AVAYA

Avaya Breeze™ Release Notes

Release 3.2 SP GA
Issue 2
December 2016

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 by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its 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 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 its hardware and Software (“Product(s)”). 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: http://www.avaya.com/support

Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, http://support.avaya.com/Licenseinfo ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 AUTHORIZED RESELLER; 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. 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. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

License type(s)

CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation 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

Each Product has its own ordering code. Note that each instance of a Product must be separately licensed and ordered. "Instance" means one unique copy of the Software. For example, if the end user customer or Business Partner would like to install 2 instances of the same type of Products, then 2 Products of that type must be ordered.

Third-party components

"Third Party Components" mean certain software programs or portions thereof included in the Software that 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"). 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 Documentation or on Avaya's website at: http://support.avaya.com/ThirdPartyLicense/. You agree to the Third Party Terms for any such Third Party Components.

Note to Service Provider

The Product may use Third Party Components that have Third Party Terms that do not allow hosting and may need to be independently licensed for such purpose.

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: http://www.avaya.com/support.

Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, 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 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, and “Linux” is a registered trademark of Linus Torvalds.

Downloading documents

For the most current versions of documentation, see the Avaya Support website:

http://www.avaya.com/support

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product.

For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Table of Contents

Issues fixed in this release

1. **Resolved Problem:** Call drops when Engagement Designer adds a participant in a two party make call scenario.

   Reference: ZEPHYR-44933, ZEPHYR-44898
   Keywords: Engagement Designer

2. **Resolved Problem:** Documentation Updates.
   Reference: ZEPHYR-44791, ZEPHYR-44747, ZEPHYR-44704
   Keywords: Documentation updates

3. **Resolved Problem:** Calls drop when conferenced in to AAC Service Management page.
   Reference: ZEPHYR-44702
   Keywords: Conference, AAC

4. **Resolved Problem:** High CPU occupancy on Reliable Eventing Broker during traffic.
   Reference: ZEPHYR-44666
   Keywords: Reliable Eventing

5. **Resolved Problem:** Cluster Element Manager validations.
   Reference: ZEPHYR-44657
   Keywords: Element Manager

6. **Resolved Problem:** Avaya Aura Media Server MEDIA_PROCESSED message gets lost when Answering party and Called party fields do not match.
   Reference: ZEPHYR-44618
   Keywords: One party make Call

7. **Resolved Problem:** Engagement Call Control (ECC) traffic failures after 7 hours of run.
   Reference: ZEPHYR-44551
   Keywords: Engagement Call Control

8. **Resolved Problem:** Disable Call restruction by default.
   Reference: ZEPHYR-44550
   Keywords: Call reconstruction

9. **Resolved Problem:** Memory shortage in CECommonSpace.
   Reference: ZEPHYR-44509
   Keywords: Gigaspaces

10. **Resolved Problem:** When using CEnetSetup to change the hostname, System Manager does not recognize the Avaya Breeze™ version or other status information. This causes the system to be in a bad, unrecoverable state.
    Reference: SMGR-36726
    Keywords: CEnetSetup, hostname, OVA deploy

11. **Resolved Problem:** Presence Services snap-in can be used with Avaya Breeze™ 3.2 beta load.
    Reference: ZEPHYR-40511
    Keywords: Presence Service Snap-in

12. **Resolved Problem:** Eventing Connector can now be uninstalled from the System Manager Service Management page.
    Reference: ZEPHYR-39679
    Keywords: Eventing Connector, Unistall

13. **Resolved Problem:** ClicktoCall sample app now works via SBC when it is used to route HTTP requests to an Avaya Breeze™ load balancer that hosts the snap-in.
    Reference: ZEPHYR-39584
    Keywords: ClicktoCall

14. **Resolved Problem:** The Eclipse plug-in does not get stuck when incorrect ports are configured for System Manager/ Avaya Breeze™.
    Reference: ZEPHYR-39081
    Keywords: Eclipse plug-in

15. **Resolved Problem:** When using the ClicktoCall snap-in, the Calling Identity is now displayed correctly to the Called party.
    Reference: ZEPHYR-37944
    Keywords: ClicktoCall

16. **Resolved Problem:** traceHTTP now runs successfully every time it is run after deploying the Avaya Breeze™ OVA.
    Reference: ZEPHYR-34900
    Keywords: traceHTTP

17. **Resolved Problem:** When ECC getVoicemail API retrieves the media link using SDK API MediaFactory.createPlayItem().setSource(wavurl), it does not fail if the file has no extension. There is no need to append a dummy file name extension to the media file.
    Reference: ZEPHYR-41035
    Keywords: ECC Voicemail

18. **Resolved Problem:** With Callable snap-ins, call intercepts now work correctly. 200OK ACKs are propagated as expected.
    Reference: ZEPHYR-43193

Keywords: Callable snap-in

19. **Resolved Problem:** After deploying Avaya Breeze™ with the SDM Client, adding the VM host in System Manager SDM, and performing the trust establishment operation on the Avaya Breeze™ VM, the Trust establishment now works successfully from the System Manager SDM.
    Reference: ZEPHYR-38547
    Keywords: SDM, Trust establishment

20. **Resolved Problem:** For an Inbound call to Agent from an external number (H.323 station in another Communication Manager), calls do not drop after 30 seconds.
    Reference: ZEPHYR-39683
    Keywords: Call drop

