data Center 1. In this failure mode, the Avaya Oceana® Solution supports a maintenance mode. When in maintenance mode, the Avaya Oceana® Solution does not add any new contacts to the queue, so that agents can handle the existing queued contacts before the shutdown. This failure mode results in an unavoidable system downtime and the loss of all contacts that are still queueing.
Unplanned total outage of Avaya Oceana® Solution at Data Center 1	This failure mode involves the failure of Avaya Oceana® Solution components at Data Center 1. In this failure mode, you can switch the Contact Center functionality to Data Center 2 if the Aura infrastructure functionality is operational. Communication Manager and Application Enablement Services components continue to be operational in Data Center 1. This failure mode requires you to reconfigure the Avaya Oceana® Solution components at Data Center 2, and ensure

Table continues…

Failure mode	Description
	that the Avaya Oceana® Solution components point to Application Enablement Services at Data Center 1. **Important:** • Do not make any administration changes while Data Center 2 is functioning. If you make any changes, the Avaya Oceana® Solution handles the changes in the same manner as if there was an ESS switchover. • This failure mode does not support WebRTC voice and video calls.
Unplanned total outage of Communication Manager at Data Center 1	This failure mode involves the failure of Communication Manager at Data Center 1. If the failure of Communication Manager results ESS switchover to Data Center 2, you must manually switchover the Avaya Oceana® Solution components to Data Center 2. When you identify the failure of Communication Manager, you must immediately commence the manual switchover of all Avaya Oceana® Solution channels to ensure that the Avaya Oceana® Solution voice routing is operational without a delay.
Unplanned partial outage of Avaya Oceana® Solution components at Data Center 1	This failure mode involves the failure of one or more Avaya Oceana® Solution components at Data Center 1. When you identify the failure of a Avaya Oceana® Solution component, you must either recover the component at Data Center 1 or carry out a complete switchover to Data Center 2. When a partial failure occurs, you must determine whether the downtime to recover the components is preferable, or the disruption caused by a complete switchover is preferable.
Split WAN	This failure mode involves a WAN outage. Avaya Oceana® Solution does not support an active-active mode of operation. Therefore, if a split WAN occurs, Data Center 1 continues to operate in isolation from Data Center 2. The data replication for Avaya Aura® System Manager, Avaya Control Manager, Unified Collaboration Administration (UCA), and Omnichannel Provider (OCP) breaks temporarily.

Table continues…

Failure mode	Description
	After the WAN connection is restored, Avaya Oceana® Solution components synchronize data from Data Center 1 to Data Center 2. The synchronization depends on the WAN outage time. Avaya Oceana® Solution components can buffer only a limited number of changes that can be synchronized with Data Center 2 after recovery. Once the buffer limit is reached, the Avaya Oceana® Solution components start to overwrite oldest changed records. When an extended WAN outage occurs, it can be necessary to manually synchronize data from Data Center 1 to Data Center 2.

Chapter 4: Disaster Recovery deployment

Web Voice and Web Video requirements

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

A data center switch is done by changing the DNS mapping to the alternative data center. For example:

- Initial DNS mapping:
  - 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:
  - 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

Data Center 1 deployment

System Manager installation in Data Center 1

Install and configure System Manager in Data Center 1. For more information, see *Deploying Avaya Oceana® Solution*.

Note:

Configure trust certificates between System Manager and the LDAP provider on both instances of System Manager.

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

Before you begin

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

Procedure

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

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

   Important:

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

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

Setting the UCAStoreService attributes in Data Center 1

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze™** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. In the **Cluster** field, click Avaya Oceana® Cluster 1.
   b. In the **Service** field, click **UCAStoreService**.
3. In **Startup Configuration**, identify **Oceana disaster recovery role** and do the following:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, select `GEO_MASTER`.
4. In **Geographic Redundancy**, identify **Geographical server cluster name** 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 2.
5. Click **Commit**.

Enabling geo-redundancy in Context Store

About this task

Use this procedure to enable geo-redundancy in Context Store in Data Center 1

Before you begin

Create and download the keystore certificate from the System Manager web console by navigating to **Services** > **Security** > **Certificate** > **Authority**.

Procedure

1. On Avaya Breeze™, navigate to `/opt/Avaya/dcm/gigaspace/security/` and add the keystore certificate in each Avaya Breeze™ node in the cluster.

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

   Important:

   The replication does not work without the SSL encryption.
2. On the System Manager web console, click **Elements** > **Avaya Breeze** > **Configuration** > **Attributes**.

3. 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**.

       Configure the other geo attributes. All attributes related to geo-redundancy configuration are prefixed with GEO. For details, see the Enabling Geo redundancy in Context Store section in *Avaya Context Store Snap-in Reference*.
    c. Enter an appropriate value in each of the following fields:
        - **ContextStore ManagerSpace DataGrid Settings**
        - **ContextStoreSpace DataGrid Settings**
        - **EDM: Mirror Service container size**
4. Click **Commit**.
5. Repeat steps 1 to 4 for Avaya Oceana® Cluster 1 in Data Center 2.

Enabling External Data Mart

Before you begin

Create the database tables in the External Data Mart (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. In the **External Data Mart Configuration** in the **EDM: Enable Persistence to database** field, type `true`.
    d. Configure the other EDM attributes. For more information, see *Avaya Context Store Snap-in Reference*
    e. 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**.
4. Repeat steps 1 to 3 for Avaya Oceana® Cluster 1 in Data Center 2.

Communication Manager, ESS, and Application Enablement Services configuration

Configure Communication Manager according to the standalone deployment of Avaya Oceana® Solution. For more information, see *Deploying Avaya Oceana® Solution*.

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

Data Center 2 deployment

System Manager installation in Data Center 2

Install and configure System Manager in Data Center 2. For more information, see *Deploying Avaya Oceana® Solution*.

Note:

Configure trust certificates between System Manager and the LDAP provider on both instances of System Manager.

Installing services in Data Center 2

Procedure

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

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

2. In Data Center 2, install the same set and same version of the services that you installed in Data Center 1.

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

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

Before you begin

OceanaMonitorService must be 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. **(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. On the Oceana Manager page, do the following:
   a. Check the status of the clusters.
   b. If the status of the clusters is `ACTIVE`, click **Set Cluster Group to Standby** to change the status to `STANDBY`.
   c. On the confirmation message box, click **OK**.
   d. **(Optional)** If the Oceana Manager page does not display the updated status after some time, click **Refresh**.

Setting the UCAStoreService attributes in 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 Avaya Oceana® Cluster 1.
   b. In the **Service** field, click **UCAStoreService**.
3. In **Startup Configuration**, identify **Oceana disaster recovery role** and do the following:
   a. Select the **Override Default** check box.

b. In the **Effective Value** field, select `GEO_SLAVE`.

4. In **Geographic Redundancy**, identify **Geographical server cluster name** 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.
5. Click **Commit**.

Unified Collaboration Administration data synchronization

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

Before restoring the UCAStoreService to Data Center 2, you must uninstall the UCAStoreService from Avaya Oceana® Cluster 1 and Gigaspaces.

Note:

Reboot the cluster to ensure that the UCAStoreService is removed and reinstall the UCAStoreService once the restore is complete.

