Implementing Avaya Proactive Outreach Manager

Release 4.0
Issue 2
April 2021

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.

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.

License types

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

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

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, 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. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

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

Compliance with Laws

You acknowledge and agree that it is Your responsibility 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.

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.

Change history

Issue	Date	Summary
2.0	April, 2020	Added the following topics: • Enabling Zookeeper authentication • Reverting the Zookeeper authentication • Enabling Zookeeper authentication on external Kafka server
1.0	December, 2020	Content for the following Proactive Outreach Manager features are added: • A new chapter for Federal Information Processing Standards (FIPS) has been added. • The Configuration chapter has been updated to add content on converting POM into non-telephony mode. • The chapter on Geo redundancy has been updated to add content on POM certificate exchange in multiple site scenario. • A new chapter on Cache service.

Chapter 2: 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 Experience Portal.

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 Experience Portal	✔	✔	✔	✔	✔	Avaya Experience Portal is an external system, POM resides on Avaya Experience Portal. For more information about the hardware requirements for installing Avaya Experience Portal, see *Administering Avaya 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 Experience Portal on a single server* or *Implementing Avaya Experience Portal on multiple servers*.

Table continues…

No.	External server/ system	Deployment mode					Notes
		None	CC Elite	AACC-SBP	AACC	Oceana	
2	Database server	✔	✔	✔	✔	✔	The Database server can be PostgreSQL, Oracle. Enterprise Edition 64 bit, or Microsoft SQL Server. For lab setup, you can use local PostgreSQL database that comes preinstalled with Avaya Experience Portal. In production environment, do not install POM database schema on local PostgreSQL. You must 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, a manual license, an SMS license, or an email license. For more information about licenses, see *Avaya 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.

Table continues…

No.	External server/ system	Deployment mode					Notes
		None	CC Elite	AACC-SBP	AACC	Oceana	
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 *Avaya Proactive Outreach Manager Integration*.
6	Avaya Oceana®					✔	You must install Avaya Oceana®. For more information, see *Deploying Avaya Oceana®*.
7	Custom Agent Desktop		✔		✔		You can design your own desktop using the agent APIs. For more information about agent APIs, see *Proactive 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.

Table continues…

No.	External server/ system	Deployment mode					Notes
		None	CC Elite	AACC-SBP	AACC	Oceana	
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 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 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 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
- Geo-redundant deployment

RT Socket connection requirements

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

Note:

For High Availability deployments, the HACMS parameters must be set to true in the `rta.conf` file. You can configure all CMSs can to use the same port and in the POM CMS configuration, you can configure using the that port for all connections.

- 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 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	Avaya Solutions Platform (also known as Avaya Converged Platform (ACP)) 110 DELL SRVR P5 EQX SNR. Profile #5 Core 2.6 GHz with 40 GB RAM, 28 CPU and 500 GB of hard disk storage. If Cache is enabled on POM servers, the resource requirement on database reduces to 24 CPUs and 34 GB RAM.
3	1000-2000	0	200	Avaya Solutions Platform 110 DELL SRVR P5 EQX SNR. Profile #5 Core 2.6 GHz with 40 GB RAM, 28 CPU and 500 GB of hard disk storage.
4	0	1-2200	50	Avaya Solutions Platform 110 DELL SRVR P5 EQX SNR. Profile #5 Core 2.6 GHz with 40 GB RAM, 28 CPU and 500 GB of hard disk storage.

For more details, see POM server specifications on page 32.

Database requirements

- PostgreSQL
- Oracle Enterprise/Standard Edition
- Microsoft SQL Server Enterprise/Standard Edition

See the compatibility matrix tool at http://support.avaya.com/CompatibilityMatrix/Index.aspx for the supported versions of these databases.

- If you configure POM with the MSSQL database and are not using the Cache service, then ensure that for an operational database, READ_COMMITTED_SNAPSHOT parameter is set to ON.
- If you are using an operational database instead of the Cache service, 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 12 CPU, 16 GB of RAM and 300 GB hard disk storage. For more details, see 500 agents profile in POM server specifications on page 32.
2	500-1000	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 12 CPU, 16 GB of RAM and 300 GB hard disk storage. For more details, see 1000 agents profile in POM server specifications on page 32

Table continues…

Sr. No.	Agents	Outbound Ports (Notification)	No. of Jobs	Application server specification
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 12 CPU, 16 GB of RAM and 300 GB hard disk storage. For more details, see 2000 agents profile in POM server specifications on page 32.
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 GHz12 CPU, 16 GB of RAM and 300 GB hard disk storage. For more details, see POM server specifications on page 32.

Software requirements

- Avaya Experience Portal
- Red Hat Enterprise Linux
- Apache *Tomcat*® for local application server

See the compatibility matrix tool at http://support.avaya.com/CompatibilityMatrix/Index.aspx for the latest required software and versions.

Additional resources required on each POM server for using Cache service

Requirements	Description	Conditions
Memory	Total 3 GB distributed as follows: • 1 GB heap memory for POM Cache service. • 2 GB off-heap memory for Apache Ignite. **Note:** This is the default configuration.	Any of the following or both: • Number of jobs running is less than or equal to 100. • Number of filtered contacts is less than or equal to 1 million.
	Total 7 GB distributed as follows: • 3 GB heap memory for POM Cache service. • 4 GB off-heap memory for Apache Ignite.	Any of the following or both: • Number of jobs running is more than 100 and less than or equal to 200. • Number of filtered contacts is more than 1 million and less than or equal to 5 million.
CPU	Additional 4 vCPU for each POM server.	-

Note:

The requirement is derived from a test in which the customer hit rate was 60% call answer and the agent count was 1000. The number of campaigns in total were 170 and individually were 20 ECR, 20 Cruise Control, 60 Preview, 60 Progressive, and 10 Notification.

For more information about how to configure the capacity of memory for Cache service, see Cache service advance setting on page 122.

Database login requirements

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 the login has the same permissions as the login listed in the following table:

Property	MSSQL	Oracle	PostgreSQL
Database Administration Login	sa For other user, see Database user requirement on page 20.	system For other user, see Database user requirement on page 20.	postgres
Database Administration Password	password for sa	password for system	password for postgres

You do not need to provide complete DBA permission to POM database user. If you need to control the permissions or privileges, see Database user requirement on page 20 for required role or privileges.

If database users have database owner access that are supported by POM, the following access is not required for different databases:

Access	Database
sa	Microsoft SQL Server
system	Oracle
postgres	Postgres

The database server acts as a central repository for all information that POM stores and retrieves. For scalability, fault tolerance, and security required for your organization, you can install and configure database servers in multiple ways. Therefore, specific configuration instructions are not part of this guide.

Important:

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

Database user requirement

Oracle Database - privileges for new user

The following are the required privileges:

- CREATE SESSION
- CREATE TABLE
- CREATE VIEW
- CREATE PROCEDURE
- CREATE TRIGGER
- CREATE SEQUENCE
- CREATE MATERIALIZED VIEW

- QUOTA UNLIMITED on TABLESPACE

MSSQL

For MSSQL, user with the *dbcreator* role privilege is required.

Important:

- For the currently installed POM configured to use the Oracle database with system user - Upgrading POM using new database user or changing system user to new user with restricted privileges is not supported. Therefore, the users who already installed POM with system user cannot use new user with restricted privileges.
- For the POM fresh installation with restricted privileges user - Fresh installation is supported. All the operations are supported as the object is created by new user and the user has all privileges. Upgrading from the current version to the next version is also supported. Therefore, the users who install POM with new restricted privileges, can perform fresh install and upgrade.

Network configuration

Configure all components of the Experience Portal environment on the same LAN switch.

These components are:

- EPM or POM
- MPPs
- Databases
- Speech servers
- Application servers

Enabling the encryption of transparent data for the Oracle database

About this task

Use this procedure to enable the encryption of data from the Oracle database to the POM server.

Procedure

1. On the POM server, stop all POM services that are running.
2. Log on to the Oracle database server and enable the encryption of transparent data.
3. Restart the Oracle database server.
4. On the POM server, start all POM services.

Enabling the encryption of transparent data for the MSSQL database

About this task

Use this procedure to enable the encryption of data from the MSSQL database to the POM server.

Procedure

1. On the POM server, stop all POM services that are running.
2. Log on to the MSSQL database server and enable the encryption of transparent data.
3. Restart the MSSQL database server.
4. On the POM server, start all POM services.

Implementing encryption of data for PostgreSQL database

About this task

Use this procedure to implement encryption of data at rest for PostgreSQL database.

Procedure

1. Install RHEL operating system on the POM server.
2. Use the relevant Red hat documentation to enable the encryption for data at rest.
3. On the POM server, install POM and then configure the POM schema.
4. On the POM server, start all POM services.

Chapter 3: Installing POM on Avaya Experience Portal

Configuring Experience Portal for setting up POM system installation

Before you begin

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

Perform the following steps before you install POM:

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.

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

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 POM servers `/etc/hosts` file.

Installing POM on the primary EPM server 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 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... ***
   *******************************************************************
   *******************************************************************
   *** EP service status [OK]***
   *******************************************************************
   *******************************************************************
   *** Stopping vpms service, please wait... ***
   *******************************************************************
   *******************************************************************
   *** vpms service stopped... Starting POM Installation... ***
   *******************************************************************
   Running CLI installation program...

   Welcome to the installation of Avaya POM POM.04.00.00.00.00.xxx!
   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 Orchestration Designer application

By default, the system selects all packages and you can cancel the selection of Avaya 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 Orchestration Designer application package.

   Note:

   To install Avaya 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 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. It is not recommended to use self signed certificate.

    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

Exporting the unencrypted private..
Importing keystore /opt/Avaya/avpom/POManager/config/pom.p12
to /opt/Avaya/avpom/POManager/config/pomKeyStore...

Entry for alias pomservercert successfully imported.

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

Warning:
The JKS keystore uses a proprietary format. It is recommended to
migrate to PKCS12 which is an industry standard format using
"keytool -importkeystore -srckeystore /opt/Avaya/avpom/POManager/
config/pomKeyStore -destkeystore /opt/Avaya/avpom/POManager/config/
pomKeyStore -deststoretype pkcs12".
Executing sslEnabledForAppserver Fresh Install Case
Making Appserver server configuration changes...
SSL is NOT enabled in /opt/AppServer/Tomcat/tomcat/conf/server.xml
at port 7443, now making POM specific changes.....
mv: '/opt/AppServer/Tomcat/tomcat/conf/server.xml.ssl' and '/opt/
AppServer/Tomcat/tomcat/conf/server.xml.ssl' are the same file
```

```
/opt/AppServer/Tomcat/tomcat/conf/server.xml changes done .....
Updating the catalina.sh
JAVA_OPTS_POM_APP Variable is already found
/opt/AppServer/Tomcat/tomcat/bin/catalina.sh changes done ....
Encrypting the private key...
Private key encryption done.
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. To enable classification of SIP response code 403 as ‘CALL_FORBIDDEN’ then run the following command as root user: **`$POM_HOME/bin/updatePOMConfig CallForbidden true`**

16. Restart the system by typing `reboot`.

17. Install Oracle driver or MS SQL driver. For more information, see Installing the Oracle driver on page 66 or Installing the MS SQL driver on page 66.

18. Configure the database. For more information, see Configuring the POM database on the primary POM server on page 42.

Installing POM on the auxiliary EPM server using the interactive mode

Before you begin

POM must be installed on the primary EPM.

Procedure

1. Log in to auxiliary Avaya 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 Orchestration Designer application

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

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

       ✱ **Note:**

       To install Avaya 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 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`.

POM server specifications

The following tables list the minimum configuration for POM as per agent profiles. This includes:

- Primary EPM with POM
- Auxiliary EPM with POM
- External database server for POM
- Application server for POM
- MPP for POM

Note:

The MPP configuration can be different when you use Experience Portal with POM for inbound as compared to when you use Experience Portal with POM for outbound. Therefore, use the following tables for POM even though Experience Portal can support lower specifications for MPP.

If Cache Service is enabled, the hardware requirements for POM increases. For more information, see Additional resource requirement for Cache service in *Implementing Avaya Proactive Outreach Manager*.

All the servers in the following agent profiles had hyper-threading enabled.

