Maintaining and Troubleshooting Avaya Oceana®

Release 3.10.0.1
Issue 1
May 2025

Notices

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

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

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

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

License types

Copyright

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

Virtualization

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

Third Party Components

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

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H 3 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

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

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

Contents

Chapter 1: Introduction

Purpose

This document contains maintenance and troubleshooting procedures for the routine maintenance and required troubleshooting of Avaya Oceana®. Routine maintenance practices include the scheduled backup and restoration process.

This document is intended for people who perform Avaya Oceana® maintenance and troubleshooting tasks, are familiar with the solution, and are trained to handle software errors. To handle software errors not documented in this guide, contact Avaya support.

New in this release

Avaya Oceana® 3.10.0.1 supports the following:

- Avaya Oceana® Release 3.10.0.1 supports migration from previous releases. For more information and procedure to migrate, refer to the following documents:
  - Migrating Avaya Oceana®
  - Avaya Oceana® Disaster Recovery and Migration
- Avaya Oceana® Release 3.10.0.1 supports:
  - Breeze Release 3.9.0.2
  - VMWare Release 8.0
  - Centralized Logging on Common Service Platform

Chapter 2: Maintenance

Taking a backup of the System Manager database

About this task

Use this procedure to backup of the System Manager database to preserve the System Manager configuration.

Before you begin

To store the backup on the default remote server, configure the following information on the SMGR Element Manager page:

- IP address, port number, user name, and password of the remote server
- Filename of the backup file with complete path

You can access the SMGR Element Manager page by clicking **Services** > **Configurations** > **Settings** > **SMGR** > **SMGR Element Manager**.

Procedure

1. On the System Manager web console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.

   System Manager displays the Backup page.
3. Select the **Remote** option to store the backup on a remote server.

   For System Manager upgrade or migration from 7.x to 8.x, the System Manager server is replaced and powered off. Therefore, you must take the backup on a remote server.
4. Do one of the following:
   - To store the backup on the default remote server, select the **Use Default** check box.
   - To store the backup on a particular remote server, clear the **Use Default** check box.
5. **(Optional)** If you clear the **Use Default** check box, do the following:
   a. In the **File transfer protocol** field, click `SCP` or `SFTP`.
   b. In the **Remote Server IP** field, enter the IP address of the remote server.
   c. In the **Remote Server Port** field, enter the port number of the remote server.
   d. In the **User Name** field, enter the username of the remote server.
   e. In the **Password** field, enter the password of the remote server.

f. In the **File Name** field, enter the filename of the backup file with the complete path.

6. Click **Now**.

   After the backup is successful, the Backup and Restore page displays the following message:

   ```
   Backup job submitted successfully. Please check the status detail below!!
   ```

   Note:

   Record the /etc/hosts entries from System Manager, such as FQDN, vFQDN, IP, Subnet Mask, Gateway IP, Domain, Time server, and DNS. Also, record the type of licenses in use. You require these details when installing System Manager 8.0.

7. Shut down System Manager.

Taking a backup of UCAStoreService

About this task

UCAStoreService stores information related to users, accounts, attributes, providers, and resources. The Avaya Breeze® platform migration do not preserve the UCAStoreService database. You must create a backup to retain the data. Avaya Control Manager, Unified Collaboration Administration (UCA), and the Omnichannel server backup the data independently. Therefore, you must create the backups and restore them in coordination.

Procedure

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

   System Manager displays the Backup Storage Configuration page.

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

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

10. Click **Test Connection**.
11. In the Test Connection Result dialog box, the System Manager must display the following messages:

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

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

    Note:

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

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

    System Manager displays the Cluster DB Backup page.

16. Select the **UCAStoreService** check box.
17. In the **Backup Password** field, enter a password for the backup.

    Important:

    Note the password, as it is required to restore the UCAStoreService database.

18. In the **Schedule Job** field, click **Run immediately**.
19. Click **Backup**.

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

Taking a backup of Engagement Designer workflows

About this task

Use this procedure to take a backup of Engagement Designer workflows. Taking a backup of workflows is optional and depends on your requirement.

Procedure

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

   The System Manager displays the Backup Storage Configuration page.

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

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

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

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

    Note:

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

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

    Important:

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

Taking a backup of 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 the Omnichannel database

About this task

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

For information about how to take a backup of the Omnichannel database that has a cache mirror, see *Avaya Oceana® and Avaya Analytics™ Disaster Recovery*.

Note:

- Ensure that you take backups of the Omnichannel database at regular intervals.
- The backup is taken from the active database if it was previously in an HA mirrored configuration on Data Center 1.

Procedure

1. Log in to the Omnichannel server.
2. Do one of the following:
   - For Avaya Oceana® 3.5.x or 3.6, go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\Oceana\BackupAndRestore` folder.
   - For Avaya Oceana® 3.7 or higher version, go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement` folder.
3. Do one of the following:
   - For Avaya Oceana® 3.5.x or 3.6, right-click the `BackupAndRestore.exe` file and select **Run as Administrator**.
   - 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.

Taking a backup of Avaya Control Manager databases

About this task

Use this procedure to take a backup of the following databases before upgrading Avaya Control Manager:

- ACCCM
- ACCCMAVP
- ACCCMONEXDB
- ACCCMCMSYSLOG
- ACCCMSYNC

Procedure

1. On the SQL server used for Avaya Control Manager, open the SQL Management Studio application.
2. In the Connect to Server window, enter the following information:
   - Server type
   - Server name
   - Authentication
   - User name
   - Password
3. Click **Connect**.
4. In the Object Explorer pane, expand the Databases navigation tree and select the ACCCM database.
5. Right-click the database and click **Tasks** > **Back Up**.

   The SQL server displays the Back Up Database window.
6. In the Select a page pane, click **General**.
7. In the **Backup type** field, click **Full**.
8. In the Destination area, click **Add**.
9. In the **File name** field, browse and select the directory where you want to store the backup file.

   You must store the file in the `.bak` format.
10. Click **OK**.

11. Repeat Step 4 to Step 9 to take a backup of the remaining databases.

Restoring the UCAStoreService data

Before you begin

On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services** and uninstall UCAStoreService from Avaya Oceana® Cluster 1. When uninstalling the service, select the check box for the database so that the database is also removed. After uninstalling the service, restart the nodes of the Avaya Oceana® Cluster 1 to delete UCAStoreSpace.

Procedure

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

Restoring UCMService data for Avaya Oceana® Cluster 1

Before you begin

- Ensure that all agents are logged out of their accounts.
- Ensure that the state of Avaya Oceana® Cluster 1 and Avaya Oceana® Cluster 3 is `Deny New Service`.
- Uninstall UCMService from Avaya Oceana® Cluster 1 and restart all nodes of the cluster to delete the ucm-space-pu and the ucm-oc-pu.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.

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

   Note:

   Deferred email contacts not present in the UCM DB that was copied over need to be manually requeued using Oceana Data Viewer component.
10. Change the state of Avaya Oceana® Cluster 1 and Avaya Oceana® Cluster 3 to `Accept New Service`.

Restoring the Omnichannel database

About this task

Use this procedure to restore the Omnichannel database onto your Microsoft Windows Server 2019 (Desktop Experience) Omnichannel server. This procedure applies to a standalone Omnichannel database that does not have a database mirror. For more information on how to restore the Omnichannel database that has a database mirror, see *Avaya Oceana® and Avaya Analytics™ Disaster Recovery*.

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 the same account.

Procedure

1. Log in to the Omnichannel server as an administrator.
2. Do one of the following:
   - For Avaya Oceana® 3.5.x or 3.6, go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\Oceana\BackupAndRestore` folder.

- For Avaya Oceana® 3.7 or later, go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement` folder.

3. Do one of the following:
   - For Avaya Oceana® 3.5.x or 3.6, right-click the `BackupAndRestore.exe` file and select **Run as Administrator**.
   - For Avaya Oceana® 3.7 or later, 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. Navigate to the **Select file to restore from** section.
7. The **Allow Restore if user file is missing** option is checked by default.

   Note:

   The **Allow Restore if user file is missing** option ensures that the restore continues without error, even if a User file is missing while the Restore file is present on a folder.
8. Click **Browse**.
9. Select the backup file and click **Open**.
10. Click **Restore Database**.

    The application displays the Drive restore screen.
11. In the **Select your database drive letter** field, select the drive that you specified for the Omnichannel database when installing the Omnichannel server software.
12. In the **Are you restoring a mirrored backup** field, select one of the following options:
    - Select **Yes** if you take the backup from the server with mirroring configured.
    - Select **No** if you take the backup from a system with no mirroring configured.
13. Click **Restore**.

    Important:

    If the Omnichannel server displays the Cache Post Restore Script terminal window, keep the window open until the process in the window is completed.

    Note:

    If the **Allow Restore if user file is missing** option is cleared and a user file is missing, the restore is not completed, and a message box appears. To complete the restore, you must select the **Allow Restore if user file is missing** option and restart the restore process.

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

14. **(Optional)** Modify the passwords again after the restore process because the backup does not contain the previously modified passwords.

    Note:

    Perform this step if you had modified the default passwords of the Omnichannel database previously.

15. **(Optional)** Reconfigure the server for secure connections after the restore process.

    Note:

    Perform this step if you had previously configured the Omnichannel server for secure connections.

Restoring Avaya Control Manager databases

About this task

Use this procedure to restore the following databases after upgrading Avaya Control Manager:

- ACCCM
- ACCCMAVP
- ACCCMONEXDB
- ACCCMCMSYSLOG
- ACCCMSYNC

Procedure

1. On the SQL server used for Avaya Control Manager, open the SQL Management Studio application.
2. In the Connect to Server window, enter the following information and click **Connect**:
   - Server type
   - Server name
   - Authentication
   - User name
   - Password
3. In the Object Explorer pane, expand the Databases navigation tree and select the ACCCM database.
4. Right-click the database and click **Tasks** > **Restore** > **Database**.

   The SQL server displays the Restore Database window.
5. In the Select a page pane, click **General**.

6. In the Source area, click **Device**.
7. Browse and select the backup file.
8. In the Backup sets to restore area, select the **Restore** check box.
9. In the Select a page pane, click **Options**.
10. In the Restore options area, select the **Overwrite the existing database (WITH REPLACE)** check box.
11. In the Tail-Log backup area, select the **Take tail-log backup before restore** check box.
12. Click **OK**.

    The SQL Management Studio application displays the following message after the database is restored:

    ```
    Database 'ACCCM' restored successfully.
    ```

13. Repeat Step 3 to Step 12 to restore the remaining databases.

EASG-based authentication of Web Administrative Interfaces for Avaya Oceana®

EASG overview

Enhanced Access Security Gateway (EASG) is a challenge-response authentication and authorization solution that service engineers can use to access Web-based applications of Avaya Oceana®. Avaya service engineers can access these applications without redirection to Avaya Breeze® Authorization Service or System Manager (SMGR).

EASG configuration

EASG is already configured with SMGR and SSH-Login. You need to install Avaya Breeze platform with EASG enabled option.

EASG supports the following login IDs: `craft`, `init`, `inads`, and `sroot`.

Prerequisites for EASG authentication

- You should be able to log in to Avaya Oceana® Oceana Manager and DataViewer.
- Authentication implementation must be compatible with Avaya SAL Policy Manager, which is based on point-to-point access to the end systems.

Using EASG to access applications

Application	Access Procedure
SMGR	You can enable or disable EASG authorization in SMGR. In the EASG authentication config section, you can select **true** or **false** in the **Effective Value** column to enable or disable EASG Authentication. You can disable EASG authorization only for Oceana Manager and Oceana DataViewer. 1. Use the appropriate URL to open the SMGR login page. For example: `https://{SMGR_FQDN}/services` 2. In the **Username** field, type `init` or `craft` and then click **Next**. 3. Copy the Product ID, Login Name, and Challenge one by one to the corresponding fields on the EASG Web Mobile Response page. 4. Click **Query** to generate the Response token. 5. Click **Copy Response to Clipboard** to copy the Response token. 6. Go back to the SMGR login page to enter the token in the **Response** field. 7. Click **Login** to successfully log in to SMGR.

Table continues…

Application	Access Procedure
OceanaMonitor	1. Use the appropriate URL to open the OceanaMonitor login page. For example: `https://{cluster_fqdn}/services/OceanaMonitorService/services-login.html` 2. In the **Username** field, type one of the following login names: `init`, `inads`, `sroot`, or `craft`. Then click **Next**. 3. Copy the Product ID, Login Name, and Challenge one by one to the corresponding fields on the EASG Web Mobile Response page. 4. Click **Query** to generate the Response token. 5. Click **Copy Response to Clipboard** to copy the Response token. 6. Go back to the OceanaMonitor login page to enter the token in the **Response** field. 7. Click **Login** to successfully log in to OceanaMonitor.
Oceana DataViewer	1. Use the appropriate URL to open the DataViewer login page. For example: `https://{Cluster_OCP_FQDN}/services/OceanaDataViewer/easgLogin.jsp` 2. In the **Username** field, type one of the following login names: `init`, `inads`, `sroot`, or `craft`. Then click **Next**. 3. Copy the Product ID, Login Name, and Challenge one by one to the corresponding fields on the EASG Web Mobile Response page. 4. Click **Query** to generate the Response token. 5. Click **Copy Response to Clipboard** to copy the Response token. 6. Go back to the DataViewer login page to enter the token in the **Response** field. 7. Click **Login** to successfully log in to DataViewer.

Limitations

- You should have access to EASG Web Mobile.
- You must know the full URL path of the EASG login page.

Chapter 3: VMware ESXi host maintenance

Hosts running virtual machines that are part of Avaya Oceana®, Avaya Analytics™ and/or Avaya Breeze® platform, must be kept up-to-date, including VMware ESXi.

Host software maintenance and updates must be planned into a maintenance windows where the contact center is not in service. In these maintenance windows, one or more physical hosts may be out of service, including all the virtual machines running on these hosts.

Performing host maintenance in Avaya Oceana® and Avaya Analytics™ production system

Procedure

1. For the selected host(s), identify any Avaya Oceana® virtual machines that have DRS Override rules enabled. Manually move all the virtual machines to other hosts.
2. Using the VMware host **Maintenance Mode** flag, manually place the host into maintenance mode. This invokes DRS to automatically migrate the remaining virtual machines, including Avaya Analytics™ virtual machines, to other hosts in the cluster. For more detailed information on using this method, see https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.resmgmt.doc/GUID-8F705E83-6788-42D4-93DF-63A2B892367F.html.
3. When all the virtual machines from Avaya Oceana®, Avaya Analytics™, and other applications are no longer running on the host, the host enters the **Maintenance Mode**.
4. With the required virtual machines migrated on the new set of hosts, the Avaya Oceana® solution operates in production mode in parallel.
5. An alternative process is to complete the host maintenance, restore all virtual machines to the updated host, and place the Avaya Oceana® and Avaya Analytics™ solutions back into production using the updated host. This is a longer maintenance mode window for the Avaya Oceana® solution.
6. To verify that Avaya Oceana® solution is fully operational after placed back into production, see *Deploying Avaya Oceana®* and *Maintaining and Troubleshooting Avaya Oceana®* documents.

Important:

- There may be instances where it is necessary to restart Avaya Oceana® clusters to restore full production capabilities post **vMotion** activities.

VMware ESXi host maintenance operations using vMotion for Avaya Oceana® and Avaya Analytics™ deployments

If ESXi host maintenance is required, you may need to move running virtual machines from the host machine. One efficient method is to use the **Maintenance Mode** setting on the host machine, which invokes **vMotion** to automatically move the running virtual machines to other hosts in the same VMware cluster. After all the virtual machines are migrated to other hosts, the initial host machine can be updated as required before getting back into the production mode. See *Upgrading Avaya Analytics™ ESXi hosts"* section in the *Maintaining and Troubleshooting Avaya Analytics™ for Avaya Oceana®* manual.

The use of **vMotion** to migrate Avaya Oceana® and Avaya Analytics™ virtual machines requires planning and considerations. For optimal outcome when using **vMotion** with Avaya Oceana® and Avaya Analytics™ applications, ensure the following:

- The use of **vMotion** is permitted in Avaya Oceana® and Avaya Analytics™ maintenance windows. It is not supported on Avaya Oceana® and Avaya Analytics™ virtual machines in production mode. That is, while routing contacts, with agents are logged in, and other similar scenarios.
- The **vMotion** network must be a minimum of 10Gbps. **vMotion** network speed can affect **vMotion** durations and virtual machine stun times and may potentially impact the performance of running virtual machines. Multiple simultaneous usage of **vMotion** leads to bandwidth contention and affects the performance of virtual machines.
- For physical hosts in the VMware cluster, ensure a host is available with sufficient free capacity to move virtual machines from a host undergoing maintenance.
- All hosts in the VMware cluster must have identical processor specifications or have greater specifications than the Avaya Oceana® and Avaya Analytics™ reference processors.
- All hosts in the VMware cluster must have identical vCenter permissions according to the *Deploying Avaya Analytics™* document before migrating any Avaya Analytics™ virtual machines.
- If DRS override rules have been used for any of the Avaya Oceana® virtual machines, you must manually migrate those virtual machines to another host before using **vMotion** to place the existing host into maintenance mode. For more information on **vMotion** process, see https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vcenterhost.doc/GUID-D19EA1CB-5222-49F9-A002-4F8692B92D63.html#:~:text=vMotion%20migration%20to%20another%20host,to%20the%20running%20virtual%20machine.

- For any issues encountered while following the **vMotion** maintenance window, restart Avaya Oceana® and Avaya Analytics™ virtual machines to restore normal operation.

Important:

Failure to comply with these requirements can lead to instability within Avaya Oceana® and Avaya Analytics™ deployments, and may require a system restart.

Chapter 4: Configure Alarms and Events

Configure Alarms and Events

System Manager provides an Operating System (OS)-level SNMP Master (Net-SNMP) agent for platform monitoring, notification sending, and notification destination & SNMPv3 user management.

If you change the Trap Listener settings as an administrator, you must create a new SNMP target profile for the System Manager IP address and a new SNMPv3 user profile for System Manager. The values in the new profiles must match the values in the Trap Listener settings. In addition, you must attach the System Manager SNMPv3 user profile to the System Manager target profile, and then attach the new SNMP target profile to all Serviceability Agents.

For more information about creating SNMP user profiles and target profiles and attaching the target profiles to Serviceability Agents, see *Administering Avaya Aura® System Manager*.

For more information about SNMP, see *Avaya Aura® System Manager SNMP Whitepaper*.

Creating an SNMPv3 user profile

About this task

Use this procedure to create a user profile with read and write privileges for SNMP MIBs.

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Serviceability Agents** > **SNMPv3 User Profiles**.
2. On the SNMPv3 User Profiles page, click **New**.
3. On the New User Profile page, perform the following steps:
    a. In the **User Name** field, enter the user name.

       Specify the user name as initial.
    b. In the **Authentication Protocol** field, select the authentication protocol.
    c. In the **Authentication Password** field, enter an authentication password.
    d. In the **Confirm Authentication Password** field, re-enter the authentication password.
    e. In the **Privacy Protocol** field, select the privacy protocol.
    f. In the **Privacy Password** field, enter a privacy password.
    g. In the **Confirm Privacy Password** field, re-enter the privacy password.

h. In the **Privileges** field, select `Read/Write`.

i. Click **Commit**.

Creating an SNMP target profile

About this task

The System Manager TrapListener service receives traps from different applications and displays the information on the System Manager Alarming page.

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Serviceability Agents** > **SNMP Target Profiles**.
2. On the SNMP Target Profiles page, click **New**.
3. On the New Target Profile page, on the Target Details tab, perform the following steps:
   a. In the **Name** field, enter a name for the target profile.
   b. In the **Description** field, enter a description for the target profile.
   c. In the **IP Address** field, enter the appropriate IP address
   d. In the **Port** field, enter the appropriate port number.
   e. In the **Notification Type** field, select the notification type.
   f. In the **Protocol** field, select the protocol.

   This information must match with the Trap Listener profile. You can view the Trap Listener profile by clicking **Services** > **Configurations** > **Settings** > **SMGR** > **TrapListener**
4. On the New Target Profile page, on the Attach/Detach User Profile tab, perform the following steps:
   a. Select the initial user profile.
   b. Click **Assign**.
   c. Click **Commit**.

Assigning Serviceability Agents

About this task

The Serviceability Agent is an enhanced version of the SAL agent for forwarding logs, harvesting logs, and alarming. The Serviceability Agent sends SNMPv3 traps and notifies the configured NMS destinations. System Manager and the SAL gateway are the two mandatory destinations.

Using the Serviceability Agent user interface you can:

- Manage and configure SNMPv3 users remotely
- Manage and configure SNMP trap destinations remotely
- Create, edit, view, and delete user and target profiles

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Serviceability Agents** > **Serviceability Agents**.
2. On the Serviceability Agents page, select the relevant nodes and click **Manage Profiles**.
3. On the Manage Profile page, perform the following steps:
   a. Select the **SNMP Target Profiles** tab.
   b. Select the SNMP target profile that you created.
   c. Click **Assign**.
   d. Select the **SNMPv3 User Profiles** tab.
   e. Select the user profile that you created.
   f. Click **Assign**.
   g. Click **Commit**.

Verifying the configuration

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Serviceability Agents** > **Serviceability Agents**.
2. Select the nodes for which you want to generate alarms.
3. Click **Generate Test Alarm**.

   System Manager generates a test alarm. You can view the alarm by clicking **Services** > **Events** > **Alarms**.

Oceana Breeze Node Identity certificate expiry alarm

Oceana Breeze Node Identity certificate alarm

Avaya nodes in an Avaya Oceana® solution can be integrated with the Avaya Aura® System Manager simple network management protocol listener service to capture all keystore identity certificates expiry alarms starting from 60 days to expiry date. These alarms can be viewed under **Services** > **Events** > **Alarms**. Avaya Aura® System Manager must have the Simple Network Management Protocol (SNMP) components configured appropriately for the alarms to be captured and displayed. The Avaya Aura® System Manager is configured with access to a network management application or a simple mail server mailbox, these alarms can then be forwarded to a authorized administrator support personnel.

Avaya Aura® System Manager provides an operating system level Simple Network Management Protocol (SNMP) Master agent (Net-SNMP) for basic Internet Protocol (IP) discovery, for monitoring operating system platform, for sending and receiving notifications and for SNMP user management. The SNMP agent is started by default. The Avaya Aura® System Manager console provides a user interface for activation of serviceability agents, establishment of SNMP user profiles, and management and establishment of SNMP target profiles.

The SNMP user, target and filter profiles are assigned to the SMGR and its managed element's (serviceability agents).

For more information on configuring system manager to receive alarms from its managed elements and generate SNMP alarms/alerts, refer to https://support.avaya.com/search-landing/?query=Avaya%20Aura%AE%20System%20Manager%207.1%20SNMP%20Whitepaper

Omnichannel Database Server (OCP) Identity certificate expiry alarm

Avaya Oceana® introduces support generating a new alarm in the Avaya Aura® System Manager event viewer for the Omnichannel database server identity certificates expiring within 60 days from the actual expiry date.

Configuring Avaya Aura® System Manager for capturing alarms or traps

About this task

Use this procedure to configure Avaya Aura® System Manager for capturing alarms or traps from its managed elements. The alarms generated are displayed on events page on the administrator's user interface.

Procedure

1. Log on to the Avaya Aura® System Manager web console.
2. To verify the configuration of the trap listener, navigate to **Home** > **Services** > **Configurations** > **Settings** > Avaya Aura® System Manager > **Trap Listener**.
3. Create a new target profile for Avaya Aura® System Manager.
4. Configure the target profile details at **Home** > **Services** > **Inventory** > **Manage Serviceability Agents** > **SNMPv3 Target Profiles**.
5. Attach the new target profile to your SNMP user profile.
6. Configure the SNMP user profile details at **Home** > **Services** > **Inventory** > **Manage Serviceability Agents** > **SNMPv3 Target Profiles**.
7. Configure **Serviceability Agent** for all managed elements.
8. Enable all the managed elements such as Avaya .
9. Configure the manage elements at **Home** > **Services** > **Inventory** > **Manage Serviceability Agents** > **Serviceability Agents**.
10. Click **Generate Test Alarm**.
11. Configure the Avaya Aura® System Manager with an on-premise mail server and mailbox credentials.

