Avaya Breeze® platform FAQ and Troubleshooting for Snap-in Developers

Release 3.9
Issue 1
January 2024

© 2024, Avaya LLC. All Rights Reserved

AVAYA SOFTWARE DEVELOPMENT KIT LICENSE AGREEMENT

REVISED: January 14, 2022

READ THIS CAREFULLY BEFORE ELECTRONICALLY ACCESSING OR USING THIS PROPRIETARY PRODUCT!

THIS IS A LEGAL AGREEMENT ("AGREEMENT") BETWEEN YOU, INDIVIDUALLY, AND/OR THE LEGAL ENTITY FOR WHOM YOU ARE OPENING, INSTALLING, DOWNLOADING, COPYING OR OTHERWISE USING THE AVAYA SOFTWARE DEVELOPMENT KIT ("SDK") (COLLECTIVELY, AS REFERENCED HEREIN, "YOU", "YOUR", OR "LICENSEE") AND AVAYA INC. OR ANY AVAYA AFFILIATE (COLLECTIVELY, "AVAYA"). IF YOU ARE ACCEPTING THE TERMS AND CONDITIONS OF THIS AGREEMENT ON BEHALF OF A LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL LEGAL AUTHORITY TO ACCEPT ON BEHALF OF AND BIND SUCH LEGAL ENTITY TO THIS AGREEMENT. BY OPENING THE MEDIA CONTAINER, BY INSTALLING, DOWNLOADING, COPYING OR OTHERWISE USING THE AVAYA SOFTWARE DEVELOPMENT KIT ("SDK") OR AUTHORIZING OTHERS TO DO SO, YOU SIGNIFY THAT YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT HAVE SUCH AUTHORITY OR DO NOT WISH TO BE BOUND BY THE TERMS OF THIS AGREEMENT, SELECT THE "DECLINE" BUTTON AT THE END OF THE TERMS OF THIS AGREEMENT OR THE EQUIVALENT OPTION AND YOU SHALL HAVE NO RIGHT TO USE THE SDK.

1.0 DEFINITIONS.

1.1 "Affiliates" means any entity that is directly or indirectly controlling, controlled by, or under common control with Avaya Inc. For purposes of this definition, "control" means the power to direct the management and policies of such party, directly or indirectly, whether through ownership of voting securities, by contract or otherwise; and the terms "controlling" and "controlled" have meanings correlative to the foregoing.

1.2 "Avaya Software Development Kit" or "SDK" means Avaya technology, which may include Software, Client Libraries, Specification Documents, Software libraries, application programming interfaces ("API"), Software tools, Sample Application Code and Documentation.

1.3 "Client Libraries" mean any enabler code specifically designated as such and included in a SDK. Client Libraries may also be referred to as "DLLs", and represent elements of the SDK required at runtime to communicate with Avaya products or other SDK elements.

1.4 "Change In Control" shall be deemed to have occurred if any person, entity or group comes to own or control, directly or indirectly, beneficially or of record, voting securities (or any other form of controlling interest) which represent more than fifty percent (50%) of the total voting power of the Licensee.

1.5 "Derivative Work(s)" means any translation (including translation into other computer languages), port, compiling of Source Code into object code, combination with a pre-existing work, modification, correction, addition, extension, upgrade, improvement, compilation, abridgment or other form in which an existing work may be recast, transformed or adapted or which would otherwise constitute a derivative work under the United States Copyright Act. Permitted Modifications will be considered Derivative Works.

1.6 "Documentation" includes programmer guides, CDs, manuals, materials, and information appropriate or necessary for use in connection with the SDK. Documentation may be provided in machine-readable, electronic or hard copy form.

1.7 "Intellectual Property" means any and all: (i) rights associated with works of authorship throughout the world, including copyrights, neighboring rights, moral rights, and mask works, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, algorithms, designs and other industrial property rights, (v) all other intellectual and industrial

property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

1.8 "Permitted Modification(s)" means Licensee's modifications of the Sample Application Code as needed to create applications, interfaces, workflows or processes for use with Avaya products.

1.9 "Specification Document" means any notes or similar instructions in hard copy or machine readable form, including any technical, interface and/or interoperability specifications that define the requirements and conditions for connection to and/or interoperability with Avaya products, systems and solutions.

1.10 "Source Code" means human readable or high-level statement version of software written in the source language used by programmers and includes one or more programs. Source Code programs may include one or more files, such as user interface markup language (.mxml), action script (.as), precompiled Flash code (.swc), java script (.js), hypertext markup language (.html), active server pages (.asp), C# or C# .Net source code (.cs), java source code (.java), java server pages (.jsp), java archives (.jar), graphic interchange format (.gif), cascading style sheet (.css), audio files (.wav) and extensible markup language (.xml) files.

1.11 "Sample Application Code" means Software provided for the purposes of demonstrating functionality of an Avaya product through the Avaya Software Development Kit.

1.12 "Software" means data or information constituting one or more computer or apparatus programs, including Source Code or in machine-readable, compiled object code form.

2.0 LICENSE GRANT.

2.1 SDK License.

A. Provided Licensee pays to Avaya the applicable license fee (if any), Avaya hereby grants Licensee a limited, non-exclusive, non-transferable license (without the right to sublicense, except as set forth in 2.1B(iii)) under the Intellectual Property of Avaya and, if applicable, its licensors and suppliers to (i) use the SDK solely for the purpose of Licensee's internal development efforts to develop applications, interfaces, value-added services and/or solutions, workflows or processes to work in conjunction with Avaya products; (ii) to package Client Libraries for redistribution with Licensee's complementary applications that have been developed using this SDK, subject to the terms and conditions set forth herein; (iii) use Specification Documents solely to enable Licensee's products, services and application solutions to exchange messages and signals with Avaya products, systems and solutions to which the Specification Document(s) apply; (iv) modify and create Derivative Works of the Sample Application Code, Specification Documents and Documentation solely for internal development of applications, interfaces, workflows or processes for use with Avaya products, integration of such applications, interfaces, workflows and processes with Avaya products and interoperability testing of the foregoing with Avaya products; and (v) compile or otherwise prepare for distribution the Sample Application Code with Permitted Modifications, into an object code or other machine-readable program format for distribution and distribute the same subject to the conditions set forth in Section 2.1B.

B. The foregoing license to use Sample Application Code is contingent upon the following: (i) Licensee must ensure that the modifications made to the Sample Application Code as permitted in clause (iv) of Section 2.1A are compatible and/or interoperable with Avaya products and/or integrated therewith, (ii) Licensee may distribute Licensee's application that has been created using this SDK, provided that such distribution is subject to an end user pursuant to Licensee's current end user license agreement ("Licensee EULA") that is consistent with the terms of this Agreement and, if applicable, any other agreement with Avaya (e.g., the Avaya DevConnect Program Agreement), and is equally as protective as Licensee's standard software license terms, but in no event shall the standard of care be less than a reasonable degree of care, and (iii) Licensee ensures that each end user who receives Client Libraries or Sample Application Code with Permitted Modifications has all necessary licenses for all underlying Avaya products associated with such Client Libraries or Sample Application Code.

