Implementing Avaya Proactive Outreach Manager

Release 3.1.1
Issue 1
August 2018

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

License types

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

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

Licenses

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

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

Heritage Nortel Software

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

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

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

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

Avaya is a registered trademark of Avaya Inc.

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

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

Contents

Chapter 1: Introduction

Purpose

This document describes procedures to install, configure, and uninstall Avaya Proactive Outreach Manager.

The audience includes and is not limited to implementation engineers, field technicians, business partners, and customers.

Chapter 2: New in this release

New in this release

This release supports the following enhancements:

- Support for Avaya Oceana™ Solution by using a new Oceana™ install mode.
- Certificate management for the POM trusted certificate.

Chapter 3: Planning and preconfiguration

Knowledge and skills

Before deploying POM, ensure that you have the following:

Knowledge

- Creating, installing, configuring, and administering a database.
- Installing, configuring, and administering Avaya Aura® Experience Portal.
- How to deploy POM on Apache Tomcat.

Skills

- How to execute shell scripts.
- How to edit files on Linux by using a text editor such as vi or vim.
- How to execute database scripts and queries.
- How to validate logs.
- How to validate error messages.
- How to use a command line.

POM deployment modes

The following is the list of POM deployment modes:

- CC Elite
- AACC-SBP [Skills-Based Pacing for Agentless POM]
- None
- AACC [Integrated and Blending]
- Oceana

Based on the deployment mode that you select, you must install and configure certain other products before installing POM. For information about the products that are required for each deployment mode, see System requirements on page 11.

System requirements

The following table describes the system requirements for each deployment mode:

No.	External server/ system	Deployment mode					Notes
		None	CC Elite	AACC-SBP	AACC	Oceana	
1	Avaya Aura® Experience Portal	✔	✔	✔	✔	✔	Although Avaya Aura® Experience Portal is an external system, POM resides on Avaya Aura® Experience Portal. For more information about the hardware requirements for installing Avaya Aura® Experience Portal, see *Administering Avaya Aura® Experience Portal*. To install POM on an Experience Portal system that requires support for the languages other than English, you must install appropriate fonts. For more information about non-English language support on Experience Portal, see *Implementing Avaya Aura® Experience Portal on a single server* or *Implementing Avaya Aura® Experience Portal on multiple servers*.
2	Database server	✔	✔	✔	✔	✔	The Database server can be PostgreSQL, Oracle. Enterprise Edition 64 bit, or Microsoft SQL Server. You can install the PostgreSQL database as a local database. In production environment, do not install POM database schema on local PostgreSQL. You must

Table continues…

No.	External server/ system	Deployment mode					Notes
		None	CC Elite	AACC-SBP	AACC	Oceana	
							install PostgreSQL, Oracle and Microsoft SQL Server database only on an external server.
3	License server	✔	✔	✔	✔		License server is mandatory, and can be a local or an external license, installed on the license server. The license can be either POM ports predictive license, a preview license, an SMS license, or an email license. For more information about licenses, see *Proactive Outreach Manager Overview and Specification*.
4	Avaya Aura® Call Center Elite (Call Center Elite)		✔				You must install Call Center Elite to run agent-based campaigns or to run agent-less automated skill-based campaigns.
5	Avaya Aura® Contact Center			✔	✔		You must install Avaya Aura® Contact Center to run automated skill-based campaigns or agent-based campaigns. For more information on multicast configuration, see *Integrating Proactive Outreach Manager*.
6	Avaya Oceana™ Solution					✔	You must install Avaya Oceana™ Solution. For more information see, *Deploying Avaya Oceana™ Solution*.
7	Custom Agent Desktop		✔		✔		You can design your own desktop using the agent APIs. For more information about agent APIs, see *Proactive*

Table continues…

No.	External server/ system	Deployment mode					Notes
		None	CC Elite	AACC-SBP	AACC	Oceana	
							Outreach Manager Agent API.
8	Application Enablement Services (AES) server		✔	✔	✔	✔	AES is mandatory for agent outbound calls. For Avaya Aura® Contact Center, you need AES only if you use Avaya Aura® Communication Manager.
9	Call Management System (CMS)		✔				CMS is used for skill-based pacing and blending in Call Center Elite. To create and run skill-based campaigns, you must configure the RT_socket package, which provides a TCP stream socket real- time interface from CMS. While configuring the RT Socket to send CMS real time data to POM server, ensure you use the *tvi1* report format.
10	Avaya Contact Recorder						Avaya Contact Recorder is optional.
11	Operating system						Red Hat Enterprise Linux or Avaya Enterprise Linux

In addition to the requirements mentioned in the table, the following are the other requirements for POM:

- Licenses: Ensure that the number of telephony ports in Avaya Aura® Experience Portal are more than or equal to the number of POM ports. Acquire the Text to Speech (TTS) or Automated Speech Recognition (ASR) licenses.
- Speech servers: Configure at least one TTS to use the AvayaPOMNotifier application or any custom Avaya Aura® Orchestration Designer application that requires TTS.
- VoIP connections: Configure Session Initiation Protocol (SIP) ports or H.323 ports.
- SA8874 feature: Activate the SA8874 feature, that is, call status messages, for 7434ND IP phones on Avaya Aura® Communication Manager. When you activate the SA8874 feature, you can use the Call Classification Analysis (CCA) feature for H.323 ports.
- Port Distribution: Ensure that the H.323 or SIP ports on Avaya Aura® Experience Portal are in service.

Note:

To run agent-based campaigns, a SIP connection is mandatory. Ensure you have enough SIP ports reserved for POM applications and campaigns.

- Experience Portal Manager (EPM) and Media Processing Platform (MPP) server: Use the primary EPM, auxiliary EPM, and MPP servers with the recommended sizing tool.

Deployment scenarios

The following are the deployment scenarios for POM:

- Single-server deployment
- Multiple-server deployment with zones
- Multiple-server deployment without zones

RT Socket connection requirements

Based on your deployment, configure the RT Socket connections as follows:

- If your deployment only includes CMS High Availability:
  - Configure one connection between the primary CMS and each POM server in the data center
  - Configure one connection between the secondary CMS and each POM server in the data center
- If your deployment only includes POM Geo-Redundancy:
  - Configure one connection between CMS and each POM server in Data Center 1
  - Configure one connection between CMS and each POM server in Data Center 2
- If your deployment includes CMS High Availability and POM Geo-Redundancy:
  - Configure one connection between the primary CMS and each POM server in Data Center 1
  - Configure one connection between the secondary CMS and each POM server in Data Center 1
  - Configure one connection between the primary CMS and each POM server in Data Center 2
  - Configure one connection between the secondary CMS and each POM server in Data Center 2

Database server requirements

Hardware requirements

Sr. No.	Agents	Outbound Ports (Notification)	No. of Jobs	Database server
1	1-500	0	100	HP Gen7 with 2.4 GHz 16 CPU, Quad Core processor with 12 GB RAM and a minimum of 300 GB of hard disk storage. OR HP Gen9 with 2.4 GHz 24 CPU, Hexa-Core processor with 32 GB RAM and a minimum of 500 GB of hard disk storage.
2	500-1000	0	200	HP Gen9 with 2.4 GHz 24 CPU, Hexa-Core processor with 32 GB RAM and minimum of 500 GB of hard disk storage.
3	1000-2000	0	200	HP Gen9 with 2.4 GHz 24 CPU, Hexa-Core processor with 32 GB RAM and minimum of 500 GB of hard disk storage.
4	0	1-2200	50	HP Gen9 with 2.4 GHz 24 CPU, Hexa-Core processor with 32 GB RAM and minimum of 500 GB of hard disk storage.

Database requirements

- PostgreSQL 9.6 64 bit
- Oracle 11g R2 Enterprise/Standard Edition 64 bit
- Oracle 12C Enterprise/Standard Edition 64 bit
- Microsoft SQL Server 2012 Enterprise/Standard Edition
- Microsoft SQL Server 2014 Enterprise/Standard Edition
- Microsoft SQL Server 2016 Enterprise/Standard Edition

Note:

- In the production environment, do not install the POM database schema on the local PostgreSQL. You must install PostgreSQL, Oracle, or Microsoft SQL Server database only on an external server.

- If you configure POM with the MSSQL database, then ensure that for an operational database, READ_COMMITTED_SNAPSHOT parameter is set to false.
- For an operational database, ensure that you have a minimum of 5 GB database size to support a load of :
  - 200 contact lists with 10,000 records in each contact list
  - 20 - 25 filtering, and 10 sort conditions
  - 173 contact attributes (system + custom)
  - 1000 agents
  - 200 concurrent jobs
  - Generated Outbound load: 60,000 Busy Hour Call Completion (BHCC). To get 60,000 BHCC outbound attempts with maximum 2,000 attempts for agent less campaigns, maximum 5,000 attempts for Email campaigns, maximum 5,000 attempts for SMS campaigns, and maximum 48,000 for agent based campaigns.
- Operational database purging is not required.
- The total index size might increase up to two times of the actual data size. Therefore, ensure that you have additional storage for the increased index size.

Application server requirements

Hardware requirements

Sr. No.	Agents	Outbound Ports (Notification)	No. of Jobs	Application server specification
1	1-500	0	100	HP Gen7 with 2.4 GHz 16 CPU, Quad Core processor with 12 GB of RAM and a minimum of 300 GB of hard disk storage OR HP Gen9 with 2.4 GHz 24 CPU, Hexa-Core processor with 32 GB of RAM and a minimum of 500 GB hard disk storage.
2	500-1000	0	200	HP Gen7 with 2.4 GHz 16 CPU, Quad Core processor with 12 GB of RAM and a minimum

Table continues…

Sr. No.	Agents	Outbound Ports (Notification)	No. of Jobs	Application server specification
				of 300 GB hard disk storage. OR HP Gen9 with 2.4 GHz 24 CPU, Hexa-Core processor with 32 GB of RAM and a minimum of 500 GB hard disk storage.
3	1000-2000	0	200	HP Gen7 with 2.4 GHz 16 CPU, Quad Core processor with 12 GB of RAM and a minimum of 300 GB hard disk storage. OR HP Gen9 with 2.4 GHz 24 CPU, Hexa-Core processor with 32 GB of RAM and a minimum of 500 GB hard disk storage.
4	0	1-2200	50	HP Gen7 with 2.4 GHz 16 CPU, Quad Core processor with 12 GB of RAM and a minimum of 300 GB of hard disk storage OR HP Gen9 with 2.4 GHz 24 CPU, Hexa-Core processor with 32 GB of RAM and a minimum of 500 GB of hard disk storage

Software requirements

- Red Hat Enterprise Linux 6.8
- Avaya Aura® Experience Portal 7.2.
- Tomcat 8.5.11 or later for a local application server

Requirements for a database login

The POM database server requires an administrative login with Database Administrator (DBA) read-write privileges The following table shows the values for this administrative login. If you use a different administrative login, ensure that login has the same permissions as the login listed in the following table:

Property	Microsoft SQL Server	Oracle	PostgreSQL
Database Administration Login	`sa`	`system`	`postgres`
Database Administration Password	password for `sa`	password for `system`	password for `postgres`

Database servers act as a central repository for all the information that POM stores and retrieves. You can install and configure database servers in multiple ways to provide scalability, fault tolerance, and security to meet the requirements of your organization.

Important:

Database server installation and configuration are beyond the scope of this manual. Consult a qualified DBA to deploy your chosen database platform.

Network configuration

All of the machines in the Experience Portal environment (EPM/POM, MPPs, Database, Speech Servers, and Application Servers) should be configured on the same LAN switch. All physical network connections to these servers should be at least 1 Gbps.

Chapter 4: Installing POM on Avaya Aura ® Experience Portal

Configuring Experience Portal for setting up POM system installation

Perform the following steps before you install POM:

Before you begin

Install Avaya Aura® Experience Portal 7.2. For more information, see *Implementing Avaya Aura® Experience Portal on a single server* and *Implementing Avaya Aura® Experience Portal on multiple servers*.

Procedure

1. On the primary EPM, you must:
   a. Edit the `/var/lib/pgsql/data/pg_hba.conf` file, and add the IP address of the POM server.

      Sample `pg_hba.conf` file:

      ```
      host all postgres xxx.xxx.xxx.xxx/xx md5
      ```

      where xxx.xxx.xxx.xxx is the POM server address and postgres is the database user name.

   b. Restart the Postgres service by typing the command `/sbin/service postgresql restart`. This service is useful only if you configure POM on a local Postgres database.

      Tip:

      In production environment, do not install POM database schema on local PostgreSQL. You must install PostgreSQL, Oracle, or Microsoft SQL Server database only on an external server.

   c. Set the database password on Avaya Aura® Experience Portal by typing the command `/opt/Avaya/ExperiencePortal/Support/Security-Tools/SetDbPassword.sh` on the command line. For more information about the database password, see *Administering Avaya Aura® Experience Portal*.

Note:

Step c is only required for local postgres database installation in a non-production environment.

2. To install POM on more than one system, include all auxiliary POM server host names in the primary EPM `/etc/hosts` file. You must also have the primary EPM host name in all auxiliary servers `/etc/hosts` file.

Installing POM on a primary EPM using the interactive mode

Before you begin

Ensure that the EPM server is running that is VPMS service is in the running state.

Procedure

1. Log in to primary Avaya Aura® Experience Portal as a root user for Red Hat Enterprise Linux (RHEL) or Avaya Enterprise Linux (AEL).
2. To mount the POM iso image on the server, in the command line, type `mount –o loop <absolute path of iso image> /mnt`.
3. To change the directory to mnt, type `cd /mnt`.
4. Type `./installPOM`, and press `Enter`.

   The system checks if the Experience Portal Manager (EPM) is running successfully. The system also checks the Tomcat server and the other services displayed in the list.

```
[root@pupomcpe17315 mnt]# ./installPOM
*** Starting POM Installation ***
************************************************************
*** Restarting and checking vpms service status, please wait... ***
************************************************************
tomcatd ( pid xxxx  ) is running...
SL ( pid xxxx  ) is running...
ActiveMQ is running ...
Overall Status: VPMS is running
************************************************************
*** EP service status [OK]***
************************************************************
************************************************************
*** Stopping vpms service, please wait... ***
************************************************************
Stopping individual components:
Stopping Tomcat.............Counter: 1. Tomcat is not running: 1
... successful
Stopping SL..... successful
Stopping ActiveMQ..... successful

VPMS Shutdown Status:                                  [  OK  ]
Overall Status: VPMS is stopped (all processes are stopped)
************************************************************
```

```
*** vpms service stopped... Starting POM Installation... ***
****************************************************************
Running CLI installation program...

Welcome to the installation of Avaya POM POM.03.01.00.00.00.00i x!
The homepage is at: http://www.avaya.com/


Press 1 to Continue, 2 for Previous, 3 to Redisplay or 4 to Quit [1]
```

5. On the Welcome screen, type one of the following:
   - `1` to continue.
   - `2` to go back to previous step.
   - `3` to redisplay menu options.
   - `4` to quit the installation.