All tests were performed on VMWare server with the following hardware configuration:

- Manufacturer: Dell Inc., Model: VxFlex-R640
- Processor : Intel(R) Xeon(R) Gold 6248 CPU @ 2.50GHz * 40 Cores * 2 Sockets
- RAM 1.4 TB
- Hard disk type SSD, 900GB*6 configured in VxFlex mode (similar to vSAN of VMWare)
- Input/Output Operations Per Second (IOPS): 12-server cluster giving 5,00,000 IOPS
- Minimum network bandwidh required: 1 GBPS

1 to 100 agents (Predictive/Preview/Manual) or outbound ports per notification

Number of simultaneous jobs**	Servers	CPUs	RAM	Storage	Bare Metal Processor	VMWare Reservation
10	One EPM/POM server Local Postgres database server Local MPP Local application server	24	24 GB	500 GB	HP Gen9 Hexa Core 2.4 GHz	Processor: 57600 MHz Memory: 24 GB

101 to 500 agents (Predictive/Preview/Manual) or outbound ports per notification

Number of simultaneous jobs**	Servers	CPUs	RAM	Storage	Bare Metal Processor	VMWare Reservation
85	One EPM/POM server	24	32 GB	500 GB	HP Gen9 Hexa Core 2.4 GHz	Processor: 57600 MHz Memory: 32 GB
	Three MPP servers with 500 ports*	12	16 GB	300 GB	HP Gen9 Hexa Core 2.4 GHz	Processor: 28800 MHz Memory: 16 GB
	One database server	24	32 GB	500 GB	HP Gen9 Hexa Core 2.4 GHz	Processor: 57600 MHz Memory: 32 GB
	One application server**	12	16 GB	300 GB	HP Gen9 Hexa Core 2.4 GHz	Processor: 28800 MHz Memory: 16 GB

501 to 1000 agents (Predictive/Preview/Manual) or outbound ports per notification

Number of simultaneous jobs**	Servers	CPUs	RAM	Storage	Bare Metal Processor	VMWare Reservation
174	Two EPM/POM servers	24	40 GB	500 GB	Avaya Solutions Platform (also known as Avaya Converged Platform (ACP)) 110 DELL SRVR P5 EQX SNR. Profile #5 - Core 2.6 GHz	Processor: 62400 MHz Memory: 40 GB
	Six MPP servers with 500 ports*	12	16 GB	300 GB	HP Gen9 Hexa Core 2.4 GHz	Processor: 28800 MHz Memory: 16 GB
	One database server	28	40 GB	500 GB	Avaya Solutions Platform 110 DELL SRVR P5 EQX SNR. Profile #5 - Core 2.6 GHz	Processor: 72800 MHz Memory: 40 GB
	Two application servers**	12	16 GB	300 GB	HP Gen9 Hexa Core 2.4 GHz	Processor: 28800 MHz Memory: 16 GB

1001 to 2000 agents (Predictive/Preview/Manual) or outbound ports per notification

Number of simultaneous jobs	Servers	CPUs	RAM	Storage	Bare Metal Processor	VMWare Reservation
200	Four EPM/POM servers	24	40 GB	500 GB	Avaya Solutions Platform 110 DELL SRVR P5 EQX SNR. Profile #5 - Core 2.6 GHz	Processor: 62400 MHz Memory: 40 GB
	Twelve MPP servers with 500 ports*	12	16 GB	300 GB	HP Gen9 Hexa Core 2.4 GHz	Processor: 28800 MHz Memory: 16 GB

Table continues…

Number of simultaneous jobs	Servers	CPUs	RAM	Storage	Bare Metal Processor	VMWare Reservation
	One database server	28	40 GB	500 GB	Avaya Solutions Platform 110 DELL SRVR P5 EQX SNR. Profile #5 - Core 2.6 GHz	Processor: 72800 MHz Memory: 40 GB
	Four application servers**	12	16 GB	300 GB	HP Gen9 Hexa Core 2.4 GHz	Processor: 28800 MHz Memory: 16 GB

* MPP server is not required in case of POM in non-telephony mode.

** Application server is not required if POM system is in non-telephony mode and email campaigns are not used.

MPP running a server specification of 24 x 2900 MHz CPU and 32 GB RAM can support up to 750 Outbound ports. The minimum total number of ports required for supporting an agent profile is 2.5 times the number of agents.

If MPP is configured with 1500 ports, then maximum of 900 to 1000 ports are used.

For more information on Profile #5, see Avaya Solutions Platform documentation.

Chapter 4: 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.

Table continues…

Options	Remarks
-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. 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 the primary EPM server using the silent mode

Procedure

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

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

Installing POM on the auxiliary EPM server using the silent mode

Procedure

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

```
./installPOM -s -t aux -i <Primary>:80 -p ddapps
```

3. Press `Enter`.

Chapter 5: POM configuration

Checklist for configuring a POM server

Planning tasks

Perform the following planning tasks.

No.	Task	Reference	Notes	✔
1	Enabling FIPS	See Enabling FIPS on page 116.	You can enable FIPS in Proactive Outreach Manager after installing Proactive Outreach Manager.Enabling FIPS is optional.	
2	Configure the POM database.	See Configuring the database on page 42.	Select the installation mode and the database type for configuring the database.	
3	Configure the POM servers.	See Configuring the POM server on page 46.	After you install the POM server, configure the POM server using the web interface.	
4	Configure Avaya Aura® Call Center Elite or Avaya Aura® Contact Center.	See *Using Avaya Proactive Outreach Manager*.	Integrate POM with Avaya Aura® Call Center Elite or Avaya Aura® Contact Center for agent functionality and running agent-based campaigns.	
5	Add users or assign POM specific privileges to existing users.	See Adding users on page 65.	Add users after adding the POM server.	
6	Change the default country setting.	See Changing Home Country on page 65.	Change the default country to a country of your choice.	
7	Exchange certificates for the Avaya Orchestration Designer application server.	See Exchanging certificates for Avaya Aura® Orchestration Designer application server on page 57.	To use the Avaya Orchestration Designer application server, you must exchange certificates between each application server and POM.	
8	Configure the application server.	See Configuring the applications and licenses on page 48.	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

Complete POM implementation.

Procedure

1. Determine the type of database and the server where you want to install the database. For example, a local server for lab environment or an external server for production environment.

   Tip:

   When you install the POM database schema on a local or an external database, you are responsible for the administration of the database.

2. Create two database instances if you are not using Cache service, one for the POM database and the other for an operational database.

   Note:

   Except for the Oracle database, the POM database schema name and the operational schema name must not be same. 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 prompts you to enter the name of the operational database.

   You must install the operational database on the same server where the POM database is present.

3. 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 by running the **`postgresql restart`** command.

4. For a secure database connection, add the third-party certificate in the POM Truststore by using **`$POM_HOME/bin/importCertInPomTruststore.sh`**

   For more information, see Importing Certificate in POM truststore through Command Line Interface on page 88.

5. Configure a desired server such as Postgres, Oracle, or Microsoft SQL Server.

   For installing Oracle drivers and Microsoft SQL drivers, see the instructions in the chapter *Installing POM*.

6. Log in to the primary EPM as a root or sroot user.

7. Type `cd $POM_HOME/bin` and press `Enter`.

8. 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
   ```

9. 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)
   ```

10. Type the database type. You can configure a Postgres, Oracle, or Microsoft SQL server. For installing Oracle drivers and Microsoft SQL drivers, see the instructions in the chapter *Installing POM*.

11. 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, POM displays the Data Center Configuration page. For details, see *Using Proactive Outreach Manager*.

    b. Type the Availability Group Listener FQDN name.

    c. For all other databases, type the database server IP address or host name.

12. Type the port number.

    The default port is 5432 for Postgres database, 1521 for Oracle database, and 1433 for Microsoft SQL Server.

13. Type the name of the database.

14. Type the name of the operational database.

15. Type the user name and password to connect to the database.

The POM system displays the message

```
Does Database require secured connection (Y/N):
```

Note:

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

16. Type `n`.

    The POM system displays the message

    ```
    Do you want to enable POM Cache Service (Y/N):
    ```

    Note:

    Operational database is not used when Cache is enabled. You need additional resources when Cache is enabled.

    You can enable or disable Cache service afterwards, by using a script. For more information, see the chapter on Cache service in this guide.

17. Type `y` to enable Cache service or `n` to disable.

    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 database configuration in the PIMHibernate.cfg.xml file
    and POM Cache flag in DB.
    4. Reconfigure database settings
    5. Exit from this utility
    ```

18. **(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.

19. 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.

20. 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`.

21. To exit, type `5`.

⚠ **Caution:**

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

22. For any errors or exceptions, see the log file at `$POM_HOME/logs/installDB.log`.

Manual dialing mode

Manual dialing

The manual dialing feature has been provided in POM so that the POM does not dial a customer number automatically. Instead, an agent must dial a customer number manually using any third-party software or device. If you want to have a dedicated POM server setup in non-telephony mode, you can convert the POM into non-telephony mode. However, you cannot run preview, predictive, or progressive campaigns in the non-telephony configuration mode. In this configuration mode, POM does not have any telephony communication, that is, SMS, voice, or voice notification to MPP. However, POM can have email campaigns.

Note:

In new POM installations, the default configuration with telephony operations is enabled. When you migrate to POM 4.0, POM retains the existing configuration.

Related links

Converting POM into non-telephony mode on page 45

Converting POM into non-telephony mode

About this task

Use this procedure to convert POM into non-telephony mode.

Note:

In POM systems dedicated for Manual dialing mode, you do not need to configure MPP and application server. However, application server is required for AvayaPOMEmail application, if you are going to use email campaigns in dedicated dialing mode.

After your POM system is converted into the non-telephony mode, it cannot be reverted to the telephony mode.

Before you begin

- Stop all active campaigns.
- Stop agtmgr service.
- Stop cmpmgr service.
- For Geo redundancy, stop Passive DC Agent Manager and Campaign Manager processes on all primary and auxiliary POM servers.

Procedure

1. Log in to the primary POM server.
2. Run the script `enablenonTeleMode.sh`

   The POM system prompts you with the message, **`Have you stopped all running campaigns? (y/n)`**
3. Type **`y`**.

   The POM system prompts you with the message, **`Have you stopped Campaign manager and Agent Manager on all the POM servers including Data centers connected to this setup? (y/n)`**
4. Type **`y`**.

   `This script will enable Manual Dialing mode. Are you sure you want to convert the dialer into the non-telephony mode? (y/n)`
5. Type **`y`**.

   You can see the messages on your screen as the script runs.

   You can start the Passive DC Agent Manager processes after the script completes execution. You can view the logs at `$POM_HOME/logs/enableNonTeleMode.log` during execution of script.

   After the non-telephony mode is enabled, POM home page displays the message, `The system is converted to manual mode`.

   After successful execution of the script, you must start the Agent Manager and Campaign Manager services on all POM servers.

Related links

Manual dialing mode on page 45

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 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 Experience Portal administrator credentials. The Avaya 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 an Avaya Experience Portal certificate, click **Fetch**.
   b. In the **Name** field, type the unique name of an EPM certificate.
   c. In the **Location** field, type `https://<EPM IP Address>`.
   d. Click **Continue**.

      The system adds the Avaya 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 `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 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 center.

     You can configure only one active data center.
   - Click **Standby** to configure the selected data center as a standby data center.
7. Click **Save**.

Configuring applications and licenses

Before you begin

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

Procedure

1. Log in to EPM using the user name and password provided during the Avaya 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 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 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, the IP address of the aux hosting the application server must be mentioned as an alternate IP in the applications configuration.

a. Log in 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 Orchestration Designer applications are installed.

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

i. Select **PomDriverApp**, and from the Speech Servers option, select the TTS resource and add a selected voice.

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" keystoreType="JKS" "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 Experience Portal.
    - Email channel: Sends email messages using Simple Mail Transfer Protocol (SMTP). Ensure you have an email channel configured license on Avaya Experience Portal.
    - Voice channel: Assigns various Avaya 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 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 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:

Security Mode	Location		Description
`Non FIPS`	$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.
`FIPS`		pomKeyStore.bks	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.

If the POM system contains multiple IP addresses, you must include system FQDN in the Common Name (CN) and Subject Alternate Name (SAN) attributes of the certificate. When adding POM server from the **Add POM Server** page, provide the FQDN of the POM system for **POM Server IP Address**.

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 `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.
4. Type `./pomCertificateGenerate.sh` and press **Enter**.

   The POM system prompts you to enter a validity period. The default value is 1186.