    Once the bove configurations are complete, an alert is sent to the administrator for specific alarms such as Avaya node identity certificate expiry alarms. Avaya generates an alarm starting at 60 days from its actual expiration date for all identity certificates deployed into any of the 9 key stores on the node. Using the existing capabilities of Avaya Aura® System Manager, these alarms can be captured in the event viewer and then sent to either a

network monitoring application or a monitored mailbox on a mail server. Additionally, an alarm is also displayed for the Omnichannel database server identity certificate expiry starting at 60 days from the expiry date.

Chapter 5: Oceana Monitor Service and Gigaspaces Viewer

Using the Oceana Monitor Service

The Monitor Service page provides the following information about each cluster of the 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
- The number of CPUs per node
- The amount of RAM per node
- Cluster view of the snap-ins installed
- View of snap-in lifecycle messages

Viewing information about the nodes of the cluster

To access the Monitor Service page, perform the following steps:

1. On the System Manager web console, navigate to **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, from the **Service URL** drop-down list, select **Oceana Monitor**. The Oceana Monitor Service opens in a new tab.

   You can also access each cluster's Monitor Service page directly using the following URL:

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

   Tip:

   You can bookmark the Oceana Monitor Service for each cluster.
3. Click on the cluster that you want to monitor.

To view service details:

1. On the Monitor Service page, click **Show Service Details**.

   The Monitor Service page lists the services installed on the cluster.
2. Click **Service Messages** to view the events associated with each service.

To view node details:

1. On the Monitor Service page, click **Show Node Details**.
2. Ensure that each node has the required number of CPUs and the required amount of RAM memory.

To view information about the processing units (PUs) of the cluster:

1. On the Monitor Service page, click **Show Grid Info**.
2. Ensure all the PUs show a **Status** of **INTACT**.

To view the service messages for all the snap-ins installed on the cluster:

1. On the Monitor Service page, click **Show Cluster Messages**.
2. Review the messages across all nodes in the cluster.

Common issues with Oceana Monitor Service

The following table describes common issues that can occur when using the Oceana Monitor Service, and how to troubleshoot these issues.

Issue description	Action
Oceana Monitor Service shows a 503 Service Temporarily Unavailable message	• Verify that the Oceana Monitor Service has finished installing on all nodes. • Ensure that the cluster state is set to Accepting.
Oceana Monitor Service fails to display cluster information	• Verify that the Oceana Monitor Service attributes are configured.
Oceana Monitor Service fails to display cluster information and the following warning appears: “Could not connect to cluster 'http://{Cluster_IP_address}'. Check attributes are correct.”	• Verify that https is configured correctly using the following steps: 1. Check that the **Only allow secure web communications** attribute on the cluster is enabled. 2. If the **Only allow secure web communications** attribute is enabled, you must ensure that the **Secure Connection** OceanaMonitorService attribute is also set.

Using gigaspaces viewer

About this task

The gigaspaces viewer web interface provides information about the state of a running cluster. This also monitors the running components such as physical hosts, deployed processing units, spaces and space instances. It also allows for querying data and viewing class metadata.

Procedure

1. In your web browser, enter the following URL to view the gigaspaces viewer login page:

   `http://<Cluster IP>/services/OceanaMonitorService/Gs_webui.jsp`

2. On the login page, enter the administrator username and password.
3. In the **Locators** field, enter `<Cluster IP>:7000`.
4. Click **Login**.

   The gigaspaces viewer displays the Hosts page.

   From the Hosts page, you can monitor the physical resources of your cluster. The physical resources include the hosts and virtual machines.

   Expand the entry in the **Name** column to view elements existing on a host. The Hosts page mainly displays columns with CPU usage, memory utilization, processing units, and used heap to understand current the usage of physical resources.

Viewing the Oceana Dashboard

Procedure

1. On the System Manager web console, navigate to **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, from the **Service URL** drop-down list, select **Oceana Dashboard**.

   The Oceana Dashboard displays the channels and the status of each channel.

3. Click the channel icons to view additional details about each channel.

   The status of each channel is depicted in different colors. For example, green status indicates that the channel is working fine. Alternatively, use the **Filter** option to reorder the channels by their statuses.

Using gigaspaces viewer from Oceana Manager

About this task

You can access the gigaspaces viewer even from the Oceana Manager page.

Before you begin

Ensure that you login to Oceana Manager as an administrator or user with an administrator role. The gigaspaces viewer is available only to an administrator or user with an administrator role.

Procedure

1. On the System Manager web console, navigate to **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, from the **Service URL** drop-down list, select **Oceana Manager**. The Oceana Manager opens in a new tab.

You can also access each cluster's manager page directly using the following URL:

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

The Oceana Manager page displays the list of clusters with their activity status and details.

3. Enter the administrator credentials to view gigaspaces.

   The gigaspaces viewer displays the Hosts page.

4. On the required cluster row, click **Show Node Details** to display the information about cluster nodes.

   The row expands to display the cluster node details.

5. Choose a node that you want to inspect with gigaspaces viewer and click **Open Gigaspaces Viewer**.

Checking gigaspaces events, alerts, and logs

Solution

1. To view the event list, on the Hosts page, click **Events**.

   The **Events** button expands to display the list of events, messages, descriptions, time, and event status.

2. To view alerts, on the Hosts page, click **Alerts**.

   The **Alerts** button expands to display the list of alarms, their status, description, and location.

3. To view logs, on the Hosts page or Processing Units page, do the following:

   a. Expand an element in the **Name** column and select an entry.

   b. Click **Logs** to display logs for a selected processing unit or space.

Checking and managing processing units and spaces

Solution

1. On the gigaspaces viewer interface, click **Processing Units**.

   The interface displays the list of processing units for the node with status and type of processing unit.

2. Expand the processing unit to view information about space, CPU usage, and used heap size in the processing unit.

3. On the Processing Units page, in the processing unit row, click , and then click **Undeploy** to undeploy the processing unit.

4. On the Processing Units page, in the space row, click , and then click **Restart** to restart a space.

Note:

You must perform the undeploy and restart actions under the guidance of Avaya support because they impact system stability.

5. To view objects in spaces, on the gigaspaces viewer interface, click **Spaces**.

   The interface displays all spaces deployed on the node with their memory consumption.

6. On the Spaces page, select a space and click **Types**.

   You can view the instance count and types of the objects stored in space.

   To view the details of stored objects, click the link in the **Data Type Name** column. The gigapaces viewer runs a query against the space. You can view the result with details of the objects of this data type in the space.

Chapter 6: Avaya Breeze Snap-in log files

Avaya Breeze® platform Snap-in log files

Each Avaya Breeze® platform node uses a WebSphere application server to host various SVARs (service archive files). The SVAR services provide the basic functional blocks of the Avaya Oceana®.

Some of Avaya Oceana®'s SVARs also include a GigaSpaces Processing Unit (PU). A PU is the fundamental unit of deployment in the GigaSpaces In-Memory Computing Platform. The PU runs within a Processing Unit Container and is deployed onto the Service Grid. Once a PU is deployed, a PU instance becomes a run time entity.

The following table shows the Avaya Oceana®'s SVAR log files location:

Log name	Location
WebSphere Service	`/var/log/Avaya/services/`
GigaSpaces PU	`/var/log/Avaya/dcm/pu/`

Note:

If a SVAR has both Service and PU log files, the PU log file provides more diagnostic and troubleshooting information.

Each Avaya Breeze® platform node has a log file for all of the SVARs deployed on a cluster. If a cluster has two nodes, examine the log files on both nodes to troubleshoot the issue.

The following table lists the log file locations and services associated with them:

Cluster	Log name	Location	Services
1	GigaSpaces PU	`/var/log/Avaya/dcm/pu`	• CallServerConnector • ContactCenterService • ContextStoreManager • UCAStoreService • UCMDataCollector • UCMService • WorkAssignmentManagerService

Table continues…

	WebSphere Service	`/var/log/Avaya/services/`	• CallEventControl • CallServerConnector • ContactCenterService • ContextStoreManager • ContextStoreQuery • ContextStoreRest • CustomerJourneyService • CustomerManagement • EngagementDesigner • EventingConnector • OCPDataServices • OceanaCoreDataService • OceanaMonitorService • OmniCenterProvisioningCollector • UCAStoreService • UCMDataCollector • UCMService • WAIMRestService • WorkAssignmentManagerService • CRMGateway **Note:** For a footprint of 100 agents deployment, CRMGateway is installed on Cluster 1, while for deployments that support more than 100 agents CRMGateway is installed on Cluster 5.
2	GigaSpaces PU	`/var/log/Avaya/dcm/pu`	• UnifiedAgentContextService • UnifiedAgentController

Table continues…

	WebSphere Service	`/var/log/Avaya/services/`	• AuthorizationService • BotConnector • CallEventControl • EventingConnector • OceanaMonitorService • UnifiedAgentContextService • UnifiedAgentController
3	GigaSpaces PU	`/var/log/Avaya/dcm/pu`	• AgentControllerService • EmailService • CustomerControllerService • OBCService • ORCRestService **Note:** For the ORCRestService SVAR, the services log file contains most of the useful information.
	WebSphere Service	`/var/log/Avaya/services/`	• AgentControllerService • AutomationController • CallEventControl • CustomerControllerService • EmailService • EventingConnector • GenericChannelAPI • MessagingService • OBCService • OceanaDataViewer • OceanaMonitorService • ORCRestService • SMSVendorSnapin • SocialConnector
4	WebSphere Service	`/var/log/Avaya/services/`	CoBrowse

Table continues…

5	WebSphere Service	`/var/log/Avaya/services/`	• CRMGateway • ZangSmsConnector **Note:** For a footprint of 100 agents deployment, CRMGateway is installed on Cluster 1, while for deployments that support more than 100 agents CRMGateway is installed on Cluster 5.

Chapter 7: Centralized logging

Centralized Logging overview

Centralized Logging is a feature that you can use to view the logs for all services of Avaya Oceana® clusters through a centralized interface.

Checklist for centralized logging

The following table lists the tasks that you need to perform to set up centralized logging:

No.	Task	Notes	✔
1	Configure Certificate for Secure TLS connection between Breeze and CSP ElasticSearch. **Note:** Only Secure Connection is supported from Breeze Logstash to CSP ElasticSearch Connection between Breeze Logstash and CSP Elasticsearch can only be through Mutual TLS (MTLS) and it cannot be unsecured. It is necessary to perform the following procedures before updating cluster attributes and setting Centralized Logging destination to CSP Elasticsearch option on SMGR. You need to perform the following tasks: 1. Adding Breeze CA certificate to the Elasticsearch truststore on CCM on page 42 2. Adding Breeze node Common Name (CN) to CSP on page 44		

Table continues…

No.	Task	Notes	✔
2	Configure the cluster attribute for Centralized Logging. You need to perform the following tasks: 1. Changing the targeted Breeze cluster in Deny New Service state on page 45 2. Configuring Centralized Logging on the cluster editor on page 46 3. Changing the Avaya Breeze cluster state to accept new service on page 46		
3	Install Metricbeat and Packetbeat Snap-in on the Breeze cluster for metrics and traffic data related information. You need to perform the following task: • Download the latest Metricbeat and Packbeat SVAR from the Avaya Support website at https://support.avaya.com. • Installing the Metricbeat and Packbeat Snap-in on the Breeze cluster on page 47		
4	View Logs on CSP OpenSearch UI. You need to perform the following tasks: 1. Logging in to OpenSearch UI on page 47 2. Creating custom index patterns on page 48 3. Creating index policies for the custom index patterns on page 48 4. Discovering data using new index patterns on page 51 5. Recovery steps if the elasticsearch disk size is full on page 51		

Adding Breeze CA certificate to the Elasticsearch truststore on CCM

About this task

To add Breeze CA certificate to the Elasticsearch truststore on CCM, perform the following procedures:

Procedure

1. Loading the Breeze CA certificate into the Elasticsearch truststore on page 43.

2. Restarting the Elasticsearch cluster on page 43.

Loading the Breeze CA certificate into the Elasticsearch truststore

Procedure

1. Log in to the SMGR.
2. Go to **Service** > **Inventory** > **Manage Elements** and select the Breeze node.
3. From **More Actions** menu, select **Manage Trusted Certificate**.
4. Select a value from the **Store Description** column with **WEBSPHERE** as **Store Type** and click **Export**.

   The `trust-cert.pem` file is generated.
5. To transfer the `trust-cert.pem` file to the CSP CCM, run the following commands on CCM Command Line Interface (CLI):

   - `ccmcertmgr -ls trust | grep logelasticsearch`
   - `ccmcertmgr --add-trustcert logelasticsearch-certificate-default-logelasticsearch-mtls-trustedcert trust-cert.pem`

   The trust-cert.pem is the CA certificate of Breeze.

   Example of an expected output:

```
{
"status": "CREATED",
"statusCode": 201,
"timestamp": "12-03-2025 08:49:05",
"message": "logelasticsearch-certificate-default-logelasticsearch-mtls-
trustedcert : Certificate added to trusted store successfully"
}
```

Restarting the Elasticsearch cluster

About this task

This procedure does not impact the service of Analytics operations.

Procedure

1. Run the following commands as root user to restart the Elasticsearch cluster to pull in the Breeze CA certificate:

   ```
   kubectl scale statefulsets/logelasticsearch --replicas=0
   ```
2. Monitor pod state by running the following command:

   ```
   kubectl get pods | grep logelasticsearch
   ```
3. After all the logelasticsearch* pods are terminated, run the following command to bring them up:

   ```
   kubectl scale statefulsets/logelasticsearch --replicas=3
   ```

Adding Breeze node Common Name (CN) to CSP

About this task

To add Breeze node to CN to CSP, perform the following procedures:

Procedure

1. Retrieving the Breeze node CN on page 44.
2. Adding Breeze CN to CCM through CLI on page 44
3. Adding CSP CA to Avaya Breeze truststore on page 45

Retrieving the Breeze node CN

Procedure

1. Log in to the SMGR.
2. Go to **Service** > **Inventory** > **Manage Elements** and select the breeze node.
3. From **More Actions** menu, select **Manage Trusted Certificate**.
4. Check the **Subject Name** field value with **Store Type** as **WEBSPHERE** to see the CN value.

   An example of a CN value: C=US, O=Avaya, CN= <fqdn_of_the_breeze_node> where <fqdn_of_the_breeze_node> is CN for the breeze node.

Adding Breeze CN to CCM through CLI

Procedure

1. On the CCM lab, log in as a root user.
2. Obtain the `addCNMappingExt.tar.gz` file from the Avaya Support website at support.avaya.com. Place the file in the CCM lab folder `/var/avaya/artifactCache` folder of the CCM lab.
3. Run the following to change directory to `/var/avaya/artifactCache`:

   ```
   cd /var/avaya/artifactCache
   ```

4. Untar the compressed file in the CCM using the following command:

   ```
   tar -xvzf addCNMappingExt.tar.gz -C /var/avaya/artifactCache
   ```

5. Run the following to change directory to `/var/avaya/artifactCache/addCNMappingExt`:

   ```
   cd /var/avaya/artifactCache/addCNMappingExt
   ```

6. If the script file is copied from the Windows machine, convert it to Unix format using the following command:

   ```
   dos2unix addCNMappingExt.sh
   ```

7. Set the execution permissions on the script using the following command:

   ```
   chmod 755 addCNMappingExt.sh
   ```

8. The CN needs to be added using the following command for each node at a time:

   ```
   ./addCNMappingExt.sh -cn <fqdn of the breeze node>
   ```

   Repeat for each Breeze node in the Customer Engagement Breeze cluster.

   Example of an expected output: `The CN -` <fqdn of the breeze node> added successfully with READ-WRITE permissions.

Adding CSP CA to Avaya Breeze truststore

Procedure

1. On the CCM lab, log in as a root user.
2. Run the following command to get the CSP CA:

   ```
   kubectl get secrets --namespace default fluentd-ca-crt -o go-
   template='{{index .data "root-cert.pem"}}' | base64 -d > root-cert.pem
   ```

3. Transfer the `root-cert.pem` file created to your local machine using a utility tool such as, WinSCP or FileZilla.
4. Log in to SMGR and go to **Elements** > **Avaya Breeze** > **Cluster Administration** and then select the Breeze customer engagement cluster and select **Certificate Management** > **Install Trust Certificate**.
5. In the **Install Trusted Certificate** form select WEBSPHERE under **Select Store Type** to install the trusted certificate.
6. Click **Browse** to select the CSP `root-cert.pem` file on your local server and click **retrieve**.

   The CA details is displayed.

7. Click **commit** to add CA to the WEBSPHERE trust store.

Changing the targeted Breeze cluster in Deny New Service state

About this task

Change the Customer Engagement Breeze cluster status to **Deny New Service** in the SMGR.

Procedure

1. Log in to the SMGR.
2. Go to **Elements** > **Avaya Breeze** > **Cluster Administration**

3. Select the customer engagement Breeze cluster and click **Cluster state** > **Deny New Service** and then click **Continue**.

Configuring Centralized Logging on the cluster editor

About this task

Use this procedure to configure centralized logging on the cluster editor.

Procedure

1. Log in to SMGR.
2. Go to **Elements** > **Avaya Breeze** > **Cluster Administration** and select the Breeze Cluster and click **Edit** from menu.
3. In the **Cluster Attributes** section, from **Centralized logging destination** drop down menu select **CSP Elasticsearch**.

   Note:

   The check box **Use secure connection for centralized logging?** is selected by default when using CSP for the centralized logging solution. Insecure connections are not supported.
4. Provide the CSP/Analytics Cluster FQDN or IP Address in the text box **CSP Elasticsearch as destination**. For example, xyz190.abc.com:30004 (<CSP_Cluster_FQDN>:PORT)
5. Click **Commit** to save the changes.

Changing the Avaya Breeze cluster state to accept new service

About this task

Change the Breeze cluster status to **Accept New Service**.

Procedure

1. Log in to the SMGR.
2. Go to **Elements** > **Avaya Breeze** > **Cluster Administration**
3. Select the customer engagement Breeze cluster and click **Cluster state** > **Accept New Service** and then click **Continue**.

Installing the Metricbeat and Packbeat Snap-in on the Breeze cluster

About this task

Install Metricbeat and Packetbeat Snap-in on the Breeze cluster for metrics and traffic data related information.

Before you begin

Obtain the latest Metricbeat and Packbeat SVARs from the Avaya Support website at support.avaya.com.

Procedure

1. Log in to the SMGR.
2. Go to **Elements** > **Avaya Breeze** > **Service Management** > **Services** and click **Load** and then select the relevant file and accept the End User License Agreement (EULA).

   This step takes a few minutes due to the EULA load time.
3. Select the loaded service and click **Install**.
4. Select the targeted Breeze cluster and click **Install**.

Logging in to OpenSearch UI

About this task

Log in to OpenSearch UI using the following URL: `https://<csp__cluster_fqdn>/logging/`.

The following script is provided on CSP which creates a READ-WRITE user on Keycloak:

`createKibanaUser`

Procedure

1. On the CCM lab, log in as a root user.
2. Run the following command:

   ```
   ccm release common-services createKibanaUser -u adminuser -r READ-WRITE
   ```

   For example, the following message is displayed:

   ```
   User created successfully on Keycloak!
   User role assigned successfully on Keycloak!
   UserName = adminuser
    Password = Passwd@0987654321
   ```
3. Login to `https://<CSP Cluster FQDN>/logging/` using the credentials created.

Note:

When you access for the first time, you are prompted to change the password.

Creating custom index patterns

About this task

After you configure the Centralized Logging on the Breeze cluster and install the svars, indices are available in the following format: filebeat-<version>-<date> , metricbeat-<version>-metricbeat, packetbeat-<version>-<date>. For example, filebeat-8.5.3-2023.02.21.

You can create filebeat-* , metricbeat-* and packetbeat-* index patterns one by one.

Procedure

1. On the OpenSearch UI, click ☰ to display the navigation pane.
2. On the navigation pane, click **Management** > **Stack Management** > **Index Patterns** > **Create Index Pattern** and type the **Index pattern name**.
3. Click **Next step** and from the **Time field** menu select **@Timestamp**.
4. Click **Show Advanced Setting** and type the **Custom index pattern ID** same as index-pattern and click **Create Index Pattern**.

Creating index policies for the custom index patterns

About this task

Set up storage policies for the created indices. The retention values need to be adjusted according to the solution requirements and the storage size.

The fields, "min_index_age" and "min_size" under transition conditions for “read_only” and “delete” need to be configured.

Procedure

1. On the OpenSearch UI, click ☰ to display the navigation pane.
2. On the navigation pane, go to **OpenSearch Plugins** > **Index Management** and click **Create policy** and then select **JSON editor**.
3. In **Policy ID**, enter a name for the policy, for example: "breeze-default-policy-filebeat."
4. Replace the contents in **Define Policy** with the relevant files for each index pattern.

Example of a sample for "filebeat" JSON policy set for 100 agents lab with PVC Size: 80GB as below:

```
{
    "policy": {
        "description": "Adding log retention policy for Breeze logs coming from
filebeat.",
        "error_notification": null,
        "default_state": "read_write",
        "states": [
            {
                "name": "read_write",
                "actions": [
                    {
                        "retry": {
                            "count": 3,
                            "backoff": "exponential",
                            "delay": "1m"
                        },
                        "read_write": {}
                    }
                ],
                "transitions": [
                    {
                        "state_name": "read_only",
                        "conditions": {
                            "min_index_age": "2d"
                        }
                    },
                    {
                        "state_name": "read_only",
                        "conditions": {
                            "min_size": "1gb"
                        }
                    }
                ]
            },
            {
                "name": "read_only",
                "actions": [
                    {
                        "retry": {
                            "count": 3,
                            "backoff": "exponential",
                            "delay": "1m"
                        },
                        "read_only": {}
                    }
                ],
                "transitions": [
                    {
                        "state_name": "delete",
                        "conditions": {
                            "min_index_age": "7d"
                        }
                    }
                ]
            },
            {
                "name": "delete",
                "actions": [
                    {
                        "retry": {
                            "count": 3,
```

```
                            "backoff": "exponential",
                            "delay": "1m"
                        },
                        "delete": {}
                    }
                ],
                "transitions": []
            }
        ],
        "ism_template": [
            {
                "index_patterns": [
                    "filebeat-*"
                ],
                "priority": 0
            }
        ]
    }
}
```

For policy recommendations for different deployment sizes, see Policy recommendations for different deployment sizes on page 50.

Policy recommendations for different deployment sizes

The following table lists the policy recommendations for different deployment sizes:

	100 agents **PVC Size: 80GB**	**500 agents** **PVC Size: 120GB**	**1000 agents** **PVC Size: 150GB**	**2000 agents** **PVC Size: 200GB**	**4500 agents** **PVC Size: 300GB**
Filebeat policy	ready_only min_index_age: 2d ready_only min_index_size : 1GB delete min_index_age: 7d	ready_only min_index_age: 2d ready_only min_index_size : 2GB delete min_index_age: 7d	ready_only min_index_age: 2d ready_only min_index_size : 5GB delete min_index_age: 7d	ready_only min_index_age: 2d ready_only min_index_size : 5GB delete min_index_age: 7d	ready_only min_index_age: 2d ready_only min_index_size : 10GB delete min_index_age: 7d
Packetbeat policy	ready_only min_index_age: 2d ready_only min_index_size : 3GB delete min_index_age: 2d	ready_only min_index_age: 2d ready_only min_index_size : 3GB delete min_index_age: 2d	ready_only min_index_age: 2d ready_only min_index_size : 3GB delete min_index_age: 2d	ready_only min_index_age: 2d ready_only min_index_size : 3GB delete min_index_age: 2d	ready_only min_index_age: 2d ready_only min_index_size : 3GB delete min_index_age: 2d

Table continues…

	100 agents PVC Size: 80GB	500 agents PVC Size: 120GB	1000 agents PVC Size: 150GB	2000 agents PVC Size: 200GB	4500 agents PVC Size: 300GB
Metricbeat policy	ready_only min_index_age: 2d ready_only min_index_size : 3GB delete min_index_age: 2d	ready_only min_index_age: 2d ready_only min_index_size : 3GB delete min_index_age: 2d	ready_only min_index_age: 2d ready_only min_index_size : 3GB delete min_index_age: 2d	ready_only min_index_age: 2d ready_only min_index_size : 3GB delete min_index_age: 2d	ready_only min_index_age: 2d ready_only min_index_size : 3GB delete min_index_age: 2d

Note:

The min index age in the read only transition should be less than or equal to the min index age in the delete transition.

