AVAYA

Avaya Breeze® platform Release Notes

Release 3.9.0.0 GA
Issue 5
August 2024

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.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP:// WWW.MPEGLA.COM.

Table of Contents

Change history

Issue	Date	Description
1	January 16, 2024	GA Release of Avaya Breeze® platform 3.9.0.0
2	January 19, 2024	Modification to Avaya Breeze® platform 3.9.0.0 GA load components table to remove references to ISO/KVM/AWS
3	January 23, 2024	Updated GA build number to Avaya Breeze® platform 3.9.0.0 OVA for ZEPHYR-71581 identified in PSN020624u Avaya Breeze® platform 3.9.0.0 GA Release Notes v3 is introducing a new platform OVA, 3.9.0.0.390034 (PLDS ID AB000000317) that will be replacing the prior approved platform OVA 3.9.0.0.390032 (PLDS ID AB000000313) The original Breeze-3.9.0.0.390032.ova will be removed from PLDS and support.avaya.com and the updated OVA will have a PLDS ID AB000000317. The Avaya Breeze® Element Manager package BreezeEMInstall-3.9.0.0.390016.zip file remains unchanged.
4	June 3, 2024	Updated GA build number to Avaya Breeze® Element Manager package 3.9.0.0.390037 to address ZEPHYR-72568 identified in PSN006095u and ZEPHYR-72113 identified in PSN020630u. Avaya Breeze® platform 3.9.0.0 GA Release Notes v4 is introducing a new Element Manager package, 3.9.0.0.390037 (PLDS ID AB000000318) that will be replacing the prior approved Element Manager package 3.9.0.0.390016 (PLDS ID AB000000314) The original Breeze-3.9.0.0.390016.Element Manager package will be removed from PLDS and support.avaya.com and the updated Element Package will have a PLDS ID AB000000318. The Avaya Breeze® OVA Breeze-3.9.0.0.390034.ova file remains unchanged. Reference PCN2170S.
5	August 6, 2024	Updated GA build number to Avaya Breeze® Element Manager package 3.9.0.0.390038 to address ZEPHYR-73056 identified in PSN006096u and ZEPHYR-70310 general security fixes Avaya Breeze® platform 3.9.0.0 GA Release Notes v5 is introducing a new Element Manager package, 3.9.0.0.390038 (PLDS ID AB000000320) that will be replacing the prior approved Element Manager package 3.9.0.0.390037 (PLDS ID AB000000318) The Avaya Breeze® OVA Breeze-3.9.0.0.390034.ova file remains unchanged. Reference PCN2170S.

Issues fixed in this release

IMPORTANT:
Avaya Breeze® platform 3.9.0.0 GA Release Notes v5 is introducing a new Element Manager package, 3.9.0.0.390038 (PLDS ID AB000000320) that will be replacing the prior approved Element Manager package 3.9.0.0.390037 (PLDS ID AB000000318) The Avaya Breeze® OVA Breeze-3.9.0.0.390034.ova file remains unchanged.

Avaya Breeze® platform 3.9.0.0 GA Release Notes v4 is introducing a new Element Manager package, 3.9.0.0.390037 (PLDS ID AB000000318) that will be replacing the prior approved Element Manager package 3.9.0.0.390016 (PLDS ID AB000000314) The original Breeze-3.9.0.0.390016.Element Manager package will be removed from PLDS and support.avaya.com and the updated Element Package will have a PLDS ID AB000000318. The Avaya Breeze® OVA Breeze-3.9.0.0.390034.ova file remains unchanged.

Avaya Breeze platform 3.9.0.0 GA Release Notes v3 is introducing a new platform OVA, 3.9.0.0.390034 (PLDS ID AB000000317) that will be replacing the prior approved platform OVA 3.9.0.0.390032 (PLDS ID AB000000313) The original Breeze-3.9.0.0.390032.ova will be removed from PLDS and support.avaya.com and the updated OVA will have a PLDS ID AB000000317. The Avaya Breeze® Element Manager package BreezeEMInstall-3.9.0.0.390016.zip file remains unchanged.

1	**Problem Resolved:**	Demo Certificates not supported with CRL.
	Reference:	Zephyr-58182
	Keywords:	CRL, Demo Certificates
2	**Problem Resolved:**	Cluster DB not reachable.
	Reference:	ZEPHYR-67579
	Keywords:	Cluster DB, Cluster DB maintenance test fails
3	**Problem Resolved:**	WARN messages cause flooding the asm.log when running traffic flow using HelloWorld snap-in. For each call you may receive multiple messages.
	Reference:	ZEPHYR-68286
	Keywords:	Traffic runs, Logs
4	**Problem:**	Lambda expressions don’t work well with Breeze 3.7 and beyond
	Reference:	Zephyr-68025
	Keywords:	Java 8, Lambda Expressions, CallListener not initialized
5	**Problem:**	"dasrvstart status all" command shows TPS services being restarted each 10 seconds by Systemd. Manual start of the service from CLI is OK. The Systemd unit file manual “type” defaults to “simple.” Since all TPS applications are using forking where a parent process exists, Systemid believes the service is dead and tries to restart it.
	Reference:	Zephyr-68682

