Implementing Avaya Proactive Outreach Manager

Release 4.1
Issue 1
November 2025

Notices

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

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

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

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

Copyright

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

Virtualization

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

Third Party Components

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

Service Provider

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

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

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

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

Contact Avaya Support

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

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
4	November 2025	The following topic is added or updated for release 4.1: • POM monitor and POM cache service information removed from the document entirely. • Database user requirement section is updated with information about the roles and permissions required to run database heath related queries. • RT Socket connection requirements section is updated with information highlighting the requirement of RT-Socket connection for every instance of POM.
3	July 2024	The following topic is added for release 4.0.2 SP3: • Suggestions to tune the POM database to improve the performance of POM.
2	December, 2022	Updated or removed content related to Cache service for operational database.

Table continues…

Issue	Date	Summary
1	October, 2022	The following topics are updated in Release 4.0.2: • Database server requirements • POM database configuration • Installing the MS SQL driver • Enabling Geo-Redundancy for a Primary POM server on a PR site • Enabling Geo-Redundancy for a Primary POM server on a DR site • In the Database server requirements topic, a link for referring to the best practices for the specifications of a database disk or the size of a drive is added. • In the Appendix A, a topic to describe the best practices to configure the storage capacity of a database is added. • The chapter on Geo-Redundancy is updated.

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

- Executing shell scripts
- Editing files on Linux by using a text editor such as vi or vim
- Executing database scripts and queries
- Validating logs
- Validating error messages
- Using 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 12.

System requirements

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

External server/ system	Deployment mode					Notes
	None	CC Elite	AACC-SBP	AACC	Oceana	
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*.
Database server	✔	✔	✔	✔	✔	The Database server can be PostgreSQL, Oracle Enterprise Edition 64 bit, or Microsoft SQL Server.

Table continues…

External server/ system	Deployment mode					Notes
	None	CC Elite	AACC-SBP	AACC	Oceana	
License server	✔	✔	✔	✔	✔	License server is a mandatory requirement. You can install a local or an external license on the license server. The licenses can be any combination of POM Outbound ports, POM Agent licenses (Predictive, Preview, or Manual), or Multi-Media (SMS, or Email). For more information about licenses, see *Avaya Proactive Outreach Manager Overview and Specification*.
Avaya Aura® Call Center Elite (Call Center Elite)		✔				You must install Call Center Elite to run agent-based campaigns or agent-less automated skill-based campaigns.
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*.
Avaya Oceana®					✔	You must install Avaya Oceana® to enable the Outbound voice capability in Avaya Oceana®, to work with Avaya Proactive Outreach Manager. For more information, see *Deploying Avaya Oceana®*.

Table continues…

External server/ system	Deployment mode					Notes
	None	CC Elite	AACC-SBP	AACC	Oceana	
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.*
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.
Call Management System (CMS)		✔				CMS is used for skill- based pacing and agent blending in Call Center Elite.
Avaya Contact Recorder						Installation of Avaya Contact Recorder is optional.
Operating system						Red Hat Enterprise Linux or Avaya Enterprise Linux.

Other requirements

- *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. ECC licenses are required for any Enhanced Call Classification. Agent licenses are required to do Agent Based Campaigns.
- *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 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

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. Each POM node in the deployment requires at least one dedicated incoming RT-Socket connection from CMS.

While configuring the RT Socket to send CMS real time data to POM server, ensure you use the tvi1 report format and that there are enough rt_socket sessions configured to account for each reachable POM node on your deployment.

Note:

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

The following are the few example scenarios for RT Socket connection configuration based on the default deployment types:

- 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

Agents	Outbound Ports (Notification)	No. of Jobs	Database server
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.
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.
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.
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 21.

Database requirements

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

For the list of supported database versions, see the compatibility matrix tool at http://support.avaya.com/CompatibilityMatrix/Index.aspx.

For more details about the best practices to use PostgreSQL database parameters, see POM database configuration on page 145

For more details about the best practices for the specifications of a database disk or the size of a drive, see Best practices to configure the storage capacity of a database on page 148. The total index size might increase two times of the actual size. Therefore, ensure that you have additional storage for the increased index size. For more information on MSSQL tuning, refer to Suggestions to tune the POM database to improve the performance of POM on page 146.

Application server requirements

Hardware requirements

Agents	Outbound Ports (Notification)	No. of Jobs	Application server specification
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 information about specifications, see profile for 500 agents in POM server specifications on page 21.
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 information about specifications, see profile for 1000 agents in POM server specifications on page 21
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 information about specifications, see profile for 2000 agents in POM server specifications on page 21.
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 information about specifications, see POM server specifications on page 21.

Software requirements

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

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

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 19.	`system` For other user, see Database user requirement on page 19.	`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 19 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 a 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

Important:

For the current installation, POM is configured to use the Oracle database with a system user. Upgrading POM using a new database user or changing a system user to a new user with restricted privileges is not supported. Therefore, the users who already installed POM with a system user cannot use a new user with restricted privileges.

MSSQL

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

Note:

For MSSQL, POM supports database authentication and Windows authentication.

The MSSQL server authenticates a user who uses the login credentials or the Windows authentication mode to log in to the MSSQL database.

Important:

Fresh installation is supported for the POM fresh installation with restricted privileges. All the operations are supported as a new user creates the object, and the user has all privileges. Upgradation from the current version to the next version is also supported. Therefore, the users who install POM with new restricted privileges can perform a fresh installation and upgrade.

Characters supported in username

When logging in to databases, you can use @,-,\, or . characters in the username.

Oracle database - required role for database monitoring

To have SELECT access for POM user on Oracle's dynamic performance views, Database Administrator (DBA) must grant following Oracle role to POM user.

```
GRANT SELECT ANY DICTIONARY TO <pom_user>;
```

SQL Server database – required role for database monitoring

To have SELECT access for POM user on dynamic management views and functions that provide information about database health statistics, DBA must grant following SQL Server role to POM user.

```
GRANT VIEW SERVER STATE TO <pom_user>;
```

Postgres database - required role for database monitoring

To allow POM Postgres user to read pg_stat_* views which provide information about database health statistics, DBA must grant following Postgres role to POM user.

```
GRANT pg_read_all_stats TO <pom_user>;
```

Note:

POM for Postgres database require pg_stat_statements module for tracking planning and execution statistics of all SQL statements executed by a server. This module is not available globally but can be enabled for a specific database with CREATE EXTENSION.

Contact your database administrator to install and enable the pg_stat_statements extension in POM PostgreSQL database server.

Network configuration

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

- 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 running POM services.
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 data encryption from the MSSQL database to the POM server.

Procedure

1. On the POM server, stop all running POM services.
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 data encryption for PostgreSQL database

About this task

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

Procedure

1. Install the 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.

POM server specifications

The following tables list the minimum configuration requirement for POM specific to agent profiles and the number of simultaneous jobs.

This includes the following servers:

- 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 additional inbound functionality as compared to when you use Experience Portal with POM for outbound only. Therefore, use the following tables for POM even though Experience Portal can support lower specifications for MPP.

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

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

Number of simultaneous jobs**	Servers	CPUs	RAM	Storage	Bare Metal Processor	VMWare Reservation
10	One EPM/POM server Local MPP server with 300 ports* Local Postgres database server Local application server	24	24 GB	500 GB	HP Gen9 Hexa Core 2.4 GHz	Processor: 57600 MHz Memory: 24 GB

1 to 100 agents (Predictive/Preview/Manual) or outbound ports per notification - with external MPP

Number of simultaneous jobs**	Servers	CPUs	RAM	Storage	Bare Metal Processor	VMWare Reservation
10	One EPM/POM server Local Postgres database server Local application server	12	24 GB	500 GB	HP Gen9 Hexa Core 2.4 GHz	Processor: 28800 MHz Memory: 24 GB
	One MPP server with 300 ports*	8	4 GB	300 GB	HP Gen9 Hexa Core 2.4 GHz	Processor: 19200 MHz Memory: 4 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	40 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

Table continues…

Number of simultaneous jobs**	Servers***	CPUs	RAM	Storage	Bare Metal Processor	VMWare Reservation
	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
	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 for 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 you configure MPP server with 1500 ports, you can use maximum 1000 ports.

***Application servers need to be in the Load balance mode using the Experience Portal URL. POM does not support the use of an external Load Balancer for application URL.

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

Kafka Events retention

By default, the retention duration is 7 days or 168 hours. After the retention duration is complete, the system purges the events. Based on the available disk space, the value of the log.retention.hours parameter can be set in the `server.properties` file at the `$KAFKA_HOME/config/` location.

The sample performance runs with the following configuration:

- Number of Kafka servers for high availability: 3
- Number of Producers: 4 (CM, AM, CD, Event Aggregator)
- Campaign Jobs: 200
- Number of Agents: 1000
- Contacts/Attempts: 12495000
- Execution duration : 105 hours
- Disk size of kafka-store directory: 45 GB
- Number of Consumers(c): 5 (EventSDK sample client, Event Aggregator app)
- Number of topics: 6
- Replication factor(R): 3
- Retention Period in Days (RP): 7

Total Attempts	Expected Dialing Attempts Per Hour	No. of Hours divided with attempts	Total Size in GB	Per Hour Size in MB
12495000	119000	105	45	428.57

Topic	MB/hour
POM.Default.AGENT	10.17
POM.Default.AGENTSTATISTICS	1.04
POM.Default.ATTEMPT	12.58
POM.Default.ENRICHEDATTEMPTRESULT	7.49
POM.Default.JOB	1.36
POM.Default.JOBSTATISTICS	5.03
POM.Default.IMPORTSTATISTICS	0.01
POM.Default.INBOUNDSKILL	0.01
POM.HEARTBEAT	2.32
Zookeeper directory size	0.18
Total	40.19

Based on this, you can calculate our cluster-wide disk size according to retention period.

MB or hour depends on the call flow, dialing parameters, and agents for the campaigns.

SIP code, MPP code, and POM completion code mapping

The following table displays the default mappings:

SIP code	MPP code	Equivalent CCXML code for MPP code	POM completion code
UA_Unauthorized	VP_NOROUTE	noroute	Sys_Call_Forbidden / Invalid_Number
UA_PaymentRequired			
UA_Forbidden			
UA_ProxyAuthentication Required			
UA_Decline			
UA_NotFound			
UA_Ambiguous			
UA_DoesNotExistAnywhere			
UA_AddressIncomplete			
UA_MethodNotAllowed			
UA_ServerNotAcceptable			
UA_UnsupportedMediaType			
UA_NotImplemented			
UA_Gone			
UA_TransportErr	VP_NETWORK_BUSY	networkbusy	-
UA_ByeAck	VP_DISCONNECTED	nearenddisconnect	Disconnected_By_System_NuisanceApp / Disconnected_By_System_CCA
UA_ByeResp	VP_REMOTE_DISCONNECT	farenddisconnect	Disconnected_By_User_NuisanceApp / Disconnected_By_User_CCA
UA_ServiceUnavailable	VP_NORESOURCE	noresource	-
UA_RequestTimeout	VP_NOANSWER	noanswer	No_Answer / Ring_No_Answer
UA_ServerTimeout			
UA_TemporarilyUnavailable			
UA_BusyHere	VP_BUSY	busy	Call_Busy
UA_BusyEverywhere	VP_NETWORK_BUSY	networkbusy	-

Table continues…

SIP code	MPP code	Equivalent CCXML code for MPP code	POM completion code
UA_BadGateway			
UA_BadRequest	VP_UNKNOWN_DISCONNECT_REASON	unknown	-
UA_CallOrTransactionDoesNotExist			
UA_ServerInternalError			
UA_RequestEntityTooLarge			
UA_RequestURITooLong			
UA_UnsupportedURIScheme			
UA_BadExtension			
UA_ExtensionRequired			
UA_IntervalTooBrief			
UA_VersionNotSupported			
UA_MessageTooLarge			

Adding or modifying SIP Code to Completion Code Mapping

For information about how to add a mapping for a SIP code to completion code or to override the default mapping, refer the topic, SIP Codes in the *Administering Avaya Proactive Outreach Manager*

Chapter 3: Installing POM on Avaya Experience Portal

Configuring Experience Portal for setting up POM system installation

Before you begin

Ensure that Avaya Experience Portal is installed and in running state. To install Avaya Experience Portal, download and refer to the following documents:

- *Implementing Avaya Experience Portal on a single server* - Describes the installation of Avaya Experience Portal on a single server environment at a customer site.
- *Implementing Avaya Experience Portal on multiple servers* - Describes the installation of Avaya Experience Portal on a multiple server environment at a customer site.