If the Index size needs to be increased, ensure that the PVC size supports them.

Discovering data using new index patterns

Procedure

1. On the OpenSearch UI, click ☰ to display the navigation pane.
2. On the navigation pane, go to **Opensearch Dashboards** > **Discover**.
3. Use the **Add filter** and **Filter by type** options to filter the data displayed.
4. You can customize and save dashboards.

Recovery steps if the elasticsearch disk size is full

About this task

Delete the indices if the elasticsearch disk size if full.

Procedure

1. On the OpenSearch UI, click ☰ to display the navigation pane.
2. On the navigation pane, go to **Management** > **Dev Tools**.
3. Run the following command to get indices with size:

```
GET /_cat/indices?v&h=index,pri,rep,store.size
```

4. Run the following command to delete the indices of bigger sizes:

   ```
   DELETE /<index_name>
   ```

Chapter 8: Access Oceana Data Viewer

Oceana Data Viewer overview

Oceana Data Viewer is a debugging and visualization tool for Avaya Oceana®. With this tool, you can view the Chat, Email, SMS, Social, Messaging, and Generic contacts that are in Omnichannel Database.

With this tool, administrators and support engineers can directly:

- Reply to Email contacts if there is an issue in routing emails.
- Close or requeue Email and Generic contacts.
- Close Social Media, Chat, and SMS contacts.
- View transcripts for Email or Chat contacts that are sent to an external filtering service, and to mark them as permanently or temporarily failed.

Oceana Data Viewer is not a real-time application. Therefore, you must manually refresh the Oceana Data Viewer page to view updated statistics.

Supported browsers

Oceana Data Viewer supports the following browsers:

- Mozilla Firefox
- Google Chrome
- Microsoft Edge (and Chromium for Edge)

It does not support Microsoft Internet Explorer and mobile browsers. For information about the versions of the supported browsers, see *Avaya Oceana® Solution Description*.

Logging in to Oceana Data Viewer

About this task

Use this procedure to log in to Oceana Data Viewer to view the Chat, Email, SMS, Social, Generic, and Messaging contacts in Omnichannel Database.

By default, only one user can be logged in to Oceana Data Viewer at a time. When a new user logs in, any previously logged-in user is automatically logged out. To allow multiple users to log in at the same time, you must configure the **Maximum concurrent user sessions** attribute of the OceanaDataViewer service through System Manager.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, in the **Service URL** column on Avaya Oceana® Cluster 3, select **Oceana Data Viewer**.

   System Manager opens the Avaya Breeze® platform authentication page in a new browser window.
3. On the Avaya Breeze® platform authentication page, do the following:
   a. In the **Username** field, enter the user name of the Avaya Workspaces administrator configured in Avaya Control Manager.
   b. In the **Password** field, enter the password of the Avaya Workspaces administrator configured in Avaya Control Manager.
   c. Click **SIGN IN**.

      The browser window displays the Oceana Data Viewer home page.

Oceana Data Viewer home page

The following table lists the buttons on the Oceana Data Viewer home page:

Button	Description
EMAIL	The button to view the Email home page containing the details of all Email contacts.
SMS	The button to view the SMS home page containing the details of all SMS contacts.
SOCIAL	The button to view the Social home page containing the details of all Social contacts.
GENERIC	The button to view the Generic home page containing the details of all Generic contacts.
CHAT	The button to view the Chat home page containing the details of all Chat contacts.
STATISTIC	The button to view high-level statistics about contact center operations.
MESSAGING	The button to view the Messaging home page containing the details of all Messaging contacts.

Email contacts management

The following table lists the buttons on the Email home page:

Button	Description	Measures in Avaya Analytics™
New	The button to view actions from Email contacts that are not routed to an agent.	Avaya Analytics™ reports these contacts as new contacts when queuing. When alerting on Avaya Workspaces, they are offered or alerting.
Open	The button to view actions from Email contacts that are answered by an agent and are in progress.	Avaya Analytics™ reports these contacts as active or answered contacts.
Transferred To Service	The button to view actions from Email contacts that are transferred to a service. These are effectively new contacts that are not routed to an agent. When an agent answers, they are marked as open.	Avaya Analytics™ reports these contacts as new transferred-to-service or waiting contacts.
Transferred To User	The button to view actions from Email contacts that are transferred to an agent.	Avaya Analytics™ reports these contacts as new transferred-to-user contacts.
Failed	The button to view actions from Email contacts that failed to be routed to an agent.	Avaya Analytics™ reports these contacts as completed. If there is one failed Email contact listed here, Avaya Analytics™ reports 0 waiting or new contacts.
Closed	The button to view actions from Email contacts that are answered by an agent and are closed.	Avaya Analytics™ reports these contacts as completed, offered, and answered contacts.
Agent Replied	The button to view actions from Email contacts to which an agent has replied.	Avaya Analytics™ reports these contacts as completed and replied.
In Queue	The button to view actions from email outbound Email contacts that are ready to be sent.	Avaya Analytics™ reports these contacts as the contacts that are waiting but not offered.
Not Sent	The button to view actions from email outbound Email contacts that was not sent because of a reason such as invalid address.	Avaya Analytics™ does not display these contacts.
Agent Created	The button to view actions from adhoc Email contacts that are created by an agent.	Avaya Analytics™ reports these contacts as adhoc emails.
Failed	The button to view actions that failed to be sent out to an external transcript filtering service.	Avaya Analytics™ does not display these contacts.

Table continues…

Button	Description	Measures in Avaya Analytics™
Successful	The button to view actions that are successfully sent out to an external transcript filtering service.	Avaya Analytics™ does not display these contacts.
Permanently Failed	The button to view actions that permanently failed to be sent to an external transcript filtering service. The Email Service repeatedly failed to send the transcript over a 30-day period.	Avaya Analytics™ does not display these contacts.
Approved	The button to view the emails subject to email approval by an approver, and approved, and sent to the customer.	Avaya Analytics™ reports these contacts as completed, approval review approved, and work approved.
In Approval Process	The button to view the emails that are currently in the approval process, either waiting for an approver to review; or waiting for an agent to re-draft after an approver rejected it.	Avaya Analytics™ reports these contacts as contacts waiting for approval but not answered, or contacts waiting for rework but not answered.
Rejected and Closed	The button to view the emails rejected by an email approver, and subsequently closed by an agent. These emails were not sent to the customer.	Avaya Analytics™ reports rejected contacts as completed, approval review rejected, and work rejected. Rejected contacts subsequently closed by an agent are reported as completed and rework closed.
Forwarded	The button to view the emails that are forwarded to other recipients.	Avaya Analytics™ reports these contacts as answered, completed, and forwarded.
Deferred	The button to view the emails that are deferred.	Avaya Analytics™ reports these contacts as contacts waiting for approval, not answered, or deferred.

Viewing the details of an email

About this task

When viewing the list of emails in Omnichannel Database, you can view the content of an email. You can also reply to the email contact if the routing is not functional.

Procedure

1. Log in to Oceana Data Viewer.
2. On the Oceana Data Viewer home page, click **EMAIL**.
3. On the Email home page, click the button based on your requirement.

   For example, to view the list of open emails, click **Open**.

4. In the list of emails, locate the required email and click **Details**.

   Oceana Data Viewer displays the Email Details page.

   For transcripts, the Email Details page displays the body of the email.

5. To reply to the email contact, click **Direct Reply**.

   Oceana Data Viewer opens a new window in your email client to draft a new email.

   Important:

   Your email client must be able to access the mail server.

6. Copy the content of the original email from the Email Details page to the new window in your email client.

Resending a transcript

About this task

If a temporary failure occurs in sending a transcript, you can resend the transcript.

Oceana Data Viewer rejects the request to resend the transcript if:

- The transcript filtering service URL is empty.
- Omnichannel Administration Utility is set to not allow transcripts to be sent.
- The transcript is already sent successfully.

Procedure

1. Log in to Oceana Data Viewer.
2. On the Oceana Data Viewer home page, click **EMAIL**.
3. On the Email home page, click **Failed Transcripts**.
4. In the list of emails, locate the required email and click **Resend transcripts**.

   Oceana Data Viewer reads the configuration from Omnichannel Database and takes the appropriate actions.

Changing the status of a transcript

About this task

With this procedure, you can mark:

- A failed transcript as permanently failed
- A permanently failed transcript as failed.

The purpose of changing the status of a transcript is to prevent corrupted emails from being sent out to the transcript filtering service and repeatedly failing to filter.

Procedure

1. Log in to Oceana Data Viewer.

2. On the Oceana Data Viewer home page, click **EMAIL**.
3. On the Email home page, click **Failed Transcripts**.
4. In the list of emails, locate the required email and click **Mark permanently failed**.

Chat, SMS, Messaging, and Social contacts management

The following table lists the buttons on the Chat, SMS, Messaging, and Social home pages:

Button	Description	Measures in Avaya Analytics™
New	The button to view contacts that are not routed to an agent.	Avaya Analytics™ reports these contacts as new contacts when queuing. When alerting on Avaya Workspaces, they are offered or alerting.
Open	The button to view contacts that are answered by an agent and are in progress.	Avaya Analytics™ reports these contacts as active or answered contacts.
Transferred	The button to view contacts that are transferred to another service. These are effectively new contacts that are not routed to an agent. When an agent answers, they are marked as open.	Avaya Analytics™ reports these contacts as new transferred-to-service or waiting contacts.
Transferred-To-User	The button to view contacts that are transferred to another agent.	Avaya Analytics™ reports these contacts as new transferred-to-user contacts.
Failed	The button to view contacts that failed to be routed to an agent.	Avaya Analytics™ reports these contacts as completed.
Closed	The button to view contacts that are answered by an agent and are closed.	Avaya Analytics™ reports these contacts as completed, offered, and answered contacts.
Successful Transcripts	The button to view transcripts for this channel type that are successfully sent out to an external transcript filtering service.	Avaya Analytics™ does not display these contacts.
Failed Transcripts	The button to view transcripts for this channel type that failed to be sent out to an external transcript filtering service.	Avaya Analytics™ does not display these contacts.
Permanently Failed Transcripts	The button to view transcripts for this channel type that permanently failed to be sent to an external transcript filtering service. This status is reserved for the transcripts that repeatedly failed over a 30-day period or the transcripts that are marked as such in Oceana Data Viewer.	Avaya Analytics™ does not display these contacts.

Closing Social Media, SMS, Messaging, and Chat contacts

About this task

With this procedure, you can close Social Media, SMS, Messaging, and Chat contacts that are in a new or transferred state. The purpose of closing the contacts is to close old contacts that are not answered.

After you complete this procedure, the contacts are closed in the OmniResourceConnector service and Avaya Oceana®.

Procedure

1. Log in to Oceana Data Viewer.
2. On the Oceana Data Viewer home page, click **SOCIAL**.
3. On the Social home page, click **New**.
4. In the list of Social contacts, select the check boxes for the contacts that you want to close, and click **Close all checked contacts**.

   The header displays that the contacts are closed and Oceana Data Viewer redirects you to the Social home page.
5. On the Oceana Data Viewer home page, click **SMS**.
6. On the SMS home page, click **New**.
7. In the list of SMS contacts, select the check boxes for the contacts that you want to close, and click **Close all checked contacts**.

   The header displays that the contacts are closed and Oceana Data Viewer redirects you to the SMS home page.
8. On the Oceana Data Viewer home page, click **CHAT**.
9. On the Chat home page, click **New**.
10. In the list of Chat contacts, select the check boxes for the contacts that you want to close, and click **Close all checked contacts**.

    The header displays that the contacts are closed and Oceana Data Viewer redirects you to the Chat home page.

Transcripts page for messaging contacts

The following table lists the fields on the Transcripts page for messaging contacts:

Field	Description
ContactId	The current ID for this contact in Omnichannel Database.
Customer ID	The customer ID
Creation Time	Timestamp information about when the messaging contact was created

Table continues…

Field	Description
Work Request ID	The global ID used in Avaya Oceana® to identify contacts. This ID is also referred to as a context ID.
Drilldown	The button to view the drill-down information such as timestamp, sender, message length, and message type.
Resend	The button to resent the transcript
Mark permanently failed	The button to change the status of the transcript from failed to permanently failed.

Generic contacts management

The following table lists the buttons on the Generic home page:

Button	Description	Measures in Avaya Analytics™
New	The button to view actions from Generic contacts that are not routed to an agent.	Avaya Analytics™ reports these contacts as new contacts when queuing. When alerting on Avaya Workspaces, they are offered or alerting.
Open	The button to view actions from Generic contacts that are answered by an agent and are in progress.	Avaya Analytics™ reports these contacts as active or answered contacts.
Closed	The button to view actions from Generic contacts that are answered by an agent and are closed.	Avaya Analytics™ reports these contacts as completed, offered, and answered contacts.
Transferred To Service	The button to view actions from Generic contacts that are transferred to a service. These are effectively new contacts that are not routed to an agent. When an agent answers, they are marked as open.	Avaya Analytics™ reports these contacts as new transferred-to-service or waiting contacts.
Transferred To User	The button to view actions from Generic contacts that are transferred to an agent.	Avaya Analytics™ reports these contacts as new transferred-to-user contacts.
Failed	The button to view actions from Generic contacts that failed to be routed to an agent.	Avaya Analytics™ reports these contacts as completed. If there is one failed contact listed here, Avaya Analytics™ reports 0 waiting or new contacts.

Statistics home page

The Statistics home page of Oceana Data Viewer displays the following high-level statistics about contact centre operations:

Statistic	Description
Customers	The total number of customers in Omnichannel Database.
Contacts	The total number of contacts in Omnichannel Database.
Attachments	The total number of attachments in Omnichannel Database.
Oldest Waiting Contact Time	The list of contacts that are not yet answered by agents.
Contacts per Customer	The list of customers with a large number of contacts. Avaya recommends not to have more than 100 contacts per customer.
Contacts closed by DataViewer	The list of contacts that are closed through Oceana Data Viewer.
Contacts with Processing Errors	The list of contacts that are not correctly processed.
Contacts in Renew Process	The list of contacts that are being renewed.
Inboxes	The list of inbox details of contacts.

Downloading to CSV

About this task

You can download a comma separated file that displays the output of any of the data pages in Oceana Data Viewer.

Procedure

1. Open a data page of the information that you want to view.

   For example, on the Oceana Data Viewer home page, click **SMS** and then click **Permanently Failed SMS Transcripts**.

   The Viewing All Permanently Failed SMS Transcripts page displays all the SMS contacts that permanently failed.

2. On the menu bar, click **Download to CSV**.

   A comma separated CSV file downloads to your system, containing information about all permanently failed SMS contacts.

Chapter 9: Troubleshooting licensing

Troubleshooting licensing

This topic describes issues related to licensing in an Avaya Oceana®, and how to troubleshoot these issues.

Checking System Manager WebLM licenses

About this task

Use this procedure to check System Manager WebLM licenses.

Procedure

1. Log on to the System Manager web console.
2. Navigate to **Services** > **Licenses**.
3. In the **Product Name** column, look for licenses for each Avaya Oceana® feature.
4. In the navigation pane, click **AVAYA_OCEANA** > **View license capacity** to view license details.
5. If you are missing a license key, in the navigation pane, click **Server properties** and use the **Primary Host ID** value to obtain the missing license from Avaya PLDS.

   Important:

   - If your solution includes Avaya Experience Portal and is using the WebLM on this System Manager as the license server, ensure that you have a **Voice_Portal** license. To check this, in the navigation pane, click **Voice_Portal** > **View license capacity**.
   - If your solution includes an Avaya Aura® Media Server (MS) and is using the WebLM on this System Manager as the license server, ensure you have a **Media_Server** license. To check this, in the navigation pane, click **Media_Server** > **View license capacity**.

Checking Avaya Oceana® SVAR licenses

About this task

Use this procedure to check Avaya Oceana® SVAR licenses

Procedure

1. On the System Manager web console , click **Avaya Breeze®** > **Service Management** > **Services**.
2. Ensure that each **Installed** SVAR that requires a license has a green check mark in the **License Mode** column.
3. If you are missing a SVAR license key, navigate to **Licenses** > **Server properties** and use the **Primary Host ID** value to obtain the missing SVAR license from Avaya PLDS.

Troubleshooting Avaya Control Manager licensing problems

License server service not starting

Condition

License server service not starting

Cause

WebLMNet.dll related error in logs of license server service.

Solution

Install C++ Redistributable 2013 and 2015-2019(x86) on Control Manager server and then try to start license server service.

No valid license found error when you login to Control Manager

Condition

No valid license found error when you login to Control Manager.

Cause

Control Manager is in Restricted Mode and Grace period of 30 days is over

Solution

1. Install valid Control Manager license on WebLM server and configure WebLM server in Control Manager through Health Monitoring tool.
2. On the Control Manager server, start Health Monitoring Diagnostics from system tray.
3. Click on **WebLM Server** tab.
4. Enter WebLM server URL in this format, for example https://<WebLM_Server_IPAddress>:52233/WebLM/LicenseServer
5. Click **Test** to verify connectivity.
6. Click **Save**.
7. Restart ACCCM license server service.

User cannot access Avaya Oceana® admin screens when Control Manager is in grace mode

Condition

User receives licensing related error messages while administering features like Avaya Oceana® admin screens when Control Manager is in Grace mode

Cause

Valid license file is not installed on WebLMServer or WebLM server is down or WebLMis being upgraded. This WebLMis configured with Control Manager.

Solution

To continue Control Manager to work in Grace Mode with all features, Work around to this issue is either remove WebLM configuration from Control Manager or install valid license file on WebLM server and restart license service on Control Manager server.

Control manager showing grace mode warning message

Condition

Control manager showing grace mode warning message

Cause

No valid license details received from WebLMWebLM server due to:

- Incorrect WebLM server is configured
- Valid Control Manager license file is not installed on WebLM server
- Control Manager is not able to reach WebLM server due to network issues
- Installed Control Manager's major version (9 in 9.x.x.x) does not match the major version of Control Manager (9 in 9.x.x.x) recorded with the WebLM license installed on the WebLM server. If the major version does not match, then Control Manager enters in the Grace mode

Solution

1. Configure WebLM Server in Control Manager, test connection and if connection is successful then restart license server service. Ensure that you have valid control manager license file installed on WebLM server.
2. If WebLM server is already configured then check whether valid Control Manager license is installed on WebLM server and ACM is able to communicate with it by testing WebLM server connectivity.
3. Navigate to **Configuration** > **License** > **WebLM Server** and edit the existing WebLM server and click **Test**. If connection is not successful then verify that WebLM server is active and reachable from Control Manager.
4. Check whether Control Manager server in WebLM license file has reached to its limit. If yes, either free some licenses by shutting down Control Manager or request for new license.
5. If test connection to the WebLM server is not successful or anytime WebLM server is shutdown or being upgraded then remove the WebLM configuration from Control Managerand restart the license service for continuous access in Grace mode.

Loading license files in System Manager

About this task

Use this procedure to load the license files for Avaya Breeze® platform nodes and services that are used in Avaya Oceana®.

Procedure

1. On the System Manager web console, click **Services** > **Licenses**.
2. Click **Install License**.
3. On the Install License page, perform the following steps:
   a. Browse to the location of the license that you want to install and select the license file.
   b. Click **Accept the License Terms & Conditions**.
   c. Click **Install**.

      The system installs the license.
4. In the navigation pane, click **Licensed Products** to view the installed license.
5. Perform steps 2 through 4 to install the license for the following services:
   - Context_Store
   - COLLABORATION_ENVIRONMENT (For the Avaya Breeze® platform)
   - Avaya_Oceana

     This license also covers UCM_Reporting.
   - Collaborative_Browsing_Snap_In
   - Work_Assignment
   - Collaboration_Designer
   - Control_Manager
6. In the navigation pane, click **WebLM Home** to verify that the WebLM Home page displays all the licenses.
7. After the services are running, perform the following steps to verify the licenses:
   a. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
   b. On the Services page, verify that the **License Mode** column for all the services displays a check mark.

Chapter 10: Troubleshooting Unified Collaboration Administration

Troubleshooting Unified Collaboration Administration

The Unified Collaboration Administration (UCA) snap-in maintains a space-based store of common administrative data for Avaya Oceana® components and supports a common set of APIs (REST and Java) which allow Avaya Oceana® components to access the data. Although some components set and get data directly, most interact with UCA by registering listeners which fire in response to changes made through the REST API.

The UCA snap-in is installed as part of Avaya Oceana® Cluster 1. Changes to the space-based store are replicated to a postgreSQL database located on the cluster. The space is re-populated from the database on a restart of the cluster or service. Avaya Breeze® platform supports utilities to backup and restore the database. In an Avaya Oceana®, Avaya Control Manager provides a user interface which translates administrative tasks into the appropriate REST operations. Independent use of the REST API is not supported.

Log files location

Refer to the log files to search for a cause when issues occur with UCA. The following table describes the log files for troubleshooting UCA and their location:

Location	Error description	Action
`/vr/log/Avaya/sm/deploy.log`	No response to any REST API	Look for service deployment errors.
`/var/log/Avaya/sm/TextLog_yy.mm.dd_hh.mm.ss.log`	No response to particular REST API	Check `apache.wink` messages.
	Database is not updated.	Check postgreSQL database messages.
`/var/log/Avaya/dcm/gs-gsc*.log`	REST API responds with 500 or 503 error.	Check if space is deployed (need to identify appropriate gsc instances).
	Database is not updated.	Check process is running (need to identify appropriate gsc instance).
`/var/log/Avaya/services/UCAStoreService/UCAStoreService.log`	REST API responds with 500 error.	Check java exceptions.

Solution call flows

Unified Collaboration Administration is not directly involved in handling call flows. Errors in UCA can lead to problems in the following areas:

- Logging in
- Work matching
- Call routing

Tip:

These processes can trigger log admin change events. Check if there are any missing or unexpected events which are the result of UCA issues.

Common issues with Unified Collaboration Administration

The most common issues with Unified Collaboration Administration relate to GigaSpace processes not starting correctly or losing connections. The following table lists the critical UCA attributes to check if an issue occurs:

Issue Description	Action
REST API fails continuously with 404 error.	Check if the UCA service has been deployed correctly on all the nodes. View the `asm` or `TextLog` logs.
Multiple REST methods fail with 500 or 503 error.	Check the following attributes if this issue occurs: • **DeploymentType** being set for the UCA service • The space has been deployed correctly on all the nodes: view the `gsc` log • Messages indicating lost connections between primary and backup spaces
Specific REST methods fail with 500 error.	Check the UCA log files. **Note:** NullPointerExceptions (NPEs) are often associated with space or database referential integrity problems.
Data is not replicated to the database.	This issue can occur on reboot. Check the following attributes if it occurs: • EDM being enabled • `gsc` log existing for mirror PU • Primary space of the `gsc` log

Useful test points for Unified Collaboration Administration

This section describes common troubleshooting scenarios which can be used if UCA issues occur.

Troubleshooting UCA deployment

Unified Collaboration Administration writes serviceability messages to the Manager Space on start up and space deployment. If the Monitor Service and Breeze Authorization service are installed and configured to monitor Avaya Oceana® Cluster 1, the UCA Service status information can be obtained from the Breeze Authorization service.

