Avaya Proactive Outreach Manager High Availability

Release 4.0
Issue 2
April 2021

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

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

License types

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

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

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: Introduction

Purpose

This document provides information about how to implement a highly available Avaya Proactive Outreach Manager (POM) system in a single data center. It also describes the behavior of POM when a failure occurs.

Implementation engineers, field technicians, business partners, and customers can use this document to understand high availability and failure scenarios of POM.

Change history

Issue	Date	Summary of changes
2	April, 2021	Updated the following topics: • External Kafka and Zookeeper installation and configuration • Setting up Zookeeper and Kafka • Enriched Attempt Event Aggregator • Kafka Events retention
1	December, 2020	Content for the Cache service is added in: • Chapter 3: High Availability deployment scenarios Added a new chapter: • Event SDK High Availability

Chapter 2: Overview

High Availability overview

POM supports High Availability (HA) in a single data center where all components are in the same local area network. POM supports HA for agent-less and agent-based configurations. In an HA configuration, POM can automatically recover from a failure scenario.

POM supports HA across the following components:

- Agent Manager
- Campaign Manager
- ActiveMQ
- Rule Engine
- Cache service
- Kafka service

High Availability prerequisites

The following are the prerequisites for POM High Availability:

- Ensure that the database is accessible from all operational POM servers.

  Note:

  Customers must administer the POM database if the POM database schema is installed on a local or external database.
- Deploy POM in the multi-server deployment model.
- Deploy the application server on a standalone server.
- Deploy Media Processing Platform as a standalone server.
- Ensure that the time on all POM servers is synchronized with the Network Time Protocol (NTP) server.

Chapter 3: High Availability deployment scenarios

Deployment of two POM servers in a single zone

- Configure the following POM servers in a single zone:
  - POM1 (Primary EPM)
  - POM2 (Auxiliary EPM)
- Assign the primary and auxiliary Experience Portal Manager (EPM) servers to zone 1, which is the default zone.
- Connect both servers to the external database and external application server.
- Deploy the Media Processing Platform (MPP) server, application server, and database separately.

Table 1: Status of POM components before failover

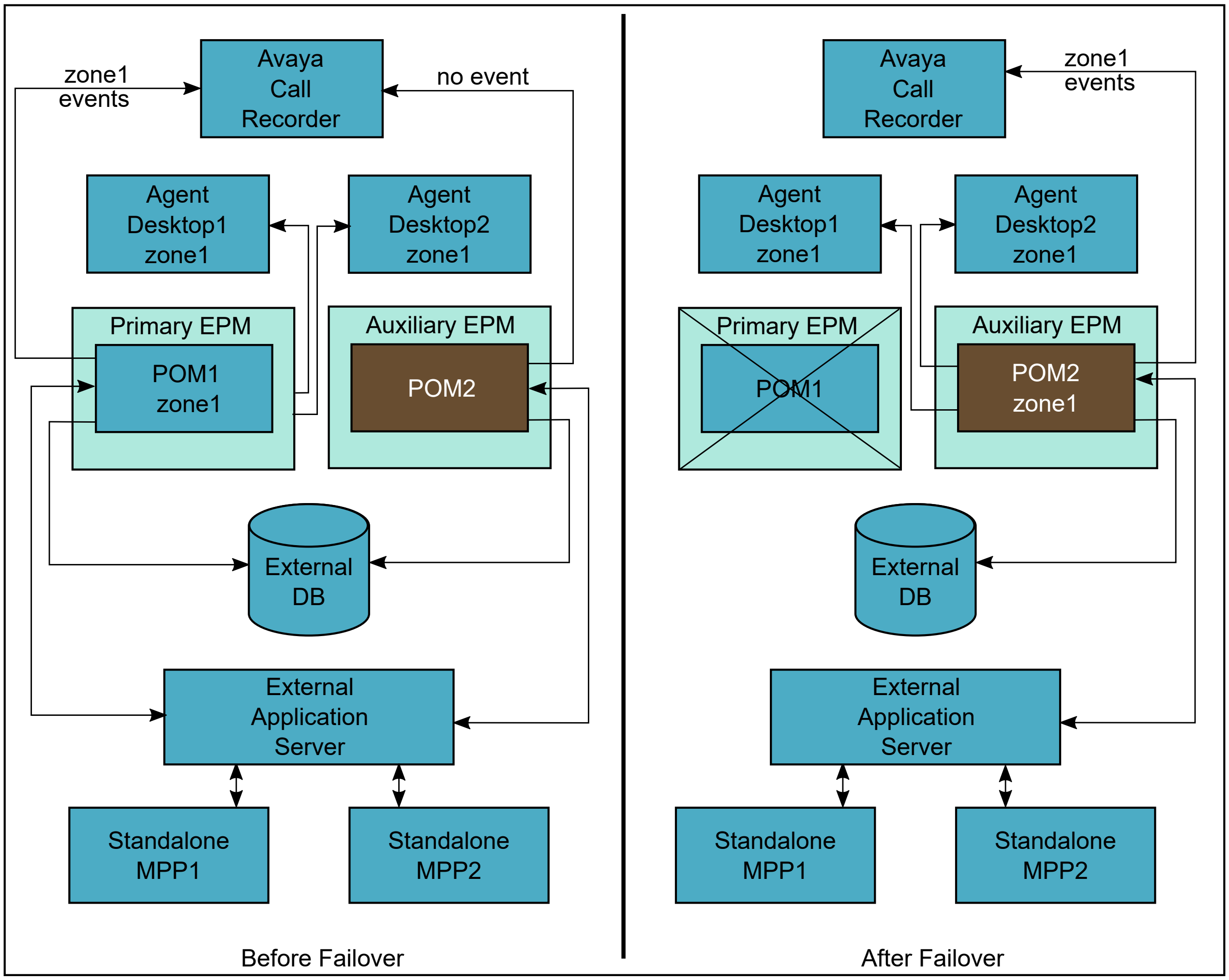
Component	POM1	POM2
Agent Manager	MASTER (zone 1)	DORMANT
POM agent SDK service	Running	Running
Rule Engine	MASTER	DORMANT
ActiveMQ	MASTER	DORMANT
Cache service	RUNNING	RUNNING

Table 2: Status of POM components after failover

Component	POM1 (Failed server)	POM2
Campaign Director	STOPPED	MASTER (Common Campaign Director, zone 1)
Campaign Manager	STOPPED	RUNNING

Table continues…

Component	POM1 (Failed server)	POM2
Agent Manager	STOPPED	MASTER (zone 1)
Rule Engine	STOPPED	MASTER
ActiveMQ	STOPPED	MASTER
Cache service	STOPPED	RUNNING



When an active POM server fails, the other server takes 10 minutes to start the services and become fully operational.

After the server failover:

- You cannot perform any administrative tasks from the user interface until the primary EPM is operational.
- If you install POM on Avaya Experience Portal, you can access the POM Monitor page.

- Any operation related to the job state change from the POM Monitor page does not take effect.
- Web service request generated from the failed server does not take effect. Therefore, to make web service calls, the web service client must use the other available POM server.
- No new dialing is possible.
- Campaign Director and Agent Manager in the POM2 server take over zone 1 of the failed POM1 server.
- ActiveMQ and Rule Engine in the POM2 server are promoted as master.
- Logged in agents can start operating from the Agent desktop.
- Campaign starts dialing in zone 1.
- Operation from the POM Monitor page takes effect.

Deployment of three POM servers in two zones

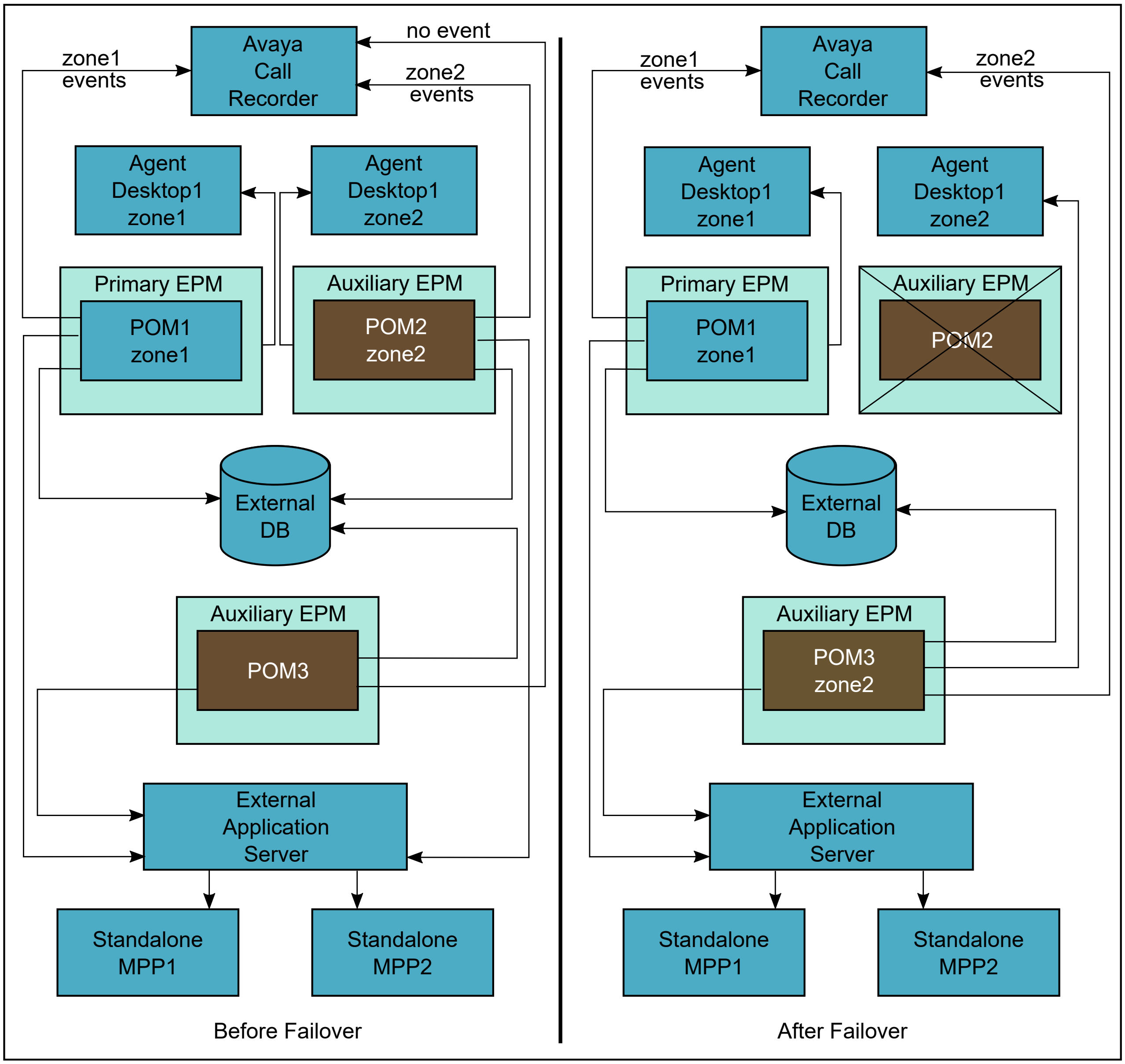
- Configure the following POM servers in two zones:
  - POM1 (Primary EPM)
  - POM2 (Auxiliary EPM)
  - POM3 (Auxiliary EPM)
- Assign all Experience Portal Manager (EPM) servers to both the zones.
- Connect all servers to the external database and external application server.
- Deploy the Media Processing Platform (MPP) server, application server, and database separately.