Your Licensee EULA must include terms concerning restrictions on use, protection of proprietary rights, disclaimer of warranties, and limitations of liability. You must ensure that Your End Users using

applications, interfaces, value-added services and/or solutions, workflows or processes that incorporate the API, Client Libraries, Sample Code or Permitted Modifications adhere to these terms, and You agree to notify Avaya promptly if You become aware of any breach of the terms of Licensee EULA that may impact Avaya. You will take all reasonable precautions to prevent unauthorized access to or use of the SDK and notify Avaya promptly of any such unauthorized access or use.

C. Licensee acknowledges and agrees that it is licensed to use the SDK only in connection with Avaya products (and if applicable, in connection with services provided by or on behalf of Avaya).

D. With respect to Software that contains elements provided by third party suppliers, Licensee may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "click-through" licenses, accompanying or applicable to the Software.

2.2 No Standalone Product. Nothing in this Agreement authorizes or grants Licensee any rights to distribute or otherwise make available to a third party the SDK, in whole or in part, or any Derivative Work in source or object code format on a standalone basis other than the modifications permitted in Section 2.1B of this Agreement.

2.3 Proprietary Notices. Licensee shall not remove any copyright, trade mark or other proprietary notices incorporated in the copies of the SDK, Sample Application Code and redistributable files in Licensee's possession or control or any modifications thereto. Redistributions in binary form or other suitable program format for distribution, to the extent expressly permitted, must also reproduce Avaya's copyright, trademarks or other proprietary notices as incorporated in the SDK in any associated Documentation or "splash screens" that display Licensee copyright notices.

2.4 Third-Party Components. You acknowledge certain software programs or portions thereof included in the SDK may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the SDK ("Third Party Terms"). Information identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the attached Schedule 1 (if any), SDK, Documentation, or on Avaya's web site at: http://support.avaya.com/Copyright (or such successor site as designated by Avaya). The open source software license terms provided as Third Party Terms are consistent with the license rights granted in this Agreement, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over this Agreement, solely with respect to the applicable Third Party Components, to the extent that this Agreement imposes greater restrictions on You than the applicable Third Party Terms. Licensee is solely responsible for procuring any necessary licenses for Third Party Components, including payment of licensing royalties or other amounts to third parties, for the use thereof.

2.5 Copies of SDK. Licensee may copy the SDK only as necessary to exercise its rights hereunder.

2.6a No Reverse Engineering. Licensee shall have no rights to any Source Code for any of the software in the SDK, except for the explicit rights to use the Source Code as provided to Licensee hereunder. Licensee agrees that it shall not cause or permit the disassembly, decompilation or reverse engineering of the Software. Notwithstanding the foregoing, if the SDK is rightfully located in a member state of the European Union and Licensee needs information about the Software in the SDK in order to achieve interoperability of an independently created software program with the Software in the SDK, Licensee will first request such information from Avaya. Avaya may charge Licensee a reasonable fee for the provision of such information. If Avaya refuses to make such information available, then Licensee may take steps, such as reverse assembly or reverse compilation, to the extent necessary solely in order to achieve interoperability of the Software in the SDK with an independently created software program. To the extent that the Licensee is expressly permitted by applicable mandatory law to undertake any of the activities listed in this section, Licensee will not exercise those rights until Licensee has given Avaya twenty (20) days written notice of its intent to exercise any such rights.

2.6.b License Restrictions. To the extent permissible under applicable law, Licensee agrees not to: (i) publish, sell, sublicense, lease, rent, loan, assign, convey or otherwise transfer the SDK; (ii) distribute, disclose or allow use the SDK, in any format, through any timesharing service, service bureau, network or by any other means; (iii) distribute or otherwise use the Software in the SDK in any manner that causes any portion of the Software that is not already subject to an OSS License to become subject to the terms of any OSS License; (iv) link the Source Code for any of the software in the SDK with any software licensed under the Affero General Public License (Affero GPL) v.3 or similar licenses; (v) access information that is solely available to root administrators of the Avaya products, systems, and solutions; (vi) develop applications, interfaces, value-added services and/or solutions, workflows or processes that causes adverse effects to Avaya and third-party products,

services, solutions, such as, but not limited to, poor performance, software crashes and cessation of their proper functions; and (vii) develop applications, interfaces, value-added services and/or solutions, workflows or processes that blocks or delays emergency calls; (viii) emulate an Avaya SIP endpoint by form or user interface design confusingly similar as an Avaya product ; (ix) reverse engineer Avaya SIP protocol messages; or (x) permit or encourage any third party to do any of (i) through (x), inclusive, above.

2.7 Responsibility for Development Tools. Licensee acknowledges that effective utilization of the SDK may require the use of a development tool, compiler and other software and technology of third parties, which may be incorporated in the SDK pursuant to Section 2.4. Licensee is solely responsible for procuring such third party software and technology and the necessary licenses, including payment of licensing royalties or other amounts to third parties, for the use thereof.

2.8 U.S. Government End Users. The SDK shall be classified as "commercial computer software" and the Documentation is classified as "commercial computer software documentation" or "commercial items," pursuant to FAR 12.212 or DFAR 227.7202, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the SDK or Documentation by the Government of the United States shall be governed solely by the terms of the Agreement and shall be prohibited except to the extent expressly permitted by the terms of the Agreement.

2.9 Limitation of Rights. No right is granted to Licensee to sublicense its rights hereunder. All rights not expressly granted are reserved by Avaya or its licensors or suppliers and, except as expressly set forth herein, no license is granted by Avaya or its licensors or suppliers under this Agreement directly, by implication, estoppel or otherwise, under any Intellectual Property right of Avaya or its licensors or suppliers. Nothing herein shall be deemed to authorize Licensee to use Avaya's trademarks or trade names in Licensee's advertising, marketing, promotional, sales or related materials.

2.10 Independent Development.

2.10.1 Licensee understands and agrees that Avaya, Affiliates, or Avaya's licensees or suppliers may acquire, license, develop for itself or have others develop for it, and market and/or distribute applications, interfaces, value-added services and/or solutions, workflows or processes similar to that which Licensee may develop. Nothing in this Agreement shall restrict or limit the rights of Avaya, Affiliates, or Avaya's licensees or suppliers to commence or continue with the development or distribution of such applications, interfaces, value-added services and/or solutions, workflows or processes.

2.10.2 Nonassertion by Licensee. Licensee agrees not to assert any Intellectual Property related to the SDK or applications, interfaces, value-added services and/or solutions, workflows or processes developed using the SDK against Avaya, Affiliates, Avaya's licensors or suppliers, distributors, customers, or other licensees of the SDK.