   Note:

   At any point during the installation, if you press `4` to quit, the system displays the following confirmation message:

   ```
   1 Yes
   2 No
   Do you want to exit? [2]
   ```

6. On the End User License Agreement page, type `1` and press `Enter`.

   The screen refreshes with `1 - I accept the terms of the license agreement as the selected option`.

7. Press `Enter` and then, type one of the following:
   - `1` to continue.
   - `2` to go back to the previous step.
   - `3` to redisplay menu options.
   - `4` to quit the installation.

8. Type the installation path manually, or press `Enter` to select the default path. The default path is `/opt/Avaya/avpom`.

   Note:

   If you are installing POM on AEL, you must select the default path.

   If the installation path that you specify, exists then the system displays the following message:

   ```
   The directory already exists! Are you sure you want to install
   here and possibly overwrite existing files?
   1. Yes
   2. No
   ```

```
Do you want to continue?
```

- Type `1` to overwrite the existing files or type `2` to specify the installation path.

9. Type one of the following:
   - `1` to continue.
   - `2` to go back to previous step.
   - `3` to redisplay menu options.
   - `4` to quit the installation.
10. For the Primary EPM, install the following packages:
    - EPMS plug-in
    - POM server
    - Avaya Aura® Orchestration Designer application

    By default, the system selects all packages and you can cancel the selection of Avaya Aura® Orchestration Designer application. The EPMS plug-in and the POM server package are mandatory.

    a. Type `3` and press `Enter` to select or clear the Avaya Aura® Orchestration Designer application package.

    Note:

    To install Avaya Aura® Orchestration Designer after you install POM, run the `InstallAppServer.sh` script file and copy `*.war` files from `$POM_HOME/DDapps` to `$APPSERVER_HOME/webapps`, and copy files from `$POM_HOME/DDapps/lib/*` to `$APPSERVER_HOME/lib/` folder. To check the path of the `InstallAppServer.sh`, see the *Avaya Aura® Experience Portal* documentation.

    b. Type `r` to redisplay.

    c. Type `c` to continue and press `Enter`.
11. Type one of the following:
    - `1` to continue.
    - `2` to go back to previous step.
    - `3` to redisplay menu options.
    - `4` to quit the installation.
12. Type `0` to create a new certificate or `1` to import the security certificate from specified location, and press `Enter`.

    Note:

    To import the security certificate, ensure that the certificate format is a `PKCS#12` file and stores both the root certificate and the root certificate key.

The system displays the security certificate.

13. Type one of the following:
    - `1` to continue.
    - `2` to go back to previous step.
    - `3` to redisplay menu options.
    - `4` to quit the installation.

    The system displays the Installation Summary screen, which consists of:

    ```
    The installation path
    All the packages that you select for installation
    The space occupied by each package
    The used and free system space
    ```

    The system also displays the following message:

    ```
    The last portion of the install might take several minutes
    Please be patient and wait for the Post Installation Summary to
    begin
    IMPORTANT: PLEASE DO NOT ABORT THE INSTALLATION
    ```

14. Type one of the following:
    - `1` to continue.
    - `2` to go back to previous step.
    - `3` to redisplay menu options.
    - `4` to quit the installation.

    Caution:

    If you type `2` after this step, you cannot navigate back to change the installation.

    Important:

    Do not quit the installation until the system displays the Post Installation Summary screen.

    The system begins the installation. After the installation is complete, the system displays the following message:

    ```
    Installation was successful.
    Application installed on <installation path>
    ==============================================================
    [ Console installation done ]
    /etc/alternatives/java_sdk_1.8.0//bin/java
    Entry for alias pomservercert successfully imported.
    ```

```
Import command completed:  1 entries successfully imported, 0
entries failed or cancelled.

MAC verified OK

Moving installation log files to: /opt/Avaya/avpom/POManager/logs
================================================================

If you are using an external application server and you have
installed the POM AAOD Application package while installing POM,
you need to:

a--> Copy the *.war files from $POM_HOME/DDapps to $CATALINA_HOME/
webapps of the external application server.

b--> Copy files from $POM_HOME/DDapps/lib/* to $CATALINA_HOME/lib
of your external application server.

c--> Enable the SSL Configurations for application server.

d--> Restart the external application server.

Please restart the system now !
```

15. Restart the system by typing `reboot`.

Installing POM on an auxiliary EPM using the interactive mode

Procedure

1. Log in to auxiliary Avaya Aura® Experience Portal as a root user for Red Hat Enterprise Linux (RHEL) or Avaya Enterprise Linux (AEL).
2. To mount the POM iso image on the server, in the command line, Type `mount –o loop <absolute path of iso image> /mnt`.
3. Type `cd /mnt` to change the directory to mnt.
4. Type `./installPOM`, and press `Enter`.
5. On the Welcome screen, type one of the following:
   - `1` to continue.
   - `2` to go back to previous step.
   - `3` to redisplay menu options.
   - `4` to quit the installation.

   Note:

   At any point during the installation, if you press `4` to quit, the system displays a confirmation message:

```
Type 1 to quit or type 2 to cancel quitting the installation.
```

6. On the End User License Agreement page, type `1` and press `Enter`.

   The screen refreshes with the `1 - I accept the terms of the license agreement as the selected option` message.

7. Press `Enter` and type one of the following:

   - `1` to continue.
   - `2` to go back to previous step.
   - `3` to redisplay menu options.
   - `4` to quit the installation.

8. Type the installation path manually, or press `Enter` to select the default path. The default path is `/opt/Avaya/avpom`.

   Note:

   If you are installing POM on AEL, you must select the default path.

   If the installation path that you specify exists, the system displays the following message:

   ```
   The directory already exists! Are you sure you want to install
   here and possibly overwrite existing files?
   1. Yes
   2. No
   Do you want to continue?
   ```

   - Type `1` to overwrite the existing files or type `2` to specify the installation path.

9. Type one of the following:

   - `1` to continue.
   - `2` to go back to previous step.
   - `3` to redisplay menu options.
   - `4` to quit the installation.

   The installer detects whether the system is a primary or an auxiliary EPM.

10. For an auxiliary EPM, install the following packages as required:

    - POM server
    - Avaya Aura® Orchestration Designer application

    By default, the system selects all packages and you can cancel the selection of Avaya Aura® Orchestration Designer package. POM server package is mandatory.

    a. Type `2` and press `Enter` to select or clear the Avaya Aura® Orchestration Designer application package.

Note:

To install Avaya Aura® Orchestration Designer after you install POM, run the `InstallAppServer.sh` script file and copy `*.war` files from `$POM_HOME/DDapps` to `$APPSERVER_HOME/webapps`, and copy files from `$POM_HOME/DDapps/lib/*` to `$APPSERVER_HOME/lib/` folder. To check the path of the `InstallAppServer.sh`, see the *Avaya Aura® Experience Portal* documentation.

b. Type `r` to redisplay.

c. Type `c` to continue and press **Enter**.

11. Type one of the following:
    - `1` to continue.
    - `2` to go back to previous step.
    - `3` to redisplay menu options.
    - `4` to quit the installation.
12. Type the IP address of the primary POM server to import the certificate for POM server. Ensure you enter port number as `80`.
13. Type `0` to create a new certificate or type`1` to import the security certificate from the specified location, and press `Enter`.

    Note:

    To import the security certificate, ensure that the certificate format is a `PKCS#12` file and stores both the root certificate and the root certificate key. Ensure that the file is encrypted and is password protected.

    The system displays the security certificate.
14. Type one of the following:
    - `1` to continue.
    - `2` to go back to previous step.
    - `3` to redisplay menu options.
    - `4` to quit the installation.

    The system displays the Installation Summary screen, which consists of:

    ```
    The installation path
    All the packages that you select for installation
    The space occupied by each package
    The used and free system space
    ```

    The system also displays the following message:

    ```
    The last portion of the install might take several minutes
    ```

```
Please be patient and wait for the Post Installation Summary to
begin

IMPORTANT : PLEASE DO NOT ABORT THE INSTALLATION
```

15. Type one of the following:
    - `1` to continue.
    - `2` to go back to previous step.
    - `3` to redisplay menu options.
    - `4` to quit the installation.

    Caution:

    If you type `2` after this step, you cannot navigate back to change the installation.

    Important:

    Do not quit the installation until the system displays the Post Installation Summary screen.

    The system begins the installation. After the installation is complete, the system displays the following message:

```
Installation was successful.

Application installed on <installation path>
==============================================================

[ Console installation done ]

Moving installation log files to: /opt/Avaya/avpom/POManager/logs
==============================================================

If you are using a external application server and you have
installed the POM AAOD Application package while installing POM,
you need to:

a--> Copy the *.war files from $POM_HOME/DDapps to $CATALINA_HOME/
webapps of the external application server.

b--> Copy files from $POM_HOME/DDapps/lib/* to $CATALINA_HOME/lib
of your external application server.

c--> Enable the SSL Configurations for application server.

d--> Restart the external application server.

Please restart the system now !
```

16. Restart the system by typing `reboot`.

Chapter 5: Silent installation

Silent installation

Silent installation of POM creates an xml configuration file for the izpack installer. However, you can create your own xml configuration file and customize values in the file for the izpack installer.

During a silent installation, you do not need to provide inputs to the system.

To perform a silent installation, use the following options while running the *installPOM* script:

Options	Remarks
`-s`	You must use this option while performing a silent install of POM. If you do not use this option, the system ignores the following options: • `-d` • `-p` • `-t` • `-c` • `-f` • `-i`
`-d`<installation directory path>	Use this option to do the following: • To specify a path to install POM • To specify a path to install POM Manager directory
`-p` <package name>	Use this option to select one of the following installation packages: • `vpmsplugin` • `pomserver` • `ddapps` You can select the same package multiple times.
`-t`<primary | aux>	Use this option to select one of the following installation types: • `primary` • `aux` If you select `primary`, the script selects both the `vpmsplugin` and `pomserver` packages.

Table continues…

Options	Remarks
	If you select `aux`, the script selects the `pomserver` package.
`-c`<import path>	Use this option to specify a path to import an existing certificate from an external server to the Experience Portal (EP) server. If you do not use this option, the system creates a new certificate on the Experience Portal (EP) server.
`-I`<primary ipaddress:port>	Use this option in the following cases: • If you use `-t` with `aux`. • If you change `install_type` in `aux`.
`-f`<config file path>	Use this option to specify a path to install a configuration file on the EP server. The config file has the following parameters: `install_dir_path`=<path> `cert_path`=<path> `pack`=< vpmsplugin | pomserver | ddapps> `install_type`=<primary | aux> `primary_ip_port`=<ipaddress:port> If you specify installation parameters while installing POM, the system does not use the default installation parameters. You can specify parameters by using the command line options. For example, if you use both `-d` <install path> and `-f` <config file> and the POM configuration file contains the `install_dir_path` parameter, the system ignores the default `install_dir_path`. The system uses the parameter `-d` that you specify for installation.
`-h`	Use this option to see detailed help on POM installation options.

Example

```
[root@pupomcpe17317 mnt]# ./installPOM -h

Usage: installPOM [-s]
                  [-d <install path>]
                  [-p vpmsplugin|pomserver|ddapps]
                  [-t primary|aux]
                  [-i <primary ip address:port>]
                  [-c <cert import path>]
                  [-P <cert password>]
                  [-f <config file>]
                  [-h]
                  [-?]


    -s
        Required for silent install.
        Following options will work only with -s:
        -d, -p, -t, -c, -f, -i, -P

    -d  <install path for POM>
         Specify the path on the linux system where POM should
```

```
       be installed. Directory "POManager" will be created
       under the path specified.

      e.g. installPOM -s -d /testdir/avpom
      (This will install POM under /testdir/avpom/POManager,
        and set POM_HOME to /testdir/avpom/POManager)

  -p <package name>
      Specifies the package which needs to be installed
      during POM installation.

      Package name can be one of :
          vpmsplugin
          pomserver
          ddapps

      This option can be used more than once to specify multiple
      packages.

      e.g. installPOM -s -p vpmsplugin -p pomserver

      (This will install vpmsplugin and pomserver packages
        during POM installation)

  -t <installation type>
      Specifies the installation type. The installation type
      can be one of:
          primary
          aux

      If type is "primary", then the following packages
        are selected automatically:
          vpmsplugin, pomserver

      If type is "aux", then only pomserver package is selected.

      This option can be specified only once.

  -i <primary IP:port>
      Specifies the IP address and port of the primary POM server.

      This is applicable only when installing aux POM server using
        -t "aux" or insall_type="aux" in the config file (-f option)

  -c <certificate import path>
      If this option is used, then the certificate is picked up
      from the location specified as the argument to -c.

      If this option is not used, then a new certificate is created
      during POM installation.

      e.g. installPOM -s -c /opt/certs/pom_pki.crt

  -P <certificate password>
      This option is used to specify the certificate password when
      a certificate is imported (see option -c).

      This option is applicable only with -c option.

  -f <config file path>
      If this option is used, then the properties are read
      from the file specified. This file can have the following
      property value pairs:

      install_dir_path=<path>
```

```
        cert_path=<path>
        cert_password=<password>
        pack=<vmpsplugin|pomserver|ddapps>
        install_type=<primary|aux>
        primary_ip_port=<IP address:port>

        Command line options will be given preference over
        parameters in the config file.

        e.g. Contents of the config file /tmp/mypom.conf:

        install_dir_path=/opt/Avaya/pominstalldir
        pack=ddapps
        pack=pomserver
        pack=vpmsplugin
        cert_path=/tmp/mypkicertificate.crt


        Usage from command line:
        installPOM -s -f /tmp/mypom.conf

[root@pupomcpe17317 mnt]#
```

Installing POM on primary EP by using silent mode

Procedure

1. On the primary EP server, open a command prompt window.
2. In the command prompt window, type the following script:

   `./installPOM -s -t primary -p ddapps`
3. Press `Enter`.

Installing POM on auxiliary EP by using silent mode

Procedure

1. On the auxiliary EP server, open a command prompt window.
2. In the command prompt window, type the following script:

   `./installPOM -s -t aux -i <ipaddressofprimaryepm:80> -p ddapps`
3. Press `Enter`.

Chapter 6: POM configuration

Checklist for configuring a POM server

Planning tasks

- You must configure the POM database on primary EPM.

No.	Task	Reference	Notes	✔
1	Configure the POM database.	See Configuring the database on page 33.	Select the installation mode and the database type for configuring the database.	
2	Configure the POM servers.	See Configuring the POM server on page 35.	After you install the POM server, configure the POM server using the web interface.	
3	Configure Avaya Aura® Call Center Elite or Avaya Aura® Contact Center.	See *Using Proactive Outreach Manager*.	Integrate POM with Avaya Aura® Call Center Elite or Avaya Aura® Contact Center for agent functionality and running agent-based campaigns.	
4	Add users or assign POM specific privileges to existing users.	See Adding users on page 50.	Add users after adding the POM server.	
5	Change the default country setting.	See Changing Home Country on page 51.	Change the default country to a country of your choice.	
6	Exchange certificates for the Avaya Aura® Orchestration Designer application server.	See Exchanging certificates for Avaya Aura® Orchestration Designer application server on page 45.	To use the Avaya Aura® Orchestration Designer application server, you must exchange certificates between each application server and POM.	
7	Configure the application server.	See Configuring the applications and licenses on page 37.	Specify the external applications and license requirements.	