Taking a backup of UCAStoreService

About this task

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

Note:

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

Procedure

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

   System Manager displays the Backup Storage Configuration page.
3. In the **FQDN or IP Address** field, enter the FQDN or IP Address of the backup storage server.

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

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

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

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

    Note:

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

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

    Important:

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

Restoring the UCAStoreService data

About this task

Use this procedure to restore the UCAStoreService data.

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.
3. On the System Manager web console, click **Elements** > **Avaya Breeze™** > **Cluster Administration**.
4. From the **Backup and Restore** field, select **Restore**.
5. On the Backup and Restore Status page, in the Backup and Restore Jobs section, select the check box of the latest backup file and click **Restore**.
6. In the Cluster Database Restore Confirmation dialog box, select Avaya Oceana® Cluster 1 and click **Continue**.
7. On the Backup and Restore Status page, ensure that the **Status** column for the restore operation displays the value `Completed`.

Omnichannel Database Server installation

Install Omnichannel Windows Server in Data Center 1 and Data Center 2. For details, see *Deploying Avaya Oceana® Solution*.

Avaya Control Manager installation

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

Engagement Designer disaster recovery

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

Note:

Before starting Engagement Designer Designer Console, you must temporarily take the cluster out of the Denying mode.

You can customize Engagement Designer workflows by adding new interaction blocks to the workflow. While making these changes, ensure that any addresses required for these flows are

exposed as variables in Engagement Designer. Once the variables are available, you can configure these variables through Engagement Designer.

For example, the sample OceanaChatAssistedService workflow makes the OmniChannelDataServiceIP parameter available for editing. You can modify the OmniChannelDataServiceIP parameter through Engagement Designer to point to the local resources of the site where you deployed the OceanaChatAssistedService workflow.

Adding a Maintenance Mode flag to workflows

About this task

To facilitate a planned shutdown of Avaya Oceana® Solution Contact Center without losing the queued contacts, you must include a flag in Avaya Engagement Designer workflows specific to Avaya Oceana® Solution. By including a flag, you can put the workflows in Maintenance Mode. When you enable Maintenance Mode, new contacts are not added to the queue. However, the contacts which are already in the queue continue to be processed.

Note:

You must enable the Maintenance Mode flag for Chat, Web Voice, and Video.

Procedure

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

   `https://AOC1 FQDN>/services/EngagementDesigner/index.html`

   <AOC FQDN> is the FQDN of Avaya Oceana® Cluster 1 that you have added in the Windows hosts file.

2. Click **Properties** tab and do the following:

   a. Click **Add New Property**.

   b. In the **Name** field, enter `MaintenanceMode`.

   c. In the **Value** field, enter `false`.

   d. Click **OK**.

3. Open the workflow and verify that the **Exclusive Gateway** node is added after the **Start** node.

   The **Exclusive Gateway** node value is used to verify the value of Maintenance Mode. If the value is set to true, then the workflow terminates. If the value is set to false, then the workflow continues with normal operation.

Cache Mirroring configurations

Cache Mirroring with a backup server

Checklist for configuring Cache Mirroring with a backup server

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

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 25.	
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 27.	
3	Secure the Cache Mirror on the active Omnichannel Database server in Data Center 1.	See Securing the Cache Mirror on the active Omnichannel Database server in Data Center 1 on page 29.	
4	Secure the Cache Mirror on the backup Omnichannel Database server in Data Center 2.	See Securing the Cache Mirror on the backup Omnichannel Database server in Data Center 2 on page 30.	

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. 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. On Cache Management Portal, click **System Administration** > **Configuration** > **Mirror Settings** > **Enable Mirror Service**.
4. On the Edit Service dialog box, select the **Service Enabled** check box and click **Save**.
5. 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**.
6. In the Services window, do the following:
    a. Double-click the ISCAgent service.
    b. In the Properties dialog box, click **Start**.
    c. In **Startup type**, select **Automatic**.
    d. Click the **Recovery** tab.
    e. In the **First failure**, **Second failure**, and **Subsequent failures** fields, select the **Restart the Service** option.
    f. In the **Reset fail count after** field, type `120`.
    g. In the **Restart service after** field, type `0`.
    h. Click **Apply**.
    i. Click **OK**.
7. On Cache Management Portal, click **System Administration** > **Configuration** > **Mirror Settings** > **Create Mirror**.
8. On the Create Mirror page, do the following:
    a. In the **Mirror Name** field, type `AOCMIRROR`.
    b. **(Optional)** If you do not require a secure connection, clear the **Use SSL/TLS** check box.

        If you select this check box, you must provide the details of the certificate to use for TLS.
    c. Clear the **Use Arbiter** check box.
    d. Clear the **Use Virtual IP** check box.
    e. In the **Port** field, enter the port number as `2188`.

f. Click **Save**.

9. On Cache Management Portal, take a backup of the database by doing the following:
   a. Click **Menu** > **Configure Databases** > **Add to mirror**.
   b. Select the **MULTIMEDIA_DATA** and **COBROWSE_DATA** check boxes, and then click **Add**.
10. Go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\Oceana\BackupAndRestore` folder.
11. Double-click the `BackupAndRestore.exe` file.
12. In the **Select/create file to backup to** field, click **Browse**.
13. 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.
    c. Click **Save**.
14. Click **Backup Database**.

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

    Note:

    The drive where you store the backup `zip` file must have sufficient space to store the backup `zip` file and the `cbk` file that you extract from the `zip` file.

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

Procedure

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

   `http://<DC2OmnichannelServerIP>:57772/csp/sys/UtilHome.csp`

   <DC2OmnichannelServerIP> is the IP address of the backup Omnichannel Database server in Data Center 2.
2. On the Cache Management Portal login page, do the following:
   a. In the **User Name** field, type `_admin`.
   b. In the **Password** field, type `Oceana16`.
   c. Click **LOGIN**.
3. On Cache Management Portal, click **System Administration** > **Configuration** > **Mirror Settings** > **Enable Mirror Service**.

4. On the Edit Service dialog box, select the **Service Enabled** check box and click **Save**.
5. 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**.
6. In the Services window, do the following:
    a. Double-click the ISCAgent service.
    b. In the Properties dialog box, click **Start**.
    c. In **Startup type**, select **Automatic**.
    d. Click the **Recovery** tab.
    e. In the **First failure**, **Second failure**, and **Subsequent failures** fields, select the **Restart the Service** option.
    f. In the **Reset fail count after** field, type `120`.
    g. In the **Restart service after** field, type `0`.
    h. Click **Apply**.
    i. Click **OK**.
7. On Cache Management Portal, click **System Administration** > **Configuration** > **Mirror Settings** > **Join as Async**.
8. On the Join as Async page, do the following:
    a. In the **Mirror Name** field, type `AOCMIRROR`.
    b. In the **Agent Address on Failover System** field, enter the IP address of the active Omnichannel Database server in Data Center 1.
    c. In the **Cache Instance Name** field, type `CCDSINSTANCE`.
    d. Click **Save**.
9. Close the Cache Management Portal window before starting the restore process.

    If you do not close the Cache Management Portal window, Cache Management Portal displays an error message.
10. Copy the backup `zip` file from the active Omnichannel Database server in Data Center 1 to the backup Omnichannel Database server in Data Center 2.