2.11 Feedback and Support. Licensee agrees to provide any information, comments, problem reports, enhancement requests and suggestions regarding the performance of the SDK (collectively, "Feedback") via any public or private support mechanism, forum or process otherwise indicated by Avaya. Avaya monitors applicable mechanisms, forums, or processes but is under no obligation to implement any of Feedback, or be required to respond to any questions asked via the applicable mechanism, forum, or process. Licensee hereby assigns to Avaya all right, title, and interest in and to Feedback provided to Avaya.

2.12(a) Fees and Taxes. To the extent that fees are associated with the license of the SDK, Licensee agrees to pay to Avaya or pay directly to the applicable government or taxing authority, if requested by Avaya, all taxes and charges, including without limitation, penalties and interest, which may be imposed by any federal, state or local governmental or taxing authority arising hereunder excluding, however, all taxes computed upon Avaya's net income. If You move any Software, including the SDK, and as a result of such move, a jurisdiction imposes a duty, tax, levy or fee (including withholding taxes, fees, customs or other duties for the import and export of any such Software), then You are solely liable for, and agree to pay, any such duty, taxes, levy or other fees.

2.12(b) Audit. Avaya shall have the right, at its cost and expense, to inspect and/or audit (i) by remote polling or other reasonable electronic means at any time and (ii) in person during normal business hours and with reasonable notice Licensee's books, records, and accounts, to determine Licensee's compliance with this Agreement. In the event such inspection or audit uncovers non-compliance with this Agreement, then without prejudice to Avaya's termination rights hereunder, Licensee shall promptly pay Avaya any applicable license fees. Licensee agrees to keep a current record of the location of the SDK.

2.13 No Endorsement. Neither the name Avaya, Affiliates nor the names of contributors may be used to endorse or promote products derived from the Avaya SDK without specific prior written permission from Avaya.

2.14 High Risk Activities. The Avaya SDK is not fault-tolerant, and is not designed, manufactured or intended for use or resale as on-line control equipment or in hazardous environments requiring failsafe performance, such as in the operation of nuclear facilities, aircraft navigation or aircraft communications systems, mass transit, air traffic control, medical or direct life support machines, dedicated emergency call handling systems or weapons systems, in which the failure of the Avaya SDK could lead directly to death, personal injury, or severe physical or environmental damage ("high risk activities"). If Licensee uses the Avaya SDK for high risk activities, Licensee does so at Licensee's own risk and Licensee assumes all responsibility and liability for such use to the maximum extent such limitation or exclusion is permitted by applicable law. Licensee agrees that Avaya and its suppliers will not be liable for any claims or damages arising from or related to use of the Avaya SDK for high risk activities to the maximum extent such limitation or exclusion is permitted by law.

2.15 No Virus. Licensee warrants that (i) the applications, interfaces, value-added services and/or solutions, workflows or processes Licensee develops using this SDK will not contain any computer program file that includes time code limitations, disabling devices, or any other mechanism which will prevent the Avaya product (including other software, firmware, hardware), services and networks from being functional at all times (collectively "Time Bombs"); and (ii) the applications, interfaces, value-added services and/or solutions, workflows or processes Licensee develops using this SDK will be free of computer viruses, malicious or other harmful code, black boxes, malware, trapdoors, and other mechanisms which could: a) damage, destroy or adversely affect Avaya product, or services and/or end users; b) allow remote/hidden attacks or access through unauthorized computerized command and control; c) spy (network sniffers, keyloggers), and d) damage or erase such applications, interfaces, value-added services and/or solutions, workflows or processes developed using this SDK or data, or any computer files or systems of Avaya, Affiliates, and/or end users (collectively "Virus"). In addition to any other remedies permitted in the Agreement, if Licensee breaches its warranties under this Section, Licensee will, at its expense, take remedial action to eliminate any Time Bombs and/or Viruses and prevent re-occurrence (including implementing appropriate processes to prevent further occurrences) as well as provide prompt, reasonable assistance to Avaya to materially reduce the effects of the Time Bomb and/or Virus.

2.16 Disclaimer. Any software security feature is not a guaranty against malicious code, deleterious routines, and other techniques and tools employed by computer "hackers" and other third parties to create security exposures. Compromised passwords represent a major security risk. Avaya encourages You to create strong passwords using three different character types, change Your password regularly and refrain from using the same password regularly. You must treat such information as confidential. You agree to notify Avaya immediately upon becoming aware of any unauthorized use or breach of Your user name, password, account, API Key, or other credentials as provided by Avaya for use of the SDK, or subscription. You are responsible for ensuring that Your networks and systems are adequately secured against unauthorized intrusion or attack and regularly back up of Your data and files in accordance with good computing practices.

2.17 Third Party Licensed Software

A. "Commercial Third Party Licensed Software" is software developed by a business with the purpose of making money from the use of that licensed software. "Freeware Licensed Software" is software which is made available for use, free of charge and for an unlimited time, but is not Open Source Licensed Software. "Open Source Software" or "OSS" is as defined by the Open Source Initiative ("OSI") https://opensource.org/osd and is software licensed under an OSI approved license as set forth at https://opensource.org/licenses/alphabetical (or such successor site as designated by OSI). These are collectively referred to herein as "Third Party Licensed Software".

B. Licensee represents and warrants that Licensee, including any employee, contractor, subcontractor, or consultant engaged by Licensee, is to the Licensee's knowledge, in compliance and will continue to comply with all license obligations for Third Party Licensed Software used in the Licensee application created using the SDK including providing to end users all information required by such licenses as may be necessary. LICENSEE REPRESENTS AND WARRANTS THAT, TO THE LICENSEE'S KNOWLEDGE, THE OPEN SOURCE LICENSED SOFTWARE EMBEDDED IN OR PROVIDED WITH LICENSEE APPLICATION OR SERVICES DOES NOT INCLUDE ANY OPEN SOURCE LICENSED SOFTWARE CONTAINING TERMS REQUIRING ANY INTELLECTUAL PROPERTY OWNED OR LICENSED BY AVAYA OR END USERS TO

BE (A) DISCLOSED OR DISTRIBUTED IN SOURCE CODE OR OBJECT CODE FORM; (B) LICENSED FOR THE PURPOSE OF MAKING DERIVATIVE WORKS; OR (C) REDISTRIBUTABLE ON TERMS AND CONDITION NOT AGREED UPON BY AVAYA OR END USERS.

C. Subject to any confidentiality obligations, trade secret or other rights or claims of Licensee suppliers, Licensee will respond to requests from Avaya or end users relating to Third Party Licensed Software associated with Licensee's use of Third Party Licensed Software. Licensee will cooperate in good faith by furnishing the relevant information to Avaya or end users and the requester within two (2) weeks from the time Avaya or end user provided the request to Licensee.