	Keywords:	Systemd, TPS services
6	**Problem Resolved:**	ADA 8.1.1 (or earlier ADA release) will not work with Breeze 3.7 and beyond
	Reference:	Zephyr-68688
	Keywords:	ADA
7	**Problem Resolved:**	ClusterDB: Test Connection leave garbage test files on SMGR in /swlibrary/wildfly_java_tmp
	Reference:	ZEPHYR-69692
	Keywords:	ClusterDB
8	**Problem Resolved:**	Installation – upgradeSolution failed due to change of underlying tool location when we run auto upgrade on SMGR 10.1.2
	Reference:	ZEPHYR-71546
	Keywords:	Oceana, upgradeSolution, mgmtia
9	**Problem Resolved:**	Some calls coming to Attendant Clients from Queue have not Audio
	Reference:	ZEPHYR-71285
	Keywords:	Attendant, media
10	**Problem Resolved:**	Breeze initiates an OFFER SDP template request with inactive media attribute
	Reference:	ZEPHYR-70406
	Keywords:	Call Processing, SDP, Media
11	**Problem Resolved:**	SAML PU does not recover from stale GSC
	Reference:	ZEPHYR-70298
	Keywords:	SAML, Gigaspaces, GSC
12	**Problem Resolved:**	During EM patch(3.8.1.0.381005) installation on SMGR servers zem.ear file is getting corrupted on secondary server when it was in standby mode
	Reference:	ZEPHYR-70289
	Keywords:	Element Manager, Geo-Redundant
13	**Problem Resolved:**	Redo logs generated by Gigaspace are not getting cleared leading to disk overload
	Reference:	ZEPHYR-70138
	Keywords:	Gigaspaces, Overload
14	**Problem Resolved:**	One way video when High Profile enabled
	Reference:	ZEPHYR-69661

	Keywords:	Video
15	**Problem Resolved:**	addParticipant exception 'java.lang.IllegalStateException: Request timed out after 5000 ms'
	Reference:	ZEPHYR-69574
	Keywords:	
16	**Problem Resolved:**	JBoss event log has incorrect permissions on roll-over prevent spirit agent from parsing for alarms
	Reference:	ZEPHYR-71581
	Keywords:	Alarming, JBoss, Management
17	**Problem Resolved:**	asm_assign_policy asm_region_community tables missing from breeze_adopterconfig_39.xml
	Reference:	ZEPHYR-72568
	Keywords:	ASM, User Management, Replication
18	**Problem Resolved:**	Breeze EM: closed clusters "coreplatorm" and "work-assignment" need to have the clusterDBMigration service listed as an optional snap-in allowed to be installed on any new or existing cluster
	Reference:	ZEPHYR-72113
	Keywords:	Presence, Closed Cluster, Optional Snap-in, coreplatform
19	**Problem Resolved:**	Breeze EM: upgrade from 10.1.0.x, 10.1.2.x,10.1.3.1 to 10.1.3.3 fails to upgrade the Breeze EM.
	Reference:	ZEPHYR-73056
	Keywords:	Breeze Element Manager, SMGR
20	**Problem Resolved:**	Breeze EM: misc security fixes CVE-2024-7477: Avaya Aura System Manager SQL injection vulnerability CVE-2024-7480: Improper access control in Avaya Aura System Manager
	Reference:	ZEPHYR-70310
	Keywords:	Breeze Element Manager, SMGR

Known issues and workarounds

1.	**Problem:**	Additional procedures are required to upgrade Avaya Breeze® platform in a Dual System Manager configuration.
	Workaround:	For assistance in upgrading Avaya Breeze® platform in a Dual System Manager configuration, contact Avaya Support.
	Keywords:	Dual System Manager
2.	**Problem:**	OPTIONs pings failed from WAS toward ASSET after upgrade. Any SIP operation with outbound OOD (INVITE and REFER) that are going toward Session Manager fail.

	Workaround:	Restart WebSphere by executing “restart WebSphere”.
	Keywords:	WebSphere, SIP, MakeCall
3.	**Problem:**	Unable to add Trusted addresses for converting to use X-Real-IP for session affinity by clicking the plus button
	Workaround:	Contact Avaya Support for assistance.
	Reference:	ZEPHYR-71512
	Keywords:	X-Real-IP, Session Affinity, Element Manager
4.	**Problem:**	REF fails to recover fully when Breeze goes into overload
	Workaround:	Reboot the impacted cluster to recover the reliable eventing group
	Reference:	ZEPHYR-71281
	Keywords:	Reliable Eventing, Oceana, Overload
5.	**Problem:**	WebSphere hangs if JDBC connection fails
	Workaround:	Resolve external JDBC connection issue, if an internal JDBC connection is hung them reboot impacted node. If your solution requires a full cluster reboot, do that instead as all Breeze nodes may need use this JDBC connection.
	Reference:	ZEPHYR-71280
	Keywords:	JDBC, Overload, Hung Thread, WebSphere
6.	**Problem:**	Number of raised alarms not cleared from the cluster dashboard even after being cleared from alarms page
	Workaround:	Refer to the System Manager > Services> Events> Alarms page and confirm that there are no new alarms and to get the accurate count.
	Reference:	ZEPHYR-71039
	Keywords:	Element Manager, Alarming
7.	**Problem:**	Secure Grid does not function properly when enable on the Cluster Administration page for a Breeze 3.9 Cluster
	Workaround:	Disable secure grid feature
	Reference:	ZEPHYR-71500
	Keywords:	Secure Grid, Platform, Gigaspaces
8.	**Problem:**	Sort order on the Implicit User Profiles form is lost after adding new entries
	Workaround:	Re-sort by choosing the field to reflect ascending or descending order after adding the entry.
	Reference:	ZEPHYR-71251
	Keywords:	Implict User Profile, Element Manager
9.	**Problem:**	upgradeSolution for Oceana zips: logging (solution-upgrade.log) indicates error in resolving Breeze version when a patch is present. Log statement only no functional issue and upgradeSolution finishes successfully. *ERROR: Breeze node x.x.x.x in cluster 'AOCCoBrowser2' still running 3.8.1.1.02381105 instead of 3.8.1.1.381105*

