



Avaya Oceana[®] and Avaya Analytics[™] Disaster Recovery and Migration

Release 3.10.0.2
Issue 1
March 2026

Notices

© 2026 Avaya LLC. All Rights Reserved.

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

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

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

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE). THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/licenseinfo) UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE

TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

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

License types

Copyright

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

Virtualization

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

Third Party Components

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

Service Provider

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.



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

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



Contents

Chapter 1: Introduction	8
Purpose	8
Chapter 2: Overview	9
Overview	9
Supported Avaya Oceana® migration paths	10
Prerequisite for migration	10
Chapter 3: Perform Planned Partial Failover to DC2	12
Overview	12
Checklist for partial controlled switchover	12
Preparation and Validation	17
Validate identical software levels	17
Validate Avaya Oceana® components replication	17
Validate Avaya Oceana® snap-in shutdown or deployment status in DC1 and DC2	22
Launch Oceana Monitor for DC1 and DC2 locations and verify PUs	26
Planned Switchover	27
Configure the primary site voice channel shutdown	27
Configure the primary site email shutdown	28
Configure the primary site chat shutdown	28
Configuring the primary site MessagingService shutdown	29
Configure the primary site GenericChannelAPI service shutdown	30
Restore UCMSvc after switchover	30
Taking a backup of UCMSvc	32
Taking a backup of UCASvc in Data Center 1	33
Setting the maintenance mode for front end web voice and web video	33
Oceana POM switchover	34
Validating contacts	34
Logging out supervisors and agents	34
Changing the Cluster Activity status for the clusters in Data Center 1	34
Omnichannel database switchover	35
Switching over Avaya Analytics™ from DC1 to DC2	37
Promoting Avaya Analytics™ on DC2 as primary	39
Configuration and Validation	40
Verifying the CSC deployment status in DC2	40
Preparing UCMSvc in DC2 for database restore	40
Restoring the UCMSvc data for Avaya Oceana® Cluster 1 in Data Center 2	41
Configure the DR site EmailService startup	41
Configure the DR site Chat startup	42
Configure the DR site MessagingService for Social, SMS or Async startup	42
Configure the DR site GenericChannelAPI Service startup	43

Verify the DR Application Enablement Services.....	44
Changing cluster activity status for clusters in Data Center 2.....	44
Avaya Workspaces Agent switchover.....	45
Using Toggle button to switch Avaya Control Manager in Data Center 1 to use Avaya Oceana® applications in Data Center 2.....	46
Validate and test deployed channels.....	46
Verify the real time and historical reports on DC2.....	46
Chapter 4: Migrating Avaya Oceana® and Avaya Analytics™ on DC1.....	47
Overview.....	47
Upgrading the Omnichannel server.....	48
Enabling or disabling a scheduled computer maintenance in Windows 2019.....	48
Upgrading Omnichannel servers from Avaya Oceana® 3.8.1.1 and later versions to Avaya Oceana® 3.10.0.2 version on Data Center 1.....	48
Remove the current Cache Mirroring configuration in Data Center 1.....	48
Removing Cache Mirroring from the backup Omnichannel server.....	49
Taking a backup of the Omnichannel database for failure upgrade.....	49
Upgrading the latest version of the Omnichannel server software on the Omnichannel server in Data Center 1.....	50
Avaya Analytics™ Installation and migration on DC1.....	51
Promoting Avaya Analytics™ on DC2 as primary and configuring Avaya Analytics™ on DC1 as standby.....	52
Migrating Avaya Analytics 4.x Crunchy 2 data to Avaya Analytics 4.3 Crunchy 5 data.....	54
Setting Source Crunchy 2 Environment.....	54
Setting up target Crunchy 5 environment and migrating the data.....	55
Chapter 5: Perform Planned Switchback to DC1.....	58
Overview.....	58
Checklist for Partial controlled switchback.....	58
Preparation and Validation.....	61
Verifying the CallServerConnector component in the primary site.....	61
Verifying deployment mode status of primary site email snap-in.....	61
Verifying the shutdown mode status of primary site CustomerController chat snap-in.....	62
Verifying the shutdown mode status of primary site MessagingService snap-in.....	62
Verifying the shutdown mode status of primary site GenericChannelAPI snap-in.....	63
Verifying deployment status of AMC snap-in for Avaya WebRTC Connect contacts.....	63
Preparing DC1 for UCA and UCM database restore.....	64
Logging out supervisors and agents from the DR site.....	65
Validating contacts.....	65
Planned Partial Switchback.....	66
Shut down and switch back DR site voice channel to primary site.....	66
Configuring DR site email shutdown.....	67
Configuring DR site MessagingService shutdown.....	67
Configuring DR site chat shutdown.....	68
Configuring DR site GenericChannelAPI Service shutdown.....	68

Setting the maintenance mode for web voice and web video.....	69
Oceana POM switchback.....	69
Changing the Cluster Activity status for the clusters in Data Center 2.....	69
Backing up UCMSERVICE in DC2.....	70
Restoring UCMSERVICE data in DC1.....	71
Restoring UCAStoreService data in DC1.....	72
Installing UCAStoreService in DC1.....	72
Changing cluster activity status from Standby to Active for clusters in Data Center 1.....	73
Restoring the External Data Mart server.....	74
Reconfiguring Avaya Oceana® addresses to DC1.....	76
Pointing ACM to the Omnichannel database server in DC1.....	77
Completing the migration from Avaya Analytics™ 4.x to Avaya Analytics™ 4.3.....	77
Restarting orca-dbmgr pod.....	81
Restarting mstr-srv pod.....	81
Planned switch back to DC1.....	82
Configuration and Validation.....	84
Clean up Mirror setup on DC1 and DC2.....	84
Configuring the Web Voice and Web Video after Switchback.....	87
Avaya Workspaces agent switchover.....	88
Validate and test deployed channels.....	88
Verify the real time and historical reports on DC1.....	88
Chapter 6: Migrating to Avaya Oceana® and Avaya Analytics™ on DC2.....	89
Overview.....	89
Upgrading the Omnichannel server.....	90
Enabling or disabling a scheduled computer maintenance in Windows 2019.....	90
Upgrading Omnichannel servers from Avaya Oceana® 3.8.1.1 and later versions to Avaya Oceana® 3.10.0.2 version on Data Center 2.....	90
Checklist for Omnichannel server upgrade.....	90
Taking a backup of the Omnichannel database for failure upgrade.....	91
Upgrading the latest version of the Omnichannel server software on the Omnichannel server in Data Center 2.....	92
Avaya Analytics™ Installation on DC2.....	92
Promoting Avaya Analytics™ on DC1 as primary and configuring Avaya Analytics™ on DC2 as standby.....	93
Install Avaya Analytics™ version 4.3.1.1 and configure Geo.....	95
Setting up DC2 for 4.3.1.1.....	95
Configuring DC1 as a Geo Primary.....	96
Configuring DC2 as a Geo Standby.....	97
Chapter 7: Post migration tasks.....	99
Post migration checklist.....	99
Deploying Engagement Designer workflows.....	99
Recommission of Disaster Recovery.....	100
Validating and configuring UCAStoreService Geographic Redundancy.....	100

Validating and configuring Avaya Context Store Geographic Redundancy.....	101
Recommission of Disaster Recovery.....	102
Configuring Context Store for Disaster Recovery.....	102
Configuration Checklist.....	102
Enabling SSL connection for Context Store replication from DC1 to DC2.....	103
Retrieving the System Manager root certificate.....	103
Creating a new keystore certificate file.....	104
Creating a new keystore certificate file for Data Center 1 of Avaya Oceana® Cluster 1.....	105
Adding CA root certificate and keystore certificate files to Data Center 2 Cluster 1 nodes....	106
Enabling Context Store integration to External Data Mart in Data Center 1.....	107
Configuring Omnichannel for disaster recovery	107
Omnichannel database mirroring configurations.....	107
Verifying the Omnichannel Database mirroring status.....	108
Configuring Cache Mirroring on the backup Omnichannel Database server in Data Center 2.....	108
Securing the Cache Mirror on the Omnichannel Database server on Data Center 1.....	110
Chapter 8: Validate replication status between DC1 and DC2.....	112
Checklist to validate replication status between DC1 and DC2.....	112
Validate the System Manager and Avaya Breeze® platform replication status.....	113
Validating the Avaya Control Manager database HA deployment.....	113
Verifying the UCA replication status.....	113
Verify the Context Store replication status.....	115
Verifying the Omnichannel database mirroring status.....	115
Verifying the Avaya Analytics DB replication from DC1 to DC2.....	116
Chapter 9: Resources.....	117
Documentation.....	117
Finding documents on the Avaya Support website.....	118
Avaya Documentation Center navigation.....	119
Training.....	120
Support.....	123

Chapter 1: Introduction

Purpose

This document provides information on how to migrate Avaya Oceana® and Avaya Analytics™ Disaster Recovery (DR) setup for Avaya Oceana® 3.10.0.2 release.

This document is intended for administrators of Avaya Oceana® and Avaya Analytics™ for Avaya Oceana®.

Important:

- This document is based on the assumption that you have deployed Avaya Oceana®, Avaya Analytics™ for Avaya Oceana®, and the required components and services on Data Centers 1 and 2.
- This document refers to the primary data center as Data Center (DC) 1 and the secondary data center as Data Center (DC) 2.

Chapter 2: Overview

Overview

Disaster Recovery migration provides a planned approach to migrate Data Center 1 (DC1) and Data Center 2 (DC2) with partial outage approach to migrate both DC1 and DC2. The migration process for DC1 and DC2 are identical.

The two data centers are linked with each other for replication. Post replication, one is the primary site designated as DC1, and the other is the secondary or disaster recovery site set as DC2.

This document provides instructions to migrate DC1 and DC2 with a planned partial outage maintenance activity.

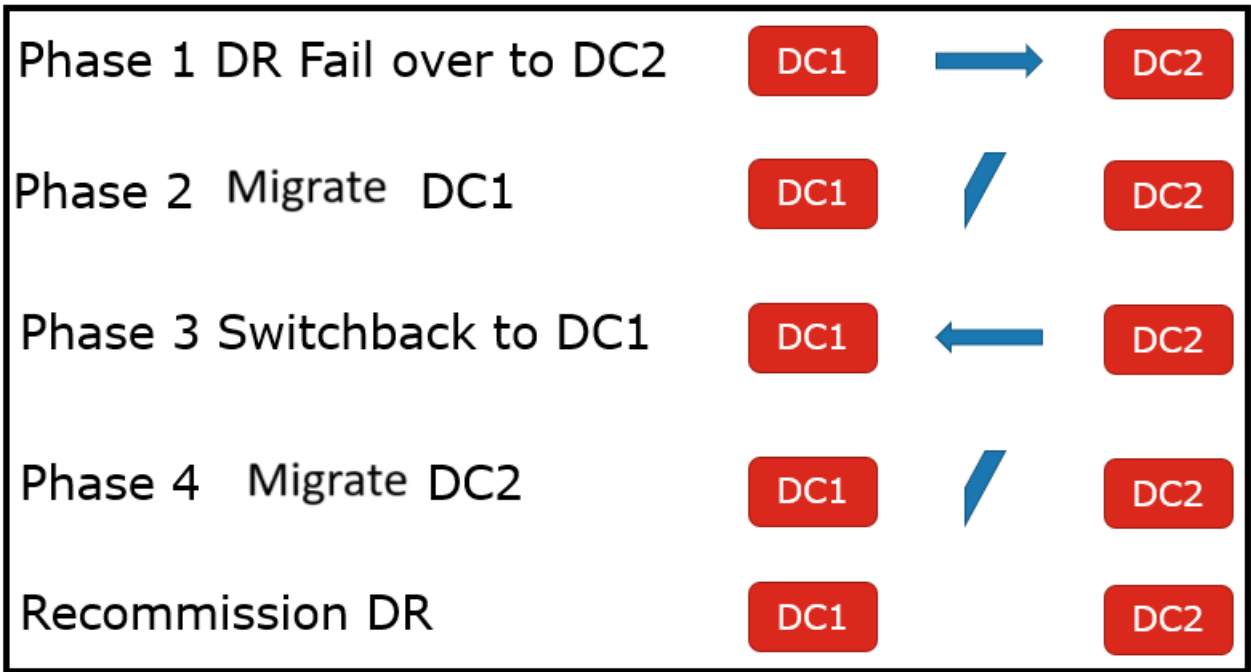


Figure 1: Disaster Recovery migrate flow diagram

Supported Avaya Oceana® migration paths

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

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

! Important:

- Before migrating to a later Avaya Oceana® release, you must review the target release hardware requirements to ensure that your hardware meets the minimum specifications. For more information about Avaya Oceana® hardware requirements, see *Avaya Oceana® Solution Description*.
- Before migrating to a later Avaya Oceana® Release, you must review the component interoperability requirements for the target release to ensure the versions used in your solution are supported. Compatibility Matrix provides compatibility information for the Avaya products that are supported with the various releases of Avaya Oceana®. Access the Compatibility Matrix page at <https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml>.

Prerequisite for migration

Avaya Analytics™

Avaya Analytics™ 4.3.1.1 is compatible with Avaya Oceana® 3.10.0.2 release. If you are on Avaya Analytics™ 4.1.x or 4.1.2 release, then you have to migrate the Avaya Analytics™ to 4.3.1.1. If you are on Avaya Analytics™ 4.2, 4.3, or 4.3.1.0 release, then you have to upgrade to Avaya Analytics™ 4.3.1.1. For information about the upgrade, see Avaya Analytics™ 4.3.1.1 release notes.

Other requirements

- Identify hardware resources to deploy Avaya Aura®, Avaya Breeze® platform, and Omnichannel Provider database components.
- Identify if your environment is on the supported migration paths.
- Check for third-party integrated software compatibility.
- Download the Avaya Oceana® 3.10.0.2 software from the Avaya Support website at <https://support.avaya.com>.
- An additional 2 GB of RAM for each Avaya Breeze® platform node as compared to the older release.

- An additional 5 GB of disk space for each Avaya Breeze® platform node as compared to older release.
- Additional storage is required as the new and old Avaya Breeze® platform nodes co-exist until the migration is completed.
- For more information about hardware requirement for Avaya Analytics™ 4.3.1.1, refer to the *Deploying Avaya Analytics™ for Avaya Oceana®* documentation available on the Avaya Support website at <https://support.avaya.com>.

Chapter 3: Perform Planned Partial Failover to DC2

Overview

You can perform a planned partial switchover even when there are no failures in any part of the solution. Partial switchovers may be required to perform software and patch upgrades. Testing the DR capabilities of the Avaya Oceana® and Avaya Analytics™ components, supports the planning of scheduled maintenance times required to perform these activities.

Checklist for partial controlled switchover

Preparation and Validation

The following is a checklist of the preparation and validation steps before you perform a partial controlled switchover.

No.	Task	Description	✓
1	Prepare for switchover - Before starting any switchover operations on a production Avaya Oceana® and Avaya Analytics™ DR system, you must refer to several key documents.	See the following documents: • Administering Avaya Aura® System Manager • Installing Avaya Control Manager • Administering Avaya Aura® Communication Manager • Administering Avaya Aura® Application Enablement Services	

Table continues...