3. OWNERSHIP.

3.1 As between Avaya and Licensee, Avaya or its licensors or suppliers shall own and retain all Intellectual Property rights, in and to the SDK and any corrections, bug fixes, enhancements, updates, improvements, or modifications thereto and Licensee hereby irrevocably transfers, conveys and assigns to Avaya, its licensors and its suppliers all of its right, title, and interest therein. Avaya or its licensors or suppliers shall have the exclusive right to apply for or register any patents, mask work rights, copyrights, and such other proprietary protections with respect thereto. Licensee acknowledges that the license granted under this Agreement does not provide Licensee with title or ownership to the SDK, but only a right of limited use under the terms and conditions of this Agreement.

3.2 Grant Back License to Avaya. Licensee hereby grants to Avaya an irrevocable, perpetual, non-exclusive, sublicensable, royalty-free, fully paid up, worldwide license under any and all of Licensee's Intellectual Property rights related to any Permitted Modifications, to (i) use, make, sell, execute, adapt, translate, reproduce, display, perform, prepare derivative works based upon, distribute (internally and externally) and sublicense the Permitted Modifications and their derivative works, and (ii) sublicense others to do any, some, or all of the foregoing.

4.0 SUPPORT.

4.1 No Avaya Support. Avaya will not provide any support for the SDK provided under this Agreement or for any Derivative Works, including, without limitation, modifications to the Source Code or applications built by Licensee using the SDK. Avaya shall have no obligation to provide support for the use of the SDK, or Licensee's application, services or solutions which may or may not include redistributable Client Libraries or Sample Application Code, to any third party to whom Licensee delivers such applications, services or solutions. Avaya further will not provide fixes, patches or repairs for any defects that might exist in the SDK or the Sample Application Code provided under this Agreement. In the event that Licensee desires support services for the SDK, and, provided that Avaya offers such support services (in its sole discretion), Licensee will be required to enter into an Avaya DevConnect Program Agreement or other support agreement with Avaya.

4.2 Licensee Obligations. Licensee acknowledges and agrees that it is solely responsible for developing and supporting any applications, interfaces, value-added services and/or solutions, workflows or processes developed under this Agreement, including but not limited to (i) developing, testing and deploying such applications, interfaces, value-added services and/or solutions, workflows or processes; (ii) configuring such applications, interfaces, value-added services and/or solutions, workflows or processes to interface and communicate properly with Avaya products; and (iii) updating and maintaining such applications, interfaces, value-added services and/or solutions, workflows or processes as necessary for continued use with the same or different versions of end user and/or third party licensor products, and Avaya products.

5.0 CONFIDENTIALITY.

5.1 Protection of Confidential Information. Licensee acknowledges and agrees that the SDK and any other Avaya technical information obtained by it under this Agreement (collectively, "Confidential Information") is confidential information of Avaya. Licensee shall take all reasonable measures to maintain the confidentiality of the Confidential Information. Licensee further agrees at all times to protect and preserve the SDK in strict confidence in perpetuity, and shall not use such Confidential Information other than as expressly authorized by Avaya under this Agreement, nor shall Licensee disclose any Confidential Information to third parties without Avaya's written consent. Licensee further agrees to immediately 1) cease all use of all

Confidential Information (including copies thereof) in Licensee's possession, custody, or control; 2) stop reproducing or distributing the Confidential Information; and 3) destroy the Confidential Information in Licensee's possession or under its control, including Confidential Information on its computers, disks, and other digital storage devices upon termination of this Agreement at any time and for any reason. Upon request, Licensee will certify in writing its compliance with this Section. The obligations of confidentiality shall not apply to information which (a) has entered the public domain except where such entry is the result of Licensee's breach of this Agreement; (b) prior to disclosure hereunder was already rightfully in Licensee's possession; (c) subsequent to disclosure hereunder is obtained by Licensee on a non-confidential basis from a third party who has the right to disclose such information to the Licensee; (d) is required to be disclosed pursuant to a court order, so long as Avaya is given adequate notice and the ability to challenge such required disclosure.

5.2 Press Releases. Any press release or publication regarding this Agreement is subject to prior written approval of Avaya.

6.0 NO WARRANTY.

The SDK and Documentation are provided "AS-IS" without any warranty whatsoever. AVAYA SPECIFICALLY AND EXPRESSLY DISCLAIMS ANY WARRANTIES OR CONDITIONS, STATUTORY OR OTHERWISE, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT AND SATISFACTORY QUALITY. AVAYA DOES NOT WARRANT THAT THE SDK AND DOCUMENTATION ARE SUITABLE FOR LICENSEE'S USE, THAT THE SDK OR DOCUMENTATION ARE WITHOUT DEFECT OR ERROR, THAT OPERATION WILL BE UNINTERRUPTED, OR THAT DEFECTS WILL BE CORRECTED. FURTHER, AVAYA MAKES NO WARRANTY REGARDING THE RESULTS OF THE USE OF THE SDK AND DOCUMENTATION. NEITHER AVAYA NOR ITS SUPPLIERS MAKE ANY WARRANTY, EXPRESS OR IMPLIED, THAT THE SDK OR DOCUMENTATION IS SECURE, SECURITY THREATS AND VULNERABILITIES WILL BE DETECTED OR SOFTWARE WILL RENDER AN END USER'S OR LICENSEE'S NETWORK OR PARTICULAR NETWORK ELEMENTS SAFE FROM INTRUSIONS AND OTHER SECURITY BREACHES.

7.0 CONSEQUENTIAL DAMAGES WAIVER.

EXCEPT FOR PERSONAL INJURY CLAIMS, AVAYA SHALL NOT BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH, ARISING OUT OF OR RELATING TO THIS AGREEMENT OR USE OF THE SDK, OR FOR THE LOSS OR CORRUPTION OF DATA, INFORMATION OF ANY KIND, BUSINESS, PROFITS, OR OTHER COMMERCIAL LOSS, HOWEVER CAUSED, AND WHETHER OR NOT AVAYA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

8.0 LIMITATION OF LIABILITY.

EXCEPT FOR PERSONAL INJURY CLAIMS, IN NO EVENT SHALL AVAYA'S TOTAL LIABILITY TO LICENSEE IN CONNECTION WITH, ARISING OUT OF OR RELATING TO THIS AGREEMENT EXCEED FIVE HUNDRED DOLLARS ($500). THE PARTIES AGREE THAT THE LIMITATIONS SPECIFIED IN THIS SECTION WILL APPLY EVEN IF ANY LIMITED REMEDY PROVIDED IN THIS AGREEMENT IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE.