   The POM 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:40:34:91:05:7
   E: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]:
```

5. Perform the post execution steps. See Post execution steps on page 54.

   The `pomCertificateGenerate.sh` creates self-signed certificate with only one IP address in the SAN (Subject Alternate Name) field of the generated certificate. If the POM system has multiple IP addresses, you must have FQDN in the CN and SAN fields of the certificate. When adding POM server from the **Add POM Server** page, provide the FQDN of the POM system for **POM Server IP Address**.

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 to 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 on to the Avaya 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, in the **POM Server Name** column, click the name of the server.
4. On the Edit POM Server page, click **Apply** to import the certificate.
5. Select the **Trust the certificate** check box.
6. Click **Save**.
7. On the POM Server page, click **Export** to save the certificate on your local system.

   Note:

   If you have multiple POM servers, export and save all the changed certificates for each server.
8. Click **Save**.

Adding a POM certificates to Avaya Experience Portal trust store

About this task

Use this procedure to add a Proactive Outreach Manager certificate to experience portal. You need to add Proactive Outreach Manager certificates to experience portal trust store for every Proactive Outreach Manager server.

Procedure

1. Log in to the Avaya Experience Portal web console with the Administrator user role.
2. In the navigation pane, click **POM** > **POM Home**.
3. On the POM Home page, click **Configurations** > **POM Servers**.
4. On the POM servers page click the **Export** link for the POM server.
5. Click **Save** to store the downloaded certificate as a `.pem` file.
6. On the Avaya Experience Portal in the navigation pane, click **Certificates**.
7. Click the **Trusted Certificates** tab. Click **Upload**.
8. In the **Name** field, type a name for the certificate that you want to add.
9. In the **Type** field, type select the type of certificate. The default certificate type is application.
10. Browse to the location of the `pom.pem` file and select the file.
11. Click **Continue**.
12. 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. To add the certificate by using the self-signed method, do the following:
    a. Log in to the Avaya 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. Click **Save** to store the downloaded certificate as a `.pem` file.

       For example, `pom.pem`.
    f. Log on to the application server.
    g. In the navigation pane, click **Certificates**.
    h. On the Certificates page, click **Add**.
    i. In the **Name** field, type a name for the certificate that you want to add.
    j. Browse to the location of the `pom.pem` file and select the file.
    k. On the Add Certificate page, click **Continue**.
2. To add the certificate by using the custom certificates method, do the following:
    a. Log in to the application server.
    b. In the navigation pane, click **Certificates**.
    c. On the Certificates page, click **Add**.
    d. In the **Name** field, type a name for the certificate that you want to add.
    e. Browse to the location of the `cacert.pem` file and select the file.
    f. Click **Continue**.
    g. Click **Save**.

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 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 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. You can install the Avaya 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. If you are using an external application server and you have installed POM Avaya Orchestration Designer application package then 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"
   keystoreType="JKS" 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 -keyalg RSA`**

   e. Type the password as `changeit` and type other appropriate details.
8. Using the browser window, log in to the Avaya 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 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 **Keystore 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 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.

       The Common Name (CN) field should have Hostname/FQDN.

       If Enable Server Identity Validation parameter is set to Yes under the security settings, in the Certificate tab of the Experience Portal, then you must have Hostname/FQDN set in SAN field.

       If you have configured orchestration designer applications with the URI containing the IP address under the **Applications** tab of the system configuration in the Experience Portal, then you must have the IP address set in the SAN field.

    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 primary EPM certificate.

   The system displays the Add Certificate page.

   Note:

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

   If EPM certificate signing is disabled using the **Disable Signing** button from **Security** > **Certificate** > **EP signing certificate** and custom CA signed certificates are used, you must import all the CA certificates into POM truststore using POM trusted certificates page under Configurations.

   If EPM signing is enabled, you must import the EP root certificate, that is, EP signing certificate, into POM trust store using POM trusted certificate page.

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 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 have saved the certificate exported in step 9p.

    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 primary EPM certificate from all auxiliary EPM servers.

    g. Click **Continue**.

       The system displays the Certificates page.

    h. Click **Save**.

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

    Note:

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

14. In the navigation pane, click **POM** > **POM Home**.

15. Click **Configurations** > **POM Servers**.

16. Click **Fetch** to fetch the primary EPM certificate.

    The system displays the Add Certificate page.

    Note:

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

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

18. In the **Enter Certificate Path** field, type the client URL as `https://<EPM IP address>/axis2`
19. Click **Continue**.

    The system displays the Certificates page.
20. Click **Save**.
21. Using the browser window, log in to the EPM as an administrator.

    Note:

    For multiple POM servers, log in to the primary EPM.
22. In the navigation pane, click **POM** > **POM Home**.
23. Click **Configurations** > **POM Servers**.
24. Import the certificate exported in step 3.
25. In the **Name** field, type the name of the certificate. For example, epmroot.
26. Click **Continue**.
27. Click **Save**.
28. Using the browser window, log in to the EPM as an administrator.

    Note:

    For multiple POM servers, log in to the primary EPM.
29. In the navigation pane, click **POM** > **POM Home**.
30. Click **Configurations** > **POM Servers**.
31. Import the certificate exported in step 9h.
32. In the **Name** field, type the name of the certificate. For example, appserver.
33. Click **Continue**.
34. Click **Save**.
35. Restart the application server, all MPPs, and all auxiliary servers.

Checking the POM server installation status

About this task

Use this procedure to check the POM server installation status on the primary or 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 `POM status`. Ensure that this command returns a confirmation from the system that the Campaign Manager, Campaign Director, Agent Manager and Rule Engine, Advance List Management, Kafka server, and Agent SDK 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.

   You can also use "**`journalctl -f -u <service name>`**" to check the detailed output of the services.

   - To start, stop, and get the status of the POM Manager service
     - `POM start`
     - `POM stop`
     - `POM status`

   On the command prompt, type the following commands to start, stop, or get the status of the services such as Advance list management, Kafka server, and Agent SDK.

   - To start, stop, and get the status of the Campaign Manager service you can use **`systemctl start service name`** or **`service service name start`** .

     For example, for campaign manager you can use **`systemctl start cmpmgr`** or **`service cmpmgr start`** .

     - `service cmpmgr start`
     - `service cmpmgr stop`
     - `service cmpmgr status` or `cmpmgrstatus`
   - To start, stop, and get the status of the Campaign Director service, type:
     - `service cmpdir start`
     - `service cmpdir stop`
     - `service cmpdir status` or `cmpdirstatus`
   - To start, stop and get the status of the Agent Manager, type:
     - `service agtmgr start`
     - `service agtmgr stop`
     - `service agtmgr status` or `agtmgrstatus`

- To start, stop and get the status of the Active MQ, type:
  - `service pomactmq start`
  - `service pomactmq stop`
  - `service pomactmq status` or `pomactmqstatus`
- To start, stop and get the status of the Rule Engine, type:
  - `service ruleeng start`
  - `service ruleeng stop`
  - `service ruleeng status` or `rulengstatus`
- To start, stop and get the status of the POM Kafka, type:
  - `service pomkafka start`
  - `service pomkafka stop`
  - `service pomkafka status` or `pomkafkastatus`
- To start, stop and get the status of the Advance List Management, type:
  - `service advlistmgmt start`
  - `service advlistmgmt stop`
  - `service advlistmgmt status` or `advlistmgmtstatus`
- To start, stop and get the status of the POM Agent SDK, type:
  - `service pomagentsdk start`
  - `service pomagentsdk stop`
  - `service pomagentsdk status` or `pomagentsdkstatus`
- To start, stop, and get the status of POM dashboard service, type:
  - `service pomdashboard start`
  - `service pomdashboard stop`
  - `service pomdashboard status` or `pomdashboardstatus`
- To start, stop, and get the status of POM Cache service, type:
  - `service pomcache start`
  - `service pomcache stop`
  - `service pomcache status` or `pomcachestatus`
- To start, stop, and get the status of POM multitenancy service, type:
  - `service multitenancy start`
  - `service multitenancy stop`
  - `service multitenancy status` or `multitenancystatus`

Adding users to the POM system

Before you begin

POM installation status must be in running state.

About this task

By default, the Avaya Experience Portal administrator has all POM privileges. The administrator can add new users in the same way as in Avaya 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 Experience Portal.
    - POM Supervisor
    - Org POM Supervisor

      Note:

      Org POM Supervisor privilege is available only if organizations are enabled on Avaya Experience Portal.
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.

Changing the Home country setting

Procedure

1. In the navigation pane of Experience Portal, click **POM Home** > **Configurations** > **Global Configurations**.
2. In the Contact settings area, select the **Home country**.
3. Click **Apply** to save the change.

Installing the Oracle driver

To configure the POM database on Oracle, you must download the latest supported Oracle driver 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 Experience Portal before installing the Oracle driver for POM. For more information about downloading and installing the Oracle driver for Avaya Experience Portal, see the *Implementing Avaya Experience Portal on a single server* guide, and *Implementing Avaya Experience Portal on multiple servers* guide or *Upgrading to Avaya Experience Portal* guide on the Support site at http://support.avaya.com.

For installing the Oracle driver for POM, 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 `latest supported` Oracle driver file 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 downloaded driver files 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 `.jar`.

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

Installing the MS SQL driver

About this task

Use this procedure to install the MS SQL driver if you are using Avaya Proactive Outreach Manager with the MS SQL database. To configure the POM database on MS SQL, download the

MS SQL driver `mssql-jdbc-8.2.1.jre8.jar` file from https://www.microsoft.com and install it on the POM system.

Note:

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

Before you begin

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

Procedure

1. Download the `mssql-jdbc-8.2.1.jre8.jar` MS SQL driver from https://www.microsoft.com.

   Note:

   If you are unable to find the `jar` file on https://www.microsoft.com, copy the file from the machine where Avaya Experience Portal is installed, from the location `opt/Tomcat/apache-tomcat-8.5.57/common/lib/mssql-jdbc-8.2.1.jre8.jar`. Ensure to copy or download the correct jar file.

2. Log in to Linux on the EPM server as a user with root or sroot privileges.
3. Create a folder `~/POMMssqlJDBC` by running the command: **`mkdir –p ~/POMMssqlJDBC`**.
4. Copy the driver files `mssql-jdbc-8.2.1.jre8.jar` to the folder `~/POMMssqlJDBC`.
5. Install the JDBC driver by typing bash command **`$POM_HOME/bin/InstallPOMMsSqlJDBC.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 `mssql-jdbc-8.2.1.jre8.jar`.

   Keep the MS SQL JDBC driver files in the folder `~/POMMssqlJDBC` even after installing or upgrading Avaya Experience Portal. You need these files when you install or upgrade POM.

Provisioning a Kafka server

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

```
$POM_HOME/kafka_xxx/kafka-store
```

By default, POM keeps data of events of last seven days in the `kafka-store` file and generates approximately 50 GB of data per one million attempts. Therefore, you must provision disk space on the POM server.

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

The default retention period is seven days (168 hours). You can modify the retention period by setting the properties in the following files:

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

Enabling Zookeeper authentication

About this task

Kafka uses Zookeeper to store meta information. By default, Zookeeper Access Control Lists (ACL) are configured with Any identity, that is, Zookeeper meta information is accessible by anyone who has access to the network. Enabling authentication on Zookeeper helps to restrict access to anyone.

Procedure

1. Run the script **`$POM_HOME/bin/enableZookeeperAuth.sh`** on all POM servers, one by one.
2. If you are using external Kafka server, follow steps 1 through 4 from the section Enabling Zookeeper authentication on external Kafka server on page 69.
3. Run the script **`POM_HOME/bin/zookeeperACLMigration.sh`** script on all POM servers, one by one.
4. If you are using external Kafka server, follow steps 5-9 from the section Enabling Zookeeper authentication on external Kafka server on page 69.

Reverting Zookeeper authentication

About this task

Use the following steps to revert the configuration you have performed to enable Zookeeper authentication on POM server.

Procedure

Run the script **`POM_HOME/bin/revertZookeeperACLConfiguration.sh`**.

Enabling Zookeeper authentication on external Kafka server

Procedure

1. Add the following configuration in `<Kafka_Home>/config/zookeeper.properties`:***`authProvider.1=org.apache.zookeeper.server.auth.SASLAuthenticationProvider`***

2. Copy `$KAFKA_HOME/config/zookeeper_server_jaas.conf` file from any POM server to `<Kafka_Home>/config/`.

3. Set the following variable when starting Zookeeper server:

   ```
   -Djava.security.auth.login.config=<Kafka_Home>/config/
   zookeeper_server_jaas.conf -
   Dzookeeper.allowSaslFailedClients=false"
   ```

   For example:

   ```
   KAFKA_OPTS="-Djava.security.auth.login.config=<Kafka_Home>/config/
   zookeeper_server_jaas.conf -
   Dzookeeper.allowSaslFailedClients=false" <Kafka_Home>/bin/
   zookeeper-server-start.sh <Kafka_Home>/config/zookeeper.properties
   ```

4. Restart the Zookeeper server.

5. Copy `$KAFKA_HOME/config/zookeeper_client_jaas.conf` file from any POM server to `<Kafka_Home>/config/`.

6. Run the following command to perform ACL migration using the tool **`zookeeper-security-migration.sh`**.

   ```
   sudo KAFKA_OPTS="-Dzookeeper.sasl.clientconfig=ZkClient -
   Djava.security.auth.login.config=<Kafka_Home>/config/
   zookeeper_client_jaas.conf" <Kafka_Home>/bin/zookeeper-security-
   migration.sh --zookeeper.acl secure --zookeeper.connect
   localhost:2181
   ```

7. Set the following environment variable when starting the Kafka server:

   ```
   -Dzookeeper.sasl.client=true
   ```

   ```
   -Dzookeeper.sasl.clientconfig=ZkClient
   ```

   ```
   -Djava.security.auth.login.config=<Kafka_Home>/config/
   kafka_server_jaas.conf
   ```

   For example:
   ```
   KAFKA_OPTS="-Dzookeeper.sasl.client=true -
   Dzookeeper.sasl.clientconfig=ZkClient -
   Djava.security.auth.login.config=<Kafka_Home>/config/
   zookeeper_client_jaas.conf" <Kafka_Home>/bin/kafka-server-start.sh
   <Kafka_Home>/config/server.properties
   ```

8. (Optional) To verify whether pomzookeeper user with Create, Delete, Read, Write, and Admin (CDRWA) permission and sasl authtenticaion scheme is created, use the command **`<Kafka_Home>/bin/zookeeper-shell.sh localhost:2181 getAcl /`**.
9. Add the property, `zookeeper.set.acl=true` to `<Kafka_Home>/config/server.properties`.
10. Restart the Kafka server.

Creating or deleting directory structure for import and export

With this enhancement, new directories are created in **`$POM_HOME`** for import, export and archival for each organization including default tenant. These directories are created for default and new organization.

For default organization

When you install POM the following directories are created for default organization:

```
$POM_HOME/public/default/dncimport

$POM_HOME/public/default/contactlistimport

$POM_HOME/public/default/export

$POM_HOME/archive/default/contactlistimport

$POM_HOME/archive/default/dncimport

$POM_HOME/archive/default/splitter
```

For newly created organization

When you install POM the following directories are created for newly created organization:

```
$POM_HOME/public/<orgid>/export

$POM_HOME/public/<orgid>/contactlistimport

$POM_HOME/public/<orgid>/dncimport

$POM_HOME/archive/<orgid>/contactlistimport

$POM_HOME/archive/<orgid>/dncimport

$POM_HOME/archive/<orgid>/splitter
```

For delete organization

When you delete an organization , then organization specific directories are deleted from the system.