Procedure

1. On the primary EPM, you must 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.

2. 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.
3. Set the database password on Avaya Experience Portal. For more information, see Setting database password on Avaya Experience Portal on page 29.
4. To install POM on more than one system, include all auxiliary POM server hostnames in the primary EPM `/etc/hosts` file. You must also have the primary EPM hostname in all POM servers `/etc/hosts` file.

Setting database password on Avaya Experience Portal

About this task

Use this procedure to set the password for the internal postgres database.

Procedure

1. Log on to Linux on the Experience Portal server with root privileges.
2. Enter the `cd $AVAYA_HOME/Support/Security-Tools/SetDbPassword` command, where `$AVAYA_HOME` is an environmental variable pointing to the name of the installation directory specified during the Experience Portal software installation.
3. Enter the `bash SetDbPassword.sh update -u` *username* command, where *username* is the name of the user account whose password you want to change.
4. Type the password you want to use for this account and press `Enter`.

   When you change the password for the postgres account, Experience Portal stops and then restarts the **vpms** service.
5. Enter the `/sbin/service vpms status` command to verify if the **vpms** service has started.

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.04.00.02.00.00.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 locally instead of using an external application server, 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--> If the file log4j-1.2.15.jar is present in $CATALINA_HOME/
lib, then delete it from your external application server.

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

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

e--> Restart the external application server.

Please restart the system now !
```

Note:

The Primary server folder `$POM_HOME/DDapps/lib*` and the External Application Server folder `$CATALINA_HOME/lib` must contain the same files. If the External Application Server folder `$CATALINA_HOME/lib` contains any other files than the Primary server folder `$POM_HOME/DDapps/lib`, ensure you keep only JAR versions of files that are available in `$POM_HOME/DDapps/lib`.

15. Restart the system by typing `reboot`.
16. Install Oracle driver or MS SQL driver. For more information, see Installing the Oracle driver on page 73 or Installing the MS SQL driver on page 74.
17. Configure the database. For more information, see Configuring the POM database on the primary POM server on page 46.
18. To enable classification of SIP response code 403 as `CALL_FORBIDDEN`, run the following command as root user:

    `$POM_HOME/bin/updatePOMConfig CallForbidden true`

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 locally instead of using an external application server, 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--> If the file log4j-1.2.15.jar is present in $CATALINA_HOME/
lib, then delete it from your external application server.

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

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

e--> Restart the external application server.

Please restart the system now !
```

Note:

The Primary server folder `$POM_HOME/DDapps/lib*` and the External Application Server folder `$CATALINA_HOME/lib` must contain the same files. If the External Application Server folder `$CATALINA_HOME/lib` contains any other files than the Primary server folder `$POM_HOME/DDapps/lib`, ensure you keep only JAR versions of files that are available in `$POM_HOME/DDapps/lib`.

16. Restart the system by typing `reboot`.

Running scripts on the existing POM server after Experience Portal upgrade

About this task

Use this procedure if you upgrade Experience Portal on the POM server.

Procedure

1. To stop vpms, run **`systemctl stop vpms`**
2. To stop POM, run **`POM stop`**
3. To stop httpd, run **`systemctl stop httpd`**
4. Run the following script:

   `$POM_HOME/bin/vpUpgrade.sh`
5. Run the following script:

   `$POM_HOME/bin/updateVPMSConf.sh`
6. To start httpd, run **`systemctl start httpd`**
7. To start vpms, run **`systemctl start vpms`**
8. To start POM, run **`POM start`**

Related links

Running scripts after EP upgrade to 8.1.2 when POM server connects to an Oracle database on page 38

Running scripts after EP upgrade to 8.1.2 when POM server connects to an Oracle database

About this task

If your POM server connects to an Oracle database, after you upgrade EP to Release 8.1.2, you must do the following:

Procedure

1. On Avaya Experience Portal, to stop vpms service, run **/sbin/service vpms stop**
2. To navigate to the database directory, run **cd $AVAYA_HOME/Support/Database**
3. To install the JDBC driver, run the following bash command:

   ./InstallOracleJDBC.sh
4. On the POM server, go to bin directory and run **./InstallPOMOracleJDBC**

Related links

Running scripts on the existing POM server after Experience Portal upgrade on page 38

Root partitioning and storage expansion for VMware-based system

About this task

Use this procedure to increase the storage of the root file when you deploy the POM system with Experience Portal 8.0 OVA or 8.0 AVL ISO with fresh installation option.

Procedure

1. Deploy OVA or AVL.
2. Turn off the system.
3. Use VMware to change the disk size to 500 GB from 160 GB.

   VMWare does not allow disk size expansion when snapshots are present.
4. Turn on the system.
5. Log in with root user account.
6. To check and note the partition size, run the following command:

   df /
7. To expand the disk size, run the following command:

   /opt/Avaya/LinuxInstaller/bin/expand_root.sh
8. Follow the instructions displayed on the screen, and then reboot the system.
9. To check and note the partition size, log in with root user account, and run the following command:

   df /
10. Use the system with larger disk size.

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 to do the following: • To specify a path to install POM • To specify a path to install POM Manager directory
`-p` <package name>	Use 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 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 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 in the following: • If you use -t with aux. • If you change install_type in aux.
-f<config file path>	Use 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 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 by 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 -p
   pomadminportal
   ```

3. Press `Enter`.

Installing POM on the auxiliary EPM server by 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 -p pomadminportal
   ```

3. Press `Enter`.

Chapter 5: POM configuration

Checklist for configuring a POM server

Planning tasks

Perform the following planning tasks.

Task	Reference	Notes	✔
Enabling Federal Information Processing Standards (FIPS)	See Enabling FIPS on page 132.	You can enable FIPS in Proactive Outreach Manager after installing Proactive Outreach Manager.Enabling FIPS is optional.	
Configure the POM database.	See Configuring the database on page 46.	Select the installation mode and the database type for configuring the database.	
Configure the POM servers.	See Configuring the POM server on page 55.	After you install the POM server, configure the POM server using the web interface.	
Configure Avaya Aura® Call Center Elite or Avaya Aura® Contact Center.	See *Administering Avaya Proactive Outreach Manager*, *Avaya Proactive Outreach Manager Integration*.	Integrate POM with Avaya Aura® Call Center Elite or Avaya Aura® Contact Center for agent functionality and running agent-based campaigns.	
Add users or assign POM specific privileges to existing users.	See Adding users on page 72.	Add users after adding the POM server.	
Change the default country setting.	See Changing Home Country on page 73.	Change the default country to a country of your choice.	
Exchange certificates for the Avaya Orchestration Designer application server.	See Exchanging certificates for Avaya Aura® Orchestration Designer application server on page 65.	To use the Avaya Orchestration Designer application server, you must exchange certificates between each application server and POM.	
Configure the application server.	See Configuring the applications and licenses on page 56.	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 a database instance for the POM database.
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 the section on Importing Certificate in POM truststore through Command Line Interface in *Implementing Avaya Proactive Outreach Manager*.

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
6. CCaaS-Outbound
```

9. Type `1` ,`2`, `3`, `4`, `5` or `6` 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 `y` and press `Enter`.

    The system displays the following message:

    ```
    Please select from one of the following choices:
    1. Test DB Connection
    2. Create POM Schema on the given DB
    3. Save database configuration
    4. Configure database settings
    5. Configure database settings for reports (Optional)
    6. Exit from this utility
    ```

    Type `4` and press `Enter`.

11. 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*.

12. 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.

       POM supports Geo-Redundancy on Standard/Enterprise edition of MS SQL database.

       If you enable Geo-redundancy, POM displays the Data Center Configuration page. For details, see *Administering Avaya Proactive Outreach Manager*.

    b. Type the Availability Group Listener FQDN.

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

13. Type the port number.

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

14. If you select the database type as `MSSQL`, then the system displays the following message:

    ```
    Please select an option connecting to MSSQL DB using SQL Server or
    Windows Authentication.
    1.SQLServer
    2.Windows
    Enter an option (1/2):
    ```

    If you select the database type as `Oracle`, then the system displays the following message:

    ```
    Please select an option connecting to Oracle DB using SID or
    Service Name.
    1.SID
    2.Service Name
    Enter an option (1/2):
    ```

    Type the appropriate option and press `Enter`.

15. Type the name of the database.
16. Type the username 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 hostname or FQDN of the database server.

17. To enable Secure Connection, type `y`, or to disable type `n`.

    POM 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 DB
    3. Save database configuration
    4. Configure database settings
    5. Configure database settings for reports (Optional)
    6. 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`.

    It creates the POM schema. You cannot use the database immediately, unless you save this configuration by using option 3 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 hostname, or the port number, type `4`.

21. POM 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 DB
    3. Save database configuration
    4. Configure database settings
    5. Configure database settings for reports (Optional)
    6. Exit from this utility
    ```

    To exit, type `6`.

    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`.

    For information about configuring a separate database for POM reports, refer Configuring separate database for POM Reports in *Implementing Avaya Proactive Outreach Manager guide*

Configuring separate database for POM Reports

About this task

Use this procedure to configure separate database for POM Reports only on the primary POM server. Do not use this procedure on the auxiliary POM server.

Before you begin

Complete POM implementation and POM database configuration.

Ensure that a replicated POM database is provisioned and is always up to date with the POM database. It is of the same type, same schema, and the same version as the active POM database and contains the same data as the active POM database.

Procedure

1. 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.

2. 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 the section on Importing Certificate in POM truststore through Command Line Interface in *Implementing Avaya Proactive Outreach Manager*.

3. Log in to the primary EPM as a root or sroot user.
4. Type `cd $POM_HOME/bin` and press `Enter`.
5. 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
   6. CCaaS-Outbound
   ```

6. Type `1` ,`2`, `3`, `4`, `5` or `6` 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)
   ```

7. Type `y`and press `Enter`.

   The system displays the following message:

   ```
   Please select from one of the following choices:
   1. Test DB Connection
   2. Create POM Schema on the given DB
   ```