    Important:

    - Ensure that you copy the correct backup `zip` file that you created on the active Omnichannel Database server.
    - The drive where you store the backup `zip` file must have sufficient space to store the backup `zip` file and the `cbk` file that you extract from the `zip` file.

11. Go to the location where you copied the backup `zip` file.
12. Extract the `zip` file to obtain the `cbk` file.
13. Go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\Oceana\BackupAndRestore` folder.
14. Double-click the `BackupAndRestore.exe` file.
15. In the **Select file to restore from** field, click **Browse**.
16. 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**.
17. On the Backup and Restore screen, click **Restore Database**.
18. For **Are you restoring a mirrored backup**, click **Yes**.
19. On the Drive restore screen, do the following:
    a. In the **Select your database drive letter** field, select the drive where you installed the Omnichannel database.

       For example, `(MULTIMEDIA drive):\Avaya\CCMM\Databases\CCMM\COBROWSE\DATA`.
    b. 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.
20. 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® Solution databases in the list.

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

Before you begin

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

Procedure

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. On Cache Management Portal, click **System Administration** > **Configuration** > **Mirror Settings** > **Edit Mirror**.
4. On the Edit Mirror page, click **Set up SSL/TLS**.
5. On the Edit SSL/TLS Configurations for Mirror page, do the following:
   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 type** field, select the type of key.
   e. In the **Password** field, select **Enter new password**.
   f. In the **Private key password** field, enter the new password.
   g. In the **Private key password (confirm)** field, reenter the password.
   h. In the **Protocols** field, select the appropriate protocol.
   i. Click **Save**.
6. On the Edit Mirror page, do the following:
   a. Click **Verify SSL**.
   b. On the Verification dialog box, click **Okay** after successful verification.
   c. Select the **Use SSL/TLS** check box.
   d. Click **Save**.

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

Before you begin

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

Procedure

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

   `http://<DC2OmnichannelServerIP>:57772/csp/sys/UtilHome.csp`

<DC2OmnichannelServerIP> is the IP address of the backup Omnichannel Database server in Data Center 2.

2. On the Cache Management Portal login page, do the following:
   a. In the **User Name** field, type `_admin`.
   b. In the **Password** field, type `Oceana16`.
   c. Click **LOGIN**.
3. On Cache Management Portal, click **System Administration** > **Configuration** > **Mirror Settings** > **Edit Async**.
4. On the Edit Async page, click **Set up SSL/TLS**.
5. On the Edit SSL/TLS Configurations for Mirror page, do the following:
   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 type** field, select the type of key.
   e. In the **Password** field, select **Enter new password**.
   f. In the **Private key password** field, enter the new password.
   g. In the **Private key password (confirm)** field, reenter the password.
   h. In the **Protocols** field, select the appropriate protocol.
   i. Click **Save**.
6. On the Edit Async page, do the following:
   a. Click **Verify SSL**.
   b. On the Verification dialog box, click **Okay** after successful verification.
   c. Select the **Use SSL/TLS** check box.
   d. Click **Save**.

Cache Mirroring with failover and backup servers

Checklist for configuring Cache Mirroring with failover and backup servers

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

No.	Task	Description	✔
1	Configure Omnichannel Database High Availability (HA) with active and standby Omnichannel Database servers within Data Center 1.	See *Deploying Avaya Oceana® Solution*.	
2	Secure the Cache Mirror on the backup Omnichannel Database server in Data Center 2.	See Securing the Cache Mirror on the backup Omnichannel Database server in Data Center 2 on page 30.	
3	Authorize the backup Cache Mirror on the active Omnichannel Database servers in Data Center 1.	See Authorizing the backup Cache Mirror on the active Omnichannel Database server on page 32.	
4	Authorize the backup Cache Mirror on the standby Omnichannel Database servers in Data Center 1.	See Authorizing the backup Cache Mirror on the standby Omnichannel Database server on page 33.	

Authorizing the backup Cache Mirror on the active Omnichannel Database server

Procedure

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

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

   <ActiveOmnichannelServerIP> is the IP address of the 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 from the Cache Management Portal on the backup Omnichannel Database server by clicking **System Administration** > **Configuration** > **Mirror Settings** > **Edit Async**.

6. Click **Save**.

Authorizing the backup Cache Mirror on the standby Omnichannel Database server

Procedure

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

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

   <StandbyOmnichannelServerIP> is the IP address of the server containing the standby 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 from the Cache Management Portal on the backup Omnichannel Database server by clicking **System Administration** > **Configuration** > **Mirror Settings** > **Edit Async**.
6. Click **Save**.

Adding Context Store addresses for Data Center 1 and Data Center 2 in Avaya Aura® Experience Portal

About this task

Use this procedure to add Context Store addresses for Data Center 1 and Data Center 2 in Experience Portal so that, Experience Portal can continue to interact with Context Store during a switchover.

Procedure

1. Log in to Avaya Aura® Experience Portal with administrator user role.
2. Click **System Configuration** > **EPM Server** > **Data Storage Settings**.
3. Expand **Engagement Development Platform**.
4. In the **Context Store Address** field, enter the IP address of both Data Center 1 and Data Center 2, separated by | character.

Configuring Avaya Analytics™

Configuring Oracle Data Guard

Avaya Analytics™ supports Oracle Data Guard where one instance of Oracle® Database runs on two virtual servers: a Primary server and a Standby server. You can use the Oracle Data Guard feature for disaster recovery. Using this feature, you can recover after a complete outage of your primary data center. For more information about deploying and configuring Oracle Data Guard for disaster recovery, see *Deploying Avaya Analytics™ for Oceana™*.

Chapter 5: Switchover

Planned maintenance of Avaya Oceana® Solution components

Overview

For a planned switchover to Data Center 2 without losing any queued contacts:

- Configure Contact Center to prevent additional contacts from being added to queues.
- Enable agents to process the currently queued contacts.
- Clear queued contacts before the shutdown of Data Center 1.

Using Avaya Workspaces, you can view real-time reports to monitor queues.

Voice channel shutdown

For a planned shutdown of the Voice channel, Avaya Aura® Experience Portal must have a flag at the start of the workflow. 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.

Configuring EmailService shutdown

About this task

For a planned switchover of EmailService, an administrator must shut down EmailService on Data Center 1 by using a flag in Avaya Oceana® Cluster 3. When the administrator shuts down the EmailService:

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

On completion of the switchover, emails are sent from Data Center 2.

Procedure

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

      Ensure that you also set this value to `true` on Data Center 2.
4. Click **Commit**.

Setting the MaintenanceMode attribute for Chat

Before you begin

In the Windows hosts file, add an entry containing the Cluster IP address and FQDN of Avaya Oceana® Cluster 1. The FQDN in the entry must be different from the FQDNs of Avaya Oceana® Cluster 1 nodes.

Procedure

1. In your web browser, enter the following URL to open the Engagement Designer administration web console:

   `https://<AOC1 FQDN>/services/EngagementDesigner/admin.html`

   <AOC1 FQDN> is the FQDN of Avaya Oceana® Cluster 1 that you have added in the Windows hosts file.
2. On the Workflows tab, select the Chat workflow and click **Attributes**.
3. On the Workflow Attributes tab, do the following:
   a. Change the value of the **MaintenanceMode** field from `False` to `True`.
   b. Click **Close**.