Table 3: Status of POM components before failover

Component	POM1	POM2	POM3
Campaign Director	MASTER (Common Campaign Director, zone1)	DORMANT (zone2)	DORMANT
Campaign Manager	RUNNING	RUNNING	RUNNING
Agent Manager	MASTER (zone1)	MASTER (zone2)	DORMANT
Rule Engine	MASTER	DORMANT	DORMANT
ActiveMQ	MASTER	DORMANT	DORMANT
Cache service	RUNNING	RUNNING	RUNNING

Table 4: Status of POM components after failover

Component	POM1	POM2 (Failed server)	POM3
Campaign Director	MASTER (Common Campaign Director, zone1)	STOPPED	DORMANT (zone2)
Campaign Manager	ACTIVE	STOPPED	RUNNING
Agent Manager	MASTER (zone1)	STOPPED	MASTER (zone2)
Rule Engine	MASTER	STOPPED	DORMANT
ActiveMQ	MASTER	STOPPED	DORMANT
Cache service	RUNNING	STOPPED	RUNNING



When an active POM server fails, the other server takes 10 minutes to start the services and become fully operational.

After the server failover:

- Dialing continues for zone 1.
- Dialing is stopped in zone 2.
- Any operation from the POM Monitor page for zone 2 does not take effect.

  For example, manual movement of agent from one job to another job in zone 2.
- Web service request generated from the failed server does not take effect. Therefore, to make web service calls, the web service client must use the other available POM server.

- No new dialing is possible for the contacts in zone 2.
- Agents from zone 2 can perform operations from the Agent desktop.
- Campaign Director and Agent Manager from the POM2 server take over zone 1 of the failed POM server.
- Logged in agents of zone 2 can start operating from the Agent desktop.
- Campaign starts dialing in zone 2.
- Operation from the POM Monitor page for zone 2 takes effect.

Deployment of four POM servers in two zones

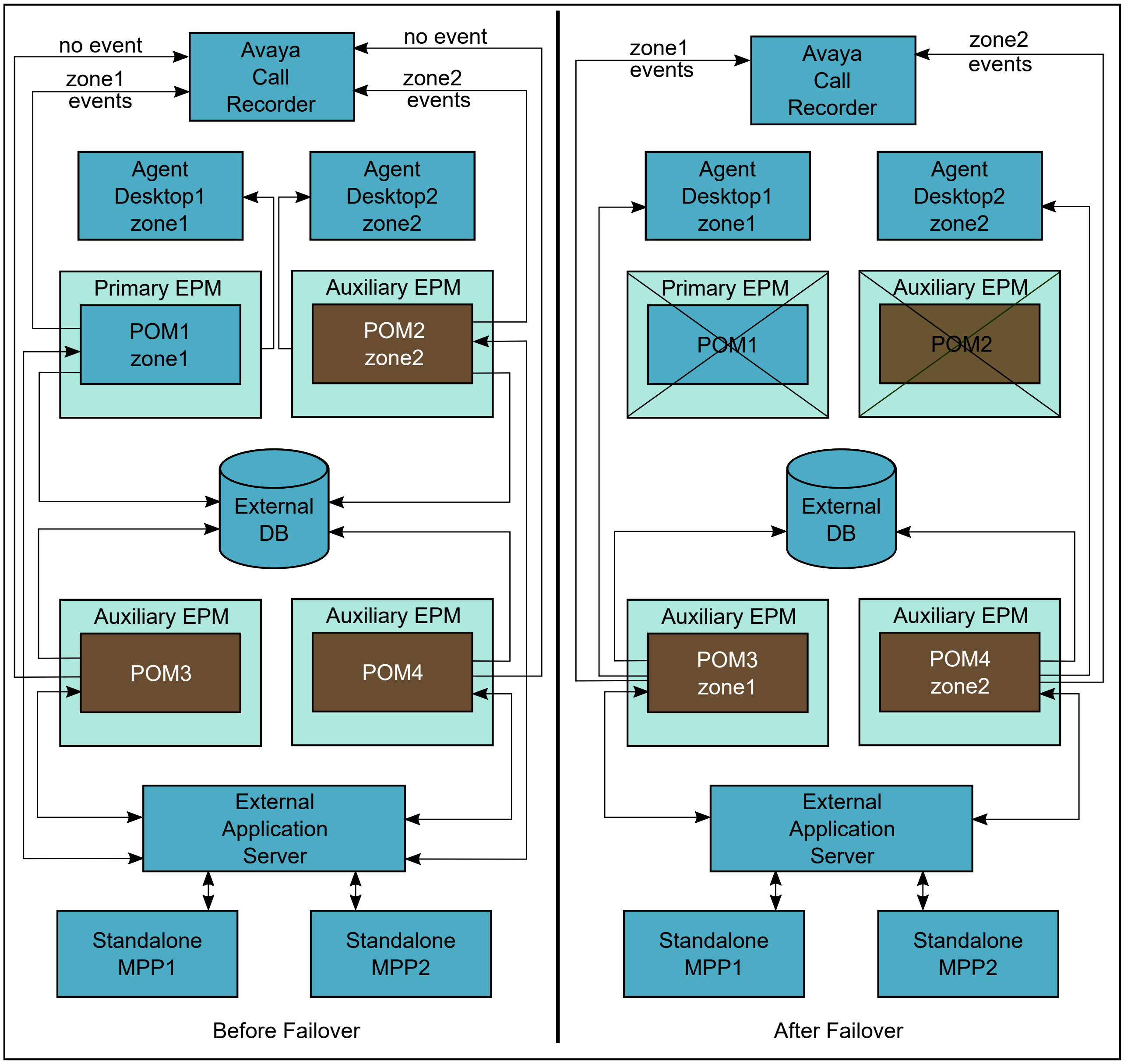
- Configure the following POM servers in two zones:
    - POM1 (Primary EPM)
    - POM2 (Auxiliary EPM)
    - POM3 (Auxiliary EPM)
    - POM4 (Auxiliary EPM)
- Assign all Experience Portal Manager (EPM) servers to both the zones.
- Connect all servers to the external database and external application server.
- Deploy the Media Processing Platform (MPP) server, application server, and database separately.

Table 5: Status of POM components before failover

Component	POM1	POM2	POM3	POM4
Campaign Director	MASTER (Common Campaign Director, zone 1)	DORMANT (zone 2)	DORMANT	DORMANT
Campaign Manager	RUNNING	RUNNING	RUNNING	RUNNING
Agent Manager	MASTER (zone 1)	MASTER (zone 2)	DORMANT	DORMANT
Rule Engine	MASTER	DORMANT	DORMANT	DORMANT
ActiveMQ	MASTER	DORMANT	DORMANT	DORMANT
Cache service	RUNNING	RUNNING	RUNNING	RUNNING

Table 6: Status of POM components after failover

Component	POM1 (Failed server)	POM2 (Failed server)	POM3	POM4
Campaign Director	STOPPED	STOPPED	MASTER (Common Campaign Director, zone1)	DORMANT (zone2)
Campaign Manager	STOPPED	STOPPED	RUNNING	RUNNING
Agent Manager	STOPPED	STOPPED	MASTER (zone1)	MASTER (zone2)
Rule Engine	STOPPED	STOPPED	MASTER	DORMANT
ActiveMQ	STOPPED	STOPPED	MASTER	DORMANT
Cache service	STOPPED	STOPPED	RUNNING	RUNNING



When an active POM server fails, the other server takes 10 minutes to start the services and become fully operational.

Campaign Director allocates the zones to the least busy server. Therefore, the zone assignment to the POM server depends on the point of failure. Both zones are assigned to separate POM servers.

After the server failover:

- You cannot perform any administrative tasks from the user interface.
- If POM is installed on Avaya Experience Portal, you can access the POM Monitor page by using the following URL:

`https://<POM2Server_IP address>/VP_POM_Monitor/faces/login.xhtml`

Where, *<POM2Server_IP address>* is the IP address of the POM2 server.

Important:

To access this URL, use Microsoft Internet Explorer 11 and later. You might need to enter the user name and password twice.

- Any operation related to the job state change from the POM Monitor page does not take effect.
- Web service request generated from the failed server does not take effect. Therefore, to make web service calls, the web service client must use the other available POM server.
- No new dialing is possible for the contacts in zone1.
- Campaign Director and Agent Manager in the POM3 server take over zone 1 of the failed POM1 server.
- Campaign Director and Agent Manager in the POM4 server take over zone 2 of the failed POM2 server.
- ActiveMQ and Rule Engine from the POM3 server are promoted as master.

  The auxiliary server to be promoted as master depends on the algorithm that you use.
- Logged in agents of zone 1 and zone 2 can start operating from the Agent desktop.
- Campaign starts dialing in zone 1 and zone 2.
- Operations from the POM Monitor page for zone 1 and zone 2 take effect.