21. **Resolved Problem:** AS: No entry is created under the Authorization Service Instances tab when AS is assigned to an empty cluster.
    Reference: ZEPHYR-42506
    Keywords: Authorization

22. **Resolved Problem:** Avaya Breeze™ does not function if the disk space is full.
    Reference: ZEPHYR-39079
    Keywords: Platform

23. **Resolved Problem:** HTTP Proxy exclusion – the CEnetsetup tool accepts Blank and invalid characters for HTTP Proxy hostname and port.
    Reference: ZEPHYR-43315
    Keywords: Platform, CEnetsetup tool

24. **Resolved Problem:** File not found errors seen while installing/uninstalling 3.2 patch.
    Reference: ZEPHYR-44984
    Keywords: Patch Installation

25. **Resolved Problem:** Snap-in install - ClusterDB upgrade scripts are not run if properties.xml has EOL characters in non-UNIX format.
    Reference: ZEPHYR-44685
    Keywords: ClusterDB

26. **Resolved Problem:** Wrong display on the caller after parallel forking.
    Reference: ZEPHYR-44638
    Keywords:

27. **Resolved Problem:** During ISO upgrade, JDK version mismatch causes a warning to be shown to the user.
    Reference: ZEPHYR-44607
    Keywords: Upgrade

28. **Resolved** After an AES interchange for some stations, event subscriptions may not

Problem: work as expected.
Reference: CCC-68
Keywords: Engagement Call Control

29. **Resolved Problem:** Deletion of a service fails if a snap-in is not in /emdata/svars.
Reference: ZEPHYR-42466
Keywords: Element Manager

Known issues and workarounds

Generic Avaya Breeze™ related

30. **Problem:** If three wrong attempts are made to reset the Avaya Breeze™ password (used passwords that do not meet the password strength criteria), it will lockout the account temporarily.
Workaround: Wait for the specified period and then re-attempt to reset the password. The default wait period is 20 minutes.
Reference: ZEPHYR-44223
Keywords: Password reset

31. **Problem:** When multiple versions of snapinalarm are installed, the alarm definition of the most recently installed snapinalarm will prevail. When that most recently installed snapinalarm is uninstalled, the alarm definition should revert to the previously installed snapinalarm. Currently that does not happen – the alarm definition of the uninstalled snapinalarm prevails.
Workaround: All versions of snapinalarm must be uninstalled to delete the alarm definition. Then the version of the desired alarm definition can be installed.
Reference: ZEPHYR-44220
Keywords: Alarm definition, snapinalarm

32. **Problem:** On rare occasions the Avaya Breeze™ node can go into a state where all snap-ins fail to load either through the GUI or the Eclipse plugin.

On the System Manager GUI the error message that pops up says:

/opt/Avaya/AUS/snapin-alarms/tmp/CEServices_1.0_0_EPBaseRules_orig.xml]

Workaround: This happens when CEServices_1.0_0_EPBaseRules_orig.xml is missing from the system and the version in /opt/Avaya/AUS/snapin-alarms is of 0 length. Steps for the workaround:

1. Login to System Manager CLI
2. Run
   `cp $AUS_HOME/snapin-alarms/CEServices_1.0_0_EPBaseRules_orig.xml file /home/admin/`
3. Remove the
   `xsi:type="tns:SOMRuleGroupConfigurationType"`
   attribute from the `<tnsa:SPIRITConfiguration>` element from

the `/home/admin/CEServices_1.0_0_EPBaseRules_orig.xml` file.

4. Run the command `sed -e 's/ xsi:type=/ type=/g' CEServices_1.0_0_EPBaseRules_orig.xml > CEServices_1.0_0_EPBaseRules_orig.xml.tmp`
5. Run the command `cp CEServices_1.0_0_EPBaseRules_orig.xml.tmp $AUS_HOME/snapin-alarms/tmp/CEServices_1.0_0_EPBaseRules_orig.xml`
6. Login to the System Manager UI and load the snap-in.

Reference: ZEPHYR-44180

Keywords: Snap-in installation

33. **Problem:** Port numbers for two ports for the same service cannot be swapped. An error message of the following type displays:
'Entered port number value for port A is already in use on cluster X. Entered port number value for port B is already in use on cluster X'

Workaround: If the administrator needs to swap ports with port A=1100 and B=1200, do the following:
1. Update Port 1100 to 1108 (1108 is just a placeholder, make sure 1108 is unused) - then commit.
2. Update Port 1200 to 1100 - then commit.
3. Update Port 1108 to 1200 - then commit.

Reference: ZEPHYR-3988

Keywords: Update Port numbers

34. **Problem:** Applicable only to multi-node clusters. During an upgrade of the platform – TextLog (on the in-service remaining nodes) will overrun because it takes up to 20-30 minutes before the other node is back, and up to 40 minutes before replication is done and the grid is up. This overrun prevents seeing any other issues going on that are logged to the TextLog on the remaining in-service nodes. All information prior to the start of the upgrade on NodeC is wiped out on NodeA and NodeB in a three node cluster, for example.

The below message is printed every five seconds for each service deployed (so it is a multiplier based on the number of services deployed).