Setting the MaintenanceMode attribute for SMS

About this task

The SMS channel utilizes a third-party gateway component that reads the incoming SMS messages from the network provider.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze™** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. **Cluster**: Select Avaya Oceana® Cluster 3.
   b. **Service**: Select WebTextConnector Snap-in.
3. For **MaintenanceMode**:
   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 MaintenanceMode attribute for SocialConnector

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze™** > **Configuration** > **Attributes**.
2. Click **Service Cluster** tab, and do the following:
   a. **Cluster**: Select Avaya Oceana® Cluster 3.
   b. **Service**: Select SocialConnector.
3. For **MaintenanceMode**:
   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

About this task

For a planned switchover, you must modify the Engagement Designer workflow and change the workflow into a Maintenance mode. In the Maintenance mode, the workflow rejects any new contacts but processes the existing contacts.

Important:

You must appropriately set the Maintenance mode for the Web Voice and Web Video workflows in Data Center 1 and Data Center 2. For example, if you set the Maintenance mode in Data Center 1 as `True`, then you must set the Maintenance mode in Data Center 2 as `False`.

Before you begin

In the Windows hosts file, add an entry containing the Cluster IP address and FQDN of Avaya Oceana® Cluster 1. The FQDN in the entry must be different from the FQDNs of Avaya Oceana® Cluster 1 nodes.

Procedure

1. In your web browser, enter the following URL to open the Engagement Designer administration web console:

   `https://<AOC1 FQDN>/services/EngagementDesigner/admin.html`

   <AOC1 FQDN> is the FQDN of Avaya Oceana® Cluster 1 that you have added in the Windows hosts file.
2. On the Workflows tab, select the Web Voice workflow and click **Attributes**.
3. On the Workflow Attributes tab, do the following:
   a. Change the value of the **MaintenanceMode** field from `False` to `True`.
   b. Click **Close**.
4. Repeat Step 2 and Step 3 for the Web Video workflow.

Outbound shutdown

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

Switchover from Avaya Aura® Communication Manager to ESS

You must shutdown the Communication Manager in Data Center 1 so that the ESS in Data Center 2 can come into operation. The phonesets and gateways re-register with the ESS. Once the registration is complete, the agents can start handling voice contacts that are routed through Avaya Aura® Call Center Elite.

Switching the voice traffic to Data Center 2

Procedure

1. Log in to the Avaya Aura® 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**.

Shutdown of Data center 1 services

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

Before you begin

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

Procedure

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

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

   Important:

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

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

System Manager switchover

Checklist for Avaya Aura® System Manager switchover

No.	Task	Description	Notes	✔
1	Disable the Geographic Redundancy replication	Disable Avaya Aura® System Manager Geographic Replication at Data Center 1.	For more information, see Administering Avaya Aura® System Manager	
2	Shut down System Manager at Data Center 1	Avaya Aura® System Manager must be shut down in order to trigger the Breeze snap-ins to switch to the SMGR instance at Data Center 2.	For more information, see Administering Avaya Aura® System Manager	
3	Activate System Manager at Data Center 2	Activate Avaya Aura® System Manager at Data Center 2.	For more information, see Administering Avaya Aura® System Manager	
4	Verify the Breeze node controller	Confirm that the Breeze nodes are switched from System Manager in Data Center 1 to System Manager in Data Center 2.	For more information, see Verifying Breeze node controller on page 55.	

Verifying Avaya Breeze™ node controller for Data Center 2

About this task

Use this procedure to verify, that the Avaya Breeze™ nodes are switched from System Manager in Data Center 1 to System Manager in Data Center 2.

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™ nodes.

Omnichannel Database switchover

You must manually switchover the Omnichannel Database server in Data Center 1 to the Omnichannel Database server in Data Center 2. The switchover procedure varies depending on the status of the Omnichannel Database server in Data Center 1.

Note:

Do not restart the cluster.

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

Promoting the async server when active and async servers are available

About this task

Use this procedure to promote the async server in Data Center 2 when the active server in Data Center 1 and async server in Data Center 2 are available.

Before you begin

Deploy the following Omnichannel Database servers:

- Server A as the active server in Data Center 1
- Server B as the async server in Data Center 2

Procedure

1. On Server B, do the following:
   a. Go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\Oceana\BackupAndRestore` folder.
   b. Double-click the `BackupAndRestore.exe` file.
   c. Click **Mirror Configuration**.
   d. In the **Select mirror scenario** field, select `Switchover Cache up on both servers`.
   e. Click **Execute**.

      Important:

      The process can take up to 30 seconds. Do not close the terminal window.
2. On Server A, do the following:
   a. From the Windows system tray, right-click the **Cache** icon and click **Start Cache** to start the Cache.
   b. After starting the Cache, go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\Oceana\BackupAndRestore` folder.

c. Double-click the `BackupAndRestore.exe` file.

d. Click **Mirror Configuration**.

e. In the **Select mirror scenario** field, select `Demote to Async`.

f. Click **Execute**.

Promoting the async server when Data Center 1 is offline

About this task

Use this procedure to promote the async server in Data Center 2 when Data Center 1 is offline.

Before you begin

Deploy the following Omnichannel Database servers:

- Server A as the active server in Data Center 1
- Server B as the async server in Data Center 2

Procedure

On Server B, do the following:

a. Go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\Oceana\BackupAndRestore` folder.

b. Double-click the `BackupAndRestore.exe` file.

c. Click **Mirror Configuration**.

d. In the **Select mirror scenario** field, select `Switchover primary server down`.

e. Click **Execute**.

Promoting the async server after failure of the active server

About this task

Use this procedure to promote the async server in Data Center 2 after failure of the active server in Data Center 1.

Before you begin

Deploy the following Omnichannel Database servers:

- Server A as the active server in Data Center 1
- Server B as the async server in Data Center 2

Procedure

On Server B, do the following:

a. Go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\Oceana\BackupAndRestore` folder.

b. Double-click the `BackupAndRestore.exe` file.

c. Click **Mirror Configuration**.

d. In the **Select mirror scenario** field, select `Switchover Primary server down`.

e. Click **Execute**.

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

Promoting the async server when active, standby, and async servers are available

About this task

Use this procedure to promote the async server in Data Center 2 when the active and standby servers in Data Center 1 and async server in Data Center 2 are available.

Before you begin

Deploy the following Omnichannel Database servers:

- Server A as the active server in Data Center 1
- Server B as the standby server in Data Center 1
- Server C as the async server in Data Center 2

Remove Cache Mirroring from Server B in Data Center 1. For information about how to remove Cache Mirroring, see *Deploying Avaya Oceana® Solution*.

Procedure

1. Remove Cache Mirroring from Server B in Data Center 1.

   For information about how to remove Cache Mirroring, see *Deploying Avaya Oceana® Solution*.

2. On Server C, do the following:
   a. Go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\Oceana\BackupAndRestore` folder.
   b. Double-click the `BackupAndRestore.exe` file.
   c. Click **Mirror Configuration**.
   d. For **Select mirror scenario**, select `Switchover Cache up on both servers`.
   e. Click **Execute**.

      Important:

      The process can take up to 30 seconds. Do not close the terminal window.