Deployment of two POM servers in a single zone for workspaces

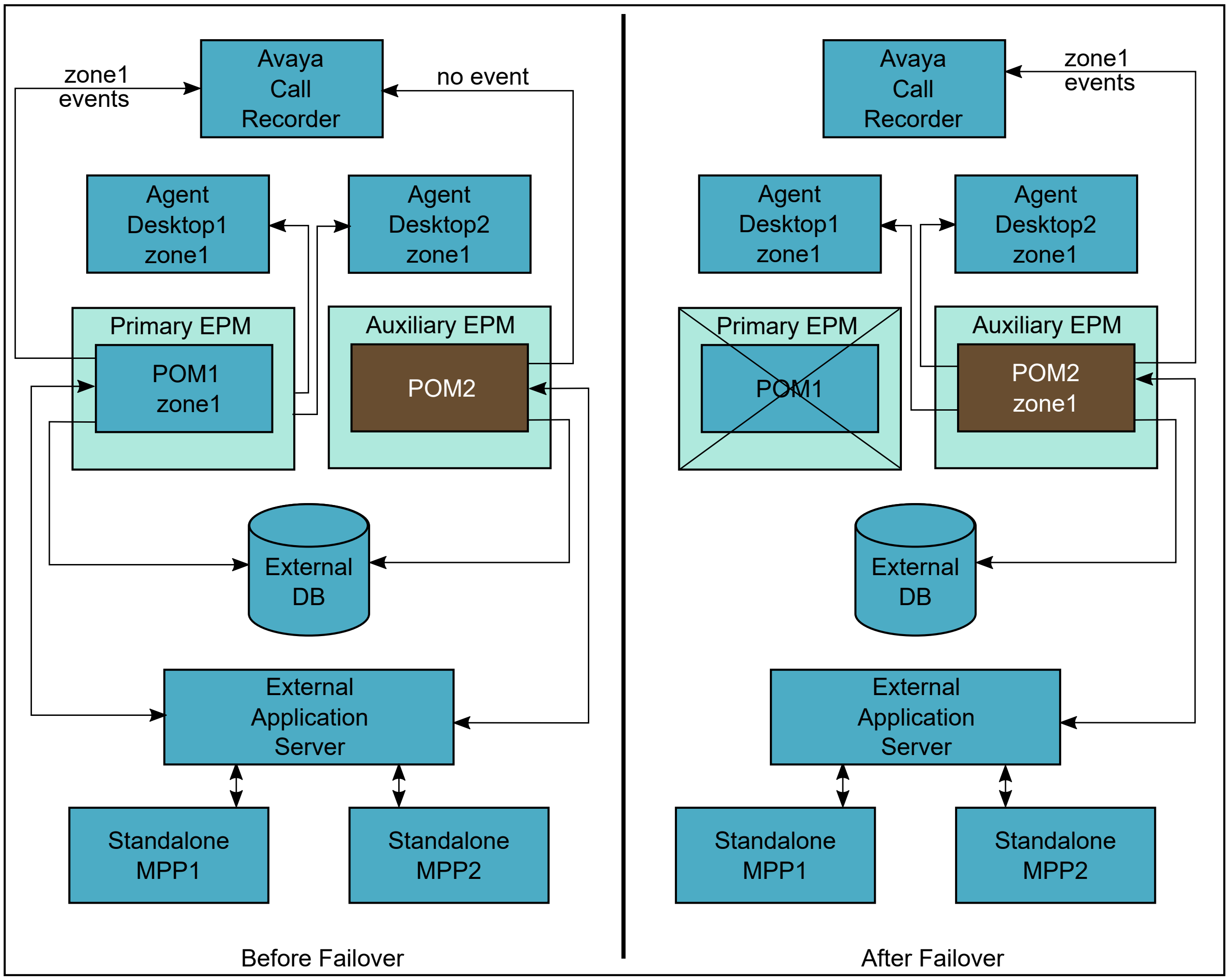
- Configure the following POM servers in a single zone:
  - POM1 (Primary EPM)
  - POM2 (Auxiliary EPM)
- Assign the primary and auxiliary Experience Portal Manager (EPM) servers to zone 1, which is the default zone.
- Connect both servers to the external database and external application server.
- Deploy the Media Processing Platform (MPP) server, application server, and database separately.

Table 7: Status of POM components before failover

Component	POM1	POM2
Agent Manager	MASTER (zone 1)	DORMANT
POM agent SDK service	RUNNING	RUNNING
Cache service	RUNNING	RUNNING

Table 8: Status of POM components after failover

Component	POM1 (Failed server)	POM2
Agent Manager	STOPPED	MASTER (zone 1)
POM agent SDK service	STOPPED	STOPPED
Cache service	STOPPED	STOPPED



When an active POM server fails, the other server takes ten minutes to start the services and become fully operational.

After the server failover:

- You cannot perform any administrative tasks from the user interface until the primary EPM is operational.
- TCP Socket connection of the service with the Agent Manager breaks. Agent Manager logs out all the agents. Agents who are busy with the customer on telephone get logged out after the call is finished.
- All the calls with agent are disposed with Desktop Error completion code.
- All in-progress calls which are answered are marked as nuisance.
- JavaScript SDK Library receives socket disconnect and notifies same to the Widget.
- JavaScript SDK library tries to establish connection with secondary POMAgentSDKService IP.
- After successful connection with POMAgentSDKService, agent logs in again and starts working on campaigns.

Chapter 4: Component level High Availability

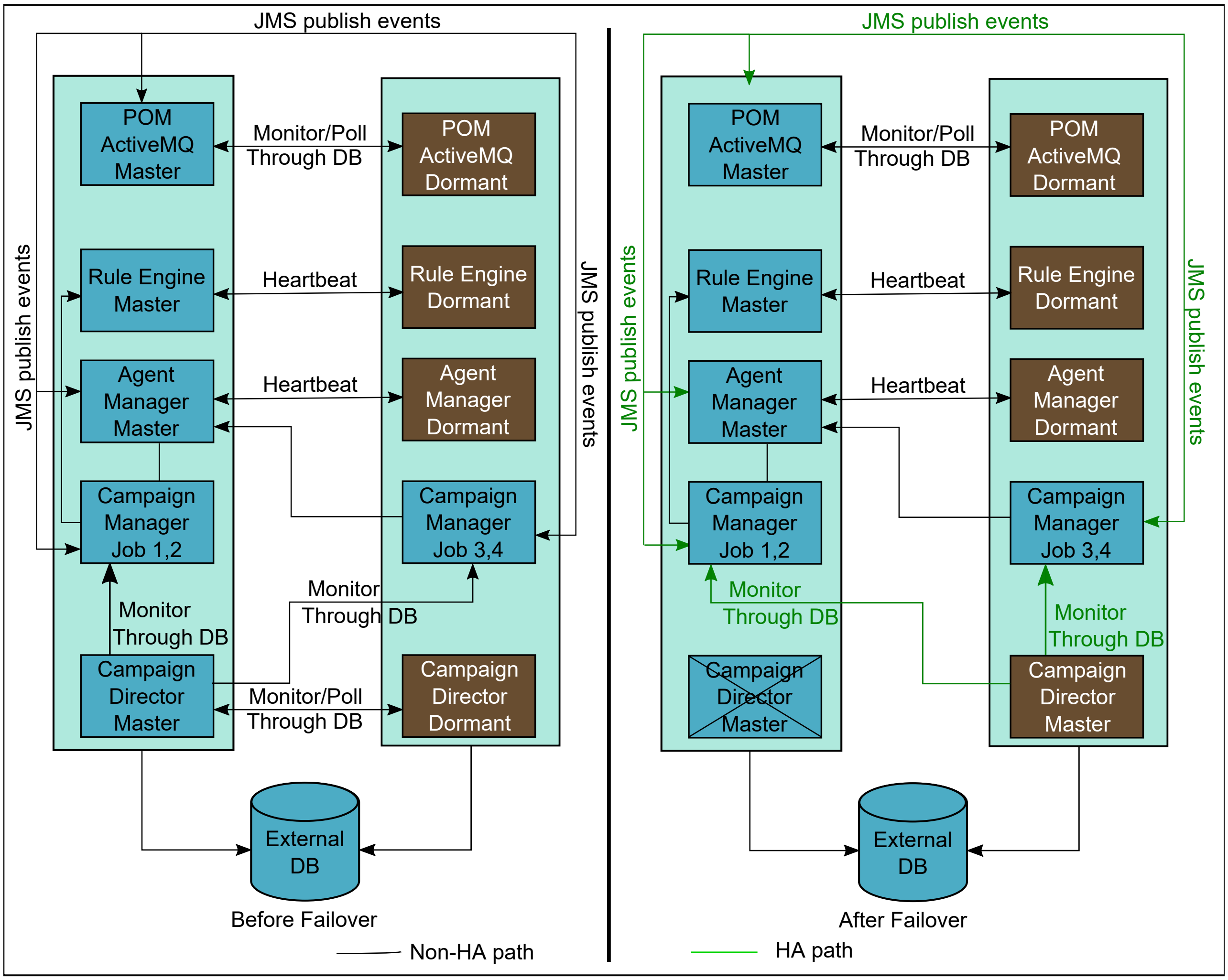
Campaign Director High Availability

In a multi-server deployment of POM, the Campaign Director service runs in the master or dormant mode within a single data center.

Campaign Director consists of the following components:

Component	Description
Common Campaign Director	Common Campaign Director manages all common tasks across zones, such as scheduling, filtering campaign data, creating historical data, and exporting campaign data. The master Campaign Director is the Common Campaign Director.
Zone Director	Each zone has a Zone Director within a Campaign Director. A single Campaign Director can handle multiple zones. You can assign multiple zones to a Campaign Director.

If the master Campaign Director process fails gracefully, the other Campaign Director immediately becomes master and all operations, except purging, are resumed. If the master Campaign Director process fails ungracefully, another Campaign Director becomes the master after 2 minutes and 20 seconds of the failover time.



Impact of the Common Campaign Director failure

Function	Impact
Job state	The jobs that are started from the user interface remain in the queued state. The campaign does not get completed even when the system dials all contacts or the finish criteria is met. Such campaigns finish when the Campaign Director is functional again.
Pausing and resuming campaigns based on user action	The job state remains unchanged until the dormant Campaign Director takes over.
Triggering campaigns and data imports at scheduled date and time	The scheduled imports and campaign schedules do not work for the time for which the connection is unavailable.
Export	The export function stops. When the Campaign Director is functional again, the export function resumes from where it stopped.

Table continues…

Function	Impact
Purging	The purging function stops during the purge operation if the Campaign Director becomes non-functional. When the Campaign Director is functional again, the purging does not resume. The purging starts at the next scheduled date and time.
Campaign Post Processing	The campaign post processing function stops. When the Campaign Director becomes functional again, the campaign post processing function resumes from where it stopped. The completion code trend report might show stale data for the time for which the Campaign Director is non-functional.
Terminating campaigns if the finish criteria specified are met	Campaign Director does not perform periodic checks for the finish criteria, and the campaign does not stop dialing until the dormant Campaign Director takes over the failed server.
Trend calculation	Trend calculation, Campaign progress chart, and multiple campaign summary on the POM Monitor page show stale data for the time for which the Campaign Director is non-functional.
Report	The completion code trend report might show stale data for the time for which the Campaign Director is non-functional.
Nuisance rate and alarm generation	Nuisance call rate calculation and alarm generation stop until the Campaign Director is functional again.
Job allocation	When the master Campaign Director and Campaign Manager simultaneously fail, then the job handled by that Campaign Manager is not allocated to any other Campaign Manager until the Campaign Director is functional again.

Impact of the Zone Director failure

Function	Impact
Data import	The running import jobs resume after any other Zone Director process inside the Campaign Director takes over. However. the status on the user interface reflects as **Running**. The import function stops. When the Campaign Director is functional again, the import function resumes from where it stopped.

Reconfiguration of a zone

When the failed Campaign Director becomes operational again, it acts as the dormant server. However, it takes back the zone responsibility allocated to it before the failover.