Configuring the POM database on the primary POM server

About this task

Use this procedure to configure the POM database only on the primary POM server. For the auxiliary POM server, you do not need to configure the POM database explicitly. When you add an auxiliary POM server from the POM Servers page, the auxiliary server can access the database.

Before you begin

1. Install POM.
2. Determine the type of the database that you want to use and also whether you want to install the database on a local server or an external server.

   Tip:

   In the production environment, do not install the POM database schema on a local PostgreSQL.

   When you install the POM database schema on a local or an external database, the administration of this local or external database is the responsibility of the customer. For more information on database types and configurations, see *Appendix B*.
3. Create two database instances: One for the POM database and another for an operational database.

   Note:

   The POM database schema name and the operational schema name must not be same except for the Oracle database. If you are using the Oracle database, the system prompts for the following confirmation message:

   ```
   Do you want to use the same (pomdb) database for operational database? (y/n):
   ```

   - For y: The system uses the same name as the POM database schema.
   - For n: The system asks to enter the operational db name.

   You must install the operational database on the same server where the POM database is present.
4. For the external postgres server, in the `pg_hba.conf` file located at `/var/lib/pgsql/data/`, type the IP address of the POM server.

   Note:

   If you edit the `pg_hba.conf` file, restart the postgres service. To restart, on the command line, type `/sbin/service postgresql restart`.
5. For a secure database connection, add the 3rd party certificate in the Java keystore by typing `keytool -keystore $JAVA_HOME/jre/lib/security/cacers -import -file<absolute path of certificate file>`. When the system prompts for a password, type the default Java keystore password as `changeit`.
6. Configure a desired server. You can configure a Postgres, Oracle, or Microsoft SQL Server. For Installing Oracle drivers, see *Installing an Oracle driver*.

Procedure

1. Log in to the primary EPM as a root or sroot user.
2. Type `cd $POM_HOME/bin` and press `Enter`.
3. Type `./installDB.sh` and press `Enter`.

   The system displays the following message:

   ```
   Please select Contact Center Configuration mode from the following
   options:
   1. CCElite
   2. AACC-SBP [Skills-Based Pacing for Agentless POM]
   3. None
   4. AACC [Integrated & Blending]
   5. Oceana
   ```

4. Type `1` ,`2`, `3`, `4` or `5` and press `Enter`:

   The system displays the following message

   ```
   This script can modify $POM_HOME/config/PIMHibernate.cfg.xml or
   Test the DB connection.
   Do you like to continue? (y/n)
   ```

5. To start the database configuration, type `y`.
6. Type the database type. You can configure a Postgres, Oracle, or Microsoft SQL server. For Installing Oracle drivers, see *Installing an Oracle driver*.
7. If you select the MSSQL database, do the following:
   a. The system displays the following message `Do you want to enable the POM Geo configuration? Please select(y/n)`, type `y` to enable Geo-redundancy.

      If you enable Geo-redundancy, the POM UI displays the Data Server configuration page. For details, see *Using Proactive Outreach Manager*.

   b. Type the Availability Group Listener DSN name.
   c. For all other databases, type the database server IP address or host name.
8. Type the port number.

   The default port is 5432 for Postgres database, 1521 for Oracle database, and 1433 for Microsoft SQL Server.
9. Type the name of the database.
10. Type the name of the operational database.
11. Type the user name and password to connect to the database.

Note:

To configure the Microsoft SQL Server database as a secured connection, type the host name or FQDN of the database server.

The system displays the following message after the database connection is created:

```
Please select from one of the following choices:
1. Test DB connection
2. Create POM schema on the given database
3. Save this configuration in the PIMHibernate.cfg.xml file.
4. Reconfigure database settings
5. Exit from this utility
```

12. **(Optional)** Type `1` to verify the database connection.

    If the command returns `SUCCESS`, go to the next step.

    If the command returns `FAILURE`, the system displays the reason for failure on the console.

13. To create a POM schema on the specified database, type `2`

    The system displays the following message:

    ```
    Do you want to save the values on the config file(y/n)?
    ```

    To save the values in the configuration file, type `y`. If you type `n`, then it creates the POM schema. You cannot use the database immediately, unless you save this configuration by using option 3 in STEP 11 because EPM restarts after you save the configuration.

14. To reconfigure the settings, such as changing the login credentials, the type of the database, the server IP address or the host name, or the port number, type `4`.

15. To exit, type `5`.

    Caution:

    Ensure that the POM and VPMS services are not running before you restart your database.

Configuring the POM server

About this task

POM runs with both the primary and the auxiliary EPM. Use this procedure to configure the POM server on the primary EPM and perform similar steps for auxiliary servers.

Before you begin

Avaya Aura® Experience Portal uses Network Time Protocol (NTP) to control and synchronize the clocks when the EPM, POM software, and POM database are running on different servers. The POM database server and the primary EPM refer to the same time source to sync with each other. The auxiliary EPM can point to the primary EPM as a reference clock. The time and the time zones on all systems must be the same.

Procedure

1. Log in to the web interface by using Avaya Aura® Experience Portal administrator credentials. The Avaya Aura® Experience Portal administrator role inherits all POM specific roles.
2. In the navigation pane, click **POM** > **POM Home**.
3. Click **Configurations** > **POM Trusted Certificates**, and do the following:
   a. To fetch a Avaya Aura® Experience Portal certificate, click **Fetch**.
   b. In the **Name** field, type the unique name of a EPM certificate.
   c. In the **Location** field, type `https://<EPM IP Address>`.
   d. Click **Continue**.

      The system adds the Avaya Aura® Experience Portal certificate .
4. Click **Configurations** > **POM Servers**, and do the following:
   a. To add the POM server, click **Add**.
   b. Type the POM server name and IP address.

      After you configure the POM server, you can change the IP address of the POM server. For more information, see *Using Proactive Outreach Manager*.
   c. Click **Continue**.
   d. Select the **Trust this certificate** check box.
   e. Click **Save**.
5. Click **Configurations** > **POM Servers** > **Outbound Settings** > **EPM** and provide the user name and password with Outcall privileges.
6. Click **Save**.
7. To start POM Manager, do one of the following:
   - In the command line interface, type `/sbin/service POM start`.
   - Click **Configurations** > **POM Servers** > **POM Manager**.
8. If you have enabled Geo-redundancy, do the following:
   a. Click **POM Home** > **Data Center Configuration** .
   b. Click **Add**.

      The system displays the Add data center group page.

c. In the **Group Name** field, type the name of the data center.

d. Select the **Active** or **Standby** for the **Mode** button.

e. Click **Save**.

You can add only one active data center.

Configuring the POM server after enabling geo-redundancy

Procedure

1. Log on to Avaya Aura® Experience Portal by using the credentials of an administrator.
2. In the navigation pane, click **POM** > **POM Home**.
3. Click **Configurations** > **Data Center Configuration**.
4. Click **Add**.

   The system displays the Add data center group page.
5. In the **Group Name** field, type the name of a data center.
6. In the **Mode** field, click one of the following:
   - Click **Active** to configure the selected data center as an active data centre. You can configure only one active data center.
   - Click **Standby** to configure the selected data center as a standby data centre.
7. Click **Save**.

Configuring the applications and licenses

Before you begin

If you are using an external application server, ensure that you install Java 1.8.0_121 and tomcat version 8.5.11 and later.

Procedure

1. Log in to EPM using the user name and password provided during the Avaya Aura® Experience Portal installation.
2. To configure the applications on primary or auxiliary EPM using the web interface, in the left pane, click **System Configuration** > **Applications**. All application names, except

PomDriverApp and Nailer, are case-sensitive. You must spell the application names exactly as follows:

a. PomDriverApp: *https://<application server ip>:port-number-configured-on-application-server/PomDriverApp/ccxml/start.jsp* where the application type is POM:Driver, Enable TTS, Outbound Type

b. Nailer:*https://<application server ip>:port-number-configured-on-application-server/Nailer/ccxml/start.jsp* Application Type= POM:Nailer, Outbound Type

c. AvayaPOMNotifier: *https://<application server ip>:port-number-configured-on-application-server/AvayaPOMNotifier/Start* Application Type = POM:Application/VXML, Outbound Type

d. AvayaPOMAnnouncement: *https://<application server ip>:port-number-configured-on-application-server/AvayaPOMAnnouncement/Start* Application Type = POM:Application/VXML, Outbound Type

e. AvayaPOMAgent: *https://<application server ip>:port-number-configured-on-application-server/AvayaPOMAgent/Start* Application Type = POM:Application/VXML, Outbound Type

f. AvayaPOMSMS: *https://<application server ip>:port-number-configured-on-application-server/AvayaPOMSMS/Start* Application Type = SMS, Inbound Type

g. AvayaPOMEmail: *https://<application server ip>:port-number-configured-on-application-server/AvayaPOMEmail/Start* Application Type = Email, Inbound Type

Note:

You must configure at least one application with the name Nailer and PomDriverApp respectively with POM:Nailer and POM:Driver type.

For a multi zone setup, configure minimum one nailer application and one driver application on a POM system for the each zone.

For an organization enabled system, you must configure both the `Nailer` and `PomDriverApp` applications for the default organization for each zone.

Each organization in the zone must have the same **URI** because POM supports only one application server in one zone.

3. The following steps are to configure the Avaya Aura® Orchestration Designer applications *only* on primary EPM using the `$POM_HOME/bin/insert_POM_Apps.sh` script. This step is not applicable for configuring auxiliary EPM setup. In case, the application server is local to EPM, then the IP of aux hosting the application server must be mentioned as alternate IP in the applications configuration.

   a. Login to command line interface using root credentials.

   b. Type `cd $POM_HOME/bin`.

   c. Type `./insert_POM_Apps.sh`

   d. Type the EPM web administrator user name.

e. Type the EPM web administrator password.

f. Reenter the password for verification.

g. Type the IP address of the EPM application server on which the Avaya Aura® Orchestration Designer applications are installed.

h. On web user interface click **System Configurations** > **Applications** to verify the applications added by Avaya Aura® Experience Portal.

i. Select **PomDriverApp**, and from the Speech Servers option, select the TTS resource.

4. If you use an external application server, do the following:

   a. Copy the `*.war` files from *$POM_HOME/DDapps* to *$CATALINA_HOME/webapps* of the application server.

   b. Copy files from *$POM_HOME/DDapps/lib/** to *$CATALINA_HOME/lib* of the application server.

   c. Edit `<APPSERVER_HOME>/conf/server.xml` and add the following connector node:

```
<Connector protocol="HTTP/1.1" port="7443" minSpareThreads="5"
maxSpareThreads="75" enableLookups="true" disableUploadTimeout="true"
acceptCount="100"  maxThreads="200" scheme="https" secure="true"
SSLEnabled="true" keystoreFile="/opt/AppServer/Tomcat/tomcat/conf/
myTrustStore" keystorePass="changeit" clientAuth="false"
sslEnabledProtocols="TLSv1.2"
ciphers="TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_C
BC_SHA384,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
384,TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384,TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,TLS_
ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_ECDH_ECDSA_WI
TH_AES_256_CBC_SHA,TLS_ECDH_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256
_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SH
A256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,TL
S_ECDH_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256,TLS
_DHE_RSA_WITH_AES_128_CBC_SHA256,TLS_DHE_DSS_WITH_AES_128_CBC_SHA256,TLS_ECDH
E_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_
AES_128_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDH_RSA_WITH_AES_128
_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_128_CBC_SHA,TL
S_EMPTY_RENEGOTIATION_INFO_SCSV"/>
```

   d. Edit `<APPSERVER_HOME>/bin/catalina.sh` file to append the *JAVA_OPTS* variable `export JAVA_OPTS="$JAVA_OPTS -Dorg.xsocket.connection.client.ssl.sslengine.enabledProtocols=TLSv1.2″`. If it is not defined, then declare new *JAVA_OPTS* variable `export JAVA_OPTS="-Dorg.xsocket.connection.client.ssl.sslengine.enabledProtocols=TLSv1.2"`

5. Restart the external application server.

6. Use Avaya WebLM to configure the license information for POM. Configure licenses for the following three channels:

   - SMS channel: Sends SMS using Short Message Peer-Peer Protocol (SMPP). Ensure you have an SMS channel configured license on Avaya Aura® Experience Portal.

- Email channel: Sends email messages using Simple Mail Transfer Protocol (SMTP). Ensure you have an email channel configured license on Avaya Aura® Experience Portal.
- Voice and video channel: Assigns various Avaya Aura® Orchestration Designer applications for live voice or answering machine as part of the contact strategy.

7. Specify the host name or IP address of the License Server with the port number on Avaya Aura® Experience Portal. The administrator allocates licenses for telephony ports, ASR, and TTS connections.

Configuring POM certificates

For internal and external communications, POM uses digital certificates. Through these certificates, POM communicates with dependent components such as Experience Portal, Axis2, and application server.

The following are the requirements of a custom certificate:

- User certificate
- Private key of the user certificate
- Certificate Authority (CA) certificate that you used to sign the user certificate

The formats of the user certificate and CA certificate are `.pem (x509)`, `.crt`, or `.der`. However, the certificate vendor might also provide the user certificate and private key in PKCS12 format.

The following are the two methods to use certificates in POM:

- Generating self-signed certificates by using the built-in utility.
- Importing custom certificates from a trusted certificate provider.

The following table lists the locations where POM stores certificates:

Location	Description
`$POM_HOME/config/pomKeyStore`	The location to store the user certificate and the private key of the user certificate. When POM serves as a client, it uses the certificate stored in this location for the intended server.
`$POM_HOME/config/pomTrustStore`	The location to store the CA certificates of all trusted CAs. When POM serves as a server, it uses the certificates stored in this location to validate the client certificate.

After creating, adding, or exchanging the certificates, you must restart Experience Portal Management System and POM services.

Generating a self-signed certificate

About this task

Use this procedure to generate a self-signed certificate by using the internal utilities that POM provide.

Procedure

1. Log in to the primary EPM as a root or sroot user.
2. Type `cd $POM_HOME/bin` and press **Enter**.
3. Type `./pomCertificateGenerate.sh` and press **Enter**.