3. On Server A, do the following:
   a. Right-click the Cache icon to start the Cache.
   b. Once the Cache is up, run `BackupAndRestore.exe`
   c. Click **Mirror Configuration**.

d. For **Select mirror scenario**, select `Demote to Async`.

e. Click **Execute**.

Promoting the async server when Data Center 1 is offline

About this task

Use this procedure to promote the async server in Data Center 2 when Data Center 1 is offline.

Before you begin

Deploy the following Omnichannel Database servers:

- Server A as the active server in Data Center 1
- Server B as the standby server in Data Center 1
- Server C as the async server in Data Center 2

Procedure

On Server C, do the following:

a. Go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\Oceana\BackupAndRestore` folder.

b. Double-click the `BackupAndRestore.exe` file.

c. Click **Mirror Configuration**.

d. In the **Select mirror scenario** field, select `Switchover primary server down`.

e. Click **Execute**.

Promoting the async server after failure of active and standby servers

About this task

Use this procedure to promote the async server in Data Center 2 after failure of active and standby servers in Data Center 1.

Before you begin

Deploy the following Omnichannel Database servers:

- Server A as the active server in Data Center 1
- Server B as the standby server in Data Center 1
- Server C as the async server in Data Center 2

Procedure

On Server C, do the following:

a. Go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\Oceana\BackupAndRestore` folder.

b. Double-click the `BackupAndRestore.exe` file.

c. Click **Mirror Configuration**.

d. In the **Select mirror scenario** field, select `Switchover Primary server down`.

e. Click **Execute**.

Oracle® Database switchover from DC1 to DC2

Switching over to the Standby Oracle® Database

About this task

In an Oracle Data Guard configuration, an instance of Oracle® Database runs on two separate servers: a Primary server and a Standby server, each installed at a different Data Center. You can switch over to the Standby server at any time without the risk of data loss. Use this procedure to perform a switchover.

Procedure

Connect to the Primary Oracle® Database *orcl* and run the following command to switch over to the Standby Oracle® Database *orcl_stby*.

$ dgmgrl sys/Avaya123@orcl

```
DGMGRL for Linux: Version 12.1.0.2.0 - 64bit Production

Copyright (c) 2000, 2013, Oracle. All rights reserved.

Welcome to DGMGRL, type "help" for information.
Connected as SYSDBA.
```

```
DGMGRL> SWITCHOVER TO orcl_stby;
Performing switchover NOW, please wait...
Operation requires a connection to instance "orcl" on database "orcl_stby"
Connecting to instance "orcl"...
Connected as SYSDBA.
New primary database "orcl_stby" is opening...
Operation requires start up of instance "orcl" on database "orcl"
Starting instance "orcl"...
ORACLE instance started.
Database mounted.
Switchover succeeded, new primary is "orcl_stby"
DGMGRL>
```

Checking the status on the original Primary Oracle® Database post switchover

About this task

Perform this procedure on the original Primary Oracle® Database to confirm the switchover was successful.

Procedure

Type `show database orcl;`.

The screen displays the following:

```
Database - orcl
  Role:               PHYSICAL STANDBY
  Intended State:     APPLY-ON
  Transport Lag:      0 seconds (computed 1 second ago)
  Apply Lag:          0 seconds (computed 1 second ago)
  Average Apply Rate: 24.00 KByte/s
  Real Time Query:    OFF
  Instance(s):
    orcl
Database Status:
SUCCESS
DGMGRL>
```

Checking the status on the new Primary Oracle® Database post switchover

About this task

Perform this procedure on the new Primary Oracle® Database to confirm the switchover was successful.

Procedure

Type `show database orcl;`.

The screen displays the following:

```
Database - orcl_stby
  Role:               PRIMARY
  Intended State:     TRANSPORT-ON
  Instance(s):
    orcl
Database Status:
SUCCESS
DGMGRL>
```

Oracle® Database switchover from DC2 to DC1

Switching back to the Primary Oracle® Database

About this task

Use this procedure to switch back to the original Primary Oracle® Database.

Procedure

On the new Primary Oracle® Database *orcl_stby* , run the following command to switch over to the new Standby Oracle® Database *orcl*.

$ dgmgrl sys/Password1@orcl_stby

```
DGMGRL for Linux: Version 12.1.0.2.0 - 64bit Production

Copyright (c) 2000, 2013, Oracle. All rights reserved.
```

```
Welcome to DGMGRL, type "help" for information.
Connected as SYSDBA.
```

```
DGMGRL> SWITCHOVER TO orcl;
Performing switchover NOW, please wait...
Operation requires a connection to instance "orcl" on database "orcl"
Connecting to instance "orcl"...
Connected as SYSDBA.
New primary database "orcl" is opening...
Operation requires start up of instance "cdb1orcl" on database "orcl_stby"
Starting instance "orcl"...
ORACLE instance started.
Database mounted.
Switchover succeeded, new primary is "orcl"
DGMGRL>
```

Checking the status on the Primary Oracle® Database after switching back

About this task

Perform this procedure on the original Primary Oracle® Database to confirm that the switchover was successful.

Procedure

Type `show database orcl;`.

The screen displays the following:

```
DGMGRL> show database orcl
Database - orcl
  Role:               PRIMARY
  Intended State:     TRANSPORT-ON
  Instance(s):
    orcl
Database Status:
SUCCESS

DGMGRL>
```

Checking the status on the Standby Oracle® Database after switching back

About this task

Perform this procedure on the original Standby Oracle® Database to confirm that the switchover was successful.

Procedure

Type `show database orcl;`.

The screen displays the following:

```
Database - orcl_stby
  Role:               PHYSICAL STANDBY
  Intended State:     APPLY-ON
  Transport Lag:      0 seconds (computed 0 seconds ago)
  Apply Lag:          0 seconds (computed 0 seconds ago)
  Average Apply Rate: 4.00 KByte/s
  Real Time Query:    OFF
  Instance(s):
    orcl
```

```
Database Status:
SUCCESS
DGMGRL>
```

Oracle® Database failover

About this task

In an Oracle Data Guard configuration, if the Primary Oracle® Database or the Data Center fails, use this procedure to fail over to the Standby Oracle® Database.

Important:

The installation script for Oracle® Database enables database flashback by default, which allows you to reinstate the original Primary Oracle® Database as the Standby. Database flashback expires after 24 hours; you must reinstate the original Primary Oracle® Database within this time. If you do not reinstate the original Primary Oracle® Database within 24 hours, you must rebuild a new Standby server.

Procedure

1. Run the following command on Standby Oracle® Database *orcl_stby*:

   $ dgmgrl sys/Avaya123@orcl_stby

   ```
   DGMGRL for Linux: Version 12.1.0.2.0 - 64bit Production

   Copyright (c) 2000, 2013, Oracle. All rights reserved.

   Welcome to DGMGRL, type "help" for information.
   Connected as SYSDBA.
   DGMGRL> FAILOVER TO orcl_stby;
   Performing failover NOW, please wait...
   Failover succeeded, new primary is "orcl_stby"
   DGMGRL>
   ```

   Note:

   Back up the new Primary Oracle® Database immediately.