No.	Task	Description	✓
2	Validate identical software levels on the following applications across DC1 and DC2: • Avaya Aura® System Manager • Avaya Control Manager • Avaya Aura® Communication Manager • AES • Avaya Oceana® • Avaya Analytics™ • Avaya Breeze® platform • Omnichannel	See Validate identical software levels on page 17.	
3	Validate Avaya Oceana® solution replication before switchover.	See Validate Avaya Oceana components replication on page 17.	
4	Validate Avaya Aura® System Manager primary to DR replication status and health status from DC1 to DC2 is fully operational.	Validate the System Manager primary to DR replication status on page 18.	
5	Validate Avaya Aura® System Manager and Avaya Breeze® platform replication status to all Avaya Breeze® platform nodes in DC1 and DC2.	See Validate the System Manager and Avaya Breeze platform replication status on page 18.	
6	Validate the Avaya Control Manager database HA replication status.	See Validating the Avaya Control Manager database HA deployment on page 21.	
7	Verify the Context Store replication status from DC1 to DC2.	See Verify the Context Store replication status on page 20.	
8	Verify the Omnichannel database mirroring status from DC1 to DC2.	See Verifying the Omnichannel database mirroring status on page 21.	
9	Verify Avaya Aura® Communication Manager to ESS data replications.	See Verifying Avaya Aura Communication Manager to ESS data replications on page 21.	
10	Verify the Avaya Analytics™ DB Replication from DC1 to DC2.	See Verifying the Avaya Analytics DB replication from DC1 to DC2 on page 22.	
11	Validate snap-in shutdown or deployment status in the DR site.	See Validate Avaya Oceana snap-in shutdown or deployment status in DC1 and DC2 on page 22.	

Table continues...

No.	Task	Description	✓
12	Verify UCA replication status from DC1 to DC2.	See Verifying the UCA replication status on page 19.	
13	Verify the deployment status of EmailService in DC2.	See Verifying the deployment status of EmailService in DC2 on page 22.	
14	Verify the shutdown status of CustomerControllerService in DC2.	See Verifying the shutdown status of CustomerControllerService in DC2 on page 23.	
15	Verify the shutdown status of MessagingService in DC2.	See Verifying the shutdown status of MessagingService in DC2 on page 23.	
16	Verify the shutdown status of GenericChannelAPI in DC2.	See Verifying the shutdown status of GenericChannelAPI in DC2 on page 24.	
17	Verify the deployment status of the AMC snap-in for Avaya WebRTC Connect.	See Verifying the deployment status of the AMC snap-in for Avaya WebRTC Connect on page 24.	
18	Verify the CSC deployment status in DC1 and DC2.	See the following: • Verifying the CSC deployment status in DC1 on page 25 • Verifying the CSC deployment status in DC2 on page 25	
19	Launch Oceana Monitor for DC1 and DC2 locations and verify there are no un-deployed PUs across all Oceana clusters.	See the following: • Launch Oceana Monitor for DC1 and DC2 locations and verify PUs on page 26 • Viewing Oceana Monitor Service pages on page 26 • Oceana Services Overview page on page 26 • Monitor Service page on page 26	

Partial controlled switchover

The following is a checklist of the list of steps to perform a Partial Controlled Switchover.

No.	Task	Description	✓
1	Configure the primary site voice channel shutdown.	See Configure the primary site voice channel shutdown on page 27.	
2	Configure the primary site email shutdown.	See Configure the primary site email shutdown on page 28.	
3	Configure the primary site chat shutdown.	See Configure the primary site chat shutdown on page 28.	
4	Configure the primary site MessagingService shutdown.	See Configuring the primary site MessagingService shutdown on page 29.	
5	Take a backup of UCASStoreService and UCMSService (on remote server).	See Taking a backup of UCASStoreService in Data Center 1 on page 33 and Taking a backup of UCMSService on page 32.	
6	Configure the primary site GenericChannelAPI service shutdown.	See Configure the primary site GenericChannelAPI service shutdown on page 30.	
7	Set the maintenance mode for front end web voice and web video.	See Setting the maintenance mode for front end web voice and web video on page 33.	
8	Switch to DR site Oceana and POM system.	See Oceana POM switchover on page 34.	
9	Validate contacts in DC1.	See Validating contacts on page 34.	
10	Log out supervisors and agents from DC1.	See Logging out supervisors and agents on page 34.	
11	Change the cluster activity status for clusters in DC1.	See Changing the Cluster Activity status for the clusters in Data Center 1 on page 34.	
12	Switch over the Omnichannel database server in the primary site DC1 to the Omnichannel database server in the DR site DC2.	See the following: • Omnichannel database switchover on page 35. • Removing cache mirroring from Campus Standby on page 35. • Promoting Omnichannel server in DC2 on page 36. • Pointing ACM to the new Omnichannel database server in DC2 on page 37.	
13	Switch over Avaya Analytics™ from DC1 to DC2.	See Switching over Avaya Analytics from DC1 to DC2 on page 37.	

Configuration and Validation

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

No.	Task	Description	✓
1	Verify CSC deployment status in DC2.	See Verifying the CSC deployment status in DC2 on page 25.	
2	Restore the UCMSERVICE data for Avaya Oceana® cluster 1 in Data Center 2.	See Preparing UCMSERVICE in DC2 for database restore on page 40 See Restoring the UCMSERVICE data for Avaya Oceana Cluster 1 in Data Center 2 on page 41.	
3	Configure the DR site EmailService startup.	See Configure the DR site EmailService startup on page 41.	
4	Configure the DR site Chat startup.	See Configure the DR site Chat startup on page 42.	
5	Configure the DR site MessagingService for Social or SMS startup.	See Configure the DR site MessagingService for Social, SMS or Async startup on page 42.	
6	Configure the DR site GenericChannelAPI Service startup.	See Configure the DR site GenericChannelAPI Service startup on page 43.	
7	Verify DR Application Enablement Services server to enable switch connection.	See Verify the DR Application Enablement Services on page 44.	
8	Change the cluster activity status for clusters in DC2.	See Changing cluster activity status for clusters in Data Center 2 on page 44.	
9	Avaya Workspaces Agent switchover: Login Agents using DC2 Workspaces and test deployed Channel Routing.	See Avaya Workspaces Agent switchover on page 45.	
10	Use the Toggle button to switch Avaya Control Manager in DC 1 to use Avaya Oceana® applications in DC2.	See Using Toggle button to switch Avaya Control Manager in Data Center 1 to use Avaya Oceana applications in Data Center 2 on page 46.	
11	Validate and test deployed channels: Launch Oceana Dashboard and verify all deployed channels are in the Green status.	See Validate and test deployed channels on page 46.	

Preparation and Validation

Validate identical software levels

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

You must validate the following applications and platforms:

- Avaya Aura® System Manager
- Avaya Control Manager
- Avaya Breeze® platform
- Avaya Aura® Communication Manager and ESS
- Avaya Aura® Application Enablement Services
- Avaya Analytics™
- Avaya Oceana® Snap-ins

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

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

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

Validate Avaya Oceana® components replication

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

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

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

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

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

 Important:

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

Validate the System Manager primary to DR replication status

About this task

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

Procedure

1. On the primary System Manager web console, in the **Application State** widget, verify the following states:

- GR Server Role is PRIMARY
- GR Server Mode is ACTIVE
- GR Replication is ENABLED

2. Click **Services > Geographic Redundancy > GR Health**.

Verify the following elements are in a Successful state and in green:

- Database Replication
- File Replication
- Directory Replication

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

3. On the DR System Manager web console, in the **Application State** widget, verify the following states:

- GR Server Role is SECONDARY
- GR Server Mode is STANDBY
- GR Replication is ENABLED

4. Verify the status of elements in **GR Health**.

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

Validate the System Manager and Avaya Breeze® platform replication status

About this task

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

Procedure

1. On the System Manager web console, click **Services > Replication**.
2. Validate that the synchronization status of all replica groups is **Synchronized**.
System Manager displays the word **Synchronized** in green.
3. Click **Avaya Breeze replica group**.
4. Check if the **Breeze Node Synchronization** status is in the **Synchronized** state and that the synchronization date is one month or less from the current date.

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

Verifying the UCA replication status

About this task

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

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

Important:

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

Procedure

1. Log on to the System Manager.
2. On the System Manager web console, click **Elements > Avaya Breeze® > Cluster Administration > Primary Cluster**.
3. In the **Cluster** field, select **Oceana Monitor**.
4. To view the PU status of all the snap-ins, select **Cluster 1 > Grid Info**.
5. Verify if the PU status of **ucaStoreSpace-GATEWAY** is **INTACT**.
If the status is **Scheduled** or **Broken**, UCA replication is not operational.
You must correct the issue before proceeding with the switchover.
6. On the primary site, in the **Show Cluster Messages** tab, select the **UCAStoreService** PU.
7. Verify that the **HEARTBEAT** message for the replication channel state is **ACTIVE**.
8. Repeat steps 1 to 6 for Avaya Oceana® Cluster 1 in Data Center 2.

 Note:

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

 Important:

Perform the subsequent steps after successfully completing steps 1 to 6.

9. Log on to the Avaya Control Manager on DC1.
10. Add a new test attribute and save the attribute to the primary UCA instance.

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

 Note:

If the test attribute does not appear, UCA replication is not operational from primary to DR or the request to save a new attribute to the primary UCA server is not successful. Ensure that you correct these issues before proceeding with the switchover.

11. Reload the cluster message, select **UCAStoreService**, and check the new time of the cluster DB updated message.

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

Verify the Context Store replication status

About this task

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

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

Procedure

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

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

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

7. Verify that the context is present in DC1 Context Store and in DC2 Context Store.

Validating the Avaya Control Manager database HA deployment

About this task

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

Note:

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

Verifying the Omnichannel database mirroring status

About this task

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

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

Procedure

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

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

Verifying Avaya Aura® Communication Manager to ESS data replications

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

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

Verifying the Avaya Analytics DB replication from DC1 to DC2

About this task

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

Procedure

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

```
ccm release orca analytics
```

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

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

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

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

Verifying the deployment status of EmailService in DC2

About this task

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

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

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

Procedure

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

3. On the Service Clusters tab, do the following:
 - a. **Cluster:** Select DR Avaya Oceana® Cluster 3.
 - b. **Service:** Select **EmailService**.
4. In the **Deployment status of emailmanager** attribute, verify if the value is set to `false`.
 If this field is set to `true`, set it to `false` and commit the change.
 If you change this value to `true`, there is no need to reboot Avaya Oceana® Cluster 3.

Verifying the shutdown status of CustomerControllerService in DC2

About this task

The CustomerControllerService snap-in handles chat contacts within the Avaya Oceana® solution. Before the switchover to the DR site, use this procedure to ensure that the shutdown mode status attribute in the DR site for the CustomerControllerService snap-in is set as `true`.

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

Procedure

1. Log on to System Manager.
2. On the System Manager web console, click **Elements > Avaya Breeze® > Configuration > Attributes**.
3. On the Service Clusters tab, do the following:
 - a. **Cluster:** Select DR Avaya Oceana® Cluster 3.
 - b. **Service:** Select **CustomerControllerService**.
4. In the **Shutdown Mode** attribute field, verify if the value is set to `true`.
 If you change this value to `true`, there is no need to reboot Avaya Oceana® Cluster 3.

Verifying the shutdown status of MessagingService in DC2

About this task

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

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

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

Procedure

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

3. On the Service Clusters tab, do the following:
 - a. **Cluster:** Select DR Avaya Oceana® Cluster 3.
 - b. **Service:** Select **MessagingService**.
4. In the **Shutdown Mode** attribute field, verify if the value is set to `true`.

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

Verifying the shutdown status of GenericChannelAPI in DC2

About this task

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

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

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

Procedure

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

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

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

About this task

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

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

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

Procedure

1. Log on to System Manager.
2. On the System Manager web console, click **Elements > Avaya Breeze® > Cluster Administration > DR Cluster 1**.
3. In the **Cluster** field, select **Oceana Monitor**.

4. To view the PU status of all the snap-ins, select **Cluster 2 > Grid Info**.
5. Verify that the PU status is `Intact`.

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

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

Verifying the CSC deployment status in DC1

About this task

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

Procedure

1. In your web browser, enter the following URL to view the Monitor Service page:
`https://<Cluster IP>/services/OceanaMonitorService/monitor.html`
2. On the Monitor Service page, click **Cluster 1 > Show cluster Messages**.
The page displays all the PUs in Cluster 1.
3. From the **Filters** column, select the **CallServerConnector** PU.
4. Verify that the `HEARTBEAT` message for the **CallServerConnector** PU is `INTACT`.

Verifying the CSC deployment status in DC2

About this task

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

Procedure

1. In your web browser, enter the following URL to view the Monitor Service page:
`https://<Cluster IP>/services/OceanaMonitorService/monitor.html`
2. On the Monitor Service page, click **Cluster 1 > Show cluster Messages**.
The page displays all the PUs in Cluster 1 (DR site).
3. From the **Filters** column, select the **CallServerConnector** PU.
4. Verify that the `HEARTBEAT` message for the **CallServerConnector** PU is `ACTIVE`.

Launch Oceana Monitor for DC1 and DC2 locations and verify PUs

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

Viewing Oceana Monitor Service pages

Procedure

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

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

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

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

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

Oceana Services Overview page

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

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

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

Monitor Service page

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

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

- View of snap-in lifecycle messages.

Monitor Service page field descriptions

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

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

Planned Switchover

Configure the primary site voice channel shutdown

About this task

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

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

Procedure

1. Log in to the Avaya Experience Portal web portal with the Administrator user role.
2. In the navigation pane, click **System Configuration > Applications**.
3. Select the appropriate application and click **Configurable Application Variables**.
4. In the **Active Data Center** field, click **DataCenter2**.
5. Click **Save**.

Configure the primary site email shutdown

About this task

Use this procedure to set the primary site EmailService on Avaya Oceana® Cluster 3 to false. If the email channel is not deployed on Avaya Oceana®, you can skip this procedure.

Procedure

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

Configure the primary site chat shutdown

About this task

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

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

* Note:

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

Procedure

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

4. Click **Commit**.

 Note:

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

Configuring the primary site MessagingService shutdown

About this task

Use this procedure to set the primary site MessagingService on Avaya Oceana® Cluster 3 to true. If the SMS, Social, or Async channels are not deployed on Avaya Oceana®, you can skip this procedure.

 Note:

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

Procedure

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

 Note:

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

Configure the primary site GenericChannelAPI service shutdown

About this task

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

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

Procedure

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

Note:

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

Restore UCMService after switchover

Backing up the UCMService database during planned switchover and switchback

About this task

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

You must take backups during the following events:

- Planned switchover and recovery
- Unplanned switchover and recovery

Note:

You can skip the procedure for the following:

- The email channel is not deployed at this installation, and, therefore, there are no deferred email capabilities.

- The partial or full DR switchover is for test purposes, and do not keep new UCM data post switch back to the primary site.
- You are not restoring the UCM DB from the DR site.

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

Before you begin

Ensure that all agents are logged out of their accounts.

Procedure

1. On the System Manager web console, click **Elements > Avaya Breeze® > Cluster Administration**.
 2. From **Backup and Restore**, select **Configure**.
System Manager displays the **Backup Storage Configuration** page.
 3. In the **FQDN or IP Address** field, enter the FQDN or IP Address of the backup storage server.
 4. In the **Login** field, enter the user name that you use to log in to the backup storage server.
 5. In the **Password** field, enter the password that you use to log in to the backup storage server.
 6. In the **SSH Port** field, enter the port number of the backup storage server.
 7. In the **Directory** field, enter the path to a directory in the backup storage server.
 8. In the **Retained backup copies per cluster per snap-in DB** field, specify the maximum number of backup file copies to retain on the backup storage server.
If you do not specify any value, the backup storage server retains all backup files.
 9. Click **Commit**.
 10. Select the check box for Avaya Oceana® Cluster 1.
 11. From **Backup and Restore**, select **Backup**.
System Manager displays the Cluster DB Backup page.
 12. On the **Cluster Database Backup** confirmation dialog box, select the **UCMService** check box, and click **Continue**.
 13. In **Backup Password**, enter a password for the backup.
-  **Important:**
- Note the password entered. You will require this password to restore the UCMService.
14. In **Schedule Job**, click **Run immediately**.
 15. Click **Backup**.

16. After the backup process is complete, verify the **Status** column on the **Backup and Restore Status** page. The status must display *Completed*.

Taking a backup of UCMSERVICE

About this task

Use this procedure to take a backup of the UCMSERVICE database. This service persists metadata related to deferred emails and requires this data to retrieve expired deferred emails and route them back to the appropriate agent. This service is installed on Avaya Oceana® Cluster 1.

Before you begin

Ensure that all agents are logged out of their accounts.