```
3. Save database configuration
4. Configure database settings
5. Configure database settings for reports (Optional)
6. Exit from this utility
```

Type `5` and press `Enter`.

8. Type the database type.
9. Type the database server IP address or hostname.

   If Geo-Redundancy is enabled and database type is MSSQL, then type the Availability Group Listener FQDN of the replicated database, or IP address/hostname of the replicated database.

10. Type the port number.

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

11. If you select the database type as `MSSQL`, then the system displays the following message:

    ```
    Please select an option connecting to MSSQL DB using SQL Server or
    Windows Authentication.
    1.SQLServer
    2.Windows
    Enter an option (1/2):
    ```

    If you select the database type as `Oracle`, then the system displays the following message:

    ```
    Please select an option connecting to Oracle DB using SID or
    Service Name.
    1.SID
    2.Service Name
    Enter an option (1/2):
    ```

    Type the appropriate option and press `Enter`.

12. Type the name of the database.
13. 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 hostname or FQDN of the database server.

14. To enable Secure Connection, type `y`, or to disable type `n`.

The system will test the connection to the database. If the test connection fails, the system displays the reason for FAILURE on the console.

If the test connection is SUCCESS, then system displays the following message:

```
Do you want to save the values in Database(y/n)?
```

Type `y` and press Enter.

This will restart the VPMS service.

15. The system displays the following message:

```
Please select from one of the following choices:
1. Test DB Connection
2. Create POM Schema on the given DB
3. Save database configuration
4. Configure database settings
5. Configure database settings for reports (Optional)
6. Exit from this utility
```

To exit, type `6`.

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

Changing configuration mode

About this task

Use this procedure to change the POM configuration mode. Use the **`setConnectorMode.sh`** script for the following mode changes:

- AACC-SBP to AACC
- None to CC Elite
- None to AACC
- None to AACC-SBP
- None to Oceana

To make any other mode changes, re-install and reconfigure the POM database. For example, you can change the mode from AACC to CC Elite when you re-install and reconfigure the POM database.

Procedure

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

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

2. Run the following script:

$POM_HOME/bin/setConnectorMode.sh

POM 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
```

3. Type `1`, `2`, `3`, `4`, or `5`, and press `Enter`.
   - For an invalid mode change with this procedure, POM asks the user to re-install and reconfigure the POM database.
   - For a valid mode change, POM displays the following message:

     ```
     Current Contact Center Configuration mode is <current mode name>.
     ```

     ```
     Contact Center Configuration mode will change from <current mode
     name> to <new mode name>. Do you want to continue(y/n)?
     ```
4. Type `y` to confirm the mode change.
5. After POM asks to restart the vpms service, type `y`.

Manual dialing mode

Manual dialing

With the manual dialing feature, POM does not automatically dial a customer number. Instead, an agent uses third-party software or a device to manually dial a customer number. For a dedicated POM server setup in non-telephony mode, you can configure POM into non-telephony mode. However, in non-telephony mode, you cannot run the preview, predictive, or progressive campaigns. In this mode, POM does not have telephony communication such as SMS, voice, or voice notification to MPP. However, POM can have email campaigns.

Note:

With the new POM installations, the default configuration with telephony operations is enabled. When you upgrade POM, POM retains the existing configuration.

Related links

Converting POM into non-telephony mode on page 54

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 53

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 **Proactive Outreach** > **Manager**.
3. Click **Configurations** > **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** > **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 *Administering Avaya Proactive Outreach Manager*.
   c. Click **Continue**.
   d. Select the **Trust this certificate** check box.
   e. Click **Save**.
5. Click **Configurations** > **Servers** > **Outbound Settings** > **EPM** and provide the user name and password with Outcall privileges.
6. Click **Save**.

7. To start POM Manager, click **Configurations** > **Servers** > **POM Manager**.
8. If you have enabled Geo-redundancy, do the following:
    a. Click **Proactive Outreach** > **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 **Proactive Outreach** > **Manager**.
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 username and password provided during the Avaya Experience Portal installation.
2. To configure the applications locally 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 URL.
3. The following steps are to configure the Avaya Orchestration Designer applications only locally 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 username.

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. If the file `log4j-1.2.15.jar` is present in `$CATALINA_HOME/lib`, then delete it from your external application server.

Note:

The Primary server folder `$POM_HOME/DDapps/lib*` and the External Application Server folder `$CATALINA_HOME/lib` must contain the same files. If the External Application Server folder `$CATALINA_HOME/lib` contains any other files than the Primary server folder `$POM_HOME/DDapps/lib`, ensure you keep only JAR versions of files that are available in `$POM_HOME/DDapps/lib`.

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

d. 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_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_G
CM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_12
8_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_EMPTY_RENEGOTIATION_IN
FO_SCSV"/>
```

e. 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=T
LSv1.2"
```

5. Restart the external application server.

   Note:

   The Primary server folder `$POM_HOME/DDapps/lib*` and the External Application Server folder `$CATALINA_HOME/lib` must contain the same files. If the External Application Server folder `$CATALINA_HOME/lib` contains any other files than the Primary server folder `$POM_HOME/DDapps/lib`, ensure you keep only JAR versions of files that are available in `$POM_HOME/DDapps/lib`.

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 hostname 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

POM uses digital certificates for internal and external communications. POM communicates with dependent components such as Experience Portal and Application server through these certificates.

The following are the requirements for a custom certificate:

- A user certificate
- The private key of the user certificate
- The 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 also provides the user certificate and a private key in PKCS12 format.

The following are the two methods for using certificates in POM:

- Generating self-signed certificates 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 Fully Qualified Domain Name (FQDN) of the system in the Common Name (CN) and Subject Alternate Name (SAN) attributes of the certificate. When adding the 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

To generate a self-signed certificate, use the internal utilities that POM provides.

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 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 63.

   The `pomCertificateGenerate.sh` creates a self-signed certificate with one IP address in the (Subject Alternate Name) SAN 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 the 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

Import a CA-signed certificate and replace the existing POM certificate. 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 POM 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 POM 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** > **Proactive Outreach** > **Configurations** > **Servers**.
3. On the Servers page, in the **POM Server Name** column, click the server name.
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 **Proactive Outreach** > **Manager**.
3. On the menu bar, click **Configurations** > **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 **Proactive Outreach** > **Manager**.
   c. Click **Configurations** > **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 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 **Proactive Outreach** > **Manager**.
3. Click **Configurations** > **Trusted Certificates**.
4. On the 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 **Proactive Outreach** > **Manager**.
5. Click **Configurations** > **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. If the file `log4j-1.2.15.jar` is present in `$CATALINA_HOME/lib`, then delete it from your external application server.

      Note:

      The Primary server folder `$POM_HOME/DDapps/lib*` and the External Application Server folder `$CATALINA_HOME/lib` must contain the same files. If the External Application Server folder `$CATALINA_HOME/lib` contains any other files than the Primary server folder `$POM_HOME/DDapps/lib`, ensure you keep only JAR versions of files that are available in `$POM_HOME/DDapps/lib`.

   c. 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_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_G
CM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_12
8_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_EMPTY_RENEGOTIATION_IN
FO_SCSV"/>
```

Note:

d. In the Command Line Interface (CLI), navigate to `$APPSERVER_HOME/conf`.

e. Run the command **`keytool -keystore myTrustStore -genkey -alias dummy -keyalg RSA`**

f. 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 **Proactive Outreach** > **Manager**.
15. Click **Configurations** > **Trusted Certificates**.
16. Import the certificate exported in step 9h.
17. In the **Name** field, type the name of the certificate. For example, appserver.
18. Click **Continue**.
19. Click **Save**.
20. 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 **Proactive Outreach** > **Manager**.
3. In the drop-down menu, click **Configurations > 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 beginning date and time of the logs.

   - 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 zookeeper service, type:
  - `service pomzookeeper start`
  - `service pomzookeeper stop`
  - `service pomzookeeper status`

Adding users to the POM system

About this task

By default, the Avaya Experience Portal administrator has all POM privileges. The administrator can add new users similar to that in Avaya Experience Portal.

Before you begin

POM installation must be in running status.

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 create.

   The 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

Before you begin

Ensure that you set the Home country at initial installation and do not change the Home country setting.

Procedure

1. In the navigation pane of Experience Portal, click **Proactive Outreach** > **Manager** > **Configurations** > **Global Configurations**.
2. In the Contact settings, select a **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.

Before installing the Oracle driver for POM, you must download and install the Oracle driver for Avaya Experience Portal. For more information about downloading and installing the Oracle driver for Avaya Experience Portal, see the following guides on the Support site at http://support.avaya.com:

- *Implementing Avaya Experience Portal on a single server*
- *Implementing Avaya Experience Portal on multiple servers*
- *Upgrading to Avaya Experience Portal*

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 the 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. To create a folder `~/POMOracleJDBC`, run the following command:

   ```
   mkdir –p ~/POMOracleJDBC
   ```

4. Copy the downloaded driver files to the folder `~/POMOracleJDBC`.
5. To install the JDBC driver, type the following:

   ```
   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. Then 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 use Avaya Proactive Outreach Manager with the MS SQL database. To configure the POM database on MS SQL, download the MS SQL driver `mssql-jdbc-10.2.0.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 use the MS SQL database as a contact data source.

Procedure

1. Download the `mssql-jdbc-10.2.0.jre8.jar` MS SQL driver from https://www.microsoft.com.

   Note:

   If you cannot 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-10.2.0.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-10.2.0.jre8.jar` to the folder `~/POMMssqlJDBC`.
5. To install the JDBC driver, type the following 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. Then, rename the file to `mssql-jdbc-10.2.0.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 POM system, POM stores the events at the following location:

`$POM_HOME/kafka_server/kafka-store`

By default, POM keeps event-specific data of the 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 the retention period and the purge interval of the Kafka server.

The default retention period is three days (72 hours). To modify the retention period, you can set the properties in the following files:

File name	Property name
server.properties	`log.retention.hours` = *72*
zookeeper.properties	`autopurge.purgeInterval` = *168*

Setting up external Kafka

About this task

Use this procedure to set up external Kafka server. The required version of Kafka server is 2.13.-3.2.0.

Procedure

1. Access POM Primary.
2. Ensure the successful execution of ./enabledKafkaHA.sh script on the primary POM server with the details of the external Kafka server.
3. Add external server machine entry in the `/etc/hosts` file on all POM servers.
4. Copy `$POM _HOME/kafka_server` directory from primary POM server to external Kafka server.
5. Set `KAFKA_HOME` environment variable to `kafka_server` directory.
6. Remove all data and directories from `$KAFKA_HOME/kafka_store` directory.
7. Add entries for all POM servers in `etc/hosts` file on external Kafka machine.

Configuring ZooKeeper

Procedure

1. Open `$KAFKA_HOME/config/zookeeper.properties` file and change daraDir to `$KAFKA_HOME/kafka-store/zookeeper`.

   You can find the property details in the ZooKeeper administrator's guide on Apache ZooKeeper web site.
2. Create zookeeper directory, under `$KAFKA_HOME/kafka-store`.
3. Create myid file in `$KAFKA_HOME/kafka-store/zookeeper` directory.

   The `myid` file must contain unique zookeeper id and it must match with x in server.x mentioned for external Kafka entry in `$KAFKA_HOME/config/zookeeper.properties`.

   Example: If server.3 is mentioned, 3 becomes the zookeeper ID for `myid` file.

4. The following are the Kakfa server configuration properties, highlighted in bold text, that gets updated after above configurations:

```
dataDir=<KAFKA_HOME>/kafka-store/zookeeper
secureClientPort=2182
tickTime=2000
initLimit=5
syncLimit=2
server.1=<IP_Primary_POM>:2888:3888
server.2=<IP_AUX_POM>:2888:3888
server.3=<IP_EXTERNAL_KAFKA>:2888:3888
```

5. Start ZooKeeper using the command `$KAFKA_HOME/bin/zookeeper-server-start.sh $KAFKA_HOME/config/zookeeper.properties`.

Configuring Kafka

Procedure

1. Open `$KAFKA_HOME/config/server.properties` file and change `log.dirs` to `$KAFKA_HOME/kafka-store/kafka`.
2. Modify `broker.id` to unique number across all servers.