[11/11/15 20:48:19:245 EST] 00010225 LookupLocator W net.jini.discovery.LookupLocatorDiscovery$LocatorReg tryGetProxy Failed to connect to LUS on 10.129.145.56:7000, retry in 5001ms
java.net.ConnectException: Connection refused
at java.net.Socket.connect(Socket.java:643)
at com.sun.jini.discovery.internal.MultiIPDiscovery.getSingleResponse(MultiIPDiscovery.java:152)
at com.sun.jini.discovery.internal.MultiIPDiscovery.getResponse(MultiIPDiscovery.java:99)
at net.jini.discovery.LookupLocatorDiscovery$LocatorReg.doUnicastDiscover

y(LookupLocatorDiscovery.java:6
at
net.jini.discovery.LookupLocatorDiscovery$LocatorReg.tryGetProxy(LookupLocatorDiscovery.java:566)
at
net.jini.discovery.LookupLocatorDiscovery.regTryGetProxy(LookupLocatorDiscovery.java:1401)
at
net.jini.discovery.LookupLocatorDiscovery.access$900(LookupLocatorDiscovery.java:301)
at
net.jini.discovery.LookupLocatorDiscovery$DiscoveryTask.tryOnce(LookupLocatorDiscovery.java:830)
at com.sun.jini.thread.RetryTask.run(RetryTask.java:92)
at
com.sun.jini.thread.TaskManager$TaskThread.run(TaskManager.java:408)

Workaround: Execute an additional command on the in-service nodes prior to upgrading the out-of-service nodes as "cust" user:

```
was set trace
*=info:org.openspaces.admin.internal.admin.*=off:net.jini.discovery.*=off:net.jini.lookup.*=off
```

The above command must be completed on each upgraded node, prior to upgrading the remaining nodes to avoid the same log flooding issue.

When all upgrades are completed, execute the following command on the command line of each Avaya Breeze™ node as "cust" user:

```
was set trace *=info
```

Reference: ZEPHYR-36743

Keywords: TextLog

35. **Problem:** This issue is specific to System Manager R 7.0.1. Steps related to the issue:

1.When System Manager 7.0 GA version is installed.
2. Install build x of 7.0.1.
3.Take a snapshot in VMWare.
4. Install build y where y>x of 7.0.1.
5. Revert the snapshot using vmware client.

The /emdata partition does not get reverted.
Therefore the svars that were loaded earlier are still present in the emdata folder maintained by Avaya Breeze™ .

Workaround: Preventive workaround recommended:
1. Power off System Manager.
2. Edit VM settings under the Hardware tab to mark all hard disks as 'non independent' by unchecking the "Independent" box under "Mode".
3. Take snapshots.

This results in reversal for /emdata too. Note: If you have previously taken snapshots of the System Manager VM, delete these prior to making the above changes as the operation is blocked when snapshots are present.

Reference: ZEPHYR-44171

Keywords: Snapshot, SMGR

36. **Problem:** Newly installed certificates are not picked up automatically by the Email Connector.

Workaround:
1. Install the certificates.
2. Uninstall Email Connector.
3. Reinstall Email Connector.

Reference: ZEPHYR-43704

Keywords: Email Connector

37. **Problem:** Service Profiles with a leading '+' in the Service Profile name cannot be edited. An error is encountered when committing it.

Workaround: Do not use '+' in the Service profile name.

Reference: ZEPHYR-42574

Keywords: Service Profile name

38. **Problem:** Alarming intermittently stops working after System Manager Integrated Patch application. The Serviceability profile gets disassociated with element after upgrade:

Workaround:
1. Login to Avaya Breeze™ CLI – "service spiritAgent stop"
2. Login to System Manager CLI – "sh /opt/Avaya/Mgmt/7.0.9/remoteSnmpConfig/utility/recoverAgent.sh < Avaya Breeze™ Management IP address>"
3. Login to Avaya Breeze™ CLI
    a. Reinitialize the System Manager SA – "sh /opt/spirit/scripts/utils/reinitilizeSnmpdConfiguration.sh"
    b. Restart Spirit Agent service – "service spiritAgent restart"

Reference: ZEPHYR-44920, ZEPHYR-24537

Keywords: Upgrade, Alarming

39. **Problem:** You have two services (serviceOne and serviceTwo) using the same ports loaded on System Manager. Attempts to install serviceTwo on the same cluster as serviceOne are not blocked in some circumstances.

Workaround: Wait until the service state is reporting as "Installed" on the Service Management page for ALL services in the targeted cluster. Do not solely rely on the Server Administration nor the Cluster Administration page for service install state. Service Management must also report as "Installed". Port conflicts are correctly detected in this case.

Reference: ZEPHYR-44134

Keywords: Service Ports, Snap-in installation

40. **Problem:** Sometimes under heavy traffic, during one party call and a subsequent play announcement, play completed event does not get triggered causing a hung call.

Workaround: If you are using Engagement Designer, a short delay must be introduced between the time the "collect digit" from the prompt and collect operation completes, and the time the subsequent play operation is started.

If you are writing your own application, the recommended way to achieve the delay is to use a timer to start the play operation after 1 second instead of thread.sleep as it will have significant performance impacts.

Reference: ZEPHYR-40138

Keywords: Playing Announcements

41. **Problem:** NotificationOID is not validated with Orgtype (<p:organization>) within the alarms.xml. This is internal to Avaya snap-ins.

Workaround: While creating snap-in alarms.xml, ensure NotificationOIDs fall in the Orgtype (<p:organization>) hierarchy.