9.0 INDEMNIFICATION.

Licensee shall defend, indemnify and hold harmless Avaya, Affiliates and their respective officers, directors, agents, suppliers, customers and employees "Indemnified Parties") from and against all claims, demand, suit, actions or proceedings ("Claims") and damages, losses, liabilities, costs, expenses, and fees (including fees of attorneys and other professionals) ("Damages") based upon an allegation pertaining to wrongful use, misappropriation, or infringement of a third party's Intellectual Property right arising from or relating to Licensee's use of the SDK, alone or in combination with other software, such as operating systems and codecs, and the, direct or indirect, use, distribution or sale of any software, Derivative Works or other products (including but not limited to applications, interfaces, and application programming interfaces) developed utilizing the SDK.

Licensee shall defend, indemnify and hold harmless the Indemnified Parties from and against all Claims and Damages arising out of or related to: (i) personal injury (including death); (ii) damage to any person or tangible property caused, or alleged to be caused by Licensee or Licensee's application created by using the SDK; (iii) the failure by Licensee or Licensee's

application created by using the SDK to comply with the terms of this Agreement or any applicable laws; (iv) the breach of any representation, or warranty made by Licensee herein; or (v) Licensee's breach of any obligation under the Licensee EULA.

10.0 TERM AND TERMINATION.

10.1 This Agreement will continue through December 31st of the current calendar year. The Agreement will automatically renew for one (1) year terms, unless terminated as specified in Section 10.2 or 10.3 below.

10.2 Either party shall have the right to terminate the Agreement, upon thirty (30) days written notice to the other party.

10.3 Notwithstanding language to the contrary, Avaya may terminate this Agreement immediately, upon written notice to Licensee for breach of Section 2 (License Grant), Section 5 (Confidentiality) or Section 12 (Compliance with Laws). Avaya may also terminate this Agreement immediately by giving written notice if a Change In Control should occur or if Licensee becomes insolvent, or voluntary or involuntary proceedings by or against Licensee are instituted in bankruptcy or under any insolvency law, or a receiver or custodian is appointed for Licensee, or proceedings are instituted by or against Licensee for corporate reorganization or the dissolution of Licensee, which proceedings, if involuntary, have not been dismissed within thirty (30) days after the date of filing, or Licensee makes an assignment for the benefit of its creditors, or substantially all of the assets of Licensee are seized or attached and not released within sixty (60) days thereafter, or if Licensee has ceased or threatened to cease to do business in the regular course.

10.4 Upon termination or earlier termination of this Agreement, Licensee will immediately cease a) all uses of the Confidential Information; b) Licensee agrees to destroy all adaptations or copies of the Confidential Information stored in any tangible medium including any document or work containing or derived (in whole or in part) from the Confidential Information, and certify its destruction to Avaya upon termination of this License. Licensee will promptly cease use of, distribution and sales of Licensee products that embody any such Confidential Information, and destroy all Confidential Information belonging to Avaya as well as any materials that embody any such Confidential Information. All licenses granted will terminate.

10.5 The rights and obligations of the parties contained in Sections 2.3, 2.6, 2.7, 2.10, 2.11, 2.12, 3, and 5 through 17 shall survive any expiration or termination of this Agreement.

11.0 ASSIGNMENT.

Avaya may assign all or any part of its rights and obligations hereunder. Licensee may not assign this Agreement or any interest or rights granted hereunder to any third party without the prior written consent of Avaya. The term "assign" includes, but is not limited to, any transaction in which there is a Change In Control or reorganization of Licensee pursuant to a merger, sale of assets or stock. This Agreement shall terminate immediately upon occurrence of any prohibited assignment.

12.0 COMPLIANCE WITH LAWS AND IMPORT/EXPORT CONTROL.

Licensee shall comply with all applicable laws and regulations, including without limitation those applicable to data privacy, intellectual property, trade secret, and fraud. Licensee is advised that the Technical Information is of U.S. origin and subject to the U.S. Export Administration Regulations ("EAR") and may be subject to applicable local country import/export laws and regulations. Diversion contrary to U.S. and/or applicable local country law and/or regulation is prohibited. Licensee agrees not to directly or indirectly export, re-export, import, download, or transmit the Technical Information to any country, end user or for any use that is contrary to applicable U.S. and/or local country regulation or statute (including but not limited to those countries embargoed by the U.S. government). Licensee represents that any governmental agency has not issued sanctions against Licensee or otherwise suspended, revoked or denied Licensee's import/export privileges. Licensee agrees not to use or transfer the Technical Information for any use relating to nuclear, chemical or biological weapons, or missile technology, unless authorized by the U.S. and/or any applicable local government by regulation or specific written license. Additionally, Licensee is advised that the Technical Information may contain encryption algorithm or source code that may not be exported to government or military end users without a license issued by the U.S. Bureau of Industry and Security and any other country's governmental agencies, where applicable.

13.0 WAIVER.

The failure to assert any rights under this Agreement, including, but not limited to, the right to terminate in the event of breach or default, will not be deemed to constitute a waiver of the right to enforce each and every provision of this Agreement in accordance with their terms.

14.0 SEVERABILITY.

If any provision of this Agreement is determined to be unenforceable or invalid, this Agreement will not be rendered unenforceable or invalid as a whole, and the provision will be changed and interpreted so as to best accomplish the objectives of the original provision within the limits of applicable law.

15.0GOVERNING LAW AND DISPUTE RESOLUTION.

15.1 Governing Law. This Agreement and any dispute, claim or controversy arising out of or relating to this Agreement ("Dispute"), including without limitation the formation, interpretation, breach or termination of this Agreement, or any issue regarding whether a Dispute is subject to arbitration under this Agreement, will be governed by New York State laws, excluding conflict of law principles, and the United Nations Convention on Contracts for the International Sale of Goods.

15.2 Dispute Resolution. Any Dispute will be resolved in accordance with the provisions of this Section 15. The disputing party shall give the other party written notice of the Dispute in accordance with the notice provision of this Agreement. The parties will attempt in good faith to resolve each controversy or claim within 30 days, or such other longer period as the parties may mutually agree, following the delivery of such notice, by negotiations between designated representatives of the parties who have dispute resolution authority.