```
$POM_HOME/public/<org-id>

$POM_HOME/archive/<org-id>
```

Note:

When advance list management service is started or restarted, ensure that the VPMS service is running. If the file import fails due to the user error, the administrator must resolve the issue and copy the file to an import location as per the organization.

Archiving the CSV file during an import

Archiving for contact list data sources

With this enhancement, the `CSV` files are archived to avoid duplicate processing of files in the data source.

Archiving the CSV file for the local file data source execution

During local file data source execution , file is archived and the original file is removed. Once the file is copied to `$POM_HOME/Upload` location the import manager deletes the original file configured by the user during the file copying state. After the import job is processed, the file is moved from `$POM_HOME/Upload` location to `$POM_HOME/archive/<org-id>/contactlistimport/` during creating history state.

When the contact list import is executed from the CSV file using the local configuration in the data source, then the configured CSV file is moved in the archive directory matching to organization of the data source.

For example, if the local path configured in data source is `$POM_HOME/public/<org-id>/contactlistimport/CollectionData.csv` Then this file is moved to `$POM_HOME/archive/<org-id>/contactlistimport/CollectionData.csv_<importjobid>_<timestamp>` once the file is processed.

FTP/SFTP configuration in data source:

For FTP/SFTP data source execution, the file is downloaded to `$POM_HOME/Upload` location and then moved to `$POM_HOME/archive/<org-id>/contactlistimport` The original file configured from remote server is not removed.

When the contact list import from `CSV` file is executed using FTP/SFTP configuration in the data source Then the configured CSV file is archived in the archive directory. The configured file is not deleted automatically.

For example, for the FTP/SFTP configuration in data source is `$POM_HOME/public/<org-id>/contactlistimport/CollectionData.csv`

Then this file is downloaded from configured system and archived to `$POM_HOME/archive/<org-id>/contactlistimport/CollectionData.csv_<importjobid>_<timestamp>` location once the file is processed.

Upload type of data source file

For upload type of data source, the file is moved from `$POM_HOME/Upload` location to `$POM_HOME/archive/<org-id>/contactlistimport/` location.

For example, if the `CSV` file is located at the `$POM_HOME/Upload/CollectionData.csv` path in the POM system after FTP/SFTP. Then this file is backed up at `$POM_HOME/archive/orgid/contactlistimport/CollectionData.csv_<importjobid>_<timestamp>` once the file is processed.

When the contact list import from the CSV file is executed and if any interim file is created by import process then it needs to be deleted after the contact list is processed.

If the contact list import process creates temporary file in the upload directory, then it this file is deleted.

The archive location is identified based on organization of the data source. For data source created by administrator (non-organization) the `$POM_HOME/archive/default/contactlistimport/` location is used. In case data source job goes to error state then file is archived after 3 retries.

Note:

When advance list management service is started or restarted, ensure that the VPMS service is running. If the file import fails due to the user error, the administrator must resolve the issue and copy the file to an import location as per the organization.

Archiving the CSV file during a DNC import

Archiving the CSV file using local Configuration in data source

With this enhancement, the `CSV` files are archived that are being used in DNC import so that it cannot be used further during an import and can be persisted for audit purpose.

Archiving the CSV file for the local file data source execution

When the DNC list is imported from the `CSV` file using the local configuration in data source, then the configured CSV file is then moved in the archive directory matching to the organization directory after it is processed.

For example, if the local path configured in data source is `$POM_HOME/public/<org-id>/dncimport/GlobalDnc.csv` Then this file is moved to `$POM_HOME/archive/<org-id>/dncimport/GlobalDnc.csv_DNCAdd_<timestamp>` for add type of datasource and `$POM_HOME/archive/<org-id>/dncimport/GlobalDnc.csv_DNCRemove_<timestamp>`for remove type of datasource once the file is processed.

In case, data source job goes to error state then file is archived after 3 retries.

When the DNC list is imported using the `CSV` file, the interim file created by DNC import process is deleted.

FTP/SFTP configuration in data source

When the DNC list is imported from the `CSV` file using the FTP/SFTP configuration in data source. then the configured `CSV` file is archived in the archived directory. The configured file is not deleted automatically.

For example, if the `CSV` file is located at the path `$POM_HOME/Upload/GlobalDnc.csv` in POM system, then this file is moved to `$POM_HOME/archive/<org-id>/dncimport/GlobalDnc.csv_DNCAdd_<timestamp>` for add type of datasource and `$POM_HOME/archive/<org-id>/dncimport/GlobalDnc.csv_DNCRemove_<timestamp>`for remove type of datasource once the file is processed.

Archiving the CSV file used in splitter

Archiving the CSV file used in splitter

The CSV file used in Splitter is archived. This is implemented to avoid duplicate processing and is persisted for audit purpose. The sublists that are created using splitter are also archived. When you execute the splitter for a CSV file, all the sublists CSV files from `$POM_HOME/archive/<org-id>/splitter/<splitter-id>/sublist.csv` are archived at `$POM_HOME/archive/<org-id>/contactlistimport/sublist.csv_<splitter-id>_timestamp`.

Archiving the CSV file for the local configuration in the data source

When the administrator runs the splitter to import the sublist using the local configuration in data source, the configured CSV file is moved in the archive directory matching to organization of the data source and the file name is not valid for the next splitter.

For example, if the local path configured in data source is `$POM_HOME/public/<org-id>/contactlistimport/collectiondata.csv`, the file is deleted. The file available at `$POM_HOME/archive/<org-id>/splitter/<splitter-id>/collectionData.csv_<splitter-id>` is moved to `$POM_HOME/archive/<org-id>/contactlistimport/collectiondata.csv_<splitter-id>_timestamp` after the file is processed.

The remaining CSV and error CSV files are also archived from `$POM_HOME/archive/<org-id>/splitter/<splitter-id>/remaining.csv` to `$POM_HOME/archive/<org-id>/contactlistimport/remaining.csv_<splitter-id>_timestamp`.

Archiving the CSV file for FTP or SFTP configuration in data source

When the administrator executes the splitter from CSV file using the FTP/SFTP configuration in the data source execution, the configured CSV file is moved in the archive directory matching to organization of the data source and the file name is not valid for the contact list import.

For example, for the FTP/SFTP configuration in data source is the file is located at $POM_HOME/archive/<org-id>/splitter/CollectionData.csv, the file is moved to `$POM_HOME/archive/<org-id>/contactlistimport/CollectionData.csv_<splitter-id>_timestamp` location after the file is processed.

Note:

If the splitter is configured such that the local path is another location than POM_Home, the write permissions must be given recursively to the files and the file must be owned by the avayavpgroup.

The following command is used in such instances:

```
chmod -R 777 filename
chown avayavp:avayavpgroup filename
```

NFS mount point directory structures for contact list import in Multi-POM setup

Direct contact list import or import using file splitter (mandatory NFS mount paths in $POM_HOME/archive)

The following are the mandatory directory structures for NFS mounts:

Note:

`$POM_HOME` environment variable mentioned below is based on the path where POM is installed.

The default path is `$POM_HOME is /opt/Avaya/avpom/POManager`

- `$POM_HOME/archive/<org-id>/contactlistimport`

  This path is used to store archive files in case of direct list import for a particular organization.
- `$POM_HOME/archive/<org-id>/dncimport`

  This path is used to store archive files for DNC list import for a particular organization.
- `$POM_HOME/archive/<org-id>/splitter`

  This path is used to store archive files in case of list import through splitter for a particular organization.

The `<org-id>` is an integer id of each organization created on the POM system.

A default organization on the system is always available, irrespective of organization being created.

The default organization sub-directory is represented by the string default and not by an integer.

So, a default sub-directory is present under `$POM_HOME/archive`, which has the same sub-folder structure. These paths for default organization have to be mandatorily NFS mounted.

If you want to use contact lists in default organization, the following paths are used:

- `$POM_HOME/archive/default/contactlistimport`

  This path is used to store archive files if the direct list import is for the default organization.
- `$POM_HOME/archive/default/dncimport`

  This path is used to store archive files for DNC list import for the default organization.
- `$POM_HOME/archive/default/splitter`

  This path is used to store archive files if it is a list import via splitter for the default Organization.

Note:

Instead of mounting individual full directory paths mentioned above, you can mount the parent directory structure **$POM_HOME/archive** to an NFS server mount point, so that all the required sub-directories present under it would become part of the NFS mount.

For automatic contact list import (mandatory NFS mount paths)

Following are the mandatory directory structures for NFS mounts

- `$POM_HOME/public/<org-id>/contactlistimport`

  This is the path to keep the raw file for automatic list import in the particular organization.

  The `<org-id>` is an integer id of each organization created on the POM system.

  A default organization is available on the system, irrespective of organizations being created.

  The default organization sub-directory is represented by the string default and not by an integer.

  So, a default sub-directory is present under `$POM_HOME/public`, which has the same sub-folder structure. This path for default organization has to be mandatorily NFS mounted if you want to use contact lists in default organization.

- `$POM_HOME/public/default/contactlistimport`

  This is the path to keep the raw file for automatic list import in the default organization.

  Note:

  Instead of mounting individual full directory paths mentioned above, you can mount the parent directory structure `$POM_HOME/public` to an NFS Server mount point, so that all the required sub-directories under it becomes part of the NFS mount.

For contact list import or for an import using file splitter (recommended NFS mount paths)

Following are the paths that are recommended to be NFS mounted:

Note:

These paths are recommended to be used, and are not mandatory.

- `$POM_HOME/public/<org-id>/contactlistimport`

  This is the path to keep the raw file for normal list import for the particular organization

- `$POM_HOME/public/default/contactlistimport`

  This is the path to keep the raw file for automatic list import in the default organization.

After these paths are mounted, you can keep the raw files for import in the path corresponding to the `<org-id>` on which they want to import the list or the default organization based on which organization and the list belongs to.

Note:

Instead of mounting individual full directory paths mentioned above, you can just mount the parent directory structure `$POM_HOME/public` to an NFS Server mount point, so all the required sub-directories under it would become part of the NFS mount.

Additionally, you can also choose any other NFS mount path for keeping their raw file for normal list imports that is scheduled or manual.

Following are the advantages of keeping the raw file in public path:

- Tenant-wise data segregation and systematic management of files. You can easily search and clean up unwanted files. Administrator can search at specific location under `$POM_HOME/public or $POM_HOME/archive` locations for used files.
- Automatic contact list import feature can be used. The POM service has listeners specifically for contact list import directories created under each organization. The third party tool can have configuration for fixed path on POM server.

Creating an export file in the organization directory

Creating an export file in the organization folder

When POM executes the campaign export, the export files containing the campaign attempted contact records are available in the respective organization directory.

The export location is `$POM_HOME/public/<org-id>/export/`. The finite and infinite campaigns are also considered for creating the export file in the organization folder.

Note:

The campaign setting option for mentioning the directory option on the Global Configuration screen on the POM user interface is removed. This export file is created in the respective organization's folder.

Retrieving the Organization ID from the organization name

Retrieving Organization ID from the name

With this tool, you can retrieve the Organization ID from the organization name. You can get the Organization ID by executing the following script in the directory $POM_HOME/bin.

```
./getOrgID [orgname]
```

For example, if the organization name is CC then you need to execute the following command to get the Organization ID for the organization CC. With this utility, you can identify the archive or contactlistimport location which further helps to locate the organization location.