   For example, if `broker.id` on primary is 1 and aux server is 2, then the broker.id on external machine must be any valid positive number except 1 or 2.
3. Update the hostname in listeners and advertised listeners to the hostname of the external server machine.
4. Generate keyStore using below keytool command: **`keytool -genkeypair -keystore <keystore> -dname "CN=test, OU=<Organization Unit name>, O=<Organization name>" -keypass <keypwd> -storepass <storepass> -keyalg RSA -alias <alias_name> -ext SAN=dns:<DNS_NAME>,ip:<IP_ADDRESS>`**.

   For example: **`keytool -genkeypair -keystore pomKeyStore -dname "CN=test, OU=POM, O=Avaya" -keypass changeit -storepass changeit -keyalg RSA -alias externalkafkaserver -ext SAN=dns:test.abc.com,ip:127.0.0.1`**
5. Verify the generated keystore.
6. Provide the path of the keystore generated in step 4 in `ssl.keystore.location` of `$KAFKA_HOME/config/server.properties`.
7. Export the generated server certificate from keystore using the following command **`keytool -export -alias <alias name> -storepass changeit -file <cert name> -keystore <keystore>`**.

   For example: **`keytool -export -alias externalkafkaserver -storepass changeit -file pim.crt -keystore pomKeyStore`**

8. Verify the generated certificate.
9. Import the certificate generated in step 7 to the pomTrustStore of the primary server using POM Trusted Certificates page.

   Note:

   Restart pomkafka on all POM servers after updating pomTrustStore.

10. Copy the modified `$POM_HOME/config/pomTrustStore` of the primary POM server and paste it on external Kafka server and update `ssl.truststore.location` property in `$KAFKA_HOME/config/server.properties`.
11. Change ssl.keystore.password, ssl.key.password, and ssl.truststore.password in `$KAFKA_HOME/config/server.properties`.

    Note:

    Set the password that is used while generating certificate.

12. The following are the Kafka server configuration properties, highlighted in bold, that will get updated after the above configurations:

```
broker.id=3
num.network.threads=3
num.io.threads=8
socket.send.buffer.bytes=102400
socket.receive.buffer.bytes=102400
socket.request.max.bytes=104857600
log.dirs=<KAFKA_HOME>/kafka-store/kafka
num.partitions=1
num.recovery.threads.per.data.dir=1
offsets.topic.replication.factor=3
transaction.state.log.replication.factor=3
transaction.state.log.min.isr=1
log.retention.hours=72
log.segment.bytes=1073741824
log.retention.check.interval.ms=300000
zookeeper.connect=148.147.XX.XX:2182,148.147.XX.XX:2182,148.147.XX.XX:2182
zookeeper.connection.timeout.ms=30000
group.initial.rebalance.delay.ms=0
listeners=SSL://kafkaexternal:9093
advertised.listeners=SSL://kafkaexternal:9093
ssl.keystore.location=/opt/config/pomKeyStore
ssl.keystore.password=changeit
ssl.key.password=changeit
ssl.truststore.location=/opt/config/pomTrustStore
ssl.truststore.password=changeit
ssl.client.auth=required
ssl.keystore.type=JKS
ssl.truststore.type=JKS
ssl.enabled.protocols=TLSv1.2
ssl.cipher.suites=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_1
28_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128
_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_EMPTY_RENEGOTIATION_INFO_SCS
Vsecurity.inter.broker.protocol=SSL
default.replication.factor=3
```

13. Start Kafka using the following command:

```
$KAFKA_HOME/bin/kafka-server-start.sh $KAFKA_HOME/config/
server.properties
```

Creating appserver.service

Before you begin

Use this procedure if you are using an application server installed locally on any of the primary or auxiliary POM servers.

Procedure

1. On POM system where application server is installed and is being used, verify whether the `appserver.service` file exists. Use the command **`ls -l /etc/systemd/system/appserver.service`**.

   If the file exists, you do not need to take any further action.

2. If the file is not present, ensure the following environment variables are set:
   a. echo $APPSERVER_HOME
   b. echo $VP_HOME
3. Ensure that each command mentioned in step 2 returns a valid path.
4. If the paths are valid, run the command: **`sed "s@%%APPSERVER_HOME%%@$APPSERVER_HOME@" $VP_HOME/Support/AppServer/appserver.service > /etc/systemd/system/appserver.service`**

Creating or deleting directory structure for import and export

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

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.

SFTP configuration in data source

For 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 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 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 `$POM_HOME/Upload/CollectionData.csv` path in the POM system after SFTP. Then this file is backed up at `$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

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.

SFTP configuration in data source

When the DNC list is imported from the CSV file using the 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 SFTP configuration in data source

When the administrator executes the splitter from CSV file using the 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 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)

Following are the mandatory directory structures for NFS mounts:

Note:

`$POM_HOME` environment variable 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 in earlier releases of POM 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 **Manager** > **Configuration-** > **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 **Proactive Outreach** > **Manager** > **Configuration** > **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_server/config/server.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 and IP address similar to the values specified in the configuration tool.
4. If you are using the POM server (database on same server), 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 **Manager** > **Configuration-** > **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 **Proactive Outreach** > **Manager** > **Configuration** > **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_server/config/server.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.
   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 **mpp** service by entering the **service mpp stop** command.

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 neat tool as described in your Red Hat documentation.
   c. 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.
   d. 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`

eventSettingOperation utility

Use this utility to:

- Apply the customized settings to alarms and events of POM 4.1 on premise.
- Rollback to the default settings of alarms and events of POM 4.1.

Configuring Event setting

About this task

Use this procedure to do the following:

- Set the parameters of new alarms.
- Enable POM to turn on an alarm.
- Enable POM to turn off an alarm.
- Update the event level, the throttle interval, and the alarm severity of an alarm.

Before you begin

Ensure that you have the credentials of a root user.

Procedure

1. Open an SSH session to the primary POM server.

   You can use an application such as PuTTY.

2. Go to `$POM_HOME/bin`
3. To run the EventSetting tool, run the following command:

   `./eventSettingOperation.sh`

4. The EventSetting tool displays the following:

```
Available Options for Event Setting
1.    Exit EventSetting Operation
2.    Update to Default New Event Setting
3.    Update POM Event Level based on EventCode
4.    Update ThrottleInterval based on EventCode
5.    Update EP Alarm Severity based on EventCode
6.    ON/OFF Alarm based on EventCode
7.    Show All Available Operations
```

5. To apply the default EventSetting using POM release 4.1, select 2.
6. To update the event level based on the EventCode, select 3.
7. To update the throttle interval based on the EventCode, select 4.
8. To update the alarm severity level based on the EventCode, select 5.

   If you select this option, restart the vpms service.

9. To enable POM to turn on or turn off the alarm based on the EventCode, select 6.

   If you select this option, restart the vpms service.

Result

During a fresh installation or an upgrade, based on the Connector Mode, POM does the following:

- Reads the settings in `PIMEventCodeType` file.
- Inserts the eventsetting in the `pim_event_setting` table in the POM database.

- Updates the new entries in the `pim_event_setting` table in the POM database.
- Generates alarms based on the setting you apply.
- Utilizes a buffer time of 5 minutes if POM has not read the eventsetting.

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.

POM creates and manages the `TrustStore.xml` file. POM creates this file when a user adds or deletes a certificate in the POM truststore using the POM User interface. POM copies this file on all the POM servers in a multi-POM setup. Do not edit this file manually to avoid connectivity failure issues between POM server and other servers.

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.

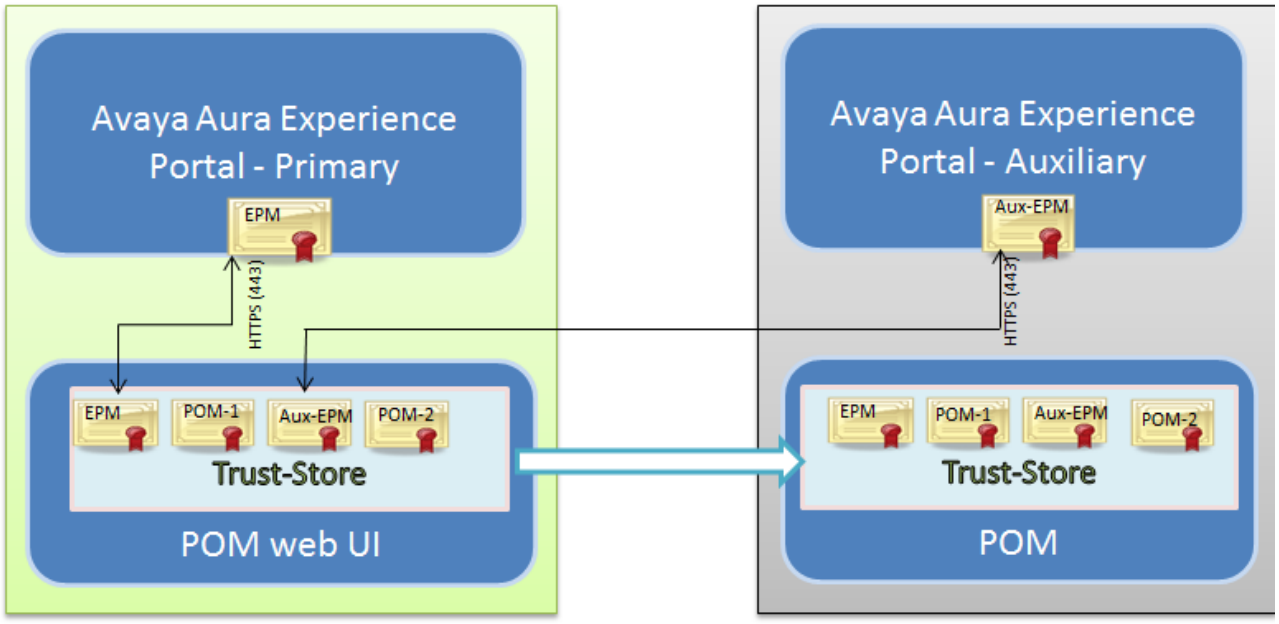
POM integrates with Avaya Oceana®, Context Store, AES, and AACC. You must import or fetch respective certificates on the POM Trusted Certificate page. To add the POM server installed on

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

Field	Description
Name	The name of the certificate.

Table continues…

Field	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 a custom CA certificate and then POM with a custom certificate, ensure that you establish communication among 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 **Proactive Outreach** > **Manager**.
3. In the content pane, click **Configurations** > **Trusted Certificates**.

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

5. On the Add Certificates page, do the following:
   a. In **Name**, type the name of the certificate.
   b. In **Enter Certificate Path**, 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. For the changes to take effect, restart all POM services on the server.

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 **Proactive Outreach** > **Manager**.
3. Click **Configurations** > **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 **Proactive Outreach** > **Manager**.
3. Click **Configurations** > **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 **Proactive Outreach** > **Manager**.
3. Click **Configurations** > **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** > **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 as a Disaster Recovery solution 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 can also be referred to as a data center in this context.

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 a POM system on more than one site.

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

- Active

  Specifies the production site.

- Standby

  Specifies the redundant or standby site.

When a site has a complete failure, for example, because of a power outage, network outage, or natural disaster, the standby site can be used for production. Geo-Redundancy enables continued operation with minimized impact if an outage occurs. In case of POM, this is achieved through a manual failover process and requires administrator intervention to switch operations from the active site to the standby site and vice versa. For Geo-Redundancy, the components or products on which POM depends must be administered identically in all the sites.