   The system displays the following message:

```
------------- Started ------------
Generating a 2048 bit RSA private key
.............+++
.....................................................................
.....................................................+++
writing new private key to '/tmp/pim.key'
-----
Return value: 0
Generated Certificate:
Owner: CN=pomdev7391, O=Avaya, OU=POM
Issuer: CN=pomdev7391, O=Avaya, OU=POM
Serial number: 87f831e773e71be9
Valid from: Wed Jan 11 13:57:45 IST 2017 until: Sat Jan 09
13:57:45 IST 2027
Certificate fingerprints:
         MD5:  CA:52:D8:06:FE:A9:59:84:69:FD:3E:78:40:54:EB:D8
         SHA1: 10:B2:44:9E:A8:13:50:A9:1C:3C:CF:2A:
1B:CC:F3:16:FC:D2:0D:54
         SHA256: 41:E8:4A:7C:44:9E:3B:6F:4B:B5:87:7A:EA:
82:32:49:6D:3E:40:34:91:05:7E:45:F4:41:86:CD:83:63:CB:98
         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

#1: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 4D 88 74 4B CF F2 BE 2A   FC 62 CD C6 46 41 08 54
M.tK...*.b..FA.T
0010: 8A 64 12 B5                                        .d..
]
]

#2: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
```

```
  CA:true
  PathLen:2147483647
]

#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 4D 88 74 4B CF F2 BE 2A   FC 62 CD C6 46 41 08 54
M.tK...*.b..FA.T
0010: 8A 64 12 B5                                        .d..
]
]

Return value: 0
Result of keyfile copy: 0
Result of cert copy 1: 0
/opt/Avaya/avpom/POManager/bin/pomCertificateInstall.sh: Returning
0
/usr/java/default/bin/java
Existing entry alias pomservercert exists, overwrite? [no]:
```

4. Type `yes` and press **Enter**.

   A new CA certificate and its private key are generated and added to `pomKeyStore`. You can use the CA certificate as the user certificate.

   If you do not want to use the CA certificate as the user certificate, you can generate your own CA certificate and self-signed certificate by using openssl commands or any other method.

5. Perform the post execution steps.

Importing a CA-signed custom certificate

About this task

Use this procedure to import a CA-signed certificate and replace the existing POM certificate.

About this task

The formats of the user certificate and private key of the user certificate can be in raw formats. Therefore, you must convert them in PKCS12 format.

Procedure

1. Log in to the primary EPM as a root or sroot user.
2. Type `cd $POM_HOME/bin` and press **Enter**.
3. Type `./pomCertificateImport.sh` *<newcert.p12>* *<password_of_newcert.p12>* and press **Enter**.

Where,

- *<newcert.p12>* is the name of the certificate file.
- *<password_of_newcert.p12>* is the password of the certificate file.

The system displays the following message:

```
[sroot@pomdev7391 bin]# ./pomCertificateImport.sh  ~craft/
rootCA.p12 ASDzqxw123
POM Certificate Import is started on date=Wed Jan 11 14:18:17 IST
2017
------------ Started ------------
MAC verified OK
MAC verified OK
MAC verified OK
Result of keyfile copy: 0
Result of cert copy 1: 0
/opt/Avaya/avpom/POManager/bin/pomCertificateInstall.sh: Returning
0
/usr/java/default/bin/java
Existing entry alias pomservercert exists, overwrite? [no]:
```

4. Type `Yes` and press **Enter**.

   The system displays the following message:

   ```
   Entry for alias pomservercert successfully imported.
   Import command completed:  1 entries successfully imported, 0
   entries failed or cancelled
   MAC verified OK
   ./pomCertificateImport.sh: Returning 0
   POM Certificate Import and Installation is completed on date=Wed
   Jan 11 14:18:22 IST 2017
   ------------ COMPLETED ------------
   ```

5. Add the CA certificate to `pomTrustStore`.
6. Perform the post execution steps.

Post execution steps

Procedure

1. Log in to the Avaya Aura® Experience Portal web console with the administrator credentials.
2. In the navigation pane, click, **EPMS** > **POM Home** > **Configurations** > **POM Servers**.
3. On the POM Servers page, click the **POM** server link.
4. To fetch the certificate, on the Edit POM Server page, click **Apply**.
5. Select the **Trust the certificate** check box.
6. Click **Save**.

7. On the POM Server page, click **Export** and save the certificate on your local system.

   Note:

   If you have multiple POM servers, you must export and save all the changed POM certificates.

8. In the navigation pane, click **Certificates**.
9. Add/replace the existing POM certificate.
10. Click **Save**.

Adding the POM certificate to the application server

About this task

Use this procedure to add the POM certificate to the application server

Procedure

1. If you added the certificate by using the self-signed method, do the following to download the CA certificate:
   a. Log in to the Avaya Aura® Experience Portal web console of the primary EPM.
   b. In the navigation pane, click **POM** > **POM Home**.
   c. Click **Configurations** > **POM Servers**.
   d. On the POM Servers page, click the **Export** link for the POM server.

      Ensure that you click the link for the POM server for which you want to download the CA certificate.

   e. Save the certificate.
2. If you added the certificate by using the custom certificates method, do the following:
   a. Log in to the application server.
   b. Go to **Certificates**.
   c. Click **Add**.
   d. Enter an alias name.
   e. Browse and select the `cacert.pem` certificate from your local machine.

      The `cacert.pem` certificate is already available in your local machine.

   f. Click **Continue**.

Configuring the certificate for POM SDK

About this task

If you are using the POM SDK client, the certificate exchange is the primary requirement for a successful communication with POM. Therefore, you must import the root CA certificate in the POM server. The root CA certificate is used to sign the certificate of the SDK client.

Before you begin

Copy the CA certificate to your local machine.

Procedure

1. Log in to the Avaya Aura® Experience Portal web console of the primary EPM.
2. In the navigation pane, click **POM** > **POM Home**.
3. Click **Configurations** > **POM Trusted Certificates**.
4. On the POM Trusted Certificates page, click **Import**.
5. On the Add Certificates page, do the following:
   a. In the **Name** field, enter a name for the certificate.
   b. Browse and select the CA certificate.
   c. Click **Continue**.

Exchanging and configuring certificates

About this task

Use this procedure to exchange and configure certificates for Avaya Aura® Orchestration Designer on a single or multiple application servers.

Important:

For multiple application servers, repeat all steps for each application server.

Before you begin

Configure the POM database.

Procedure

1. Using the browser window, log in to the EPM as an administrator.

   Note:

   For multiple POM servers, log in to the primary EPM.

2. In the navigation pane, click **Security** > **Certificates**.

3. On the **Root Certificates** tab, click **Export**, and then save the certificate on the local system.
4. In the navigation pane, click **POM** > **POM Home**.
5. Click **Configurations** > **POM Servers**.
6. Click **Export** on the listed certificate tab and save it on your local system.

   Note:

   For multiple POM servers, you must export and save all the POM certificates.
7. If you are using external application server, install the Avaya Aura® Orchestration Designer application server on the same server where you install POM. In such cases the IP address of the application server and the IP address of the EPM primary server is the same. The default port is 7443. while installing POM, you must:
   a. Copy the `*.war` files from `$POM_HOME/DDapps` to `$APPSERVER_HOME/webapps` of the external application server.
   b. Copy files from `$POM_HOME/DDapps/lib/*` to `$APPSERVER_HOME/lib` of your external application server. After copying the files, edit `$APPSERVER_HOME/conf/server.xml` and add the following:

```
<Connector protocol="HTTP/1.1"
port="7443" minSpareThreads="5" maxSpareThreads="75"
enableLookups="true" disableUploadTimeout="true"
acceptCount="100"  maxThreads="200"
scheme="https" secure="true" SSLEnabled="true"
keystoreFile="/opt/AppServer/Tomcat/tomcat/conf/myTrustStore"
keystorePass="changeit"
clientAuth="false" sslEnabledProtocols="TLSv1.2"
ciphers="TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_C
BC_SHA384,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
384,TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384,TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,TLS_
ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_ECDH_ECDSA_WI
TH_AES_256_CBC_SHA,TLS_ECDH_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256
_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SH
A256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,TL
S_ECDH_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256,TLS
_DHE_RSA_WITH_AES_128_CBC_SHA256,TLS_DHE_DSS_WITH_AES_128_CBC_SHA256,TLS_ECDH
E_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_
AES_128_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDH_RSA_WITH_AES_128
_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_128_CBC_SHA,TL
S_EMPTY_RENEGOTIATION_INFO_SCSV"/>
```

   c. In the Command Line Interface (CLI), navigate to `$APPSERVER_HOME/conf`.
   d. Run the command **`keytool -keystore myTrustStore -genkey -alias dummy`**.
   e. Type the password as `changeit` and type of other appropriate details.
   f. Restart the external application server.
8. Using the browser window, log in to the Avaya Aura® Orchestration Designer application server by specifying the URL *https://<application server IP address>:port number/runtimeconfig* using the default user name and the password as *ddadmin.* .

The system prompts to set runtimeconfig password at the first login to the local application server.

9. On the Avaya Aura® Orchestration Designer web interface, do the following:
   a. In the navigation pane, Click **Certificates**.
   b. On the Certificates page, select the default certificate and click **Delete**.
   c. Click **Change**.

      The system displays Change Keystore page.
   d. In the `Ketstore Path` field, type *`Absolute-path appserver-home>/conf/myTrustStore`*.

      If you have installed the application server on the same server where you install POM, then the *<Absolute-path-appserver-home>* is set in the *{$APPSERVER_HOME}* environmental variable.
   e. In the **Password** field, type `changeit`.

      Note:

      To use a different trust store and the password, change the *Absolute-path-appserver-home>/conf/server.xml* file accordingly, and ensure that the *server.xml* keystore path is valid and matches with Avaya Aura® Orchestration Designer application certificate as *<Absolute-pathappserver-home>/conf/myTrustStore.*
   f. In the **Confirm** field, type `changeit`.
   g. Click **Save**.
   h. On the Certificates page, click **Generate**.
   i. Enter the appropriate values in all fields. Input for all fields is mandatory. You can enter any custom defined values.

      Note:

      For SAN field, enter the values in the `IP:<IP address> or DNS:<hostname>` format.

      The self-signed certificate is valid only for 1186 days.
   j. Click **Continue**.

      The system displays the Certificates page.
   k. Click **Save**.
   l. Click **Add**.

      The system displays the Add Certificate page.
   m. Type a name for the EPM certificate and browse to find the path where you saved the primary EPM root certificate exported in step 3.
   n. Click **Continue**.

The system displays the Certificates page.

o. Click **Save**.

p. Select the application server self-signed certificate generated and export the certificate on your local system.

q. Click **Fetch** to fetch the axis2 certificate for primary EPM.

The system displays the Add Certificate page.

Note:

In a multiple POM server environment, you must fetch the axis2 certificate from all auxiliary EPM servers.

r. In the **Name** field, type the name of the certificate. For example, axis_prim or axis_aux.

s. In the **Enter Certificate Path** field, type the client URL as *https://<EPM IP address>/axis2*

The Avaya Aura® Orchestration Designer application fetches the axis2 certificate and adds it to the list of certificates.

t. Click **Continue**.

The system displays the Certificates page.

u. Click **Save**.

a. Click **Add**.

The system displays the **Add Certificate** page.

b. In the **Name** field, type a name of the POM certificate.

c. In the **Enter Certificate path** field, click **Browse** and browse the path where you saved the certificate exported in the step 6.

d. Click **Continue**.

The system displays the Certificates page.

e. Click **Save**.

f. Restart the application server.

10. Using the browser window, log in to the primary EPM as administrator.
11. Click **Security** > **Certificates**.
12. Click the **Trusted Certificates** tab and do the following:

a. Click **Upload**.

b. On the Upload Trusted Certificate page, type the name and browse the path where you saved the exported Avaya Aura® Orchestration Designer certificate.

c. Click **Continue**.

The system displays the Certificates page.

d. Click **Save**.

e. Click **Import**.

The system displays the Import Trusted Certificate page.

f. On the Import Trusted Certificate page, type the name and type the axis2 certificate path as *https://<EPM Server IP address>/axis2*.

For a multiple POM server environment, you must fetch the axis2 certificate from all auxiliary EPM servers.

g. Click **Continue**.

The system displays the Certificates page.

h. Click **Save**.

13. Restart the application server, all MPPs, and all auxiliary servers.

Checking the POM server installation status on primary and auxiliary server

Before you begin

Configure at least one POM server.

Procedure

1. Log in to EPM as an administrator.
2. In the left pane, select **POM > POM Home**.
3. In the drop-down menu, click **Configurations > POM Servers > POM Manager**.
4. Check whether the status of POM Campaign Manager is Running.
5. Log in to the CLI of the EPM as a root user.
6. Type `/sbin/service POM status`. Ensure this command returns a confirmation that the Campaign Manager, Campaign Director, Agent Manager and Rule Engine are running successfully.

   The POM service is a wrapper service around the Campaign Manager and Campaign Director. You can start and stop or get the status of these services.

   - To start, stop, and get the status of the POM Manager, type:
     - `/sbin/service POM start`
     - `/sbin/service POM stop`
     - `/sbin/service POM status`

On the command prompt, type the following commands to start, stop, or get the status of the services.

- To start, stop, and get the status of the Campaign Manager service, type:
  - `/sbin/service cmpmgr start`
  - `/sbin/service cmpmgr stop`
  - `/sbin/service cmpmgr status`
- To start, stop, and get the status of the Campaign Director service, type:
  - `/sbin/service cmpdir start`
  - `/sbin/service cmpdir stop`
  - `/sbin/service cmpdir status`
- To start, stop and get the status of the Agent Manager, type:
  - `/sbin/service agtmgr start`
  - `/sbin/service agtmgr stop`
  - `/sbin/service agtmgr status`
- To start, stop and get the status of the Active MQ, type:
  - `/sbin/service pomactmq start`
  - `/sbin/service pomactmq stop`
  - `/sbin/service pomactmq status`
- To start, stop and get the status of the Rule Engine, type:
  - `/sbin/service ruleng start`
  - `/sbin/service ruleng stop`
  - `/sbin/service ruleng status`

Next steps

Add users on the POM system.

Adding users to the POM system

Before you begin

Check the POM installation status.

About this task

By default, the Avaya Aura® Experience Portal administrator has all POM privileges. The administrator can add new users in the same manner as in Avaya Aura® Experience Portal.

Procedure

1. In the navigation pane, click **User Management** > **Users**. You can add a new user or assign the following POM administration privileges to a user:
   - POM Administration
   - POM Campaign Manager
   - Org POM Campaign Manager

     Note:

     Org POM Campaign Manager privilege is available only if organizations are enabled on Avaya Aura® Experience Portal.
   - POM Supervisor
   - Org POM Supervisor
2. Log off and log in with the user credentials that you created.

   This action ensures that the changes are in effect.

   When you assign the POM administration privileges, you can view the POM menu options in the left pane of EPM.

   If you install the POM database schema on an Oracle database, you must install the latest Oracle driver.

   Create and run campaigns. For more information, see *Using Proactive Outreach Manager*.

Changing the HOME country setting

Procedure

1. In the navigation pane of Experience Portal, click **POM Home** > **Configurations** > **Global Configurations**.
2. Change the **Home Country** property value.
3. Click **Apply** to save the changed property value.

Installing an Oracle driver

To configure the POM database on Oracle, you must download the Oracle driver `ojdbc6_g.jar` file from http://www.oracle.com and install the Oracle driver on the POM system.

You must download and install the Oracle driver for Avaya Aura® Experience Portal before installing the Oracle driver for POM 3.x. For more information about downloading and installing the Oracle driver for Avaya Aura® Experience Portal, see the *Implementing Avaya Aura® Experience*

Portal on a single server and *Implementing Avaya Aura® Experience Portal on multiple servers* or *Upgrading to Avaya Aura Experience Portal* from Support site at http://support.avaya.com.

For installing the Oracle driver for POM 3.x, perform the following procedure:

Note:

If you have a multiple POM server environment, you must install the Oracle drivers on all auxiliary POM servers.