```
./getOrgID CC
```

Changing the hostname or IP address on a dedicated auxillary server

About this task

Use this procedure to change the hostname or IP address of a dedicated auxiliary server.

Procedure

1. Log in to Avaya Experience Portal by using the credentials of an administrator.
2. Stop all the POM services.
3. Open the `/etc/hosts` file in an ASCII editor and change the hostname and the IP address similar to the values specified in the configuration tool.
4. To upgrade the new Avaya Experience Portal certificate, run the script `vpUpgrade.sh script` available at the location: `$POM_HOME/bin/vpUpgrade.sh`
5. To generate the POM certificate, run the script: `pomCertificateGenerate.sh`
6. Re-import the Avaya Experience Portal root certificate to POM truststore from the location **POM HOME** > **Configuration-** > **POM Trusted Certificates**.
    a. Delete the existing Avaya Experience Portal root POM certificate.
    b. Fetch the root certificate of Avaya Experience Portal.
7. Update the IP address in the POM server and the Trust new POM certificate.
8. Log in to the web interface by using Avaya Experience Portal administrator credentials.
9. In the navigation pane click **POM** > **POM Home** > **Configuration** > **POM Servers**.
10. Click on the POM server name. Edit the POM server and update the **Update Host Address**
11. Import the Trust new POM server certificate
12. Update POM certificate in appserver, Avaya Experience Portal truststore.
13. Update the hostname in the following property files:

    Before updating, take backup of the files.

    ```
    $POM_HOME/config/pomDashboardAnalytics.properties
    ```

    ```
    pomDashboardAnalytics.properties:BOOTSTRAP_SERVERS_CONFIG=SSL://
    pomdev7663:9093
    ```

    ```
    pomDashboardAnalytics.properties:vpmsIp=pomdev7663
    ```

    ```
    $POM_HOME/kafka_2.12-2.2.0/configserver.properties listeners=SSL://
    pomdev7663:9093 advertised.listeners=SSL://pomdev7663:9093
    ```

Changing the hostname or IP address on a dedicated primary server

About this task

Use this procedure to change the hostname or IP address of a dedicated primary POM server.

Procedure

1. Log in to Avaya Experience Portal by using the credentials of an administrator.
2. Stop all the POM services.
3. Open the `/etc/hosts` file in an ASCII editor and change the hostname hostname and IP address similar to the values specified in the configuration tool.
4. If you are using the POM server (database on same server) then run `installDB tool` and follow the prompts to set the new hostname or IP address.
5. Select the following options and continue:
    a. Test DB Connection
    b. Save this configuration in the `PIMHibernate.cfg.xml` file.

    Note:

    Ensure you are not selecting any other option.
6. To upgrade the new Avaya Experience Portal certificate, run the script `vpUpgrade.sh` script available at: `$POM_HOME/bin/vpUpgrade.sh`
7. To generate the POM certificate, run the script `pomCertificateGenerate.sh`
8. Re-import the Avaya Experience Portal root certificate to POM truststore from the location **POM HOME** > **Configuration-** > **POM Trusted Certificates**.
    a. Delete the existing Avaya Experience Portal root POM certificate.
    b. Fetch the root certificate of Avaya Experience Portal.
9. Update the IP address in the POM server and the Trust new POM certificate.
10. Log in to the web interface by using Avaya Experience Portal administrator credentials.
11. In the navigation pane click **POM** > **POM Home** > **Configuration** > **POM Servers**.
12. Click on the POM server name. Edit the POM server and update the **Update Host Address**
13. Import the Trust new POM server certificate
14. If the application server is co-resident with the Avaya Experience Portal single server system, verify and/or change the hostname or IP address referenced in the **System Configuration** > **Applications**.
15. For Certificate exchange with `app server/EP/POM` refer to Avaya Experience Portal documentation.

16. Update the hostname at the following locations:

    ```
    $POM_HOME/config/pomDashboardAnalytics.properties
    ```

    ```
    pomDashboardAnalytics.properties:BOOTSTRAP_SERVERS_CONFIG=SSL://
    pomdev7663:9093
    ```

    ```
    pomDashboardAnalytics.properties:vpmsIp=pomdev7663
    ```

    ```
    $POM_HOME/kafka_2.12-2.2.0/configserver.properties listeners=SSL://
    pomdev7663:9093 advertised.listeners=SSL://pomdev7663:9093
    ```

Changing the hostname or IP address for a dedicated EPM server

About this task

If you need to change the IP address or hostname of a dedicated primary EPM server after the EPM software is installed, or if you need to move the primary EPM software to a new server that has a different IP address and hostname, you need to change the information stored in the Avaya Experience Portal database to match the new system configuration.

Procedure

1. Log on to Linux on the Avaya Experience Portal primary EPM server.
    a. If you are an Avaya Services representative, and use Avaya Enterprise Linux, or if the Avaya Service accounts are installed on this server, log on to the local Linux console as root.
    b. Otherwise, log on remotely as a non-root user, and then change the user to root by entering the **`su - root`** command.
2. Stop the vpms service by entering the **`systemctl stop vpms`** command.

    You will see a series of messages as the command starts to shut down EPM components. When the command has successfully stopped all relevant components, the system displays the message: VPMS Shutdown Status: [OK].
3. If you want to change the hostname or IP address of the current server:
    a. If you are using Avaya Enterprise Linux, enter the **`system-config-network`** command and follow the prompts to set the new IP address or hostname.
    b. If you are using Red Hat Enterprise Linux Server, use the appropriate tool as described in Red Hat documentation.
    c. Open the `/etc/hosts` file in an ASCII editor and change the IP address and hostname to the values you specified with the configuration tool.
    d. Reboot the EPM server.

    e. If the vpms service starts automatically after the reboot, stop the vpms service by entering the **systemctl stop vpms** command.

4. Navigate to the **do_UpdateHost** script directory by entering the **$AVAYA_HOME/Support/UpdateHostAddress** command.
5. Enter the **bash do_UpdateHost** command to change the hostname in the database to the hostname of the current server. The system displays a message to confirm whether you want to restart the **vpms** services.
6. Select **Y** to restart EPM and press **Enter**.

   After all relevant components are started successfully, the VPMS `Start Status: [ OK ]` message is displayed.

Changing the hostname or IP address for a dedicated MPP server

About this task

If you need to change the IP address or hostname of a dedicated MPP server after the MPP software has been installed, or if you need to move the MPP software to a new server that has a different IP address and hostname, you need to change the information stored in the Experience Portal database to match the new system configuration.

Procedure

1. Log on to Linux on the Experience Portal MPP server.
   1. If you are an Avaya Services representative, and use Avaya Enterprise Linux, or if the Avaya Service accounts are installed on this server, log on to the local Linux console as root.
   2. Otherwise, log on remotely as a non-root user, and then change the user to root by entering the **su - root** command.
2. Stop the **mpp** service by entering the **service mpp stop** command.
3. If you want to change the hostname or IP address of the current server:
   1. If you are using Avaya Enterprise Linux, enter the **system-config-network** command and follow the prompts to set the new IP address or hostname.
   2. If you are using Red Hat Enterprise Linux Server, use the neat tool as described in your Red Hat documentation.
   3. Open the `/etc/hosts` file on the MPP server in an ASCII editor and change the IP address and hostname to the values you specified with the configuration tool.
   4. Log on to Linux on the Experience Portal Primary EPM server. If you are an Avaya Services representative, and use Avaya Enterprise Linux, the Avaya Service accounts

will not be available after the Avaya Enterprise Linux upgrade. The Avaya Service accounts will be available through EASG configuration during the Experience Portal upgrade.

- Log on to the local Linux console as root.
- Or log on remotely as a non-root user and then change the user to root by entering the **`su - root`** command.

e. Open the /etc/hosts file on the primary EPM server in an ASCII editor and change the IP address and hostname for the MPP to the values you specified with the configuration tool.

f. Reboot the EPM server.

g. Reboot the MPP server.

4. Log on to EPM web interface.

   If Avaya Services is maintaining this system and you are an Avaya Services representative, log on to EPM by using the init EPM account that is created during the EPM software installation.

   Otherwise, log on to EPM by using an account with the Administrator user role.
5. From the Experience Portal main menu, select **System Configuration > MPP Servers**.
6. On the MPP Servers page, click on the name of the MPP whose hostname or IP address you changed.
7. On the Change MPP Server page, make sure that the information in the **Host Address** field matches the new IP address or hostname.

   If you logged in using the init account, ensure that the LDN number specified in the **LDN** field matches the information in the Avaya Services database for this server.
8. Click **Save**.

Copying custom attribute data to system attribute

About this task

Use this procedure to copy Custom Attribute data to the System Attribute - System AgentId. You must do this task only when you have performance issues with any single Custom attribute using the webservice `Get Contact Batch from Contact List`.

Note:

To avoid performance issues, you must stop all POM services before you run this script. This script is a one-time activity for migration of existing Custom attribute to System attribute. Any subsequent changes in custom attribute does not automatically reflect in System attribute.

Procedure

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

   POM displays a message confirming that the migration has started.

   Example: `Started with Migration Script - Mon Oct 12 21:02:08 IST 2020. Please enter below details for Migration of Custom Attribute to System Attribute - Custom attribute name:`
4. Type the Custom Attribute name and press **Enter**.

   POM displays the messsage `Do you want to migrate this attribute for all Contact lists? (Y/N):`
5. Type No and press **Enter**.

   If you select Yes, POM does not prompt you for Contact list names and migrates all contact lists using this custom attribute.

   POM displays the following message:

   ```
   Please provide Contact list names using this attribute separated by
   comma(,):
   ```
6. Type Contact List Names separated by comma and press **Enter**.

   POM displays the following message:

   ```
   Migration is in progress now.….
   ```

   ```
   Migration is completed now - xxx xx xx xx:xx:xx xxx xxxx
   ```

Enabling support for non-English fonts in POM reports

About this task

Use this procedure to run a script on the primary POM server. The script enables POM to display non-English fonts in POM reports.

While running the script, you must provide inputs to the system.

Before you begin

Ensure that:

- The server is running and connected to the internet.
- You know the name and location of the specific `.ttf` file in your POM system.

  The file contains non-English fonts.

Procedure

1. Log on to the POM server as a root user.

   You can open an SSH session to the POM server by using an application such as PuTTY.

2. Go to the following path:

   ```
   cd /opt/Avaya/avpom/POManager/bin/
   ```

3. Run the following script:

   ```
   ./setNonEnglishFontForPOMReports.sh/usr/share/fonts/ja/TrueType/
   xxxxx
   ```

   where,

   xxxxx is the `.ttf` file in your POM system.

   The file contains non-English fonts.

   For example, `font_file.ttf`

Chapter 6: 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 the internal and external components of POM. Trust Management provides an identity to establish authenticated TLS sessions.

Using the **POM Trusted 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 require 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:**

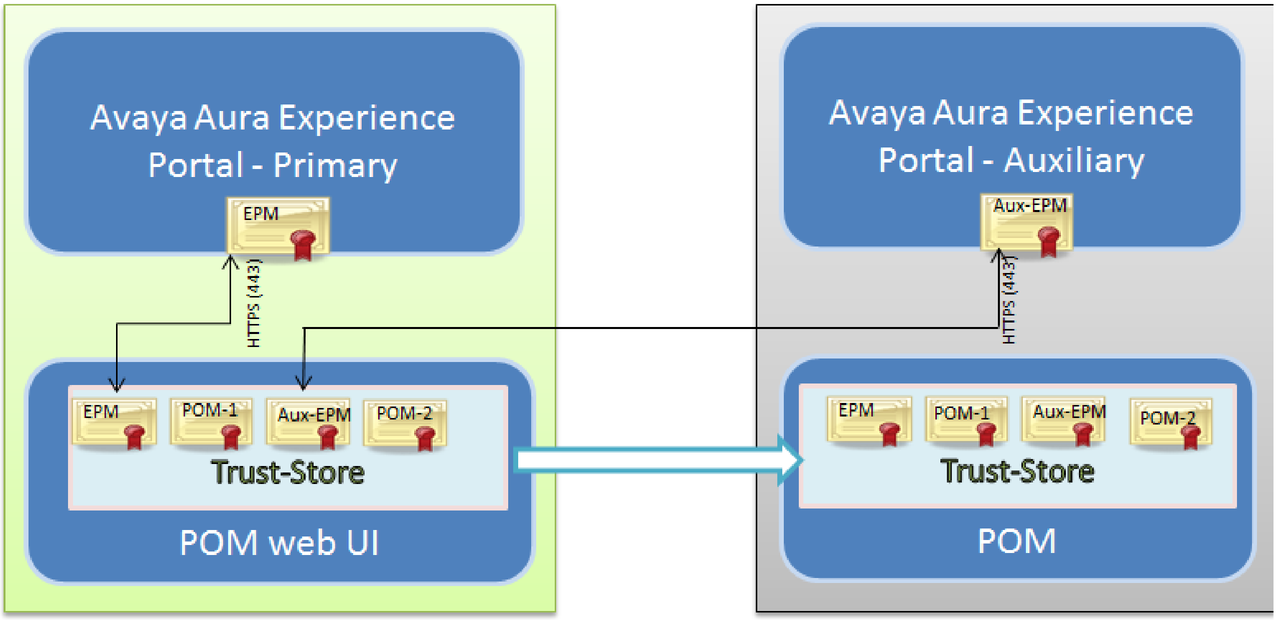
You must restart the POM server after any modification.

POM integrates with Avaya Oceana®, 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.

Note:

In FIPS mode it is mandatory to import AACC certificate in POM trust store.

The following diagram shows the multi POM setup containing primary Avaya Experience Portal and POM. The system fetches the EPM certificate 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.

Table continues…

Name	Description
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` • `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

Use this procedure to do the following:

- Download a CA certificate file to the POM server.
- Place the downloaded CA certificate file into the trust store of the POM server.

On Experience Portal, if you install both a custom CA certificate and then POM with a custom certificate, ensure that you establish communication between all internal POM servers.

To establish communication, you must first ensure that POM completes the exchange of certificates, and copies the updated trust store of the primary POM server on all auxiliary POM servers.

Location of the trust store on the POM primary server: `$POM_HOME/config/pomTrustStore`

Procedure

1. Log in to Avaya Experience Portal with the credentials of an administrator.
2. In the navigation pane, click **POM** > **POM Home**.
3. In the content pane, click **Configurations** > **POM Trusted Certificates**.

   POM displays all trusted certificates that you can import.
4. On the POM Trusted Certificates page, click **Import**.

5. On the Add Certificates page, do the following:
    a. In the **Name** field, type the name of the certificate.
    b. In the **Enter Certificate Path** field, click **Choose File**.

        From the location of the file, select the file.
    c. Click **Continue**.
6. Open a command prompt terminal to the POM server.
7. In the terminal, run the following command:

    ```
    POM restart
    ```
8. On the server, for the changes to take effect, restart all POM services.

Removing the trusted Certificate Authority (CA) certificate

Procedure

1. Log in to the Avaya 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 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.

Importing Certificate in POM truststore through Command Line Interface

About this task

You can import certificates in Proactive Outreach Manager Truststore using the command line interface.

Procedure

1. Log in as a root user.
2. Execute command **`./importCertInPOMTruststore.sh <certificate-alias> <certificate-file-path>`** where certificate-alias is an alias for the certificate being imported and certificate-file-path is the absolute path of the certificate file.

   ✱ **Note:**

   The certificate file must be a valid X509 Certificate file. The supported certificate file extension are pem, cer, crt and der.

   On successful completion, the following output is displayed on the screen:

   ```
   Certificate certificate.crt imported successfully in POM
   Truststore!
   ```

Changing passwords of POM certificate stores

Overview

You can change the password of the POM certificate stores, such as Keystore and Truststore, by using the following script:

`$POM_HOME/bin/updatePOMCertificateStorePassword.sh`

Modes to run the script::

On the command line, run the script by using the following modes:

- Interactive

  In this mode, while running the script, you provide inputs to the system.
- Silent

  In this mode, before running the script, your inputs are a part of the command to run the script.

Viewing the Usage information of a script

About this task

Use this procedure to see the usage information and conditions for using a script for changing the password of a POM Certificate Store.

Procedure

1. Log on to the POM server as a root user.

   You can open an SSH session to the POM server by using an application such as PuTTY.

2. Go to the following path:

   ```
   $POM_HOME/bin
   ```

3. To see the Usage information of the script, use the following command:

   ```
   ./updatePOMCertificateStorePassword.sh --help
   ```

Changing the POM Keystore password by interactive mode

About this task

Use this procedure to change the password of the POM Keystore.

While running the script, you provide inputs to the POM system.

Before you begin

Ensure that the POM server is running and connected to the internet.

Procedure

1. Log on to the POM server as a root user.

   You can open an SSH session to the POM server by using an application such as PuTTY.

2. Go to the following path:

   ```
   $POM_HOME/bin
   ```

3. To see the current password of the POM Keystore, run the following command:

   ```
   ./POMSecurityManagementTool.sh -i
   GET_POM_KEYSTORE_PASSWORD_DECRYPTED
   ```

4. To initiate the process of updating a password, run the following command:

   ```
   ./updatePOMCertificateStorePassword.sh
   ```

   The system displays the following message:

   ```
   Please select following options to change the password for:

   1. POM TrustStore
   ```

```
2. POM KeyStore
3. Usage Information
4. Exit
```

5. Type `2`, and then press `Enter`.

   The system displays the following message:

   ```
   Enter the existing POM KeyStore Password:
   ```

6. Type the existing password of the POM KeyStore and press `Enter`.

   The system displays the following message:

   ```
   Enter the new password for POM KeyStore:
   ```

7. Type the password that you want to set for the POM Keystore and press `Enter`.

   The system displays the following message:

   ```
   Re-Enter the new password for POM KeyStore
   ```

8. Type the password again, and then press `Enter`.

   The system updates the password and then displays the following messages:

   ```
   Update POM KeyStore Password Completed Successfully at xxxxx
   ```

   where, `xxxxx` is the timestamp of the system.

   ```
   Warning: vpms and POM service will need to be restarted on all POM
   Servers for the changes to take effect.
   ```

   ```
   Note: Verify vpms and POM service is running after restarting them
   on Primary POM server. Once verified, restart vpms and POM service
   on all Auxiliary POM Servers.
   ```

9. Restart the VPMS and POM service on the primary POM server.

10. Restart the VPMS and POM service on all Auxiliary POM Servers.

    Important:

    Before restarting the VPMS and POM service on all Auxiliary POM servers, verify that the VPMS and POM service has started on the primary POM server.

Changing the POM Keystore password by silent mode

About this task

Use this procedure to run a script to change the password of the POM Keystore.

In this mode, your inputs become a part of the command to run the script.

Before you begin

Ensure that the POM server is running and connected to the internet.

Procedure

1. Log on to the POM server as a root user.

   You can open an SSH session to the POM server by using an application such as PuTTY.
2. Go to the following path:

   ```
   $POM_HOME/bin
   ```
3. To see the current password of the POM Keystore, run the following command:

   ```
   ./POMSecurityManagementTool.sh -i
   GET_POM_KEYSTORE_PASSWORD_DECRYPTED
   ```
4. To change the password, run the following command:

   ```
   ./updatePOMCertificateStorePassword.sh -certstore KEYSTORE -oldpass
   <old-password> -newpass <new-password>
   ```

   where,

   <old-password> is the earlier password of the Keystore.

   <new-password> is the password that you want to set for the Keystore.

   The system updates the password and then displays the following messages:

   ```
   Update POM KeyStore Password Completed Successfully at xxxxx
   ```

   where, `xxxxx` is the timestamp of the system.

   ```
   Warning: vpms and POM service will need to be restarted on all POM
   Servers for the changes to take effect.
   ```

   ```
   Note: Verify vpms and POM service is running after restarting them
   on Primary POM server. Once verified, restart vpms and POM service
   on all Auxiliary POM Servers.
   ```
5. Restart the VPMS and POM service on the primary POM server.
6. Restart the VPMS and POM service on all Auxiliary POM Servers.

   > **Important:**
   >
   > Before restarting the VPMS and POM service on all Auxiliary POM Servers, verify that the VPMS and POM service has started on the primary POM server.

Changing the POM Truststore password by interactive mode

About this task

Use this procedure to change the password of the POM Truststore.

While running the script, you provide inputs to the POM system.

Before you begin

Ensure that the POM server is running and connected to the Internet.

Procedure

1. Log on to the POM server as a root user.

   You can open an SSH session to the POM server by using an application such as PuTTY.

2. Go to the following path:

   ```
   $POM_HOME/bin
   ```

3. To see the current password of the POM Truststore, run the following command:

   ```
   ./POMSecurityManagementTool.sh -i
   GET_POM_TRUSTSTORE_PASSWORD_DECRYPTED
   ```

4. To initiate the process of updating a password, run the following command:

   ```
   ./updatePOMCertificateStorePassword.sh
   ```

   The system displays the following message:

   ```
   Please select following options to change the password for:

   1. POM TrustStore

   2. POM KeyStore

   3. Usage Information

   4. Exit
   ```

5. Type `1`, and then press `Enter`.

   The system displays the following message:

   ```
   Enter the existing POM TrustStore Password:
   ```

6. Type the existing password of the POM Truststore and press `Enter`.

   The system displays the following message:

   ```
   Enter the new password for POM TrustStore:
   ```

7. Type the password that you want to set for the POM Truststore and press `Enter`.

   The system displays the following message:

   ```
   Re-Enter the new password for POM TrustStore
   ```

8. Type the password again, and then press `Enter`.

   The system updates the password and then displays the following messages:

   ```
   Update POM TrustStore Password Completed Successfully at xxxxx
   ```

   where, `xxxxx` is the timestamp of the system.

```
Warning: vpms and POM service will need to be restarted on all POM
Servers for the changes to take effect.
```

```
Note: Verify vpms and POM service is running after restarting them
on Primary POM server. Once verified, restart vpms and POM service
on all Auxiliary POM Servers.
```

9. Restart the VPMS and POM service on the primary POM server.
10. Restart the VPMS and POM service on all Auxiliary POM Servers.

   Important:

   Before restarting the VPMS and POM service on all Auxiliary POM servers, verify that the VPMS and POM service has started on the primary POM server.

Changing the POM Truststore password by silent mode

About this task

Use this procedure to change the password of the POM Truststore.

In this mode, your inputs become a part of the command to run the script.

Before you begin

Ensure that the POM server is running and connected to the internet.

Procedure

1. Log on to the POM server as a root user.

   You can open an SSH session to the POM server by using an application such as PuTTY.

2. Go to the following path:

   ```
   $POM_HOME/bin
   ```

3. To see the current password of the POM Truststore, run the following command:

   ```
   ./POMSecurityManagementTool.sh -i
   GET_POM_TRUSTSTORE_PASSWORD_DECRYPTED
   ```

4. To change the password, run the following command:

   ```
   ./updatePOMCertificateStorePassword.sh -certstore TRUSTSTORE -
   oldpass <old-password> -newpass <new-password>
   ```

   where,

   <old-password> is the earlier password of the Truststore.

   <new-password> is the password that you want to set for the Truststore.

   The system updates the password and then displays the following messages:

   ```
   Update POM TrustStore Password Completed Successfully at xxxxx
   ```

where, `xxxxx` is the timestamp of the system.

```
Warning: vpms and POM service will need to be restarted on all POM
Servers for the changes to take effect.
```