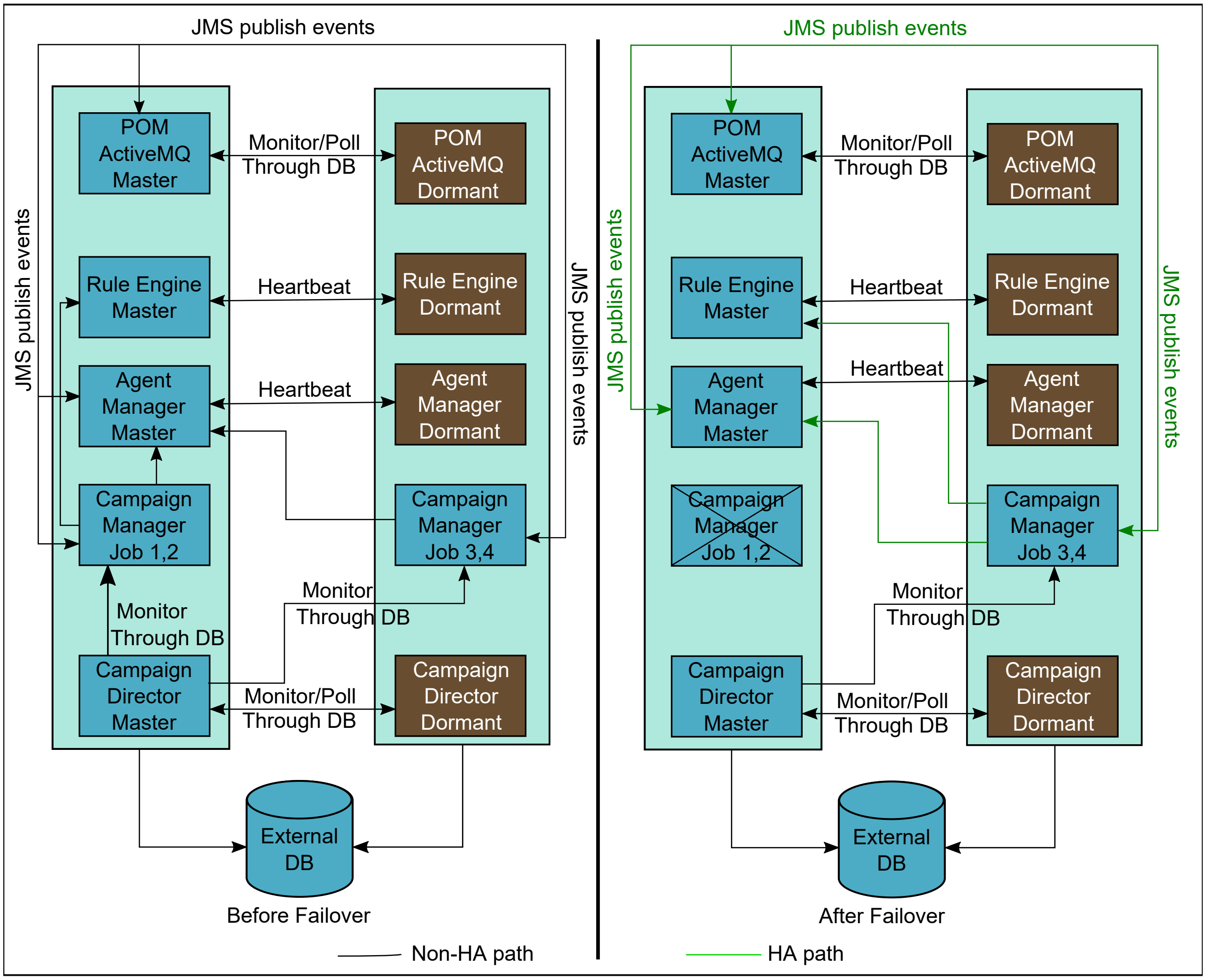
Campaign Manager High Availability

Campaign Manager is the component that manages outbound attempts. The Campaign Manager service operates in the running mode within a single data center. If the running Campaign

Manager process fails gracefully, the other Campaign Managers immediately take over the jobs. If the running Campaign Manager process fails ungracefully, another Campaign Manager takes over the jobs after 5 minutes from the time when the running Campaign Manager process fails.

Note:

For the auxiliary Campaign Manager to take over the failed server, the master Campaign Director must be operational. Otherwise, the master Campaign Director does not allocate the jobs handled by the failed Campaign Manager to any other server.



The following activities occur during 5 minutes failover time:

- On the POM Manager page of the failed server displays the service state as **Running**, but the Campaign Manager is not operational.
- Dialing is stopped for jobs that are handled by the failed Campaign Manager.
- Campaign Director allocates the responsibilities of the failed Campaign Manager to other Campaign Managers based on the algorithm. For more information. see *Avaya Proactive Outreach Manager Overview and Specification*.

Note:

If the Campaign Manager process stops ungracefully and the campaigns are running, some contacts might be stuck and the campaign remains in the running state indefinitely without making any new attempts. You must manually stop such campaigns.

When Campaign Manager takes over the jobs of the failed servers, it starts filtering the contacts for the jobs. However, it starts dialing from where the failed Campaign Manager stopped. When the failed Campaign Manager becomes operational again, it does not manage the previously assigned jobs.

Agent Manager High Availability

The Agent Manager service runs in the any of the following modes within a single data center.

- If the Agent Manager service is handling a zone, it runs in the master mode.
- If the Agent Manager service is not handling a zone, it runs in the dormant mode..

An Agent Manager can manage multiple zones. You can deploy the Agent Manager in the active-active mode, where each Agent Manager manages one or more unique zones. In a single zone, you can deploy Agent Manager in the active-passive mode, where one Agent Manager manages the zone and the other Agent Manager remains in the dormant mode.

Agent Manager failover

When an Agent Manager failure occurs, the dormant Agent Manager takes over all zones of the failed server.

The following is the sequence of events that occurs during the failure of an Agent Manager handling a default zone and zone 1:

- All logged in agents in the failed server zone receive the `POMNotAvailable` notification.
- Agent handling the existing calls continue. However, they cannot operate from the desktop.
- No new dialing is possible for the contacts in the failed server zone.
- All in-progress calls in the failed server zone that are answered with live voice are marked as nuisance calls.

  Note:

  If the Agent Manager fails when the Call Queuing feature is enabled and the calls are queued for an agent to get free, no queued calls are assigned to the agent after the failover.
- The run-time changes that you make to the jobs of the failed server zone from the POM Monitor page are not saved.
- Agent movement of the failed server zone from the POM Monitor page does not take effect.
- The dormant Agent Manager takes over the zone of the failed servers.
- All logged in agents in the failover server zones receive the `POMAvailable` notification.

- Disconnected calls during the failover time are communicated to the agent desktop, and the agents handling the calls move to the wrap-up state.
- The logged in agent can start operating from the agent desktop.
- Campaign starts dialing in the zones of the failover servers.
- The run-time changes that you make to the jobs of the failed server zone from the POM Monitor page are saved.
- Agent movement of the failed server zone from the POM Monitor page takes effect.
- The failover server starts sending failover server zones events to ACR.

Based on the desktop implementation, Agent Desktop might handle the `POMavailable` and `POMnotavailable` messages differently.

After the dormant Agent Manager becomes master, it checks the agent state with the desktop. If the Agent Manager finds a state mismatch, then the call gets updated with the Desktop Error completion code. The system forcefully logs out the agents. After getting logged out, the agents need to login again.

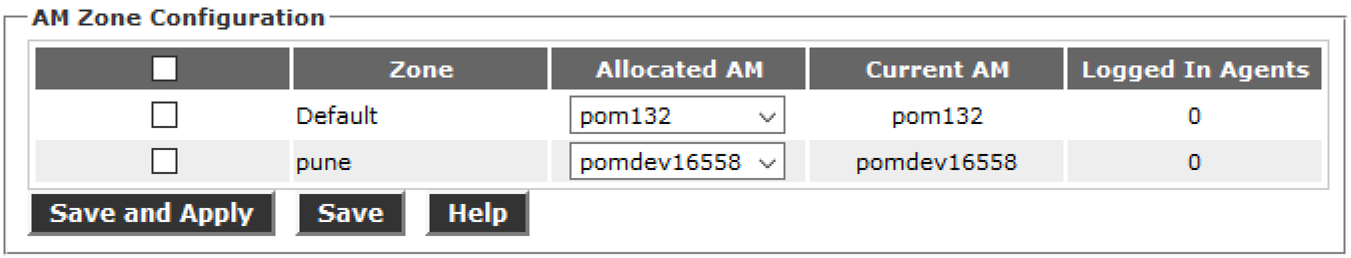
If the Agent Manager fails to receive the Disconnect event from the platform, the agent cannot perform any operation even after the `POMavailable` notification. Therefore, the agent must login again. If the agent is handling a call, the call gets updated with the Desktop Error completion code.

Reconfiguration of zone

When the failed Agent Manager becomes operational again, it acts as a dormant server. The administrator can assign the zone responsibility back to the original server from the Manage Zone Configuration page.

Note:

- When the administrator clicks **Save** for the Agent Manager zone configuration after changing the allocated server of a zone, the changes are only saved in the database while the zone ownership remains unchanged.
- When the administrator clicks **Save and Apply** for the Agent Manager zone configuration after changing the allocated server of a zone, the system displays a warning message `AM Zone reset will force log out all agents. Would you like to continue?` If administrator selects **Yes**, then the current Agent Manager forcefully logs out all the agents and releases the zone ownership. The allocated Agent Manager server takes the ownership of the zone.