Reference: ZEPHYR-46875

Keywords: Snap-in alarms, Snap-in alarms.xml

42. **Problem:** If snap-in version V1 is loaded without Orgtype (<p:organization>) within the alarms.xml and then another version V2 is loaded with Orgtype (<p:organization>) “6889.1.63” or “6889.2.63” as product id within the alarms.xml then alarm definitions are not updated on System Manager/ Avaya Breeze™ . This is internal to Avaya snap-ins.

Workaround: Do not use product id as “6889.1.63” or “6889.2.63”. It is reserved for Avaya Breeze™ and also used if a snap-in does not provide any Orgtype (<p:organization>).

Reference: ZEPHYR-46874

Keywords: Snap-in alarms, Snap-in alarms.xml

43. **Problem:** On an installed Authorization Client snap-in, addition of grants to the client fails. This happens when the cluster on which the snap-in has been installed, has a name containing braces. System Manager rejects the request thinking the URL contains a cross-site script.

Workaround: Change the cluster name to not include braces in the name.

Reference: ZEPHYR-46929

Keywords: Element Manager, Authorization

44. **Problem:** When a patch is being installed on a system, if the system is not fully idle, requests may come in from services that the VM is not currently capable of handling. This causes javacore logs.

The patch process warns the user that service disruptions may occur if the VM is not idle. These disruptions can include javacore errors.

Workaround: Following the patch installation process should prevent these javacores.

A patch should only be installed on an idle system. There is a warning message to that effect provided to the installer during the patch installation. However, the key aspects when patching to prevent the logs are:

1. Ensure the VM is in Deny New Service.
2. Wait for existing services to complete, so that requests for these will not trigger failures. (This is required for all services, as patching the Avaya Breeze™ typically requires a reboot, and that will delete all data for the service.)
3. When the VM is idle, the patch can be installed. Check the service activity counter on the Cluster Administration dashboard and ensure all pre-existing activity has ceased.

However, the javacore log does not imply the patch did not install correctly. It is only a side-effect that the patch installer completed the patch installation while one or more calls were still active, causing the javacore error.

Reference: ZEPHYR-45011

Keywords: Patching, Patch Installation, Javacore

45. **Problem:** A user Alice calls User Bob, and Bob does an attended transfer to User Carol. When Bob completes the transfer, Carol’s display does not update

from Bob to Alice.

Workaround: There is no workaround.

Reference: ZEPHYR-46891

Keywords: Call transfer

46. **Problem:** If a Zookeeper connection goes down due to a network outage, ActiveMQ master broker node goes down, and master election does not happen in the broker cluster. It can be verified from Reliable Eventing Administration dashboard page on System Manager that when this issues occurs, the master node has no broker status and the other two slave broker nodes stay in the “slave” or “electing” state.

Workaround: When this issue occurs, the broker group cannot serve for event delivery without a master broker node. Steps to recover from this situation:

1. Identify the Avaya Breeze™ node where the broker went wrong:
   a. Run the `statapp -l1` command on the Avaya Breeze™ node to verify the status of activemqd process.
   b. No broker status shown on the Broker Status page on System Manager.
2. Restart the activemqd process by running `restart activemqd` from the command line on the Avaya Breeze™ node.
3. If you cannot identify on which Avaya Breeze™ node the master broker went wrong, run `restart activemqd` on all three broker nodes, one at a time.

Reference: ZEPHYR-47213

Keywords: REF, ActiveMQ, Broker

47. **Problem:** Engagement Designer Service Install Status Fails to Run when Engagement Designer is not able to connect to the cluster database.

Workaround: Uninstall Engagement Designer, wait for it to get fully uninstalled, then install Engagement Designer again.

Reference: ZEPHYR-45053

Keywords: ClusterDB

48. **Problem:** Authorization Samples fail to compile with error: The forked VM terminated without properly saying goodbye. VM crash or System.exit called.

Workaround: Include this snippet in the snap-in war pom.xml under <build><plugins> section

```
<plugin>
    <groupId>org.apache.maven.plugins</groupId>
    <artifactId>maven-surefire-plugin</artifactId>
    <configuration>
        <argLine>-Xms512m -Xmx512m</argLine>
    </configuration>
    </plugin>
```

Reference: ZEPHYR-46421

Keywords: Authorization

49. **Problem:** System enters overload, and does not recover from the overload condition.

Workaround:

1. Log on to the Avaya Breeze™ node as "cust"
2. Remove `/var/avaya/sol via "rm /var/avaya/sol`
3. Run `restart mgmt` to restart the mgmt process.

Reference: ZEPHYR-47295

Keywords: System Overload

50. **Problem:** After an Avaya Breeze™ software upgrade, ActiveMQ broker and Zookeeper do not run. When upgrading one of the Avaya Breeze™ nodes in a cluster that is configured with REF HA, the ActiveMQ broker and Zookeeper may not be able to automatically join back to the broker group after the software upgrade. When the issue occurred, the upgraded node had no broker and Zookeeper status available from the Reliable Eventing Administration dashboard page on System Manager.

Workaround: Reboot the upgraded node again after moving it to Allow New Services mode.

Reference: ZEPHYR-47321

Keywords: REF, ActiveMQ, Broker, Zookeeper, upgrade

51. **Problem:** There is no way to configure the EmailConnector to not use TLS if the email server offers it.

Workaround: Procedure to follow when you upgrade System Manager integrated patch:

Purge all the previous EmailConnectors from System Manager prior to upgrading to the 7.0.1.2 System Manager Integrated patch (with Avaya Breeze™ 3.2.0.1 EM) . There will be a service impact as email will not be available for the entire duration of the upgrade. The emailConnector must be purged prior to applying the integrated patch because the connectors come pre-loaded with the EM. This will guarantee that the changes will be reflected after the upgrade of System Manager is complete.