	Workaround:	No workaround is required, ignore the error logs
	Reference:	ZEPHYR-71268
	Keywords:	Patch, upgradeSolution, Oceana
10.	**Problem:**	Level DB fills up ActiveMQ data partition with update to latest version 5.16.7
	Workaround:	Disable Reliable Eventing
	Reference:	ZEPHYR-71781
	Keyworks:	Oceana, REF, Reliable Eventing
11.	**Problem:**	Gigaspaces grid requires reboot if Breeze node count is reduced from 3 to 2 or 2 to 1.
	Workaround:	Reboot the cluster after making cluster node membership changes
	Reference:	ZEPHYR-71241
	Keywords:	Gigaspaces, dcm, cluster
12.	**Problem:**	SSL configuration for Postgres not always happening during first boot due to concurrency issue with SMGR during initTM
	Workaround:	If deploying more than 1 Breeze node, stagger power on of the VM by 5 minutes between each node. Only needed during initial deployment.
	Reference:	SMGR-72613, ZEPHYR-71238
	Keywords:	SMGR, data replication

Avaya Breeze® platform 3.9.0.0 GA load components

Component	Version
Avaya Breeze® platform OVA	3.9.0.0.390034
Avaya Breeze® platform Patch	N/A
System Manager	Latest SMGR 10.1.2.x GA version + latest SMGR Hotfix Latest SMGR 10.1.3.x GA version + latest SMGR Hotfix Latest SMGR 10.2.x GA version + latest SMGR Hotfix
Avaya Breeze® 3.9.0.0 Element Manager Package	3.9.0.0.390038
Avaya Aura Media Server	8.0.2.218 or higher 10.1.0 or higher
SDK	3.9.0.0.390016
WebRTC	3.9.0.0.390016
Avaya WebRTC SDK	3.9.0.0.390016
ClusterDBMigration (Used for clusterDB Migrations from pre-3.9)	3.9.0.0.390016
Authorization	3.9.0.0.390016
External Authorization Client SDK	3.9.0.0.390016
Reliable Event Streaming Adapter	3.9.0.0.390034
Centralized Logging (Used with Oceana)	replaced by new solution integrated with Analytics (see documentation for details)
Zang Call Connector	3.9.0.0.390016
Zang SMS Connector	3.10.0.0.158008

System Manager interoperability

Avaya Aura® System Manager release 10.1.2.x, 10.1.3.x or 10.2.x with the latest SMGR HotFix is supported with the Avaya Breeze® platform 3.9.0.0 GA load. See *Deploying Avaya Breeze® platform*; https://downloads.avaya.com/css/P8/documents/101087264 (chapter 4 *Running the upgradeSolution script for System Manager Release**)*** for more information.

Note: Avaya Aura® System Manager may release additional Integrated Patches, Hot Fixes etc. that may need to be applied additionally on this GA version.

Avaya Breeze® platform can be deployed with Avaya Aura® System Manager:

- Release 10.1.2.x by installing the Avaya Breeze® platform 3.9.0.0 Element Manager using the upgradeSolution utility provided in the latest hot fix release of Avaya Aura® System Manager.
- Release 10.1.3.0 with the latest System Manager Hotfix by installing the Avaya Breeze® platform 3.9.0.0 Element Manager using the upgradeSolution utility provided in the latest hot fix release of Avaya Aura® System Manager.
- Release 10.1.3.1 with the latest System Manager Hotfix by installing the Avaya Breeze® platform 3.9.0.0 Element Manager using the upgradeSolution utility provided in the latest hot fix release of Avaya Aura® System Manager.
- Release 10.1.3.2 with the latest System Manager Hotfix (if available), by installing the Avaya Breeze® platform 3.9.0.0 Element Manager using the upgradeSolution utility provided in the release of Avaya Aura® System Manager.
- Release 10.1.3.3 with the latest System Manager Hotfix (if available), by installing the Avaya Breeze® platform 3.9.0.0 Element Manager using the upgradeSolution utility provided in the release of Avaya Aura® System Manager

- Release 10.2.0.0 with the latest System Manager Hotfix (if available) for Avaya Aura® System Manager, by installing the Avaya Breeze® platform 3.9.0.0 Element Manager using the upgradeSolution utility provided in the release of Avaya Aura® System Manager.

Deployment of Avaya Breeze® platform Release 3.9.0.0 with System Manager Release 10.1.2.x and 10.1.3.x allows you to avoid a full System Manager upgrade. Instead, this deployment requires that you run a special script to install the Avaya Breeze® platform 3.9.0.0 Element Manager with the older System Manager.

Important:

When you have applied the Avaya Breeze® platform Release 3.9.0.0 Element Manager to System Manager Release 10.1.2.x, 10.1.3.0, 10.1.3.1, 10.1.3.2, 10.1.3.3, 10.2.x subsequent integrated patches and hot fixes will leave the 3.9.0.0 Element Manager intact and no further action is required to work with Avaya Breeze® platform 3.9.0.0.

Session Manager interoperability

Avaya Breeze® platform 3.3 or later is required if Session Manager 7.1 IPv6 features are to be enabled. Failure to ensure this will result in Avaya Breeze® platform nodes becoming unusable in this environment.