Before you begin

1. Add at least one user with POM-specific privileges.
2. Install the Oracle driver to configure the POM database schema on the Oracle database or to use Oracle database as a contact data source.

Procedure

1. Download the `ojdbc6_g.jar` Oracle driver from http://www.oracle.com.
2. Log in to Linux on the EPM server as a user with root or sroot privileges.
3. Create a folder `~/POMOracleJDBC` by running the command: `mkdir –p ~/POMOracleJDBC`.
4. Copy the driver files `ojdbc6_g.jar` to the folder `~/POMOracleJDBC`.
5. Install the JDBC driver by typing `bash $POM_HOME/bin/InstallPOMOracleJDBC.sh`.

   Important:

   Some web browsers change the file name extension of these files to `.zip`, when you download the files. In this case, rename the file to `ojdbc6_g.jar`.

   Keep the Oracle JDBC driver files in the folder `~/POMOracleJDBC` even after installing or upgrading Avaya Aura® Experience Portal. You need these files when you install or upgrade POM.

Provisioning a Kafka server

When you enable an event SDK feature on the system, POM stores the events at the following location:

`$POM_HOME/kafka_xxx/kafka-store`

POM generates around approximately 50GB of data per 1 million attempts. By default, POM keeps data of events of last 7 days in the `kafka-store` file.

You must provision disk space on the POM server.

To reduce the disk requirement, you must reduce both the retention period and the purge interval of the Kafka server.

By default, the retention period is 7 days (168 hours).

You can configure the retention period by setting the following properties in the following files:

File name	Property name
server.properties	`log.retention.hours` = *168*
zookeeper.properties	`autopurge.purgeInterval` = *168*

Chapter 7: POM trusted certificate management

Overview

You must use the POM Trusted Certificate Management web user interface page for the certificate management to ensure the secure communication between POM's internal and external components. Trust Management provides an identity to establish authenticated TLS sessions.

Using the **POM Certificate Management** page, you can do the following:

- View installed Trusted Certificates on the POM server.
- Add or remove Trusted Certificates on the POM server.
- Fetch https certificate for POM integrated components.
- Import a certificate for POM integrated components.

POM maintains all the configured certificates in `pomTruststore` file located at the `$POM_HOME/config` folder on the primary EPM server. In case of a multi-server installation, the system pushes all configured certificates to the POM servers. POM supports .cer, .pem, and der formats of the certificate.

You can use POM to configure the validity of an identity certificate of an Avaya product. You can set the certificate validity to maximum 1186 days.

Avaya products using digital certificates and supporting the generation of alarms enable an administrator to generate an alarm notification. An administrator can configure the system to generate an alarm sixty days before a digital certificate expires. By default, the system generates alarm notifications daily until the administrator stops them.

Note:

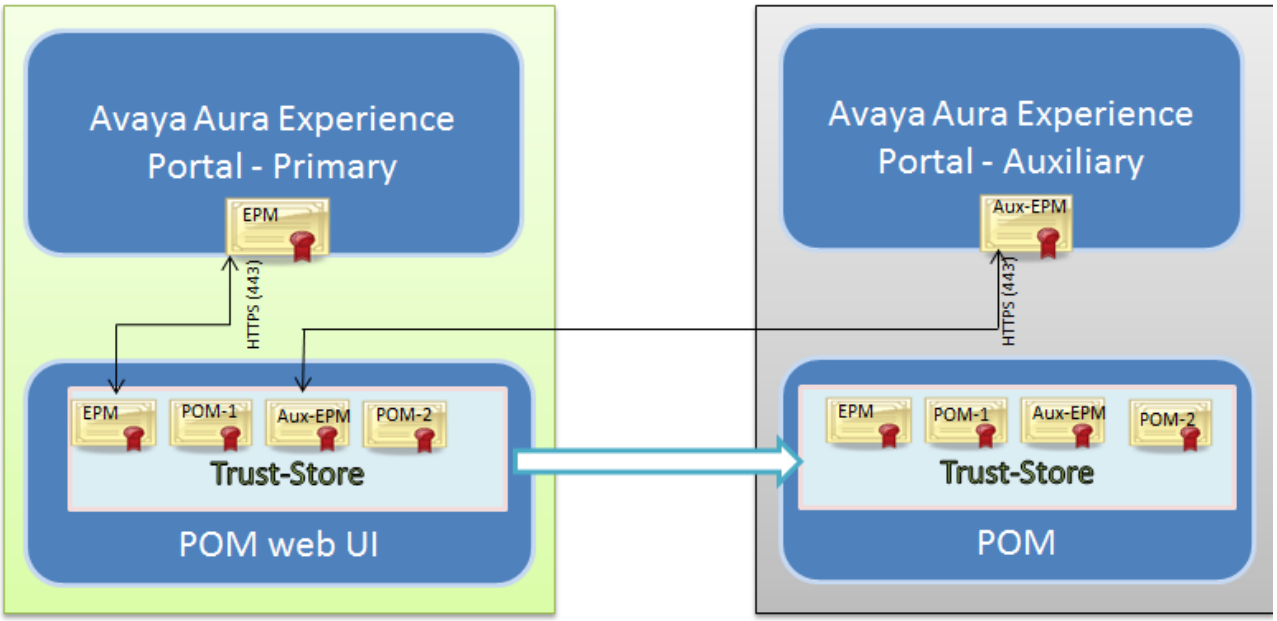
To sync with the primary `epm truststore` file, ensure that all the auxiliary server EPM service is up and running.

Warning:

You must restart the POM server after any modification.

POM integrates with Avaya Oceana™ Solution, Context Store, AES, and AACC. You must import or fetch respective certificates on the POM Trusted Certificate page. To add the POM server installed on the auxiliary EPM server, you must first fetch the auxiliary server's EPM certificate on the POM Trusted Certificate and then add the POM server.

The following diagram shows the multi POM setup containing primary Avaya Aura® Experience Portal and POM. EPM's certificate is fetched on the POM Trusted Certificate page.



Trust store management

Store Type	Purpose	Protocol	Note
pomTrustStore	Maintains the POM Trusted certificates	TLS	Path is `$POM_HOME/config`

POM Trusted Certificates page field description

Name	Description
Name	The name of the certificate.
Certificates	The detail text of the certificate. The system displays the following details of the certificate: • `Owner` • `Issuer` • `Serial Number` • `Signature Algorithm` • `Valid from — until` • `Certificate fingerprints`

Table continues…

Name	Description
	• Subject Alternative Names

Button	Description
Import	Click to import a new certificate.
Fetch	Click to fetch a new certificate
Delete	Click to delete one or more certificates from the list.

Adding trusted Certificate Authority certificates

About this task

You can import a trusted certificate either from the pem certificate file or from the https URL.

Procedure

1. Log in to the Avaya Aura® Experience Portal web console with the Administrator user role.
2. In the navigation pane, click **POM** > **POM Home**.
3. Click **Configurations** > **POM Trusted Certificates**.

   The system displays all the trusted certificates.
4. Click **import**, and do the following:
   a. Click **Browse** and locate the file on the local system.
   b. Click **Continue**.
5. To fetch the certificate, do the following:
   a. Click **Fetch**.
   b. Click **alias** and type the certificate URL with the https prefix.
   c. Click **Continue**.

Removing trusted Certificate Authority (CA) certificate

Procedure

1. Log in to the Avaya Aura® Experience Portal web console with the Administrator user role.
2. In the navigation pane, click **POM** > **POM Home**.
3. Click **Configurations** > **POM Trusted Certificates**.

   The system displays all the trusted certificates.

4. Select one or more certificates and click **Delete**.

Viewing trusted Certificate Authority (CA) certificates

Procedure

1. Log in to the Avaya Aura® Experience Portal web console with the Administrator user role.
2. In the navigation pane, click **POM** > **POM Home**.
3. Click **Configurations** > **POM Trusted Certificates**.

   The system displays all the trusted certificates.

Replacing Identity Certificates

About this task

Use this procedure to replace the installed self-signed certificate with the Certificate Authority (CA) signed third party certificate.

Procedure

1. Go to ssh command line under `$POM_HOME/bin` folder.
2. To import the new CA signed certificate, execute the shell script **`./pomCertificateImport.sh < pkcs12_cert_file complete path> < pkcs12_password >`**.
3. After importing the certificate successfully, do the following to fetch the new certificate entry on POM Servers page:
   a. Navigate to **POM Home** > **Configurations** > **POM Servers**.
   b. Click the **POM server** link.
   c. On the Edit POM Server page, click **Apply**.
   d. Select the **Trust Certificate** check box.
   e. Click **Save**.

      You must also update each Application server certificate and POM certificate. For more information on the certificate exchange, see the *Certificate Exchange* section.

      The system displays the new certificate in the list.
   f. For the new certificate to take effect, restart the POM and application server services.

Chapter 8: Troubleshooting tips

Primary or auxiliary EPM is not installed

The installer fails to detect either a primary or auxiliary EPM, and quits.

Proposed solution

Procedure

Install a primary or auxiliary EPM on the server. See *Avaya Aura® Experience Portal* documentation for installing primary or auxiliary EPM.

No license is allocated to secondary POM Server in multi POM set up

A license is not allocated to the auxiliary POM server in a multiple POM server setup.

Proposed solution

Procedure

1. Verify that the EPM is running and that the system accepts the certificate.

   If the auxiliary VPMS or EPM does not respond, follow the steps to reauthorize the primary VPMS or EPM from the auxiliary VPMS or EPM.
2. Login to the auxiliary VPMS or EPM as root or sroot.
3. Change the directory by entering `/opt/Avaya/VoicePortal/Support/VP-Tools/` command.
4. Type `setup_vpms.php` command.

Server error

Installation of Proactive Outreach Manager aborts as Proactive Outreach Manager server restarts.

Proposed solution

Procedure

1. Go to the bin directory by typing `cd $POM_HOME/bin`.
2. Type `./uninstallPOM.sh`.
3. If you do not find the bin directory, then go to the root directory by typing `cd`, followed by `rm -rf $POM_HOME`.

Database Name Error

Name of database does not exist

The database name is incorrect.

Proposed solution

Procedure

Verify the name of the database. You have to manually create the database before you try and establish a connection with the database.

Database Connection Error

Database Connection Attempt Failed

You cannot connect to the POM database.

Proposed solution

Procedure

Verify the host name or the IP address of the database server.

Failed to connect to the database

The system displays the following message:

```
FATAL: no pg_hba.conf entry for host "IP address", user "admin",
database "VoicePortal", SSL off
```

Proposed solution

Procedure

1. Enter the IP address of the database server in the `pg_hba.conf`, at the following location: `/var/lib/pgsql/data/pg_hba.conf`.
2. Provide valid server IP address of the server connecting to the database, port, user name, and password.

Database Password Error

Log in failed

You cannot login to the database.

Proposed solution

Procedure

Verify the password used for connecting to the database.

Database Port Number Error

Invalid port number

You cannot connect to the POM database, because the port number that you use to connect to the database is incorrect.

Proposed solution

Procedure

Verify the port number of the database connection. The default port number is 5432 for a PostgreSQL database, 1521 for an Oracle database, and 1433 for a Microsoft SQL server.

Database Type Error

Enter Oracle, Postgres, or Microsoft SQL Server as dbtype

You cannot connect to the database as database name is incorrect.

Proposed solution

Procedure

Verify you enter the correct name. The database type is case-sensitive and has to be entered as medial capital or camel case.

Database User Error

Database user does not exist

You are unable to connect to the POM database as the user name is incorrect.

Proposed solution

Procedure

Verify the user name you specify before you try to connect to the POM database.

Unsupported version of Avaya Aura® Experience Portal

If you try to install POM on an unsupported Avaya Aura® Experience Portal version, the installer quits.

Proposed solution

Procedure

Install the latest version of Avaya Aura® Experience Portal. See the *Implementing Avaya Aura® Experience Portal on a single server* and *Implementing Avaya Aura® Experience Portal on multiple servers* documentation for installation.

Installation Aborted Error

Proactive Outreach Manager is fully or partially installed

Installation quits.

Proposed solution

Procedure

Uninstall Proactive Outreach Manager.

User does not have sufficient privileges

The system displays this error message if the user name you provide while running `./installDB.sh` does not have sufficient privileges.

Proposed solution

Procedure

Ensure the user has the Create Table, and the Alter Table privileges.

Certificate Error

Condition

POM service displays the following error message:`|P_POMCM002|INFO|POMCM|||Out Call Web Service returned fault: Connection has been shut down: javax.net.ssl.SSLHandshakeException:`

```
sun.security.validator.ValidatorException: No trusted certificate found|
pomdev17388####.
```

Cause

The axis2/ EPM certificate not fetched on the POM trust store page.

Solution

1. Log in to the Avaya Aura® Experience Portal web console with the Administrator user role.
2. In the navigation pane, click **POM** > **POM Home**.
3. Click **Configurations** > **POM Trusted Certificates**.

   The system displays all the trusted certificates.
4. To fetch the certificate, do the following:
   a. Click **Fetch**.
   b. Click **alias** and type the certificate URL with the https prefix.
   c. Click **Continue**.
5. On the Certificates page, ensure that the certificate you fetched is listed.

POM truststore is corrupted or deleted

Condition

POM truststore is corrupted or deleted.

Solution

1. To re-create POM key store and trust store, do the following:
   a. Login to the Command Line Interface (CLI) with the root user.
   b. To change the directory path run the command **`cd $POM_HOME/bin`**.
   c. Run **`$POM_HOME/bin/pomCertKeystore.sh`**.
   d. To create a new pomTrustStore, make a copy POM key store with the name pomTrustStore.
   e. To empty the truststore, run the command **`keytool --delete -alias pomservercert -keystore $POM_HOME/config/pomTrustStore -storepass changeit`**.
2. To create a blank pomTrustStore, do the following:
   a. Login to the Command Line Interface (CLI) with the root user.
   b. Run the command **`openssl pkcs12 -export -name pomservercert -in $POM_HOME/web/pom_cert/pom.crt -inkey 164 $POM_HOME/web/pom_cert/pom.key -out $POM_HOME/config/pom.p12 -password pass:changeit`**.

c. Run **keytool -importkeystore -srckeystore $POM_HOME/config/pom.p12 -srcstoretype PKCS12 -srcstorepass changeit destkeystore $POM_HOME/config/pomTrustStore -deststorepass changeit**.

d. To empty the truststore, run the command **keytool --delete -alias pomservercert -keystore $POM_HOME/config/pomTrustStore -storepass changeit**.

Ensure that the pomKeyStore and pomTrustStore are case sensitive and must be located at `POM_HOME/config`.

Chapter 9: Uninstalling POM

Overview

Uninstalling POM does not uninstall the Avaya Aura® Experience Portal application server.

After you uninstall POM, the system deletes related service files. The details of the deleted service files are at `/PomUnInstall.log`.