2. On the original Primary Oracle® Database, type the following command to reinstate the database:

   REINSTATE DATABASE orcl

   ```
   Reinstating database "orcl", please wait...
   Operation requires shut down of instance "orcl" on database "orcl"
   Shutting down instance "orcl"...
   ORACLE instance shut down.
   Operation requires start up of instance "orcl" on database "orcl"
   Starting instance "orcl"...
   ORACLE instance started.
   Database mounted.
   Continuing to reinstate database "orcl" ...
   Reinstatement of database "orcl" succeeded
   DGMGRL>
   ```

Enable Avaya Oceana® Solution components in DC2

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

Before you begin

OceanaMonitorService must be 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. **(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. On the Oceana Manager page, do the following:
   a. Verify that the status of the clusters is `STANDBY`.
   b. Click **Set Cluster Group to Active** to change the status to `ACTIVE` and place all nodes in the Accept New Service mode.
   c. On the confirmation message box, click **OK**.
   d. **(Optional)** If the Oceana Manager page does not display the updated status after some time, click **Refresh**.

Configuring the Web Voice and Web Video switchover

Procedure

1. In Data Center 1, set the state of the AvayaMobileCommunications cluster to `Denying`.
2. In Data Center 2, set the state of the AvayaMobileCommunications cluster to `Accepting`.
3. 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.

4. 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.
5. Change the DNS mapping of the AvayaMobileCommunications cluster FQDN to map to the public address of the AvayaMobileCommunications cluster in Data Center 2.
6. In Data Center 1, set the Maintenance mode for the Web Voice and Web Video workflows to `True`.
7. In Data Center 2, set the Maintenance mode for the Web Voice and Web Video workflows to `False`.

   After the DNS changes take effect, all new call requests from web and mobile clients go to Data Center 2.

Control Manager switchover

Automated switchover

The Control Manager high availability service monitors the SQL server instance and a switchover is triggered if the service is unable to connect to the database on the primary site.

Manual switchover

To trigger a manual switchover shut down the SQL server service is on the primary data center. Once the Avaya Control Manager high-availability service detects that the database connection has been lost, it reconfigures both Avaya Control Manager servers to connect to the database in Data Center 2. It also stops the services on Data Center 1 and starts the services on Data Center 2.

Switching over Avaya Control Manager manually

About this task

In some cases, the Avaya Control Manager instance in Data Center 2 does not update the database connection when a complete outage occurs in the Avaya Control Manager instance in Data Center 1. Use the procedure below as a workaround to switch over Avaya Control Manager when a complete outage occurs in the Avaya Control Manager in the Data Center 1.

Procedure

1. Stop the high-availability service on the secondary application server that is on ACM-APP-2.
2. On the ACM-APP-2 server, ensure that the high-availability service is set to the Manual mode.

   This is to ensure that the service does not start automatically during the procedure.

3. On the ACM-APP-2 server, update the`C:\Windows \System32\Nav360Config.xml` file to point the connection string to the secondary database.
4. Ensure that the `C:\Windows\Syswow64\Nav360Config.xml` file is also auto-updated with the change you made in `C:\Windows\System32\Nav360Config.xml` file.
5. On the ACM-APP-2 server., start the Audit Log and License Tracker services.

   Supervisors and administrators must use the new url for Avaya Control Manager instance in Data Center 2 after the switchover.

Reconfiguring Avaya Oceana® Solution settings with Avaya Control Manager

Configuring the Communication Manager IP address

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Team Engagement** > **Communication Manager**.
2. On the Communication Manager List page, select the check box for Communication Manager and click **Edit**.
3. In the following fields, enter the Communication Manager details:

   In the **CM IP Address** field, replace the CM IP address from Data Center 1 with the ESS IP address from Data Center 2.

   The new IP address communicates with the ESS in Data Center 2.
4. Click **Save**.

Configuring the UCA URL to point to Data Center 2

About this task

Use this procedure to update the Oceana Server Details within Avaya Control Manager to point to the Avaya Oceana® Cluster 1 address in Data Center 2.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Server Details**.
2. On the Avaya Oceana Server List page, double-click the UCAServer server.
3. On the Avaya Oceana Server Edit page, in the **API URL** field, update the URL to point to the Avaya Oceana® Cluster 1 address in Data Center 2.

Configuring access to Omnichannel Administration Utility

About this task

Use this procedure to re-configure Avaya Control Manager to start Omnichannel Administration Utility from the **Launch OC Database Administration Client** tile on the Avaya Control Manager web interface.

Before you begin

Remove the OCP administration client from the primary system, before starting it from the Omnichannel server instance in Data Center 2.

Procedure

1. Log on to Avaya Control Manager.
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 IP address pointing to the Omnichannel server in Data Center 2.

Agent switchover

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

Chapter 6: Recovery and switchover

Recovery to primary Data Center from Data Center 2 to Data Center 1

After failure, once the Data Center 1 is functional and ready to resume contact processing, you must re-instate Data Center 1 as the operational data center. The disaster recovery at Data Center 2 functions only for a limited time period due to the licensing restrictions with ESS.

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

Note:

You need a maintenance window to perform the recovery. During this maintenance window, all incoming contacts are rejected.

Preparing Data Center 1

Configuring UCA as standalone in Data Center 1

Procedure

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

5. Restart the cluster.

Traffic shutdown of Data Center 2

For the traffic shutdown of the Data Center 2, ensure that all the queued contacts are cleared. For details on how to perform the shutdown, see *Planned maintenance of Oceana components*.

Note:

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

Avaya Aura® System Manager switchover from DC2 to DC1

Checklist for Avaya Aura® System Manager switchover

No.	Task	Description	Notes	✔
1	Deactivate the secondary System Manager server	Deactivate the secondary System Manager server.	For more information, see Administering Avaya Aura® System Manager	
2	Restore the primary System Manager server	Once you deactivate the secondary System Manager server, restore the Primary System Manager server.	For more information, see Administering Avaya Aura® System Manager	
3	Verify the Breeze node controller	Confirm that the Breeze nodes are switched from System Manager in Data Center 2 to System Manager in Data Center 1.	-	

Verifying Avaya Breeze™ node controller

About this task

Use this procedure to verify, that the Avaya Breeze™ nodes are switched from System Manager in Data Center 2 to System Manager in Data Center 1.

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™ nodes.

Switch over from ESS to Avaya Aura® Communication Manager

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 EmailService on recovery of Data Center 1

About this task

On recovery of Data Center 1, you must start EmailService on Data Center 1 by using a flag in Avaya Oceana® Cluster 3.

Procedure

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

      Ensure that you also set this value to `false` on Data Center 2.

4. Click **Commit**.

Configuring CallServerConnector attributes on Data Center 2

About this task

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

Procedure

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

Switching over of Voice to Data Center 1

Procedure

1. On the Experience Portal Management Web Console, click **System Configuration** > **Applications**
2. In the **Active Data Center** field, select **Data Center1**.
3. Click **Save**.

Restoring UCA

Taking a backup of UCAStoreService in Data Center 2

About this task

Use this procedure to take a backup of UCAStoreService. This service stores static information of Avaya Oceana® Solution. For example, the information related to users, accounts, attributes, providers, and resources. Therefore, you must take a backup of this service at regular intervals.