If you encounter problems with the above procedure –

1. Login to the System Manager command line as admin.
2. scp or ftp /var/avaya/svars/emailConnector-3.2.0.1.320110.svar to your remote fileserver/PC.
3. Delete all the EmailConnector snap-ins (including this one) from System Manager.
4. Reload the 3.2.0.1 EmailConnector snap-in from your fileserver/PC on System Manager.

.

Reference: ZEPHYR-43705

Keywords: Email Connector, Upgrade

52. **Problem:** Due to persisted data repository getting full, ActiveMQ broker blocks the producer from sending new events. When this occurs, the /data file system shows 100% used from df command.

Workaround: The ActiveMQ broker is designed to block the send() call until some messages are consumed and space becomes available on the broker. Here are the steps to recover it:

1. Verify whether the consumer snap-in is still running and receiving events. Restart the consumer snap-in if needed.
2. Purge the destination from the Reliable Eventing Administration Destination Status page on System Manager.
3. If you are unable to clean up disk space using the above steps, remove and re-create the broker group.

Reference: ZEPHYR-47283

Keywords: REF, ActiveMQ, Broker, Zookeeper, Upgrade

53. **Problem:** HTTP Load balancing gets configured but cannot recover from a reboot of the active load balancing Avaya Breeze™ node when the nodes in the cluster have the management address administered as an FQDN.

Workaround: Change the management address from the FQDN to the IP Address. Follow the steps below to change from FQDN to IP based administration or vice versa.

1. Place the cluster in DENY mode.
2. Remove all the nodes from the cluster.
3. On the Server Administration page, select the server, and click Edit. Change the Management Network Interface address from the FQDN to the IP Address. Commit your changes, and repeat for each node in the cluster.
4. Execute initDRS on command line of all the nodes.
5. When command execution is completed successfully followed by replication with System Manager, edit the cluster and reassign nodes.

Reference: ZEPHYR-47742

Keywords: HTTP Load balancing , FQDN

Engagement Call Control (ECC) API-related known issues

54. **Problem:** When A calls B, who is an out of provider resource, events do not mention 'isExternalConnection', which indicates that the call is made to an out of provider resource.

Workaround: getcallInfo response can provide the information about the call being made to out of provider.

Reference: ZEPHYR-4887

Keywords: ECC out of provider resource

55. **Problem:** Single Step Transfer to an unavailable number drops the call from the transferred end and hangs the other connection.

Workaround: Drop Call can be used to end the hung call on the original calling party.

Reference: ZEPHYR-4207

Keywords: Single Step Transfer

56. **Problem:** When Single Step Transfer is performed to an out of provider number :

1. WCC may show transfer failed, but transferee gets the call.
2. The participant list may contain three participants in the answered event when the transferee party answers the call.
3. Transferred event could be missing.

getCall details will not inform the transferee address until the transferee party answers the call.

Workaround: No Workaround.

Reference: ZEPHYR-45056, ZEPHYR-45085

Keywords: Single Step Transfer

57. **Problem:** AgentId is not getting populated in the call events.

Workaround: Ensure the below configuration is in place in Avaya Communication Manager.

1.change system-parameters customer-options:
a.Set 'Computer Telephony Adjunct Links?' to 'Y' in page 4.
b.Set 'ASAI PROPRIETARY FEATURES' to 'Y' in page 10.
2.Save the Communication Manager configuration (save trans).
3.Restart AES . (Proprietary features are negotiated when the transport link comes up for the first time so a restart of AES is needed.)

Reference: ZEPHYR-45862

Keywords: AgentId

58. **Problem:** A Null Pointer Exception occurs when the getConnectionByAddress API is invoked. This happens when stale completed Resource Interaction entries get stuck in UCM space.

Workaround: Restart the cluster.

Reference: ZEPHYR-45032

Keywords: Engagement Call Control

59. **Problem:** Under high CPU usage in the nodes with Common Components installed, CSC PU does not progress.

Workaround: Restart the cluster.

Reference: KHEPRI-339

Keywords: Engagement Call Control

Avaya Breeze™ 3.2.0.1 GA Load Components

Avaya Breeze™ OVA and ISO	Breeze OVA 3.2.0.1.320111 (*Required if upgrading from Collaboration Environment R3.0.x)* Breeze ISO 3.2.0.1.320111 *ISO UPGRADE SUPPORTED ONLY IF COMING FROM R3.1 or later (GA/GA Patch/Service Pack)*
Avaya Breeze™ Avaya Aura Media Server OVA and ISO update	7.7.0.334 OVA with Media Server update 7.7.0.375 and System Layer update 7.7.0.21
SDK	SDK 3.2.0.1.320111
WebRTC	3.2.0.1.320111
Avaya-WebRTC-SDK	3.2.0.1.320111
ECC Avaya Breeze™ SDK	3.2.0.1.320119
Engagement Call Control (ECC)	3.2.0.1.320119
Web Call Controller (WCC)	3.2.0.1.320119
Unified Collaboration Model (UCM)	UCM 3.2.0.1.4933
Call Server Connector (CSC)	CSC 3.2.0.1.41103
UCAStoreService	UCA 3.2.0.1.41551

System Manager interoperability

Avaya Aura System Manager release **7.0.1.2** is supported with the Avaya Breeze™ 3.2.0.1 GA load. The System Manager 7.0.1.2 release can be applied on top of the generally available Avaya Aura System Manager 7.0.0.0 or the generally available Avaya Aura System Manager 7.0.0.1, 7.0.1.0 (including GA service pack releases such as 7.0.1.1 and pre-release 7.0.1.2).