```
Note: Verify vpms and POM service is running after restarting them
on Primary POM server. Once verified, restart vpms and POM service
on all Auxiliary POM Servers.
```

5. Restart the VPMS and POM service on the primary POM server.
6. Restart the VPMS and POM service on all Auxiliary POM Servers.

   Important:

   Before restarting the VPMS and POM service on all Auxiliary POM Servers, verify that the VPMS and POM service has started on the primary POM server.

Exchanging POM certificates in a multiple site setup

About this task

For POM deployments that support Geo redundancy, you must export POM self-signed or Custom certificates from each POM server and install it in the trust store of other POM servers in multi-site setup.

Important:

Ensure that all exported certificates are imported into the trust store of every other POM site.

Use the following procedure to export POM self-signed or Custom certificates and import the certificates into other POM servers in multi-site setup:

Procedure

1. Using the browser, log in to Experience Portal.
2. In the navigation pane, click **POM** > **POM Home**.
3. Click **Configurations** > **POM Servers**.
4. Click **Export** on the listed certificate tab and save it on your local system.
5. Log in to other POM systems in the setup.
6. Click **Configurations** > **POM Trusted Certificates**.
7. In **Name**, type the name of the certificate.
8. Click **Choose File** to navigate to the certificates and select the certificate.
9. Click **Continue**.

   Note:

   Restart VPMS and POM services on all after the certificate exchange is complete.

Chapter 7: 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 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 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 a power outage, network outage, or 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 data centers.

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

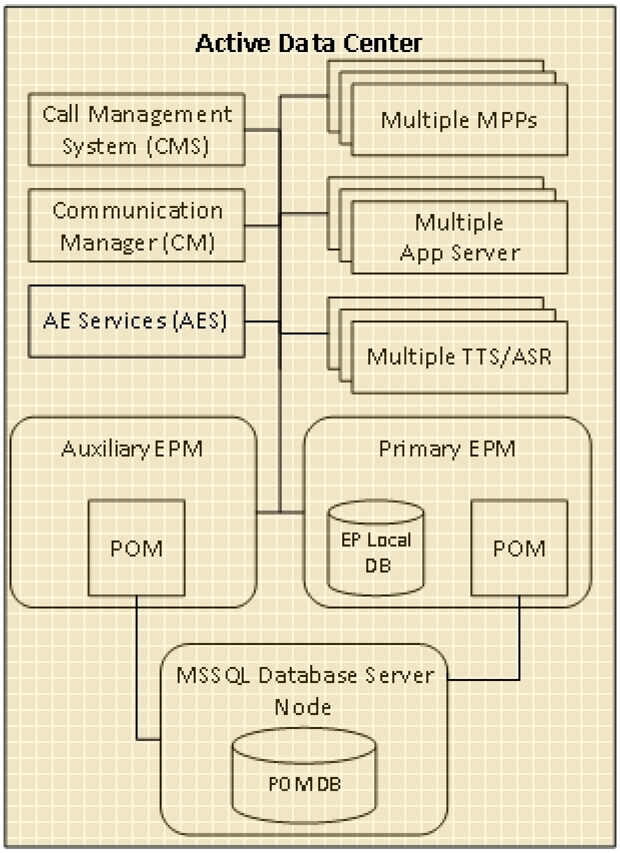
Experience Portal synchronization is required as POM is deployed on the Experience Portal platform. Organizations, zones, and users created on Experience Portal are stored in the local database of Experience Portal. There is no High Availability (HA) solution available to synchronize multiple Experience 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 the Geo-Redundancy HA mode. Avaya Call Management System is deployed in the HA mode.

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

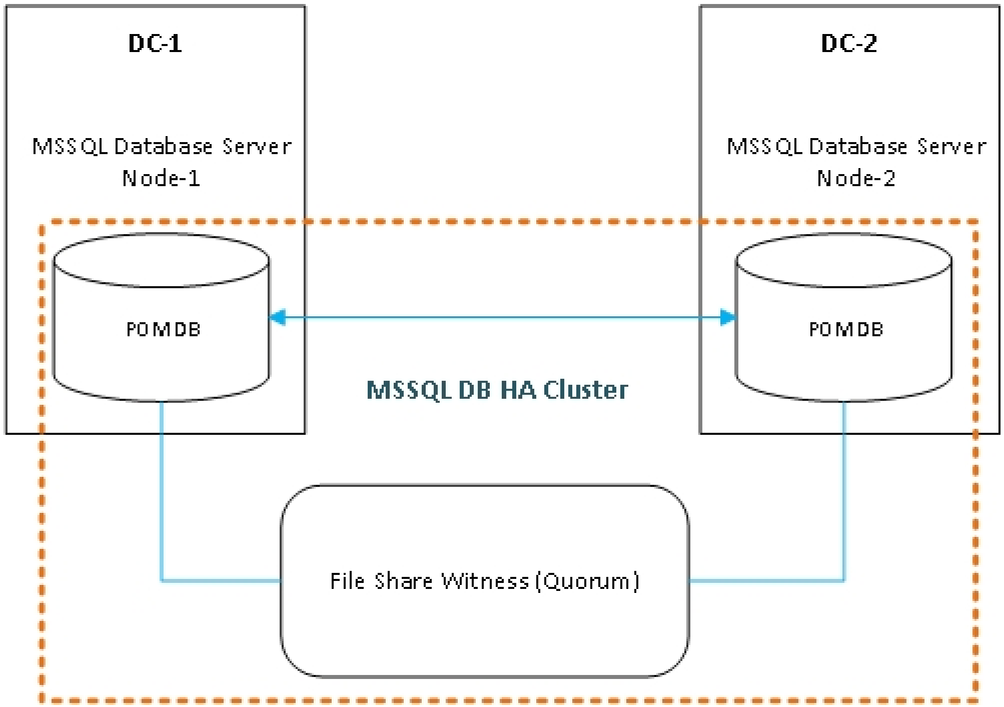
Architecture

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.


DC-1
MSSQL Database Server Node-1
POMDB
DC-2
MSSQL Database Server Node-2
POMDB
MSSQL DB HA Cluster
File Share Witness (Quorum)

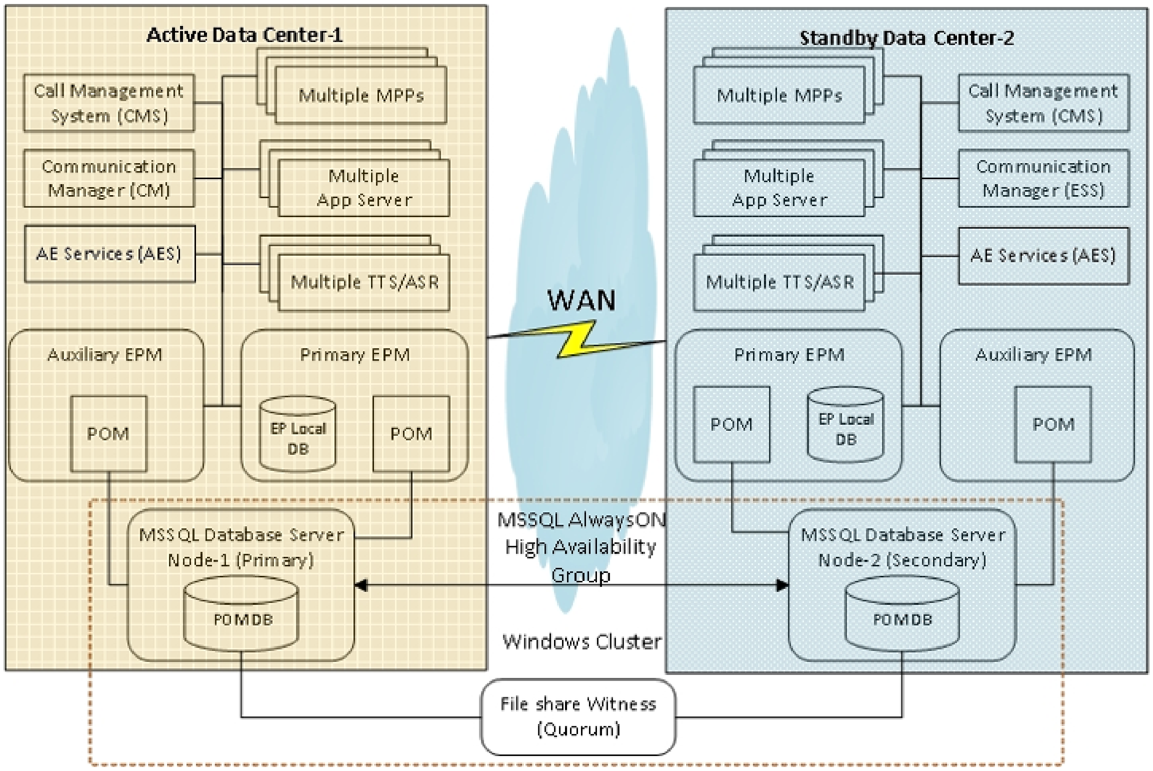
To install and configure MSSQL AlwaysOn, see the Microsoft documentation. It is the responsibility of the customer to setup and configure Windows Server Failover Cluster (WSFC) and the MSSQL AlwaysOn feature.

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.

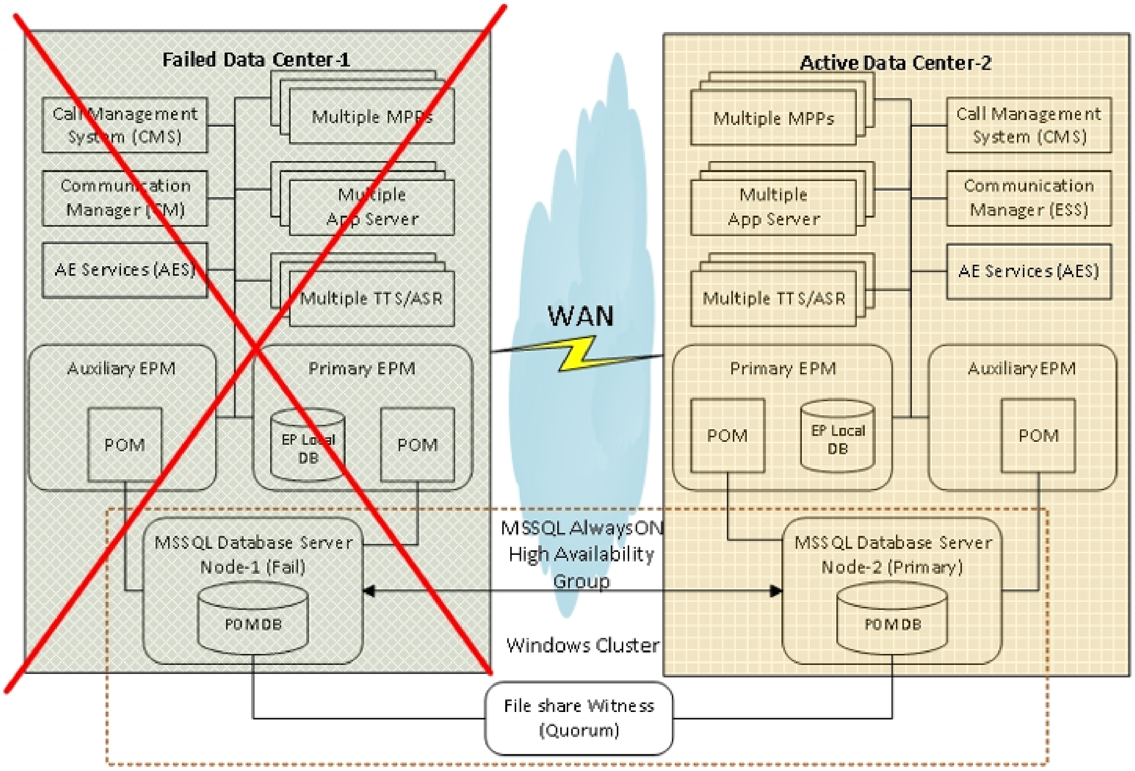
The following diagram is an example of two data centers configured for Geo-Redundancy.



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.
- In multi-site POM setup, install the POM certifcates on each other's trust store. For more information, see Exchanging POM certificates in a multiple site setup on page 94.

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 into 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. If you have enabled Cache service on the active data center, you must enable it on all other data centers too.

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

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.

Note:

If two hundred campaigns are going to run on the Geo system, then set the value as three hundred for parameter hibernate.c3p0.max_size_PIMCM in the file `PIMHibernate.cfg.xml`. The file is located at `POM_Home/config` on Proactive Outreach Manager server. The default value of the environment variable *POM_Home* is `/opt/Avaya/avpom/POManager`.

Enabling Geo-Redundancy for a new installation

About this task

Use this procedure on primary and auxiliary POM servers.

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 availability group listener FQDN
    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 Experience Portal web console.
2. In the navigation pane, click **POM** > **POM Home**.
3. Click **Configurations** > **Data Center Configuration**.
4. Click **Add**.
5. In the Configure EPM Servers area, verify the POM server of the current data center and all the configured auxiliary POM servers.
6. In the **Group Name** field, type the name of the group.
7. Type the **EPM User Name** and **EPM Password** of all POM servers listed in the Configure EPM Servers area.
8. Click **Save**.
9. 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 data center groups is set to **Standby**.

Deleting a data center group

Procedure

1. Log in to the Avaya 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**.

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 the default zone are as follows:

Service	Status
Campaign Manager	RUNNING
Campaign Director	MASTER
Agent Manager	MASTER
ActiveMQ	MASTER
RuleServer	MASTER
Kafka Server	RUNNING
Advance List Management	RUNNING
POM Agent SDK	RUNNING
Cache Service	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
Advance List Management	STOPPED
POM Agent SDK	STOPPED
Cache Service	STOPPED

Disabling Geo-Redundancy

About this task

To disable Geo-Redundancy for a data center, you must first delete the Geo-Redundancy group of the data center.

Procedure

1. Log in to the Avaya 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. On the Data Center Configuration page, verify that the data center group is deleted.
7. Log in to the POM server as a root user.
8. In the command prompt, type the following commands and press **Enter**.
   a. **`cd $POM_HOME`**
   b. **`cd bin`**
   c. **`./installDB.sh`**
9. In the **Please select Contact Center Configuration mode from following options** field, select `1 CCElite` and press **Enter**.
10. In the **Please enter the database configuration**, type `MSSQL` and press **Enter**.
11. In the **Do you want to enable the POM Geo configuration? Please select(y/n)**, type `n` and press **Enter**.
12. In the **FQDN of MSSQL Domain Controller**, type the availability group listener FQDN
13. In the **Database Port**, type the port number of the database.
14. In the **Database Name**, type the name of the database.
15. In the **Operational Database Name**, type the name of the operational database.
16. In the **User**, type the name of the user.
17. In the **Password**, type the password of the user.
18. In the **Does Database require secured connection (Y/N)**, type `Y`.
19. Choose the appropriate option to test the database connection.
20. **(Optional)** If the test is successful, save the configuration.
21. To exit the `installDB.sh` script, select the option 5 and press **Enter**.
22. Follow Step 7 to Step 18 to configure the database for POM servers in the data centers that do not belong to the Geo-Redundancy group.

Activating a data center

About this task

When all data center groups are created and are in the standby mode, you must determine the data center that must go in to production. At a 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 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. Log out of Avaya Experience Portal web console and log in again.
8. Click **Configurations** > **POM Zone Configuration**.
9. In the CD Zone Configuration area, select the appropriate Campaign Director.
10. Click **Save and Apply**.
11. In the AM Zone Configuration area, select the appropriate Agent Manager.
12. Click **Save and Apply**.
13. Start POM services.
14. Verify the status of POM services.
15. On the standby data center, do the following to stop POM services:
    a. Log in to the POM server command line interface as a root user.
    b. On the command prompt, type the **`POM stop`** command.
    c. Repeat Step a and Step b for all other POM servers.

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 the 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 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. Log in to all the POM servers configured in Data Center-1 as a *root* user.
7. Stop the POM services.
8. Verify that the status of all the services of the new standby Data Center-1 are as listed in the Service status on page 104.
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 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 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 Experience Portal web console.
20. In the navigation pane, click **POM** > **POM Home**.

    Note:

    When the Active site fails and is unreachable, the POM Manager page of the Standby site might take a couple of minutes to load.
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 primary POM server of Active Data center and click **Start**.

    You need to wait until all primary POM services started or running.

    Now select Aux POM server of Active Data center and click **Start**.

    POM services are now started on all POM servers of Active Data Center.

    If cache service is enabled you also need to select cache service under **POM Manager** > **POM Server**.

30. Verify the status of all the services of the newly active Data Center-2 are as listed in the Service status on page 104.

Shifting to the 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 **`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 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 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 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:
    1. Select the CTI Group of Data Center-1 and set it as `Standby`.
    2. Select the CTI Group of Data Center-2 and set it as `Active`.
21. Click **Configurations** > **POM Servers** > **POM Manager**.
22. Select primary POM server of Active Data center and click **Start**.

    You need to wait until all primary POM services are started or running.

    Now select Aux POM server of Active Data center and click **Start**.

    POM services are now started on all POM servers of Active Data Center.
23. Verify the status of all the services of the newly active Data Center-2 are as listed in the Service status on page 104.

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 104.
- 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 111.

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 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 **`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 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 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 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 104.

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 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 104.
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 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 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 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 104.

Chapter 8: FIPS

FIPS overview

Proactive Outreach Manager supports Federal Information Processing Standards (FIPS) 140-2. There are standard cryptographic algorithms that are approved by FIPS and these certified algorithms are used in the cryptography in Proactive Outreach Manager.There are four levels of security defined in the FIPS 140-2, however, Proactive Outreach Manager has implemented the application security.

Prerequisites for enabling FIPS

The following are the prerequisites for enabling FIPS in Proactive Outreach Manager:

- The operating system must be in FIPS mode.
- Experience Portal must be set up in FIPS mode before runnning the FIPS script on Proactive Outreach Manager.

Enabling FIPS

About this task

Use this procedure to enable FIPS mode on Proactive Outreach Manager. The following changes happen when you enable FIPS on POM:

- The Fetch button on POM Trusted Certificates page is disabled. For any operation related to fetching the certificates, you must use Import option instead of Fetch.
- Existing certificate stores `pomKeyStore` and `pomTrustStore` in `JKS` format is converted to `pomKeyStore.bks` and `pomTrustStore.bks` in `BCFKS` formats respectively. POM refers to the new formats.

If you enable FIPS on primary server, then you need to enable FIPS on auxiliary server also.

Procedure

1. Log in to the POM server as a root user.
2. Stop the VPMS, POM, and APPSERVER processes.

3. Run the following command on the POM server to enable the FIPS: `$POM_HOME/bin/POM_FIPS_setup.sh`
4. Reboot the POM system.

Disabling FIPS

About this task

Use this procedure to disable FIPS mode on Proactive Outreach Manager.

Procedure

1. Log in to the POM server as a root user.
2. Stop the VPMS, POM, and APPSERVER processes.
3. Run the command on the POM server to disable the FIPS: `$POM_HOME/bin/POM_FIPS_remove.sh`

   ⚠ **Warning:**

   If you disable FIPS in POM, then you must disable FIPS in Experience Portal too, otherwise POM services do not start.

Enabling FIPS connection between AES and POM

Proactive Outreach Manager supports FIPS connection with Avaya Aura® Application Enablement Services. You must enable secure connection in Proactive Outreach Manager configuration.

For more information about enabling FIPS in AES, see *Administering Avaya Aura® Application Enablement Services*.

Enabling FIPS connection between CMS and POM

Proactive Outreach Manager supports FIPS connection with Avaya Call Management System. You need to enable secure connection with Avaya Call Management System in Proactive Outreach Manager configuration.

For more information about enabling FIPS in CMS, see *Deploying Avaya Call Management System*.

Supporting FIPS for POM applications on external Tomcat APPSERVER

About this task

To use external tomcat in FIPS mode, follow this procedure for POM:

Proactive Outreach Manager supports only Bouncy Castle as the security provider for FIPS.

Procedure

1. Ensure that FIPS is enabled on operating system. To add Bouncy Castle as the FIPS provider in JAVA, refer to Bouncy Castle documentation https://www.bouncycastle.org/documentation.html
2. Stop the APPSERVER.
3. For more information, refer and perform the steps mentioned in *Avaya Orchestration Designer* documentation.
4. Convert the existing JKS format KeyStore to BCFKS format KeyStore which is a FIPS complaint bouncy castle KeyStore. Proactive Outreach Manager supports bouncy castle as the FIPS provider.
    a. Create a backup of the existing KeyStore with a different name.
    b. Use the following command to convert the keystore.

    ```
    keytool -importkeystore -srckeystore <existing keystore> destkeystore
    <target keystore> -srcstoretype JKS -deststoretype BCFKS -srcstorepass
    <existing keystore password> -deststorepass <target keystore password> -
    providerpath <FIPS provider jar path> -provider
    org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider
    ```

    c. Rename the converted keystore to existing keystore name.

    Note:

    The supported FIPS provider jar file is available in the following location: `$POM_HOME/lib/common/bc-fips-1.0.1.jar.`
5. Configure `$APPSERVER_HOME/conf/server.xml` to use BCKFS as KeyStore Type by changing the value of attribute keystoreType in the element Connector to BCFKS.
6. Start the APPSERVER.

Disabling FIPS on Tomcat APPSERVER

About this task

Use this procedure to disable FIPS on the external Tomcat APPSERVER. For local Tomcat APPSERVER, use the script `$POM_HOME/bin/POM_FIPS_remove.sh` to disable FIPS on POM as well as the APPSERVER.

Procedure

1. Ensure you stop the APPSERVER before proceeding.
2. For more information, refer and perform the steps mentioned in the Avaya Orchestration Designer documentation.
3. Convert the existing BCFKS format KeyStore to JKS format KeyStore.
    a. Create a backup of the existing KeyStore.

    b. Use the following command to convert the keystore.

    ```
    keytool -importkeystore -srckeystore <existing keystore> destkeystore
    <target keystore> -srcstoretype BCFKS -deststoretype JKS -srcstorepass
    <existing keystore password> -deststorepass <target keystore password> -
    providerpath <FIPS provider jar path> -provider
    org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider
    ```

    c. Rename the converted keystore to existing keystore name.

    Note:

    The supported FIPS provider jar can be located on POM Server at $POM_HOME/lib/common/bc-fips-1.0.1.jar.
4. Configure `$APPSERVER_HOME/conf/server.xml` to use JKS as KeyStore Type by changing the value of attribute keystoreType in the element Connector to JKS.
5. When FIPS is disabled on OS and JVM is not running in FIPS mode, start the APPSERVER.

Chapter 9: Cache Services

Cache service overview

Currently, POM stores the operational data required for dialing into the operational database. This causes POM services to frequently query the database to access the data, which impacts the performance of the system.

The POM Cache (pomcache) service service is able to cache the data into the memory (RAM), which makes the data read or write process faster. The operational database is migrated from database into the POM Cache service. For implementing this service, POM uses the Apache Ignite framework as the in-memory database. Apache Ignite is an in-memory database that stores the data in key values pair and provides SQL interface for querying the data. This service is a spring boot service that starts Apache Ignite in the cluster mode to also support multi-POM deployments. When the Job is started, all the filtered records are added into the Cache instead of operational database. So, the Contacts data is read and written from the Cache (RAM).

Each Cache service from the multi-POM deployment setup forms a cluster of Apache ignite data node. Agent manager, Campaign Manager, and Campaign director services also start Ignite instance but they join as a client node into the cluster.

All POM cache service in the cluster have Cache replication mode of Ignite as replicated. With this option, every POM server has Cache for operational tables for all running jobs.

Cache service modes overview

You can use Cache service for operational database by running script available under `$POM_HOME/bin` folder. By default, Persistance off mode is enabled for Cache service.

Persistence off: When Ignite is started with persistence off setting, Ignite has all the data that is loaded into the physical memory and there is no persistence storage available. POM Cache service starts all Ignite nodes in replication mode so the data loaded into the memory is replicated across multiple nodes.

- Single POM system: If Cache service fails, the service recovers the data from the historical database after the Cache service operation restarts.
- Multi-POM system: If Cache service fails on one of the POM servers, the service recovers the data from Cache service running on other POM servers. In case both the Cache service nodes fail, the service recovers the data from the historical database after the Cache service operation restarts.

Enabling Cache service

About this task

Use this procedure to enable Cache service.

Procedure

1. Ensure that all jobs are stopped.
2. Navigate to **`$POM_HOME/bin folder`**.
3. Run the following script on the Proactive Outreach Manager server to enable the Cache Service:

   ```
   ./enable_PomCache true
   ```

   POM Cache service is enabled. A prompt is displayed `Do you want to continue? (y/n):`
4. Type `y`.
5. Restart VPMS service on all POM servers.

Disabling Cache service

About this task

Use this procedure to disable cache service.

Procedure

1. Ensure that all jobs are stopped.
2. Ensure that Proactive Outreach Manager Cache service is stopped on all POM servers.
3. Navigate to **`$POM_HOME/bin`** folder.
4. Run the following script on the Proactive Outreach Manager server to disable the Cache service:

   ```
   ./enable_PomCache false
   ```

   POM Cache service is disabled. A prompt is displayed `Do you want to continue? (y/n):`
5. Type `y`.
6. Restart POM and VPMS service on all POM servers.

Cache service advance setting

About this task

If you are running more than 100 jobs or if the total contacts in all the running jobs are more than 1 million, follow below steps to increase the POM Cache service memory:

Use this procedure to enable Cache service advance setting.

Procedure

1. Navigate to `$POM_HOME/bin` folder.
2. Run the following script on the server to increase the Cache memory:

   `updateServiceMemory.sh`
3. A prompt is displayed `Do you want to continue? (y/n): y`.
4. Enter the Service Identifier Name `pomcache`.
5. A prompt to enter the number of memory to be allocated is displayed.

   Number of GB memory to be allocated to Service is 3 GB.
6. A prompt is displayed `Do you want to restart pomcache service now? [Y/n]`.
7. Type `y`.

Increasing POM cache Off-heap memory

About this task

If you are running more than 100 jobs or if the total contacts in all the running jobs are more than 1 million then follow these steps to increase the POM Cache Off-heap memory.

Procedure

1. Navigate to `$POM_HOME/bin` folder.
2. Run the following script on the server to increase the Cache Off-heap memory:

   `./updateCacheConfigParams.sh`

   The POM system displays a prompt `Please enter preferred choice`.
3. Select option `3` as Maximum Offheap Memory.

   The POM system displays the prompt `Enter Size in MB [2048 MB]:`
4. Enter memory in MB, that is, 4096.

Note:

Offheap maximum memory value must not be greater than 20% of total server memory.

The POM system displays the prompt `Please enter preferred choice`:

5. Select option 4 as Exit.
6. Restart POM and VPMS service on all POM servers.

Obtaining the version number of Apache Ignite

About this task

Use this procedure to retrieve the number of the latest installed version of Apache Ignite from the `PomCacheService.out log` file on the POM server.

Before you begin

Ensure that the internet connection between your machine and the POM server is active.

Procedure

1. Log on to the POM server as a root user.

   You can open an SSH session to the POM server by using an application such as PuTTY.

2. Go to the following path:

   `$POM_HOME/logs`

3. Open the `PomCacheService.out` file.

   The version number is in the line after the Apache Ignite banner.

   For example, in ver. `2.8.1`#20200521-sha1:86422096, the version number is `2.8.1`

Cache service parameters

POM cache service loads the following parameters on start. All these parameters are available in the POM database under pim_config table.

Parameter	Description
CACHE_SERVICE_PORT	This parameter indicates the port on which all Ignite nodes starts and forms the cluster. Default value of the port is 6999. This parameter is configurable from the Global Configuration page on the POM user interface.

Table continues…

CACHE_CLIENT_PORT	This parameter indicates the port on which all the thin clients can connect to Ignite node. Default value of the port is 10800. This parameter is configurable from the Global Configuration page on the POM user interface.
CACHE_INITIAL_MEM_SIZE	This parameter indicates the amount of initial memory in MB to be allocated by Ignite as off heap memory. This is physical memory initially used by ignite to store data. The default value is 2048 MB. This parameter is configured using the script.
CACHE_MAX_MEM_SIZE	This parameter indicates maximum memory in MB to be allocated by Ignite as off-heap memory. This is physical memory initially used by ignite to store data. Default value is 2048 MB. This parameter is configured by using the script.
CACHE_CLEANUP_INTERVAL	Cache service runs the cleanup job after fix duration. This parameter decides the interval cleanup frequency. The default value is 30 seconds.
CACHE_FAILURE_DETECTION_TIMEOUT	There is heartbeat mechanism between all nodes in the cluster. This parameter decided interval after which node should be detected as failed node and removed from the cluster. The default value is 60000 ms.
CACHE_BACKUPS	This parameter is applicable only when cache mode is PARTITIONED.
CACHE_THREAD_POOL_SIZE	This parameter is used to configure ignite rebalance thread pool size. Rebalance threads are used to reliance ignite partition when ignite node is added or removed from the cluster or job tables are added or deleted from the cache. Default value is 2. This value should not be greater that Ignite system thread pool size. Ignite system thread pool size is equal to number of CPU core present in the system.

Chapter 10: Uninstalling POM

Uninstalling POM

About this task

Use this procedure to uninstall POM. This procedure does not uninstall the Avaya Experience Portal application server.

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

Procedure

1. Log on to the Avaya Experience Portal server by using the credentials of a root user.
2. On the Avaya 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 Experience Portal server:

   ```
   reboot
   ```

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

Chapter 11: 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. For more information, see *Avaya 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 Experience Portal

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

Proposed solution

Procedure

Install the latest version of Avaya Experience Portal. See the *Implementing Avaya Experience Portal on a single server* and *Implementing Avaya 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 EPM certificate not fetched on the POM trust store page.

Solution

1. Log in to the Avaya 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:
   1. Click **Fetch**.
   2. Click **alias** and type the certificate URL with the https prefix.
   3. 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 keystore and truststore, do the following:
   a. Log in to the Command Line Interface (CLI) with the root user.
   b. To change the directory path, run the command: **`cd $POM_HOME/bin`**
   c. Run the command: **`$POM_HOME/bin/pomCertKeystore.sh`**
   d. To create a new pomTrustStore, make a copy of the POM keystore 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. Log in 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 12: 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
Migrating Avaya Proactive Outreach Manager	Provides information about migrating Proactive Outreach Manager.	Implementation engineers
Using Avaya Proactive Outreach Manager	Provides general information about field descriptions and procedures for using Proactive Outreach Manager.	Users
Using Avaya Workspaces for Avaya Proactive Outreach Manager	Provides instructions on using Avaya Workspaces for Proactive Outreach Manager.	Users
Using Avaya Proactive Outreach Manager supervisor dashboard	Provides instructions on using Proactive Outreach Manager supervisor dashboard.	Supervisors
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 Experience Portal before you install POM. You will find references to Avaya Experience Portal documentation at various places in the POM documentation.

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.

2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.
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 only displays the documents for the selected category.
7. Click **Enter**.

Support

Go to the Avaya Support website at https://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

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 66.

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 more information, see Installing an Oracle driver on page 66.
Microsoft SQL Server	An external server

For more information about database configurations, see Different configurations for the database on page 136.

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 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 Experience Portal custom reports and POM reports is possible.
POM schema is installed on external Oracle database, and the Avaya 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 Experience Portal custom reports and POM reports is not possible.
POM schema is installed on external Microsoft SQL Server database, and the Avaya 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 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 Experience Portal standard reports.
- An Avaya 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 Experience Portal call detail report. This report helps you get campaign-specific call details. For example, you can generate a custom Avaya 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 Experience Portal systems share a common reporting database, then:

- If you install a POM system on a single Avaya Experience Portal system, you can create the POM schema with the common reporting database. In this case, cross filtering of Avaya Experience Portal custom reports and POM reports is possible.
- If you install a POM system on multiple Avaya 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 Experience Portal system in a separate database. In this case, cross filtering of Avaya 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.
```