Procedure

1. On the System Manager web console, click **Elements > Avaya Breeze® > Cluster Administration**.
2. From the **Backup and Restore** field, select **Configure**.
System Manager displays the Backup Storage Configuration page.
3. In the **FQDN or IP Address** field, enter the FQDN or IP Address of the backup storage server.
4. In the **Login** field, enter the user name you use to log in to the backup storage server.
5. In the **Password** field, enter the password you use to log in to the backup storage server.
6. In the **SSH Port** field, enter the port number of the backup storage server.
7. In the **Directory** field, enter the path to a directory in the backup storage server.
8. In the **Retained backup copies per cluster per snap-in DB** field, specify the maximum number of backup file copies to retain on the backup storage server.
If you do not specify any value, the backup storage server retains all backup files.
9. Click **Commit**.
10. Select the check box for the Avaya Oceana® Cluster 1.
11. From the **Backup and Restore** field, select **Backup**.
12. On the Cluster Database Backup Confirmation dialog box, select the **UCMSERVICE** check box and click **Continue**.
13. In the **Backup Password** field, enter a password for the backup.
 **Important:**
Note the password because you require this password to restore UCMSERVICE.
14. In the **Schedule Job** field, click **Run immediately**.
15. Click **Backup**.

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

Taking a backup of UCASStoreService in Data Center 1

About this task

Use this procedure to take a backup of UCASStoreService.

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 **UCASStoreService** 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`.

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

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

Oceana POM switchover

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

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

Validating contacts

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

Logging out supervisors and agents

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

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

Before you begin

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

Procedure

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

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

Important:

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

2. **(Optional)** To open the Oceana Manager page through System Manager, do the following:
 - a. On the System Manager web console, click **Elements > Avaya Breeze® > Cluster Administration**.
 - b. On the Cluster Administration page, in the **Service URL** column for Avaya Oceana® Cluster 1, select **Oceana Manager**.
3. Log in to Oceana Manager using an Admin account.

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

Omnichannel database switchover

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

Note:

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

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

OCP DB switchover with Campus HA 2+1

Removing cache mirroring from Campus Standby

About this task

Use this procedure to remove cache mirroring from Campus Standby.

Procedure

1. In your web browser, enter the following URL to open Cache Management Portal:
`http://<IP>:57772/csp/sys/UtilHome.csp`
<IP> is the IP address of the standby Omnichannel server in Data Center 1.
2. On the Cache Management Portal login page, do the following:
 - a. In the **User Name** field, type `_admin`.
 - b. In the **Password** field, type `Oceana16`.
 - c. Click **LOGIN**.
3. Go to **System Administration > Configuration > Mirror Settings > Edit Mirror > Remove Mirror Configuration**.

4. To remove the mirrored attribute, click **Yes** and then click **Remove**.

Switching over DR server

Promoting Omnichannel server in DC2

About this task

Use this procedure to promote the async server in the DR site when the active server in primary and async server in DR location is available, and mirroring is operational for planned maintenance windows. You can use this procedure irrespective of whether a dual server pair is deployed on the primary site.

Procedure

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

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

For more information on setting up the ACM to point to the new Omnichannel database, see [Pointing ACM to the new Omnichannel database server in DC2](#) on page 37.

Demoting primary to async

About this task

Use this procedure to demote the primary server to async.

Procedure

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

1. Navigate to **CCDINSTANCE** and click **Start Caché**.
2. Navigate to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement` folder.
3. Double-click the `OceanaDataManagementTool.exe` file.
4. In the Oceana Data Management utility, click **Backup And Restore**.
5. In the navigation pane, click **Backup And Restore node > Backup And Restore**.
6. Click **Mirror Configuration**.

7. In the **Select Mirror Scenario** field, select **Demote to Async**.
8. Click **Execute**.

Pointing ACM to the new Omnichannel database server in DC2

About this task

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

Procedure

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

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

Switching over Avaya Analytics™ from DC1 to DC2

About this task

Using the following steps you can switch over to DC2 standby.

Note:

- You must perform this switch over only during a maintenance window.
- Ensure that the data replication between DC1 and DC2 is functional. To check replication status, see *Maintaining and Troubleshooting Avaya Oceana®* document.
- If source version is older than 4.2 mstr data between DC1 and DC2 does not sync during the Geo. MSTR configuration at DC1 is not replicated to DC2 during Geo.
- Take mstr database and Analytics database backup on DC1. For more information, see *Maintaining and Troubleshooting Avaya Oceana®* document.

Before you begin

Ensure that the secondary data center is on standby mode.

Procedure

1. Log in to the Cluster Control Manager (CCM) console on DC2 as the customer user.

2. To switch to the root user, type `su` and press **Enter**.
3. To run the `Analytics Administration` script, use the following command:

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



Warning:

You must use this option only on the secondary data center.

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

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



Important:

If source version (version from which you have planned the upgrade) is 4.2 and above, then perform the following steps.

9. To restart below services using post install scripts, do the following:
 - a. Restart Measure Processors.
To run `Analytics Administration` script, use the following command:

```
ccm release orca analytics
```
 - b. Select **Troubleshooting > General > Restart Measure Processors**.
Wait till all the measure processors are up. After restarting Measure Processors, pods restart.
 - c. Verify whether the pods restart successfully using the following command:

```
kubect1 get pods | grep orca
```


For a successful restart, all the pods must be in 1/1 state.
- a. Restart orca-scheduler and orca-admin-data-service.
- b. Restart mstr pods (required when upgrading from 4.2 release).

```
Run k delete pods -n mstr <msr-srv-pod-name> --force --grace-period=0
```

```
Run k delete pods -n mstr <msr-web-pod-name> --force --grace-period=0
```

10. To return to the previous page, type **b** and press **Enter**.
11. To exit from the current page, type **q** and press **Enter**.
12. To return to the main menu, type **m** and press **Enter**.

Next steps

Run the reports at DC2 in MicroStrategy to ensure that all the required data is available at the DC2. Ensure that all MicroStrategy configurations are available at DC2.

Promoting Avaya Analytics™ on DC2 as primary

About this task

Important:

Perform this procedure only if Avaya Analytics™ version is older than 4.2.

Using the following steps you can promote DC2 to primary role after a fail over.

Procedure

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


```
ccm release orca analytics
```
 - d. To select the **Geo/High Availability** option, enter the corresponding number.
 - e. To select the **Geo Options** option, enter the corresponding number.
 - f. To configure the primary cluster, select **Configure Primary Geo cluster** by entering the corresponding number.
 - g. In the **Proceed to Primary Geo cluster config** field, enter `y`.
 - h. Enter the CCM IP address of the Geo Standby cluster (DC2).
 - i. Enter the username to login to CCM of the Geo Standby cluster (DC2).
 - j. Enter the password to login to CCM of the Geo Standby cluster (DC2) and click **Enter**.
 - k. Note the IP address that you receive at the end of this process.

Note:

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

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

2. To return to the previous page, type **b** and press **Enter**.

3. To exit from the current page, type `q` and press **Enter**.
4. To return to the main menu, type `m` and press **Enter**.

Configuration and Validation

Verifying the CSC deployment status in DC2

About this task

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

Procedure

1. In your web browser, enter the following URL to view the Monitor Service page:
`https://<Cluster IP>/services/OceanaMonitorService/monitor.html`
2. On the Monitor Service page, click **Cluster 1 > Show cluster Messages**.
The page displays all the PUs in Cluster 1 (DR site).
3. From the **Filters** column, select the **CallServerConnector** PU.
4. Verify that the `HEARTBEAT` message for the **CallServerConnector** PU is `ACTIVE`.

Preparing UCMService in DC2 for database restore

About this task

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

Procedure

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

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

About this task

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

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

Before you begin

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

Procedure

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

Configure the DR site EmailService startup

About this task

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

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

Procedure

1. On the System Manager web console of Data Center 2, click **Elements > Avaya Breeze® > Configuration > Attributes**.
2. On the DR site Service Clusters tab, do the following:
 - a. **Cluster**: Select DR site Avaya Oceana® Cluster 3.
 - b. **Service**: Select **EmailService**.
3. In **Deployment status of emailmanager**, do the following:
 - a. Select the **Override Default** check box.

- b. In **Effective Value**, change the value from `false` to `true`.
4. Click **Commit**.

Configure the DR site Chat startup

About this task

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

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

Procedure

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

Note:

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

Configure the DR site MessagingService for Social, SMS or Async startup

About this task

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

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

Procedure

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

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

 Note:

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

Configure the DR site GenericChannelAPI Service startup

About this task

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

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

Procedure

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

 Note:

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

Verify the DR Application Enablement Services

About this task

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

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

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

Procedure

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

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

- Switch Connection 1
- Switch Connection 2

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

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

The two switch connections are displayed in this menu.

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

Changing cluster activity status for clusters in Data Center 2

Before you begin

Ensure that the OceanaMonitorService is installed on the clusters in Data Center 2.

Procedure

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

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

 Important:

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

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

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

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

Avaya Workspaces Agent switchover

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

The default Avaya Workspaces URL for both locations are:

- **Primary Site:**

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

- **DR Site:**

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

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

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

Before you begin

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

Procedure

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

For a partial DR switchover, select Avaya Oceana® and Avaya Analytics™.

4. Click **Toggle** to use the applications from Avaya Oceana® in DC2

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

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

Validate and test deployed channels

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

Verify the real time and historical reports on DC2

Ensure that you can see all required historical data using MSTR. When Avaya Analytics™ on DC2 is connected to Avaya Oceana® on DC2, ensure that all the real time and historical data is available in Avaya Analytics™. If you are upgrading from version older than 4.2, then ensure that MSTR is configured on DC2. For more information, refer *Using Avaya Analytics™ Reports for Avaya Oceana®*.

Chapter 4: Migrating Avaya Oceana[®] and Avaya Analytics[™] on DC1

Overview

The subsequent sections contains the reference to procedures for migrating Avaya Oceana[®] and Avaya Analytics[™].

Avaya Analytics[™]

Avaya Analytics[™] 4.3.1.1 is compatible with Avaya Oceana[®] 3.10.0.2 release. If you are on Avaya Analytics[™] 4.1.x or 4.1.2 release, then you have to migrate the Avaya Analytics[™] to 4.3.1.1. For more information, see *Migrating Avaya Oceana[®]* documentation available on the Avaya Support website at <https://support.avaya.com>. If you are on Avaya Analytics[™] 4.2, 4.3, or 4.3.1.0 release, then you have to upgrade to Avaya Analytics[™] 4.3.1.1. For information about the upgrade, see Avaya Analytics[™] 4.3.1.1 release notes.

For information about migrating from Avaya Analytics[™] 4.x to 4.3.1.1, see *Migrating Avaya Oceana[®]* document available on the Avaya Support website at <https://support.avaya.com>.

For information about upgrading from Avaya Analytics[™] 4.2 to 4.3.1.1, see *Migrating Avaya Oceana[®]* document available on the Avaya Support website at <https://support.avaya.com>.

Migrate Avaya Oceana[®]

The Avaya Oceana[®] migration procedure replaces each existing Avaya Breeze[®] platform server in the cluster with a new server installed from the latest release of Avaya Breeze[®] platform OVA.

The migration procedure consists of the following sections:

- Prerequisite for migration
- Pre-migration tasks
- Migration tasks
- Post migration tasks

For more information about the detailed migration procedure and migrating Omnidatabase server from 2019 to 2022, see *Migrating Avaya Oceana[®]* document available on the Avaya Support website at <https://support.avaya.com>.

Important:

Do not accept services for all DC1 clusters after completing the migration.

Upgrading the Omnichannel server

Enabling or disabling a scheduled computer maintenance in Windows 2019

About this task

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

Procedure

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

Upgrading Omnichannel servers from Avaya Oceana® 3.8.1.1 and later versions to Avaya Oceana® 3.10.0.2 version on Data Center 1

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

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

Data Center 1 has the Campus installation and Data Center 2 has the DR installation. This procedure provides instructions for upgrading the Omnichannel server in DC1 after completing the Planned Partial Failover to DC2.

Remove the current Cache Mirroring configuration in Data Center 1

In the Mirroring configuration with failover and backup servers (Campus HA and DR, 2+1), ensure that you have deployed the following Omnichannel Database servers:

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

- Omnichannel Server C as the original async member on DC1 which is now the primary member after switchover.

Remove the Omnichannel Database Mirroring in the following order:

Remove Omnichannel Database Mirroring from the backup server (Server A) in Data Center 1.

Removing Cache Mirroring from the backup Omnichannel server

Before you begin

Use this procedure to remove Cache Mirroring from the backup Omnichannel server.

Procedure

1. Open web browser and enter the following URL to open Cache Management Portal:
`http://<BackupOmnichannelServerIP>:57772/csp/sys/UtilHome.csp`
 <BackupOmnichannelServerIP> is the IP address of the backup Omnichannel Database server in Data Center 1.
2. On the Cache Management Portal login page, enter the following details:
 - a. In the **User Name** field, type `_admin`.
 - b. In the **Password** field, type `Oceana16`.
 - c. Click **LOGIN**.
3. Go to **System Administration > Configuration > Mirror Settings > Edit Mirror > Remove Mirror Configuration**.
4. Click **Yes** and then **Remove** to remove the mirrored attribute.

Taking a backup of the Omnichannel database for failure upgrade

About this task

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

Procedure

1. Log in to the Omnichannel server.
2. For Avaya Oceana® 3.7 or higher version, go to the
`OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement` folder.
3. For Avaya Oceana® 3.7 or higher version, double-click the
`OceanaDataManagementTool.exe` file.
4. In the Oceana Data Management utility, click **Backup and Restore**.
5. In the navigation pane, click **Backup and Restore**.
6. In the **Select/create file to backup to** field, click **Browse**.

7. On the Save As screen, do the following:
 - a. Select the location to save the backup file.
Do not save the backup file to the software, journal, or multimedia drive.
 - b. Specify a name for the backup file. When naming the file, use English or numeric characters only.
 - c. Click **Save**.
8. Click **Backup Database**.
The utility displays the Backup complete! message when the backup process is complete.
9. Verify that the backup file is created at the specified location.

Upgrading the latest version of the Omnichannel server software on the Omnichannel server in Data Center 1

About this task

Use this procedure to upgrade the Omnichannel server in the following order:

1. Upgrade Omnichannel server A
2. Upgrade Omnichannel server B

Important:

You must install, run, and patch the Omnichannel server software using a Windows Administrator account with full Administrator privileges. You must run the Oceana Data Management Tool using this same account.

Procedure

1. Log in to the Omnichannel server A.
2. Right-click the OCEANA_x.x.xxx.iso file and click **Mount**.
3. Double-click the Setup.exe file.
4. If the installer prompts you to restart the server, click **Yes**.
5. Click **Next**.
6. On the AVAYA GLOBAL SOFTWARE LICENSE TERMS screen, click **I ACCEPT THE LICENSE TERMS**.
7. After the installation is complete, click **Restart**.
8. Repeat step 1 to step 7 for Omnichannel server B.

Avaya Analytics™ Installation and migration on DC1

Use the following checklist for upgrading Avaya Analytics™. The following table has a high level procedure to install Avaya Analytics™ version 4.3.1.1 at DC1 and start data migration from DC2 to DC1.

*** Note:**

For this release, Avaya Analytics™ 4.3.1.1 is supported.

! Important:

Avaya Analytics™ supports migration from:

- versions 4.0.0.1, 4.1.0.1, 4.1.1.0 and 4.1.2.0 to 4.2
- versions 4.1.1.0 and 4.1.2.0 to 4.3.1.1

Avaya Analytics™ does NOT support the migration from versions 4.0.0.1, 4.1.0.1 to 4.3.1.1.

Table 1: Upgrading from Avaya Analytics™ version 4.2 and above

No.	Task	Description	✓
1	Install Avaya Analytics™ version 4.3.1.1 at DC1.	Refer “Deploying Avaya Analytics™ online” and “Deploying Avaya Analytics™ offline” in the <i>Deploying Avaya Analytics™ for Avaya Oceana®</i> document.	
2	Promote DC2 Avaya Analytics™ as Primary and configure DC1 Avaya Analytics™ version 4.3.1.1 as Standby.	Refer Promoting Avaya Analytics on DC2 as primary and configuring Avaya Analytics on DC1 as standby on page 52.	