Session Manager interoperability

Avaya Aura Session Manager 6.3.8 and beyond support the Avaya Breeze™ 3.2.0.1 GA load.

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™ can be upgraded at any time after Avaya Aura System Manager and Avaya Aura Media Server (if used) are upgraded.

Avaya Aura Media Server and Avaya Breeze™ should be upgraded together. Avaya Breeze™ 3.2.0.1 is compatible only with Avaya Aura Media Server R7.7.

When upgrading from Avaya Breeze 3.1.1.1 or earlier, follow the below upgrade procedure:

1) From System Manager delete all versions of the emailConnector via the Avaya Breeze™ Service Management page – if using the emailConnector, you will need to uninstall it first then delete it from System Manager. This will be an outage for snap-ins accessing email until the System Manager upgrade has been completed and the new email connector has been installed.
2) Upgrade System Manager to the 7.0.1.2 GA load.
3) Schedule a maintenance window for the Avaya Breeze™ upgrade as this will be service impacting.
4) Place the cluster in DENY .
    a. On System Manager, in Elements, click Avaya Breeze™ > Cluster Administration.
    b. Select the cluster that contains the servers you want to upgrade.
    c. From the Cluster State drop-down menu, select Deny New Service.
    d. Verify that the system displays Denying in the Cluster State column.
5) If using cluster database, make a backup of the cluster database via the Avaya Breeze™ Cluster Administration page. (See *Deploying Avaya Breeze*, chapter 6.)
6) Edit the cluster and remove all Avaya Breeze™ nodes from the cluster – this will require disabling Load Balancing if applicable. To disable Load Balancing, while editing the cluster, go to the General tab, and uncheck the “Is Load Balancer enable?” field.
7) Verify all services have been undeployed for each Avaya Breeze™ node by logging in via the command line and executing **deploy_service –l**. When the query comes back empty, all services have been uninstalled.
8) Upgrade all the Avaya Breeze™ nodes simultaneously to 3.2.0.1 via the ISO binary using **upgradeCE**.
    a. Verify that you have copied the ISO upgrade file to the server that you are upgrading.
    b. Log on to the Avaya Breeze™ server.
    c. Enter the command **upgradeCE *<full_path/iso_filename>*** .
    d. Step through prompts until the upgrade is installed.
9) During the upgrade, you can optionally edit the cluster and choose to upgrade your mandatory services and any other snap-ins to the latest versions available. This action is allowed on an empty cluster and can save time if the newer versions of these snap-ins are desired. NOTE: If you are using the cluster database and want to restore your database, remove the snap-ins that are using the cluster database that you will be restoring. This will be a preresquite for the restore operation.
10) After the ugprades have completed, the nodes are replicating with the System Manager, and tests are passing on the server administration page, edit the cluster and place all Avaya Breeze™ nodes back into the cluster and commit. Remember to re-enable load-balancing if previous used.
11) At this time, the new services (if applicable) will also be installed from step (9).
12) If restoring the cluster database, do so at this time, then post restore, reinstall the service utilizing that database. (See *Deploying Avaya Breeze*, chapter 6.)
13) After all services have been installed and the cluster dashboard reports all healthy (green checks across the board) place the cluster in accept new service.

When upgrading from Avaya Breeze 3.2, follow this upgrade procedure. For additional information about any of these steps, see the ISO upgrade procedure in *Upgrading Avaya Engagement Development Platform Release 3.1*.

1. Before upgrading Avaya Breeze™, upgrade the following in this order to the required release:
   System Manager
   Session Manager
2. Upgrade Avaya Aura® Media Server.
3. On the Cluster Administration page, identify the cluster you want to upgrade. For clusters with multiple servers, determine the sequence in which you want to upgrade the servers.
   NOTE: If using the cluster database, upgrade idle nodes first, and then upgrade the standby. After the upgrade of the standby, request a manual failover to move the active to the upgraded standby server. Then upgrade the new standby Avaya Breeze™ server.
4. Download the ISO file from PLDS. Copy the ISO file to each Avaya Breeze™ server you will be upgrading.
5. Verify that the **Enrollment Password** is not expired.
6. Change the state of the server you are upgrading to **Deny New Service**.
7. Verify that the server **Activity** field is zero.
8. Upgrade the Avaya Breeze™ software. To do this, enter the command **upgradeCE<*iso filename*>**.
9. Verify data replication between System Manager and Avaya Breeze™.
10. Run Avaya Breeze™ maintenance tests for the server.
11. On the **Server Administration** page verify the following for the upgraded server:
    - The **Service Install Status** is a green checkmark
    - The **Security Module** is Up
    - The **License mode** is a green checkmark
    - The **Version** displays release 3.2.0.1
12. Change the state to **Accept New Service** for the upgraded Avaya Breeze™ server.
13. Verify the Avaya Breeze™ SIP Entity Link with Session Manager.
14. Repeat this procedure for each server you are upgrading.
15. Upgrade all mandatory services.