Appendix C: Security management tool

Encrypting data by interactive mode

About this task

Use this procedure for running a script to convert data into unidentifiable patterns (encrypted data) to prevent unauthorized access.

While running the script, you must provide inputs to the system.

Before you begin

Ensure that the POM server is running and connected to the internet.

Procedure

1. Log on to the POM server as a root user.

   You can open an SSH session to the POM server by using an application such as PuTTY.

2. Go to the following path:

   ```
   $POM_HOME/bin
   ```

3. To open the POM Security Management Tool Menu, run the following command:

   ```
   POMSecurityManagementTool.sh
   ```

   The system displays the following message:

   ```
   ==================================

   POM Security Management Tool Menu:

   ==================================

   1. Encrypt

   2. Decrypt

   3. Tool Usage Information

   4. Exit

   ==================================

   Please enter your preferred choice :
   ```

4. Type `1`, and then press `Enter`.

The system displays the following message:

```
Enter data:
```

5. Type the data that you want to encrypt, and then press `Enter`.

   The system encrypts the data and then displays the following message:

   ```
   Encrypted Data: xxxxx
   ```

Decrypting data by interactive mode

About this task

Use this procedure for running a script to convert encrypted data into identifiable data.

While running the script, you must provide inputs to the system.

Before you begin

Ensure that the POM server is running and connected to the internet.

Procedure

1. Log on to the POM server as a root user.

   You can open an SSH session to the POM server by using an application such as PuTTY.

2. Go to the following path:

   ```
   $POM_HOME/bin
   ```

3. To open the POM Security Management Tool Menu, run the following command:

   ```
   POMSecurityManagementTool.sh
   ```

   The system displays the following message:

   ```
   ==================================
   POM Security Management Tool Menu:
   ==================================
   1. Encrypt
   2. Decrypt
   3. Tool Usage Information
   4. Exit
   ==================================
   Please enter your preferred choice :
   ```

4. Type `2`, and then press `Enter`.

The system displays the following message:

```
Enter data:
```

5. Type the data that you want to decrypt, and then press `Enter`.

   The system decrypts the data and then displays the following message:

   ```
   Decrypted Data: xxxxx
   ```

Encrypting data by silent mode

About this task

Use this procedure to run a script to convert data into unidentifiable patterns (encrypted data) to prevent unauthorized access to the data.

In this mode, your inputs become a part of the command to run the script.

Before you begin

Ensure that the POM server is running and connected to the internet.

Procedure

1. Log on to the POM server as a root user.

   You can open an SSH session to the POM server by using an application such as PuTTY.

2. Go to the following path:

   ```
   $POM_HOME/bin
   ```

3. To encrypt data by using silent mode, run the following command:

   ```
   ./POMSecurityManagementTool.sh -o ENCRYPT -r 4.X_ONWARDS -d <data>
   ```

   where,

   `<data>` is the data that you want to encrypt.

   Note:

   For the silent mode, the POM security management tool does not display error messages.

   To see any errors while encrypting the data, read the system logs in the following file:

   ```
   $POM_HOME/logs/POMSecurityManagementTool.log
   ```

Decrypting data by silent mode

About this task

Use this procedure to run a script to convert encrypted data into identifiable data.

In this mode, your inputs become a part of the command to run the script.

Before you begin

Ensure that the POM server is running and connected to the internet.

Procedure

1. Log on to the POM server as a root user.

   You can open an SSH session to the POM server by using an application such as PuTTY.

2. Go to the following path:

   ```
   $POM_HOME/bin
   ```

3. To decrypt data by using silent mode, run the following command:

   ```
   ./POMSecurityManagementTool.sh -o DECRYPT -r 4.X_ONWARDS -d <data>
   ```

   where,

   `<data>` is the data that you want to decrypt.

   Note:

   For the silent mode, the POM security management tool does not display error messages.

   To see errors while decrypting the data, read the system logs in the following file:

   ```
   $POM_HOME/logs/POMSecurityManagementTool.log
   ```

Index