Table 2: Migrating from Avaya Analytics™ version 4.1.1.0 or 4.1.2.0

No.	Task	Description	✓
1	Install Avaya Analytics™ version 4.3.1.1 at DC1.	Refer “Deploying Avaya Analytics™ online” and “Deploying Avaya Analytics™ offline” in the <i>Deploying Avaya Analytics™ for Avaya Oceana®</i> document.	
2	Start migration from 4.1.1.0 or 4.1.2.0 to Avaya Analytics™ 4.3.1.1 on DC1	Refer “Migrating Avaya Analytics™ 4.x Crunchy 2 data to Avaya Analytics™ 4.3 Crunchy 5 data”.	

Promoting Avaya Analytics™ on DC2 as primary and configuring Avaya Analytics™ on DC1 as standby

About this task

! Important:

Perform this procedure when you are upgrading from Avaya Analytics™ version 4.2 and above.

Before you begin

Install Avaya Analytics™ version 4.3.1.1 at DC1.

Procedure

1. If you are upgrading from Avaya Analytics™ version 4.2 and above, on the DC2, which is currently the primary site, do the following on the Cluster Control Manager (CCM) console:
 - a. To run the `Analytics Administration` script as root user, use the following command:

```
ccm release orca analytics
```
 - b. To select the **Geo/High Availability** option, enter the corresponding number.
 - c. To select the **Geo options** option, enter the corresponding number.
 - d. To configure DC2 to start replicating data back to DC1, select the **Configure Primary Geo cluster** option by entering the corresponding number.
 - e. Enter CCM IP address of the Geo Standby cluster (DC1).
 - f. Enter the username to login to CCM of the Geo Standby cluster (DC1).
 - g. Enter the password to login to CCM of the Geo Standby cluster (DC1) and click **Enter**.
 - h. Note the IP address and PV names that you receive at the end of this process.

* Note:

The script takes a few minutes to run, meanwhile it returns **IP address** and **PV name**.

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

After completing the above procedure, a backup job is triggered. You have to wait for backup job to complete and then proceed with the next step.

2. On the DC1 to make it a standby, do the following on the Cluster Control Manager (CCM) console:
 - a. Log in to the Cluster Control Manager (CCM) console in the DC1 cluster as the cust user.

- b. To switch to the root user, enter `su`.
- c. To disable firewall on DC1(standby), do the following:
- d. Run `cluster_ssh`.

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

- a. `node164182.puneccq.avaya.com`
 - b. `node164183.puneccq.avaya.com`
 - c. `node164184.puneccq.avaya.com`
- e. Run the firewall config command for each node and exit.

 Note:

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

- f. For example; Select [1].

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

3. To run the Analytics Administration script as root user, use the following command:

ccm release orca analytics

4. To select the **Geo/High Availability** option, enter the corresponding number.
5. To select the **Geo options** option, enter the corresponding number.
6. To configure the standby cluster, select the **Configure Standby Geo cluster** option by entering the corresponding number.
7. In the **Proceed to Standby Geo cluster config** field, enter `y`.
8. At the prompt for IP address, enter the IP address and PV names that you noted from the DC2. See step 1h.

 Note:

The script takes a few minutes to run.

At this point, DC2 is primary and data is now replicating from DC2 to DC1.

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

 Note:

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

The MSTR will not be accessible for standby data center.

For more information, see *Avaya Oceana® and Avaya Analytics™ Disaster Recovery* document.

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

Setting Source Crunchy 2 Environment

About this task

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

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

Before you begin

A single node cluster is deployed.

Procedure

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

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

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

In `orca-dbmgr-x.0.x`, substitute x for the version of orca-dbmgr running in the environment.

4. Log in to the Cluster Control Manager (CCM) console of the source system as the customer user.
5. Switch to being the root user by entering the command `su`.
6. Go to the directory where the script file is copied in the source system. The script file must have required permission.

7. Run the following command:

```
./HAsourcemigrate2to5.sh
```

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

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

Setting up target Crunchy 5 environment and migrating the data

About this task

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

Before you begin

A single node cluster must be deployed.

A Source system with Crunchy 2 environment must be configured.

Procedure

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

```
ccm release orca-dbmgr migration2to5.sh
```

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

* Note:

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

5. Enter the postgres password for the source database.

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

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

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

* Note:

The migration process on the target system can fail if the script on the source system does not finish its process. If the migration process fails on the target system, go

to the source system and ensure that the script `./HASourcemigrate2to5.sh` has successfully completed and shows status as `Process complete`.

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

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

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

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

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

 Note:

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

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

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

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

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

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

 Note:

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

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

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

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

This option is to exit the script.

Chapter 5: Perform Planned Switchback to DC1

Overview

In a partial switchback, Data center 2 (DC2) site is switched from the previous release to the latest Avaya Oceana® 3.10.0.2 release.

 Note:

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

Checklist for Partial controlled switchback

Preparation and validation

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

No.	Task	Description	✓
1	Prepare for switchback: Before starting any switchback operations on a production Avaya Oceana® and Avaya Analytics™ DR system, you must refer several key documents.	See the following documents: • Administering Avaya Aura® System Manager • Installing Avaya Control Manager • Administering Avaya Aura® Communication Manager • Administering Avaya Aura® Application Enablement Services	

Table continues...

No.	Task	Description	✓
2	Verify the CallServerConnector component in the primary site.	See Verifying the CallServerConnector component in the primary site on page 61.	
3	Verify deployment mode status of primary site email snap-in.	See Verifying deployment mode status of primary site email snap-in on page 61.	
4	Verify the shutdown mode status of primary site CustomerController chat snap-in.	See Verifying the shutdown mode status of primary site CustomerController chat snap-in on page 62.	
5	Verify the shutdown mode status of primary site MessaginService snap-in.	See Verifying the shutdown mode status of primary site MessagingService snap-in on page 62.	
6	Verify the shutdown mode status of primary site GenericChannelAPI snap-in.	See Verifying the shutdown mode status of primary site GenericChannelAPI snap-in on page 63.	
7	Verify deployment status of AMC snap-in for Avaya WebRTC Connect contacts.	See Verifying deployment status of AMC snap-in for Avaya WebRTC Connect contacts on page 63.	
8	Prepare primary DC1 Avaya Oceana® for potential UCA and UCM DB restore.	See the following: • Preparing DC1 for UCA and UCM database restore on page 64 • Preparing UCAStoreservice in DC1 for database restore on page 64 • Preparing UCMService in DC1 for database restore on page 65	
9	Validate contacts in DC2.	See Validating contacts on page 65.	
10	Log out supervisors and agents from DC2.	See Logging out supervisors and agents from the DR site on page 65.	

Partial controlled switchback

The following is a checklist of the list of steps to perform a Partial controlled switchback.

No.	Task	Description	✓
1	Shut down and switch back DR site voice channel to primary site.	See Shut down and switch back DR site voice channel to primary site on page 66.	
2	Configure the DR site email shutdown.	See Configuring DR site email shutdown on page 67.	
3	Configure the DR site MessagingService shutdown.	See Configuring DR site MessagingService shutdown on page 67.	
4	Configure the DR site chat shutdown.	See Configuring DR site chat shutdown on page 68.	
5	Configure the primary site GenericChannelAPI service shutdown.	See Configuring DR site GenericChannelAPI Service shutdown on page 68.	
6	Set the maintenance mode for web voice and web video.	See Setting the maintenance mode for web voice and web video on page 69.	
7	Shut down DR outbound channel.	See Oceana POM switchback on page 69.	
8	Change the cluster activity status for clusters in DC2.	See Changing the Cluster Activity status for the clusters in Data Center 2 on page 69.	
9	Install ClusterDBMigrationScript on Avaya Breeze® platform 3.9.0.x cluster 1.	See <i>Migrating Avaya Oceana®</i> document.	
10	Take a backup of UCASStoreService and UCMSERVICE on DC2.	See Backing up UCMSERVICE in DC2 on page 70.	
11	Restore UCASStoreService and UCMSERVICE data on DC1.	See Restoring UCASStoreService data in DC1 on page 72, Installing UCASStoreService in DC1 on page 72, and Restoring UCMSERVICE data in DC1 on page 71.	
12	Change the cluster activity status for clusters in DC1.	See Changing cluster activity status from Standby to Active for clusters in Data Center 1 on page 73.	
13	Restore the External Data Mart server.	See Restoring the External Data Mart server on page 74	
14	Reconfigure Avaya Oceana® addresses to DC1.	See Reconfiguring Avaya Oceana addresses to DC1 on page 76.	

Configuration and Validation

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

No.	Task	Description	✓
1	Clean up mirror setup on DC1 and DC2.	See Clean up Mirror setup on DC1 and DC2 on page 84.	
2	Configure Omnichannel Database High Availability (HA) with active and standby Omnichannel Database servers within Data Center 1	See <i>Deploying Avaya Oceana®</i> document.	
3	Configure the Web Voice and Web Video after Switchback.	See Configuring the Web Voice and Web Video after Switchback on page 87.	
4	Avaya Workspaces Agent switchover.	See Avaya Workspaces agent switchover on page 88.	
5	Validate and test deployed channels.	See Validate and test deployed channels on page 88.	

Preparation and Validation

Verifying the CallServerConnector component in the primary site

About this task

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

Procedure

1. On the Monitor Service page, click **Cluster 1 > Show cluster Messages**.
You can see all the PUs in Cluster 1.
2. From the **Filters** column, select **CallServerConnector** PU.
3. Verify that the HEARTBEAT message for **CallServerConnector** PU is **INTACT**.

Verifying deployment mode status of primary site email snap-in

About this task

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

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

Procedure

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

2. On the primary site Service Clusters tab, do the following:
 - a. **Cluster:** Select primary Cluster 3.
 - b. **Service:** Select `EmailService`.
3. In the **Advanced** area, in the **Deployment status of emailmanager** field, ensure that the field value is set to `true`.

 Note:

Setting the field value to `true` triggers the deployment as it is the default value.

4. Click **Commit**.

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

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

About this task

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

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

Procedure

1. On the System Manager web console, click **Elements > Avaya Breeze® > Configuration > Attributes**.
2. On the primary Site Service Clusters tab, do the following:
 - a. **Cluster:** Select `primary Cluster 3`.
 - b. **Service:** Select `CustomerControllerService`.
3. In the **Advanced** area, in the **Shutdown mode status** field, ensure that the field value is set to `false`.
4. Click **Commit**.

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

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

About this task

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

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

Procedure

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

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

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

About this task

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

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

Procedure

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

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

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

About this task

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

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

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

Procedure

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

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

Preparing DC1 for UCA and UCM database restore

About this task

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

Procedure

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

Important:

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

5. Click **Commit**.

Preparing UCAStoreservice in DC1 for database restore

About this task

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

Procedure

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

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

Preparing UCMService in DC1 for database restore

About this task

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

Procedure

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

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

Logging out supervisors and agents from the DR site

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

Validating contacts

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

 Note:

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

Planned Partial Switchback

Shut down and switch back DR site voice channel to primary site

About this task

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

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

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

Procedure

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

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

Configuring DR site email shutdown

About this task

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

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

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

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

Procedure

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

Configuring DR site MessagingService shutdown

About this task

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

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

Procedure

1. On the System Manager web console, click **Elements > Avaya Breeze® > Configuration > Attributes**.
2. On the Service Clusters tab, do the following:
 - a. **Cluster:** Select DR site Avaya Oceana® Cluster 3.
 - b. **Service:** Select **MessagingService**.
3. In **Shutdown Mode** status, do the following:
 - a. Select the **Override Default** check box.

- b. In the **Effective Value** field, change the value from `false` to `true`.
4. Click **Commit**.

Configuring DR site chat shutdown

About this task

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

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

Procedure

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

Configuring DR site GenericChannelAPI Service shutdown

About this task

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

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

Procedure

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

4. Click **Commit**.

Setting the maintenance mode for web voice and web video

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

Oceana POM switchback

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

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

Before you begin

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

Procedure

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

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

Important:

Create a bookmark for this URL in your web browser to open the Oceana Manager page even when System Manager is unavailable.

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

- e. Refresh the Clusters page in Avaya Breeze® platform EM and validate that all the clusters in the DR site are in the Deny state.

Backing up UCMService in DC2

About this task

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

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

- Planned switchover and switchback
- Unplanned switchover and switchback

Note:

You can skip the procedures for the following:

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

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

Before you begin

Ensure that all agents are logged out of their accounts.

Procedure

1. On the System Manager web console, click **Elements > Avaya Breeze® > Cluster Administration**.
2. From the **Backup and Restore** field, select **Configure**.
System Manager displays the Backup Storage Configuration page.
3. In the **FQDN or IP Address** field, enter the FQDN or IP Address of the backup storage server.
4. In the **Login** field, enter the user name that you use to log in to the backup storage server.
5. In the **Password** field, enter the password that you use to log in to the backup storage server.
6. In the **SSH Port** field, enter the port number of the backup storage server.
7. In the **Directory** field, enter the path to a directory in the backup storage server.
8. In the **Retained backup copies per cluster per snap-in DB** field, specify the maximum number of backup file copies that you want to retain on the backup storage server.

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

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

Restoring UCMSERVICE data in DC1

About this task

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

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

Before you begin

- Ensure that all agents are logged out of their accounts.
- Uninstall UCMSERVICE data from Avaya Oceana® Cluster 1 in Data Center 1.
- Ensure that the state of Avaya Oceana® Cluster 1 and Avaya Oceana® Cluster 3 is `Deny New Service`.

Procedure

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

11. In the Confirm Install service: UCMService dialog box, select the primary Avaya Oceana® Cluster 1 check box and click **Commit**.
12. On the Services page, verify that UCMService is in the `Installed` state.
13. Reboot Avaya Oceana® Cluster 1 and then Avaya Oceana® Cluster 3.

Restoring UCASStoreService data in DC1

Before you begin

Uninstall UCASStoreService from Avaya Oceana® Cluster 1 in Data Center 1.

Procedure

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

Installing UCASStoreService in DC1

About this task

Use this procedure to install UCASStoreService 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 UCASStoreService and click **Install**.
3. In the Confirm Install service: UCASStoreService dialog box, select the check box of Avaya Oceana® Cluster 1 and click **Commit**.
4. On the Services page, verify that the state of the service is `Installing`.
The state changes to `Installed` when the installation is complete.
5. Reboot Avaya Oceana® Cluster 1.

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

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

Before you begin

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

Procedure

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

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



Important:

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

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

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

On Cluster 1, verify the PUs deployed and status is **Intact** including CSC. CSC PU is not deployed if the **Oceana > CSC > AES > CM** configuration is not done and validated. On Cluster 3, verify the PUs deployed and status is **Intact** including the Email PU. Verify that all nodes and clusters in the DR location are set to status **Accepting**. If any clusters or

nodes are in **Deny** state, then re-do the above steps or manually set them to **Accepting** state using the Avaya Breeze® platform EM cluster overview page.

Restoring the External Data Mart server

About this task

Context Store External Data Mart (EDM) is an external component of Avaya Oceana®.

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

When you restore to Data Center 1, copy the EDM contents from Data Center 2 to the EDM in Data Center 1. Ensure that you backup and restore the database to complete the restoring of Context Store EDM.

Before you begin

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

Procedure

1. Log in to the primary SQL Server hosting the EDM database in Data Center 2.
You must log in with the SQL Server domain user credentials with administrative right to all SQL Server(s) hosting the EDM on DC2.
2. Open SQL Server Management Studio.
3. In the Object Explorer pane, click **Connect > Database Engine**.
SQL Server Management Studio displays the Connect to Server dialog box.
4. In the **Server name** field, select the local instance of SQL Server.
5. In the **Authentication** field, select **SQL Server Authentication**.
6. In the **Login** and **Password** fields, enter the system administrator credentials.
The system administrator is usually the default sa user created during SQL Server installation.
7. Click **Connect**.
8. In the Object Explorer pane, click **Databases > <EDM Database>**.
9. Right-click the EDM database and click **Tasks > Back Up**.
SQL Server Management Studio displays the Back Up Database dialog box.
10. In the navigation pane, click **General**.
11. In the **Backup type** field, select **Full**.
12. In the **Destination** area, click **Add**.