To view serviceability messages, look at the `UCAStoreService.log` file in the `/var/log/Avaya/services/UCAStoreService/UCAStoreService.log` folder. See the following example of serviceability messages being sent successfully:

```
yyyy-mm-dd hh:mm:ss,990 [UCAContextListener] message.OceanaMonitorCommon INFO -
[M:writeToManagerSpace][T:null]. Finished writing 'OceanaMonitorMessage: Cluster =
Common, Node = WFEDP39130v.wf.aura.com, Service = UCAStoreService, Version =
3.2.0.0.4160.160919.083452, Status = OK, Message = UCAService installation Completed
Successfully..... , Update Time = 1474275642986'
....
yyyy-mm-dd hh:mm:ss,725 [ucaSpaceStatusThread] message.OceanaMonitorCommon INFO -
[M:writeToManagerSpace][T:null]. Finished writing 'OceanaMonitorMessage: Cluster =
Common, Node = WFEDP39130v.wf.aura.com, Service = UCAStoreService, Version =
3.2.0.0.4160.160919.083452, Status = INFO, Message = UCAService space has been deployed
successfully., Update Time = 1474275650722'
```

Troubleshooting REST API

If the UCA service is successfully deployed, when you browse to `https://<Cluster_1_IP_Address>/services/UCAStoreService/uca/channels` the following attributes return:

```
["NoChannel","Voice","Email","Chat","Fax","ScannedDocuments","SocialMedia","ShortMessage
Service","Video","CoBrowse"]
```

The following table shows the list of common errors and their cause:

Error #	Cause
error 503	The space is not yet deployed and is typically in a temporary state.
error 404	If this error occurs continuously, it indicates a service deployment issue.
error 500	If this error occurs continuously with a 503 error, it indicates problems with the space deploying.

By default, UCA requires an authentication token to be supplied in REST request headers. For troubleshooting purposes, you can disable this by changing the UCAStoreService attribute **Enable Tokenless Access** to **TRUE**. The change takes effect once System Manager replicates the setting to the nodes. When you verify the API deployment, you must change this setting back to **FALSE**.

Troubleshooting Avaya Oceana® Cluster 1 database and UCA schema

To check if the Avaya Oceana® Cluster 1 database is installed, perform the following steps:

1. Run the following command: **`hadb_ctl status`**.
2. Check if one node shows the following message:

   ```
   master up ... ready ...
   ```

3. Check if the other node shows the following message:

```
slave up ... ready ...
other up ... ready ...
```

To check if the UCA schema is installed, perform the following steps:

1. Run the following command:

   hadb_ctl listdb
2. Check if all nodes show the following message:

```
ucastoreservice ucastoreservice_ucadb 1-0-xx
```

Note:

You cannot display database content without root authorization.

Important:

To check the UCA schema installation, run the following command:

hadb_ctl printlog

This command can be used for checking UCA schema messages in normal operation.

Replication to database

To find `gsc` log files, go to the `/var/log/Avaya/dcm` folder and run the following commands:

grep uca-store-edm gs-gsc*

grep com.gigaspaces.replication.channel.ucaStoreSpace gs-gsc*

- The first **grep** command finds a `gsc` log file containing a series of messages. These messages show that the mirror service has started and identifies the `gsc` instance. Ensure that these messages end with the following:

```
GSC INFO [com.gigaspaces.grid.gsc] - Instantiated uca-store-edm-3.2.0.0.4160 [1] in
8.2 seconds
```

- The second **grep** command finds a `gsc` log file of the primary UCA space. A series of messages on the start up shows that the mirror is available. See the following successful example of these messages:

```
yyyy-mm-dd hh:mm:ss,379 uca-store-space-3.2.0.0.4160.1 [1] INFO
[com.gigaspaces.replication.channel.out.ucaStoreSpace1.primary-backup-reliable-
async-mirror-1.mirror-service] - Channel state changed from DISCONNECTED to
CONNECTED [target=mirror-service, target url=jini://*/mirror-service_container/
mirror-service?
schema=persistent&versioned=true&id=1&total_members=1,1&cluster_schema=partitioned-
sync2backup&locators=10.134.39.205:7000,10.134.39.202:7000&groups=DCM&state=started&
timeout=5000, target machine connection url=NIO://10.134.39.205:7019/pid[14160]/
260208743379_3_6475720491806715108_details[class
com.gigaspaces.internal.cluster.node.impl.router.AbstractConnectionProxyBasedReplica
tionRouter$ConnectionEndpoint(mirror-service_container:mirror-service)]]

yyyy-mm-dd hh:mm:ss,380 uca-store-space-3.2.0.0.4160.1 [1] INFO
[com.gigaspaces.replication.channel.out.ucaStoreSpace1.primary-backup-reliable-
async-mirror-1.mirror-service] - Channel state changed from CONNECTED to ACTIVE
[target=mirror-service, target url=jini://*/mirror-service_container/mirror-service?
schema=persistent&versioned=true&id=1&total_members=1,1&cluster_schema=partitioned-
sync2backup&locators=10.134.39.205:7000,10.134.39.202:7000&groups=DCM&state=started&
timeout=5000, target machine connection url=NIO://10.134.39.205:7019/pid[14160]/
260208743379_3_6475720491806715108_details[class
```

```
com.gigaspaces.internal.cluster.node.impl.router.AbstractConnectionProxyBasedReplica
tionRouter$ConnectionEndpoint(mirror-service_container:mirror-service)]]
```

Note:

A `gsc` log file can also contain messages which indicate the cause for replication failure.

Chapter 11: Troubleshooting Call Server Connector

Troubleshooting Call Server Connector

The Call Server Connector (CSC) snap-in is a voice-only Service Provider interface to the underlying switching infrastructure. CSC provides call and agent control functions.

In an Avaya Oceana®, CSC communicates with Communication Manager (CM) through the Device, Media and Call Control (DMCC) interface in Application Enablement Services (AES). CSC is implemented as a TSAPI application to receive Communication Manager events through AES. CSC uses AES to control and monitor CM voice calls and resources.

The CSC snap-in obtains administration and configuration information from the Unified Collaboration Administration (UCA) snap-in.

The CSC snap-in provides the call state and agent state to the Unified Collaboration Model (UCM) snap-in. The CSC snap-in, through the UCM snap-in, notifies Work Assignment (WA) about availability of relevant resources, as configured by Avaya Control Manager in System Manager.

Log files location

Refer to the log files if there are issues with the CSC service deployment. You can find the CSC service log file and the PU log file in the following folders:

Log name	Location	Output log files
CSC Service log file	`/var/log/Avaya/services/CallServerConnector/CallServerConnector.log`	-
PU log files	`/var/log/Avaya/dcm/pu/CallServerConnector/`	CSTA messages log `CSC-csc-<version><instance>-CstaMsgs.log` PU log `CSC-csc-<instance>.log`

Note:

Each CSC PU produces both CSTA messages and PU log files.

The log statements generated as a result of the deployment of the CSC snap-in service are written to the `CallServerConnector.log` file. CSC PU log files are written only to the Avaya Breeze® platform nodes where CSC PU instances are running.

Important:

For each configured Communication Manager there are two CSC PU instances: Primary and Backup. These are typically on two different Avaya Breeze® platform nodes. When gathering log files, ensure to copy the logs from all CSC PU instances.

The location of Primary and Backup CSC PU instances is not linked to Avaya Breeze® platform Active or Standby nodes for any Avaya Breeze® platform feature. For example, Avaya Breeze® platform Load Balancer or Cluster Database Active or Standby nodes. CSC PU Primary and Backup instances are managed by Gigaspaces.

Providing traces for troubleshooting

When providing traces for further investigation by Avaya support teams, capture the following information:

1. An approximate timestamp for the occurrence of the issue. Ensure to capture the relevant log above as the log files roll over when capturing historical data. Note that the latest version of the log file can not contain the relevant log statements for the timestamp of the issue occurrence.
2. Address of the resources. Providing the resource address simplifies the debugging of issues.
3. An accurate description of the issue. Avaya recommends that you document any steps taken to debug the issue and any other pertinent information before providing this information to Avaya support.

CSC connection to AES

About this task

To check if the Call Server Connector snap-in is connected to Application Enablement Services, perform the following steps:

Procedure

1. On the AES web console, click **Status** and then click **Status and Control**.
2. Click **DMCC Service Summary**.
3. In the Session Summary screen, for each configured AES or Communication Manager link in CSC, check for two **Khepri Call Server Connector** entries. The far-end identifier for both the CSC Primary PU instance and the CSC Backup PU instance must match the IP addresses of the node where a CSC PU instance is running.

SSL handshake failure

Condition

The CSC PU log files show the following errors:

```
18/06 11:54:23.081 [pool-10-thread-4] ERROR oClientSocket$SslTasksExecutor - run()
javax.net.ssl.SSLHandshakeException: General SSLEngine problem
```

Cause

These errors are caused by the incorrect configuration of certificates on either Application Enablement Services or on System Manager.

Solution

1. Ensure that the root certificate of the Application Enablement Services Certificate Authority (CA) is installed on Avaya Breeze® platform and added as a trusted CA to all the nodes of Avaya Oceana® Cluster 1.
2. To install this certificate on Avaya Breeze® platform, log on to the System Manager web console and click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
3. Select the cluster and click **Certificate Management** > **Install Trust Certificate (All Avaya Breeze Instances)**.
4. On the **Install Trusted Certificate** screen, select the **WEBSPHERE** store type.
5. Click **Choose File** and navigate to the location of the certificate.
6. Click **Open**.
7. Click **Commit**.

To enforce mutual TLS (MTLS) using AES configuration settings, perform the following steps:

1. Navigate to **AES** > **Security** > **Host AA** > **Service Settings**.
2. Under **DMCC**, select the **Authenticate Client Cert with Trusted Certs** check box and click **Apply Changes**.

Note:

When using this configuration, Application Enablement Services must also trust the Certificate Authority (CA) that issued the Avaya Breeze® platform node certificate. System Manager is the CA for Avaya Breeze® platform and you must download the CA certificate from System Manager and install it on AES.

Download the CA certificate from System Manager and install it on AES.

1. Download the `.pem` file from System Manager.
2. On the System Manager web console, click **Services** > **Security** > **Certificates** > **Authority**
3. In the navigation pane, click **Public Web**.
4. In the Retrieve section, click **Fetch CA Certificates**.
5. Click **Download as PEM** to download the CA certificate.
6. Import the file to AES. Navigate to **AES** > **Security** > **Certificate Management** > **CA Trusted Certificates** > **Import**.

Important:

If System Manager has been rebuilt, this can cause a new Certificate Authority to be generated. You must repeat steps 1-2 above to add the System Manager Certificate Authority certificate to AES.

7. Click **Choose File** and navigate to the location of the previously downloaded System Manager CA certificate.
8. Click **Open**.
9. Click **Apply**.

Potential other reasons for CSC not connected to AES

The following table lists potential reasons for Call Server Connector not being connected to AES:

Issue Description	Cause	Action
SSL connection is successful but CSC disconnects after logging the following line: `18/02 14:50:21.436 [CstaProv] DEBUG avaya.khepri.dmcc.CstaProvider - onSetPrivilegesNegResponse() UNKNOWN_APPLICATION`	AES is not configured with a correct license.	Check the AES License Manager for a valid AES license. Navigate to **AES** > **Licensing** > **WebLM Server Address**.
SSL connection is successful but CSC disconnects after logging the following line: `23/08 16:26:27.262 [CstaProv] DEBUG avaya.khepri.dmcc.CstaProvider - onRequestSystemStatusResponse() disabled [BOACM => link down]`	AES reports its TLINK to CM as down.	Check the status of AES-CM TLINK. Navigate to **AES** > **Status** > **Status and Control** > **TSAPI Service Summary**. **Tip:** If there are issues where AES information is not consistent with the CSC reports, restart AES.
SSL connection is successful but CSC disconnects after logging the following line: `14:41:06.082 [CstaProv] DEBUG com.avaya.khepri.dmcc.CstaProvider - onErrorResponse() SystemRegisterRequest failed: operation -> invalidParameterValue`	CSC attributes are misconfigured.	Ensure that the **cmName** in the **CSC Communication Manager list** attribute has the same value as the TLINK name on Application Enablement Services. Navigate to **AES** > **AE Services** > **TSAPI** > **TSAPI Links**.
SSL connection is successful but CSC disconnects after logging the following line: `05/03 16:16:08.157 [CstaProv ] DEBUG avaya.khepri.dmcc.CstaProvider - onErrorResponse() SystemRegisterRequest failed: operation -> generic`	The TSAPI link on AES is not secure.	Check if security is enabled on the TSAPI link. Navigate to **AES** > **AE Services** > **TSAPI** > **TSAPI Links**. Ensure that security is set to **Encrypted** or **Both**.

Table continues…

Issue Description	Cause	Action
SSL connection is successful but CSC disconnects after logging the following line: `11:52:40.090 [CstaProv] DEBUG com.avaya.khepri.dmcc.CstaProvider - onStartApplicationSessionNegResponse() Authentication failed : clientID=XML Encrypted:135.60.151.207:47588, user=csc`	CSC attributes are misconfigured.	Ensure that the **AES user** and the **AES user password** attributes are correct. Check the AES user configured for the CallServerConnector on Avaya Oceana® Cluster 1, using System Manager. Navigate to **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**. On the **Service Clusters** tab, select Avaya Oceana® Cluster 1 and CallServerConnector to view the **AES user** and the **AES user password** attributes. Ensure that the user configured in AES under **AES** > **User Management** > **User Admin** > **List All Users**, matches the AES user configured for the CallServerConnector on Avaya Oceana® Cluster 1.

Troubleshooting common problems

The following table lists common problems with Call Server Connector:

Issue Description	Details	Cause
Calls are not reflected in Unified Communications Module and Avaya Oceana®.	No calls appear in Avaya Workspaces, but calls are visible on deskphones, even though CSC is connected to Application Enablement Services and Avaya Workspaces is successfully activated. The CSC PU log file contains the following line: `dd/mm hh:mm:ss,000 [477] ERROR khepri.util.SequentialExecutor - run() java.lang.IllegalArgumentException: Mandatory parameter workRequestId must not be null or blank.`	Universal Call Identifier (UCID) support has not been properly enabled on Communication Manager.

Table continues…

Issue Description	Details	Cause
Cannot acquire a resource - acquire request fails.	The CSC PU log file contains the following line with security violation error: `dd/mm hh:mm:ss,000 [6018] DEBUG .avaya.khepri.dmcc.CstaAddress - onErrorResponse() GetDeviceIdRequest failed: operation -> securityViolation`	CTI User configuration on Application Enablement Services is invalid. CTI User has been created for Avaya Oceana® but is missing required privileges.
Agent cannot log in to Avaya Oceana®.	Ensure that an agent can login using a physical phone or One-X Agent. If they cannot, resolve this issue before attempting to log on to Avaya Oceana®.	If this problem is frequent it is not specific for Avaya Oceana® but is a general Communication Manager or Elite issue.
Logging in to Avaya Oceana® fails.	The CSC PU log file contains the following line: `01/09 14:50:48.428 [0939022001 ] DEBUG .avaya.khepri.dmcc.CstaAddress - onErrorResponse() SetAgentStateRequest failed: operation -> invalidAgentState`	The agent password obtained from Unified Collaboration Administration does not match what is configured on Communication Manager or Elite. Re-sync the agent password from Communication Manager to Avaya Control Manager or UCA. Edit the problem user in Avaya Control Manager by navigating to the Avaya Oceana tab and re-saving the user.

Agent cannot start work after logging on to Avaya Workspaces	A “Channel Request Failed” error appears in Avaya Workspaces, and the CSC PU log file contains the following line:
	`19/06 14:23:04.794 [8880006] DEBUG .avaya.khepri.dmcc.CstaAddress - onErrorResponse() SetAgentStateRequest failed: operation -> generic`
	`19/06 14:23:04.794 [8880006] INFO aya.khepri.ucm.LiveUcmProvider - sendFailureResponse() 1a8c6ed7-7458-4822-911a-08c747a1ff12, GENERIC_ERROR [1872337703]`
	`19/06 14:23:04.798 [pool-18-thread-5] INFO cm.DefaultWriteResponseHandler - callback() 1a8c6ed7-7458-4822-911a-08c747a1ff12`
		The agent has a voice channel assigned but the associated station is not logged in.
		To resolve the issue, ensure that the station associated with the agent is logged in and attempt to start work again.

Chapter 12: Troubleshooting Unified Collaboration Model

Troubleshooting Unified Collaboration Model

The Unified Collaboration Model (UCM) snap-in is a real-time object data model that abstracts the work being processed in a system. UCM represents the current state of work and resources within the system. UCM provides a normalization layer that acts as a repository of real-time state that can be passed on to clients through the client listener API.

The Avaya Oceana® uses UCM to monitor agent events and call events on the Avaya Aura® (Application Enablement Services and Communication Manager) platform, and on OmniChannel Provider (OCP). Avaya Oceana® components also use UCM to send third-party call operations to the Call Server Connector (CSC), and OmniChannel Provider . The CSC snap-in is the voice service provider connected to the Avaya Aura® voice switching platform. OCP connects to Chat, Email and SMS services.

Log files location

Unified Collaboration Model is deployed as one mandatory and three optional Service Archives (SVARs) using the System Manager deployment service. These are UCMService, ContactCentreService, and UCMDataCollector SVARs.

To find UCM REST services log file and PU services log file go to the following folders:

```
/var/log/Avaya/service/UCMService/ or UCMDataCollector/ or ContactCentreService/
/var/log/Avaya/dcm/pu/UCMService/ or UCMDataCollector/ or ContactCentreService/
```

Tip:

These log files automatically roll over. It can be necessary to analyze several log files to find relevant information.

Note:

The following PU log files are located in the `/var/log/Avaya/dcm/pu/UCMService/` folder:

```
ucm-space-pu-x.log
ucm-space-pu-x.json.log
ucm-uc-pu-x.log
ucm-dc-adaptor-pu-x.log
ucm-oc-pu-x.log
```

UCM is a distributed component. Go through the cluster to find relevant nodes.

Note:

Physical units run with paired active and standby deployment. UCM PU log files do not report any run-time activity while in backup mode.

Common problems with Unified Collaboration Model

This section provides information on how to trace and debug common issues with Unified Collaboration Model (UCM).

Routing a call

The following procedure describes the flow of a call:

1. Provider creates a RouteCommand or ActiveRoutePointInteraction in UCMSpace. These objects are updated with the latest routing state during the routing process.
2. ContactCentreService monitors the RouteCommand or ActiveRoutePointInteraction and sends a `ROUTE_REQUEST` to Engagement Designer Worflows over the Avaya Breeze® platform Entity Framework (EF).
3. Engagement Designer Worflows identify an agent and sends an `OFFER` request to ContactCentreService which forwards this to the originating provider.
4. Provider routes the call and completes the original RouteCommand or ActiveRoutePointInteraction.

If there is an issue while routing a call, find the Work Request ID in the `ucm-space-pu.log` and `ucm-oc-pu.log` files. You can also check the `ucm-affadaptor-pu.log` file. To trace the issue, look for any cancelled requests or timeouts.

Tracing Work Request ID in UCM

To trace the Work Request ID in UCM, perform the following steps:

1. Find the Work Request ID for the call by identifying it in the log files. Look for the approximate call time and calling number.
2. Check all Avaya Oceana® Cluster 1 nodes to find a match in the `ucm-space-pu.log` file. The call events for a specific call are logged to the same PU instance.

Note:

A call typically has an associated WorkRequest object, a Contact object and an ExternalConversationInteraction object. If it is routed, the call can have one or more ConversationInteraction objects.

If there is an issue, look for changes in Contact and ConversationInteraction state. Check the timing of the **COMPLETE** state of these objects, and if it lines up with the actual call end.

Checking Resource Login Details

To check the Provider ID and Resource ID of the target resource, perform the following steps:

1. Use the Station ID if using a telset station, or the Agent ID if the agent uses a phoneset. If the resource is SMS, Chat or Email, use the Agent ID to resolve to the resource.

2. Check all Avaya Oceana® Cluster 1 nodes for a match of the Resource ID in the `ucm-space-pu.log` log file. The state events for a specific call are logged to the same PU instance for the lifetime of the resource.

If there is an issue with logging in to the resource, check the following:

1. The resource state, and if it matches the resource login and logout time.
2. Check the resource properties. For Voice resources, check that the **isAcquired** property is set.

Important:

An **UNKNOWN** state can indicate a provider connectivity problem.

Checking Agent Login Details

To check the Agent login ID, perform the following steps:

1. Find the agent's User ID as configured in Avaya Control Manager.
2. Search the `ucm-uc-pu.log` file for a match of the User ID.

If there is an issue, check the User state and if the latest state matches the Agent state shown on Avaya Workspaces. The state must match the expected resource availability.

Chapter 13: Troubleshooting Engagement Designer

Troubleshooting Engagement Designer

Avaya Engagement Designer (ED) is an Avaya Breeze® platform snap-in that enables customers to create Workflow Definitions that describe and perform business processes. A Workflow Definition comprises a series of connected events and tasks. The ED graphical user interface provides a palette of available events, tasks, decision gates and data that are dragged onto the canvas and linked to construct a Workflow Definition.

Log files location

Refer to the log files if there are issues with Avaya Engagement Designer. The following table describes the log files for troubleshooting ED and their location:

Log name	Location	Description
EngagementDesigner	`var/log/Avaya/services/EngagementDesigner/EngagementDesigner.log`	This log file at **FINE** level contains all the information received and sent by Avaya Engagement Designer. **Note:** If more than one version of ED is installed, all logs are stored in the same file. Each line in the log file identifies the version of ED used to produce the log.
EventingConnector	`/var/log/Avaya/services/EventingConnector/EventingConnector.log`	This log file at **FINEST** level contains all the information on the events.

You can use a publication ID to relate interactions between the `EngagementDesigner.log` file and the `EventingConnector.log` file. The same publication ID is highlighted in the following example of an event sent to ED through EventingConnector:

```
EventingConnector.log:

2018-01-23 16:54:44,653 [WebContainer : 2] EventingConnector FINEST -
EventingConnector-3.4.0.0.340003 - servlet context is /events
2018-01-23 16:54:44,653 [WebContainer : 2] EventingConnector FINEST -
EventingConnector-3.4.0.0.340003 - doPost ENTER
2018-01-23 16:54:44,656 [WebContainer : 2] EventingConnector FINEST
- EventingConnector-3.4.0.0.340003 - EventAckServlet: populateEventMetadata
```

```
metadata: EventMetaDataImpl [user=null, userAsMatched=null, serviceProfile=null,
correlationId=18, producerName=null, producerVersion=null, valueMap={},
isImmutable=false]
2018-01-23 16:54:44,656 [WebContainer : 2] EventingConnector
FINEST - EventingConnector-3.4.0.0.340003 - doPost
eventBodyPart=com.ibm.ws.webcontainer.srt.SRTServletRequestPart@8b25414e
2018-01-23 16:54:44,656 [WebContainer : 2] EventingConnector FINEST
- EventingConnector-3.4.0.0.340003 - doPost body : {"NewString1":"ABC",
"NewString2":"EFG", "NewString3":"HJK"}

2018-01-23 16:54:44,656 [WebContainer : 2] EventingConnector FINER -
EventingConnector-3.4.0.0.340003 - createEventProducer ENTER eventBody.length=62
2018-01-23 16:54:44,656 [WebContainer : 2] EventingConnector FINER -
EventingConnector-3.4.0.0.340003 - createEventingService ENTER
2018-01-23 16:54:44,656 [WebContainer : 2] EventingConnector FINEST -
EventingConnector-3.4.0.0.340003 - populateUserHandleAndDomain user=null
2018-01-23 16:54:44,656 [WebContainer : 2] EventingConnector
FINER - EventingConnector-3.4.0.0.340003 - publish
ENTER publication=PublicationImpl [family=EliFamily, type=EliType,
eventMetaData=EventMetaDataImpl [user=null, userAsMatched=null, serviceProfile=null,
correlationId=18, producerName=EventingConnector, producerVersion=3.4.0.0.340003,
valueMap={}, isImmutable=true], effectiveUser=null, userMinusDefaultDomain=null,
userHandle=null, userDomain=null, eventBody=<not shown>, eventVersion=1.0,
actualProducerName=EventingConnector, actualProducerVersion=3.4.0.0.340003,
publicationId=a1-EventingConnect-3.4.0.0.340003-e0a38e68-d678-40bd-a547-1a0cfa2b9b5d,
publicationTimestamp=1516744484656, metaDataBitSet=CeBitSet [val=0x6], valueCount=0]

EngagementDesigner.log:

2018-01-23 16:54:44,666 [WorkManager.DefaultWorkManager : 3] EngagementDesigner
INFO - EngagementDesigner-3.4.0.0.32008 - Received event:
EliFamily:EliType Payload: EventImpl [family=EliFamily, type=EliType,
payload=<not shown>, version=1.0, publicationId=a1-EventingConnect-3.4.0.0.340003-
e0a38e68-d678-40bd-a547-1a0cfa2b9b5d, subscriptionId=EngagementDesig-3.4.0.0.32008-
a07a3593a2bec8a323d5cb4438ec96d106abc000909a57307d33cc1f53c57137, consumerName=,
consumerVersion=, metadata=EventMetaDataImpl [user=null, userAsMatched=null,
serviceProfile=null, correlationId=18, producerName=EventingConnector,
producerVersion=3.4.0.0.340003, valueMap={}, isImmutable=true],
consumerPrivateData=<not shown>, style=ASYNC, publicationTimestamp=1516744484656]
```

Modify the log level for Avaya Engagement Designer snap-ins on the System Manager Avaya Breeze® platform Logging Configuration page. To turn the logs on to the **FINE** level, perform the following steps:

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Logging**.
2. From the **Service** drop-down list, select **EngagementDesigner**.
3. Set the Log Level to **FINE**.
4. Select Avaya Oceana® Cluster 1.
5. Click **Commit**.