Uninstalling POM

Procedure

1. Log on to the Avaya Aura® Experience Portal server by using the credentials of a root user.
2. On the Avaya Aura® Experience Portal server, open a command prompt window.
3. In the command prompt window, run the following command to navigate to the bin directory:

   ```
   cd $POM_HOME/bin
   ```

4. In the command prompt window, run the following command to uninstall POM:

   ```
   ./uninstallPOM.sh
   ```

   The system displays a dialog box to confirm the uninstallation.

   The system displays the following message:

   ```
   POM UNINSTALLATION complete. Please restart the system now!
   ```

5. In the command prompt window, run the following command to restart the Avaya Aura® Experience Portal server:

   ```
   reboot
   ```

6. On the POM Server page, select the related auxiliary POM server entry.
7. Click **Delete**.

Chapter 10: Geo-Redundancy

Geo-Redundancy overview

Geo-Redundancy is defined as having multiple deployments of the same product across multiple geographic locations for low production downtime. When an entire site fails, the other site can be used in to production to minimize the impact to the business. An individual site is referred to as a Data Center.

A site is a geographical location where you deploy POM. A site contains all the components on which POM depends. To leverage the benefits of Geo-Redundancy, you must deploy POM on more than one site.

For Geo-Redundancy, you must deploy the following sites:

- Active

  Specifies the production site.

- Standby

  Specifies the redundant site.

When a site fails because of power outage, network outage, or a natural calamity, the standby site is used for production. Geo-Redundancy ensures that the operations continue with a minimal impact. For Geo-Redundancy, the components or products on which POM depends must be in sync on all the Data Centers.

POM depends on the database for all its operations. POM supports Oracle, Postgres, and MSSQL databases. Geo-Redundancy in POM is only supported by the MSSQL database. POM uses the AlwaysOn feature of MSSQL database as a base for being Geo-Redundant.

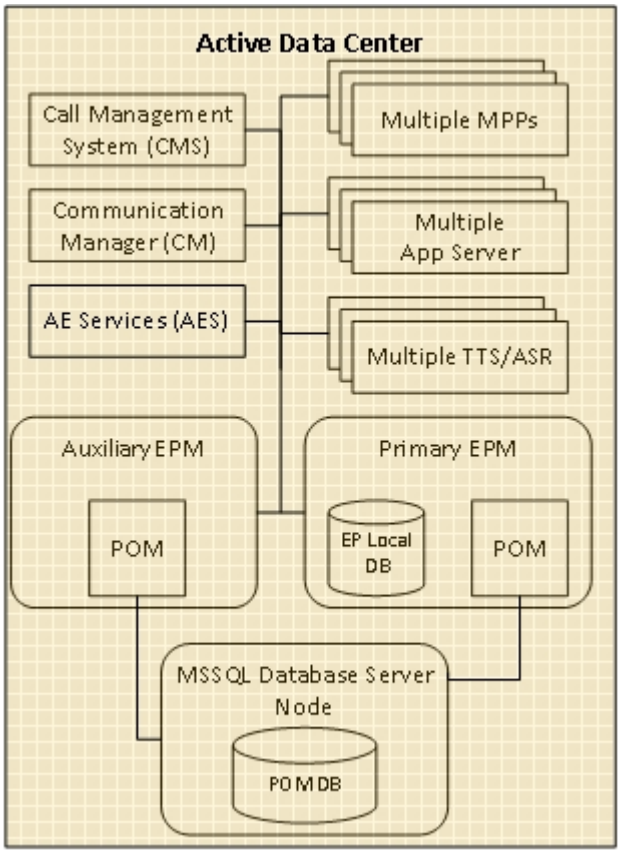
Experience Portal synchronization is required as POM is deployed on the Experience Portal platform. Organizations, zones, and users created on Experience Portal are stored in the local database of Experience Portal. There is no High Availability (HA) solution available to synchronize multiple Experience Portal servers deployed on multiple Data Centers. Therefore, you must manually create Experience Portal data on all Data Centers.

In dual Data Center configuration, Communication Manager is deployed along with Survival Core Server (ESS). Application Enablement Services is configured in Geo-Redundancy HA mode. Avaya Call Management System is deployed in HA mode.

You can only enable Geo-Redundancy when POM is installed in the CCElite mode.

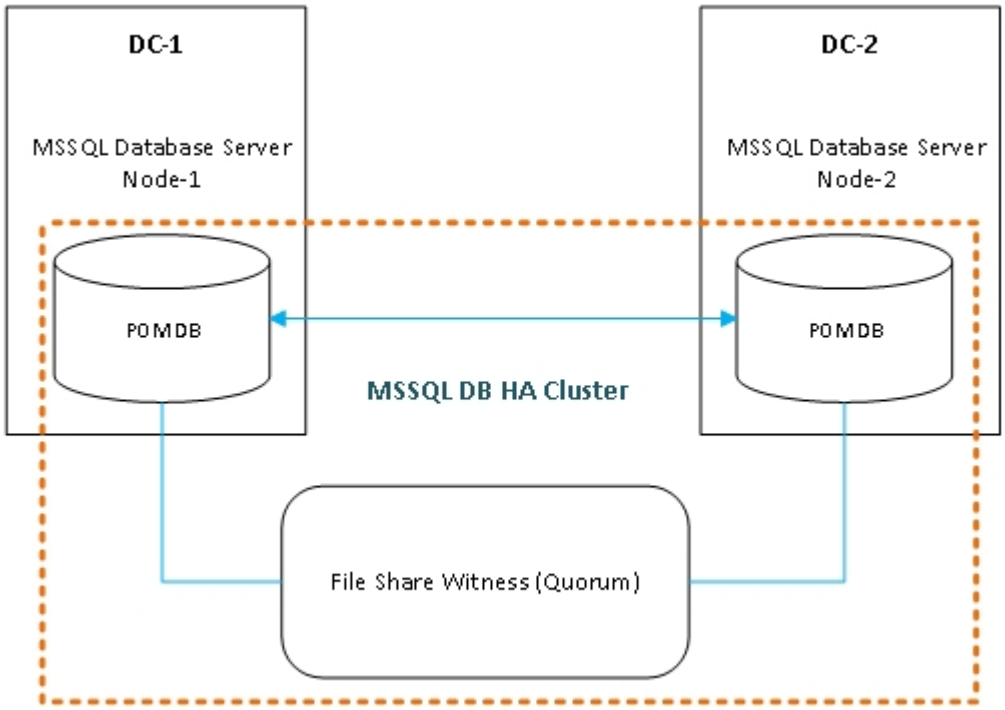
Architecture

Create a Data Center as shown in the following diagram.



POM depends on a database for all the activities. For Geo-Redundancy, the database must be highly available at both Data Centers. You must ensure databases at both the Data Centers are synchronized. MSSQL AlwaysOn is a High Availability (HA) feature of the database that is used for POM Geo-Redundancy.

A sample deployment is shown in the following diagram.



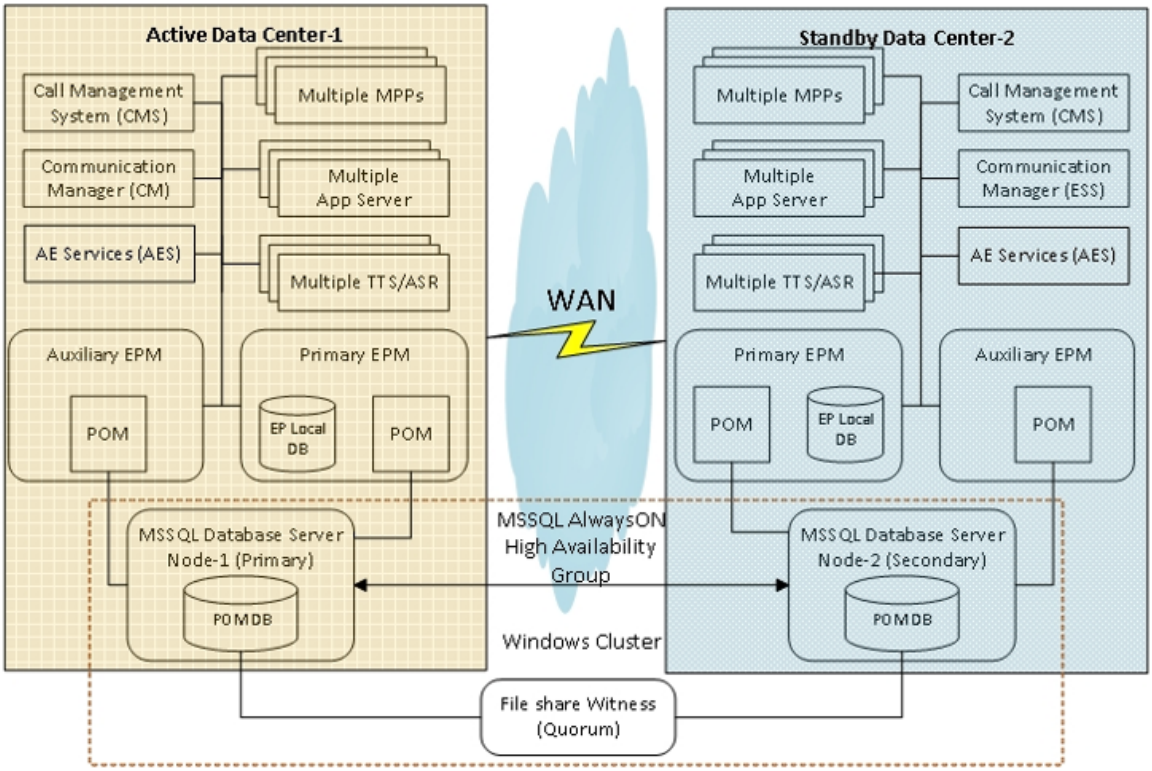
To install and configure MSSQL AlwaysOn, see the Microsoft documentation. It is the responsibility of the customer to setup and configure Windows Server Failover Cluster (WSFC) and the MSSQL AlwaysOn feature.

Customers must ensure that the primary instance of the MSSQL database is always on the active Data Center. This ensures that the database is always in close proximity to the POM server and there are no network latencies between POM server and the database. A File Share Witness is a file share available to all nodes in a High Availability (HA) cluster.

Deployment

To enable Geo-Redundancy, you need minimum two Data Centers where one Data Center is active and the other is standby. When the active Data Center fails, the standby Data Center can be made active and normal operations continue with minimal down time and impact.

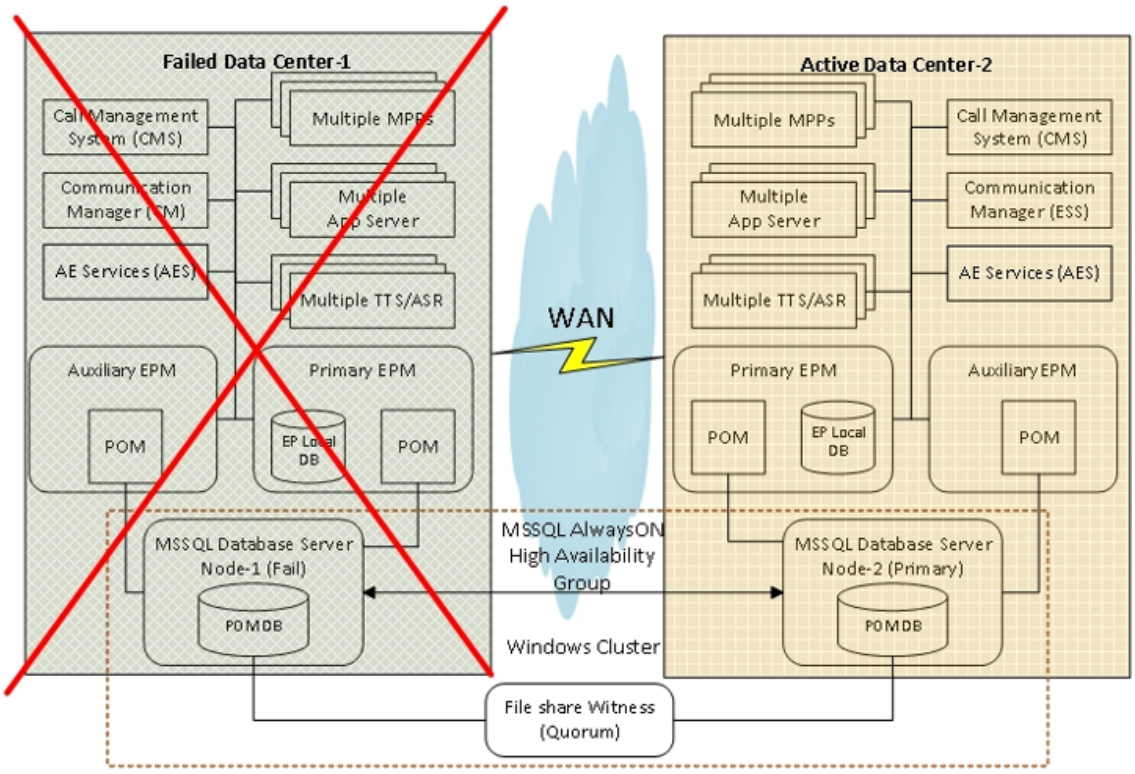
The following diagram is an example of two Data Centers configured for Geo-Redundancy.



The components shown in the diagram are for illustration purpose only. The actual Data Center can have many more components.

Campaigns run on the active Data Center-1. The POM server stores the data related to campaigns in the database. The MSSQL Database AlwaysOn feature replicates all the data from the active Data Center-1 to all the nodes of the MSSQL Database Server in Data Center-2. If a customer deploys the MSSQL Database node-3 instead of a File Share Witness, the data is also replicated to node-3.

When the active Data Center-1 fails, the standby Data Center-2 becomes active. POM services on the newly active Data Center-2 resume the services according to the data available in the new Primary Database node.



Node-2 deployed on Data Center-2 becomes Primary when Data Center-1 fails. The change of role of the database from secondary to primary does not require any manual intervention because the MSSQL database is configured for an automatic failover. The failover of POM services from Data Center-1 to Data Center-2 is a manual process.

Requirements

The following are the requirements for enabling Geo-Redundancy in POM:

- Install POM in the CCElite mode.
- Use MSSQL database version 2016 SP1 or 2014 SP2 and ensure that the database is pre-configured with its AlwaysOn feature and Automatic Failover.
- Ensure that the primary instance of the MSSQL database is on the active Data Center.
- Configure MSSQL Availability Group Listener.
- Ensure that the organizations, users, and zones available on Experience Portal in Data Center 1 are also created on Experience Portal in Data Center 2.
- Configure EPM in the ACTIVE-ACTIVE deployment and ensure that the licenses are configured on both sites.
- Configure Communication Manager in Data Center 1 with ESS server in Data Center 2.
- Configure Call Management System in the High Availability (HA) mode.

- Configure Application Enablement Services in the GRHA mode or ensure that Application Enablement Services is available in both data centers.

Experience Portal synchronization

POM is deployed on Experience Portal as a managed application. Organizations, zones, and users created on Experience Portal are stored in the local database of Experience Portal. When POM services start, this data is copied in to the POM database. The data created on Experience Portal of the active Data Center must also be manually created on Experience Portal of all the standby Data Centers to reduce the downtime during transition from active Data Center to standby Data Center.

Licensing

In a Geo-Redundancy setup, the requirement of licenses is doubled.