AM Zone Configuration

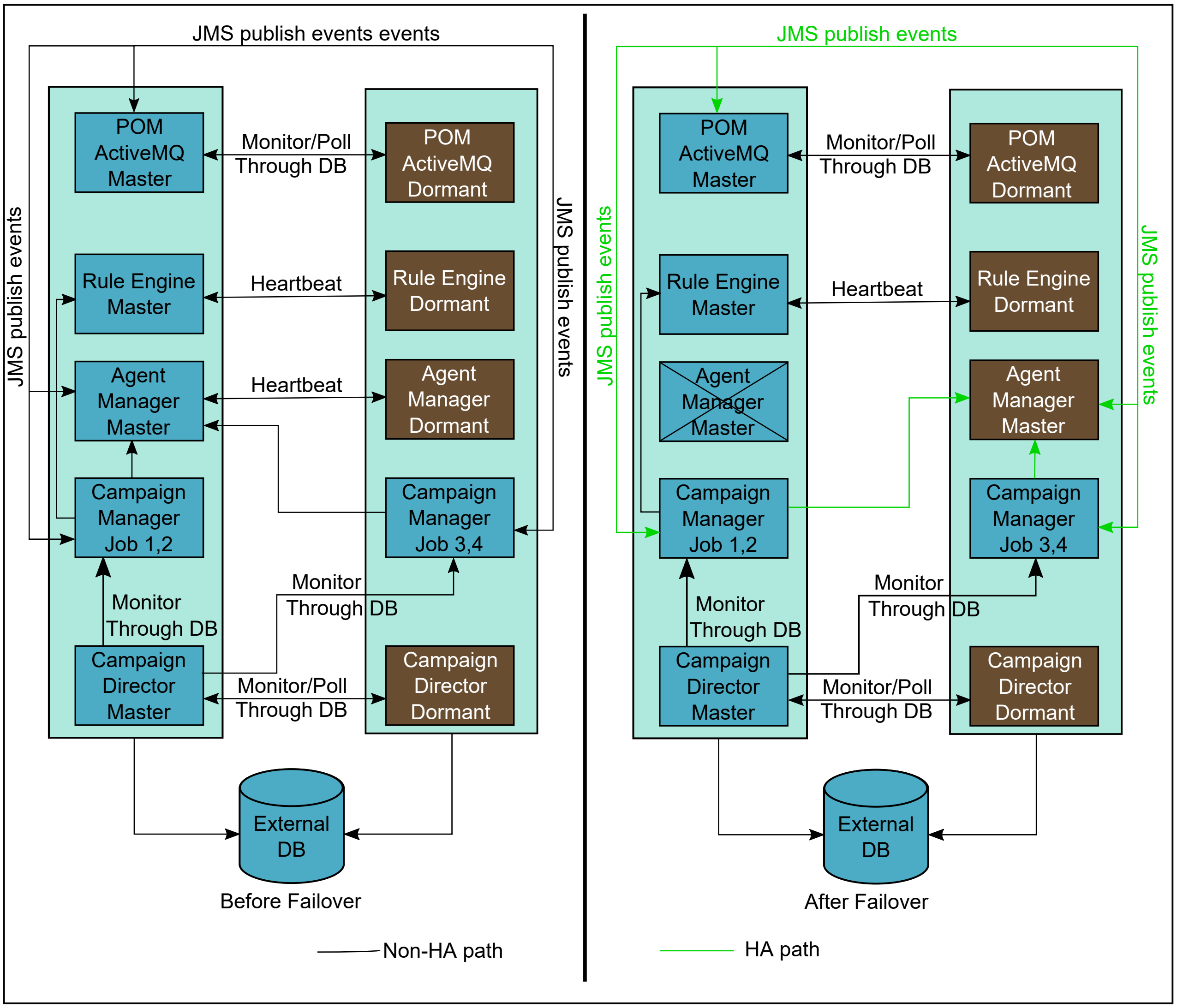
☐	Zone	Allocated AM	Current AM	Logged In Agents
☐	Default	pom132	pom132	0
☐	pune	pomdev16558	pomdev16558	0

Heartbeat connection for Agent Manager

Agent Manager maintains the heartbeat connection with the dormant server to monitor its connection. When the heartbeat connection fails, all Agent Manager servers update the database with their respective status to avoid multiple masters during a network failure. If the master Agent Manager process fails, the dormant becomes the master after 40 seconds of failover time.

Note:

- The server failover time is 40 seconds. This time does not include the zone initialization time. The zone initialization time depends on the number of logged in agents and the number of jobs running.
- During the Agent Manager failover, the database CPU rises by 30-40% and drops to normal after completion of the Agent Manager failover.



The failover duration of Agent Manager is considered as **Total HA time** and is included in the agent time for each agent. For more information on agent time summary report, see *Using Avaya Proactive Outreach Manager Reports*. You can configure the Agent Desktop heartbeat ports from the Global Configuration page. For more information, see *Using Avaya Proactive Outreach Manager*.

Desktop configuration for Agent Manager High Availability

For Agent Manager High Availability:

- The desktop must have a provision for multiple Agent Manager IP addresses.
- The desktop must be able to access the auxiliary agent script URL when the primary agent script URL is not accessible.

  Note:

  POM sends the primary and auxiliary agent script URLs to the desktop.

Application server load balancing behavior

If the application server is configured in load balancing, the nailing session of the agent is distributed across two application servers. When the dormant Agent Manager becomes master after the failover, the new master Agent Manager waits for the AppServerWaitTimeOut period in which the connection is established between the Agent Manager and both application servers. This AppServerWaitTimeOut period is configurable in the POM database using *pim_config table* and the default time is 30 seconds.

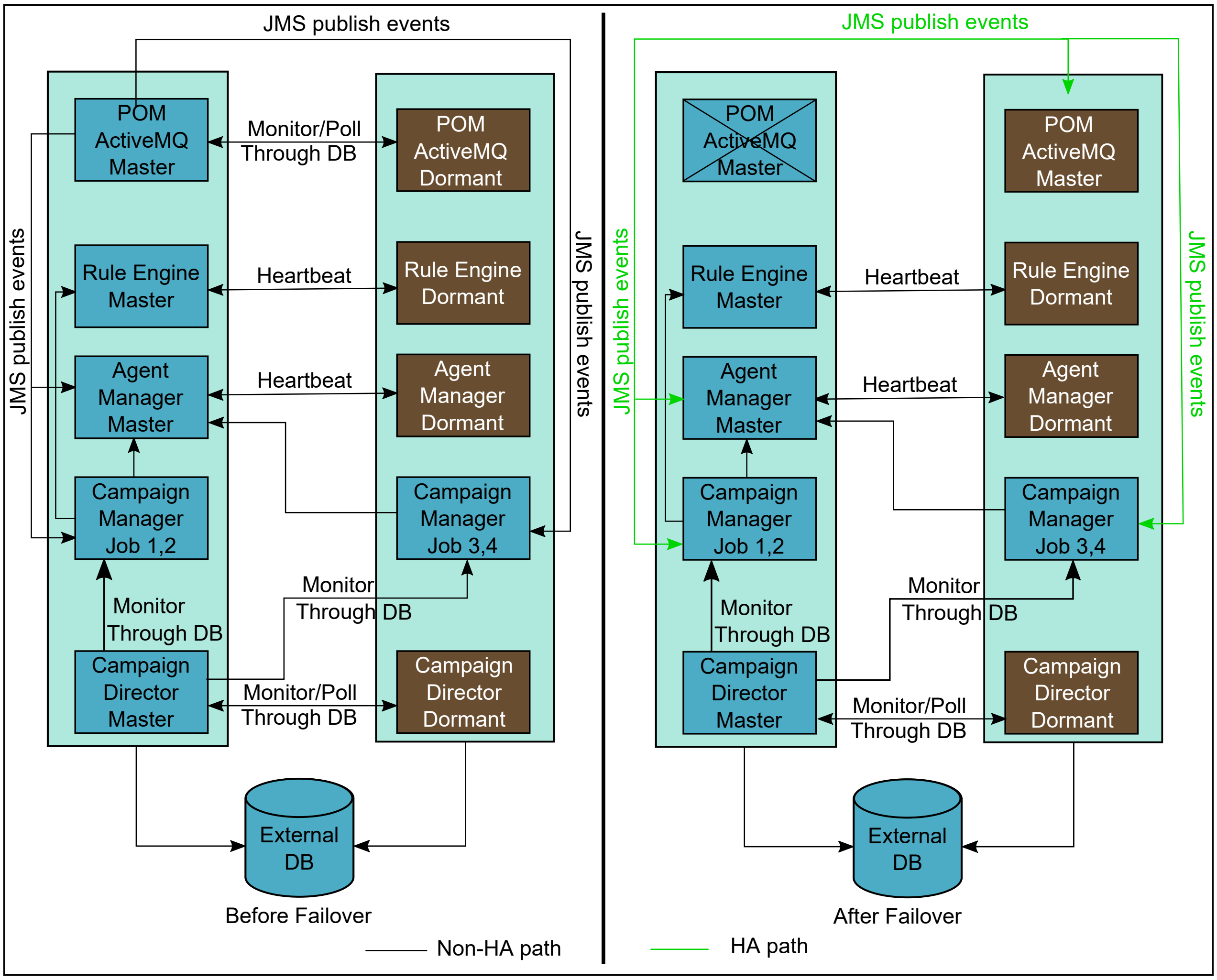
If both application servers get connected within the AppServerWaitTimeOut period, the Agent Manager loads the nailing sessions of all agents and all agents work normally. If the Agent Manager is unable to load information for the nailing session from any of the application servers within AppServerWaitTimeOut period, such agents get Unnailed and jobdetached. Agent Manager assigns these agents again as per the requirement of the jobs.

ActiveMQ High Availability

In a multi-server deployment, there is only one master ActiveMQ. If the master ActiveMQ fails, the dormant ActiveMQ takes over the failed server and ensures no functional impact.

Unlike the single server failure, you can change the run-time parameters from the POM Monitor page. You can pause, resume, and stop the imports.

If the master ActiveMQ process fails ungracefully, another ActiveMQ becomes master after 2 minutes and 20 seconds of the failover time.



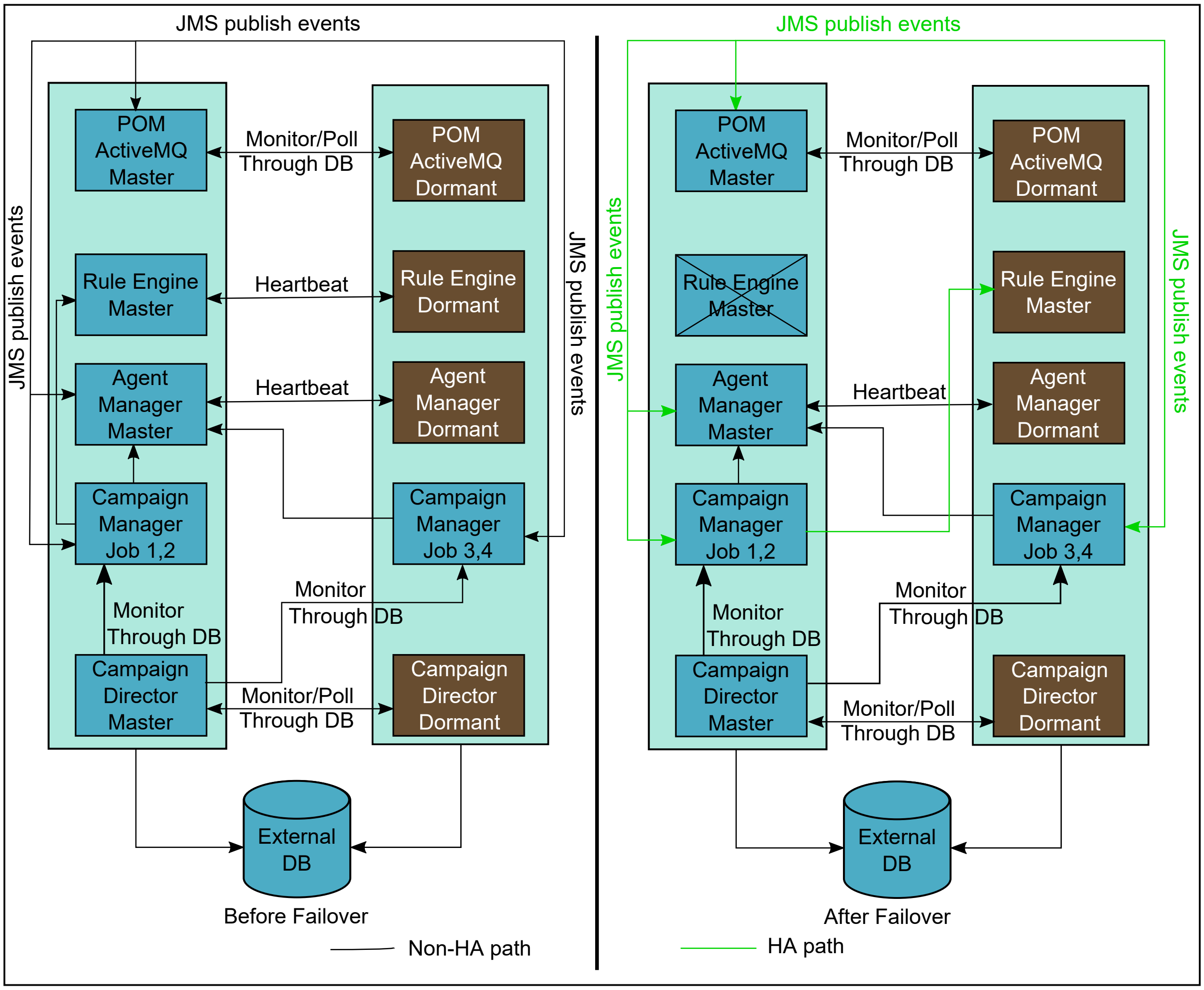
During the failover time of 2 minutes and 20 seconds:

- Run-time changes from POM Monitor does not take effect.
- Java Message Service (JMS) publish events stop working.

Rule Engine High Availability

Rule Engine works either in the master or in the dormant mode. In a multi-server deployment, there is only one master Rule Engine that executes all rules. Each Campaign Manager communicates with the master Rule Engine over a socket.

The following diagram illustrates a high-level overview of the communication between Campaign Manager and Rule Engine:



Rule Engine maintains a heartbeat connection with the other server to monitor its connection. When the heartbeat connection fails, the master and dormant servers update the database with their respective status to avoid multiple masters during a network failure. If the master Rule Engine process fails gracefully, the dormant becomes master immediately. However, for an ungraceful process shutdown, there is a failover time of 45 seconds. After the failover, Campaign Manager gets broken socket connection and polls the database to identify and connect to the new master server for communications.

Rule Engine heartbeat ports can be configured from the Global Configuration page. For more information, see *Using Avaya Proactive Outreach Manager*.

Note:

- Dialing stops during the Rule Engine failover time.
- Ignore the notification for the Rule Engine restart.

Cache Service High Availability

Overview

Cache service is a spring boot service that operates in running mode within a single data center. The service starts Apache Ignite in the cluster mode to support the deployment of POM on multiple servers. All POM cache services in the cluster have a cache replication mode of Apache Ignite. The mode helps in replicating data across nodes. Agent manager, Campaign Manager, and Campaign director services also start an instance of Apache Ignite, but they join as a client node into the cluster. If one of the nodes stop working, then all nodes contain the same data, and the other node acts as a backup.

Function

If you enable the Cache service in POM, the service performs the following functions:

- Storing operational data from POM into Random access memory(RAM).
- Managing the operational data of POM in RAM.

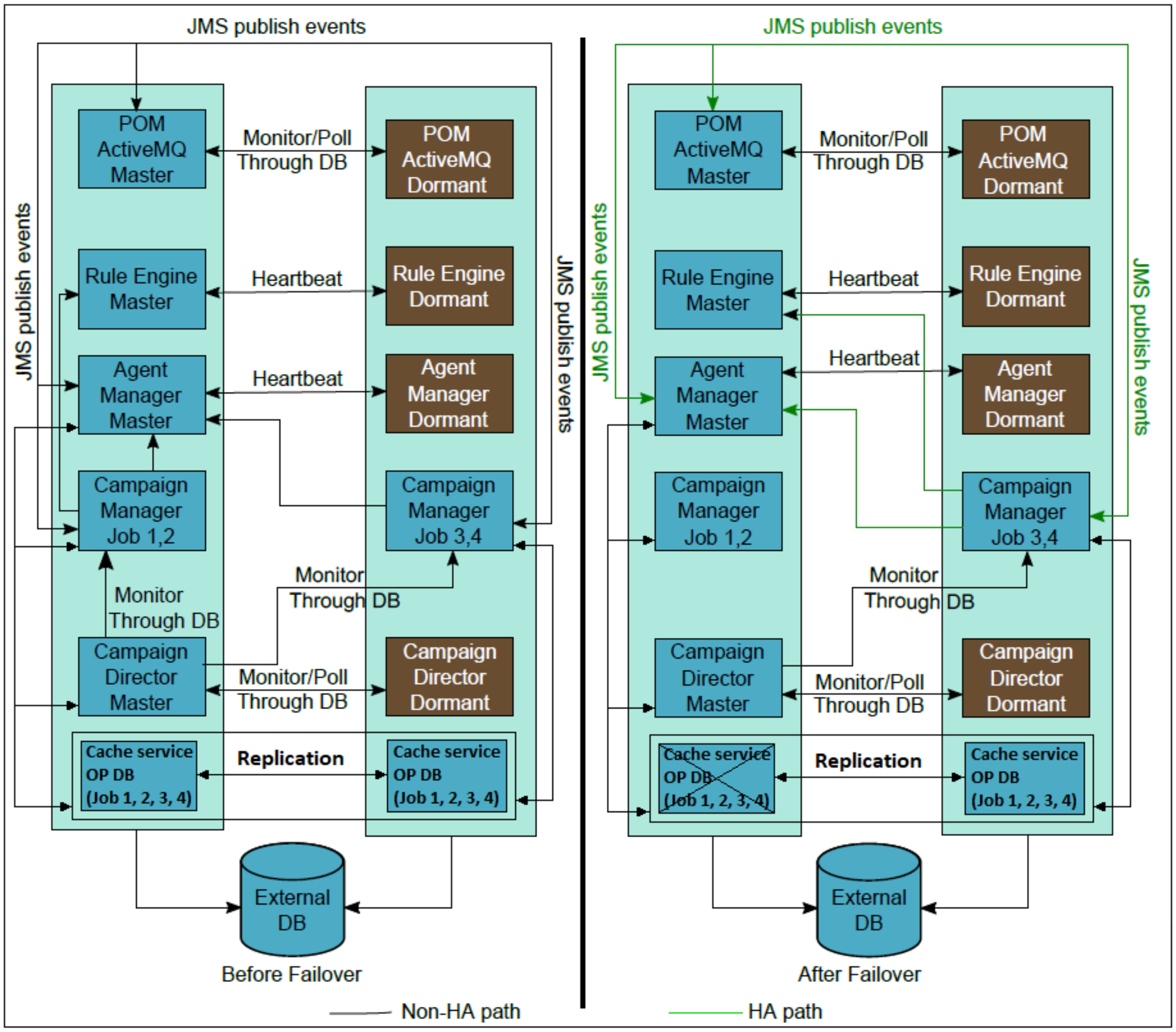
Due to this, the read and write process in POM becomes faster.

Failover

If one of the running Cache service process stops working, all operations in POM function as expected with the other running Cache service.

During a failover, the following activities occur:

- On the POM server where the Cache service stops working, the POM Manager page displays the service state as **Stopped**.
- Campaign Manager, Campaign Director, and Agent Manager service communicate with the node of the running Cache service.


JMS publish events
POM ActiveMQ Master
Monitor/Poll Through DB
POM ActiveMQ Dormant
Rule Engine Master
Heartbeat
Rule Engine Dormant
Agent Manager Master
Heartbeat
Agent Manager Dormant
Campaign Manager Job 1,2
Campaign Manager Job 3,4
Monitor Through DB
Monitor Through DB
Campaign Director Master
Monitor/Poll Through DB
Campaign Director Dormant
Cache service OP DB (Job 1, 2, 3, 4)
Replication
Cache service OP DB (Job 1, 2, 3, 4)
JMS publish events
JMS publish events
External DB
Before Failover
Non-HA path
JMS publish events
POM ActiveMQ Master
Monitor/Poll Through DB
POM ActiveMQ Dormant
Rule Engine Master
Heartbeat
Rule Engine Dormant
Agent Manager Master
Heartbeat
Agent Manager Dormant
Campaign Manager Job 1,2
Campaign Manager Job 3,4
Monitor Through DB
Campaign Director Master
Monitor/Poll Through DB
Campaign Director Dormant
Cache service OP DB (Job 1, 2, 3, 4)
Replication
Cache service OP DB (Job 1, 2, 3, 4)
JMS publish events
JMS publish events
External DB
After Failover
HA path

Agent states before and after failover

Table 9: Agent call state before and after failover

Agent Call State before failover	Agent Call State after failover		
	Customer call not disconnected during failover		**Customer call disconnected during failover**
	Agent Nail State: Nailed	Agent Nail State: UnNailed	Agent Nail State: Nailed
Idle	Idle	Idle	Idle
Talking	Talking	Wrapup	Wrapup
Wrapup	Wrapup	Wrapup	Wrapup
Held	Held	Wrapup	Wrapup
Consult	Consult	Wrapup (Owner) Idle (Passive)	Wrapup (Owner) Idle (Passive)
ConferenceOwner	ConferenceOwner	Wrapup	Wrapup
ConferencePassive	ConferencePassive	Idle	Preview
Preview	Preview	Idle	Preview
Dialing	Talking Wrapup	Wrapup	Wrapup
Callback	Callback	Callback	Callback
Pending call	Idle	Idle	Idle

Agents can have any of the following job states during the call states mentioned in the table:

- Job Attached
- Job End
- Pending Inbound
- Job Manual Inbound
- Pending Manual Job Movement

If an agent is not assigned to any job, the agent call state remains unchanged after the failover.

Chapter 5: Event SDK High Availability

About Apache Kafka

Apache Kafka® is a distributed messaging platform. Users subscribe to the platform and publish data to any number of systems or real-time applications. The platform provides a unified, high-throughput, low-latency network for handling real-time data feeds.

On the Kafka server, POM creates one topic per event type per organization. For the Default organization, POM uses the organization name for creating a topic. For other organizations, POM uses the organization ID for creating a topic.

For more information, see https://kafka.apache.org/10/documentation.html

Example 1

For Default organization, topic names are:

- POM.Default.JOB
- POM.Default.JOBSTATISTICS
- POM.Default.AGENT
- POM.Default.AGENTSTATISTICS
- POM.Default.ENRICHEDATTEMPTRESULT
- POM.Default.ATTEMPT

Example 2

For an organization with ID=1, topic names are:

- POM.1.JOB
- POM.1.JOBSTATISTICS
- POM.1.AGENT
- POM.1.AGENTSTATISTICS
- POM.1.ENRICHEDATTEMPTRESULT
- POM.1.ATTEMPT

Kafka HA

Zookeeper Ensemble

Apache Kafka uses ZooKeeper to store cluster metadata. ZooKeeper is a distributed, open-source coordination service for distributed applications. Zookeeper keeps track of the status of the Kafka cluster nodes and it also keeps track of Kafka topics, partitions, etc.