Repeat the steps above to turn the logs on to the **FINEST** level.

Warning:

Changing log levels can impact the performance of Avaya software. You must change log levels only when Avaya support teams recommend the change to troubleshoot issues.

Common issues with Engagement Designer

This section describes common problems which can occur with Engagement Designer, and how to troubleshoot these issues.

Verifying the Engagement Designer Workflow Engine installation

To verify the ED Workflow Engine installation, perform the following steps:

1. Open Engagement Designer **Designer** console by entering the following URL in your web browser:

   `https:/<Cluster FQDN>/services/EngagementDesigner/index.html`

2. View the palette on the left to verify that the Engagement Designer snap-in is deployed properly along with the corresponding tasks. Ensure that the palette shows core ED task drawers such as **Events** and **Gateways**, and also shows Oceana task drawers such as **Oceana** and **WorkAssignment**.
3. Open the Engagement Designer **Admin** console by entering the following URL in your web browser:

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

4. Navigate to the **Instances** tab to check if the flows are kicked off.

   Note:

   Each time a Contact is created, a new flow is kicked off.

Other common issue related to Engagement Designer

The following table lists common problems that can occur with the Engagement Designer snap-in, and how to troubleshoot these issues:

Issue Description	Solution
Engagement Designer console cannot be accessed.	1. Check the DNS settings. 2. Check if the cluster is in **Accepting** state. 3. SSH to the node where Engagement Designer is deployed. 4. Run the following command: **`deploy_service -lv`** 5. Check the log files to identify exceptions.

Table continues…

Issue Description	Solution

Instances on Engagement Designer **Admin** console are not displayed.	1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
	2. On the Service Clusters tab, select Avaya Oceana® Cluster 1 and the **EngagementDesigner** service.
	3. Check if the **Completed instances to be deleted or not** attribute has a value of `true`.
	4. Check if ContactCenterService PU logs are available in the `/var/log/Avaya/dcm/pu/ContactCenterService/ucm-affadapter-pu*` folder on Avaya Oceana® Cluster 1, and if they include correct events.
	5. Ensure that the event `ROUTE_CONTACT_<Channel>` is triggered to the correct Engagement Designer URL. To verify, in the /var/log/Avaya/dcm/pu/ContactCenterService/ucm-affadapter-pu* log, ensure that logging similar to the following appears:
	`ROUTE_CONTACT_Channel`
	`...`
	`Sent request to [http://<ED Cluster IP>:<Port>/services/EventingConnector/events?affinity=<IP>]`

Properties do not open when **Tasks** are double-clicked in the Workflows.	Ensure that you are using the latest version of Chrome. Use Chrome 56 or later.
Engagement Designer workflow fails.	1. Open the Engagement Designer **Admin** console. 2. Click the **Instances** tab and open the failed instance. 3. Double-click the failed task to check the Input and Output. **Note:** The workflow can fail but on the **Instances** tab of the ED Admin console, the flow shows as **COMPLETED**. If the flow failed, "Error Handled" is set to true. You can filter failed workflows using the ED Admin console by searching for "true" in the **Advanced** search box.

Chapter 14: Troubleshooting Context Store

Troubleshooting Avaya Context Store

Avaya Context Store (Context Store) is an Avaya Breeze® platform snap-in that enables context-sensitive, real-time customer contact information to be updated from multiple sources and shared between the various components and touch points in the enterprise through which a customer passes.

For detailed information about troubleshooting Context Store see the *Avaya Context Store Snap-in Reference*document.

Log files location

Refer to the log files if there are issues with Context Store. The following table describes the log name and the location of the logs related to Context Store:

Log name	Location	Description
Context Store service logs	/var/log/Avaya/services/<ServiceName>/<ServiceName>.log	Logs related to Context Store services, such as Context Store Manager and Context Store Rest.
External Data Mart logs	/var/log/Avaya/dcm/pu/ContextStoreManager/ContextStoreManager-cs-edm-<x>.log	Logs related to the External Data Mart feature.
Event logs	/var/log/Avaya/services/event.log	Event logs raised by Context Store.
Data-grid logs	/var/log/Avaya/dcm/	Data-grid log stores the message in a grid view.
ASM logs	/var/log/Avaya/sm/asm.log /var/log/Avaya/sm/deploy.log	Platform logging, which provides information on problems that can be blocking services or service deployment.
Text logs	/var/log/Avaya/sm/TextLog_<date_time>.log	Platform logging which provides information on problems that can be blocking services.
Alarm log	/var/log/Avaya/breeze/alarms.log	Alarms raised by Context Store.

Verifying Context Store deployment and connection

This section describes how to verify successful Avaya Context Store deployment, its connection to External Data Mart, and how to troubleshoot common issues.

Verifying Context Store successful deployment

To verify Avaya Context Store deployment, create and retrieve test Contexts through the Context Store REST interface. Submit requests to the Cluster IP address or directly to the security module IP address of a server to verify that they are working as expected. The Cluster IP address sends round-robin requests to each available Context Store REST instance.

Important:

If you create Contexts without specified Context IDs with the short ID parameter set to **True**, the first 1 - 3 digits of the returned, auto-generated Context ID matches the last octet of the security module IP address of the server on which the Context was created. To verify that each of the servers is processing requests, send **Create** requests to the Cluster IP address. For example, set parameters in the following way:

```
URL: http://<IP_ADDRESS>/services/ContextStoreRest/cs/contexts/?shortid=true
Body: {"contextId":"","data":{"key1_name":"value1_data","key2name":"value2_data"}}
```

Submit test requests using either a REST client such as Postman (for Google Chrome) or the live API built-in to CS REST itself:

```
http://<IP_ADDRESS>/services/ContextStoreRest/
```

Note:

Sample Postman request collections are available to download from Avaya DevConnect for all Context Store REST operations and features.

Verifying Context Store successful connection to the External Data Mart

If you have access to the database, to verify Context Store connection to the External Data Mart, do the following:

1. Create a Context with the **`persistToEDM`** attribute set to `true`:

   ```
   {"contextId":"PersistedContext","persistToEDM":"true","data":
   {"key1_name":"value1_data"}
   ```

2. Run an SQL query to search the database for this Context:

```
select * from cs_operation where context_id = 'PersistedContext'
```

```
select * from CS_RESURRECT where context_id = 'PersistedContext'
```

If you cannot query the database directly, use the Context Store Query REST interface to verify that the Context has been written to the External Data Mart:

```
http://<IP_ADDRESS>/services/ContextStoreRest/edm/contexts/resurrect/PersistedRequest
```

Troubleshooting when Context Store cannot connect to the External Data Mart

You must configure the External Data Mart (EDM) database username and password attributes to insert and retrieve information from the EDM. If you configure the details incorrectly, Context Store

cannot connect to the EDM and the EDM Database Security Settings can lock the account. If this occurs, do the following:

1. Verify that the correct EDM database password attribute is set for the ContextStoreManager, ContextStoreQuery, and OceanaConfiguration SVARs.
2. Clear any cached login attempts from your EDM database.
3. Login to your EDM database as an administrator and unlock the EDM user account.
4. Reboot the Context Store Avaya Breeze® platform nodes and the Avaya Breeze® platform nodes deployed on Avaya Oceana® Cluster 1.

Troubleshooting problems with Data-Grid deployment

This section describes common problems which can occur with Data-Grid deployment, and how to troubleshoot these issues.

The configured deployment fails if the resources available in the cluster of Avaya Breeze® platform servers are not sufficient for it. Refer to the Context Store release notes for attribute values for each deployment.

Using your web browser, navigate to `https://<Oceana Cluster 1 IP address>/services/ContextStoreManager` to open the Context Store Manager homepage. The following error returned on the Context Store Manager homepage can indicate a Data-Grid deployment failure:

```
Error 503: Internal error Could not read statistics object, check
CSSpace settings. EDM PU deployment failed, check EDM settings, or
try accessing the homepage via load balancer IP or other node GEO PU
deployment failed, review GEO settings, or try accessing the homepage
via load balancer IP or other node.
```

If this occurs, check your configuration settings and the `/var/log/Avaya/services/ContextStoreManager` and `/var/log/Avaya/dcm/gs-esm-<X>.log` files for errors related to deployment.

Important:

The nodes must be shutdown at the same time to ensure that the Data-Grid is fully undeployed before the next deployment attempt takes place. Otherwise, the last node standing keeps the Data-Grid alive. In this case, the Data-Grid is not redeployed as the nodes have already started back up before the last standing shutdown.

The following lines in the CS Manager log file indicate a correct fresh start of the cluster:

```
grid.EsmGrid INFO - [M eployElasticSpace][T:null]. ContextStoreManagerSpace not found,
deploying...
grid.EsmGrid INFO - [M eployElasticPU][T:null]. ContextStoreSpace not found,
deploying...

grid.EsmGrid INFO - [M:deployStateless][T:null]. EDM-Mirror-Service is deployed with
status BROKEN.
Followed quickly by manager.AbstractPUManager INFO - [M:checkDeploymentStatus][T:null].
[EDM-Mirror-Service] is in status [INTACT] a few seconds later
```

If these messages do not appear in any CS Manager log files after restart, it indicates you have not restarted the cluster correctly. In this case, the following lines are present:

```
grid.EsmGrid INFO - [M eployElasticSpace][T:null]. space with name
ContextStoreManagerSpace is already deployed
grid.EsmGrid ERROR - [M:deployElasticPU][T:null]. space ContextStoreSpace is already
deployed.
```

Chapter 15: Troubleshooting Work Assignment

Troubleshooting Work Assignment

The Avaya Work Assignment Snap-in to Avaya Breeze® platform is an extensible, highly scalable, highly available and resilient next generation work distribution system that manages the assignment of work items to resources across the enterprise. The snap-in uses a single universal resource pool model and both attribute and analytics driven routing.

The following table describes the log name and location of the logs related to Work Assignment:

Log name	Location	Description
Processing unit logs	`/var/log/Avaya/dcm/pu/`	The Work Assignment processing unit logs. For example: • `wa-impu-*.log` • `wa-metrics-agent-pu-*.log` • `wa-wae-pu-*.json.log` • `wa-wae-pu-*.log`
Work Assignment services log	`/var/log/Avaya/services/`*`ServiceName`*`/`*`ServiceName`*`.log`	Logs related to Work Assignment services.
Event logs	`/var/log/Avaya/services/event.log`	Logs related to the Work Assignment alarms and events.
Platform logs	`/var/log/Avaya/sm/asm.log`	Service logs for Avaya Breeze® platform that are related to the Snap-in deployment.
Text logs	`/var/log/Avaya/sm/TextLog_date_time.log`	Provides information on problems that can be blocking services.
DCM logs	`/var/log/Avaya/dcm/dcm.log`	DCM Console output log file.
Data grid logs	`/var/log/Avaya/dcm/gs/`	Location of data grid log files.

Note:

If you enter an invalid attribute or priority in the async request, the match update fails and the error is logged in the Callback server log file.

Debugging Work Assignment issues

Perform the following steps to debug problems related to Work Assignment:

1. In your web browser, enter the following URL:

   ```
   http://<Oceana Cluster 1 IP address>/services/WAIMRestService/wa/imrest/v2/matches/check
   ```

2. Ensure that the following text appears in your browser:

   ```
   Work Assignment Service has started
   IMPU is alive
   State of WAE Service: ACTIVE.UCAM and UCA spaces are active
   ```

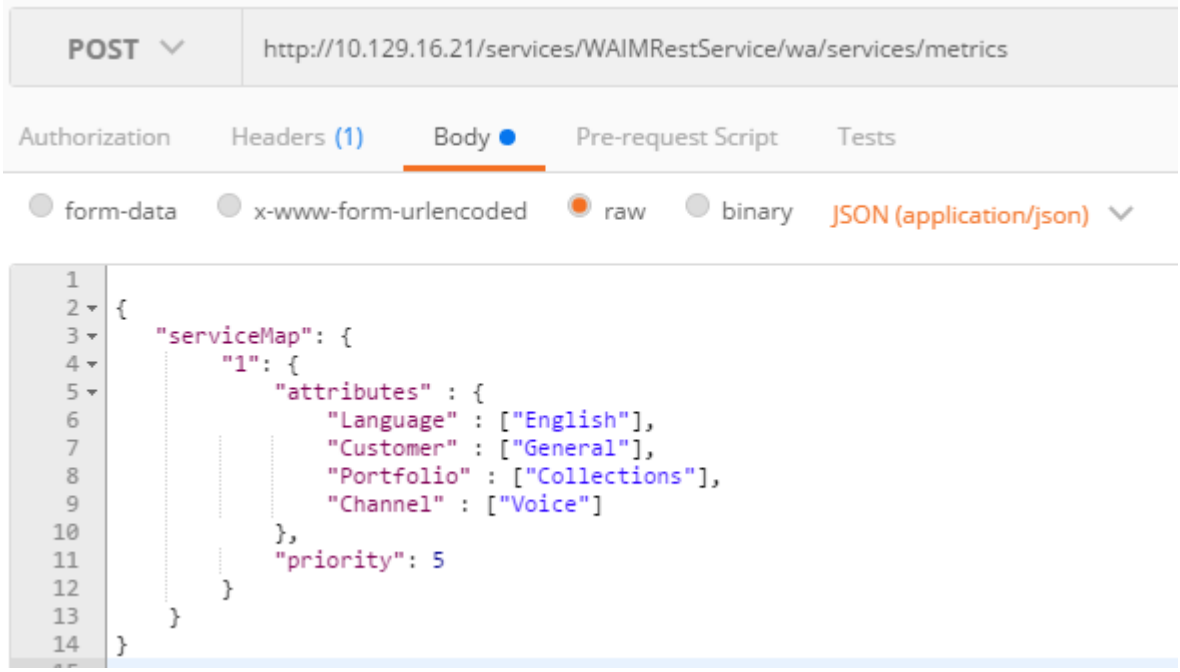
3. Run a metrics request from POSTMAN. For example:

   Note:

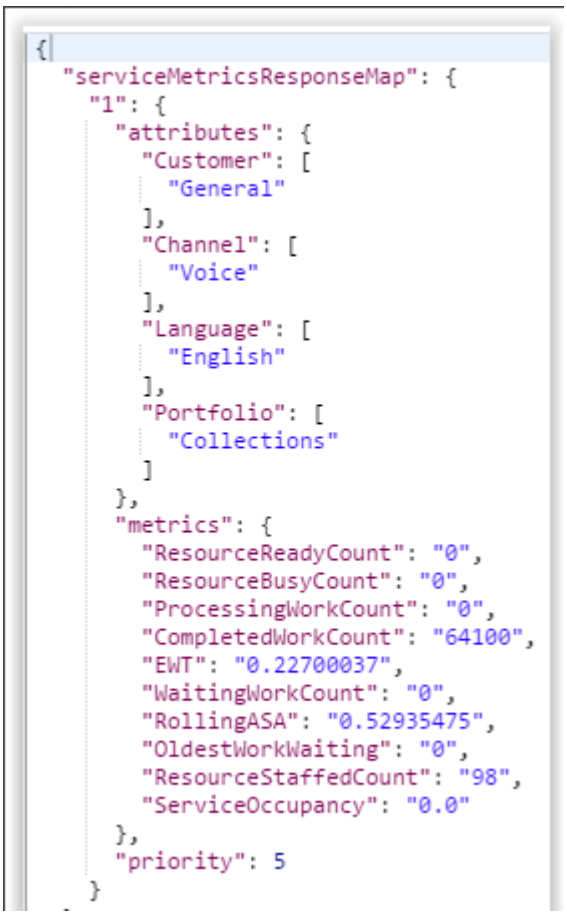
   POSTMAN is a plugin for Google Chrome and is a 3rd party tool. You must download the tool into your local machine before using it.

   Note:

   POSTMAN chrome is deprecated from the link : https://chrome.google.com/webstore/detail/postman/fhbjgbiflinjbdggehcddcbncdddomop?hl=en. You can download the Postman Native apps for MacOS, Windows, and Linux at http://www.getpostman.com/downloads

4. The response from Work Assignment is successful if it includes the following data and can be used to check if there are agents available with these attributes:



5. Perform a WA query for available agents for a particular work ID:

The response shows all of the resources for this work ID.

Checking that the UCM REST Service is enabled

To check if the UCM REST Service is enabled perform the following steps:

1. In your web browser, enter the following URL:

   `http://<Oceana Cluster 1 IP address>/services/OpenUCM/ucm/rp/check`

2. Ensure that the following text appears in your browser:

   ```
   UCM RP REST Service is up
   ```

Checking WA is receiving Agent status changes

To check if WA is receiving Agent status changes perform the following steps:

1. Retrieve the most recent `wa-wae-pu-*.log` file from the following location:

   ```
   /var/log/Avaya/dcm/pu/WAManagerService/
   ```

2. Log in as an Agent and go RDY.

Ensure that messages in the `wa-wae-pu-*.log` are similar to the following:

```
yyyy-mm-dd hh:mm:ss,855 [wa-engine-thread    ] INFO   WaeEventMapper                -
[.2.0.0.480_1][M:processInboundEvent(ResourceStateEvent)][T:]. Resource state change
for ResourceStateEvent
[triggeringWorkId=00002000521474393284,state=NOT_READY,nativeResourceId=6006800,sourceId
=e_CM_1,channel=Voice,accountId=6006800,workLimit=1,activeWorkCount=0] successfully
processed

yyyy-mm-dd hh:mm:ss,576 [tion-pool-1-thread-1] INFO   ResourceListener              -
[.2.0.0.480_1][M:eventHappened][T:agent5]. Event: state=READY, agent5 resource = {}

yyyy-mm-dd hh:mm:ss,577 [wa-engine-thread    ] WARN   EventProcessor               -
[.2.0.0.480_1][M:updateResourceAgent][T:]. resourceId 4 Unable to find resource for
```

```
account Account[id=agent5_OCP ChatRoutableAddressOCP ChatWITH_RP,nativeAccId=agent5_OCP
ChatRoutableAddress,sourceName=OCP
Chat,accountName=<null>,deploymentType=WITH_RP,raapId=agent5_OCP
ChatRoutableAddress_OCP Chat]

yyyy-mm-dd hh:mm:ss,577 [wa-engine-thread    ] INFO   WaeEventMapper                -
[.2.0.0.480_1][M:processInboundEvent(ResourceStateEvent)][T:]. Resource state change
for ResourceStateEvent
[triggeringWorkId=<null>,state=READY,nativeResourceId=6006800,sourceId=e_CM_1,channel=Vo
ice,accountId=6006800,workLimit=1,activeWorkCount=0] successfully processed 2016-09-20
12:45:50,906 [tion-pool-1-thread-5] INFO   ResourceListener               -
[.2.0.0.480_1][M:eventHappened][T:agent5]. Event: state=READY, agent5 resource = {}
```

Chapter 16: Troubleshooting Unified Agent Controller

Troubleshooting Unified Agent Controller

Unified Agent Controller (UAC) is one of the snap-in services installed on Avaya Oceana® Cluster 2 (UAC Cluster) along with Oceana Monitor Service, Avaya Mobile Communications, and BotConnector. It is available as a Service Archive (SVAR) file and downloadable from Avaya PLDS.

The UAC Cluster provides high availability and scaling by distributing the services across multiple Avaya Breeze® platform nodes. With this distribution of services, the system achieves overall throughput and avoids interruption in the event of failure. Clients access the services through a Cluster IP address that supports high availability.

Log files location

Refer to the log files if there are issues with the Unified Agent Controller:

Log name	Location
`SVAR log` file	`/var/log/Avaya/services/UnifiedAgentController`
`PU log` file	`/var/log/Avaya/dcm/pu/UnifiedAgentController`

Chapter 17: Troubleshooting Avaya Workspaces for Avaya Oceana®

Avaya Workspaces does not load real-time data

Cause

Cross-Origin Resource Sharing (CORS) is not configured appropriately.

Solution

Check the deployment spreadsheet to see if following fields are configured:

config:orca-streams-data-publisher:virtualService:allowOriginsSingleExact

config:orca-streams-rest:virtualService:allowOriginsSingleExact

The field value should be taken from the origin field of the HTTP request to the orca-streams-rest and orca-streams-data-publisher. For example, Go to **WORKSPACES** > **Chrome** > **Developer tools** > **Network** > **XHR** > **any orca-streams-rest URL**.

For more information on configuring the deployment spreadsheet, see *Preparing the deployment spreadsheet* section in *Deploying Avaya Analytics™ for Avaya Oceana®* guide.

Chapter 18: Troubleshooting Avaya Control Manager

Adding a WebLM server

About this task

Before you begin

Configure a WebLM server.

Procedure

1. On the Control Manager web portal, navigate to **Configuration** > **Licenses** > **WebLM Server**.
2. Click **Add**.
3. In the **WebLM Address** field, enter the WebLM address.
4. To check the connectivity, click **Test**.
5. Click **Save**.

Troubleshooting Avaya Control Manager

Avaya Control Manager runs on a dedicated Windows server. It provides the web based administration interface for the Avaya Oceana®. It interacts mainly with the UCA component of the solution and relies heavily on the UCA REST interface functioning correctly.

Log files location

Control Manager contains a number of Windows services which must be running for Control Manager to function correctly. Each of these services can generate their own log files. Logging is on by default and the log level can be configured in Control Manager.

To generate a log file, perform the following steps:

1. Log on to Avaya Control Manager and navigate to the **Configuration Portal** and then to the **Services** tile.
2. Select one of the services and click on the **Local Log Settings** tab.

3. The log files are generated in a `Logs` folder under the service executable location, for example:

```
C:\Program Files (x86)\Avaya\Avaya Control Manager 7.1.3.0\Services\ACCCM UCA Proxy Service\Logs
```

There are a number of other log files created which you can use when troubleshooting Control Manager issues:

1. Log files can be generated by various Control Manager web portals. They are stored under the portal folders on the Avaya Control Manager server. For example, `C:\Program Files (x86)\Avaya\Avaya Control Manager 7.1.3.0\Web\ACCCM WEB\Logs`.
2. Internet Information Services (IIS) generates log files by tracking the requests that hit the web server. These requests are recorded in the following folder: `C:\inetpub\logs\LogFiles\W3SVC1`.
3. Windows Event Viewer records events on the server.

Common issues with Avaya Control Manager

The following table describes common issues which can occur with Avaya Control Manager, and how to troubleshoot these issues.

Name of the issue	Troubleshooting
Avaya Control Manager Services Fail to start.	To confirm that Avaya Control Manager Services are running, perform the following steps: 1. Confirm that the Avaya Control Manager services share a common location. By default, the Avaya Control Manager services are part of the Avaya Control Manager standard locations. 2. If any of the services have been moved to new locations, verify that all services share this location. Otherwise, the services cannot communicate with each other. 3. Verify that the SQL server database service is running.
Error is displayed when clicking on the **Providers** tab.	To add a Provider to an Oceana server, the Oceana instance must first be associated with a Location in Avaya Control Manager. If you do not add an Oceana instance to a location, an error occurs when you click the **Providers** tab on the **Server Details** tile.

Chapter 19: Troubleshooting OmniChannel Provider

Troubleshooting OmniChannel Provider

Avaya Oceana® uses Unified Collaboration Model (UCM) to send third-party call operations to the OmniChannel Provider (OCP) and Call Server Connector (CSC). The OCP connects to chat, email and SMS services.