13. In the Select Backup Destination dialog box, select the backup folder location, specify the backup file name with the `.bak` extension, and click **OK**.

Ensure that the SQLService User login (services.msc) has full permissions on the backup folder.

14. To provide full permissions to the SQLService User login, do the following:
 - a. Go to the backup folder location.
 - b. Right-click the backup folder and click **Properties**.
 - c. On the Security tab, select the SQLService User login and click **Edit**.
 - d. In the **Permissions** area, select the **Full control** check box.
 - e. Click **OK**.
15. In the navigation pane, click **Media Options**.
16. In the **Overwrite media** area, select **Overwrite all existing backup sets**.
17. In the **Reliability** area, select the **Verify backup when finished** check box.
18. In the navigation pane, click **Backup Options**.
19. In the **Description** field, type a description for the backup.
20. In the **Set backup compression** field, select **Compress backup**.
21. Click **OK**.
22. Log in to the primary SQL Server hosting the EDM database in Data Center 1.
 You must log in with the SQL Server domain user credentials with administrative right to all SQL Server(s) hosting the EDM on DC1.
23. Open SQL Server Management Studio.
24. In the Object Explorer pane, click **Connect > Database Engine**.
 SQL Server Management Studio displays the Connect to Server dialog box.
25. In the **Server name** field, select the local instance of SQL Server.
26. In the **Authentication** field, select **SQL Server Authentication**.
27. In the **Login** and **Password** fields, enter the credentials of the system administrator.
 The system administrator is usually the default sa user created during SQL Server installation.
28. Click **Connect**.
29. In the Object Explorer pane, click **Databases > <EDM Database>**.
30. Right-click the EDM database and click **Tasks > Restore > Database**.
 SQL Server Management Studio displays the Restore Database dialog box.
31. In the navigation pane, click **General**.

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

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

For example:

```
USE CSEDM;  
GO  
sp_change_users_login @Action='update_one', @UserNamePattern='csEDMLogin',  
    @LoginName='csEDMLogin';  
GO
```

Reconfiguring Avaya Oceana® addresses to DC1

About this task

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

Procedure

1. Log in to Avaya Control Manager with an administrator user role.
2. On the Avaya Control Manager webpage, click **Configuration > Avaya Oceana™ > Server Details**.
3. Double-click the **UCAServer** instance.
4. Select the **System Properties** tab.
5. Expand **Omni Channel**.
6. In the **Omni Channel Database Server** field, type the hostname or IP address pointing to the Omnichannel server in Data center 1.

Note:

Enter the hostname of the VIP if using Omnichannel database mirroring. Otherwise, enter the name of the Omnichannel database server as administered in the

HTTPS certificate installed on the Omnichannel database server. However, for lab deployments customers you can use IP address.

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

Pointing ACM to the Omnichannel database server in DC1

About this task

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

Procedure

1. Log on to Avaya Control Manager.
2. Navigate to **Configuration > Avaya Oceana™ > Server Details**.
3. Double-click the administered Avaya Oceana® server or select the administered Avaya Oceana® server and click **Edit**.
4. Click the **System Properties** tab.
5. Expand **Omni Channel**.
6. In **Omni Channel Database Server**, enter the name, host name, or IP address of the Omnichannel Database in DC1 as administered in the HTTPS certificate installed on the Omnichannel Database server. The name must match the name on the certificate, and the certificate must also be trusted to avoid any certificate errors.

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

Completing the migration from Avaya Analytics™ 4.x to Avaya Analytics™ 4.3

About this task

Perform the procedure only when source version is older than Avaya Analytics™ 4.2.

Related links

[Breaking link to source and making target independent](#) on page 78

[Migrating the Microstrategy Database](#) on page 79

[Renaming the database](#) on page 80

Breaking link to source and making target independent

About this task

Perform this procedure in the maintenance window and when there are no incoming contacts entering the system.

Caution:

Post the procedure you cannot migrate any data from DC2 to DC1.

Perform this procedure on the target DC1.

Before you begin

Check the migration status for row count before breaking the link between source and target database.

Procedure

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

```
ccm release orca-dbmgr migration2to5.sh
```

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

Note:

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

5. Enter the postgres password for the source database.

The default system password for postgres user on the system is `myflexuser01`.

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

The following options are displayed on the screen:

- ```
1)migrate source to target
2)cleanup failed attempt
3)break link to source make target independent
4)check migration status
5)quit
```

Choose option to run: Options list:

**! Important:**

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

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

6. Type 3 for the **Break link to source make target independent**, enter the corresponding number.

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

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

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

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

This option is to exit the script.

**Related links**

[Completing the migration from Avaya Analytics 4.x to Avaya Analytics 4.3](#) on page 77

**Migrating the Microstrategy Database****About this task**

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

**Before you begin**

Single node cluster must be deployed.

Source system with Crunchy 2 environment must be configured.

Target system with Crunchy 5 environment must be configured.

**Procedure**

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

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

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

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

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

5. When prompted, enter the Microstrategy host, and port values noted from the output of running the **HAsourcemigrate2to5.sh** script on the source CCM in the *Setup Source Crunchy 2 Environment* section.
6. Run the following commands in the primary pod:

```
bash-4.4$ cd pgdata
bash-4.4$ pg_dump -U postgres -W -f mstr.sql avaya_analytics_md --if-exists --
clean --create -h Microstrategy_HOST -p Microstrategy_PORT
bash-4.4$ psql -f mstr.sql
bash-4.4$\l
```

#### \* Note:

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

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

7. Run the command **exit** to exit from pod and return to CCM.

## Related links

[Completing the migration from Avaya Analytics 4.x to Avaya Analytics 4.3](#) on page 77

## Renaming the database

### About this task

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

### Before you begin

Complete [Migrating the Microstrategy Database](#) on page 79.

### Procedure

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

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

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

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

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

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

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

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

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

#### 5. Run the command `\q` to exit psql.

#### 6. Run the command `exit` to exit the pod and return to CCM.

### Related links

[Completing the migration from Avaya Analytics 4.x to Avaya Analytics 4.3](#) on page 77

## Restarting orca-dbmgr pod

### About this task

Use this procedure to restart the orca-dbmgr pod. Perform this procedure on DC1.

### Procedure

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

### \* Note:

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

## Restarting mstr-srv pod

### About this task

Use this procedure to restart the mstr-srv pod.

### Before you begin

Single-node to multinode cluster migration must be completed.

Upscaling of Avaya Analytics™ database must be completed.

## Procedure

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

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

Both passwords must be the same.

4. To stop the mstr-srv pod, run the following command:

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

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

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

 **Note:**

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

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

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

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

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

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

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

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

 **Note:**

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

## Next steps

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

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

## Planned switch back to DC1

### Switching back to DC1 as primary

#### About this task

Use this procedure to switch back to DC1 as primary on Avaya Analytics™.

 **Note:**

- Perform this procedure only when upgrading from Avaya Analytics™ 4.2 Patch 2, 4.3 Patch 3, or 4.3.1.0 and above release.

- Perform this procedure during maintenance window.

### Before you begin

- Stop new calls from entering the system.
- Wait for the final processing of existing calls which is the main process contributing to the downtime. This depends on the system load during the cut over phase.
- Wait for the final Extract, Transform, Load (ETL) process after the last call is processed. After the last call is processed, the final ETL must take place within 15 minutes and takes around five to ten minutes to complete.

### Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Switch to being the root user by entering the command `su`.
3. Do the following to promote DC1 to Geo Primary:
  - a. Run the following command:  

```
ccm release orca analytics
```
  - b. To select **Geo/High Availability**, enter the corresponding number.
  - c. To select **Geo Options**, enter the corresponding number.
  - d. To select **Switch over**: promote secondary data center database to primary option, enter the corresponding number.
4. To restart below services using post install scripts, do the following:
  - a. Restart Measure Processors.  
 To run `Analytics Administration` script, use the following command:  

```
ccm release orca analytics
```
  - b. Select **Troubleshooting > General > Restart Measure Processors**.  
 Wait till all the measure processors are up.
  - c. Restart `orca-scheduler` and `orca-admin-data-service`.
5. Configure the required connections to communicate with Avaya Oceana® on DC1.

#### **Note:**

- You can also do this step outside the maintenance window.
- Run the reports at DC1 in MicroStrategy to ensure that all the required data is available at the DC1. Ensure that all MicroStrategy configuration is available at DC1.

### Result

At the end, DC1 Avaya Analytics™ 4.3.1.1 no longer syncs data from 4.x DC2.

---

## Configuration and Validation

### Clean up Mirror setup on DC1 and DC2

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

 **Important:**

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

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

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

 **Note:**

If you do not have dual server setup on DC1, you can ignore [Removing mirroring configuration on Omnichannel Server B](#) on page 85.

### Removing mirroring configuration on Omnichannel Server A

#### Procedure

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

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

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

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

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

- a. In the **User Name** field, type `_admin`.
- b. In the **Password** field, type `Oceana16`.
- c. Click **LOGIN**.

3. Go to **System Administration > Configuration > Mirror Settings > Edit async**.

4. Select **Remove mirror configuration**.

5. For Remove mirror attribute, select `Yes`.

6. Click **Remove**.

7. Remove any Journal files beginning with MIRROR in

`E:\AVAYA\OCEANA\DATABASES\JOURNAL` where E represents the Journal drive.

## Removing mirroring configuration on Omnichannel Server B

### Procedure

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

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

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

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

2. On the Cache Management Portal login page, do the following:
  - a. In the **User Name** field, type `_admin`.
  - b. In the **Password** field, type `Oceana16`.
  - c. Click **LOGIN**.
3. Go to **System Administration > Configuration > Mirror Settings > Edit mirror**.
4. Select **Remove mirror configuration**.
5. Select **Clear mirror flag**.
6. In the System Management tray, right-click the greyed out Cache cube icon.
7. Select **Stop Cache**.
8. Select **Restart**.
9. Navigate to the Cache Management Portal.
10. Go to **System Administration > Configuration > Mirror Settings > Edit mirror**.
11. Select **Remove mirror configuration**.
12. For Remove mirror attribute, select `Yes`.
13. Click **Remove**.
14. Remove any Journal files beginning with MIRROR in  
`E:\AVAYA\OCEANA\DATABASES\JOURNAL` where E represents the Journal drive.

## Removing mirroring configuration on Omnichannel Server C

### Procedure

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

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

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

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

2. On the Cache Management Portal login page, do the following:
  - a. In the **User Name** field, type `_admin`.

- b. In the **Password** field, type Oceana16.
  - c. Click **LOGIN**.
3. Navigate to **System Administration > Configuration > Mirror Settings > Edit mirror**.
4. Select **Remove mirror configuration**.
5. Select **Clear mirror flag**.
6. In system management tray, right-click the greyed out Cache cube icon.
7. Select **Stop Cache**.
8. Select **Restart**.
9. Navigate to the Cache Management Portal.
10. Navigate to **System Administration > Configuration > Mirror Settings > Edit mirror**.
11. Select **Remove mirror configuration**.
12. For Remove mirror attribute, select **Yes**.
13. Click **Remove**.
14. Remove any Journal files beginning with MIRROR in  
E : \AVAYA\OCEANA\DATABASES\JOURNAL where E represents the Journal drive.

## Creating a data backup on Server C

### Procedure

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

#### **Important:**

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

7. Specify a name for the backup file.

#### **Note:**

When naming the file, use English or numeric characters only.

8. Click **Save**.
9. Click **Backup Database**.

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

## Next steps

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

## Restoring data on Server A

### Procedure

1. Copy the backup file from Server C to Server A.
2. Navigate to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement` folder.
3. Double-click the `OceanaDataManagementTool.exe` file.
4. In the Oceana Data Management utility, click **Backup And Restore**.
5. In the navigation pane, click **Backup And Restore**.
6. In the **Select file to restore from** field, click **Browse**.
7. On the Open dialog box, browse to the location where you stored the backup file.
8. Select the backup `.cbk` file.
9. Click **Open**.
10. Click **Restore Database**.
11. For **Are you restoring a mirrored backup**, click **Yes**.
12. Click **Restore**.

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

## Configuring the Web Voice and Web Video after Switchback

### About this task

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

### Procedure

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

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

## Avaya Workspaces agent switchover

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

The default Avaya Workspaces URL for both locations are:

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

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

## Validate and test deployed channels

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

## Verify the real time and historical reports on DC1

Ensure that you can see all required historical data using MSTR. When Avaya Analytics on DC1 is connected to Avaya Oceana on DC1, ensure that all the real time and historical data is available in Avaya Analytics. If you are upgrading from version older than 4.2, then ensure that MSTR is configured on DC1. For more information, refer Using Avaya Analytics™ Reports for Avaya Oceana®.

# Chapter 6: Migrating to Avaya Oceana® and Avaya Analytics™ on DC2

---

## Overview

The subsequent sections contain the reference to procedures for migrating Avaya Oceana® and Avaya Analytics™.

### Avaya Analytics™

Only Avaya Analytics™ 4.3.1.1 is compatible with Avaya Oceana® 3.10.0.2 release. If you are on Avaya Analytics™ 4.1.x or 4.1.2 release, then you have to migrate the Avaya Analytics™ to 4.3.1.1. For more information, see *Migrating Avaya Oceana®* documentation available on the Avaya Support website at <https://support.avaya.com>. If you are in Avaya Analytics™ 4.2, 4.3, or 4.3.1.0 release, then you have to upgrade to Avaya Analytics™ 4.3.1.1. For information about the upgrade, see Avaya Analytics™ 4.3.1.1 release notes.

For information about migrating from Avaya Analytics™ 4.x to 4.3.1.1, see *Migrating Avaya Oceana®* document available on the Avaya Support website at <https://support.avaya.com>.

For information about upgrading from Avaya Analytics™ 4.2 to 4.3.1.1, see *Migrating Avaya Oceana®* document available on the Avaya Support website at <https://support.avaya.com>.

### Migrate Avaya Oceana®

The Avaya Oceana® migration procedure replaces each existing Avaya Breeze® platform server in the cluster with a new server installed from the latest release of Avaya Breeze® platform OVA.

The migration procedure consists of the following sections:

- Migration tasks
- Post migration tasks

For more information about the detailed migration procedure and migrating Omnidatabase server from 2019 to 2022, see *Migrating Avaya Oceana®* document available on the Avaya Support website at <https://support.avaya.com>.

### Important:

Do not accept services for all DC2 clusters after completing the migration.

---

## Upgrading the Omnichannel server

### Enabling or disabling a scheduled computer maintenance in Windows 2019

#### About this task

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

#### Procedure

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

### Upgrading Omnichannel servers from Avaya Oceana® 3.8.1.1 and later versions to Avaya Oceana® 3.10.0.2 version on Data Center 2

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

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

Data Center 1 has the Campus installation and Data Center 2 has the DR installation. This procedure provides instructions for upgrading the Omnichannel server in DC2 after completing the Planned Partial Failback to DC1.