ZooKeeper service to be active, there must be a majority of non-failing machines that can communicate with each other. To create a deployment that can tolerate the failure of F machines, you should count on deploying 2xF+1machines.

For example, if one zookeeper died, another zookeeper will jump in. This behavior also applies to Kafka brokers, in this case, the system is fault-tolerant

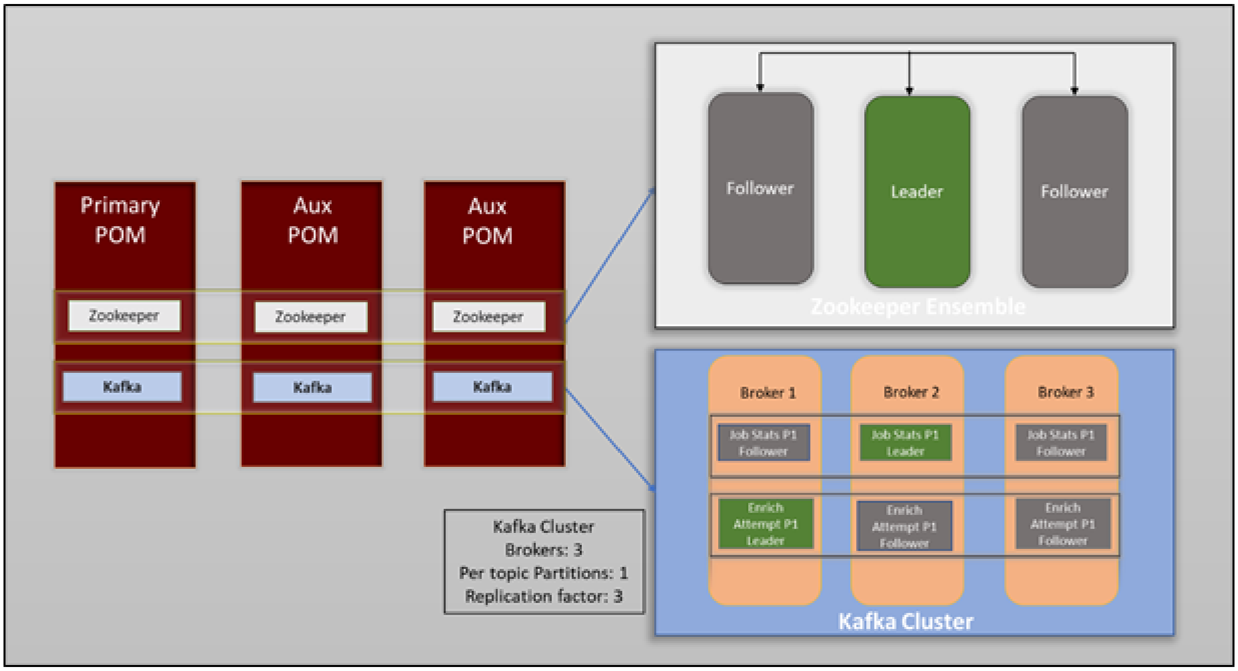
Thus, a deployment that consists of three machines can handle one failure, and a deployment of five machines can handle two failures.

Deployment of six machines can only handle two failures since three machines is not a majority. For this reason, ZooKeeper deployments are usually made up of an odd number of machines.

Note:

POM HA deployment also supports Kafka HA deployment.

The proposed architecture shows ZooKeeper and Kafka deployment on three POM instances (without external Kafka-Zookeeper):



Kafka Broker

Partitioning

POM supports one partition per topic.

Replicas

The list of nodes that replicate the log for this partition regardless of whether they are the leader or even if they are currently alive.

The minimum replication factor recommended for each topic is three to support HA. Hence, we require a Kafka cluster with three nodes as depicted in the diagram, see Zookeeper Ensemble on page 34.

The replication factor has to be less than or equal to the total broker count.

ISR

Set of "in-sync" replicas. This is the subset of the replicas list that is currently alive and caught-up to the leader.

Producer

No impact of Primary producer going down and dormant becoming master.

The producer reads configuration properties from PIM_Kafka_Producer_Config in POM database.

Producer configuration properties

```
retries                2
value.serializer       org.apache.kafka.common.serialization.StringSerializer
request.timeout.ms    120000
acks                  all
max.block.ms           50000
retry.backoff.ms       10000
key.serializer         org.apache.kafka.common.serialization.StringSerializer
```

Enriched Attempt Event Aggregator

The Stream Processor or aggregator service starts on all configured POM machines along with the Dashboard service.

However, due to the same groupID and single partition, only one stream processor processes the events.

External Kafka and Zookeeper installation and configuration

The Zookeeper is primarily responsible for managing a Kafka cluster. Three ZooKeeper servers are the minimum recommended size for an ensemble. Also, to support HA, the minimum replication factor recommended for each topic is three.

If a customer has one primary and one auxiliary POM server in its setup, it effectively has two pomkafka servers. Since three servers are the minimum requirement for an enseable, the customer can introduce a third node using an external Kafka server. External Kafka sever means a server that is operational on a machine where POM is not installed.

In case of external Kafka and Zookeeper installations, the Zookeeper Ensemble and the Kafka cluster must be configured manually.

The following section contains details about installing and configuring the nodes manually:

Note:

POM supports only one external Kafka server.

Setting up ZooKeeper and Kafka

Procedure

1. Access POM Primary.
2. Ensure successful execution of ./enabledKafkaHA.sh script on primary POM server.
3. Add external server machine entry in the `/etc/hosts` file on all POM servers.
4. Copy `$POM _HOME/kafka_2.x-2.x.x` directory from primary POM server to external Kafka server.
5. Set `KAFKA_HOME` environment variable to `kafka_2.x-2.x.x` directory.
6. Remove all data and directories from `$POM _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
   clientPort=2181
   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 host name in listeners and advertised listeners to the host name 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:2181,148.147.XX.XX:2181,148.147.XX.XX:2181
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_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_2
```

```
56_CBC_SHA384,
TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDH_RS
A_WITH_AES_256_CBC_SHA384,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,TLS_ECDHE_
ECDSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_ECDH_ECDSA_WIT
H_AES_256_CBC_SHA,
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_DSS_WIT
H_AES_256_CBC_SHA,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_
RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256,TLS_DH
E_RSA_WITH_AES_128_CBC_SHA256,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDHE
_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDH_RSA_WITH
_AES_128_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_128_CBC_SHA,TLS_EMPTY_RENEGO
TIATION_INFO_SCSV
security.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`

Upgrading Kafka

Before you begin

- Refer to the Zookeeper/Kafka upgrade documentation for detailed steps on backup and restore the kafka config and event data.
- Refer Kafka documentation on how to backup and restore of event data.
- Confirm that the Kafka and Zookeeper version are in sync with the Kafka and Zookeeper installed with POM server.

Procedure

1. Back up all configuration files before upgrading. This includes, for example, /kafka, /kafka-rest, and /etc/schema-registry.
2. Event Data Backup: In the case of POM server, the event data is stored at $KAFKA_HOME/kafka-store/kafka location. Take a backup of the kafka-store directory.

   Note:

   The location may vary.
3. Upgrade the software by following instructions available at https://kafka.apache.org/10/documentation/streams/upgrade-guide.
4. Update the server config to match with the older one.
5. Restore the event data.
6. Start the zookeeper and kafka server.

Enabling Kafka HA Configuration

Kafka and Zookeeper co-residing with POM

The Zookeeper and Kafka gets installed on each POM server as part of POM installation under directory $POM_HOME/kafka_2.12-2.2.0

The post-install script enableKafkaHA.sh at $POM_HOME/bin location must be executed to update Kafka and Zookeeper config files in case of Co-residing setup. The primary POM server will sync the configuration required for HA to auxiliary POM servers.

In case of event data exists on the system, we recommend referring to the Zookeeper/Kafka documentation for detailed steps on the backup of the Kafka config and event data.

Follow the steps to backup the existing event data:

Enabling Event SDK-Kafka HA

Procedure

1. Log in to a primary POM server using the command prompt.
2. Navigate to $POM_HOME/bin directory.
3. 2. Run the script ./`enableKafkaHA.sh`

   The system prompts you with the message:

   ```
   Please enter number of brokers to handle HA[Recommended is an odd
   number]:
   ```
4. Specify 3 or above and press Enter.

   POM prompts you with the message:

   ```
   Is there an external server to be configured? (y/n)
   ```
5. Specify *y* in case of external Kafka server and press Enter.

   Note:

   Maximum allowed external server is one.
6. Specify *n* and POM prompts you with the message:

   POM prompts you with the message:

   ```
   This script can modify properties files of Kafka. Would you like
   to continue? (y/n)
   ```
7. Specify *y* and press Enter.

   POM prompts you with the message:

   ```
   Please enter IP address of POM server 1
   ```
8. Specify the IP address of POM server 1.

POM prompts you with the message:

```
Please enter zookeeper clientPort[DefaultPort = xxxx]
```

9. Specify the port number of the zookeeper and press Enter.
10. 9. Repeat steps 7 and 8 for POM server 2 and POM server 3.
11. Follow the instructions displayed on console after successful execution of the script.
12. Refer to section Verifying Kafka HA Configuration on page 41 to ensure successful Kafka-HA configuration.

Verifying Kafka HA Configuration

Procedure

1. Execute $POM_HOME/bin/enableKafkaHA.sh.
2. Check if zookeeper and Kafka servers are up and running on all POM systems.

   On external Kafka server verify using Java Virtual Machine Process Status Tool (jps).
3. If all servers are up and running, verify the number of brokers (Kafka servers) joined the cluster with the below command:

   ```
   $KAFKA_HOME/bin/zookeeper-shell.sh localhost:2181 ls /brokers/ids
   ```

   Note:

   Check if highlighted broker id matches with number of kafka servers & their respective ids.
4. Check if Kafka topics are created successfully.

   ```
   $KAFKA_HOME/bin/kafka-topics.sh --zookeeper localhost:2181 –list
   ```
5. If topics are created, verify that replicas of all topic partitions are distributed over all the brokers.

   ```
   $KAFKA_HOME/bin/kafka-topics.sh --zookeeper  localhost:2181 –describe
   ```
6. Stop the broker (Kafka server) which is leader for one of the topic partition and check leader is changing for that topic partition and same broker id is not getting listed in replicas for all the partitions.
7. Start the broker again and check broker id is getting listed in Isr replicas for all the partitions.