The UCM snap-in is a real-time object data model that abstracts the work being processed in a system. UCM represents the current state of work and resources within the system.

Log files location

The following tables lists the log files for troubleshooting OCP and their locations:

Table 1: Chat log files

Log name	Location
Agent Controller service log files	`/var/log/Avaya/services/AgentControllerService`
Customer Controller PU log files	`/var/log/Avaya/dcm/pu/CustomerControllerService`
Customer Controller service log files	`/var/log/Avaya/services/CustomerControllerService`

Table 2: Email log files

Log name	Location
Email service PU log files	`/var/log/Avaya/dcm/pu/EmailService`

Table 3: SMS log files

Log name	Location
Messaging service log files	`/var/log/Avaya/services/MessagingService`
SMS vendor log files	`/var/log/Avaya/services/SMSVendorSnapin`

Table 4: ORCRestService log files

Log name	Location
ORCRestService service log files	`/var/log/Avaya/services/ORCRestService`
ORCRestService PU log files	`/var/log/Avaya/dcm/pu/ORCRestService`

Table 5: OCP admin/OCMT log files

Log name	Location
OCMT logs	`%Appdata%\Avaya\Logs\OCMT_1.log`
OCP Admin logs	`%Appdata%\Avaya\Logs\Admin_1.log`

Adjusting Logging and Trace Levels

To adjust logging and trace levels perform the following steps:

1. Log on to System Manager.
2. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Logging**.
3. Select the Cluster on which OCP is installed.
4. Select a type of log file needed, for example, select **CustomerControllerService** from the **Service** drop-down list.
5. Select **FINE** from the **Log Level** menu to enable debug-level logging.
6. Select **ALL** from the **Log Level** menu to enable trace-level logging.
7. Click **Commit** to save the changes.

Warning:

Changing log levels can impact the performance of Avaya software. You must change log levels only when Avaya support teams recommend the change to troubleshoot issues.

Troubleshooting OmniChannel Provider database performance issues

Condition

The performance of search queries, such as Avaya Oceana® Data Viewer or Avaya Workspaces for Avaya Oceana® search queries, is slow.

Cause

The number of contacts and customers in the OmniChannel Provider (OCP) database exceeds the supported limits. This issue also occurs if the number of contacts per customer exceeds supported limits.

Solution

1. Ensure that the number of contacts and customers in the OCP database is within supported limits.
2. Ensure that the number of contacts per customer is within supported limits.

   Use the Oceana Data Management utility to clean up the OCP database if the number of contacts per customer exceeds supported limits. For more information about supported limits of contacts per customer, see Statistics home page on page 61.
3. If the issue persists, review the performance of the disk on which the OCP database is mounted.

Troubleshooting Chat

Examining UCA attributes, user profiles and other features

To debug Unified Collaboration Administration, go to each of the following URLs twice in your browser, once for each node:

```
http://<Oceana Cluster 1 IP address>/services/UCAStoreService/uca/attributes
http://<Oceana Cluster 1 IP address>/services/UCAStoreService/uca/userprofiles
```

If UCA is active, attributes configured by Avaya Control Manager appear in the response. For example, if the attribute **Language.English** has been configured, **{"category":{"name":"Language"},"value":"English"}** appears in the response.

Checking certificates in the keystore

To check which certificates are included in the keystore, do the following:

1. SSH into the Avaya Breeze® platform node.
2. Switch to the root user by entering the following command:

   su sroot
3. Run the following command to obtain the keystore password:

   usr/java/default/bin/java -cp/opt/Avaya/aus/db/cdb.sh:/opt/jboss/lib/jbosssx.jar com.avaya.asm.mgmt.cli.JBossFilePasswordDecoder/opt/jboss/server/mgmt/conf/tm/keystore.password
4. Run the following command to see certificates in the keystore:

   keytool -list -keystore/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/config/cells/${NODENAME}/trust.jks -storepass${PASSWORD} –v

   Note:

   The keystore password appears as **${PASSWORD}** in this example.

Important:

${NODENAME} generally obeys the following syntax:

${hostname}Node${nodeNumber}.

Common issues

The following table lists common issues related to Chat, and how to troubleshoot these issues:

Issue Description	Cause	Action
The Web UI reports a connection error when opening a chat with an unencrypted WebSocket.	The Web UI server has not been whitelisted in the OmniChannel Admin as an approved origin for the chat.	To check if UCA is active, open the OmniChannel Admin and ensure that the External Web Server Domain entry is not blank. For testing, set this to * to allow connections from all origins.
The Web UI opens a chat, but a connection error occurs. The CustomerController PU log files show that there was a new connection from the localhost 127.0.0.1.	This issue occurs when there are multiple snapshot versions of the same PU in Gigaspaces, and it does not distinguish between them.	Perform the following steps: 1. Uninstall the CustomerControllerService SVAR. 2. Remove any instance of CustomerControllerWeb from the `/var/avaya/dcm/gigaspace/deploy` folder on the OCP node. 3. Reinstall the CustomerControllerService.
Automated chat fails. The BotConnector log files show errors similar to: `API [/v1/startchatsession] failed for chatId [<not available>]. Error code: [CHAT_ENGINE_REQUEST_ERROR] Error Message [Automated chat returned error while starting the session]`	This issue can be caused by interference from old TLS certificates.	Remove all the old certificates and re-install them.
The chat is opened, and there is an immediate internal error message. The CustomerController PU log files show that there is a NullPointerException while creating the contact in ORC.	This issue occurs when ORC is not able to access Context Store to create a work request ID.	Reinstall the Context Store Rest service and try again.

Table continues…

Issue Description	Cause	Action
Chats routes to an agent, but agent cannot answer them. The AgentController log files show the message similar to the following: `Contact UUID does not exist in database.`	This issue can occur when the AgentController points at the wrong Caché database.	Ensure that the correct cluster is selected from the drop-down list in the ContactCenterService attributes. If you change the setting, verify in the logs that the value has been updated.

Troubleshooting Email

Common issues

The following table lists common issues related to Email, and how to troubleshoot these issues:

Issue Description	Cause	Action
New emails not being processed. The Email Manager logs show the following error: `SERVICE IMPACTING EVENT`	The number of new emails is exceeding the **Max Active Emails** setting configured in the Omnichannel Administration Utility.	Increase the **Max Active Emails** setting, or reduce the number of new emails in the backlog.
Chat transcripts are not being sent to the customer.	Chat headers are not defined.	1. Ensure that the correct email address is entered on the Web interface. 2. Ensure that there is a default chat transcript header configured in the OCP Administration tool.

Table continues…

Issue Description	Cause	Action
Connecting to Microsoft Exchange results in failed authentication. The Email Manager logs show the following error: `javax.mail.AuthenticationFailedException`	POP3/IMAP can occasionally stop working on Microsoft Exchange. Check for username issues, and if Exchange expects the username to be the email address.	1. Access the Exchange server using SSH or Telnet. 2. Open the Exchange Management Shell, and then run the following commands: • `Get-ServerComponentstate -Identity odl-exchange` • `Set-ServerComponentState -Identity odl-exchange -Component PopProxy -Requester HealthAPI -State Active` • `Set-ServerComponentState -Identity odl-exchange -Component ImapProxy -Requester HealthAPI -State Active` • `Get-ServerComponentstate -Identity odl-exchange` 3. Ensure that the mailbox name is configured correctly in the OCP Administration tool.

Table continues…

Issue Description	Cause	Action

When using Gmail, certificate-related errors appear similar to the following:
`unable to find valid certification path to requested target`
When you connect to Office365 it displays the following error:
`java.net.SocketTimeoutException`
	The certificate has expired, or the full certificate chain was not imported.
	This issues occurs because there is no access to the following locations from:
	• outlook.office365.com
	• smtp.office365.com
	• graph.microsoft.com
		1. Export and save the CA certificate for your Gmail account.
		2. Import the certificate:
		• On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
		• Select the OCP node and select **Manage Trusted Certificates** from the **More Actions** drop-down list.
		• Click **Add**.
		• Click **Choose File** and browse to the location of the CA certificate.
		• Click **Open**.
		• Click **Retrieve Certificate**.
		• Click **Commit**.
		• Restart the OCP node.
		Disable CRL and then reboot all the clusters.

Table continues…

Issue Description	Cause	Action
Incoming or outgoing emails stop working with the following error: `No issuer certificate for certificate in certification path found.`	The mail provider issued a new certificate because the old one expired or is close to expiring.	1. Identify the IP address of your mail server. 2. Import the certificate using TLS: • On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**. • Select the OCP node and select **Manage Trusted Certificates** from the **More Actions** drop-down list. • Click **Add**. • Click **Import using TLS**. • In the **IP Address** field, add the IP address of the mail server. • In the **Port** field, add the port number of the email protocol the mail server uses. • Click **Retrieve Certificate**. • Check the expiry date and compare with the current certificates to verify the certificate is newly issued. • Click **Commit**. • Restart the OCP node.

Table continues…

Issue Description	Cause	Action
New incoming email contacts are not coming from configured Microsoft Office365 mailbox.	Microsoft Office365 mail servers cannot be reached.	Ensure that: 1. Office365 mail servers can be reached from the network where Avaya Oceana® OCP Avaya Breeze® platform nodes exist. 2. Mail servers configured using OCP Administration tool have correct encryption option and port number set as mentioned in the Microsoft Office365 documentation. 3. Install Office365 certificates, including root and intermediate root certificates on each Avaya Oceana® OCP cluster Avaya Breeze® platform node. You must reboot the OCP cluster or re-install EmailService after installing certificates.
O365 mailbox may produce the `java.security.cert.CRLException: Empty input` error in logs or in inbox statistics.	O365 fails to get the OAuth access token because CRL is enabled.	1. Log on to Avaya Aura® System Manager. 2. Navigate to **Global** > **Revocation Configuration**. 3. In the **Certificate Revocation Validation** field, select `NONE`. 4. Click **Commit**. 5. Reboot all servers.
An attempt to get access token fails. The following error displays: `401: Unauthorized`	• Either the user's credentials are not valid or the user is not authorized to get access tokens. • OAuth certificate expired.	Ensure that the correct details are configured in the OCP Administration tool: • OAuth credentials: Secret or Certificate store details • OAuth certificate terms.

Table continues…

Issue Description	Cause	Action
An attempt to get access token fails. The following error displays: `400: Bad request`	• The user's credentials are not valid. • The token access request has incorrect parameters. • OAuth certificate expired.	Ensure that you correctly configure the following details in the OCP Administration tool: • OAuth Client ID • Scopes • Token uri • OAuth certificate terms.
An attempt to get access token fails.	Issues other than the two mentioned above are logged in the following error report: `[M:executeGetAccessTokenRequest][T:null]. Failed to get access token`	Check and resolve the issues in: `[M:executeGetAccessTokenRequest][T:null]. Failed to get access token`
If you use MS graph to connect to MS Office365, you may find that the outbound email which you sent, is in the draft folder.	The outbound email gets sent to the destination address. MS Office365 has mail duplication issue.	Check the draft folder and manually clean old draft emails, that is, emails older than three or more days.
You cannot delete an email template through Control Manager.	The email template is still assigned to a partition. You cannot delete the template unless you unassign the template from the partition.	1. On the Control Manager web portal, navigate to the **Groups** tile, or search for `Groups` in the global search. 2. In the **Entity Assignment** tab, check the `Email Template Group` nodes in the listed partitions for the email template that you want to delete. 3. Click **Unassign** for the email template to unassign the template from the partition.
Avaya Oceana® cannot send email if the **TO** field contains incorrect or unresolvable Microsoft Office365 mailbox addresses. The Email Manager logs show the following error: `com.sun.mail.smtp.SMTPAddressFailedException: 550 5.7.54 SMTP; Unable to relay recipient in non-accepted domain`	Exchange Server is not configured to handle incorrect addresses.	1. On your Exchange Server, navigate to Exchange admin center. 2. In the navigation pane, click **mail flow**. 3. Click **accepted domains**. 4. To accept all domains, add `*` to the domains list. You can also add specific domains to the list.

Table continues…

Issue Description	Cause	Action

The following exception message displays in the EmailService processing unit (PU) logs, indicating that EmailService cannot connect to a mailbox:
`_javax.mail.MessagingException: Connect failed`
`at com.sun.mail.pop3.POP3Store.protocolConnect(POP3Store.java:219)`
`at javax.mail.Service.connect(Service.java:366)`
`at com.avaya.ocp.emailcommon.mail.hostaccess.services.MailStore.performOpen(MailStore.java:538)`
`at com.avaya.ocp.emailcommon.mail.hostaccess.services.MailStore.open(MailStore.java:396)`
`at com.avaya.ocp.emailcommon.mail.hostaccess.threadpool.WorkerThread.executeRetrieve(WorkerThread.java:194)`
`at com.avaya.ocp.emailcommon.mail.hostaccess.threadpool.WorkerThread.executeRequest(WorkerThread.java:157)`
`at com.avaya.ocp.emailcommon.mail.hostaccess.threadpool.WorkerThread.run(WorkerThread.java:108)`
`Caused by: javax.net.ssl.SSLHandshakeException: Remote host closed connection during handshake`
`at sun.security.ssl.SSLSocketImpl.readRecord(SSLSocketImpl.java:994)`
`at sun.security.ssl.SSLSocketImpl.performInitialHandshake(SSLSocketImpl.java:1367)`
`at sun.security.ssl.SSLSocketImpl.startHandshake(SSLSocketImpl.java:1395)`
`at sun.security.ssl.SSLSocketImpl.startHandshake(SSLSocke`
	This connection attempt fails when you set an incorrect TLS version on the **Services** tab. The correct version is TLS 1.2.	1. Click the **Services** tab in Cluster Editor.
		2. In the Assigned Services section, select **TLS 1.2** in the **Select TLS Version for Selected Snap-ins** list.

Issue Description	Cause	Action
tImpl.java:1379) at com.sun.mail.util.SocketFetcher.configureSSLSocket(SocketFetcher.java:626) at com.sun.mail.util.SocketFetcher.createSocket(SocketFetcher.java:400)		

Debugging EmailService PU logs

The EmailService processing unit logs provides information indicating whether the email address of the distribution group is set for each outbound email.

The following information is available in the EmailService PU log:

```
2020-08-06 12:12:20.400+0100 [I: SendMail-1:
c.a.o.m.m.o.s.s.SMTPSender] M:createMessage][T:null]. Using group email
address[OceanaGroup@avaya.com] as sender address
```

When you configure **Send as group**, but the email address of the distribution Group is not retrieved from database, an error is logged in the EmailService PU logs and mailbox's email address is used.

The following error is logged in the EmailService PU log:

```
2020-08-06 12:12:20.400+0100 [E:
SendMail-1: c.a.o.m.m.o.OutboundMailManager][M: toSMTPConfiguration]
[T:OceanaMailbox@avaya.com]. Send as group is enabled but group email
address is null for some reason. Using Inbox email address instead
```

When the mailbox does not have a proper permission to send as distribution group, an error is logged in EmailService PU logs and is written into database for display on the Statistics page of the OCPDataViewer.

Troubleshooting mounted read-only cache mirrored database

In Avaya Oceana® with intersystems cache mirroring enabled, if the primary database is read-only or mounted read-only, MountedR, and you want to mount the Primary database as Read-Write, then you must shut down the Standby Omnichannel database server. You must also disable cache mirroring on the primary Omnichannel database server.

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

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

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

2. On the Cache Management Portal login page, do the following:
   a. In the **User Name** field, type `_admin`.
   b. In the **Password** field, type `Oceana16`.
   c. Click **LOGIN**.
3. On Cache Management Portal, click **System Administration** > **Configuration** > **Mirror Settings** > **Edit Mirror** > **Remove Mirror Configuration**.
4. On the Remove Mirror Configuration page, click **Clear JoinMirror Flag**.
5. On the server, right-click the Cache icon on the toolbar and click **Stop Cache**.
6. Click **Restart**.
7. On Cache Management Portal, click **System Administration** > **Configuration** > **Mirror Settings** > **Edit Mirror** > **Remove Mirror Configuration**.

   After removing the Cache Mirroring configuration, you must take a backup of the database on the primary server, so that you can restore.

Setting expiry for username in CacheIntersystems database

About this task

Use this procedure to set the expiry date for `username` in the CacheIntersystems database.

Procedure

1. Navigate to **System** > **Security Management Portal** > **Users** > **General tab**.
2. In the **Expiration Date** field, enter the expiry date in the `yyyy-mm-dd` format.

Oceana Data Management Tool shows validation error on legit network drive path when making a backup of Omnichannel Database

Cause

1. Incorrectly entered file name or network path for backup file.
2. The backup path entered is already open somewhere else (e.g., in Windows explorer)

Solution 1

Correct the path or backup file name

Solution 2

For Windows NT 4.0, only a single set of user credentials can be used for a single server name. This issue displays the following error:

System error 1219 has occurred. Multiple connections to a server or shared resource by the same user, using more than one user name, are not allowed. Disconnect all previous connections to the server or shared resource and try again

1. Use domain name instead of IP address in network path or otherwise.
2. Restart Workstation service and try again.

Chapter 20: Troubleshooting the AEP sample application

Troubleshooting the AEP sample application

This section describes how to debug and troubleshoot the Avaya Experience Portal (AEP) sample application in Avaya Oceana®.

Checking settings in AEP

To check settings in AEP, do the following:

1. Log on to the AEP web console.
2. Select **Real-Time Monitoring** > **System Monitor**.
3. On the **ExperiencePortal Details** tab, under **Server Name**, click **LocalMPP**.
4. Under **Miscellaneous**, click **Service Menu**.
5. In the left pane, click **TTS**. Check the data in the fields.
6. In the left pane, click **Speech Servers**. Check the data in the fields.
7. In the left pane, click **Diagnostics**, and then click **Check connections to servers**. Verify that all connections are successful.

Testing Nuance server

To test the Nuance server connectivity and functions, do the following:

1. Create an application using the default MPP `intro.vxml`, for example:

   `http://<AAEP IP address>/mpp/misc/avptestapp/intro.vxml`
2. To test TTS, ring the Launch number and follow the commands to enter digits and numbers.

Common issues with the AEP sample application

This section describes common problems which can occur with the AAEP sample application, and how to troubleshoot these issues.

Sample application starting and stopping immediately

Condition:

If you dial the sample application launch number, the application appears to answer the call, then drops it immediately.

Solution:

To troubleshoot this problem do the following:

1. On the Session Manager, use traceSM to confirm that the call to the application launch number is getting to AEP.
2. Ensure that the Nuance server NSS service and NRS service are running.

```
login as: ec2-user
Authenticating with public key "imported-openssh-key"
Last login: Wed Nov  2 12:26:23 2016 from 192.168.150.150
[ec2-user@ip-192-168-119-244 ~]$ ls
aa7_key.pem  ASR_TTS_09JAN17.lic  ASR_TTS_License.lic  awssm1.crt  awssmgr2.crt  NUANCE  nuanceServices.zip
[ec2-user@ip-192-168-119-244 ~]$ service NSSservice status
NSS is running
[ec2-user@ip-192-168-119-244 ~]$ service NRSservice status
Usage: /etc/init.d/NRSservice {start|stop|restart}
[ec2-user@ip-192-168-119-244 ~]$
```

3. If these services are not running, start them, or reboot the Nuance server. Confirm the services have started.

Sample application not running with SCE Runtime Exception

Condition:

Invalid runtime license error appears in the log file of the application. The log file is located in the following folder:

`/opt/AppServer/apache-tomcat-8.0.32/webapps/WorkAssignmentSelfService-3.2.2.1.6.1/data/log/trace.log`

The following lines in the log file show the error:

```
dd/mm/yyyy hh:mm:ss:000 ERROR - 068BA7C743F1636718140911FA69C3D1:/
WorkAssignmentSelfService : channel:unknown | Error processing request
EXCEPTION>
com.avaya.sce.runtimecommon.SCERuntimeException: Invalid runtime license
at com.avaya.sce.runtimecommon.SCESession.throwRTException(SCESession.java:2554) at
com.avaya.sce.runtime.Entry.handleRequest(Entry.java:268)
...
at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:615) at
org.apache.tomcat.util.threads.TaskThread$WrappingRunnable.run(TaskThread.java:61) at
java.lang.Thread.run(Thread.java:745)
dd/mm/yyyy hh:mm:ss:000 DEBUG - 068BA7C743F1636718140911FA69C3D1:/
WorkAssignmentSerlfService : License: Use the license server url in VPMS instead -
null
```

Solution:

Rename this configuration file `\\Tomcat folder\lib\ddconfig.xml`. For example, rename the file to `ddconfig.old` and restart the Tomcat application server. A new `ddconfig.xml` file is created with a blank **invalidlicensetimer** value.

Sample application stopping and dropping the Launch Number call

Condition:

The sample AAEP application immediately stops and drops the Launch number call.