Note: Avaya Breeze® 3.6 or later is required if Session Manager 8.0.1 Routing Enhancements are to be enabled. Failure to ensure this will result in Avaya Breeze® platform nodes becoming unusable.

Refer to Session Manager documentation for complete information and implications of enabling these routing enhancements.

Upgrade compatibility and sequence

When installing updates to the Avaya Aura solution, it is important that the different components are upgraded in the correct order to ensure platform stability and manageability of the network as part of the upgrade process. Refer to Avaya Aura component release notes for the proper upgrade order. Avaya Breeze® platform can be upgraded at any time after Avaya Aura System Manager and Avaya Aura Media Server (if used) are upgraded. Please consult: https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml for the specific versions of products supported with this release of Avaya Breeze® platform.

Avaya Breeze® platform Release 3.9.0.0 is compatible with Avaya Aura Media Server Release 8.0.2 and higher as well as Avaya Aura Media Server Release 10.1 and higher.

Avaya Breeze® platform Release 3.9.0.0 requires an additional 2GB of Memory. The deployment profiles provided in the OVA have been increased to account for this new requirement. Additional resources were required due to the update in the operating system.

Avaya Breeze® platform Release 3.9.0.0 requires a platform migration as the upgrade method. If the application databases are to be preserved the clusterDBMigration service must be used on the Avaya Breeze® 3.8.x (or earlier) cluster **PRIOR** to the Avaya Breeze® Platorm 3.9.0.0 deployment. Store the database backups on a remote server off of the Avaya Breeze® 3.8.x platform. The Avaya Breeze® 3.9.0.0 migration requires the re-deployment of each targeted Avaya Breeze® node. Re-deployment requires the Breeze node to be outside of the targeted cluster, so the Breeze node should be administratively moved out of the cluster prior to beinging the OVA deployment. This upgrade is referred to as Method 1 in the *Upgrading Avaya Breeze® platform*, https://downloads.avaya.com/css/P8/documents/101087274 . This migration method is the only supported upgrade for Avaya Breeze® platform 3.9. Consult the solution documentation for additional upgrade instructions that may unique to the services installed on the Avaya Breeze® cluster.

Avaya Breeze® platform Release 3.9.0.0 is compatible with Authorization Service 3.9.0.0 and higher. Older versions of the Authorization Service for Avaya Breeze® will no longer be compatible with Avaya Breeze® platform release 3.9.0.x and higher due to a version update of a dependent software component on the Avay Breeze® platform. Therefore, if currently using Authorization Service 3.8.1.1 or older, update the Authorization service to version 3.9.0.0 in the targeted Avaya Breeze® cluster prior to putting the Avaya Breeze® nodes back into the cluster post deployment.

Note: If your snap-in relies on the data stored in the cluster database, you must restore the cluster database prior to placing the Breeze node back into service. Consult your solution documentation for more information.

Disk Alarm notes

The System Overload Monitor has been enhanced to monitor the status of disks on an Avaya Breeze® platform server in addition to the current monitoring of CPU and memory. The monitored disks are the root directory disk /, /var, and /data. If any of these disks reaches a 90% usage level the system is placed in Overload, as it is when memory or CPU reaches a threshold of 80%. This condition causes an alarm OVERLOAD_100001 to be raised with the parameter disk, and the server is placed into Deny New Service state. If the disk reaches 95% of capacity, the node is placed in Extended Overload and alarm OVERLOAD_100003 is raised. Services identified to be associated with a high number of SIP sessions will be removed from service. When the disk is cleaned (manual clearing of files may be required) down to 75% of capacity (and CPU and memory are below the clearing threshold of 60%) the alarms are cleared and the system is placed back in Accept New Service.

New Alarm Details

New alarms (related to the Centralized Logging replacement as well as warning alarms for overload conditions) are introduced in Avaya Breeze® platform 3.9. The Elasticsearch alarms are raised when the connection to the Elasticsearch Common Services Platform (CSP) cluster is lost. The audit polls external CSP Elasticsearch cluster for connectivity issues and raises alarms if necessary. The alarms for cpu, memory and disk overload are an extension to the existing alarms. The new alarms are intended to provide WARNING alarms when the threshold is being approached as opposed to only alarming after the threshold has been reached. The new alarms are described below:

Event ID	Severity	Description	Action
ELASTICSEARCHCONNECTIONERROR	Minor	Logstash is not able to make connection with CSP Elasticsearch. . CSP Elasticsearch health API is called from breeze node using configured host CSP Elasticsearch destination details and if health API call is not successful then ELASTICSEARCHCONNECTIONERROR a Minor alarm will be raised	1. First check destination CSP Elasticsearch pods are up and running, if not then get them running. 2. Check breeze CA and CN is added to CSP Elasticsearch if not then use information given on below page to add CA and CN. https://confluence.forge.avaya.com/display/ZEPHYR/Configuration+Guide+for+Sending+Breeze+Logs+to+CSP+Elasticsearch+Cluster#ConfigurationGuideforSendingBreezeLogstoCSPElasticsearchCluster-1.AddbreezeCAtotheElasticsearchtruststoreonCCM. 3. Check CSP CA is added to breeze if not then use step given on page to do so. https://confluence.forge.avaya.com/display/ZEPHYR/Configuration+Guide+for+Sending+Breeze+Logs+to+CSP+Elasticsearch+Cluster#ConfigurationGuideforSendingBreezeLogstoCSPElasticsearchCluster-3.AddCSPCAtobreeze 4. Try the health API with verbose option which shows more details about errors