Example

- Standard POM setup:
  - Total number of licenses that you must acquire from the WebLM server = 1000.
- Geo-Redundancy POM setup:
  - Total number of licenses that you must acquire from the WebLM server for the active data center = 1000
  - Total number of licenses that you must acquire from the WebLM server for the standby data center = 1000

Enabling Geo-Redundancy for a new installation

About this task

Use this procedure on primary and auxiliary POM servers.

Before you begin

Each Data Center must contain all components on which POM depends.

Geo-Redundancy in POM can only be enabled with MSSQL database configured with the AlwaysOn feature. The MSSQL database high availability nodes configured with AlwaysOn must be located on different Data Centers that are intended to be configured for Geo-Redundancy. The POM database and Operational Database must be part of Availability Database and must be synchronized with all other database nodes.

For example, if two Data Centers are planned for configuring Geo-Redundancy, each Data Center must contain:

- Components such as Experience Portal, Communication Manager, Call Management System, Media Processing Platform, and System Manager.
- MSSQL Database with AlwaysOn feature, and high-availability node on another Data Center.
- MSSQL Availability Group Listener.

Procedure

1. Start the installation.
2. On the command prompt, do the following:
   a. For `Please select Contact Center Configuration mode from following options`, select `1 CCElite` and press **Enter**.
   b. For `Please enter the database configuration`, type `MSSQL` and press **Enter**.
   c. For `Do you want to enable the POM Geo configuration? Please select(y/n):`, type `y` and press **Enter**.
   d. For `FQDN of MSSQL Domain Controller`, type the domain name.
   e. For `Database Port`, type the port number of the database.
   f. For `Database Name`, type the name of the database.
   g. For `Operational Database Name`, type the name of the operational database.
   h. For `User`, type the name of the user.
   i. For `Password`, type the password.
   j. For `Does Database require secured connection (Y/N)`, type `Y`.
3. Choose the appropriate option to test the database connection.
4. **(Optional)** If the test succeeds, save the configuration.
5. Restart all POM services.
6. Verify if all POM services are started successfully.

Enabling Geo-Redundancy for an upgrade

About this task

Use this procedure on primary and auxiliary POM servers.

Procedure

1. Log in to the POM server as root user.

2. From the command prompt, type the following commands:

   cd $POM_HOME

   cd bin

   ./installDB.sh

3. On the command prompt, do the following:
   a. For `Please select Contact Center Configuration mode from following options`, select `1 CCElite` and press **Enter**.
   b. For `Please enter the database configuration`, type `MSSQL` and press **Enter**.
   c. For `Do you want to enable the POM Geo configuration? Please select(y/n):`, type `y` and press **Enter**.
   d. For `FQDN of MSSQL Domain Controller`, type the domain name.
   e. For `Database Port`, type the port number of the database.
   f. For `Database Name`, type the name of the database.
   g. For `Operational Database Name`, type the name of the operational database.
   h. For `User`, type the name of the user.
   i. For `Password`, type the password.
   j. For `Does Database require secured connection (Y/N)`, type `Y`.
4. Choose the appropriate option to test the database connection.
5. **(Optional)** If the test succeeds, save the configuration.
6. Restart all POM services.
7. Verify if all POM services are started successfully.

Configurations menu

On the POM Home page, the **Configurations** menu displays the following options:

- **Data Center Configuration**
- **POM Servers**
- **POM Trusted Certificates**

As the Geo-Redundancy is enabled, the Data Center is treated as standby until the POM server is configured to be part of a Data Center group and made active.

Adding a Data Center group

About this task

The primary POM server and the corresponding auxiliary POM servers must be configured for Geo-Redundancy. User must create Data Center groups on each site.

Procedure

1. Log in to the Avaya Aura® Experience Portal web console.
2. In the navigation pane, click **POM** > **POM Home**.
3. Click **Configurations** > **Data Center Configuration**.
4. Click **Add**.
5. Verify that the POM server of the current Data Center and all the configured auxiliary POM servers are listed in the Configure EPM Servers area.
6. In the **Group Name** field, type the name of the group.
7. Type the **EPM User Name** and **EPM Password** of all the POM servers listed in the Configure EPM Servers area.
8. Click **Save**.

   Repeat the procedure on POM servers in the other Data Centers for Geo-Redundancy. The Group Name as mentioned in step 6 must be unique for all the Data Centers. Ensure that the mode of all the Data Center Groups is set to **Standby**.

Deleting a Data Center group

Procedure

1. Log in to the Avaya Aura® Experience Portalweb console.
2. In the navigation pane, click **POM** > **POM Home**.
3. Click **Configurations** > **Data Center Configuration**.
4. Select the Data center group that you want to delete.
5. Click **Delete**.

Service Status

The user can see the status of POM services on the POM Manager page.

In an active Data Center, the status of the POM services on a single POM server in default zone are as follows:

Service	Status
Campaign Manager	RUNNING
Campaign Director	MASTER
Agent Manager	MASTER
ActiveMQ	MASTER
RuleServer	MASTER
Kafka Server	RUNNING

In a standby Data Center, the status of the services are as follows:

Service	Status
Campaign Manager	STOPPED
Campaign Director	STOPPED
Agent Manager	STOPPED
ActiveMQ	STOPPED
RuleServer	STOPPED
Kafka Server	RUNNING

Disabling Geo-Redundancy

About this task

To disable Geo-Redundancy for a Data Center that is part of Geo-Redundancy group, the Data center group created for that Data Center must be deleted first. Thereafter Geo-Redundancy can be disabled.

Procedure

1. Log in to the Avaya Aura® Experience Portal web console.
2. In the navigation pane, click **POM** > **POM Home**.
3. Click **Configurations** > **Data Center Configuration**.
4. Select the Data center group that you want to delete.
5. Click **Delete**.
6. Ensure that the Data Center group is deleted from the Data Center Configuration page.
7. Log in to the POM server as a *root* user.
8. From the command prompt, type the following commands:

   ```
   cd $POM_HOME
   cd bin
   ```

./installDB.sh

9. On the command prompt, do the following:
   a. For `Please select Contact Center Configuration mode from following options`, select `1 CCElite` and press **Enter**.
   b. For `Please enter the database configuration`, type `MSSQL` and press **Enter**.
   c. For `Do you want to enable the POM Geo configuration? Please select(y/n):`, type `n` and press **Enter**.
   d. For `FQDN of MSSQL Domain Controller`, type the domain name.
   e. For `Database Port`, type the port number of the database.
   f. For `Database Name`, type the name of the database.
   g. For `Operational Database Name`, type the name of the operational database.
   h. For `User`, type the name of the user.
   i. For `Password`, type the password.
   j. For `Does Database require secured connection (Y/N)`, type `Y`.
10. Choose the appropriate option to test the database connection.
11. **(Optional)** If the test succeeds, save the configuration.
12. To exit the `installDB.sh` script, select the option 5 and press **Enter**.

    POM servers of the Data Centers that are not part of the Geo-Redundancy Data Center group must use a different database. Repeat steps 7 through 9 and configure a different database than the database used for Geo-Redundancy.

Activating a Data Center

About this task

When all Data Center groups are created and are in the standby mode, the user must determine the Data Center that must go in to production. At one point of time, only one Data Center can be in production. Therefore, only one Data Center group can remain Active.

Procedure

1. Log in to the Avaya Aura® Experience Portal web console.
2. In the navigation pane, click **POM** > **POM Home**.
3. Click **Configurations** > **Data Center Configuration**.
4. Click the Data center group that you want to activate.

5. Set the **Mode** as `Active`.
6. Click **Save**.
7. Click **Configurations** > **POM Zone Configuration**.
8. In the CD Zone Configuration area, select the appropriate Campaign Director.
9. Click **Save and Apply**.
10. In the AM Zone Configuration area, select the appropriate Agent Manager.
11. Click **Save and Apply**.
12. Verify the status of POM services.
13. On the standby Data Center, do the following to stop the POM services:
    a. Log in to the POM server command line interface as a *root* user.
    b. On the command prompt, type the **`service POM stop`** command.

    Repeat these steps on all POM servers in standby Data Center.

Failover

Failover is a process of shifting operations from an Active Data Center to a Standby Data Center, when the active Data Center fails.

During regular system operations, POM updates the database with the information such as campaigns, records that are being dialed, and agent states. The AlwaysOn feature of the MSSQL database maintains the database of all the replicated nodes in synchronization. When the Data Center fails because of a power outage, network outage, or natural calamity, all of the servers in that Data Center are not reachable for a long period of time. POM server in the failed Data Center loses connectivity to the database and fails to record the details of the calls into the database or records partial information to the database.

The failover process involves making standby Data Center as active and restarting the services. The POM server on the standby Data Center resumes operations from the information available in the database after it is active. There can also be a planned maintenance activity on an active Data Center because of which operations are shifted to the standby Data Center. The business operations occur from a standby Data Center until the maintenance on the active Data Center is completed.

The failover to the standby Data Center is categorized as Planned-Failover or Unplanned-Failover, based on whether the active Data Center fails abruptly while in production, or an outage is planned for maintenance.

Data Center considerations

For failover to a standby Data Center, the standby Data Center must meet the requirements before shifting the operations from the active Data Center to the standby Data Center. All the data

created on the Experience Portal of the active Data Center must also be present on the standby Data Center before the failover. For example, data such as organizations, zones, and users. POM services must be in the Stopped state on all the POM servers of the standby Data Center before the failover.

Shifting to standby Data Center for a planned failover

About this task

A failover is called a Planned-Failover when an outage is planned for maintenance activities on an active Data Center. The operations must be shifted to the standby Data Center. Planned-Failover must be performed during maintenance hours. Thus, POM is non-operational.

A maintenance activity is planned on Data Center-1 because of which operations are required to be shifted to Data Center-2. The other components that are part of POM also failover to Data Center-2.

Before you begin

- Ensure that the agentless campaigns such as email and SMS notification are not running.
- Log-off all agents from the system.
- Stop all campaigns.

Procedure

1. Log in to the Avaya Aura® Experience Portal web console of the POM server of the active Data Center-1.
2. In the navigation pane, click **POM** > **POM Home**.
3. Click **Configurations** > **Data Center configuration**.
4. Select the currently active Data Center-1 and make it standby.
5. Click **Configurations** > **POM Servers** > **POM Manager**.
6. Verify that the status of all the services of the new standby Data Center-1 are as listed in the Service Status on page 74.
7. Log in to all the POM servers configured in Data Center-1 as a *root* user.
8. Stop the POM services.
9. From the MSSQL Database AlwaysOn Dashboard, click **Start Failover Wizard** on the top right corner of the page.
10. Set the database server in Data Center-2 as `Primary`.
11. Ensure that the AlwaysOn Dashboard displays the database node of the standby Data Center-2 as `Primary`.
12. Log in to the Avaya Aura® Experience Portal web console of the Data Center-2.
13. In the navigation pane, click **System Management** > **EPM Manager**.
14. Select the primary EPM and click **Restart**.

15. Log in to the Avaya Aura® Experience Portal web console of the Data Center-2.
16. In the navigation pane, click **POM** > **POM Home**.
17. Click **Configurations** > **Data Center configuration**.
18. Select Data Center-2 and set it as `Active`.
19. Log off and log in again to the Avaya Aura® Experience Portal web console.
20. In the navigation pane, click **POM** > **POM Home**.
21. Click **Configurations** > **POM Zone Configuration**.
22. In the CD Zone Configuration area, select the Campaign Director for all zones of newly active Data Center-2.
23. Click **Save and Apply**.
24. In the AM Zone Configuration area, select the Agent Manager for all zones of newly active Data Center-2.
25. Click **Save and Apply**.
26. Click **Configurations** > **CCElite Configurations**.
27. In the CTI Configuration area, do the following:
    a. Select the CTI Group of Data Center-1 and set it as `Standby`.
    b. Select the CTI Group of Data Center-2 and set it as `Active`.
28. Click **Configurations** > **POM Servers** > **POM Manager**.
29. Select all POM servers and click **Start**.

    POM services are now started on all POM servers.
30. Verify the status of all the services of the newly active Data Center-2 are as listed in the Service Status on page 74.

Shifting to standby Data Center for an unplanned failover

About this task

Unplanned Failover occurs when an outage occurs abruptly while the active Data Center is in production. The operations must be shifted to the standby Data Center. POM might not record dialing statistics to the database and the records might get trapped into an inconsistent dialing state as updated in to the database. The impacts of this type of failure are high as compared to Planned Failover.

If Data Center-1 fails abruptly, operations are required to be shifted to Data Center-2. POM services on all POM servers of Data Center-1 must be stopped. This prevents the POM servers from updating the database which might interrupt in normal functioning of POM servers in Data Center-2. If the POM servers in Data Center-1 are not reachable, then this must be done at the earliest.

Procedure

1. Log in to the command line interface as a *root* user.
2. Run the **`service POM stop`** command to stop the POM services on all POM servers of the failed Data Center-1.
3. Open the MSSQL Database AlwaysOn Dashboard of the database node on Data Center-2.
4. Ensure that the node on Data Center-2 is the new Primary database node.

   When the active Data Center-1 fails and the database node on that Data Center becomes unavailable, database node from the other available Data Centers is designated as the new Primary. This might take some time based on the amount of data, database operations, and network speed. Thus, the MSSQL Database failover has to complete before proceeding with POM failover.
5. Log in to the Avaya Aura® Experience Portal web console of the POM server of Data Center-2.
6. In the navigation pane, click **System Management** > **EPM Manager**.
7. Select the primary EPM and click **Restart**.
8. Log in to the Avaya Aura® Experience Portal web console of the POM server of Data Center-2.
9. In the navigation pane, click **POM** > **POM Home**.
10. Click **Configurations** > **Data Center configuration**.
11. Select Data Center-2 and set it as `Active`.
12. Log off and log in again to the Avaya Aura® Experience Portal web console.
13. In the navigation pane, click **POM** > **POM Home**.
14. Click **Configurations** > **POM Zone Configuration**.
15. In the CD Zone Configuration area, select the Campaign Director for all zones of newly active Data Center-2.
16. Click **Save and Apply**.
17. In the AM Zone Configuration area, select the Agent Manager for all zones of newly active Data Center-2.
18. Click **Save and Apply**.
19. Click **Configurations** > **CCElite Configurations**.
20. In the CTI Configuration area, do the following:
    a. Select the CTI Group of Data Center-1 and set it as `Standby`.
    b. Select the CTI Group of Data Center-2 and set it as `Active`.
21. Click **Configurations** > **POM Servers** > **POM Manager**.

22. Select all POM servers and click **Start**.

    POM services are now started on all POM servers.

23. Verify the status of all the services of the newly active Data Center-2 are as listed in the Service Status on page 74.