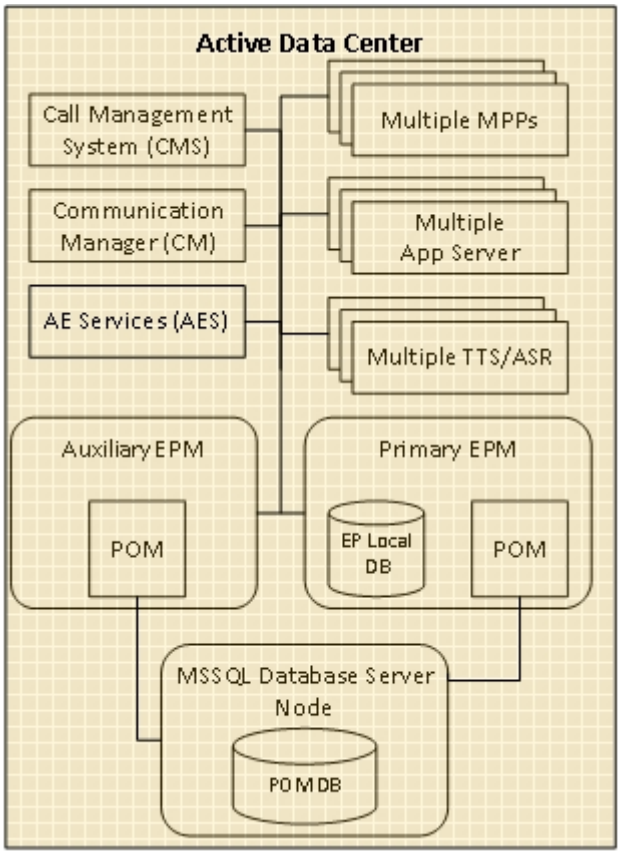
Architecture

The diagram below lists the key components that are part of the Active Data Center in the solution. The Standby Data Center needs to be deployed as a separate entity with an identical architecture.

- Microsoft SQL Server for POM database: You can enable Geo-Redundancy only when POM is installed in the CCElite mode.
- POM supports Oracle, Postgres, and MSSQL databases, but geo-redundancy is supported only with the MSSQL database.

- 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 must be 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.



- Avaya Aura as communication infrastructure including Communication Manager, Session Manager and the Application Enablement Server.

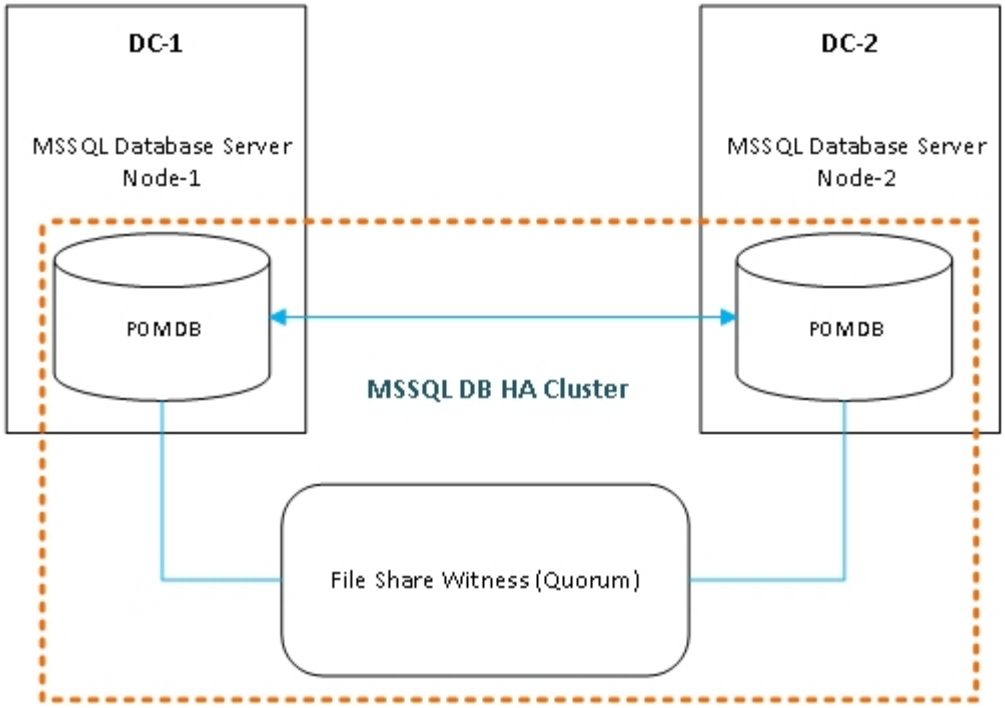
  Communication Manager must be deployed along with Survival Core Server in the standby site (fka. Enterprise Survivable Server - ESS). Application Enablement Services is configured in the Geo-Redundancy HA mode.
- Avaya Call Management System as the Reporting solution. CMS needs to be deployed in the Geo-Redundant HA (GRHA) mode.
- Avaya Experience Portal including the Experience Portal Manager (EPM) (multiple EPMs in case of local redundancy), multiple Media Processing Platform (MPP), application and speech servers – as the platform POM is deployed on.

Note that the Experience Portal in the standby data center is a separate system, and not an auxiliary.

- Experience Portal must be administered identically in all sites when related to geo-redundancy. This includes organizations, zones, and users created on Experience Portal and 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 and administer Experience Portal identically on all data centers.
- POM software running on the EPMs and the POM database.

  You can enable Geo-Redundancy only when POM is installed in the CCElite mode with Microsoft SQL Server (MSSQL) as the database. POM utilizes the MS-SQL AlwaysOn feature as the foundation for Geo-Redundancy. Geo-Redundancy is not supported when an Oracle or PostgreSQL database is used with POM.

A sample setup of the database is shown in the following diagram.



POM depends on a database for all the activities, hence, having an important role for setting up Geo-Redundancy. 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 utilized to implement POM Geo-Redundancy.

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

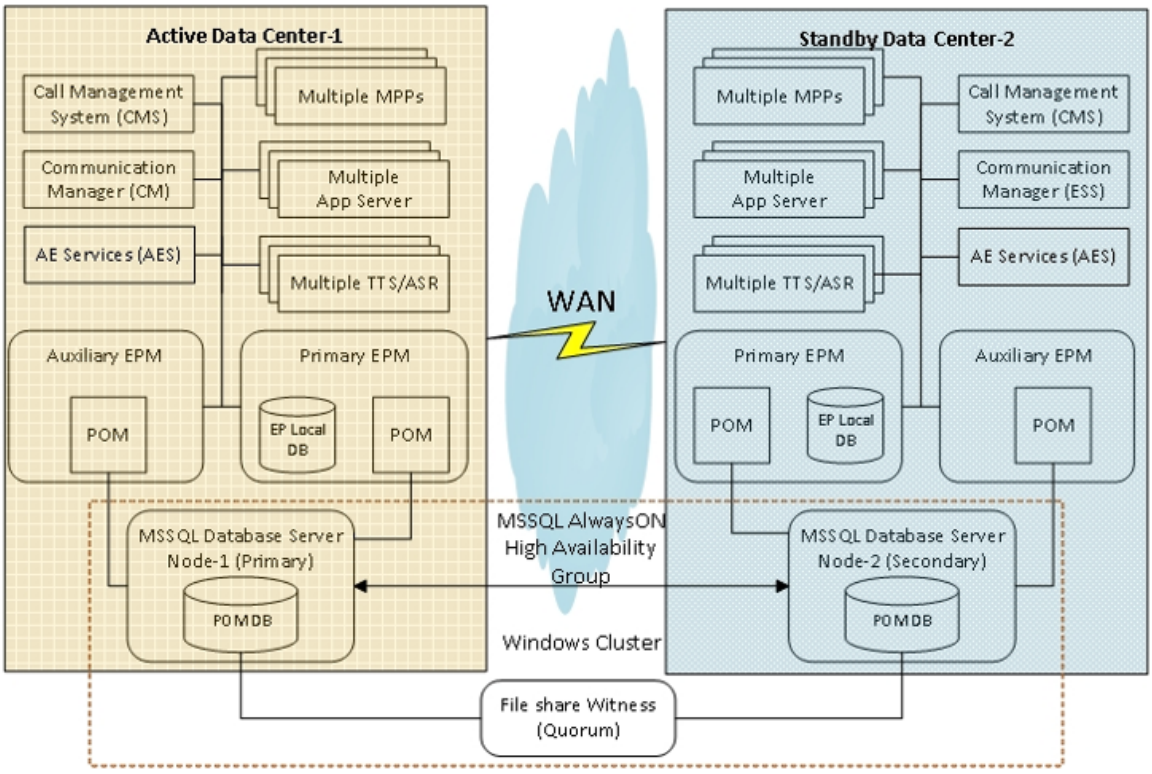
Customers must ensure that the primary instance of the MSSQL database is always on the active data center. This ensures that the database is always in close proximity to the POM server and

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 a minimum of 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.

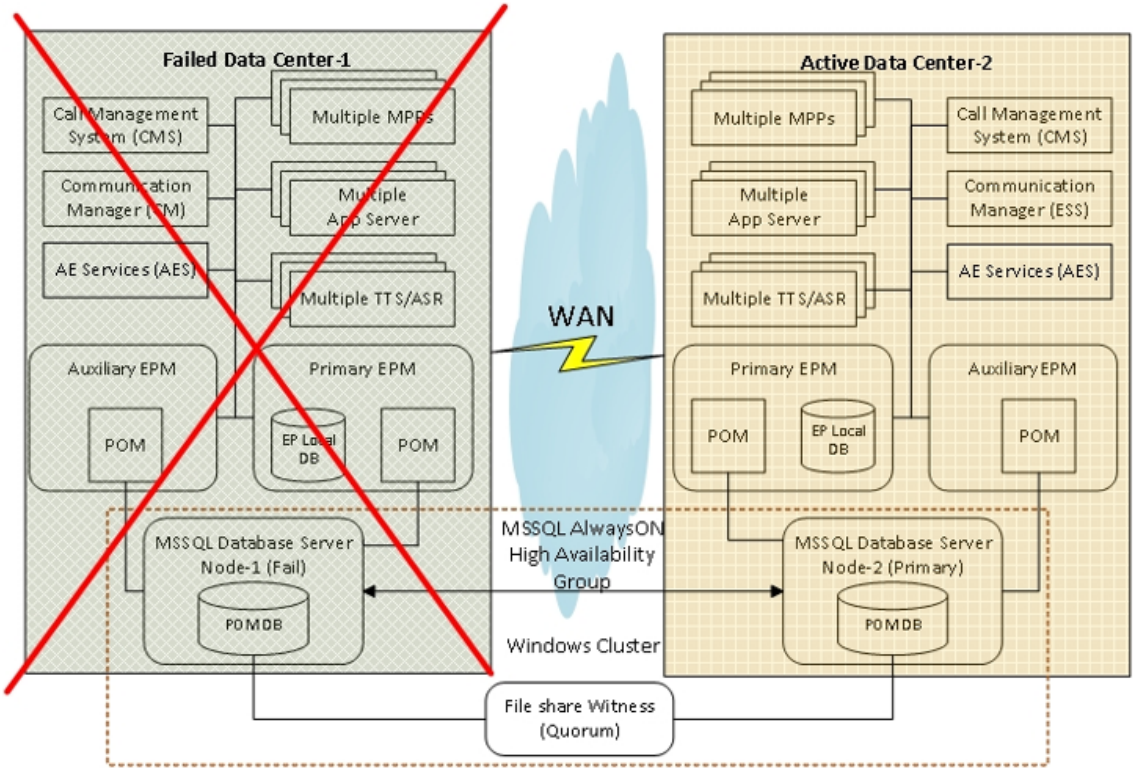
The following diagram is an example of two data centers configured for Geo-Redundancy using the architecture discussed:



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. A minimum of two database nodes are required. One in each data center. Additional nodes or the File Share Witness shown in the diagram are optional because the database needs to be configured for manual failover across the two sites.