			which caused connection loss. curl -vk --cert /etc/logstash/certs/tls_cert.pem --key /etc/logstash/certs/tls_pkcs8.key https://<cluster_fqdn>:30004/_cluster/health Example: curl -vk --cert /etc/logstash/certs/tls_cert.pem --key /etc/logstash/certs/tls_pkcs8.key https://pusntyl189.apac.avaya.com:30004/_cluster/health 5. Check logs at /var/log/Avaya/logstash/setup.log and also logstash service logs generated in file /var/log/messages
ELASTICSEARCHCONNECTIONFINE	Minor	Logstash connection with CSP Elasticsearch is restored	No action.
ELASTICSEARCHCONNECTIONAUTHERROR	Minor	Logstash is not able to make connection with CSP Elasticsearch due to a TLS authentication error.	1. Check certificates generated for logstash are not expired. 2. Certificate files in /etc/logstash/certs are not older than files in default webspehere truststore. 3. Check if cron job "/opt/logstash/bin/setup_logstash.sh update-certs" is running without any error. 4. Check breeze CA and CN is added to CSP Elasticsearch if not then use information given on below page to add CA and CN. https://confluence.forge.avaya.com/display/ZEPHYR/Configuration+Guide+for+Sending+Breeze+Logs+to+CSP+Elasticsearch+Cluster#ConfigurationGuideforSendingBreezeLogstoCSPElasticsearchCluster-1.AddbreezeCAtotheElasticsearchtruststoreonCCM. 5. Check CSP CA is added to breeze if not then use step given on page to do so. https://confluence.forge.avaya.com/display/ZEPHYR/Configuration+Guide+for+Sending+Breeze+Logs+to+CSP+Elasticsearch+Cluster#ConfigurationGuideforSendingBreezeLogstoCSPElasticsearchCluster-3.AddCSPCAtobreeze 6. Try the health API with verbose option which shows more details about errors which caused connection loss. curl -vk --cert /etc/logstash/certs/tls_cert.pem --key /etc/logstash/certs/tls_pkcs8.key https://<cluster_fqdn>:30004/_cluster/health Example: curl -vk --cert /etc/logstash/certs/tls_cert.pem --key /etc/logstash/certs/tls_pkcs8.key https://pusntyl189.apac.avaya.com:30004/_cluster/health 7. Check logs at /var/log/Avaya/logstash/setup.log and also

			logstash service logs generated in file /var/log/messages
ELASTICSEARCHCONNECTIONAUTHFINE	Minor	Logstash connection with CSP Elasticsearch is restored.	No action.
avCEAOVLD005	Warning	Collaboration Environment instance is approaching Memory Overload state.	Investigation into current traffic/load state for impacted node. Consider increasing resources if this is alarm is reoccurring without the presence of an error condition.
avCEAOVLD006	Normal	Collaboration Environment instance is no longer approaching Memory Overload state.	No action.
avCEAOVLD007	Warning	Collaboration Environment instance is approaching CPU Overload state.	Investigation into current traffic/load state for impacted node. Consider increasing resources if this is alarm is reoccurring without the presence of an error condition.
avCEAOVLD008	Normal	Collaboration Environment instance is no longer approaching CPU Overload state.	No action.
avCEAOVLD009	Warning	Collaboration Environment instance is approching Disk Overload state.	Investigation into current traffic/load state for impacted node. Check for error conditions causing excessive logging actions Consider increasing resources if this is alarm is reoccurring without the presence of an error condition.
avCEAOVLD010	Normal	Collaboration Environment instance is no longer approaching Disk Overload state.	No action.

Logging API

A new method is introduced in the Logger API. Details as shown below.

```
public void logEventAlways(final String eventId, final Object... arguments)
```

This method is used to log events/alarms even when the node is in Deny New State.

Cluster Database notes

If use of the cluster database is required on an Avaya Breeze® platform cluster, it is recommended, in most cases, that deployment profile 2 or higher is used for fresh installations. For pre-existing deployments, it is recommended, in most cases, to increase your physical memory to 10GB or higher. Consult your snap-in documentation for disk sizing recommendations.

System memory on the Active Cluster Database node can go into swap on traffic when using the cluster database. When the cluster database is enabled, it consumes system memory depending upon the usage. It takes a minimum of 300 MB when no traffic is present. The overall memory consumption by the cluster database depends upon: the number of connections made from the snap-in; the number of nodes in the cluster; traffic rate; and database schema. The sustainable traffic rate also depends on the RAM size of the Avaya Breeze® platform nodes in the cluster. It is recommended to reduce the load on nodes hosting the cluster database. To accomplish this, make the following adjustments to the cluster. First assign the active cluster database to the same node as the active load balancer (if applicable). During upgrade, the active cluster database may need to move temporarily, but steps should be taken to adjust the roles of the cluster database post platform upgrade to follow this recommendation. Second, use the following table to determine the SIP load balancing weight to assign to each server in the cluster. This requires additional administration on the Local Hostname Resolution form for Session Manager. See High Availability Administration, in *Deploying Avaya Breeze® platform* for details about the administration required.

Number of servers in the cluster	2	3	4	5
Initial primary database server	50	25	16	12
Initial backup database server	50	25	16	13
Server 3		50	34	25
Server 4			34	25
Server 5				25

The exact memory requirements for the cluster database varies by snap-in. Consult your snap-in deployment guide for further details on their specific memory needs.