Avaya Breeze™ VM Profile & ECC Snap-ins Deployment Type

It is no longer required to use Manual Deployment Type & Configuring Deployment. Now SMALL, MEDIUM or LARGE Deployment Types can be selected.

Avaya Breeze™ Profile	**UCA**	**UCM**	**CSC**	**Notes**
Profile 2-4/8, Profile 3-6/10	SMALL	SMALL	SMALL	2 cps, max 15K extensions Single node - max 2 CMs Multi node - max 3 CMs
Profile 4-8/16	MEDIUM	MEDIUM	MEDIUM	15 cps, max 30K extensions and max 3 CMs, min 2 nodes needed
Profile 4-8/16	LARGE	LARGE	LARGE	24 cps, max 41K extensions and max 3 CMs, min 2 nodes needed

ECC notes

Features added/updated:

- A new REST API sendDigits has been added to enable the user to send digits from an active participant on an ongoing call.
- An additional optional field, “consultOption” has been added to the consult call REST API for the user to specify how the consultation call would end either by transfer/conference when the consultation call is initiated.

- ECC supports sending agentId in the call events if an agent is logged in to the station.

Note: Refer to the ECC SDK REST API document for more details about the API changes. (Refer to Avaya Breeze™ 3.2.0.1 GA Load Components table above for the latest ECC SDK.)

Communication Manager configuration needed for Agent details to get populated in ECC Events:

1. change system-parameters customer-options
    a. Set 'Computer Telephony Adjunct Links?' to 'Y' in page 4.
    b. Set 'ASAI PROPRIETARY FEATURES' to 'Y' in page 10.
2. Save the Communication Manager configuration (save trans).
3. Restart AES. (Proprietary features are negotiated when the transport link comes up for the first time so a restart of AES is needed.)

Supported Subscription Rate:

The above table explains the supported call rate, but it does not mention the supported subscription request rate that ECC can handle. ECC supports 24 subscription requests per second in a LARGE deployment and 10 subscription requests per second in a SMALL/MEDIUM deployment.

Steps to Load, Configure and Install UCAStoreService

The UCA snap-in has been renamed from UCAService to UCAStoreService.

Some of the acceptable attribute values have changed. Follow the steps below to configure the new snap-in with a valid configuration:

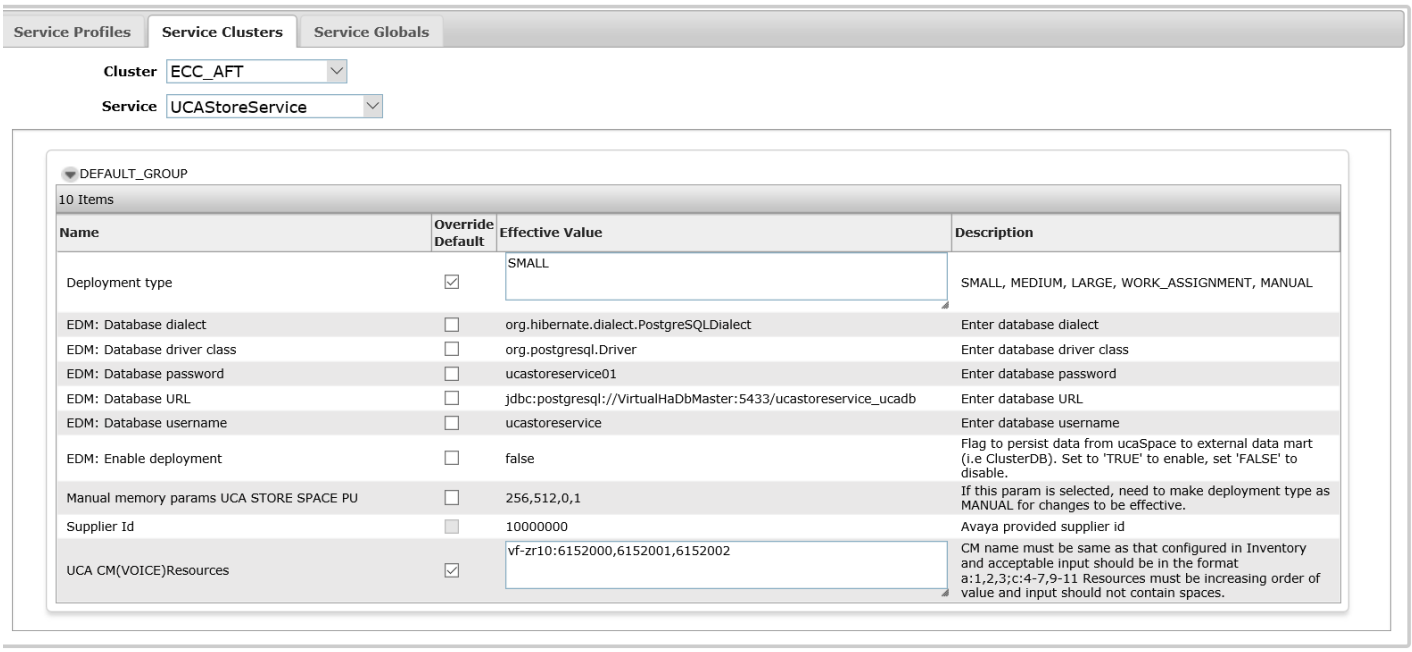
1. Ensure that “Enable Cluster Database” is checked on the cluster.