When the active Data Center-1 fails, as shown in the diagram below, 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 is changed to become the Primary when Data Center-1 fails. The change of role of the database from secondary to primary requires manual intervention because the MSSQL database is configured for manual 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 supported database version and ensure that the database is pre-configured with its AlwaysOn feature and Manual Failover.
- Use MSSQL in asynchronous commit mode as the communication is performed over the WAN between Data Center -1 and Data Center -2.
- POM supports Geo-Redundancy on Standard/Enterprise edition of MSSQL.
- Ensure that the primary instance of the MSSQL database is on the active data center.
- Configure MS SQL 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.
  - Note that Experience Portal is deployed as 2 independent systems. One Experience Portal system per data center. ACTIVE-ACTIVE refers to the way Experience Portal licenses are handled and that both systems can handle traffic in inbound scenarios.
- Configure Communication Manager in Data Center 1 with Surviable Core Server (ESS) 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 a 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 105.

  POM Geo-Redundancy with MSSQL Always On High Availability requires:
- A local Availability Group on each Data Center, grouping the local databases of the Data center.
- A Distributed Availability Group (AG) connecting both Data centers in Asynchronous mode.
- POM servers on each Data center must point to their local AG to support local Database failover within the local AG and not to the Distributed Availability Group (DAG).
- **Note:**

  Pointing POM servers to the Distributed Availability Group (DAG) is not supported.

Best practices for implementing Geo-Redundancy

MSSQL Availability Group Listener FQDN

Ensure that you configure the POM servers in all the Data Centers to point to the MSSQL Availability Group Listener FQDN. Do not configure the POM servers to point to the MSSQL database server ip/hostname/FQDN.

Primary Database Node

Ensure that the MSSQL database node for an Active Data center is always the primary replica.

If there is active Data Center-1 to standby Data Center-2 failover, you must first execute the database failover. After completing the database failover execution, ensure that the database node on the Data Center-2 is now the primary replica. Then, execute the POM failover where the Data Center-1 is marked as standby, and the Data Center-2 is marked as active.

Availability mode in Database

You must configure the MSSQL primary replica and secondary replica with the asynchronous commit mode. This allows the primary replica to commit the transaction without waiting for the secondary replica. This is helpful when the primary replica and the secondary replica are placed at

a significant distance, and the performance on the active POM Data Center is more important than the data synchronization.

Availability-Group Failover

Ensure that you configure the database with Manual failover, not with Automatic failover. The failover behavior for each secondary replica depends on which availability replica is currently the primary replica.

Refer to Microsoft documentation for:

- Additional details on “Always On” feature.
- Help on how to configure availability to asynchronous commit mode for all POM database nodes.
- Help on configuring failover mode to manual for all the POM database nodes configured in the availability group.

POM Servers

Use the **Add POM Server** option to add the POM servers of all the Data centers. Only after you add all the POM servers, execute the Data center configuration to add the Data Center. For example, If Data Center-1 has three POM servers, use the **Add POM Server** option to sequentially add the three POM servers. On the Data Center Configuration page, use the **Add Data Center** option to create Data Center-1.

Later, to add a Data Center-2 with three POM servers, use the **Add POM Server** option to add all the three POM servers. Then, on the Data Center Configuration page, you can use the **Add Data Center option** to create Data Center-2.

Note:

- The name of all the POM servers across all the Data Centers should be unique.
- The hostname of all the POM servers across all the Data Centers should be unique.
- When you add POM servers using the **Add POM Server** option:
  - If the POM server entries are available on the POM server page, verify the POM server entries in the pim_server table of the POM database.
  - If the POM server entries are present in the pim_server table for the corresponding added POM server, you can skip the addition of the POM server on the Add POM Server page.
  - If you still see the POM server entries on the POM Server page despite corresponding POM server entries are unavailable in the pim_server table, you need to delete the POM server entries from the page and again add the POM server from the Add POM Server page.
- Always use an active Geo-redundancy server for making REST requests.

Dedicated Experience Portal Zones for POM

Ensure that you provide dedicated zones for POM on the active as well as standby Experience Portal. This simplifies the management of resources substantially in case of running multiple applications on Experience Portal.

Stop processes

Before you add a Data Center using the **Add Data Center** option, ensure to stop all the POM processes on all the POM servers of all the active and standby Data Centers.

Experience Portal synchronization

POM is deployed on Experience Portal as a managed application. Organizations, zones, and users created on Experience Portal are stored in the local database of Experience Portal. When POM services start, this data is copied 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.

Special consideration is required if you are using Experience Portal to host other applications in addition to POM. Sufficient resources must be available on the primary and standby system.

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 must be a 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, App Servers, 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, set the value as three hundred for parameter hikari_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 `User`, type the name of the user.
   h. For `Password`, type the password.
   i. For `Does Database require secured connection (Y/N)`, type `Y` or `N` depending on your requirement.
3. Choose the appropriate option to test the connection to the database.
4. **(Optional)** If the test succeeds and the system indicates that the connection is secure, save the configuration.
5. Restart all POM services.

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 `User`, type the name of the user.
   h. For `Password`, type the password.
   i. 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.

Enabling Geo-Redundancy for a Primary POM server on a PR site

About this task

Use this procedure to enable Geo-Redundancy on a primary POM server in the PR site.

Before you begin

- Install the primary POM server on the PR site.
- Configure the Distributed Availability Group (DAG) for 2 MSSQL databases on each Data Center:

- Configure the Distributed Availability Group (DAG) HA POM database on PR site

  High Availability database in PR site and HA DB in DR site.
- Configure one data center on the PR site
- Configure one data center on the DR site
- Ensure that the availability group only on the PR site has 2 MSSQL servers as 2 nodes.
- Configure the IP addresses of two Availability Group listeners.
- Install the MSSQL driver script on all POM servers.

Procedure

1. Log on to the POM server as a root user.
2. In the command prompt, type the following commands:
   a. Type cd $POM_HOME and press Enter.
   b. Type cd bin and press Enter.
   c. Type ./installDB.sh and press Enter.
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 first Availability group listener IP address.
   e. For Database Port, type the port number of the database.
   f. For Database Name, type the name of the database.
   g. For User, type the name of the user.
   h. For Password, type the password.
   i. For Does Database require secured connection (Y/N), type Y or N depending on your requirement.
4. Choose the appropriate option 1, 2: to test the connection , create schema to the database.
5. If the test succeeds and the system indicates that the DB schema is created successfully, select option 3 to save the configuration.
6. Restart all POM services.
7. On the PR site, on the POM webpage, do the steps to add a Data Center configuration.

Enabling Geo-Redundancy for a Primary POM server in DR site

About this task

Use this procedure to enable Geo-Redundancy for a Primary POM server in DR site.

Before you begin

Do the failover steps for the POM Database in the PR site.

Do the failover steps for the POM database in the DR site.

Do the steps on POM Datacenter configuration.

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 **Proactive Outreach** > **Manager**.
3. Click **Configurations** > **Data Center configuration**.
4. Select the currently active Data Center-1 and make it standby.
5. Click **Configurations** > **Servers** > **POM Manager**.
6. Log in to all the POM servers configured in Data Center-1 as a root user. Stop the POM services.
7. Verify that the status of all the services of the new standby Data Center-1 are stopped.
8. From the MSSQL Database, do Failover step from First Availability group to Second Availability group.
9. Ensure that the Distributed Dashboard displays the database Second Availability group of the standby Data Center-2 as Primary.
10. Log on to the POM server as a root user.
11. In the command prompt, type the following commands and press Enter.
    a. cd $POM_HOME
    b. cd bin
    c. ./installDB.sh
12. 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 Second Availability group listener IP address.

e. For Database Port, type the port number of the database.
f. For Database Name, type the name of the database.
g. For User, type the name of the user.
h. For Password, type the password.
i. For Does Database require secured connection (Y/N), type Y or N depending on your requirement.

13. Choose the option 1 to test the connection.
14. DO NOT select option 2.
15. Then select option 3 to Save the configuration.
16. Restart all POM services.
17. After that, do all configurations on POM webpage for DR site following steps to active Data Center Configuration.
18. After that, check the POM data is displaying correctly as same as POM in PR site.

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 **Proactive Outreach** > **Manager**.
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 **Proactive Outreach** > **Manager**.
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

In a standby data center, the status of the services are as follows:

Service	Status
Campaign Manager	STOPPED
Campaign Director	STOPPED

Table continues…

Service	Status
Agent Manager	STOPPED
ActiveMQ	STOPPED
Rule Server	STOPPED
Kafka Server	RUNNING
Advance List Management	STOPPED
POM Agent SDK	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 **Proactive Outreach** > **Manager**.
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 **User**, type the name of the user.
16. In the **Password**, type the password of the user.
17. In the **Does Database require secured connection (Y/N)**, type `Y` or `N` depending on your requirement.
18. Choose the appropriate option to test the database connection.
19. **(Optional)** If the test succeeds and the system indicates that the connection is secure, save the configuration.
20. To exit the `installDB.sh` script, select the option 5 and press **Enter**.
21. 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 **Proactive Outreach** > **Manager**.
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 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 **Proactive Outreach** > **Manager**.
3. Click **Configurations** > **Data Center configuration**.
4. Select the currently active Data Center-1 and make it standby.
5. Click **Configurations** > **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 119.
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 **Proactive Outreach** > **Manager**.
14. Click **Configurations** > **Data Center configuration**.
15. Select Data Center-2 and set it as `Active`.
16. Log off and log in again to the Avaya Experience Portal web console.
17. In the navigation pane, click **Proactive Outreach** > **Manager**.

    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.

18. Click **Configurations** > **Zone Configuration**.
19. In the CD Zone Configuration area, select the Campaign Director for all zones of newly active Data Center-2.

20. Click **Save and Apply**.
21. In the AM Zone Configuration area, select the Agent Manager for all zones of newly active Data Center-2.
22. Click **Save and Apply**.
23. Click **Configurations** > **CCElite Configurations**.
24. 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`.
25. Click **Configurations** > **Servers** > **POM Manager**.
26. 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.
27. Verify the status of all the services of the newly active Data Center-2 are as listed in the Service status on page 119.

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 **Proactive Outreach** > **Manager**.
7. Click **Configurations** > **Data Center configuration**.
8. Select Data Center-1 and set it as Standby.
9. Select Data Center-2 and set it as `Active`.
10. Log off and log in again to the Avaya Experience Portal web console.
11. In the navigation pane, click **Proactive Outreach** > **Manager**.
12. Click **Configurations** > **Zone Configuration**.
13. In the CD Zone Configuration area, select the Campaign Director for all zones of newly active Data Center-2.
14. Click **Save and Apply**.
15. In the AM Zone Configuration area, select the Agent Manager for all zones of newly active Data Center-2.
16. Click **Save and Apply**.
17. Click **Configurations** > **CCElite Configurations**.
18. 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`.
19. Click **Configurations** > **Servers** > **POM Manager**.
20. 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.
21. Verify the status of all the services of the newly active Data Center-2 are as listed in the Service status on page 119.

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 119.
- 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 126.