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 Producers: 4 (CM, AM, CD, Event Aggregator)
- Campaign Jobs: 20
- Number of Agents: 1000
- Contacts/Attempts: 1707069
- Execution duration : 25 hours
- Disk size of kafka-store directory: 27 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**
1707069	67000	25	27	1.08

Topic	**MB/hour**
POM.Default.AGENT	255
POM.Default.AGENTSTATISTICS	255
POM.Default.ATTEMPT	132
POM.Default.ENRICHEDATTEMPTRESULT	12
POM.Default.JOB	40
POM.Default.JOBSTATISTICS	13
Zookeeper directory size	204
Total	859

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.

Geo redundancy

For Geo redundancy deployment we recommend running separate event client or consumers for each data center. Each client will connect to primary POM server running on that datacenter. The event client connected to kafka server of active datacenter will keep getting the events.

Once standby datacenter is active, the event client connected to that Kafka server will start getting the events. Note that only real-time or latest events will be available for consumer in case of POM geo redundancy deployments.

Chapter 6: POM failure scenarios

A single server deployment of POM provides limited capabilities to scale and failover. However, it does not support database resiliency or database failover.

Impact of failure of Cache service

On a single POM server, if the deployed Cache service stops working, the outcome is as follows:

- The currently ongoing calls with agents are unaffected.
- The agents can end the calls as usual. However, the agents cannot set any callbacks on POM.
- Any calls that are already queued by POM for dialing are dialed by the campaign and connected to the agents.
- POM Monitor does not display updated statistics.
- You cannot make runtime changes to Contact List Association by using POM Monitor.
- You cannot add contacts by using webservices.
- All REST webservices that require access to the operational POM database stop working.
- You cannot start a new job.

Impact of restoring Cache service

On a single POM server, after the stopped Cache service resumes a running state, the outcome is as follows:

- Cache service rebuilds the Cache memory.
- Filtering process starts for running campaigns.

  While loading filtered data into the Cache memory, POM changes the state of the job to **Filter in Progress**.

  After loading filtered data into the Cache memory, POM changes the state of the job to **Running**.
- Except for campaigns in **Paused** state, all statistics in the POM Monitor restore to their earlier state.

  The statistics for **Paused** campaigns restores to the earlier state when POM resumes the campaigns for dialing.

- Agents start receiving calls from the running campaigns.
- Operations that were disabled due to the stopped cache service perform their function successfully.

Impact of the POM server reboot

In a single server deployment, the POM server resumes campaign jobs and data imports while the data import operation or campaign execution is in progress.

When the POM server resumes after a reboot:

- The jobs and data source imports scheduled to kick off during the outage do not start.
- The jobs of the same campaign and the new instances of data import start.

Impact of the ActiveMQ failure

In a single server deployment, where you configure Proactive Outreach Manager (POM), Experience Portal Manager (EPM), Media Processing Platform (MPP), and POM database on a single system, you cannot change the run-time parameters from POM Monitor after the ActiveMQ failure.

For a campaign strategy, if you use the ResultProcessor of type `publish`, then any campaigns using that strategy cannot publish campaign attempt results on ActiveMQ.

Impact of the EPMS plug-in failure

POM integrates with Experience Portal Manager (EPM) to provide common administration and management tasks, such as single sign on, user management, logs, alarms, and license management. You can install the EPMS plug-in only on the primary EPM. When you install the EPMS plug-in, it registers POM as a managed application with Avaya Experience Portal, deploys the POM web application on the Tomcat server, and runs the scripts to initialize POM-related configurations.

When the EPMS plug-in does not work, you cannot update the EPM changes in POM, such as licenses update, role changes, addition or deletion of zones, and addition of an EPM server.

Impact of the Campaign Director failure

The following table lists the impact of the Campaign Director failure on various functions:

Function	Impact
Job state	The jobs that are started from the user interface remain in the queued state. The campaign does not finish even when the system dials all contacts or the finish criteria is met. Such campaigns finish when Campaign Director is functional again.
Pausing and resuming campaigns based on user action	The Job state remains unchanged unless the dormant Campaign Director takes over.
Triggering campaigns and data imports at scheduled date and time	The scheduled imports and campaign schedules do not work for the time for which the connection is unavailable.
Data import	Running import jobs are resumed after the dormant Campaign Director takes over even when the status on user interface reflects are running. Import stops execution. When Campaign Director is functional again, the import resumes from where the import was stopped.
Export	Export stops execution. When Campaign Director is functional again, the export resumes from where the export was stopped.
Purging	During the purge operation if Campaign Director becomes nonfunctional, the purging stops. When Campaign Director is functional again, the purging does not resume. The purging starts at the next scheduled date and time.
Campaign Post Processing	Campaign post processing stops. When Campaign Director becomes functional again, the post processing resumes from where it was stopped. Completion code trend report might show stale data for the time for which Campaign Director is nonfunctional.
Terminating campaigns if the finish criteria specified are met	Campaign Director does not perform periodic checks for the finish criteria and campaign does not stop dialing until the dormant Campaign Director failover the failed server.
Trend calculation	Trend calculation, Campaign progress chart, and multiple campaign summary on POM Monitor show stale data for the time for which Campaign Director is nonfunctional.
Report	Completion code trend report might show stale data for the time for which Campaign Director is nonfunctional.
Nuisance rate and alarm generation	Nuisance call rate calculation and alarm generation stop execution until Campaign Director is functional again.
Job allocation	When the master Campaign Director fails and at the same time if Campaign Manager also fails, then the job handled by that Campaign Manager is not allocated to any other Campaign Manager until Campaign Director is functional again.

Impact of the Campaign Manager failure

In a single server deployment, campaigns in the running state continue to run. However, the system does not make any new dialing attempts. The agent activities are not impacted and continue to work as earlier. The system does not assign new calls to agents because the system does not make any new dialing attempts. The scheduled campaign jobs start as normal, but the system does not make any new dialing attempts. When Campaign Manager is functional again, the system resumes the dialing and makes new dialing attempts.

If the Campaign Manager process stops ungracefully and the campaigns are running, some contacts might be stuck and the campaign remains in the running state indefinitely without new attempts being made. You must manually stop such campaigns.

Impact of the Agent Manager failure

In a single server deployment, if the Agent Manager fails, then all agents receive POMNotAvailable notification and agent cannot perform any operation from the desktop. However, the agent in busy state can continue the call but cannot dispose the call from the desktop. All in-progress calls that are answered with live voice are marked as nuisance calls.

During a network outage, POMNotAvailable notifications are not sent to the desktop. Also, all operations performed by an agent are not communicated to Agent Manager and the error message is displayed. After the network connection is re-established, the agent needs to close the desktop and forcefully login again. Such calls are marked with the disposition as the Desktop error and agents need to login again. For the multi-server setup, during the network outage, if the network goes down for more than 40 seconds of the high-availability timeout, then another Agent Manager from the dormant server takes over the zone of failed Agent Manager server. If network connection is reestablished before 40 seconds, then the same server continues to operate.

Impact of the Rule Engine failure

In a single server deployment, campaigns in the running state continue to run. However, the system does not make any new dialing attempts. The agent activities are not impacted and continue to work as earlier. The system does not assign new calls to agents because the system does not make any new dialing attempts. The scheduled campaign jobs start as normal, but the system does not make any new dialing attempts. When Rule Engine is functional again, the system resumes the dialing and makes new dialing attempts.

Impact of the application server failure

The agent activities are impacted. If the application server is down, the system displays the `9007, System error. Please check media server` message on the agent desktop for every command that the agent initiates after the application server is nonfunctional. If MPP is not reachable, the system displays the `9009, "System error. Media server not reachable"` message. The system retries all commands coming from telephony and MPP for 10 minutes. After 10 minutes, whenever application server is functional, the agent needs to forcefully login.

The campaign execution is impacted and the system does not make any new dialing attempts.

None of the POM shipped applications deployed on the application server work.

Impact of the EPM or Tomcat failure

POM web services do not work. Any updates through the agent scripts do not work. If the primary EPM or Tomcat is nonfunctional, you cannot perform POM administrative tasks. You can access the POM monitor through auxiliary EPM.

The campaigns continue to run. However, the system does not make any new dialing attempts. The ongoing calls get an attempt timeout after 2 minutes. If the EPM or Tomcat service is functional within 2 minutes, the system updates the proper disposition. For the multi-server setup, the auxiliary EPM updates the disposition.

Impact of the MPP failure

If MPP stops gracefully, the nailing drops after the grace period expires. If MPP sends AGTNailingLost to Agent Manager, then agent nailing drops and all the busy agents go to Wrapup state.

For a graceful shutdown of MPP, AGTNailinglost event is communicated to POM after 4 minutes. Therefore, if the agent does not perform any activity in 4 minutes, the agent nailing session cleanup happens correctly and the agent gets nailed from another MPP. If the agent performs any operation any time before 4 minutes from the desktop like ReleaseLine, POM receives an error with the **General_Failure** error code. This internally cleans agent states but agent nailing telephony session cleanup does not happen. Agent must drop nailing session manually.

All voice calls stop. The campaigns continue to run. However, when the system makes any new dialing attempts, the system displays an `No MPP resource` error message. If MPP stops gracefully, the voice calls are disconnected after the grace period.

If MPP stops ungracefully because of a network outage or power outage, the nailing does not drop automatically for all logged in agents. The agents must drop the nailing manually.

Recovering MPP

About this task

Use this procedure to recover MPP after a network outage or power outage.

Procedure

1. Log off all agents.

   Ensure that you wait till all agents are logged off.

2. Log in to the Experience Portal Management web console as an administrator.
3. On the Experience Portal Management web console, click **POM** > **POM Home** > **Configurations** > **POM Servers**.
4. On the POM Servers page, click **POM Manager**.
5. Select the check boxes for all POM servers and click **Stop**.
6. On the Experience Portal Management web console, click **System Management** > **MPP Manager**.
7. Select the check boxes for all MPP servers and click **Restart**.

   Ensure that there are no active nailing calls on MPP before you restart the MPP service.

8. On the Experience Portal Management web console, click **System Management** > **Application Server**.
9. Select the check box for the application server that you want to restart and click **Stop**.
10. After waiting for a few seconds, click **Start**.
11. On the Experience Portal Management web console, click **POM** > **POM Home** > **Configurations** > **POM Servers**.
12. On the POM Servers page, click **POM Manager**.
13. Select the check boxes for all POM servers and click **Start**.

Chapter 7: 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
Using Avaya Proactive Outreach Manager	Provides general information about field descriptions and procedures for using Proactive Outreach Manager.	Users
Troubleshooting Avaya Proactive Outreach Manager	Provides general information about troubleshooting and resolving system problems, and detailed information about and procedures for finding and resolving specific problems.	System administrators Implementation engineers Users
Using Avaya Proactive Outreach Manager Reports	Provides general information about the field descriptions and various reports.	Users

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. Navigate to http://support.avaya.com/.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

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

7. Click **Enter**.

Support

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

Index