15.3 Arbitration of Non-US Disputes. If a Dispute that arose anywhere other than in the United States or is based upon an alleged breach committed anywhere other than in the United States cannot be settled under the procedures and within the timeframe set forth in Section 15.2, it will be conclusively determined upon request of either party by a final and binding arbitration proceeding to be held in accordance with the Rules of Arbitration of the International Chamber of Commerce by a single arbitrator appointed by the parties or (failing agreement) by an arbitrator appointed by the President of the International Chamber of Commerce (from time to time), except that if the aggregate claims, cross claims and counterclaims by any one party against the other party exceed One Million US Dollars at the time all claims, including cross claims and counterclaims are filed, the proceeding will be held in accordance with the Rules of Arbitration of the International Chamber of Commerce by a panel of three arbitrator(s) appointed in accordance with the Rules of Arbitration of the International Chamber of Commerce. The arbitration will be conducted in the English language, at a location agreed by the parties or (failing agreement) ordered by the arbitrator(s). The arbitrator(s) will have authority only to award compensatory damages within the scope of the limitations of Section 8 and will not award punitive or exemplary damages. The arbitrator(s) will not have the authority to limit, expand or otherwise modify the terms of this Agreement. The ruling by the arbitrator(s)) will be final and binding on the parties and may be entered in any court having jurisdiction over the parties or any of their assets. The parties will evenly split the cost of the arbitrator(s)' fees, but Avaya and Customer will each bear its own attorneys' fees and other costs associated with the arbitration. The parties, their representatives, other participants and the arbitrator(s) will hold the existence, content and results of the arbitration in strict confidence to the fullest extent permitted by law. Any disclosure of the existence, content and results of the arbitration will be as limited and narrowed as required to comply with the applicable law. By way of illustration, if the applicable law mandates the disclosure of the monetary amount of an arbitration award only, the underlying opinion or rationale for that award may not be disclosed.

15.4 Choice of Forum for US Disputes. If a Dispute by one party against the other that arose in the United States or is based upon an alleged breach committed in the United States cannot be settled under the procedures and within the timeframe set forth in Section 15.2, then either party may bring an action or proceeding solely in either the Supreme Court of the State of New York, New York County, or the United States District Court for the Southern District of New York. Except as otherwise stated in Section 15.3 each party consents to the exclusive jurisdiction of those courts, including their appellate courts, for the purpose of all actions and proceedings arising out of or relating to this Agreement.

15.5 Injunctive Relief. Nothing in this Agreement will be construed to preclude either party from seeking provisional remedies, including, but not limited to, temporary restraining orders and preliminary injunctions from any court of competent jurisdiction in order to protect its rights, including its rights pending arbitration, at any time. The parties agree that the arbitration provision

in Section 15.3 may be enforced by injunction or other equitable order, and no bond or security of any kind will be required with respect to any such injunction or order.

15.6 Time Limit. Actions on Disputes between the parties must be brought in accordance with this Section within 2 years after the cause of action arises.

16.0 AGREEMENT IN ENGLISH.

The parties confirm that it is their wish that the Agreement, as well as all other documents relating hereto, including all notices, have been and shall be drawn up in the English language only. Les parties aux présentes confirment leur volonté que cette convention, de même que tous les documents, y compris tout avis, qui s'y rattachent, soient rédigés en langue anglaise.

17.0 ENTIRE AGREEMENT.

This Agreement, its exhibits, schedules and other agreements or documents referenced herein, constitute the full and complete understanding and agreement between the parties and supersede all contemporaneous and prior understandings, agreements and representations relating to the subject matter hereof. No modifications, alterations or amendments shall be effective unless in writing signed by both parties to this Agreement.

18. REDISTRIBUTABLE CLIENT FILES.

The list of SDK client files that can be redistributed, if any, are in the SDK in a file called Redistributable.txt.

Schedule 1 to Avaya SDK License Agreement
Third Party Notices

1. **CODECS**: WITH RESPECT TO ANY CODECS IN THE SDK, YOU ACKNOWLEDGE AND AGREE YOU ARE RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES, IF ANY. IT IS YOUR RESPONSIBILITY TO CHECK.

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 THE H.264 (AVC) CODEC MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Contents

Avaya Breeze® platform FAQ and Troubleshooting for Snap-in Developers..... 1
Chapter 1: SDK..... 16
Reference documents for Service Developers..... 16
Why did my SDK installation fail? 16
How do I know if the SDK install script succeeded? 17
Where do I find Avaya Breeze® platform Javadoc..... 17
Why does Eclipse show errors after I import the Helloservice?..... 18
Why does my project build fail with “Unable to locate the Javac Compiler in…”? 19
Why does the Eclipse Maven plug-in installation fail..... 21
Where is the .svar located after the project build is complete? 22
Why don’t I see service-archetype in the list when I try to start my project from within Eclipse?..... 22
Why do I have different project directories when I create a project from the archetype 23
Chapter 2: Avaya Breeze® platform Eclipse plug-in 25
Why do I see a popup message about the current maven version being lower than the minimal supported version? 25
Why is the “Edit System” menu option disabled? 25
Why are some of the Eclipse plugin actions disabled when I right click? 25
If I have added new nodes and modify cluster name, how does the Eclipse plugin get the updated configuration from System Manager? 26
I have only modified java files with no modification in properties.xml of snap-in. Do I need to re-publish the snap-in to System Manager? 26
Why can’t I see new functionality provided by a newer Eclipse plugin version?..... 26
My cluster list is not getting refreshed in the plugin System Manager Browser 27
The cluster status is Green but there is a Red icon next to some of my Avaya Breeze® platform servers. Why is that?..... 27
I was building the service and tailing logs, but now I can’t see any logs in the console for my other service 27
I have multiple Avaya Breeze® platform servers selected in a cluster and now I enabled debug mode. Can I debug my application on multiple Avaya Breeze® platform servers? 28
Cannot debug snap-ins on Avaya Breeze® platform node using the Eclipse plugin 28
Why is the Eclipse plug-in not able to connect to Avaya Breeze® platform 3.9 and System Manager 10?..... 29
Chapter 3: Services..... 30

Can I create a service that has Call related features and can be invoked through HTTP/REST interface? 30
How can I replace my service with newer iterations where I did not change the version number? (Lab only) 30
How do I replace my service with a newer version where I changed the version number? (For production use) 31
How do I remove/delete my service 32
Why don't I see my (re)deployed service? 33
Why do attributes defined by my service not appear under Service Globals? 33
How can I make HTTPS requests using the WebSphere certificate from my service? 34
How can I define alarms in my service? 35
How do I define notification OID? 35
How do I define the enterprise ID and product identifier? 36
How do I define event codes? 36
How do I enable clearing of a defined alarm? 36
How do I raise defined alarms? 37
How do I convert my Avaya Breeze® platform 3.7 or 3.8 service to a 3.9 service? 37
How do I access third-party services and APIs that require a secure (i.e., HTTPS or TLS) connection? 39
Do I need an extra attribute in properties.xml to mark my snap-in as a callable service? 39
What is trusted hosts per cluster? 40
Can the administrator assign trusted hosts to a legacy cluster? 40
Why does my snap-in encounter "SSLUtilityException (TLS version for Service cannot be lower than Default version)" when it calls createSSLContext API? 40
When my snap-in sends an HTTP response, Avaya Breeze® platform adds security headers. How can one customize the value of the headers? 41
As an ISV, how can I configure snap-ins to efficiently process customers' varying dial plans? 41
Why cannot a snap-in gain access to UCIDs of a call created by another snap-in? 42
Why is my service being invoked again after I call removeServiceFromCall? 42
Chapter 4: Service debugging 43
Why did I get "Invalid Class Name, the Class Name does not exist in the Jar File." error message? 43
Why aren't my JDBC Providers in the drop-down on the data source editor page? 43
Can I create two JDBC providers with the same name? 44
Can I create two JDBC data sources with same JNDI name on the same cluster? 44
Can I create multiple JDBC data sources for a single JDBC provider? 44