Recovering a campaign

Procedure

1. Stop the campaign from Supervisor Dashboard.
2. 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 **Proactive Outreach** > **Manager**.
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 **Proactive Outreach** > **Manager**.
14. Click **Configurations** > **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** > **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 119.

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 **Proactive Outreach** > **Manager**.
3. Click **Configurations** > **Data Center configuration**.
4. Select the currently active Data Center-2 and make it standby.
5. Click **Configurations** > **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 119.
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 **Proactive Outreach** > **Manager**.
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** > **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** > **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 119.

Database failover within the same Data Center

About this task

Use this procedure for POM to failover the database within the same data center if maintenance is planned only for database. In this case POM services are also required to be restarted along with the database failover. This type of failover must be performed during maintenance hours when POM is non-operational.

Note:

POM supports manual failover of the database within the same Data Center. Automatic failover of the database is not supported.

Before you begin

- Ensure that the agent-less campaigns such as email, SMS, and notifications are not running.
- Log off all agents from the system.

- Stop all campaigns.

Perform the following procedure on the Data Center in which database failover is planned:

Procedure

1. Log in as a *root* user to all the POM servers configured in the Data Center.
2. Stop the POM services.
3. From the MSSQL Database AlwaysOn Dashboard, click **Start Failover Wizard** on the top-right corner of the page.
4. Select the Secondary database server of the same Data Center as the new Primary.
5. Refresh the database connections in MSSQL client.
6. Ensure that after refresh, the AlwaysOn Dashboard displays the selected database node as Primary.
7. Log in to the Avaya Experience Portal web console.
8. Navigate to **POM** > **POM Home** > **Configurations** > **POM servers** > **POM Manager**.
9. Select the primary POM server of Active Data center and click Start.

   Wait till all primary POM services have started and are in running status.
10. Select Aux POM server of Active Data center and click Start.

    POM services start on all POM servers of the Active Data Center.
11. Verify the status of all the services of the current/active Data Center are as listed in the Service status on page 119.

    Note:

    After local database failover, the previous Primary database server synchronization state automatically sets to Not Syncrhonizing (data movement paused).

    You must resume data movement and start the data synchronization only during maintenance hours, when POM processes are stopped. You can start POM processes and resume POM operations when the databases are synchronized.

Chapter 8: FIPS

FIPS overview

Proactive Outreach Manager supports Federal Information Processing Standards (FIPS) 140-2. Proactive Outreach Manager uses standard cryptographic algorithms approved by FIPS. There are four levels of security in FIPS 140-2. However, Proactive Outreach Manager uses 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 running the FIPS script on Proactive Outreach Manager.

Enabling FIPS

About this task

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

- The Fetch button on POM Trusted Certificates page is disabled. Use the Import button instead for any operations related to fetching the certificates.
- Existing certificate stores convert from `JKS` format to `BCFKS` format as follows:
  - `pomKeyStore` converts to `pomKeyStore.bks`.
  - `pomTrustStore` converts to `pomTrustStore.bks`.

  POM uses the new formats.

If you enable FIPS on the primary server, you must enable FIPS on the auxiliary server.

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 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 following command on the POM server to disable FIPS:

   ```
   $POM_HOME/bin/POM_FIPS_remove.sh
   ```

   Warning:

   If you disable FIPS in POM, you must also disable FIPS on Experience Portal. For more information on disabling FIPS on Experience Portal, see Disabling FIPS in *Administering Avaya Experience Portal*.

Enabling FIPS connection between AES and POM

Proactive Outreach Manager supports FIPS connection with Avaya Aura® Application Enablement Services (AES). In FIPS mode, to enable secure connection between AES and POM, import AES CA or identity certificate into the POM truststore.

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 (CMS). In FIPS mode, to enable secure connection between CMS and POM, import CMS CA or identity certificate into the POM truststore.

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:

Procedure

1. Ensure that FIPS is enabled on the operating system.

   POM supports Bouncy Castle as the security provider for FIPS. For information about adding Bouncy Castle as the FIPS provider in JAVA, refer to Bouncy Castle documentation at https://www.bouncycastle.org/documentation.html.

2. Run the following command to stop the APPSERVER:

   `systemctl stop appserver`

3. Convert the existing JKS format KeyStore to BCFKS format KeyStore which is a FIPS complaint bouncy castle KeyStore.

   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 an existing keystore name.

   Note:

   The supported FIPS provider jar file is available at the following location:

   `$POM_HOME/lib/common/bc-fips-1.0.1.jar`

4. Configure `$APPSERVER_HOME/conf/server.xml` and use BCKFS as a KeyStore type, change the value of the attribute keystoreType in the Element Connector to BCFKS.

5. Run the following command to start the APPSERVER:

   `systemctl start appserver`

Disabling FIPS on Tomcat APPSERVER

Before you begin

Ensure you stop the APPSERVER.

About this task

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 and the APPSERVER.

Procedure

1. Convert the existing BCFKS format KeyStore to JKS format KeyStore by using the following procedure:
   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 an existing keystore name.

   Note:

   The supported FIPS provider jar can be on the POM Server at the following location:

   $POM_HOME/lib/common/bc-fips-1.0.1.jar

2. Configure `$APPSERVER_HOME/conf/server.xml` and use JKS as KeyStore type, change the value of the attribute keystoreType in the element Connector to JKS.
3. When FIPS is disabled on the Operating System, and the Java Virtual Machine (JVM) is not running in FIPS mode, start the APPSERVER.

Chapter 9: 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 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 10: 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.

Download the following documents:

- *Implementing Avaya Experience Portal on a single server* - Refer and follow the Installation worksheets.
- *Implementing Avaya Experience Portal on multiple servers* - Refer and follow the Installation worksheets.

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 hostname 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 **Proactive Outreach** > **Manager**.
3. Click **Configurations** > **Trusted Certificates**.

   system displays all the trusted certificates.

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

POM truststore is corrupted or deleted

Condition

POM truststore is corrupted or deleted.

Solution

1. To re-create POM 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 11: Resources

Documentation

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

Title	Description	Audience
Avaya Proactive Outreach Manager Overview and Specification	Provides general information about the product overview and the integration with other products.	Users
Upgrading Avaya Proactive Outreach Manager	Provides information about migrating Proactive Outreach Manager.	Implementation engineers
Administering Avaya Proactive Outreach Manager	Provides general information about field descriptions and procedures for administering 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
Avaya Proactive Outreach Manager High Availability	Provides information for implementing POM system in a single data center, and also explains functioning of POM during failure and high availability.	Users 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. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.

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

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

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 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 73.

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 73.
Microsoft SQL Server	An external server

For more information about database configurations, see Different configurations for the database on page 157.

Best practices for using PostgreSQL database parameters

On a server of 32GB of RAM, the following memory parameters are a baseline:

Parameter	Value
shared_buffers	6 GB (you can increase this value)
effective_cache_size	12 GB (you can increase this value)
maintenance_work_mem	1 GB
work_mem	8 MB
max_parallel_maintenance_workers	4
checkpoint_completion_target	0.9
wal_buffers	16MB
max_worker_processes	10
max_parallel_workers_per_gather	4
max_parallel_workers	10

If more RAM is available on the server, use the following:

Parameter	Value
shared_buffer	25% of the total RAM of your machine
effective_cache_size	50% or 75% of the total RAM of your machine

To use the autovacuum feature in PostgreSQL, enable the following parameters:

Parameter	Value
autovacuum	on
track_counts	on
autovacuum_vacuum_scale_factor	0.1 (The default value is 0.2)

Set the autovacuum_vacuum_scale_factor parameter to run on autovacuum if the POM database generates dead tuples more than 10% of the total rows in its table.

Suggestions to tune the POM database to improve the performance of POM

Condition

After you use POM for a long time, the POM database collects a large amount of data. Due to this, the performance of the POM slows. As the performance of the POM database degrades, POM displays the following:

- POM takes a longer time to load through the web browser.
- If a campaign is in the stopping or the pausing state, then the campaign does not change its state.
- The dialing of campaigns slows.

- The uploading of contacts from a data source to the POM database takes more time.

Note:

The outcomes can vary than the aforementioned ones.

Cause

The working of the POM database slows since it handles excess data.

Solution

If the POM database is an MSSQL database, do the following:

1. Run the MS-SQL database on a dedicated server.

   Ensure that no other applications use the CPU or the memory resources of that server.

2. If customer uses an MSSQL database, set the value of the READ_COMMITTED_SNAPSHOT database parameter to `ON`

   If you do not set the value, campaigns can get stuck in a load scenario. On the existing database, run the following queries to verify the READ_COMMITTED_SNAPSHOT parameter:

   ```
   SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name=
   'YourDatabase'
   ```

   ```
   Return value: 1 = READ_COMMITTED_SNAPSHOT option is ON. 0 =
   READ_COMMITTED_SNAPSHOT option is OFF (default).
   ```

   To change the value of the parameter, run the following query:

   ```
   ALTER DATABASE SET READ_COMMITTED_SNAPSHOT ON;
   ```

   Note:

   Before running this query make sure that you stop all POM servers and also stop the vpms services.

3. Since POM performs database-intensive operations, while you perform operations on the POM database, implement the following best practices:
   - Do not modify the schema of the POM database.
   - Do not insert, update, and delete the content in the tables of the POM database.
   - Do not create database level triggers on the tables.
   - Do not run queries on the POM database that can adversely affect the performance of POM.

     If you must run such queries, copy the relevant data to a separate database and then run the queries.

4. To prevent the `tempdb` from running out of space, implement the following best practices:
   - Set the value of tempdb to `auto grow`.
   - Ensure that the hard disk of the machine that houses the tempdb of POM has enough free space.

- Set the initial size of the tempdb to an optimum value, such as one third (1/3) of the size of the POM database.

  For example, if the size of the POM database is 86 GB, set the size of the tempdb database to 30 GB. If it is possible, set the tempdb up on a separate disk drive on a separate machine.

- Set the value of the recovery model of the tempdb to `SIMPLE`.

  The recovery model automatically reclaims log space. To proactively prevent the model from reclaiming log space, after the size of the tempdb increases more than 30 GB, restart both MSSQL and POM services.

5. If you have a Layer-3 network between the nodes of the SQL database, asynchronously sync the temporary SQL database to the POM database.
6. After the maintenance activity of the MSSQL database completes, ensure that you restart the MSSQL database and then restart the POM service.

Best practices to configure the storage capacity of a database

To understand distribution, let's consider POM DB size = 500GB. Based on this value, we recommend configuring storage as below. Also if client has any existing DB server then they can use size number from existing system.

These are some best practices which can help to get good performance.

Table 1: MS SQL on Windows

Hard Disk / Drive Number	Volume	Size in GB	PURPOSE	Comments
0	C:\	60	OS	Can be considered as STANDARD Fixed Size irrespective of DB size.
1	D:\	100	SQL Server Instance Home + SSMS + Application user files.	Can be considered as STANDARD Fixed Size irrespective of DB size. It provides better flexibility and management of software.

Table continues…

Hard Disk / Drive Number	Volume	Size in GB	PURPOSE	Comments
2	E:\	500	Main data files (MDF) for pomdb, pomopdb and system databases (master, model, msdb).	POM DB size – 500GB is used for example purpose.
3	F:\	250	Log data files (LDF) for pomdb, pomopdb and system databases (master, model, msdb)	50% of MDF size if DB size < 1000 GB. 750 GB if DB > 1000GB. Transaction Log FS size determined by frequency of data change, amount of data change and backup frequency of transaction log.