### Checklist for Omnichannel server upgrade

Use this checklist to upgrade Omnichannel servers from Avaya Oceana® 3.8.1.1 and later versions to Avaya Oceana® 3.10.0.2 version on Data Center 2.

| No. | Task                                                                                                      | Notes                                                                                                                                                                                         | ✓ |
|-----|-----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 1   | Download the latest version of the Omnichannel server software on the Omnichannel server.                 | You can download the latest version of the Omnichannel server software from <a href="https://support.avaya.com">https://support.avaya.com</a> . The format of the file is OCEANA_x.x.xxx.iso. |   |
| 2   | Take a backup of the Omnichannel database for failure upgrade.                                            | See <a href="#">Taking a backup of the Omnichannel database for failure upgrade</a> on page 49.                                                                                               |   |
| 3   | Upgrade the latest version of the Omnichannel server software on the Omnichannel server in Data Center 2. | See <a href="#">Upgrading the latest version of the Omnichannel server software on the Omnichannel server in Data Center 2</a> on page 92.                                                    |   |

## Taking a backup of the Omnichannel database for failure upgrade

### About this task

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

### Procedure

1. Log in to the Omnichannel server.
2. For Avaya Oceana® 3.7 or higher version, go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement` folder.
3. For Avaya Oceana® 3.7 or higher version, double-click the `OceanaDataManagementTool.exe` file.
4. In the Oceana Data Management utility, click **Backup and Restore**.
5. In the navigation pane, click **Backup and Restore**.
6. In the **Select/create file to backup to** field, click **Browse**.
7. On the Save As screen, do the following:
  - a. Select the location to save the backup file.  
Do not save the backup file to the software, journal, or multimedia drive.
  - b. Specify a name for the backup file. When naming the file, use English or numeric characters only.
  - c. Click **Save**.
8. Click **Backup Database**.  
The utility displays the `Backup complete!` message when the backup process is complete.
9. Verify that the backup file is created at the specified location.

## Upgrading the latest version of the Omnichannel server software on the Omnichannel server in Data Center 2

### About this task

Use this procedure to upgrade the Omnichannel server in the following order:

1. Upgrade Omnichannel server C

### ! Important:

You must install, run, and patch the Omnichannel server software using a Windows Administrator account with full Administrator privileges. You must run the Oceana Data Management Tool using this same account.

### Procedure

1. Log in to the Omnichannel server C.
2. Right-click the `OCEANA_x.x.xxx.iso` file and click **Mount**.
3. Double-click the `Setup.exe` file.
4. If the installer prompts you to restart the server, click **Yes**.
5. Click **Next**.
6. On the AVAYA GLOBAL SOFTWARE LICENSE TERMS screen, click **I ACCEPT THE LICENSE TERMS**.
7. After the installation is complete, click **Restart**.

---

## Avaya Analytics™ Installation on DC2

Use the following checklist for upgrading Avaya Analytics™. The following table has a high level procedure to install Avaya Analytics™ version 4.3.1.1 at DC2.

**Table 3: Upgrading from Avaya Analytics™ version 4.2 and above**

| No. | Task                                                                                                                   | Description                                                                                                                                             | ✓ |
|-----|------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 1   | Install Avaya Analytics™ version 4.3.1.1 at DC2.                                                                       | Refer “Deploying Avaya Analytics™ online” and “Deploying Avaya Analytics™ offline” in the <i>Deploying Avaya Analytics™ for Avaya Oceana®</i> document. |   |
| 2   | Promote DC1 Avaya Analytics™ version 4.3.1.1 as Primary and configure DC2 Avaya Analytics™ version 4.3.1.1 as Standby. | Refer <a href="#">Promoting Avaya Analytics on DC1 as primary and configuring Avaya Analytics on DC2 as standby</a> on page 93.                         |   |

**Table 4: Migrating from Avaya Analytics™ version 4.1.1.0 or 4.1.2.0**

| No. | Task                                             | Description                                                                                                                                                                                  | ✓ |
|-----|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 1   | Install Avaya Analytics™ version 4.3.1.1 at DC2. | Refer “Deploying Avaya Analytics™ online” and “Deploying Avaya Analytics™ offline” in the <i>Deploying Avaya Analytics™ for Avaya Oceana®</i> document.                                      |   |
| 2   | Configure Geo between DC1 and DC2.               | Refer <ul style="list-style-type: none"> <li>• <a href="#">Configuring DC1 as a Geo Primary</a> on page 96</li> <li>• <a href="#">Configuring DC2 as a Geo Standby</a> on page 97</li> </ul> |   |

## Promoting Avaya Analytics™ on DC1 as primary and configuring Avaya Analytics™ on DC2 as standby

### About this task

#### ! Important:

Perform this procedure when you are upgrading from Avaya Analytics™ version 4.2 and above.

### Before you begin

Install Avaya Analytics™ version 4.3.1.1 at DC2.

### Procedure

- On DC1, do the following on the Cluster Control Manager (CCM) console:
  - To run the `Analytics Administration` script as root user, use the following command:

```
ccm release orca analytics
```
  - To select the **Geo/High Availability** option, enter the corresponding number.
  - To select the **Geo options** option, enter the corresponding number.
  - Select the **Configure Primary Geo cluster** option by entering the corresponding number.
  - Enter CCM IP address of the Geo Standby cluster (DC2).
  - Enter the username to login to CCM of the Geo Standby cluster (DC2).
  - Enter the password to login to CCM of the Geo Standby cluster (DC2) and click **Enter**.

- h. Note the IP address and PV names that you receive at the end of this process.

 **Note:**

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

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

2. Wait for the backup job to complete and then proceed to configure the standby.

After the primary configuration is complete, a backup job starts automatically. Wait for the backup job to complete before proceeding.

3. On the DC2 to make it a standby, do the following on the Cluster Control Manager (CCM) console:

- a. Log in to the Cluster Control Manager (CCM) console in the DC1 cluster as the cust user.
- b. To switch to the root user, enter `su`.
- c. To disable firewall on DC2(standby), do the following:
- d. Run `cluster_ssh`.

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

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

- e. Run the firewall config command for each node and exit.

 **Note:**

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

- f. For example; Select [1].

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

4. To run the Analytics Administration script as root user, use the following command:

**ccm release orca analytics**

5. To select the **Geo/High Availability** option, enter the corresponding number.
6. To select the **Geo options** option, enter the corresponding number.
7. To configure the primary cluster, select the **Configure Standby Geo cluster** option by entering the corresponding number.

8. In the **Proceed to Standby Geo cluster config** field, enter `y`.
9. At the prompt for IP address, enter the IP address and PV names that you noted from the DC1. See step 1h.

 **Note:**

The script takes few minutes to run.

At this point, DC1 is primary and data is now replicating to DC2.

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

 **Note:**

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

The MSTR is not accessible for standby data center.

For more information, see *Avaya Oceana® and Avaya Analytics™ Disaster Recovery* document.

---

## Install Avaya Analytics™ version 4.3.1.1 and configure Geo

Perform this procedure if you are upgrading Avaya Analytics™ from versions 4.1.1.0, or 4.1.2.0 only.

 **Important:**

Avaya Analytics™ supports migration from:

- versions 4.0.0.1, 4.1.0.1, 4.1.1.0 and 4.1.2.0 to 4.2
- versions 4.1.1.0 and 4.1.2.0 to 4.3.1.1

Avaya Analytics™ does NOT support the migration from versions 4.0.0.1, 4.1.0.1 to 4.3.1.1.

### Related links

[Setting up DC2 for 4.3.1.1](#) on page 95

[Configuring DC1 as a Geo Primary](#) on page 96

[Configuring DC2 as a Geo Standby](#) on page 97

## Setting up DC2 for 4.3.1.1

### About this task

Use the following procedure to set up DC2 for 4.3.1.1.

## Procedure

Install the Avaya Analytics™ 4.3.1.1 software on DC2.

For more information on installing the Avaya Analytics™ 4.3.1.1 software, see the *Deploying Avaya Analytics™ online* chapter of the *Deploying Avaya Analytics™ for Avaya Oceana®* document.

### \* Note:

Note the CCM IP address and login credentials on the completed system.

## Related links

[Install Avaya Analytics version 4.3.1.1 and configure Geo](#) on page 95

# Configuring DC1 as a Geo Primary

## About this task

Use this procedure to configure the Geo configuration options for DC1 as a Geo Primary from the Analytics scripts utility. You can perform this procedure during maintenance window.

### \* Note:

Perform this procedure if you are upgrading from version older than Avaya Analytics™ 4.2.

## Before you begin

Ensure that Avaya Analytics™ 4.3.1.1 is installed on DC2.

After performing this procedure, a backup job is started. Wait for the backup job to complete and then only proceed.

## Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Switch to being the root user by entering the command `su`.
3. Do the following to configure DC1 as primary:
  - a. Run the following command:  

```
ccm release orca analytics
```
  - b. To select **Geo/High Availability**, enter the corresponding number.
  - c. To select **Geo Options**, enter the corresponding number.
  - d. To select **Configure Primary Geo cluster**, enter the corresponding number.
  - e. Enter CCM IP address of the Geo Standby cluster (DC2).
  - f. Enter the username to login to CCM of the Geo Standby cluster (DC2).
  - g. Enter the password to login to CCM of the Geo Standby cluster (DC2) and click **Enter**.

**\* Note:**

Note the IP address and PV name. The script takes some time to run and return IP address and PV name. You must use this IP address and PV name for configuring the standby data center. Wait for the backup job to complete and then proceed to configure the standby. After the primary configuration is complete, a backup job starts automatically. Wait for the backup job to complete before proceeding.

**Related links**

[Install Avaya Analytics version 4.3.1.1 and configure Geo](#) on page 95

## Configuring DC2 as a Geo Standby

**About this task**

Use the Geo configuration options to configure DC2 as a Geo Standby from the Analytics scripts utility.

**Procedure**

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Switch to being the root user by entering the command `su`.
3. To disable firewall on DC2 (standby), do the following:

- a. Run `cluster_ssh`.

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

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

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

**\* Note:**

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

- c. For example; Select [1].

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

- d. To exit from the current page, type `q` and press **Enter**.

4. Do the following to configure DC2 as Geo Standby:

- a. Run the following command:

```
ccm release orca analytics
```

- b. To select **Geo/High Availability**, enter the corresponding number.
  - c. To select **Geo Options**, enter the corresponding number.
  - d. To select **Configure Standby Geo cluster**, enter the corresponding number.
  - e. In the **Proceed to Standby Geo cluster config** field, enter `y`.
5. At the prompt for IP address, enter the IP address and PV name.
- The IP address and PV name is noted when configuring DC1 as a Geo Primary. See [Configuring DC1 as a Geo Primary](#) on page 96.
- The script takes some time to run. At this point, DC1 is primary and data is now replicating to DC2.
6. To return to the previous page, type `b` and press **Enter**.
  7. To exit from the current page, type `q` and press **Enter**.
  8. To return to the main menu, type `m` and press **Enter**.

 **Note:**

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

The MSTR will not be accessible for standby data center.

For more information, see *Avaya Oceana® and Avaya Analytics™ Disaster Recovery* document.

## Result

At the end:

- Geo-configured Avaya Oceana® and Avaya Analytics™ 4.3.1.1 is on DC1.
- DC2 Avaya Analytics™ 4.3.1.1 now Geo Standby reads data from 4.3.1.1 DC1 Geo Primary.

## Related links

[Install Avaya Analytics version 4.3.1.1 and configure Geo](#) on page 95

# Chapter 7: Post migration tasks

---

## Post migration checklist

Use the following checklist for the tasks that you must perform after completing the DR migration:

| No. | Task                                                                  | Description                                                                                            | Notes                                                                    | ✓ |
|-----|-----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|---|
| 1   | Deploy Engagement Designer workflows and bundle tasks.                | See <a href="#">Deploying Engagement Designer workflows</a> on page 99.                                | If you have deployed the workflows already, then you can skip this step. |   |
| 2   | Set the state of Avaya Oceana® Cluster 1 to <b>Deny New Service</b> . | See <a href="#">Changing the Cluster Activity status for the clusters in Data Center 2</a> on page 69. |                                                                          |   |
| 3   | Recommission of DR.                                                   | See <a href="#">Recommission of Disaster Recovery</a> on page 100.                                     |                                                                          |   |

---

## Deploying Engagement Designer workflows

### Before you begin

Download the latest version of the sample workflow from PLDS.

### Procedure

1. In your web browser, enter the following URL to open the Engagement Designer Designer Console:  
`https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`
2. Click **Import**.
3. On the Import Workflow dialog box, click **Choose File**.
4. Browse to the sample workflow and click **Import**.
5. Click **Save Workflow**.

6. On the Save Workflow dialog box, do the following:
  - a. In the **Workflow** field, type a name for the workflow.
  - b. Select the folder where you want to save the workflow.
  - c. Click **Save**.
7. Click **Deploy Workflow**.
8. On the Deployment Details dialog box, click **OK**.

 **Note:**

You can either configure the workflow attributes while deploying the workflow or at a later time.

9. In your web browser, enter the following URL to open the Engagement Designer Admin Console:  
`https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`
10. On the Workflows tab, verify that the workflow is available in the list of deployed workflows.
11. Repeat Step 2 to Step 10 to deploy and verify all remaining workflows.

---

## Recommission of Disaster Recovery

As a part of the Disaster Recovery recommission, perform the following procedures:

- Validate and configure UCASoreService Geographic Redundancy.
- Validate and configure Context Store Geographic Redundancy.
- Enabling SSL connection for Context Store replication for DC1 to DC2.
- Validate and configure Omnichannel database mirroring.
- Clean up and reconfigure mirror setup on DC1 and DC2 section.

### Related links

[Validating and configuring UCASoreService Geographic Redundancy](#) on page 100  
[Validating and configuring Avaya Context Store Geographic Redundancy](#) on page 101  
[Recommission of Disaster Recovery](#) on page 102

## Validating and configuring UCASoreService Geographic Redundancy

### About this task

Use this procedure to validate and configure UCASoreService replication status on DC1 and DC2 sites.

## Procedure

1. Log on to Avaya Aura® System Manager.
2. On the System Manager web console, click **Elements > Avaya Breeze® > Configuration > Attributes**.
3. On the Service Clusters tab, select Cluster as DC1 cluster1.
4. In the Service dropdown list, select **UCAStoreService**.
5. In the Startup Configuration group, set the **Disaster recovery role** attribute to `GEO_MASTER` on DC1 and `GEO_SLAVE` on DC2.



### Important:

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

6. Click **Commit**.

## Related links

[Recommission of Disaster Recovery](#) on page 100

# Validating and configuring Avaya Context Store Geographic Redundancy

## About this task

Use this procedure to validate and configure Avaya Context Store replication status on DC1 and DC2 sites.

## Procedure

1. Log on to Avaya Aura® System Manager.
2. On the System Manager web console, click **Elements > Avaya Breeze® > Configuration > Attributes**.
3. On the Service Clusters tab, select Cluster as DC1 cluster1.
4. In the Service dropdown list, select **ContextStoreManager service**.
5. In the Geo redundancy Configuration group, set the GEO: Enable session preservation parameter value as `true`. Set the GEO: Target cluster Id select DC2 site cluster1, set the GEO: keystore file and password.
6. Click **Commit**.

## Related links

[Recommission of Disaster Recovery](#) on page 100

## Recommission of Disaster Recovery

### About this task

Use this procedure to recommission disaster recovery.

### Procedure

1. Uninstall UCASoreService on DC2.
2. Take a backup of UCA database from DC1.
3. Prevent changing on DC1 in 30 minutes.
4. Restore UCA database on DC2.
5. Install UCASoreService on DC2.
6. Reboot Avaya Oceana® cluster 1 of DC2.

For more detailed procedure on each of these tasks, see *Configuring Avaya Oceana® for Disaster Recovery* chapter in the *Avaya Oceana® and Avaya Analytics™ Disaster Recovery* document available on the Avaya Support website at <https://support.avaya.com>.