Where do I check JDBC Data source Test Connection result? 45
Why is the JDBC Source setting not reflected? Even after I changed the JDBC data source attributes, it is giving same error/result 45
Why am I unable to uninstall/delete JDBC providers from the Service Management page? 45
Why am I getting the error “com.mysql.jdbc.Driver incompatible with javax.sql.ConnectionPoolDataSource” on the Test connection? 46
Why am I getting simply “ERROR” error message on Test Connection? 46
Why does my data source not work even with the correct configuration? 47
How can I tell if my service got installed properly? 47
Why my service is not installed even after I created a cluster and added my service in the cluster? 49
Why do I have to manually select my service for installation while creating a cluster especially since I can see some services which are already selected for installation? 49
How can I find why my service installation failed? 49
How can I tell if my service is running or gets invoked? 50
Why is my service not getting invoked 51
Why are the changes from System Manager to service attributes of my service not reflected during execution or runtime? 61
Why is my service not accessible over http but accessible over https? 62
How to use postman for https invocation to my service? 63
How do I import collections bundled with Sample Services to Postman client in Chrome? 63
How do I invoke Multi-Channel Broadcast service and Dynamic Team Formation Service for my testing 70
How do I invoke ClickToCall Sample service for my testing? 71
What are the prerequisites for the Callingpolicies Sample service? 71
How do I test the Callingpolicies Sample service? 72
My service is installed and I see logs from my service, but things are not behaving like I expected. What should I check? 73
Where do I look for the debug logs I added to my service? 78
Why does my outgoing HTTP request from my service not use the security module IP? 79
Why does HTTPS access to my services give error like “Cannot connect to real <IP address>”? 79
How do I debug media-related issues? 80

I've set up an implicit sequence pattern so that Session Manager routes calls to Avaya Breeze® platform, but some calls that match my pattern are not sent to Avaya Breeze®

platform. What might cause this? 82
How can I stop Avaya Breeze® platform from logging me out of an SSH session? 84
Why don't I see my service alarm on System Manager or Data Center? 84
Why is access to my service so slow or sometimes not accessible? 84
How can I have my service not show “Not Applicable” for my service? 85
Why does my service show a warning icon with a date? 85
Why do I have call failures when using APIs which use Avaya Aura® Media Server? 86
My service is invoked and it runs media operations, or indicates that it might run media operations. Why does the call seem to stall? 86
How do I know if the attribute was changed at the global level, cluster level, or service profile level? 87
Why do I get the attribute change notification with “newObject = null” when I change the cluster level value of an attribute to its default by doing an uncheck from the GUI? 87
My callable service is not invoked and an error is received 87
– ERR104 No callable service was found for <user@domain> 87
If I do an addParticipant() operation from my Callable Service, I see an INVITE sent back to Session Manager with the original Request URI, resulting in a 404 error 88
Identifying if my snap-in is invoked as a sequenced snap-in or is invoked as a callable service 88
How can I debug Out of Memory issues on the server? 88
How can I debug threading issues on the server? 88
How do I list snap-in attributes? 88
Why do responses to my MessageReceiver, EmailListener, SmsListener arrive late or not at all 89
When I do a play announcement or a prompt and collect media operation, why is the announcement/prompt not heard? 90
Why does log_space in properties.xml not reserve the same log space for my snap-in? 90
Test Connection action for TLS supported JDBC Datasource does not succeed even after all the correct configurations 90
Why was an IllegalStateException with a detail message of "AMS is not configured" thrown? 91
Why does a call that performs a media operation not work? I see that the asm logs complain of invalid credentials 91
Why does a call that performs a media operation not work? I see that the asm logs complain of SSL and/or TLS and/or certificate issues 92
Why does the PlatformListener class not getting the notification 92
Why does a service declaring dependencies on the cluster database, the reliable eventing group, or the datagrid show a yellow triangle when a cluster is selected for

installation from the Service Management or Bundles page or when it is assigned to the cluster from Cluster Editor? 93
What are the trace tools available for debugging environment/snap-in issues on Avaya Breeze® platform? 93
Why are the trusted certificates bundled in my snap-in not getting installed when I install my snap-in? 93
Outgoing Requests from my snap-in do not work, even though certificates are part of my snap-in and the trusted certificates are installed on Avaya Breeze® platform servers? 94
Why does loading the snap-in fail with the "Properties" file is missing the mandatory smgr element" error message? 94
Why does loading the snap-in fail with the "The Factory_Override missing one or more elements: name, type or factory sub element" error message? 95
Why does loading the snap-in fail with the "The Factory_Override type must be STRING,INTEGER or BOOLEAN" error message? 95
Why does loading the snap-in fail with the "Attribute_override must include at least one factory_Override element" error message? 95
Why does loading the snap-in fail with the "Attribute_override must include at least one override_SnapinAttribute element" error message? 96
Why does loading the snap-in fail with the "factory_override element type must match snapin element type" error message? 96
Why does loading the snap-in fail with the "no match Attribute in snapin" error message? 96
Why do asm.log and server.log contain DAO WARN message? 97
Why do some calls through Avaya Breeze® platform fail immediately? 98
Why is Avaya Breeze® platform in system overload for disk space? 98
Chapter 5: Connector debugging 99
Why was email not sent from my service? 99
Why was SMS not sent from my service 101
Why was Scopia conference not scheduled from my service? 103
Why do I see the following services – EventingConnector and CallEventControl installed on most cluster types? 105
Chapter 6: HTTP Load Balancing and High Availability 105
How to enable/disable HTTP load balancer in a cluster? 105
How to locate the HTTP load balancer nodes in a cluster? 106
How is the cluster IP address used on the load balancer? 106
Why hasn't the cluster IP address been assigned to any of the servers? 106
What if planned maintenance needs to be done on active load balancer node? 107
What if an unplanned failover happened? 107