Media Operations notes

This scenario is specific to call scenarios where the party that answers a call may differ from the party that was originally called. For example, if the called party is a Vector Directory Number (VDN) on Communication Manager, where the associated vector destination does a redirect of the call to another party. Depending on how the vector is defined, the answering party reported to a snap-in may be different than the called party.

In Collaboration Environment 3.0 the distinction between the called party and answering party was ambiguous. This resulted in behavior where a media operation invoked on the called party was applied to the answering party, even if the answering party differs from the called party.

In Avaya Breeze® platform 3.1 and later, this distinction was refined so that media operations invoked on the called party are ineffective if the answering party differs from the called party.

Snap-ins that invoke media operations (e.g. play announcement, prompt and collect, speech search) on the called party may then encounter failures if the answering party is not the called party.

The desired behavior can be achieved by invoking media operations on the answering party.

WebRTC notes

The shared string for the authorization token is “Avaya Authorization Token.” Refer to the documentation for “How to use authorization token” and to the WebRTC sample application in the WebRTC SDK for details.

Whitelist Snap-in notes

On Breeze 3.4 and later, older versions of the Whitelist Sample Snap-in are no longer supported.

Zang SMS Connector Snap-in notes

In the Avaya Breeze® 3.5.x and prior, the Zang Outbound-only SMS Connector Snap-in was bundled with Avaya Breeze® platform. Going forward the Zang SMS Connector Snap-in supporting inbound and outbound SMS is available post GA as a separate PLDS download.

Flow control

It is important to avoid traffic congestion for a service that sends a burst of voice announcement requests through Avaya Breeze® platform. The current recommendation is no more than 375 phone numbers to be included per single request to this type of service. Each request must be staggered by 15 seconds or more between subsequent requests to the same service on the same Avaya Breeze® platform instance. Empirical testing has shown that a reliable minimum delay for 10,000 requests using one Avaya Breeze® platform is 15 seconds. A lower delay value is not recommended because it increases the probability of encountering performance-related problems.

Additional consideration should be given when the sum of requests targeted for the voice announcements exceeds the maximum port allocation for a single instance of the Avaya Aura Media Server. The Avaya Aura Media Server virtual machine bundled with Avaya Breeze® platform is maximum rated at 1100 ports. A single Avaya Aura Media Server would be expected to service 1,000 announcements over a period of five minutes and therefore 2,000 announcements would be serviced over 10 minutes. Given this guideline, five Avaya Aura Media Server instances will be required at a traffic level of 10,000 voice announcement requests serviced over a ten minute time period. The same traffic distribution guidelines as discussed above apply here as well.

If the phone numbers specified in the voice announcement request contain non-SIP devices such as H.323 endpoints or non-SIP trunk resources, be sure to verify this configuration to ensure you have the needed Digital Signal Processors (DSP) resources required to support a simultaneous voice announcement request to this set of users.

The following formula can be used to estimate the number of Avaya Aura Media Server instances required to support a particular burst application.

MaxSimultaneousRequiredLicenses = (((AnncLength + MaxDelayToAnswer)/FCDelay) * (CollectionSize))*NumberOfLicensesPerCall)

TotalAMSInstances*=ceiling((MaxSimultaneousRequiredLicenses)/(AMSMaxLicenseThreshold))

AnncLength = full length of the recorded announcement in seconds.

MaxDelayToAnswer = anticipated max ringback delay prior to answer in seconds.

FCDelay = Flow Control Delay, which is the time between simultaneous collection bursts to an Avaya Breeze® platform instance in seconds (current recommendation is 15 seconds or more).

CollectionSize = For an outcalling burst application this number represents the total number of users defined within a single simultaneous request for voice announcements to an Avaya Breeze® platform instance.

AMSMaxLicenseThreshold = the default threshold is 825 (75% of current session maximum).

NumberOfLicensesPerCall = 2 (number of active sessions per call; each session uses 1 license).

*In summary, the **TotalAMSInstances** is the “rounded up” value of the total number of simultaneous licenses required, divided by the license threshold administered on a single Avaya Media Server virtual machine. See the example below for further clarification.

For example:

Using the sample service, MultiChannel Broadcast, send 10,000 voice 45-second announcements to individual phone numbers within or off enterprise. In this type of example, assume it will take no more than 15 seconds for any user to answer the calls generated from this application and a single request includes 250 phone numbers, therefore 40 requests are required to reach 10,000 phone numbers in total.

AnncLength=45 seconds
MaxDelayToAnswer=15 seconds
FCDelay = 15 seconds
CollectionSize= 250
MaxSimultaneousRequiredLicenses = (((45+15)/15)*250)*2 = 2000
TotalAMSInstances = ceiling (2000/825) = 3

request1=[phone1…phone250]; request2=[phone251…phone500], …,
request40=[phone9750…phone10000]

Each request per Avaya Breeze® platform instance would still need to be staggered by 15 seconds.

In this example, a total of three Avaya Aura Media Servers and one Avaya Breeze® platform instance could service the request for 10,000 voice announcements within 10 minutes. Note: a larger collection, longer answer delay, and/or announcement length requires additional Avaya Aura Media Server resources.

Callbacks for Media Operations

Some behaviors have changed related to media callback listener methods to improve consistency in the media portions of the API (including voice XML and speech search). The original and changed behaviors are:

1. Invoking stop on a prompt and collect media operation.

   ORIGINAL BEHAVIOR: Two invocations of MediaListener methods are made, one to the playCompleted callback method with a cause of STOPPED, and one to the digitsCollected callback method with a cause of STOPPED.