From Cluster Administration, select the cluster on which the UCAStoreService is to be installed. Click Edit. Check the “Enable Cluster Database” field.

UCAStoreService cannot be installed without the Cluster Database enabled.

2. From Service Management - Load UCAStoreService.
3. Install the snap-in.
4. From Configuration > Attributes > Service Cluster, select the cluster and the UCAStoreService from the dropdown menu.
5. Deployment type for UCA Space - Check Override Default, and set Effective Value to: SMALL/MEDIUM/LARGE using the above table based on the call rate required and the Avaya Breeze™ profile
6. Ensure EDM: Enable Deployment is set to false (the default value) for ECC-only deployment.
7. Manual memory params UCA SPACE PU - are required only if the deployment type is set to MANUAL - not required for ECC
8. Set the UCA attribute, “UCA CM(VOICE)Resources” as follows.
   A provider group always consists of an ID followed by a colon and a list of resource ranges.
   a) Provider groups are separated by semi-colons.The range must be a number and may either be a single number (effectively denoting a range of one) or may be two numbers separated by a dash. Multiple ranges may be declared per provider, separated by commas. Ranges must be in ascending order and may not overlap.
   No spaces in the string are allowed.
   Examples:
   i. a:1,2,3;b;c:4-7,9-11
   ii. CM9:70002-73590;CM7:50003-51205,52001,52002;DVITCM174:31000-31007,31101,31102,31106,31211-31217,31225-31227
   b) The value ALL is not supported for CM Filter List.
   c) Comma separated provider list is no longer supported.
9. Commit
10. Click OK on the confirmation dialog displayed.

Example for Single Node for Avaya Breeze™ VM profile 2:



Steps to upgrade ECC solution - From 3.2.0.0 GA/GA Patch to 3.2.0.1 GA Service Pack

Use the following procedure to upgrade Avaya Breeze™ nodes in the cluster:

1. Screen shot/save all administered attributes for ECC solution (ECC, CSC, UCA, UCM).
2. Place the cluster in Deny New Service.
3. Remove all nodes from the cluster.
4. Verify all services have been uninstalled by executeing "`deploy_service -l`" from the command line on each Avaya Breeze™ node. The command should return empty when all services have successfully been undeployed.
5. Upgrade all Avaya Breeze™ nodes simultaneously outside of the cluster.
6. While the upgrade of the Avaya Breeze™ nodes is underway, edit the empty ECC cluster from the Cluster Administration page and remove older versions of eventing connector, CECS and ECC snap-ins from the list of services on the cluster. Install new versions of eventing connector, CECS and ECC snap-ins at the same time, using the Cluster Editor.
7. After all Avaya Breeze™ nodes are upgraded and are verified to be up and replicating with System Manager, edit the cluster and place all nodes back into the cluster simultaneously.
8. Allow time for all snap-ins to install. Verify the services have been successfully installed on all nodes via the Server Administration page.
9. Configure attributes of ECC solution snap-ins as per described above.
   Note that there is a change in UCA attributes and some of the older snap-in attribute configuration is not supported with the new snap-in.
10. Load and install the new WCC version. Configure snap-in attributes.
11. Reboot the Avaya Breeze™ cluster (reboot nodes in cluster simultaneously).

ECC and Avaya Breeze™ Platform Versions compatibility Matrix:

ECC Version	Breeze Platform Version
3.2	3.2 and Later
3.2.0.1	3.2.0.1 and Later

Troubleshooting Note: PSTN trunks not sending delivered event.

If the external PSTN trunk configured with Avaya Communication Manager for external calls does not support sending delivered event and if a call is made from a number A (inside the organization) to an outside number B via the PSTN trunk then:

1. ECC call events ALERTING of B cannot be sent, and when B answers the call directly, ACTIVE event of A and B will be sent to A's event listener.
2. A's connection will be in UNKNOWN state until B answers.

Disk Alarm notes

The System Overload Monitor has been enhanced to monitor the status of disks on an Avaya Breeze™ 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 reach 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.

Cluster Database notes

If the use of the cluster database is required on an Avaya Breeze™ 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 8GB or higher.

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™ 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 Chapter 9, High Availability Administration, in *Deploying Avaya Breeze™* 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™ 3.1 this distinction has been refined so that media operations invoked on the called party will be 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.

Real-Time Speech (RTS) Snap-in notes

When using Real-Time Speech with Avaya Breeze™ 3.1.1.0 or later, you must use Real-Time Speech (RTS) 3.1 or later. If the previous version of the Real-Time Speech (RTS) snap-in is used in an Avaya Breeze™ instance, contact Avaya for the updated Real-Time Speech (RTS) snap-in before upgrading to Avaya Breeze™ 3.2.0.0 or later.

Flow control

It is important to avoid traffic congestion for a service that sends a burst of voice announcement requests through Avaya Breeze™. 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™ instance. Empirical testing has shown that a reliable minimum delay for 10,000 requests using one Avaya Breeze™ 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™ is maximum rated at 1100 ports. A single Avaya Aura Media Server would be expected to service 1,000 announcements over a period of 5 minutes and therefore 2,000 announcements would be serviced over 10 minutes. Given this guideline, 5 Avaya Aura Media Server instances will be required at a traffic level of 10,000 voice announcement requests serviced over a 10 minute period of time. 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 a Avaya Breeze™ 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™ 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™ 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™ 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 a 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 occur for other media operations. This new behavior better matches the behavior that occurs when a call ends.