### Related links

[Recommission of Disaster Recovery](#) on page 100

---

## Configuring Context Store for Disaster Recovery

### Configuration Checklist

| No. | Task                                                                       | Description                                                                                                                                                                                                                                                                                                                      | ✓ |
|-----|----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 1.  | Enable SSL connection for Avaya Context Store replication from DC1 to DC2. | See <a href="#">Enabling SSL connection for Context Store replication from DC1 to DC2</a> on page 103.                                                                                                                                                                                                                           |   |
| 2.  | Retrieve the System Manager root certificate.                              | See <a href="#">Retrieving the System Manager root certificate</a> on page 103.                                                                                                                                                                                                                                                  |   |
| 3.  | Create a new keystore certificate file.                                    | See, <ul style="list-style-type: none"> <li>• <a href="#">Creating a new keystore certificate file</a> on page 104.</li> <li>• <a href="#">Modifying end entity profile</a> on page 105.</li> <li>• <a href="#">Creating a new keystore certificate file for Data Center 1 of Avaya Oceana Cluster 1</a> on page 105.</li> </ul> |   |

*Table continues...*

| No. | Task                                                                           | Description                                                                                                             | ✓ |
|-----|--------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|---|
| 4.  | Add CA root certificate and keystore certificate files to DC2 Cluster 1 nodes. | <a href="#">Adding CA root certificate and keystore certificate files to Data Center 2 Cluster 1 nodes</a> on page 106. |   |
| 5.  | Enable Context Store integration to External Data Mart in DC1.                 | <a href="#">Enabling Context Store integration to External Data Mart in Data Center 1</a> on page 107.                  |   |

## Enabling SSL connection for Context Store replication from DC1 to DC2

### About this task

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

#### \* Note:

Context Store replication functions only when DC1 has the security certificate.

### Procedure

1. Download the Root CA certificate to a location from where you can import it to Avaya Oceana® Cluster 1 nodes in DC2.
2. Create a new identity certificate or keystore certificate file signed by your Root CA for the Avaya Oceana® Cluster 1 FQDN and Avaya Breeze® platform nodes in DC2.
3. Log on as a root user and copy the Root CA certificate and generated keystore file to all Avaya Oceana® Cluster 1 nodes in DC2.

If you use Avaya Aura® System Manager as a CA function, you can retrieve the Root CA certificate as a .pem file from the primary System Manager in DC1.

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

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

## Retrieving the System Manager root certificate

### About this task

Use this procedure to retrieve the System Manager root certificate.

### Before you begin

You must have access to the System Manager console.

### Procedure

1. Log in to the Avaya Aura® System Manager web console in Data Center 1.

2. On the System Manager web console, click **Services > Security > Certificate > Authority**.
3. In the navigation pane, click **CA Structures & CRLs**.  
System Manager displays information of your primary System Manager CA certificate.
4. Click **Download PEM file** link to save a copy of System Manager CA certificate to your browser `Downloads` folder.
5. Go to `Downloads` folder and copy the CA certificate to a location that is accessible to Data Center 2 applications.

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

## Creating a new keystore certificate file

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

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

### Important:

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

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

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

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

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

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

## Modifying end entity profile

### About this task

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

### Procedure

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

You can also create a new profile and use it for Avaya Oceana®.

4. Scroll down to the Other subject attributes area.
5. In the **Subject Alternative Names** field, select **DNS Name**.
6. Click **Add**.

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

7. Click **Save**.

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

### Procedure

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

You must use the user name and password while creating the certificate.

6. In the **CN Common Name** field, enter the full FQDN of DC1 Avaya Oceana® Cluster 1.
7. In the Subject Alternative Name area, in the first **DNS Name** field, enter the FQDN of DC1 Avaya Oceana® Cluster 1.
8. In the next **DNS Name** field, enter the Avaya Oceana® Cluster 1 Node 1 Management full FQDN.

9. In the next **DNS Name** field, enter the Avaya Oceana® Cluster 1 Node 2 Management full FQDN.
10. In the next **DNS Name** field, enter the Avaya Oceana® Cluster 1 Node 3 Management full FQDN.
11. In the **Token** field, select `P12 file`.
12. Click **Add**.
13. Open System Manager public web portal.
14. On the left panel, click **Public Web**.  
System Manager displays the public web portal for CA functionality.
15. In the web portal, on the **Enroll** menu, click **Create Keystore**.
16. Enter the **Username** and **Password** for the end entity certificate that you created.
17. From the **Key Length** list, select 2048 or 4096.
18. Click **Enroll**.  
The p12 certificate (keystore file) is downloaded to the `Downloads` folder in your browser.
19. Save the p12 and CA root certificates to a location that is accessible from Data Center 2. These files are copied to all Avaya Oceana® Cluster 1 nodes in Data Center 1.

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

### About this task

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

### Procedure

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

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

### About this task

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

### Before you begin

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

### Procedure

1. On the System Manager web console, click **Elements > Avaya Breeze® > Configuration > Attributes**.
2. On the Service Clusters tab, do the following:
  - a. In the **Cluster** field, click Avaya Oceana® Cluster 1.
  - b. In the **Service** field, click **ContextStoreManager**.
  - c. Scroll down to the External Data Mart Configuration area.
  - d. In the **EDM: Enable Persistence to database** field, type `true`.
  - e. Configure the other EDM attributes.  
For more information, see *Avaya Context Store Snap-in Reference*.
  - f. Enter an appropriate value in each of the following fields:
    - **ContextStore ManagerSpace DataGrid Settings**
    - **ContextStoreSpace DataGrid Settings**
    - **EDM: Mirror Service container size**
3. Click **Commit**.

---

## Configuring Omnichannel for disaster recovery

### Omnichannel database mirroring configurations

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

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

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

 **Note:**

- Ensure full hostname and FQDN resolution on Data Center 1.
- Cache Mirroring traffic on Data Center 1 is 60 MB per second of journal data at peak.
- Do not disable Internet Control Message Protocol (ICMP) on any system configured as a mirror member. Cache Mirroring relies on ICMP to detect whether members are reachable.
- Select **Require SSL/TLS** only for the configurations using SSL/TLS certificates.

## Verifying the Omnichannel Database mirroring status

### About this task

All planned full and partial DR switchovers require that the Omnichannel DB servers for both active and standby servers on DC1 are functioning properly and that data is mirrored between them.

In the event of unplanned switchovers due to Omnichannel failures, you must reinstate the failed servers first, and then reinstate the mirroring.

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

### Procedure

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

For example, navigate to

D:\Avaya\Oceana\MMDaDataManagement\OceanaDataManagementTool  
application executable for ODM.

4. Run the ODM tool using the same administrator account.
5. Navigate to **Configuration > Mirror Settings**.

The Mirror Status window shows the current mirroring status for all mirror members.

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

### Procedure

1. Start the Windows Services application by doing the following:
  - a. Click **Start > Run**.
  - b. In the Run dialog box, type `services.msc`.
  - c. Click **OK**.

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

- c. Click **Open**.
15. Click **Restore Database**.
16. For **Are you restoring a mirrored backup**, click **Yes**.
17. Click **Restore**

 **Note:**

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

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

18. To verify whether the restore was successful, do the following:
  - a. On Cache Management Portal, click **System Operation > Mirror Monitor**.
  - b. Click **Details**.

Verify both Avaya Oceana® databases in the list.

## Securing the Cache Mirror on the Omnichannel Database server on Data Center 1

### About this task

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

### Before you begin

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

### Procedure

1. Navigate to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDaDataManagement` folder.
2. Right-click the `OceanaDataManagementTool.exe` file and click **Run as administrator**.
3. Navigate to **Configuration > Mirror Settings > Create Mirror**.
4. Select the **Require SSL/TLS** checkbox.
  - In the **File containing trusted Certificate Authority X.509 certificate** field, enter the location of your CA.
  - In the **File containing this configuration's X.509 certificate** field, browse and select the server certificate.
  - In the **File containing associated private key** field, browse and select the key.
  - In the **Private key password** field, enter the new password.
5. Click **Save** or **Update** button.
6. In your web browser, enter the following URL to open Cache Management Portal:

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

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

7. On the Cache Management Portal login page, do the following:
  - In the **User Name** field, type the user name.
  - In the **Password** field, enter the password.
  - Click **Login**.
8. On Cache Management Portal, click **System Administration > Configuration > Mirror Settings > Edit Mirror**.
9. On the Edit Mirror page, look for **Pending New Members** section.
10. Tick the async server and select **Authorize**.
11. Select **OK**.

# Chapter 8: Validate replication status between DC1 and DC2

## Checklist to validate replication status between DC1 and DC2

The following is the checklist to validate replication status between DC1 and DC2.

| No. | Task                                                                                                                                  | Description                                                                                              | Notes | ✓ |
|-----|---------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|-------|---|
| 1   | Validate Avaya Aura® System Manager and Avaya Breeze® platform replication status to all Avaya Breeze® platform nodes in DC1 and DC2. | See <a href="#">Validate the System Manager and Avaya Breeze platform replication status</a> on page 18. |       |   |
| 2   | Validate the Avaya Control Manager database HA deployment.                                                                            | See <a href="#">Validating the Avaya Control Manager database HA deployment</a> on page 113.             |       |   |
| 3   | Verify UCA replication status from DC1 to DC2.                                                                                        | See <a href="#">Verifying the UCA replication status</a> on page 19.                                     |       |   |
| 4   | Verify the Context Store replication status from DC1 to DC2.                                                                          | See <a href="#">Verify the Context Store replication status</a> on page 20.                              |       |   |
| 5   | Verify the Omnichannel database mirroring status from DC1 to DC2.                                                                     | See <a href="#">Verifying the Omnichannel database mirroring status</a> on page 21.                      |       |   |
| 6   | Verify the Avaya Analytics™ DB Replication from DC1 to DC2.                                                                           | See <a href="#">Verifying the Avaya Analytics DB replication from DC1 to DC2</a> on page 22.             |       |   |

---

## Validate the System Manager and Avaya Breeze® platform replication status

### About this task

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

### Procedure

1. On the System Manager web console, click **Services > Replication**.
2. Validate that the synchronization status of all replica groups is **Synchronized**.  
System Manager displays the word **Synchronized** in green.
3. Click **Avaya Breeze replica group**.
4. Check if the **Breeze Node Synchronization** status is in the **Synchronized** state and that the synchronization date is one month or less from the current date.

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

---

## Validating the Avaya Control Manager database HA deployment

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

### \* Note:

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

---

## Verifying the UCA replication status

### About this task

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

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

 **Important:**

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

**Procedure**

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

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

You must correct the issue before proceeding with the switchover.

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

 **Note:**

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

 **Important:**

Perform the subsequent steps after successfully completing steps 1 to 6.

9. Log on to the Avaya Control Manager on DC1.
10. Add a new test attribute and save the attribute to the primary UCA instance.

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

 **Note:**

If the test attribute does not appear, UCA replication is not operational from primary to DR or the request to save a new attribute to the primary UCA server is not successful. Ensure that you correct these issues before proceeding with the switchover.

11. Reload the cluster message, select **UCAStoreService**, and check the new time of the cluster DB updated message.

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

---

## Verify the Context Store replication status

### About this task

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

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

### Procedure

1. On the System Manager web console, click **Elements > Avaya Breeze® > Cluster Administration**.
2. In the drop-down list next to the Primary Avaya Oceana® Cluster 1, select **Oceana Monitor**.
3. On the Monitor Service page, click **Cluster 1 > Grid Info** and wait for the pop-up to display the status of all snap-in PUs.
4. Verify that the PU **cs-gateway** is present with status `INTACT`.  
  
If it is not present or has a status `Scheduled` or `Broken`, it indicates that the Context Store replication is not operational. You must resolve this issue before proceeding with the switchover.
5. Repeat steps 1 to 4 for Avaya Oceana® Cluster 1 in Data Center 2.
6. Create a context in DC1 Context Store.  
  
Context Store provides a Postman collection of API calls that can be used for all context operations, such as creating and retrieving contexts from Context Store. You can download the Postman collection from **Products > Avaya Oceana Solution > Context Store Snapin > Select Release > Downloads** at [www.devconnectprogram.com](http://www.devconnectprogram.com).
7. Verify that the context is present in DC1 Context Store and in DC2 Context Store.

---

## Verifying the Omnichannel database mirroring status

### About this task

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

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

### Procedure

1. Connect to the primary Omnichannel database server.
2. Launch the Oceana Data Management (ODM) tool.
3. Log in as an administrator.

4. Navigate to **Configuration > Mirror Settings**.

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

---

## Verifying the Avaya Analytics DB replication from DC1 to DC2

### About this task

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

### Procedure

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

```
ccm release orca analytics
```

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

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

# Chapter 9: Resources

## Documentation

| Title                                                       | Use this document to:                                                                                                                                                                                                      | Audience                                                                                                                                                            |
|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Overview                                                    |                                                                                                                                                                                                                            |                                                                                                                                                                     |
| <i>Avaya Oceana® Solution Description</i>                   | Use this guide to know about the tested product characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements. | <ul style="list-style-type: none"> <li>• Sales engineers</li> <li>• Business partners</li> <li>• Solution architects</li> <li>• Implementation engineers</li> </ul> |
| Implementing                                                |                                                                                                                                                                                                                            |                                                                                                                                                                     |
| <i>Deploying Avaya Oceana®</i>                              | Use this guide to know how to deploy Avaya Oceana® Solution on the customer environment.                                                                                                                                   | <ul style="list-style-type: none"> <li>• Sales engineers</li> <li>• Business partners</li> <li>• Solution architects</li> <li>• Implementation engineers</li> </ul> |
| <i>Avaya Oceana® and Avaya Analytics™ Disaster Recovery</i> | Use this guide to know how to restore Avaya Oceana®, solution when there is a complete outage at the primary data center.                                                                                                  | <ul style="list-style-type: none"> <li>• Sales engineers</li> <li>• Business partners</li> <li>• Solution architects</li> <li>• Implementation engineers</li> </ul> |
| <i>Migrating Avaya Oceana®</i>                              | Use this guide to know how to migrate Avaya Oceana® solution from the existing version.                                                                                                                                    | <ul style="list-style-type: none"> <li>• Sales engineers</li> <li>• Business partners</li> <li>• Solution architects</li> <li>• Implementation engineers</li> </ul> |
| <i>Deploying Avaya Analytics™</i>                           | Deploy Avaya Analytics™.                                                                                                                                                                                                   | <ul style="list-style-type: none"> <li>• Sales engineers</li> <li>• Business partners</li> <li>• Solution architects</li> <li>• Implementation engineers</li> </ul> |
| Administering                                               |                                                                                                                                                                                                                            |                                                                                                                                                                     |

*Table continues...*

| Title                                                   | Use this document to:                                                                                                         | Audience                                                                                                                            |
|---------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <i>Administering Avaya Oceana®</i>                      | Administer Avaya Oceana®.                                                                                                     | <ul style="list-style-type: none"> <li>• System administrators</li> <li>• Supervisors</li> </ul>                                    |
| Using                                                   |                                                                                                                               |                                                                                                                                     |
| <i>Using Avaya Workspaces for Avaya Oceana®</i>         | Use Avaya Workspaces for Avaya Oceana®.                                                                                       | <ul style="list-style-type: none"> <li>• Agents</li> <li>• Supervisors</li> </ul>                                                   |
| <i>Using Avaya Analytics™</i>                           | Use the features and capabilities of Avaya Analytics™.                                                                        | <ul style="list-style-type: none"> <li>• Supervisors</li> <li>• Administrators</li> <li>• Report designers</li> </ul>               |
| <i>Avaya Analytics™ Data Dictionary</i>                 | Use historical and real-time measures in custom reports.                                                                      | <ul style="list-style-type: none"> <li>• Administrators</li> <li>• Report designer</li> </ul>                                       |
| Maintaining and Troubleshooting                         |                                                                                                                               |                                                                                                                                     |
| <i>Maintaining and Troubleshooting Avaya Oceana®</i>    | Perform maintenance and troubleshooting procedures for routine maintenance and troubleshooting of Avaya Oceana®.              | <ul style="list-style-type: none"> <li>• Support personnel</li> <li>• Implementation engineers</li> <li>• Administrators</li> </ul> |
| <i>Maintaining and Troubleshooting Avaya Analytics™</i> | Perform common maintenance functions of Avaya Analytics™ and use tools and utilities for troubleshooting of Avaya Analytics™. | <ul style="list-style-type: none"> <li>• Support personnel</li> <li>• Implementation engineers</li> <li>• Administrators</li> </ul> |
| <i>Avaya Oceana® Alarms</i>                             | View details about Avaya Oceana® alarms.                                                                                      | <ul style="list-style-type: none"> <li>• Support personnel</li> <li>• Administrators</li> </ul>                                     |

## Finding documents on the Avaya Support website

### Procedure

1. Go to <https://support.avaya.com>.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support > Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.  
This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.