Impacts and Recovery

The following is the list of behaviors before, during, and after a failover:

- During unplanned failover, agents handling the call cannot save or dispose the call due to disconnection. Agents are logged out of the agent application. During a planned failover, if the active Data Center-1 is made standby while the agents are logged in, the agents lose connection with the POM server.
- Specific to planned-failover — If any notification campaign, such as email, SMS campaigns were being sent out, at the time of making an active Data Center as standby, POM continues to process the records that were picked up and were present in its memory. Therefore, until all the records present in the memory are dialed out, the Campaign Manager process of the respective POM server does not stop. This delays the stopping of the POM services. Therefore stop all the campaigns prior to making any active Data Center as standby.
- Email campaigns — The number of emails displayed as sent, by POM, may not be equal to the number of emails that were actually received by the customers. This is because POM requests Experience Portal to send emails and waits for response from Experience Portal for whether the email was sent and whether the delivery receipt has been received. During failover, there are chances that the emails may have been sent but their delivery receipts were not received and therefore POM did not have the chance to record the email sent or email delivered notifications into the database.
- Campaigns running prior to failover, and not stopped during failover — After failover, when Data Center-2 is made active, the Monitor does not show any campaign as running until Campaign Manager service is running. Verify the status of all the services of the newly active Data Center-2 as mentioned in Service Status on page 74.
- If there are AUX systems configured, then the campaigns running on the Primary and AUX POM servers of Data Center-1 may not run on the same POM servers after failover. For example, if campaigns, C1 and C2, were running on Primary EPM POM Server of Data Center-1, and campaign C3 and C4 were running on AUX POM server of Data Center-1, then after failover any campaign can run on Primary EPM POM Server as well as AUX POM server of Data Center-2. That is C1 and C3 runs on Primary, and C2 and C4 runs on AUX; C1 and C4 runs on Primary, C2 and C3 runs on AUX. It is also possible that all the campaigns run on Primary alone or on AUX alone. This completely depends on Campaign Manager service of the POM server that starts early.
- If there were campaigns running on active Data Center-1 and were not stopped during failover, then the POM servers on the newly active Data Center-2 resumes those campaigns after failover. The dialing continues till the selected records are dialed. It may be possible that the campaign may not stop even after all the selected records are dialed. To confirm if such a situation has occurred, open the concerned campaign in Monitor. In the “Campaign View” observe the “Un-attempted Contacts” column. If the value remains zero for prolonged period of time, then such a situation is confirmed. During failover updates for the records being dialed out or picked for dialing may not get recorded to the database completely. Thus an

incomplete dialing transaction may be recorded in the database, due to which those records may be get trapped in the transient state. It is not possible to recover the exact state of such records as the information lies on the failed Data Center and the data is lost. To recover such a campaign, see Recovering a campaign on page 82.

Recovering a campaign

Procedure

1. Open the impacted campaign in POM Monitor.
2. Click **Stop**.
3. Redial the trapped records.
   a. Log in to the POM server as a *root* user, preferably Primary EPM of the newly active Data Center-2.
   b. On the command prompt, type the following commands:

      ```
      cd $POM_HOME
      cd bin
      ./geoCampaignHelper.sh
      ```

   c. Select `Option 1- Update Stucked Campaigns.`
   d. From the list of running jobs displayed, enter the job number of the campaign.
   e. On the prompt `Are you sure you want to update the records and dial them ? (y/n) :`, type `y`. Press **Enter**.

      A report is created with the list of ContactIDs that were updated to redial.

Fallback

Fallback is the process of shifting the operations back to the previous active Data Center after resolving all the issues due to which the Data Center had failed.

For example, consider two Data Centers configured, Data Center-1, Data Center-2, where Data Center-1 is active and operational and Data Center-2 is standby. Due to an outage failover, planned or unplanned failover occurs from Data Center-1 to Data Center-2. POM services resume on Data Center-2 and Data Center-2 becomes fully operational. After the issues with Data Center-1 are resolved and the user has to move all operations from Data Center-2 back to Data Center-1. Therefore making Data Center-1 operational again and making Data Center-2 standby as before. This reverting to previously operational Data Center-1 is called fallback. Therefore a fallback is done on a Data Center that was previously active or which had failed earlier.

As operations are being shifted from one Data Center to another, Fallback is similar to Failover. Based on whether the Fallback is planned or abrupt, it is categorized as planned-Fallback or unplanned-Fallback.

Data Center considerations for fallback

To fallback to a previously active Data Center, the Data Center must meet requirements prior to shifting the operations.

The Experience Portal of the Data Center-1 must contain all the data that was present on the Experience Portal of the active Data Center-2. For example, the organizations, zones, and users created on Experience Portal of active Data Center must also be present on the Experience Portal of the standby Data Center prior to fallback.

POM services must be in `Stopped` state on all the POM servers of the Fallback Data Center-1 prior to fallback.

Shifting to Data Center 1 for a planned fallback

About this task

A fallback is called a Planned-Fallback when shifting of operations to fallback Data Center-1 is planned. Planned-Fallback must be performed during maintenance hours.. Thus, POM is non-operational.

Before you begin

- Ensure that the agentless campaigns such as email and SMS notification are not running.
- Log-off all agents from the system.
- Stop all campaigns.

Procedure

1. Log in to the Avaya Aura® Experience Portal web console of the POM server of the active Data Center-2.
2. In the navigation pane, click **POM** > **POM Home**.
3. Click **Configurations** > **Data Center configuration**.
4. Select the currently active Data Center-2 and make it standby.
5. Click **Configurations** > **POM Servers** > **POM Manager**.
6. Verify that the status of all the services of the new standby Data Center-2 are as listed in the Service Status on page 74.
7. Log in to all the POM servers configured in Data Center-2 as a *root* user.
8. Stop the POM services.
9. From the MSSQL Database AlwaysOn Dashboard, click **Start Failover Wizard** on the top right corner of the page.
10. Set the database server in Data Center-1 as `Primary`.
11. Ensure that the AlwaysOn Dashboard displays the database node of the standby Data Center-1 as `Primary`.

12. Log in to the Avaya Aura® Experience Portal web console of the Data Center-1.
13. In the navigation pane, click **System Management** > **EPM Manager**.
14. Select the primary EPM and click **Restart**.
15. Log in to the Avaya Aura® Experience Portal web console of the Data Center-1.
16. In the navigation pane, click **POM** > **POM Home**.
17. Click **Configurations** > **Data Center configuration**.
18. Select Data Center-1 and set it as `Active`.
19. Log off and log in again to the Avaya Aura® Experience Portal web console.
20. Click **Configurations** > **POM Zone Configuration**.
21. In the CD Zone Configuration area, select the Campaign Director for all zones of newly active Data Center-1.
22. Click **Save and Apply**.
23. In the AM Zone Configuration area, select the Agent Manager for all zones of newly active Data Center-1.
24. Click **Save and Apply**.
25. Click **Configurations** > **CCElite Configurations**.
26. Select the CTI Group of Data Center-2 and set it as `Standby`.
27. Select the CTI Group of Data Center-1 and set it as `Active`.
28. Click **Configurations** > **POM Servers** > **POM Manager**.
29. Select all POM servers and click **Start**.

    POM services are now started on all POM servers.
30. Verify the status of all the services of the newly active Data Center-1 are as listed in the Service Status on page 74.

Shifting to standby Data Center for an unplanned fallback

About this task

Unplanned-Fallback occurs when the currently active Data Center-2 fails abruptly, and the operations must be shifted to the previously active Data Center-1. POM might not record dialing statistics to the database and the records might get trapped into an inconsistent dialing state as updated in to the database. The impacts of this type of failure are high as compared to Planned-Fallback.

If Data Center-2 fails abruptly, operations are required to be shifted to Data Center-1. POM services on all POM servers of Data Center-2 must be stopped. This prevents the POM servers from updating the database which might interrupt in normal functioning of POM servers in Data Center-1. If the POM servers in Data Center-2 are not reachable, this must be done at the earliest.

Procedure

1. Log in to the command line interface as a *root* user.
2. Run the **`service POM stop`** command to stop the POM services on all POM servers of the failed Data Center-2.
3. Open the MSSQL Database AlwaysOn Dashboard of the database node on Data Center-1.
4. Ensure that the node on Data Center-1 is the new Primary database node.

   When the active Data Center-2 fails and the database node on that Data Center becomes unavailable, database node from the other available Data Centers is designated as the new Primary. This might take some time based on the amount of data, database operations, and network speed. Thus, the MSSQL Database failover has to complete before proceeding with POM failover.
5. Log in to the Avaya Aura® Experience Portal web console of the POM server of Data Center-2.
6. In the navigation pane, click **System Management** > **EPM Manager**.
7. Select the primary EPM and click **Restart**.
8. Log in to the Avaya Aura® Experience Portal web console of the POM server of Data Center-2.
9. In the navigation pane, click **POM** > **POM Home**.
10. Click **Configurations** > **Data Center configuration**.
11. Select Data Center-1 and set it as `Active`.
12. Log off and log in again to the Avaya Aura® Experience Portal web console.
13. In the navigation pane, click **POM** > **POM Home**.
14. Click **Configurations** > **POM Zone Configuration**.
15. In the CD Zone Configuration area, select the Campaign Director for all zones of newly active Data Center-1.
16. Click **Save and Apply**.
17. In the AM Zone Configuration area, select the Agent Manager for all zones of newly active Data Center-1.
18. Click **Save and Apply**.
19. Click **Configurations** > **CCElite Configurations**.
20. Select the CTI Group of Data Center-2 and set it as `Standby`.
21. Select the CTI Group of Data Center-1 and set it as `Active`.
22. Click **Configurations** > **POM Servers** > **POM Manager**.
23. Select all POM servers and click **Start**.

POM services are now started on all POM servers.

24. Verify the status of all the services of the newly active Data Center-1 are as listed in the Service Status on page 74.

Chapter 11: Resources

Documentation

For information on feature administration, interactions, considerations, and security, see the following POM documents available on the Avaya Support site at http://www.avaya.com/support:

Title	Description	Audience
Avaya Proactive Outreach Manager Overview and Specification	Provides general information about the product overview and the integration with other products.	Users
Upgrading Avaya Proactive Outreach Manager	Provides information about upgrading Proactive Outreach Manager.	Implementation engineers
Using Avaya Proactive Outreach Manager	Provides general information about field descriptions and procedures for using Proactive Outreach Manager.	Users
Troubleshooting Avaya Proactive Outreach Manager	Provides general information about troubleshooting and resolving system problems, and detailed information about and procedures for finding and resolving specific problems.	System administrators Implementation engineers Users
Avaya Proactive Outreach Manager Integration	Provides conceptual and procedural information about the integration between Proactive Outreach Manager and other components.	System administrators Implementation engineers

Install Avaya Aura® Experience Portal before you install POM. You will find references to Avaya Aura® Experience Portal documentation at various places in the POM documentation.

Finding documents on the Avaya Support website

Procedure

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

5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

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

Support

Go to the Avaya Support website at http://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.

Appendix A: Database configuration

POM database configuration

The POM database can reside either on, Oracle Enterprise Edition 64 bit, PostgreSQL, or Microsoft SQL Server Standard/Enterprise Edition database. To create the POM and operational database schema on the respective database, create blank database instances.

For information about creating a PostgreSQL user, go to http://www.postgres.org. You must get the *CREATE* privilege on the database.

For information about creating an Oracle database user, go to http://www.oracle.com.. You must get the *CREATE SEQUENCE*, *CREATE SESSION*, *CREATE TABLE*, and *CREATE VIEW* privileges. See Requirements for database login on page 51.

Note:

The administration and support of the system and contents of the database is the responsibility of the customer.

Caution:

Ensure that the POM and VPMS services are not running before you restart your database.

For information about creating a Microsoft SQL Server database user, go to http://technet.microsoft.com/en-us/library/aa337545. Ensure you set the READ_COMMITTED_SNAPSHOT database parameter ON.

Database name	Server type
PostgreSQL	An external server
Oracle	An external server **Note:** Install the Oracle JDBC driver for POM 3.1. For more information, see Installing an Oracle driver on page 51.
Microsoft SQL Server	An external server

For more information about database configurations, see Different configurations for the database on page 90.

Different configurations for the POM database

You can install the POM server and the POM database in more than one way. POM supports Oracle, Microsoft SQL Server, and PostgreSQL databases. The following table lists some configurations. Using the following table, you can set up the configuration according to your database requirements.

Configuration	Database	Considerations
The POM schema is installed on an external database, which is configured as Avaya Aura® Experience Portal's external reporting database.	PostgreSQL, Oracle, and Microsoft SQL Server	• You must manually take the backup of the POM database. • Cross filtering of Avaya Aura® Experience Portal custom reports and POM reports is possible.
POM schema is installed on external Oracle database, and the Avaya Aura® Experience Portal external reporting database is configured on some other database.	Oracle	• You must manually take the backup of the databases. • Cross filtering of Avaya Aura® Experience Portal custom reports and POM reports is not possible.
POM schema is installed on external Microsoft SQL Server database, and the Avaya Aura® Experience Portal external reporting database is configured on some other database.	Microsoft SQL Server	• You must manually take the backup of the databases. • Cross filtering of Avaya Aura® Experience Portal custom reports and POM reports is not possible.

Using cross filtering, you can generate:

- A POM custom report and then use the report as a filter in the Avaya Aura® Experience Portal standard reports.
- An Avaya Aura® Experience Portal custom report and then use the report as a filter in the POM Campaign Detail Report.

For example, you can generate a custom POM Campaign Detail report and then use the report as a filter in the Avaya Aura® Experience Portal call detail report. This report helps you get campaign-specific call details. For example, you can generate a custom Avaya Aura® Experience Portal call detail report with First Prompt Latency set. Apply this as a filter in POM Campaign Detail Report to get all call records having the specified latency.

Note:

If multiple Avaya Aura® Experience Portal systems share a common reporting database, then:

- If you install a POM system on a single Avaya Aura® Experience Portal system, you can create the POM schema with the common reporting database. In this case, cross filtering of Avaya Aura® Experience Portal custom reports and POM reports is possible.
- If you install a POM system on multiple Avaya Aura® Experience Portal systems, you cannot create the POM schema with the common reporting database. You must create the POM schema for each POM system linked with every Avaya Aura® Experience Portal

system in a separate database. In this case, cross filtering of Avaya Aura® Experience Portal custom reports and POM reports is not possible.

Appendix B: Memory Allocation

Agent Manager

If the number of logged in agents increases from 500 to 1000, then increase the Agent Manager process memory by using the `updateAgentManagerMemory.sh` script from `$POM_HOME/bin` folder. Recommended memory for 1000 agents is 3 GB.

The system displays the following message when you run the `updateAgentManagerMemory.sh` script:

```
[root@PrimPom7396 bin]# ./updateAgentManagerMemory.sh

This utility will modify the amount of RAM memory to be used by Agent
Manager.
User needs to provide number of GB memory to be allocated to Agent
Manager.
The value provided by user must be a positive integer, greater than 1
and must be
less than current available RAM on the system.
(Recommended value is 3 GB.)

Do you wish to continue? [Y/n]Y

Number of GB memory to be allocated to Agent Manager: 3


Agent Manager service needs to be restarted in order to apply the
changes.
Do you want to restart Agent Manager service now? [Y/n]Y
Restarting Agent Manager service...
Stopping Agent Manager:
Warning: Agent Manager process is NOT running!
Starting Agent Manager: ......

Agent Manager restarted successfully.
```

Index

P

R

S

T

U

V