Note:

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

Procedure

1. On the System Manager web console, 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 the UCAStoreService data in Data Center 1

Before you begin

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

Procedure

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

Installing UCAStoreService in Data Center 1

About this task

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

Procedure

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

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

Restoring UCM

UCMService defer data backup

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

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

- Planned switchover and recovery
- Unplanned switchover and recovery

Taking a backup of UCMService during planned switchover and recovery

About this task

Use this procedure to take a manual backup of the UCMService database during planned switchover and recovery from Data Center 1 to Data Center 2.

Before you begin

Ensure that all agents are logged out of their accounts.

Procedure

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

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

   If you do not specify any value, the backup storage server retains all backup files.
9. Click **Commit**.
10. Select the check box for the Avaya Oceana® Cluster 1.
11. From the **Backup and Restore** field, select **Backup**.

12. On the Cluster Database Backup Confirmation dialog box, select the **UCMService** check box and click **Continue**.
13. In the **Backup Password** field, enter a password for the backup.

    Important:

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

Taking a backup of UCMService during unplanned switchover and recovery

About this task

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

Procedure

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

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

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

13. In the **Backup Password** field, enter a password for the backup.

    Important:

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

14. In the **Schedule Job** field, click **Schedule later**.
15. In the **Task Time** field, specify the date, time, and timezone for the first backup.
16. In the **Recurrence** field, select the **Tasks are repeated** option and specify the recurring backup schedule.
17. In the **Range** field, specify a range for the recurring backup schedule.
18. Click **Backup**.
19. After the backup process is complete, verify that the **Status** column on the Backup and Restore Status page displays the status `Completed`.

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

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`.
- Uninstall UCMService from Avaya Oceana® Cluster 1 and restart all nodes of the cluster to delete the ucm-space-pu and the ucm-oc-pu.

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. Restart the Avaya Breeze™ nodes of Avaya Oceana® Cluster 3.

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

10. Change the state of Avaya Oceana® Cluster 1 and Avaya Oceana® Cluster 3 to `Accept New Service`.

Installing UCMService

About this task

Use this procedure to install UCMService on Avaya Oceana® Cluster 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 UCMService and click **Install**.
3. In the Confirm Install service: UCMService 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.

Restoring OCP database server

Taking a backup of the Omnichannel database on Data Center 2

Procedure

1. Log in to the Omnichannel server.
2. Go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\Oceana\BackupAndRestore` folder.
3. Double-click the `BackupAndRestore.exe` file.
4. In the **Select/create file to backup to** field, click **Browse**.

   The Backup and Restore application displays the Save As screen.

5. Select the location where you want to save the backup file.

   Do not save the backup file to the software, journal, or multimedia drive.

6. Specify a name for the backup file.
7. Click **Save**.
8. Click **Backup Database**.

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

   Note:

   The space required for the backup is twice the size of the database. Therefore, ensure that the server has sufficient disk space. If the server does not have sufficient disk space, the Backup and Restore application displays a warning that there is not enough space for creating the `cbk` file.

   The Backup and Restore application does not display any warning after it creates the `cbk` file and starts the zipping process. Therefore, after the `zip` file is created, you must check its validity.

Restoring the Omnichannel database in Data Center 1

Procedure

1. Log in to the Omnichannel server.
2. Go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\Oceana\BackupAndRestore` folder.
3. Double-click the `BackupAndRestore.exe` file.
4. In the **Select file to restore from** field, click **Browse**.

   The Backup and Restore application displays the Open dialog box.
5. Browse to the location containing the backup file.
6. Select the backup `zip` file.
7. Click **Open**.
8. Click **Restore Database**.

   The Backup and Restore application displays the Drive restore screen.
9. In the **Select your database drive letter** field, select the drive that you specified for the Omnichannel database when installing the Omnichannel server software.
10. Click **Restore**.

    Important:

    If the Omnichannel server displays the Cache Post Restore Script terminal window, do not close the window. You must wait until the process in the window is completed.

The Backup and Restore application displays the `Restore complete!` message when the restore process is complete.

11. Verify the data in the database to ensure that the restore process is completed successfully.
12. Restart all Avaya Breeze™ nodes.

Configuring Cache Mirroring between DC1 and DC2

You must change the Cache mirroring set up. The mirror configuration between Data Center 1 and Data Center 2 must now be re-established. For details, see the *Cache Mirroring configurations* section.

Reinstate the Omnichannel Database HA after failure

If the Omnichannel server or the Cache application on one of the servers goes down, you must either startup or restart the server.

Restoring Context Store External Data Mart server

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

Verifying UCA as GEO_MASTER in Data Center 1

Before you begin

Ensure that the OCP Cache data from Data Center 2 is restored to Data Center 1.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze™** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. **Cluster**: Select Avaya Oceana® Cluster 1.
   b. **Service**: Select **UCAStoreService**.
3. For **Oceana disaster recovery role**, verify that:
   a. **Override Default** is selected.
   b. The **Effective Value** field displays `GEO_MASTER`.

4. Restart the cluster.

Enabling the Web Chat workflow

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze™** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. **Cluster**: Select Avaya Oceana® Cluster 1.
   b. **Service**: Select **Chat ED application**.
3. For **MaintenanceMode**:
   a. Select **Override Default**.
   b. In the **Effective Value** field, change the value to `false`.
4. Click **Commit**.

Enabling Web Voice and Web Video workflows

Procedure

1. In Data Center 2, set the state of the AvayaMobileCommunications cluster to `Denying`.
2. In Data Center 1, set the state of the AvayaMobileCommunications cluster to `Accepting`.
3. Change the DNS mapping of the Authorization token service FQDN to map to the public address of the Authorization token service in Data Center 1.
4. 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 1.
5. Change the DNS mapping of the AvayaMobileCommunications cluster FQDN to map to the public address of the AvayaMobileCommunications cluster in Data Center 1.
6. In Data Center 2, set the Maintenance mode for the Web Voice and Web Video workflows to `True`.
7. In Data Center 1, set the Maintenance mode for the Web Voice and Web Video workflows to `False`.

   After the DNS changes take effect, all new call requests from web and mobile clients go to Data Center 1.

Enabling Avaya Oceana® Solution components to DC1

Changing the Cluster Activity status of Data Center 1 components

About this task

You must perform these steps for all three clusters in Data Center 1. You can edit the Cluster Activity status only if the clusters are in the `Denying` state.

Before you begin

Change the state of Data Center 1 clusters to `Denying`.

Procedure

1. In your web browser, open the Oceana Manager page by clicking the bookmark that you created while deploying Data Center 1

   The browser window displays the Oceana Manager page.
2. Check the status of Avaya Oceana® Cluster 1
3. If the status of the clusters is `STANDBY`, click **Set Cluster Group to Active** to change the status to `ACTIVE`.
4. On the confirmation message box, click **OK**.
5. **(Optional)** If the Oceana Manager page does not display the updated status after some time, click **Refresh**.

Restoring Avaya Control Manager

You must restore Avaya Control Manager in DC1 to the same level of data as Avaya Aura® Communication Manager and System Manager. Avaya Control Manager is restored from a backup prior to the failure.

Reconfiguring Avaya Oceana® Solution addresses to DC1

About this task

Use this procedure to restore and reconfigure multiple fields in Avaya Control Manager to point to local 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 IP address pointing to the Omnichannel server in Data center 1.
7. Click **Save**.