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

8. Click  to display the search results.

## Avaya Documentation Center navigation

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

### Important:

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

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

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

You can do the following:

- Create, rename, and delete a collection.
- Set a collection as the default or favorite collection.
- Save a PDF of the selected content in a collection and download it to your computer.
- Share content in a collection with others through email.
- Receive collections that others have shared with you.
- Click **Watch** (👁) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

You can do the following:

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

## Training

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

**Table 5: Sales Credentials**

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

**Table 6: Pre-Sales Design**

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

**Table 7: Technical Services Partner Credentials**

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

**Table 8: Pre-requisite Courseware**

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

**Table 9: End User, Programmer, Administration**

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

*Table continues...*

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

Table 10: Other Miscellaneous Courseware

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

## Support

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

# Index

## A

|                                                      |                                          |
|------------------------------------------------------|------------------------------------------|
| Agent .....                                          | <a href="#">45</a>                       |
| AMC snap-in .....                                    | <a href="#">24</a> , <a href="#">63</a>  |
| Avaya Analytics DB replication from DC1 to DC2 ..... | <a href="#">22</a> , <a href="#">116</a> |
| Avaya support website .....                          | <a href="#">123</a>                      |

## B

|                            |                                         |
|----------------------------|-----------------------------------------|
| backup                     |                                         |
| Omnichannel database ..... | <a href="#">49</a> , <a href="#">91</a> |
| UCAStoreService .....      | <a href="#">33</a>                      |
| UCMSERVICE .....           | <a href="#">32</a> , <a href="#">70</a> |

## C

|                                                              |                                                              |
|--------------------------------------------------------------|--------------------------------------------------------------|
| CA certificate .....                                         | <a href="#">103</a>                                          |
| cache .....                                                  | <a href="#">108</a> , <a href="#">110</a>                    |
| cache mirroring .....                                        | <a href="#">49</a>                                           |
| CallServerConnector .....                                    | <a href="#">61</a>                                           |
| chat snap-in .....                                           | <a href="#">62</a>                                           |
| checklist                                                    |                                                              |
| partial controlled switchback .....                          | <a href="#">58</a>                                           |
| partial Controlled Switchover .....                          | <a href="#">12</a>                                           |
| validate replication status .....                            | <a href="#">112</a>                                          |
| checklist for upgrading Oceana and Analytics                 |                                                              |
| DC1 .....                                                    | <a href="#">92</a>                                           |
| checklist for upgrading Oceana and Analytics on DC1 .....    | <a href="#">92</a>                                           |
| Cluster Activity status .....                                | <a href="#">34</a>                                           |
| collection                                                   |                                                              |
| delete .....                                                 | <a href="#">119</a>                                          |
| edit .....                                                   | <a href="#">119</a>                                          |
| generating PDF .....                                         | <a href="#">119</a>                                          |
| sharing content .....                                        | <a href="#">119</a>                                          |
| configure                                                    |                                                              |
| data center .....                                            | <a href="#">76</a>                                           |
| Geographic Redundancy .....                                  | <a href="#">100</a> , <a href="#">101</a>                    |
| configuring .....                                            | <a href="#">41</a>                                           |
| UCAStoreService .....                                        | <a href="#">40</a> , <a href="#">64</a> , <a href="#">65</a> |
| configuring DC1 as a geo primary .....                       | <a href="#">96</a>                                           |
| configuring DC2 as a geo standby .....                       | <a href="#">97</a>                                           |
| Configuring DR site chat shutdown .....                      | <a href="#">68</a>                                           |
| configuring DR site email shutdown .....                     | <a href="#">67</a>                                           |
| configuring DR site GenericChannelAPI Service shutdown ..... | <a href="#">68</a>                                           |
| Configuring DR site MessagingService shutdown .....          | <a href="#">67</a>                                           |
| configuring shutdown .....                                   | <a href="#">30</a>                                           |
| content                                                      |                                                              |
| publishing PDF output .....                                  | <a href="#">119</a>                                          |
| searching .....                                              | <a href="#">119</a>                                          |
| sharing .....                                                | <a href="#">119</a>                                          |
| sort by last updated .....                                   | <a href="#">119</a>                                          |
| watching for updates .....                                   | <a href="#">119</a>                                          |
| create .....                                                 | <a href="#">105</a>                                          |

|                                       |                                         |
|---------------------------------------|-----------------------------------------|
| crunchy 5 .....                       | <a href="#">55</a> , <a href="#">78</a> |
| CustomerController chat snap-in ..... | <a href="#">62</a>                      |
| CustomerControllerService .....       | <a href="#">23</a>                      |

## D

|                                                           |                     |
|-----------------------------------------------------------|---------------------|
| database switchover .....                                 | <a href="#">35</a>  |
| DC1 as geo primary .....                                  | <a href="#">96</a>  |
| DC1 as primary .....                                      | <a href="#">82</a>  |
| DC2 as a geo standby .....                                | <a href="#">97</a>  |
| DC2 for 4.3.1.1 .....                                     | <a href="#">95</a>  |
| defer data backup .....                                   | <a href="#">70</a>  |
| deferred email data backup .....                          | <a href="#">30</a>  |
| deploy                                                    |                     |
| Engagement Designer workflow .....                        | <a href="#">99</a>  |
| disaster recovery .....                                   | <a href="#">9</a>   |
| documentation center .....                                | <a href="#">119</a> |
| finding content .....                                     | <a href="#">119</a> |
| navigation .....                                          | <a href="#">119</a> |
| documentation portal .....                                | <a href="#">119</a> |
| DR .....                                                  | <a href="#">65</a>  |
| DR outbound shutdown .....                                | <a href="#">69</a>  |
| DR Site Chat Startup .....                                | <a href="#">42</a>  |
| DR Site Generic ChannelAPI Service Startup .....          | <a href="#">43</a>  |
| DR Site Messaging Service for Social or SMS Startup ..... | <a href="#">42</a>  |

## E

|                            |                     |
|----------------------------|---------------------|
| EDM .....                  | <a href="#">74</a>  |
| email snap-in .....        | <a href="#">61</a>  |
| EmailService .....         | <a href="#">22</a>  |
| emailservice startup ..... | <a href="#">41</a>  |
| enabling                   |                     |
| web video workflow .....   | <a href="#">87</a>  |
| web voice workflow .....   | <a href="#">87</a>  |
| end entity profile .....   | <a href="#">105</a> |

## F

|                                               |                     |
|-----------------------------------------------|---------------------|
| finding content on documentation center ..... | <a href="#">119</a> |
|-----------------------------------------------|---------------------|

## G

|                                 |                    |
|---------------------------------|--------------------|
| GenericChannelAPI service ..... | <a href="#">30</a> |
| GenericChannelAPI snap-in ..... | <a href="#">63</a> |
| GenericChannelAPIService .....  | <a href="#">24</a> |

## I

|                                |                    |
|--------------------------------|--------------------|
| identical software level ..... | <a href="#">17</a> |
| install 4.3 .....              | <a href="#">95</a> |
| install 4.3.1.1 .....          | <a href="#">95</a> |

|                                                                         |                           |                                                                                     |                          |
|-------------------------------------------------------------------------|---------------------------|-------------------------------------------------------------------------------------|--------------------------|
| installation and migration on DC1 .....                                 | <a href="#">51</a>        | pointing ACM to the new Omnichannel database server<br>in DC1 .....                 | <a href="#">77</a>       |
| installing<br>UCASoreService .....                                      | <a href="#">72</a>        | POM switchover .....                                                                | <a href="#">34</a>       |
| <b>K</b>                                                                |                           | post migration checklist .....                                                      | <a href="#">99</a>       |
| keystore certificate file .....                                         | <a href="#">104</a>       | prerequisite .....                                                                  | <a href="#">10</a>       |
| <b>L</b>                                                                |                           | primary .....                                                                       | <a href="#">34</a>       |
| launch Oceana Monitor for DC1 and DC2 locations and<br>verify PUs ..... | <a href="#">26</a>        | primary site chat shutdown .....                                                    | <a href="#">28</a>       |
| legal notices .....                                                     |                           | primary site email shutdown .....                                                   | <a href="#">28</a>       |
| <b>M</b>                                                                |                           | primary site email snap-in .....                                                    | <a href="#">61</a>       |
| MessagingService .....                                                  | <a href="#">23</a>        | primary site message shutdown .....                                                 | <a href="#">29</a>       |
| MessagingService snapin snap-in .....                                   | <a href="#">62</a>        | promoting DC2 as primary .....                                                      | <a href="#">39</a>       |
| migrating Crunchy 2 to crunchy 5 .....                                  | <a href="#">54</a>        | <b>R</b>                                                                            |                          |
| Migrating crunchy 2 to crunchy 5 .....                                  | <a href="#">55, 78</a>    | recommission .....                                                                  | <a href="#">100, 102</a> |
| Migrating Microstrategy Database .....                                  | <a href="#">79</a>        | recovering .....                                                                    |                          |
| migration .....                                                         | <a href="#">47</a>        | primary data center .....                                                           | <a href="#">52, 93</a>   |
| DC2 .....                                                               | <a href="#">89</a>        | related documentation .....                                                         | <a href="#">117</a>      |
| migration paths .....                                                   | <a href="#">10</a>        | removing .....                                                                      | <a href="#">49</a>       |
| migration procedure analytics step 4 .....                              | <a href="#">82</a>        | Renaming the database .....                                                         | <a href="#">80</a>       |
| migration procedure analytics step 5 .....                              | <a href="#">95</a>        | restarting mstr-srv pod .....                                                       | <a href="#">81</a>       |
| migration procedure analytics step 6 .....                              | <a href="#">96</a>        | restarting orca-dbmgr .....                                                         | <a href="#">81</a>       |
| migration procedure analytics step 7 .....                              | <a href="#">97</a>        | restore .....                                                                       |                          |
| mirroring configuration on DC1 .....                                    | <a href="#">48</a>        | UCASoreService .....                                                                | <a href="#">72</a>       |
| modifying .....                                                         | <a href="#">105</a>       | UCMService .....                                                                    | <a href="#">71</a>       |
| Monitor Service page .....                                              | <a href="#">26</a>        | UCMService in DC2 .....                                                             | <a href="#">41</a>       |
| mstr db .....                                                           | <a href="#">79</a>        | retrieving .....                                                                    | <a href="#">103</a>      |
| <b>N</b>                                                                |                           | routing voice contacts .....                                                        | <a href="#">27, 66</a>   |
| new keystore certificate .....                                          | <a href="#">105</a>       | <b>S</b>                                                                            |                          |
| notices legal .....                                                     |                           | scheduled system maintenance .....                                                  | <a href="#">48, 90</a>   |
| <b>O</b>                                                                |                           | searching for content .....                                                         | <a href="#">119</a>      |
| Oceana Services Overview page .....                                     | <a href="#">26</a>        | securing .....                                                                      |                          |
| Oceana workspaces agent switchover .....                                | <a href="#">88</a>        | mirroring .....                                                                     | <a href="#">110</a>      |
| Omnichannel database mirroring .....                                    | <a href="#">21, 115</a>   | Server A .....                                                                      | <a href="#">36</a>       |
| Omnichannel Server .....                                                | <a href="#">35</a>        | set maintenance mode .....                                                          | <a href="#">33, 69</a>   |
| Omnichannel Server A .....                                              | <a href="#">84</a>        | set up crunchy 2 .....                                                              | <a href="#">54</a>       |
| Omnichannel Server B .....                                              | <a href="#">85</a>        | setting .....                                                                       |                          |
| Omnichannel Server C .....                                              | <a href="#">85</a>        | mirroring .....                                                                     | <a href="#">108</a>      |
| Omnichannel server upgrade .....                                        | <a href="#">90</a>        | Setting ACM to point to the new omnichannel database<br>primary server .....        | <a href="#">37</a>       |
| overview .....                                                          | <a href="#">9, 12, 58</a> | setting ACM to point to the new omnichannel database<br>primary server in DC1 ..... | <a href="#">77</a>       |
| <b>P</b>                                                                |                           | setting up DC2 for 4.3.1.1 .....                                                    | <a href="#">95</a>       |
| partial controlled switchback .....                                     | <a href="#">58</a>        | sharing content .....                                                               | <a href="#">119</a>      |
| partial Controlled Switchover .....                                     | <a href="#">12</a>        | snap-ins .....                                                                      |                          |
| Phase 2 checklist .....                                                 | <a href="#">92</a>        | AMC WebRTC connect .....                                                            | <a href="#">63</a>       |
|                                                                         |                           | CustomerController chat .....                                                       | <a href="#">62</a>       |
|                                                                         |                           | email .....                                                                         | <a href="#">61</a>       |
|                                                                         |                           | GenericChannelAPI .....                                                             | <a href="#">63</a>       |
|                                                                         |                           | MessagingService .....                                                              | <a href="#">62</a>       |
|                                                                         |                           | sort documents .....                                                                | <a href="#">119</a>      |
|                                                                         |                           | status .....                                                                        |                          |
|                                                                         |                           | cluster activity .....                                                              | <a href="#">44, 73</a>   |
|                                                                         |                           | support .....                                                                       | <a href="#">123</a>      |
|                                                                         |                           | switching .....                                                                     |                          |

|                                        |                    |
|----------------------------------------|--------------------|
| switching ( <i>continued</i> )         |                    |
| primary to secondary data center ..... | <a href="#">37</a> |
| switching back to DC1 as primary ..... | <a href="#">82</a> |
| switchover .....                       | <a href="#">45</a> |

## T

|                |                     |
|----------------|---------------------|
| training ..... | <a href="#">120</a> |
|----------------|---------------------|

## U

|                          |                                         |
|--------------------------|-----------------------------------------|
| UCMService .....         | <a href="#">30</a> , <a href="#">70</a> |
| upgrade .....            | <a href="#">48</a>                      |
| Omnichannel server ..... | <a href="#">50</a> , <a href="#">92</a> |
| upgrade on DC2 .....     | <a href="#">90</a>                      |

## V

|                                                                                    |                                          |
|------------------------------------------------------------------------------------|------------------------------------------|
| validate .....                                                                     | <a href="#">101</a>                      |
| UCAStoreService .....                                                              | <a href="#">100</a>                      |
| validate contacts .....                                                            | <a href="#">34</a> , <a href="#">65</a>  |
| validate database HA replication status .....                                      | <a href="#">21</a> , <a href="#">113</a> |
| validate replication status .....                                                  | <a href="#">18</a>                       |
| validate shutdown or deployment status before switchover .....                     | <a href="#">22</a>                       |
| verify PUs .....                                                                   | <a href="#">26</a>                       |
| verify the status .....                                                            | <a href="#">21</a> , <a href="#">115</a> |
| verifying Avaya Analytics DB replication from DC1 to DC2 .....                     | <a href="#">22</a> , <a href="#">116</a> |
| Verifying CSC status in DR site, verifying CSC deployment status in dc2 .....      | <a href="#">25</a> , <a href="#">40</a>  |
| Verifying CSC status in primary site, verifying CSC deployment status in dc1 ..... | <a href="#">25</a>                       |
| verifying shutdown mode status                                                     |                                          |
| CustomerController chat snap-in .....                                              | <a href="#">62</a>                       |
| GenericChannelAPI snap-in .....                                                    | <a href="#">63</a>                       |
| MessagingService snap-in .....                                                     | <a href="#">62</a>                       |
| verifying the status .....                                                         | <a href="#">22–24</a>                    |
| AMC snap-in .....                                                                  | <a href="#">63</a>                       |
| primary site email snap-in .....                                                   | <a href="#">61</a>                       |
| view                                                                               |                                          |
| Oceana Monitor Service .....                                                       | <a href="#">26</a>                       |

## W

|                 |                                         |
|-----------------|-----------------------------------------|
| watchlist ..... | <a href="#">119</a>                     |
| web video ..... | <a href="#">33</a> , <a href="#">69</a> |
| web voice ..... | <a href="#">33</a> , <a href="#">69</a> |