   NEW BEHAVIOR: A single invocation is made to the digitsCollected method with a cause of STOPPED. This new behavior aligns better with the behavior that occurs when a prompt and collect operation ends after playing prompt and collecting digits.

2. Invoking stop on a send digits operation.

   ORIGINAL BEHAVIOR: The invocation of stop has no effect, and the send digits operation continues to completion as if stop were NOT invoked. Upon completion no invocation of the MediaListener's sendDigitsCompleted method occurs.

   NEW BEHAVIOR: The invocation of stop still has no effect. However, upon completion of the send digits operation, the sendDigitsCompleted method is invoked with a cause of COMPLETE. This new behavior better reflects what has actually taken place.

3. A party drops/is dropped from a call under the following circumstances:

   a. The call termination policy is set to NO_PARTICIPANT_REMAINS.

   b. A media operation is active on the dropped party.

   ORIGINAL BEHAVIOR: An invocation of the appropriate MediaListener callback method occurs for the

operations play, prompt and collect, collect, and record. For other media operations, no listener callback methods are invoked. NOTE: The listener interface that is implemented by a snap-in for most media operations is MediaListener. For voice XML and speech search, the listener interfaces are VoiceXMLDialogListener and SpeechSearchListener, respectively.

NEW BEHAVIOR: An invocation of the recordCompleted method occurs for an active record operation. No invocation of callback methods occurs for other media operations. This new behavior better matches the behavior that occurs when a call ends.

General Operational Changes/Frequently Asked Questions

1. **Java API change** behavior from 3.2 -> 3.3
   The return value from the Java API InetAddress.getHostName() on an Avaya Breeze® platform node has changed from returning an FQDN (e.g., myhost.example.com) to returning the host's name (myhost). If the FQDN is desired, use InetAddress.getCanonicalName()."

2. **Authorization service** behaviour – The Avaya Breeze® platform Authorization Service does not support SAML Single Logout.
   The Avaya Breeze® platform Authorization Service acts as an SAML Service Provider when trying to authenticate end-users against an Identity Provider. Authentication is initiated by using an SP initiated SSO exchange. The Authorization Service then optionally creates a session for the user, and redirects the user back to the Client snap-in with an "authorization code". For the current release, SP initiated Single Logout is not supported.

3. **Authorization service** behaviour – After authenticating the user, the following error is seen on the browser: Client authentication failed. Session validation failed.
   Resolution:
   - On System Manager click **Elements> Avaya Breeze®> Cluster Administration.**
   - Select the Cluster where Authorization Service has been installed.
   - Select the "Certificate Management" tab.
   - Click on "Update/Install Identity Certificate (Authorization Service)"

Avaya Breeze® platform 3.9.0.0 port changes

There are no notable changes to port usage in Avaya Breeze® platform 3.9.0.0.

Avaya Breeze® platform traceMessage message tracer tool

Prior to release 3.3, individual execution of traceHTTP, traceBus and traceSIP were required. With traceMessage, the ability to trace and view multiple protocols within the same tool is now supported.

New with traceMessage is the ability to enable and show installed snap-in logs as well as trace AAMS media control messages over HTTPs.
NOTE: Although media server messages are HTTP messages, the trace tool generally treats media server messages separately from other HTTP tracing messages. Media server tracing is generally most useful when combined with SIP tracing. The SIP messages provide the context within which the media server messages are generated for a given call.

As with the previous trace tools, traceMessage can be performance impacting depending on the current traffic levels on the Avaya Breeze® platform server.

The Filter options can take a regular expression. Filters are also available by pressing 'f' in the application.

WARNING: traceMessage may use high CPU and memory in a busy Avaya Breeze® platform server. The trace will stop displaying packets after capturing 10000 messages.

Usage examples:

- To start a new capture, run 'traceMessage' without arguments and then press 's':
  $ traceMessage
- To filter messages from/to 1.1.1.1 and 2.2.2.2:
  $ traceMessage -i "1.1.1.1|2.2.2.2"
- To analyze previously captured files for SIP, HTTP, AAMS and the call processing logs:
  $ traceMessage call_proc.log tracer_asset.log mediaServer_http.log niginx_http.log
- To filter SIP messages containing 'Avaya' in the 'User-Agent' header field:
  $ traceMessage -g "User-Agent=Avaya"
- To filter SIP sessions that got a '487 Request Terminated' response:
  $ traceMessage -o "487 Request Terminated"

New Avaya Breeze® platform External Authorization SDK

With the introduction of Avaya Breeze® platform Authorization Service support with Oceana 3.3 / Avaya Breeze® platform Client SDK 3.2 role based authorization used by Avaya Breeze® platform Client SDK's Identity Management Services Package was removed and this package was marked obsolete. This created a solution gap for 3rd party developers wishing to create Oceana based applications. The new External Authorization SDK bridges this gap with the support of:

Authorization Code Grant Type

- Both the Application and the user are authenticated. It is a redirect-based flow.
- Application does not handle the user's credentials. It redirects the user's browser to the Avaya Breeze® platform Authorization Service (AS) for validation of credentials.
- Once validated by the Authorization Services it redirects the browser back to the application with an authorization code, which the application can then exchanges for an access token.

Authorization Code Grant Type can enable SAML-based authentication, which could include Multi-Factor Authentication (MFA).