Solution:

1. Check the sample application log file, located in the following folder:

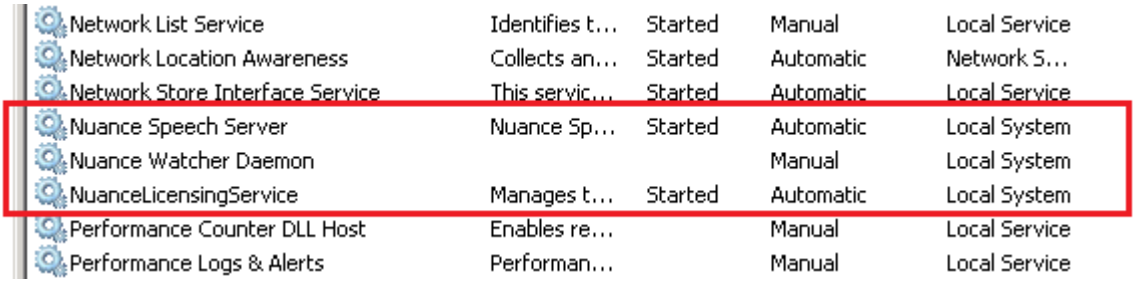
   ```
   /opt/AppServer/apache-tomcat-8.0.32/webapps/
   WorkAssignmentSelfService-3.2.2.1.6.1/data/log/trace.log
   ```

2. Restart the Nuance server and services if the log file stops at the following line:

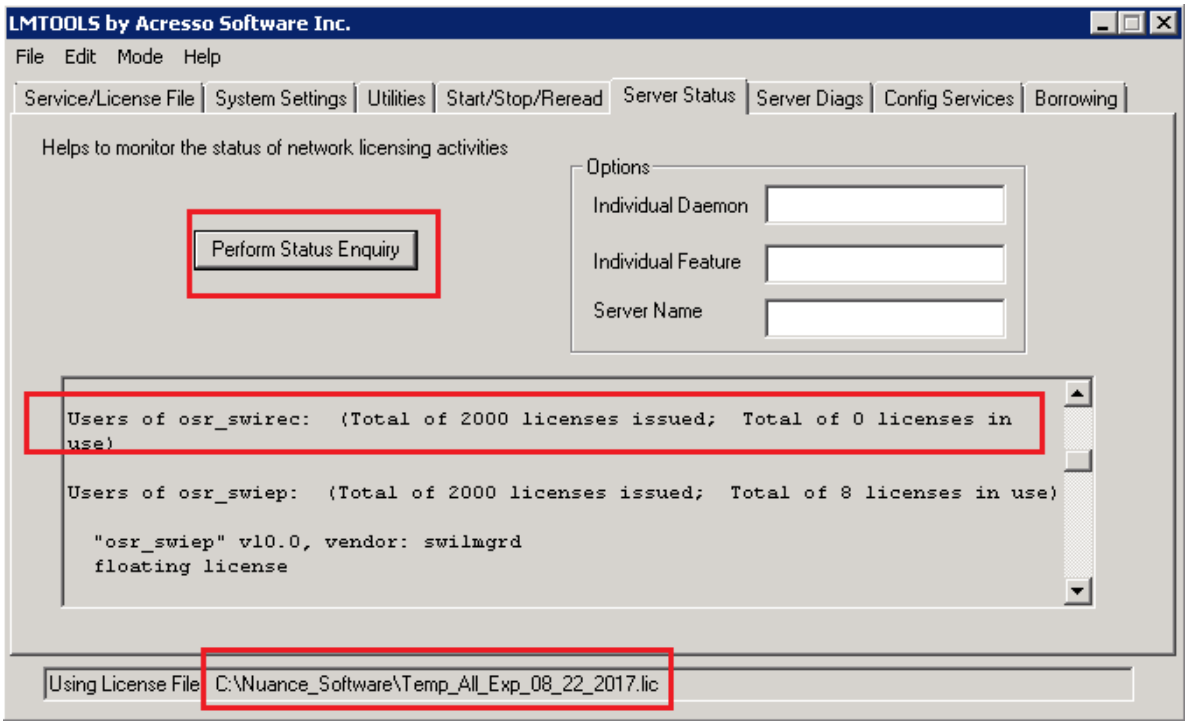
   ```
   dd/mm/yyyy hh:mm:ss:000 DEBUG - 27343971AC23532B435EC93DF6FA02E2:/
   WorkAssignmentSelfService : ServiceMap Category: [Location]
   ```

To restart the Nuance server and services do the following:

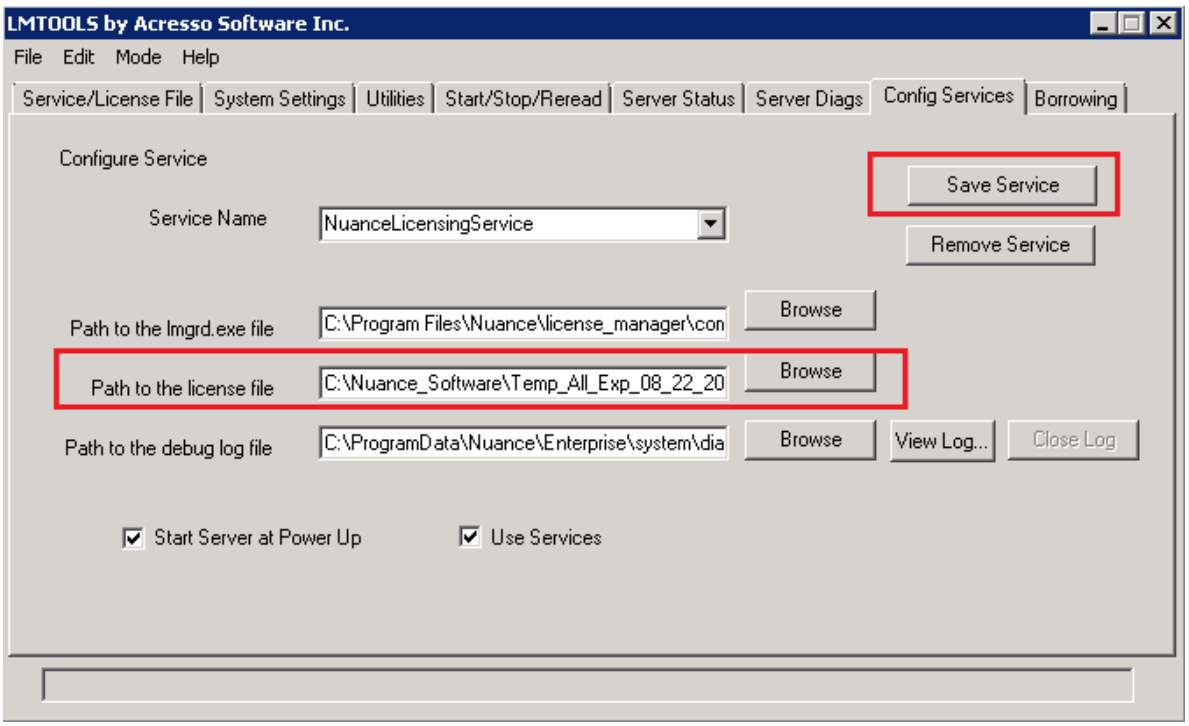
1. Log on to the Nuance TTS server.
2. Restart the Nuance services: Nuance Speech Server, Nuance Watcher Daemon, and NuanceLicensingService.



3. Ensure that the correct license file is configured, still valid, and is being used.



4. Load the updated license file if needed, click **Save Service**, and restart the Nuance services.


LMTOOLS by Acresso Software Inc.
File Edit Mode Help
Service/License File
System Settings
Utilities
Start/Stop/Reread
Server Status
Server Diags
Config Services
Borrowing
Configure Service
Service Name
NuanceLicensingService
Save Service
Remove Service
Path to the lmgrd.exe file
C:\Program Files\Nuance\license_manager\con
Browse
Path to the license file
C:\Nuance_Software\Temp_All_Exp_08_22_20
Browse
Path to the debug log file
C:\ProgramData\Nuance\Enterprise\system\dia
Browse
View Log...
Close Log
Start Server at Power Up
Use Services

Chapter 21: Troubleshooting the Avaya Breeze® platform

Troubleshooting Avaya Breeze® platform

This section describes how to troubleshoot issues related to Avaya Breeze® platform in an Avaya Oceana®. For more detailed information about troubleshooting Avaya Breeze® platform see *Maintaining and Troubleshooting* ***Avaya Breeze®***, available on the Avaya Support website at http://support.avaya.com.

Listing the Oceana services deployed on Avaya Breeze® platform

Use the following command to list all the services installed on each Avaya Breeze® platform node:

`deploy_service -lv`

The following example shows services installed on Avaya Oceana® Cluster 1, Node 1:

```
[cust@WFEDP42118V ~]$ deploy_service -lv
load: + deploy: + run: + car: + EngagementDesigner-3.4.0.0.31033
load: + deploy: + run: + car: = OceanaCoreDataService-3.4.0.0.806019
load: + deploy: + run: + car: = OmniCenterProvisioningCollector-3.4.0.0.806019
load: + deploy: + run: + car: = WorkAssignmentManagerService-3.4.0.0.806019
load: + deploy: + run: + car: = UCMService-3.4.0.0.806019
load: + deploy: + run: + car: = OpenUCM-3.4.0.0.806019
load: + deploy: + run: + car: = UCAStoreService-3.4.0.0.806019
load: + deploy: + run: + car: = WAIMRestService-3.4.0.0.806019
load: + deploy: + run: + car: = ContextStoreManager-3.4.0.0.806019
load: + deploy: + run: + car: + EventingConnector-3.4.0.0.340003
load: + deploy: + run: + car: = CallServerConnector-3.4.0.0.806019
load: + deploy: + run: + car: = UCMDataCollector-3.4.0.0.806019
load: + deploy: + run: + car: = ContextStoreRest-3.4.0.0.806019
load: + deploy: + run: + car: + CallEventControl-3.4.0.0.340003
load: + deploy: + run: + car: = OceanaMonitorService-3.4.0.0.806019
load: + deploy: + run: + car: = ContextStoreQuery-3.4.0.0.806019
load: + deploy: + run: + car: = CustomerManagement-3.4.0.0.806019
load: + deploy: + run: + car: = ContactCenterService-3.4.0.0.806019
```

The following table describes the service states:

State value	Meaning
+	good
N	no
=	not-applicable/unknown

Table continues…

State value	Meaning
load	The file is loaded onto the server in `/var/avaya/aus_svars`.
deploy	Sub-components are deployed into containers and directories.
run	Sub-components are initialized in their respective containers.
car	SIP sub-components are registered with CAR.

Listing the Oceana SVARs installed on Avaya Breeze® platform

Each Avaya Breeze® platform node uses an IBM WebSphere application server to host various Oceana SVARs (service archive files). The SVAR services provide the basic functional blocks of the Avaya Oceana®.

Use the following command to list the components installed in the WebSphere container on each Avaya Breeze® platform node:

`was app lsi`

Most of the Oceana SVARs have a component installed in WebSphere. There are additional components shown with this command that are not part of Oceana SVARs.

The following example shows components installed in the WebSphere container on Avaya Oceana® Cluster 1, Node 1:

```
[cust@WFEDP42118V ~]$ was app lsi
/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/installedApps/Node01Cell
total 0
drwxr-xr-x. 4 wsuser susers 67 Nov 17 11:42 CallEventControl-3.4.0.0.340003.ear
drwxr-xr-x. 4 wsuser susers 65 Nov 30 09:04 CallServerConnector-3.4.0.0.806019.ear
drwxr-xr-x. 4 wsuser susers 61 Nov 30 09:12 ContactCenterService-3.4.0.0.806019.ear
drwxr-xr-x. 4 wsuser susers 61 Nov 30 09:10 ContextStoreManager-3.4.0.0.806019.ear
drwxr-xr-x. 4 wsuser susers 65 Nov 30 09:14 ContextStoreQuery-3.4.0.0.806019.ear
drwxr-xr-x. 4 wsuser susers 58 Nov 30 09:08 ContextStoreRest-3.4.0.0.806019.ear
drwxr-xr-x. 4 wsuser susers 69 Nov 30 09:03 CustomerManagement-3.4.0.0.806019.ear
drwxr-xr-x. 5 wsuser susers 61 Nov 27 14:30 EngagementDesigner-3.4.0.0.31033.ear
drwxr-xr-x. 4 wsuser susers 68 Nov 17 11:43 EventingConnector-3.4.0.0.340003.ear
drwxr-xr-x. 4 wsuser susers 75 Nov 30 09:05 OceanaCoreDataService-3.4.0.0.806019.ear
drwxr-xr-x. 4 wsuser susers 73 Nov 30 09:05 OceanaMonitorService-3.4.0.0.806019.ear
drwxr-xr-x. 4 wsuser susers 62 Nov 30 09:04
OmniCenterProvisioningCollector-3.4.0.0.806019.ear
drwxr-xr-x. 4 wsuser susers 59 Nov 30 09:15 OpenUCM-3.4.0.0.806019.ear
drwxr-xr-x. 4 wsuser susers 46 Nov 17 11:19 perfServletApp.ear
drwxr-xr-x. 4 wsuser susers 54 Nov 17 11:27 platformApp.ear
drwxr-xr-x. 4 wsuser susers 60 Nov 30 09:07 UCAStoreService-3.4.0.0.806019.ear
drwxr-xr-x. 4 wsuser susers 69 Nov 30 09:17 UCMDataCollector-3.4.0.0.806019.ear
drwxr-xr-x. 4 wsuser susers 62 Nov 30 09:09 UCMService-3.4.0.0.806019.ear
drwxr-xr-x. 4 wsuser susers 61 Nov 30 09:18 WAIMRestService-3.4.0.0.806019.ear
drwxr-xr-x. 4 wsuser susers 61 Nov 30 09:16
WorkAssignmentManagerService-3.4.0.0.806019.ear
```

Listing the GigaSpaces processes running on Avaya Breeze® platform

Use the following command to list the GigaSpaces processes running on an Avaya Breeze® platform node:

`gs jvmp`

The following example shows GigaSpaces processes running on Avaya Oceana® Cluster 1, Node 1:

```
[cust@WFEDP42118V ~]$ gs jvmp
 1357   GSC   512m   224th +perf cs-space-3.4.0.0.806019
 1362   GSC   512m   253th +perf cs-space-3.4.0.0.806019
 1374   GSC   512m   190th +perf cs-space-3.4.0.0.806019
 1646   GSC  1024m   164th +perf ucm-dc-space-pu-3.4.0.0.806019
 1647   GSC  1024m   252th +perf ucm-dc-space-pu-3.4.0.0.806019
 2943   GSC   256m   148th +perf uca-store-edm-3.4.0.0.806019
 3530   GSA   128m   139th +perf
 3880    LH   384m   200th +perf
 3884   GSM   128m   151th +perf
 6650   GSC   256m   159th +perf ucm-dc-adaptor-pu-3.4.0.0.806019
 9323   GSC   512m   229th +perf ucm-space-pu-3.4.0.0.806019
 9326   GSC   512m   166th +perf ucm-space-pu-3.4.0.0.806019
 9698   GSC   200m   143th +perf CECommonSpace
11451   GSC   512m   195th +perf cs-space-3.4.0.0.806019
11453   GSC   512m   194th +perf cs-space-3.4.0.0.806019
11456   GSC   512m   216th +perf cs-space-3.4.0.0.806019
12013   GSC   128m   168th +perf ManagerSpace
12257   GSC  1024m   155th +perf cs-edm
12981   GSC  1800m   263th +perf csc-3.4.0.0.806019
19187   GSC   512m   364th +perf wa-impu-3.4.0.0.806019
19190   GSC   512m   290th +perf wa-impu-3.4.0.0.806019
22656   GSC   512m   215th +perf ucm-uc-pu-3.4.0.0.806019
24108   GSC   512m   266th +perf ucm-oc-pu-3.4.0.0.806019
25318   GSC   256m   166th +perf ucm-affadapter-pu-3.4.0.0.806019
25325   GSC   256m   196th +perf ucm-affadapter-pu-3.4.0.0.806019
25330   GSC   256m   164th +perf ucm-affadapter-pu-3.4.0.0.806019
28235   GSC  2560m   261th +perf wa-wae-pu-3.4.0.0.806019
28265   GSC   200m   148th +perf CECommonSpace
29966   GSC   512m   224th +perf cc-service-pu-3.4.0.0.806019
30140   GSC   512m   225th +perf wa-metrics-agent-pu-3.4.0.0.806019
30472   GSC   896m   153th +perf uca-store-space-3.4.0.0.806019
```

Chapter 22: Troubleshooting Avaya Mobile Communications

Troubleshooting Avaya Mobile Communications

Avaya Mobile Communications is an Avaya Breeze® platform snap-in service. Avaya Mobile Communications integrates Avaya Aura Web Gateway (AAWG) and Avaya Session Border Controller (ASBC) with the Avaya Oceana® to deliver Avaya WebRTC Connect features.

Troubleshooting client communication with AvayaMobileCommunications snap-in service

The following table lists common issues seen in client communication between the Avaya Mobile Communications and the AAWG server, and how to troubleshoot these issues:

Issue Description	Cause	Action
The following error message is displayed in your web browser: "ERR_INSECURE_RESPONSE".	The browser does not trust the server.	1. Right-click the URL and open it in a new tab to trust the server. This is a temporary solution. 2. Install the required trust certificates on the client PC running the browser to solve the issue permanently. For more information, see *Deploying Avaya Oceana®*.
XMLHttpRequest cannot load the following URL: `https://1.2.3.4/services/AvayaMobileCommunications/sessions`. The `https://1.2.3.4:8443` origin is not allowed to be accessed. The response from the server has HTTP status code 404.	The `Access-Control-Allow-Origin` header function is absent on the requested resource.	1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **HTTP Security** > **HTTP CORS**. 2. Check if **Allow Cross-origin Resource Sharing for all** is enabled for Avaya Oceana® Cluster 2.

Table continues…

Issue Description	Cause	Action
The following error message is displayed: "`Request to AMC failed`".	The configuration of the Avaya Oceana® Cluster 2 IP address is incorrect.	On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**. Check if the Avaya Oceana® Cluster 2 IP address is configured correctly.

Troubleshooting Media Devices

The following table shows how to allow permission for media devices on different platforms. For more information about deploying sample reference clients on each of these platforms, see *Deploying Avaya Oceana®*.

Platform	Action
JavaScript	1. Ensure a microphone is connected to the PC. 2. Check if permissions are allowed on your web browser. 3. In the drop-down menu that appears in the search bar of your web browser when you make a call, select **Allow**. 4. Click **Confirm**. This allows the site to use your camera and microphone.
iOS	Allow app permissions for microphone on your device: 1. Go to **Settings > Apps** and scroll down the list of apps. 2. Tap an app you want to see the permissions for. 3. Enable or disable media device permissions for the app.
Android	At install time, the device prompts you to allow app permissions for microphone at install time. After the app is installed, perform the following steps to allow app permissions for microphone: 1. Go to **Settings > Apps**. 2. Tap an app you want to see the permissions for. 3. Select **Permissions** from the drop-down menu. 4. Enable or disable media device permissions for the app.

Troubleshooting SSL certificate errors

The following table shows common SSL certificate issues on different platforms:

Platform	Issue description
JavaScript	The following error is displayed in the web console: "`ERR_INSECURE_RESPONSE`".
iOS	The following error is displayed in the logs: "`The Certificate for this server is invalid`".
Android	The following error is displayed in the logs: "`SSLHandshakeException`".

To troubleshoot SSL certificate issues, perform the following steps:

1. Install the SSL certificate for the endpoint you are making the request to.
2. If the endpoint uses self-signed certificates, trust the Certificate Authority (CA) that created the SSL certificate.

Chapter 23: Troubleshooting Avaya WebRTC Connect

Troubleshooting for Avaya WebRTC Connect agents

Failed to activate an agent

Solution

1. In the browser, do the following:
   a. Accept the certificates for the Avaya Aura® Device Services URL:

      `https://<Avaya Aura Device Services_FQDN>/acs/resources`

   b. Accept the certificates for the Avaya Aura® Web Gateway URL:

      `https://<Avaya Aura Web Gateway_FQDN>/csa/resources/tenants/default`

   c. Refresh the page and retry agent activation.
2. To accept the certificates, do the following:
   a. Clear the browser cache and repeat Step 1.
   b. **(Optional)** Restart the browser as a guest user and go to the Avaya Workspaces URL.
3. Go to the following URL for Avaya Aura® Device Services automatic configuration:

   `https://<Avaya Aura Device Services_FQDN>:8443/acs/resources/configurations`

   You can view an output similar to the following:

```
## File Generation Notes
## Avaya Dynamic Configuration Service does not recognize User-Agent -
SET SIPSECURE 0
SET SIPENABLED 1
SET SIPDOMAIN oceana.com
SET SIPUSERNAME 8832018
SET SIPHA1 b459b107705c7277cf936acb3b476d5c
SET ACSPORT 8843
SET ACSSECURE 1
SET ACSENABLED 1
SET ACSSSO 1
SET SIP_CONTROLLER_LIST 10.133.34.202:5061;transport=TLS
SET ACSSRVR 10.133.34.204
SET SIPPROXYSRVR 10.133.34.202
SET SIPPORT 5061
```

```
SET LOCKED_PREFERENCES "SIPSECURE,SIPENABLED,SIPDOMAIN,SIPUSERNAME,SIPl
SET OBSCURE_PREFERENCES ""
```

4. **(Optional)** If you do not receive an output with the user configuration details, do the following:
    a. Go to **Start** > **Administrative tools** > **Active Directory** and check if the email field is populated.
    b. **(Optional)** If the email field is empty, specify the user email in the `username@domain` format.
    c. Ensure that the user is added to the group that is used for publishing in Avaya Aura® Device Services.
    d. On the Avaya Aura® Device Services web interface, click **Server Connections** > **LDAP Configurations**.
    e. On the LDAP Configurations page, ensure that the **Role Filter** and **Role Attribute ID** fields are populated.
    f. In **User Role**, type the LDAP group name.

    For more information about the LDAP group name configuration, see *Administering Avaya Aura® Device Services*.
    g. On the Avaya Aura® Device Services web interface, click **Dynamic Configuration** > **Configuration** > **Group**.
    h. On the Group page, configure the following parameters:

    `COMM_ADDR_HANDLE_TYPE = Avaya SIP`

    `COMM_ADDR_HANDLE_LENGTH = <Length of your SIP Extensions>`
    i. Publish the LDAP group configuration.
5. Check the connection between Avaya Control Manager and UCAStoreService.
6. Check the CTI-Link from Communication Manager to the Application Enablement Services server.
7. Check whether as common certificate along with the Certificate Authority (CA) certificate is installed on the client machine.
8. Check whether Avaya Aura® Web Gateway and Avaya Aura® Device Services FQDNs are correctly configured in the UnifiedAgentController attributes.

Authentication failures

Solution

1. Check the connection between Avaya Aura® System Manager and LDAP server.
2. Check the LDAP synchronization on the User Management page in System Manager.
3. Check LDAP certificates on all Avaya Breeze® platform nodes.
4. Check authorization certificates update at the cluster level.
5. Ensure that a common certificate is installed on Avaya Breeze® platform nodes, Avaya Aura® Web Gateway, and Avaya Aura® Device Services.

6. Check whether the common certificates are expired.

Avaya Workspaces displays an error in registering the agent

Solution

1. Check the Avaya Aura® Device Services and LDAP connection on Avaya Aura® Device Services.
2. Check the Avaya Aura® Web Gateway and LDAP connection on Avaya Aura® Web Gateway.
3. Check whether a SIP handle is assigned to the System Manager user.
4. Check whether the LDAP users are assigned to the same group configured and published on Avaya Aura® Device Services.
5. Check whether the **Third-party call control** is set as `Avaya` on the Station page of the SIP station assigned to the Avaya Workspaces agent.

Avaya Workspaces displays the Provider not found error

Solution

1. Check the connection between the Call Server Connector (CSC) service and Application Enablement Services server.
2. Check the connection between Avaya Control Manager and UCAStoreService.
3. Check the CTI-Link from Communication Manager to the Application Enablement Services server.
4. Create a new agent in Avaya Control Manager.
5. Restart the Unified Agent Controller (UAC) cluster.
6. Redeploy the UAC cluster.

Cannot change agent states in Avaya Workspaces

Condition

Agent retains the Reconnecting state on Avaya Workspaces.

Solution

1. Close the existing TSAPI sessions on Application Enablement Services (AES).
2. After sessions are recreated, restart AES.
3. Reboot AES.
4. Ensure that the **Date/Time** value is the same on AES, CM, and nodes.
5. Check the CTI-Link from Communication Manager to the AES server, unlink the link, and add it again.
6. Check the connection between the Call Server Connector (CSC) service and AES server.
7. Restart the AES TSAPI and DMCC services.

8. Reboot the cluster.

Authorization error on Workspaces

Condition

Avaya Workspaces displays the following error:

```
Unable to contact the authentication server. Please try again, and if
the problem persists please contact your system administrator.
```

Solution

1. Add the AD certificates again on each node.
2. Restart the cluster.
3. Reinstall Authorization Service.

Unable to contact the authentication server on Workspaces

Solution

1. Ensure that the LDAP password is not reset.
2. On the System Manager web interface, click **Users** > **Directory Synchronization** and check the LDAP connection.
3. To Reinstall the LDAP certificate on the Session Manager and all the nodes, do the following:
    a. On the System Manager web interface, click **Services** > **Inventory** > **Manage Elements**.
    b. On the Manage Elements page, select the check box for one of the nodes of the proposed cluster.
    c. Click **More actions** > **Manage Trusted Certificates**.
    d. On the Manage Trusted Certificates page, click **Add**.
    e. On the Add Trusted Certificate page, do the following:
        a. Click **Import using TLS**.
        b. In the **IP address** field, enter the IP address of your LDAP server.
        c. In the **Port** field, enter the port number of your LDAP server.
        d. Click **Retrieve Certificate**.
        e. Click **Commit**.

Communication package error on Avaya Workspaces

Solution

1. Restart the Unified Agent Controller (UAC) cluster.
2. **(Optional)** If restarting the cluster does not solve the issue, redeploy the UAC cluster.

Error 404 on Workspaces

Solution

1. Go to **Logs of Authorization**.
2. Ensure that the log file shows the following error:

```
java.lang.IllegalArgumentException: Service AuthorizationService-3.7.0.0.370008
cannot be found on cluster
at
com.avaya.zephyr.platform.dao.AusServiceLevelTLSVersionDAO.getServiceLevelTLSVersi
onForMyCluster(AusServiceLevelTLSVersionDAO.java:228)
at
com.avaya.collaboration.ssl.util.SSLUtilityHelper.getClusterTLSVersion(SSLUtilityH
elper.java:61)
at
com.avaya.collaboration.ssl.util.SSLUtilityImpl.getClusterTLSVersion(SSLUtilityImp
l.java:405)
at
com.avaya.collaboration.ssl.util.SSLUtilityImpl.createSSLContext(SSLUtilityImpl.ja
va:85)
at
com.avaya.collaboration.ssl.util.SSLUtilityFactoryImpl.createSSLContext(SSLUtility
FactoryImpl.java:25)
at
com.avaya.collaboration.ssl.util.SSLUtilityFactory.createSSLContext(SSLUtilityFact
ory.java:104)
at
com.avaya.zephyr.services.production.AuthorizationService.startup.StartupServlet.i
nitializeHttpClient(StartupServlet.java:169)
at
com.avaya.zephyr.services.production.AuthorizationService.startup.StartupServlet.l
ambda$initializeHttpClient$0(StartupServlet.java:186)
at
com.avaya.zephyr.services.production.AuthorizationService.startup.StartupServlet$
$Lambda$50.0000000022C48410.run(Unknown Source)
at java.util.concurrent.Executors$RunnableAdapter.call(Executors.java:522)
at java.util.concurrent.FutureTask.run(FutureTask.java:277)
at
java.util.concurrent.ScheduledThreadPoolExecutor$ScheduledFutureTask.access$201(Sc
heduledThreadPoolExecutor.java:191)
at
java.util.concurrent.ScheduledThreadPoolExecutor$ScheduledFutureTask.run(Scheduled
ThreadPoolExecutor.java:304)
at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1160)
at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:635
at java.lang.Thread.run(Thread.java:811)
```

3. Log in to System Manager.
4. On the System Manager web interface, click **Elements** > Avaya Breeze® > **Cluster Administration**.
5. Select the cluster.
6. Click **Certificate Management**.
7. Update or install an Identity Certificate.