Configuring the UCA URL to point to Data Center 1

About this task

Use this procedure to update the Oceana Server Details within Avaya Control Manager to point to the Avaya Oceana® Cluster 1 address in Data Center 1.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Server Details**.
2. On the Avaya Oceana Server List page, double-click the UCAServer server.
3. On the Avaya Oceana Server Edit page, in the **API URL** field, update the URL to point to the Avaya Oceana® Cluster 1 address in Data Center 1.

Maintenance mode reset

For a planned switchover to Data Center 2, you configure the MaintenanceMode attribute for the Chat, SMS, SocialConnector, Web Voice, and Web Video workflows in Data Center 1. After the maintenance, when you reinstate Data Center 1 as the operational data center, you must reconfigure the MaintenanceMode attribute for the Chat, SMS, SocialConnector, Web Voice, and Web Video workflows in Data Center 1 so that the workflows start accepting new contacts.

Agent switchover after restoration

Agents must login to the new Data Center after a switchover. They must be provided with the new URL for Data center 1 and must use this to login after restoration.

Chapter 7: Upgrading the Disaster Recovery solution

Checklist for upgrading Omnichannel Database

Use the following checklist to upgrade the mirrored Omnichannel Database.

No.	Task	Description	✔
1	Remove Cache Mirroring from all Omnichannel Database servers.	See Removing Cache Mirroring from Omnichannel Database servers on page 69.	
2	Take a backup of the primary Omnichannel Database server on Data Center 1 and store the backup file at a preferred location.	See *Deploying Avaya Oceana® Solution*.	
3	Uninstall the Omnichannel Server software.	-	
4	Install the Omnichannel Server software.	See *Deploying Avaya Oceana® Solution*.	
5	Restore the backup on the primary Omnichannel Database server.	See *Deploying Avaya Oceana® Solution*.	
6	Configure Cache Mirroring on the primary Omnichannel Database server.	See the following: • Checklist for configuring Cache Mirroring with a backup server on page 25 • Checklist for configuring Cache Mirroring with failover and backup servers on page 31	
7	Take a backup of the mirrored primary	See *Deploying Avaya Oceana® Solution*.	

Table continues…

No.	Task	Description	✔
	Omnichannel Database server.		
8	Configure Cache Mirroring on the standby and backup Omnichannel Database servers.	See the following: • Checklist for configuring Cache Mirroring with a backup server on page 25 • Checklist for configuring Cache Mirroring with failover and backup servers on page 31	
9	Restore the mirrored backup on the standby and backup Omnichannel Database servers.	See *Deploying Avaya Oceana® Solution*.	

Removing Cache Mirroring from Omnichannel Database servers

Before you begin

Use this procedure to remove Cache Mirroring from Omnichannel Database servers before upgrading the Omnichannel Server software. After the upgrade is complete, you must reconfigure Cache Mirroring on all Omnichannel Database servers.

Procedure

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

   `http://<DC2OmnichannelServerIP>:57772/csp/sys/UtilHome.csp`

   <DC2OmnichannelServerIP> is the IP address of the backup Omnichannel Database server in Data Center 2.

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

6. 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**.
7. On Cache Management Portal, click **System Administration** > **Configuration** > **Mirror Settings** > **Edit Mirror** > **Remove Mirror Configuration**.
8. Click **Clear JoinMirror Flag**.
9. On the server, right-click the **Cache** icon and then click **Stop Cache**.
10. Click **Restart**.
11. Log in to Cache Management Portal.
12. On Cache Management Portal, click **System Administration** > **Configuration** > **Mirror Settings** > **Edit Mirror** > **Remove Mirror Configuration**.
13. Click **Yes** and then click **Remove** to remove the mirrored attribute.

Note:

If Data Center 1 is configured for High Availability, you must first remove Cache Mirroring from the standby server and then from the active server.

Chapter 8: Limitations

Limitations

Avaya Oceana® Solution disaster recovery has certain limitations. The disaster recovery does not support:

- Automatic switchover.
- Call preservation - all active, alerting and queued contacts are lost on switchover.
- Partial switchover.
- Avaya Aura® Communication Manager switchover to ESS as it requires corresponding Avaya Oceana® Solution switchover.
- Cross-WAN AES link to ESS - no Device, Media, and Call Control (DMCC) over WAN.
- WAN outage scenario - active-active mode not available.
- Avaya Aura® Communication Manager configuration changes while the disaster recovery site is active.

Avaya Oceana® Solution disaster recovery supports a single disaster recovery site, that is, a single ESS. Disaster recovery requires some down time while activating the secondary site. It also mandates that the WAN delay has to be less than 50 milliseconds (ms) for Avaya Control Manager. Due to the down time, there is some loss of historical reporting data.

Chapter 9: Resources

Documentation

Title	Use this document to	Audience
Avaya Aura® Communication Manager Overview and Specification	Know about tested product characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements.	• Sales Engineers • Business Partners • Solution Architects • Implementation Engineers
Administering Avaya Aura® System Manager	Administer Avaya Aura® System Manager	• Solution Architects • Implementation Engineers • System Administrators
Administering Avaya Aura® Communication Manager	Administer Avaya Aura® Communication Manager	• Solution Architects • Implementation Engineers • System Administrators
Deploying Avaya Oceana® Solution	Deploy the Avaya Oceana® Solution	• Sales Engineers • Business Partners • Solution Architects • Implementation Engineers
Avaya Context Store Snap-in Reference	Know about Avaya Context Store Snap-in characteristics and capabilities, including feature descriptions, interoperability, and performance specifications. The document also provides instructions on deploying, configuring, and troubleshooting the Context Store services.	• Solution Architects • Implementation Engineers • System Administrators
Avaya Context Store Snap-in Release Notes	Know about information on the features available and solution details.	• Solution Architects • Implementation Engineers • System Administrators

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com/.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

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

Training

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

Course code	Course title	Delivery Type
Avaya Oceana® Solution		
34200W	Avaya Oceana® Solution Design Fundamentals	WBT
3470T	Avaya Oceana® Solution Design Fundamentals Online Test	LMS
2116W	Avaya Oceana® Fundamentals	WBT
2410W	Customer Communications and Applications with Avaya Oceana® for Developers	WBT
24300V	Administering Avaya Oceana®	vILT
24320W	Administering Avaya Oceana® - Basic	WBT
ACIS – 7495 Avaya Oceana® Solution		
74150V	Integrating Avaya Oceana® Core and Workspaces	vILT
7495X	Avaya Oceana® Solution Integration Exam	Exam

Table continues…

Course code	Course title	Delivery Type
ACSS-7497 Avaya Oceana® Solution		
74550V	Supporting Avaya Oceana® Solution	vILT
7497X	Avaya Oceana® Solution Support Exam	Exam
Avaya Workspaces for Oceana®		
24020W	Using Avaya Workspaces for Agents	Along with the license
24040W	Using Avaya Workspaces for Supervisors	Along with the license
2415W	Introduction to Avaya Workspaces Framework for Developers	WBT
Avaya Analytics™ for Oceana®		
2431W	Administering Avaya Analytics™ for Oceana®	WBT
ACSS-7498 Avaya Analytics™		
7435V	Integrating and Supporting Avaya Analytics™ for Oceana®	vILT
7498X	Avaya Analytics™ Integration and Support Exam	Exam

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

S

T

U

V

W