The External Authorization SDK can be used with Avaya Breeze® platform Authorization Services release 3.3, 3.4,3.4 SP or 3.5, 3.5 SP, 3.6, 3.7, 3.8, 3.8 SP, and 3.9

Security -- Spectre/Meltdown

For more information on Spectre/Meltdown mitigation refer to PSN020346u.

- To mitigate the Meltdown and Spectre vulnerabilities, the processor manufacturers and operating system developers must provide software patches to their products. These are patches to the processors and operating systems, not to Avaya products.
- When these patches are received by Avaya, Avaya will test these patches with the applicable Avaya products to determine what, if any, impact these patches will have on the performance of the Avaya product.
- Avaya is reliant on our Suppliers to validate the effectiveness of their respective Meltdown and Spectre vulnerability patches.
- Avaya's test effort is targeted towards reaffirming product/solution functionality and performance associated with the deployment of these patches.
- The customer is responsible for implementing, and the results obtained from, such patches.
- Although Avaya Breeze® platform performance impact is negligible, customers should be aware

that implementing these patches may result in performance degradation.

Enhanced Security with LDAPs Connections

Issue: Avaya Breeze® platform applications that were previously able to successfully connect via LDAP over a secure connection may no longer be able to do so.

Background: Beginning with Avaya Breeze® platform 3.6.0.0, endpoint identification has been enabled on LDAP secure TLS connections. This may necessitate the need to generate a new identity certificate for the LDAP server that includes the server's Fully Qualified Domain Name (FQDN) or IP Address.

How to identify:

1. In the Avaya Breeze® platform application log for Authorization (/var/log/Avaya/services/AuthorizationService/AuthorizationService.log), check for the following exception:

```
[Root exception is javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException: No subject alternative names present]
Caused by: java.security.cert.CertificateException: No subject alternative names present
at com.ibm.jsse2.util.b.b(b.java:104)
at com.ibm.jsse2.util.b.a(b.java:88)
at com.ibm.jsse2.aD.a(aD.java:165)
at com.ibm.jsse2.aD.a(aD.java:168)
at com.ibm.jsse2.aD.a(aD.java:211)
```

Recommended Solution:

1. First, inspect the current identity certificate on the LDAP server using one of the following mechanisms:
    a. System Manager Trusted Certificates provisioning
        1. On System Manager navigate to **Services > Inventory > Manage Elements**.
        2. Select the Avaya Breeze® platform node and choose **More Actions> Manage Trusted Certificates.**
        3. Choose Add, then Import using TLS.
        4. Enter the IP address or FQDN of the LDAP server, and port 636.
        5. Push **Retrieve**.
        6. Inspect the certificate details.
    b. OpenSSL command line tool.
    c. Login to an Avaya Breeze® platform server using the cust login, or to any other machine that has the OpenSSL tools installed:
        1. Run the following command, substituting your actual LDAP FQDN or IP address for MY_LDAP_FQDN_OR_IP:

           echo | openssl s_client -showcerts -servername <*MY_LDAP_FQDN_OR_IP*> -connect <*MY_LDAP_FQDN_OR_IP*>:636 2>/dev/null | openssl x509 -inform pem -noout -text

        2. Inspect the certificate details.
2. Check the certificate for the presence of the LDAP server's FQDN in the CN or in the Subject Alternative Name (SAN) fields. The LDAP server name or IP address must match what is in the CN or SAN. Additionally, if FQDN was used, DNS must be setup with this FQDN and corresponding IP.
3. If there is not a valid FQDN or IP address in the certificate, generate a new certificate with valid FQDN or IP address (FQDN recommended) in the CN or SAN filed and provision it on your LDAP server.

4. Navigate to **Users> Directory Synchronization > Sync Users** and check the datasource. It must be configured with the exact FQDN or IP address used in the certificate.
5. If required, import either the LDAP server's certificate or the Certificate Authority (CA) certificate (recommended) as a trusted certificate for Avaya Breeze® platform by completing the process specified in 1a above. If the new certificate is signed by the same CA as had signed the previously used certificate, and if that CA certificate was previously provisioned as trusted by Avaya Breeze® platform, this step should not be required.

Refer to https://developer.ibm.com/answers/questions/475181/how-to-fix-this-ldap-ssl-error-javasecuritycertcer.html and https://www.oracle.com/technetwork/java/javase/8u181-relnotes-4479407.html?printOnly=1 for more detail on this enhanced security setting.

Upgrade instructions specific to SMGR 10.1 – UnifiedAgentController, UnifiedAgentContextService and CustomerControllerWeb

Follow the upgrade procedure and post the upgrade If VMs still have snapshot, remove all of them. Please note that customer doc for upgrade procedure include taking snapshot before upgrade, but it should also need to be removed within 48 hours after upgrade completed.

Following are the steps to update JDBC Provider snap-in when SMGR is upgrade to 10.1 from previous version.

1. Create another JDBC Provider snap-in with existing JDBC driver jar.
2. Install new JDBC Provider snap-in on required clusters.
3. Delete existing JDBC data sources, then uninstall older JDBC provider snap-in.
4. Recreate the JDBC data sources using same values like old data sources, using newly installed JDBC Provider snap-in (Created in step #1.)

Authorization Service SAML authentication support matrix

Authorization Service v 3.7.x, 3.8.x, 3.9.x

Authentication Mechanism	Windows 2012 Domain Controller	Windows 2016 Domain Controller
LDAP	Yes	Yes
SAML - Password Protected Transport	Yes	Yes
SAML – Integrated Windows Authentication	Yes	Yes
SAML - Kerberos	No	Yes