Video disabled by default Workspaces agent

Solution

1. Log in to Communication Manager.
2. Set the signaling group to **1**.
3. Set **Direct IP-IP Audio Connections** to `y`.

Troubleshooting for Avaya WebRTC Connect customers

Video calls do not work with the Avaya Aura® Web Gateway Reference Client

Solution

1. On the System Manager web interface, check the Avaya Aura® Web Gateway and Avaya Media Server licenses.
2. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

   `https://<AMS_EM_FQDN>:8443/emlogin/`
3. Click **System Configuration** > **Server Profile** > **General Settings**.
4. Select the **Firewall NAT Tunneling Media Processor** and **Video Media Processor** check boxes.
5. Click **Save**.

Avaya Aura® Web Gateway auth token error

Solution

1. Log on to the Avaya Aura® Web Gateway with your SSH credentials.
2. Navigate to `/opt/Avaya/CallSignalingAgent/version/mss/8.0.1-4_8.0.26/telportal/webapps`.
3. Rename the token generation file from `service.undeploy` to `generationservice.war`.
4. Rename the `devclient.undeploy` file to `devclient.war`.
5. To restart the Avaya Aura® Web Gateway, run the following command:

   `svc csa restart`

Unable to make a call from iOS

Condition

Your iOS device is unable to recognize the `.pem` file after the file is exported from System Manager. It also displays the following error:

```
Token Request Error. The certificate for this server is invalid.
You might be connecting to a server that is pretending to
be "pusntzd205.apac.avaya.com" which could put your confidential
information at risk.
```

Solution

Change the extension of the `.pem` file to `.crt`.

Note:

The proposed solution is for the iPhone 6s, version 13.4.1.

AMC issue on the Reference Client

Solution

Perform the configuration as described in the Avaya Knowledge Base article:

https://kb.avaya.com/kb/index?page=content&id=SOLN315270&actp=SEARCH&actp=search&viewlocale=en_US&searchid=1583237276733

Reference Client fails to create an AMC session

Solution

Restart the cluster.

Application Enablement Services and Call Server Connector service connections fail

Condition

Device, Media and Call Control (DMCC) connection, connecting Application Enablement Services (AES) and Call Server Connector service is not displayed.

Solution

Need to mention the same voice provider id on Call Server Connector attributes and restarting CSC service resolved it

1. Match the Voice Provider ID with Avaya Control Manager (ACM).
2. Add the same Voice Provider ID for Call Server Connector (CSC) attributes.
3. Restart CSC.

Video icon gets disabled for Workspaces agent after answering the video call

Condition

There is no video stream from agent after answering the video call.

Solution

Enable video configurations on Communication Manager, AAWG-AMS and Breeze-AMS as follows.

Task	Description
Configuring media servers for Web Video	See *Deploying Avaya Oceana®*.
Configuring an IP codec set for Video	
Configuring the signaling group for Web Video	
Configuring customer options	
Configuring an IP network region	

Workspaces agent enters a Not Ready state while answering the calls on Chrome browser

Condition

Workspaces agent is entering in to a Not-Ready state while answering the calls on a Chrome browser.

Chrome browser settings for 86+ versions.

Solution

Update the Chrome browser settings for 86+ versions.

Disable the following parameter in the agent's browser mDNS:

#temporary-unexpire-flags-m85

UAC status is not INTACT

Solution

Uninstall and reinstall the UAC service.

Announcement issues

Solutions

1. From Media Processing in AMS associated with, remove the `Workflows` folder.
2. Add the `Workflows` folder on AMS again and upload it to Announcements.

Issues with ACM

Condition

- Unable to create a user on Avaya Control Manager.

  Synchronization between Avaya Control Manager and Communication Manager does not work.
- Enabling video for the Avaya Control Manager user results in the following error: `Operation unsuccessful`.

Solutions

- Ensure that while creating an Avaya Control Manager user, you did not choose an existing Avaya Control Manager agent.
- For synchronization issues between Avaya Control Manager and Communication Manager, try to synchronize one entity at a time.

  Ensure that the entities exist on Communication Manager.
- For the issue with enabling video, do the following:
  1. Save the user configuration with audio-only.
  2. Select the **Video** check box and save it again.
- Ensure that the SIP extension that you assigned to the Avaya Control Manager user is synchronized with Avaya Control Manager.

  You can also run a general Avaya Control Manager synchronization to resolve such issues.

Media not going through Session Border Controller

Solution

Check whether Avaya Aura® Web Gateway has the **Enable port for remote access** attribute enabled for handling the media for external users.

Chapter 24: Troubleshooting BotConnector

Troubleshooting BotConnector

BotConnector is an Avaya Breeze® platform snap-in service installed on Avaya Oceana® Cluster 2. It provides communication with the Avaya Automated Chat system. For more detailed information about Avaya Automated Chat system, refer to the Avaya Oceana® documentation suite. For more information about troubleshooting BotConnector, see *Avaya BotConnector Snap-in Developer's and API Reference* document on the Avaya Support site.

Log files location

The following table lists the log files for troubleshooting the Avaya Breeze® platform BotConnector snap-in and their location:

Log name	Location	Description
Service installation and deployment logs	`/var/log/Avaya/sm/deploy.log`	This log file validates the snap-in service installation and deployment logs.
Service logs	`/var/log/Avaya/services/BotConnector/BotConnector.log`	This log file validates the snap-in service logs.
Alarm logs	`/var/log/Avaya/breeze/alarms.log`	This log file validates the snap-in alarm logs.
BotConnector service logs	`/var/log/Avaya/services/BotConnector/BotConnector.log`	This log file contains log messages specific to BotConnector, such as loading of adaptors, incoming REST requests, errors while processing requests, and any alarms or events generated by the service.

Chapter 25: Troubleshooting Avaya CRMGateway

Avaya CRMGateway snap-in log files

The following table describes the log files for troubleshooting the Avaya CRMGateway snap-in:

Log name	Location	Description
Service installation/ deployment logs	`/var/log/Avaya/sm/asm.log` `/var/log/Avaya/sm/TextLog_<TimeStamp>.log`	The Avaya CRMGateway snap-in deployment logs.

Service logs	`/var/log/Avaya/services/CRMGateway/CRMGateway.log`
	Centralized Logging
	`/var/log/Avaya/services/CRMGateway/CRMGateway_json.log`
		The Avaya CRMGateway snap-in logs that contain log messages such as loading of adapter, incoming REST requests, errors while processing requests, and any alarms or events generated by the service.
		Note:
		To view centralized logs, you must enable the Avaya CRMGateway log level to Finest.

Alarm logs	`/var/log/Avaya/breeze/alarms.log`	The Avaya CRMGateway snap-in alarm logs.

Changing log levels

About this task

Use the following procedure to set the log level on Avaya Breeze® .

Warning:

Changing log levels can impact the performance of Avaya software. You must change log levels only when Avaya support teams recommend the change to troubleshoot issues.

Procedure

1. On the System Manager web console, go to **Elements** > **Avaya Breeze®** > **Configuration** > **Logging**.

   System Manager displays the Logging page.

2. On the Logging page, do the following:
   a. From the **Cluster** drop-down list, select the required CRMGateway cluster.
   b. From the **Service** drop-down list, select the **CRMGateway** service.
   c. From **Log Level** drop-down list, select the required option.
3. Click **Set Log Level**.

Common issues with Avaya CRMGateway snap-in

The following table lists common problems that can occur with the Avaya CRMGateway snap-in and how to troubleshoot these issues:

Issue description	Solution
`Unable to reinitialize adapter, currently no adapter instance`	Verify the configuration on System Manager and switch the adapter on and off.
`Unable to start CRMGateway snap-in`	Verify configuration from System Manager.
`CRMGateway components are non functional. Adapter type <type> is non-functional.`	Indicates that the adapters configured are in inactive state. Verify configuration of adapters.
`Unable to stop CRMGateway snap-in`	Verify configuration from System Manager.

Managing alarms and events

About this task

Avaya CRMGateway snap-in generates alarms whenever an error occurs. Use this procedure to view, search, configure, acknowledge, and clear the alarms from the System Manager web console.

For more information on how to resolve alarms and events, see the *Avaya Oceana® Alarms* document on the Avaya Support site.

Procedure

1. To view the alarms do the following:

   On the System Manager web console, and click **Services** > **Events** > **Alarms**.

The Alarming page displays the Alarm list.

2. To change the status of the alarms after acknowledging the alarm logs, do the following:
   a. On the System Manager web console, click **Services** > **Events** > **Alarms**.
   b. Click the check box of the alarm based on the Host IP address of the Avaya Breeze® server on which the Avaya CRMGateway snap-in is deployed.
   c. Click **Change Status** > **Acknowledged**.

      The status of the selected alarm changes to `Acknowledged`.
3. To change the status of alarms after clearing the logs, do the following:
   a. On the System Manager web console, navigate to **Services** > **Events** > **Alarms**.
   b. Click the check box of the alarm based on the Host IP address of the Avaya Breeze® platform server on which the Avaya CRMGateway snap-in is deployed.
   c. Click **Change Status** > **Cleared**.

      The status of the selected alarm changes to `Cleared`.
4. To view the event logs, do the following:

   On the System Manager web console, click **Services** > **Events** > **Logs** > **Log Viewer**.

   The Logging page displays the Log list.

Chapter 26: Troubleshooting ZangSmsConnector

ZangSmsConnector log files

The following table describes the log files for troubleshooting the ZangSmsConnector snap-in.

Log name	Location	Description
Service installation/deployment logs	`/var/log/Avaya/sm/asm.log` `/var/log/Avaya/sm/TextLog_<TimeStamp>.log`	The ZangSmsConnector snap-in deployment logs.

Service logs	`/var/log/Avaya/services/ZangSmsConnector/ZangSmsConnector.log`
	For Centralized logging:
	`/var/log/Avaya/services/ZangSmsConnector / ZangSmsConnector_json.log`
		The ZangSmsConnector snap-in logs masked messages for GDPR compliance at FINEST Level.
		Avaya Oceana® Kibana dashboard displays Json logs that helps trace the SMS flow.

Alarm logs	`/var/log/Avaya/services/event.log`	The ZangSmsConnector snap-in alarm logs.

Common issues with ZangSmsConnector

The following table lists the common problems that can occur with ZangSmsConnector and how to troubleshoot these issues:

Issue description	Solution
`ZangSmsConnectorGateway initialization failed!`	Check if the **Oceana Messaging Snapin key** attribute value is same as the value in the OmniChannel Administration Database.
`Service attributes value changes are not picked by the ZangSMSConnector`	Restart the snap-in using the **Stop** or **Start** option available on the Service Management page.

Changing log levels

About this task

Use the following procedure to set the log level on Avaya Breeze® platform:

Procedure

1. On the System Manager web console, go to **Elements** > **Avaya Breeze®** > **Configuration** > **Logging**.

   System Manager displays the Logging page.

2. On the Logging page, select the options from the following mandatory fields:
   a. From the **Cluster** drop-down list, select the Oceanaocp cluster.
   b. From the **Service** drop-down list, select the **ZangSmsConnector** service.
   c. From the **Log Level** drop-down list, select the required option.

      For debugging, you must select the **ALL** option.

3. Click **Set Log Level**.
4. **(Optional)** To clear log levels, click **Clear Logs**.

Next steps

After the debugging is complete, set the **Log Level** field to **INFO**.

Managing alarms and events

About this task

ZangSmsConnector snap-in generates alarms whenever an error occurs. Use this procedure to view, search, and change status of alarms.

For more information on how to resolve alarms and events, see the *Avaya Oceana® Alarms* document on the Avaya Support site.

Procedure

1. To view the alarms, do the following:

   On the System Manager web console, navigate to **Services** > **Events** > **Alarms**.

   The Alarming page displays the Alarm list.

2. To change the status of alarms to Acknowledge, do the following:
   a. On the System Manager web console, navigate to **Services** > **Events** > **Alarms**.
   b. Click the check box of the alarm based on the Host IP address of the Avaya Breeze® platform server on which the ZangSmsConnector snap-in is deployed.

c. Click **Change Status** > **Acknowledged**.

   The status of the selected alarm changes to `Acknowledged`.

3. To change the status of alarms to Cleared, do the following:
   a. On the System Manager web console, navigate to **Services** > **Events** > **Alarms**.
   b. Click the check box of the alarm based on the Host IP address of the Avaya Breeze® platform server on which the ZangSmsConnector snap-in is deployed.
   c. Click **Change Status** > **Cleared**.

      The status of the selected alarm changes to `Cleared`.

4. To view the event logs, do the following:

   On the System Manager web console, click **Services** > **Events** > **Logs** > **Log Viewer**.

   The Logging page displays the Log list.

Chapter 27: Troubleshooting SocialConnector

SocialConnector log files

The following table describes the log files for troubleshooting the SocialConnector snap-in:

Log name	Location	Description
Service installation/ deployment logs	`/var/log/Avaya/sm/asm.log` `/var/log/Avaya/sm/TextLog_<TimeStamp>.log`	The SocialConnector deployment logs.

Service logs	`/var/log/Avaya/services/SocialConnector/SocialConnector.log`
	For Centralized Logging:
	`/var/log/Avaya/services/SocialConnector/SocialConnector_json.log`
		The SocialConnector logs that contain the masked messages at TRACE level.

Alarm logs	`/var/log/Avaya/breeze/event.log` `var/log/Avaya/breeze/alarms.log`	The SocialConnector alarm logs.

Common issues with SocialConnector

The following table lists the common problems that can occur with SocialConnector and how to troubleshoot these issues:

Issue description	Solution
`SocialConnector Gateway initialization failed!`	Check if the Oceana Messaging Snapin key attribute value is same as the value in the OmniChannel Administration DB.

Table continues…

Issue description	Solution
`Unable to find valid certification path to requested target`	This issue is related to Amazon Web Services (AWS) certificate. To resolve the certificate issue, do the following: 1. Download the Amazon SQS certificate from the Amazon AWS website. 2. Add certificate in Avaya Breeze® for Amazon SQS and Messaging snap-in. **Note:** Install the Amazon SQS certificate that is specific only to your region.

Chapter 28: Troubleshooting the co-resident Avaya Control Manager and External Data Mart

A large External Data Mart Transaction Log file is created

Condition

A large External Data Mart (EDM) Transaction Log file is created because of irregular EDM log backups or the absence of a maintenance plan.

Solution

1. Compress the backup and store it in a `.trn` file.

   A Transaction log backup is required to decrease the `.ldf` file size.

2. Shrink the database Files folder to free up unused space.
3. Regularly perform Steps 1 to 2 before the EDM Transaction Log file size decreases.

   When you perform these steps on the primary database, the changes are replicated to the secondary database.

Unable to open a connection to Microsoft SQL Server *through SQL Server Management Studio*

Condition

A connection is successfully established with the server. However, an error occurs during the login process.

Solution

1. Log in to the Avaya Control Manager server.
2. Click **Start** > **Microsoft SQL Server** > **SQL Server Configuration Manager**.
3. In the navigation pane, click **SQL Server Services**.

4. In the content pane, double-click the MSSQLSERVER.
5. In the SQL Server Properties dialog box, in the **Log on as** area, change from NT SERVICE MSSQLSERVER\ to the domain administrator user that you use to access all SQL server nodes.

Contexts are not persisting to the External Data Mart from Context Store

Condition

A connection is successfully established with the server. However, an error occurs during the login process.

Solution

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, in the **Service URL** column for Avaya Oceana® Cluster 1, do one of the following:
   - Select **Oceana Monitor** to open the Monitor Service page.
   - Select **Oceana Manager** and open the Gigaspaces Viewer from the Oceana Manager page.
3. Ensure that the status of EDM Audit or Journey processing unit is `INTACT`.
4. If the processing unit state is not visible, do the following:
   a. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
   b. Select the **Service Clusters** tab.
   c. In the **Cluster** field, select Avaya Oceana® Cluster 1.
   d. In the **Service** field, select **ContextStoreManager**.
   e. Ensure that the **EDM: Enable Persistence to database** attribute is set to `true`.
   f. Ensure that the correct processing unit is configured.
   g. In the **Cluster** field, select **ProvisioningCluster**.
   h. In the **Service** field, select **OceanaConfiguration**.
   i. Ensure that the SQL Server details are correct.
   j. Ensure that the correct processing unit is configured.
5. Check the SQL Server error log in the `ERRORLOG` and `ERRORLOG.n` files available at the following location:

   `C:\Program Files\Microsoft SQL Server\MSSQL.n\MSSQL\LOG\`

   For more information about SQL Server log locations, go to https://docs.microsoft.com/en-us/sql/relational-databases/logs/open-log-file-viewer?view=sql-server-2016.

6. In the error log files, check the following information:
   - Underlying hardware specs (CPU, RAM)
   - Default Collation Type
   - Starting up database 'CSEDM'
   - AlwaysOn Availability Groups connection with primary database established for secondary database 'CSEDM' on the availability replica 'MMSERVER49101' with Replica ID: {8bc318fd-3ca2-4ecc-b95c-2948985a9fff}. This is an informational message only. No user action is required.
   - Errors (Number, Severity & State):
     - Error: 18456, Severity: 14, State: 38.
     - Login failed for user 'NT SERVICE\ReportServer'. Reason: Failed to open the explicitly specified database 'ReportServer'.
     - Authentication Error: Could not find database requested by user.

     For detailed error number description, go to https://docs.microsoft.com/en-us/sql/relational-databases/errors-events/database-engine-events-and-errors?view=sqlallproducts-allversions.
7. Check the `cs-journey PU` and `cs-edm PU` logs available at the following location:

   `/var/log/Avaya/dcm/pu/ContextStoreManager`

SSL certificate errors in the ContextStoreQuery or CustomerJourneyService log

Condition

The ContextStoreQuery or CustomerJourneyService log shows the following SSL certificate errors when using a secure connection to the Context Store EDM Availability Group Listener:

```
EDM connection error: The driver could not establish a secure
connection to SQL Server by using Secure Sockets Layer (SSL)
encryption. Error: "com.ibm.jsse2.util.h: PKIX path building failed:
java.security.cert.CertPathBuilderException: unable to find valid
certification path to requested target".
```

Solution

1. Check the validity of the certificates.
2. Ensure that port 443 is open on the Microsoft SQL Server.
3. Check the version of the JDBC SQL driver used to connect ContextStoreQuery.

   For information about loading the JDBC SQL driver, see *Avaya Context Store Snap-in Reference*.
4. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.

5. On the Service Clusters tab, do the following:
   a. In the **Cluster** field, select Avaya Oceana® Cluster 1.
   b. In the **Service** field, select **ContextStoreManager**.
   c. Ensure that the **EDM: Database host** attribute is configured with the Availability Group Listener FQDN.
   d. Ensure that the **EDM: TLS version** attribute is set to `TLSv1.2`.
   e. In the **Service** field, select **ContextStoreQuery**.
   f. Ensure that the **EDM: Database host** attribute is configured with the Availability Group Listener FQDN.
   g. Ensure that the **EDM: TLS version** attribute is set to `TLSv1.2`.
6. In System Manager, verify that the TLS 1.2 is selected.
7. Verify that the same domain user is specified on both the SQL Servers.
8. Verify that the domain user has full administrator permissions on both the SQL Servers.
9. Verify that both the SQL Servers are using the correct certificate.

   You can check the certificates by exporting them through `certlm.msc`. For information about how to export certificates, see *Deploying Avaya Oceana®*.

Chapter 29: Troubleshooting OAuth

java.security.cert.CRLException: Empty input error

Condition

O365 mailbox may produce `java.security.cert.CRLException: Empty input` error in logs or in inbox statistics.

Solution

1. Log on to Avaya Aura® System Manager.
2. Navigate to **Services** > **Security** > **Configuration** > **Security Configuration**.
3. In the **Certificate Revocation Validation** field, select `NONE`.
4. Click **Commit**.
5. Reboot all clusters.

Chapter 30: Troubleshooting CylancePROTECT

Stopping CylancePROTECT

Procedure

To stop CylancePROTECT, run the following command:

```
systemctl stop cylancesvc.service;
```

Disabling CylancePROTECT

Procedure

To disable CylancePROTECT, run the following command:

```
systemctl disable cylancesvc.service;
```

Checking CylancePROTECT status

Procedure

To check the status of CylancePROTECT, run the following command:

```
systemctl is-enabled cylancesvc.service
```

Chapter 31: Resources

Documentation

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

Table continues…

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

Finding documents on the Avaya Support website

Procedure

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

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

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

8. Click to display the search results.

Avaya Documentation Center navigation

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

Important:

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

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

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

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

You can do the following:

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

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

  You can do the following:

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

Training

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

Table 6: 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 7: 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 8: 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 9: 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 10: End User, Programmer, Administration

Avaya Learning Center				
Course code	**Course title**	**Course duration in hours**	**Delivery type**	**Vanity Link for Attachment**
ALEU-5002 Avaya Oceana® End-User Training				
24020W	Using Avaya Workspaces for Avaya Oceana® - Agent	1.0	Web-based Training	https://www.avaya.com/oceana-agent
24040W	Using Avaya Workspaces for Avaya Oceana® - Supervisor	1.0	Web-based Training	https://www.avaya.com/oceana-supervisor
ALUC-4001 Avaya Breeze® Client SDK				
2410W	Customer Communications and Apps with Oceana® for Developers	3.0	Web-based Training	
ASDC-0010 Avaya Workspaces® Framework				
24150W	Customizing the Avaya Workspaces® Framework	3.0	Web-based Training	
24150T	Avaya Workspaces® Framework R3 Test	1.0	Online Test	
ASAC-0005 Avaya Oceana® Administration				
21160W	Avaya Oceana® Fundamentals	0.5	Web-based Training	
24300V	Administering Avaya Oceana® R3 Omnichannel	40.0	Virtual Instructor-Led Training	Attached with the sale
2430T	Administering Avaya Oceana® R3 Online Test	1.0	Online Test	
24320W	Administering Avaya Oceana® - Basic	2.5	Web-based Training	https://www.avaya.com/Oceana-admin

Table continues…

Avaya Learning Center				
Course code	**Course title**	**Course duration in hours**	**Delivery type**	**Vanity Link for Attachment**
ASAC-0031 Avaya Analytics™ R4 for Oceana® Administrator				
24380T	Administering Avaya Analytics1M R4 for Oceana8 Specialized Test	1.0	Online Test	

Table 11: 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.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips.
- Information about service packs.
- Access to customer and technical documentation.
- Information about training and certification programs.
- Links to other pertinent information.

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

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** > **Products**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. Select the release number, if applicable.
6. Click the **Technical Solutions** tab to view articles for resolving technical issues.

Appendix A: Take Avaya Oceana® out of service for voice

This section describes the configuration required to take Avaya Oceana® out of service for voice. Using this feature, you can avoid service interruption for voice if you need to take Avaya Oceana® out of service. For example, if you need to perform an upgrade or routine maintenance of hardware, you can take the Avaya Oceana® out of service and automatically route all subsequent calls to Call Center Elite. Any Avaya Oceana® voice calls already in progress are not affected. Agents can complete all Avaya Oceana® voice calls before the start of the maintenance window.

You take Avaya Oceana® out of service for voice by dialing a Feature Access Code (FAC) from any station used by Avaya Oceana®.

Index

F

G

K

L

M

N

O

P

R

S

T

U

V

W