Table continues…

Hard Disk / Drive Number	Volume	Size in GB	PURPOSE	Comments
4	G:\	750	Backups including data files and transaction logs in compressed format.	150% of MDF size. This include MDF + LDF backup. Sizing of this drive is only applicable if backup will be taken on local DB server. Backup drive size depend on backup frequency and retention of backup. Drive size can further increase if retention for backup is more on server. Ideally backup should be moved to another server so if any issue with DB server, backup will be available. Size can be decrease if remote backup setup implemented. If remote backup setup enabled, then Size this drive = 200 GB and can be used to take backup of table in case of urgency.
5	P:\	60	Pagefile	Can be considered as STANDARD Fixed Size irrespective of database size.
6	T:\	250	TempDB	50% of MDF size if DB size < 1000 GB. 750 GB if DB > 1000GB.

Table 2: MS SQL on Linux

Disk	File System	Size in GB	Purpose	Comments
0	/sql/data	500	Main data files (MDF) for pomdb, pomopdb and system databases (master, model, msdb)	POM DB size – 500GB is used for example purpose.
1	/sql/logs	250	Log data files (LDF) for pomdb, pomopdb and system databases (master, model, msdb)	50% of MDF size if DB size < 1000 GB. 750 GB if DB > 1000GB. Transaction Log FS size determined by frequency of data change, amount of data change and backup frequency of transaction log.

Table continues…

Disk	File System	Size in GB	Purpose	Comments
2	/sql/backup	750	Backups including data files and transaction logs in compress format.	150% of MDF size. This include MDF + LDF backup. Sizing of this drive is only applicable if backup will be taken on local DB server. Backup drive size depend on backup frequency and retention of backup. Drive size can further increase if retention for backup is more on server. Ideally backup should be moved to another server so if any issue with DB server, backup will be available. Size can be decrease if remote backup setup implemented. If remote backup setup enabled, then Size this drive = 200 GB and can be used to take backup of table in case of urgency.
3	/sql/tempdb	250	TempDB	50% of MDF size if DB size < 1000 GB. 750 GB if DB > 1000GB.

Table 3: Oracle on Windows

Disk Drive	Volume	Size in GB	PURPOSE	Comments
0	C:\	60	OS	Can be considered as STANDARD Fixed Size irrespective of DB size.

Table continues…

Disk Drive	Volume	Size in GB	PURPOSE	Comments
1	D:\	100	ORACLE_BASE, ORACLE_HOME, software installation directory, trace logs and patch location.	Can be considered as STANDARD Fixed Size irrespective of DB size. It provides better flexibility and management of software.
2	E:\	500	Oracle data files and control files set 1	POM DB size – 500GB is used for example purpose.
3	F:\	50	Oracle redo log files and control files set2	10% of DB size. Transaction Log FS size determined by frequency of data change, amount of data change and backup frequency of transaction log.
4	G:\	50	Oracle redo log files and control files set3	10% of DB size. Transaction Log FS size determined by frequency of data change, amount of data change and backup frequency of transaction log.
5	H:\	750	Flashback recovery area can hold archivelogs, backup, flashback logs etc	150% of DB size. If FRA feature is used to store all recovery related files otherwise size can be reduced.

Table 4: Oracle on Linux

Disk	File System	Size in GB	Purpose	Comments
0	/u01/app/oracle	60	ORACLE_BASE and software installation directory + trace logs + patch location. ORACLE_HOME will be /u01/app/oracle/product/<version>	Can be considered as STANDARD Fixed Size irrespective of DB size.
1	/u02/oradata/<DB>	500	Oracle data files and control files set 1	POM DB size – 500GB is used for example purpose.
2	/u03/oraredo/redolog1/<DB>	50	Oracle redo log files and control files set2	10% of DB size. Transaction Log FS size determined by frequency of data change, amount of data change and backup frequency of transaction log.
3	/u04/oraredo/redolog2/<DB>	50	Oracle redo log files and control files set3	10% of DB size. Transaction Log FS size determined by frequency of data change, amount of data change and backup frequency of transaction log.
4	/u99/flash_recovery_area/<DB>	750	Flashback recovery area can hold archivelogs, backup, flashback logs etc	150% of DB size. If FRA feature is used to store all recovery related files otherwise size can be reduced.

Table 5: PostgreSQL on Windows

Disk Drive	Volume	Size in GB	PURPOSE	Comments
0	C:\	60	OS	Can be considered as STANDARD Fixed Size irrespective of DB size.

Table continues…

Disk Drive	Volume	Size in GB	PURPOSE	Comments
1	D:\	100	PostgreSQL Software Install directory + Logs	Can be considered as STANDARD Fixed Size irrespective of DB size. It provides better flexibility and management of software. **Please note that PostgreSQL create data directory where software installed. Special handling required to change Data Directory.
2	E:\	500	Data directory of PostgreSQL	POM DB size – 500GB is used for example purpose.

Table continues…

Disk Drive	Volume	Size in GB	PURPOSE	Comments
3	F:\	750	Backup of PostgreSQL	150% of DB size. Sizing of this drive is only applicable if backup will be taken on local DB server. Backup drive size depend on backup frequency and retention of backup. Drive size can further increase if retention for backup is more on server. Ideally backup should be moved to another server so if any issue with DB server, backup will be available. Size can be decrease if remote backup setup implemented. If remote backup setup enabled, then Size this drive = 200 GB and can be used to take backup of table in case of urgency.

Table 6: PostgreSQL on Linux

Disk	File System	Size in GB	Purpose	Comments
0	/u01/app/PostgreSQL_<version>	100	PostgreSQL Software Install directory + Logs	Can be considered as STANDARD Fixed Size irrespective of DB size. **Please note that PostgreSQL create data directory where software installed. Special handling required to change Data Directory.

Table continues…

Disk	File System	Size in GB	Purpose	Comments
1	/u02/pgpomdata	500	Data directory of PostgreSQL	POM DB size – 500GB is used for example purpose.
2	/u02/pgpombackup	750	Backup of PostgreSQL	150% of DB size. Sizing of this drive is only applicable if backup will be taken on local DB server. Backup drive size depend on backup frequency and retention of backup. Drive size can further increase if retention for backup is more on server. Ideally backup should be moved to another server so if any issue with DB server, backup will be available. Size can be decrease if remote backup setup implemented. If remote backup setup enabled, then Size this drive = 200 GB and can be used to take backup of table in case of urgency.

Methods to configure 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 that 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.

Report creation

Using cross filtering, you can generate the following reports:

- 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: Best practices for using VMWare features

Monitoring performance of virtual machines

Use the esxtop tool on the ESXi host to monitor the performance of your virtual machines.

The following articles provide useful information on esxtop:

- Performance Monitoring Utilities: resxtop and esxtop: http://pubs.vmware.com/vsphere-51/index.jsp?topic=%2Fcom.vmware.vsphere.monitoring.doc%2FGUID-A31249BF-B5DC-455B-AFC7-7D0BBD6E37B6.html
- Interpreting esxtop Statistics: http://communities.vmware.com/docs/DOC-9279

vMotion: Host migration and storage vMotion

vMotion enables live migrations of virtual machines from one ESXi host to another. Storage vMotion enables live migration from one datastore to another. These migrations occur without any downtime of the migrating virtual machines. However, there can be side effects while migrating virtual machines running Experience Portal servers.

- vMotion is supported in Maintenance Mode only.
- vMotion is not supported in Production for reasons that affect performance.
- Storage vMotion is not supported as it can impact the following:
  - Responses of the application in real-time.
  - Processing of events on the associated virtual machines.

High Availability for VMWare

High Availability (HA) is an option for Experience Portal and POM to restart critical systems during an ESXi host failure or general failure with the virtual machine.

Virtual servers run on a failed ESXi host experience downtime until the servers start on another host in the HA cluster. The downtime is the time to detect the failure plus the time for the virtual machine to turn on and start working.

Although it is not required, VMware recommends using a secondary NIC for the management network when configuring HA.

The following are the recommended configurations to set up a HA cluster to use with Experience Portal virtual machines:

- Configure each MPP with **Restart Automatically** set to **Yes** in EPM. To check the MPP setting, go to **EPM** > **System Configuration** > **MPP Servers** and click the name of the MPP server.
- To enable the HA cluster feature, select **Turn On vSphere HA**.
- Go to **vSphere HA** cluster settings and do the following:
  - Select **Enable Host Monitoring** check box.
  - Select **Enable Admission Control** check box.
  - Configure the admission control policy to support the failure of one ESXi host.

    Note:

    When doing network maintenance, clear the **Enable Host Monitoring** check box. Otherwise, the vSphere HA can detect a false failure.

    To support vSphere HA failover, reserve one or more ESXi host(s) or a percentage of resources on each host. These settings vary based on your preferences and available ESXi resources.
- In the **vSphere HA** > **Virtual machine options**, select **Primary EPM**.
  - Set **VM Restart Priority** to **High**.
  - Set **Host Isolation Response** to **Leave powered on**.

    These settings enable the Primary EPM virtual machine to prioritize resources to reduce downtime during a failure. The MPPs, Auxiliary EPMs, and other components of the Experience Portal infrastructure have the next highest priority.
- Go to **vSphere HA** > **Virtual Monitoring**, select the Primary EPM:
  - Enable **VM and Application Monitoring**.
  - Set **VM Monitoring Sensitivity** to **High**.
  - Set **Application Monitoring** to **Include**.

    These settings enable the Primary EPM to restart if it does not receive a heartbeat in 30 seconds. You can also define and use a custom Monitoring sensitivity rule.
- Go to **vSphere HA** > **Datastore Heartbeating** and select the following:
  - Check **Select any of the cluster datastores taking into account my preferences**.
  - In the Datastores available for Heartbeat window, select the datastore where the Primary EPM VM runs.

Note:

Your configuration varies based on which failover scenarios and available resources to cover an HA failover scenario. For more information, see Create a vSphere HA cluster in VMware documents.

VM Snapshots

The following are the best practices for Experience Portal and POM:

- Experience Portal and POM are real-time applications. Ensure that Experience Portal and POM are not running when you take a snapshot or revert to a snapshot.
- To prevent side effects, shut down the virtual machine when you take or revert to a snapshot. Otherwise, the running systems can experience side effects, such as dropped calls, web sessions, and servers that are out of synchronization.
- If you take a snapshot of a live EPM virtual machine and then revert the snapshot, you must restart the EPM service from the command line to resynchronize the Experience Portal environment.

  Note:

  Log in to the console as sroot.

  - To start POM, run the **`POM start`** command.
  - To stop POM, run the **`POM stop`** command.
  - To restart POM, run the **`POM restart`** command.
  - To see the running status of POM, run the **`POM status`** command.
- If you take a snapshot of a live MPP virtual machine and then revert the snapshot, you must restart the MPP to re-synchronize the system.

  Note:

  Restart the MPP from the **System Management** > **MPP Manager** page in EPM.
- After reverting a snapshot, and when the system runs, ensure that you delete all snapshots for the virtual machine in Snapshot Manager. The overhead of running with snapshots can impact the system performance, especially with disk I/O.
- For more information, see best practices for using virtual machine snapshots in the vSphere environment article in the VMware knowledge base.

Fault Tolerance

The traditional Fault Tolerance feature is not supported with virtual machines by using multiple CPUs. All Experience Portal virtual servers are configured with four CPUs. Therefore, fault tolerance cannot be configured.

In vSphere 6.0, VMware introduced Symmetric Multi-Processing Fault Tolerance (SMP-FT), which currently supports up to four CPUs. This feature is not tested with Experience Portal.

Appendix D: 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

F

G

I

K

L

M

N

O

P

R

S

T

U

V