Why do I see both load balancers are in active state? 107
How can I tell when the HTTP Load Balancer failed over? 107
How does the load balancer distribute requests in a cluster? 108
How can I tell whether the load balancer distributes the traffic evenly in cluster? 108
How do I redirect Http Request with Load Balancer ? 109
How does Session Affinity work on load balancer? 109
Chapter 7: Eventing Framework 110
Why do I stop receiving events after 8-9 hours? 110
How can I tell which subscriptions were matched when an event is sent? 110
Why am I getting multiple event notifications for a single event? 110
Why am I not getting my expected events? 111
Why are there log statements saying the Eventing System is still initializing? 111
Why does my subscription not seem to activate? 112
Why don't I get an acknowledgement for an event? 113
Chapter 8: Snap-in bundle and dependencies debugging 114
What does the 'Load' operation of a bundle mean? 114
Is partial bundle load supported? 114
Does the bundle load fail if services within the bundle are loaded? 114
Does the bundle load fail if the service dependencies are not loaded? 114
Does bundle load fail if the service within the bundle was loaded by another bundle? 114
Why my bundle load fail? 114
What does the Install operation of a bundle mean? 115
Can I install more than one bundle at a time? 115
Can I install a bundle on multiple clusters? 115
What is the meaning of 'n of m' in the state column? 115
Why is the Partial status displayed for a cluster when the n of m state link is clicked? Are there any other status legends used? 115
Does the installation of a bundle automatically install the dependency services? 116
What happens when a dependency service in a bundle is not loaded on System Manager and triggers the bundle installation? 116
What happens when some services of a bundle are already installed on a cluster and trigger the bundle installation? 116
What happens when a service is part of multiple bundles and one of the bundle is installed? 116
What happens when a service which is part of a bundle is selected from the Services page and installed? Does it install the whole bundle? 116

What happens when a service, which is a part of an installed bundle, is uninstalled from the Services page? Does it uninstall other services of the bundle? Does it affect the functions of a bundle? 117
What happens when a bundle is installed on a cluster without Avaya Breeze® platform instances? 117
What happens when a bundle is installed on a cluster with Avaya Breeze® platform instances that are not working? 117
What happens when Avaya Breeze® platform instances of a cluster stop working during installation? 117
What happens when a service fails to install on an Avaya Breeze® platform instance in a cluster during bundle installation? 118
How do I reinstall a bundle whose installation failed? 118
How do I see the installation status of services of a bundle? 118
Can I install a service which is part of a bundle from the Cluster add edit page? Does it install the entire bundle? 118
WFDs as SVARs 118
Why are my Bundle WFDs and Tasks services not listed on Service Management page? 118
Why doesn't the Cluster Editor page display my Bundle WFDs and Tasks services to be assigned/unassigned? 119
Why does not the Service Profile page for assign/un-assign services display my Bundle WFDs and Tasks services? 119
Why don't I see service attributes after uninstalling Engagement Designer Release 3.2 or earlier? 119
Why do the cluster attributes not display after installing Engagement Designer Release 3.9 on the same cluster that has Engagement Designer Release 3.9 installed? 119
Why don't we see the service, cluster, and system attributes for WFDs if only Engagement Designer Release 3.9 or later is installed? 120
Why does the Bundle allow installation of WFDs and Tasks even though dependency of Engagement Designer Release 3.9 or later not defined in the metadata? 120
Why can't we load WFDs and Tasks services from the Service Management page? 120
Why does Engagement Designer Console display the WFDs status as deployed when the WFDs are in the installing state? 120
Chapter 9: Authorization debugging 121
Authorization key not updated after ISO upgrade 121
Connection Exception when using APIs to fetch access tokens 121
AuthorizationHelperException when using APIs to fetch access tokens 122
Authorization Helper APIs respond with "403 Forbidden. No associated scope found" . 122
How do I change the token validity time? 122

How do I change the client JWT validity time? 123
Unable to edit grants on Authorization Client 123
What user scopes are supported? 123
How do I configure SAML Authentication? 124
How do I configure LDAP authentication on the Authorization Service provided login screen? 124
How do I resolve the 'SAML profile is not deployed' error? 124
When logging an agent to Workspaces, an error : "Invalid claims in token" is seen 124
When authenticating a user on the browser, an error: "502 : Bad gateway error" is seen. 125
LDAP Authentication is failing 126
Chapter 10: Cluster Database debugging 127
How to enable cluster DB? 127
Snap-in installed successfully, DB is created but schema upgrade scripts are not run 127
Errors seen in logs related to connections exhausted 127
Where do I see the cluster db back up jobs that are scheduled to run immediately? 127
Cluster db backup is failing with message – Error: Auth fail 128
Chapter 11: Cluster and node management 129
Why aren't the certificate management and Cluster State buttons not enabled when I select a cluster on Cluster Administration page? 129
Why do I see ---- instead of values when I select an older time period, for example, 4 days ago for a cluster to view Peak Usage on System Resource Monitor page? 129
Reliable eventing group status shows Error on the Dashboard 129
Chapter 12: IPv6 management in JITC mode 131
How do I enable general IPv6 settings? 131
How do I configure IPv6 addresses on Avaya Breeze® platform? 131
How do I configure IPv6 address on Avaya Breeze® platform clusters? 131
How do I verify IPv6 addresses on Avaya Breeze® platform servers? 131

Chapter 1: SDK

Reference documents for Service Developers

- *Avaya Breeze® platform Snap-in Development Guide*
- *Getting started with Avaya Breeze® SDK*
- *Deploying Zang-Enabled Avaya Breeze® platform.*
- *Multi-Channel Broadcast Sample Snap-in*
- *Dynamic Team Formation Sample Snap-in*
- *Calling Policies Sample Snap-in*
- *Authorization Sample Bundle*
- *CallableService Sample Snap-in*
- *CallDeflection Sample Snap-in*
- *ClickToCall Sample Snap-in*
- *Web Call Controller Sample Snap-in*
- *Whitelist Sample Snap-in*
- *Zang SMS Connector Snap-in*
- *Task Dashboard and Task Repository - Sample Authorization Snap-in*
- *Outbound Https Sample Snap-in*

Why did my SDK installation fail?

Solution

1. The SDK install script runs a few Maven commands. Verify that you have Maven Release 3.6.3 or later correctly installed by running the command `mvn –version`.

   The output should show version information similar to this:

   Apache Maven 3.6.3 (ea8b2b07643dbb1b84b6d16e1f08391b666bc1e9; 2014-02-14T10:37:52-07:00) Maven home: /opt/apache-maven-3.6.3 Java version: 1.8.0_55, vendor: Oracle Corporation Java home: /usr/java/jdk1.8.0_55/jre Default locale: en_US, platform encoding: UTF-8 OS name: "linux", version: "2.6.32-358.el6.x86_64", arch: "amd64", family: "unix

   Of course, your Maven home or Java home (as well as Java version and OS name) may vary from this example.

2. If you do not see version information (or an error regarding the mvn command), review the Maven installation instructions to assure you have set up Maven correctly.
3. Relaunch install.bat or install.sh from the downloaded and extracted “Avaya-Breeze-SDK”.

How do I know if the SDK install script succeeded?

About this task

The SDK install script runs a few separate commands. If any of these commands fail, the SDK install script will exit and indicate a failure. If you scan the last few lines of output and see “success”, then the install script completed successfully.

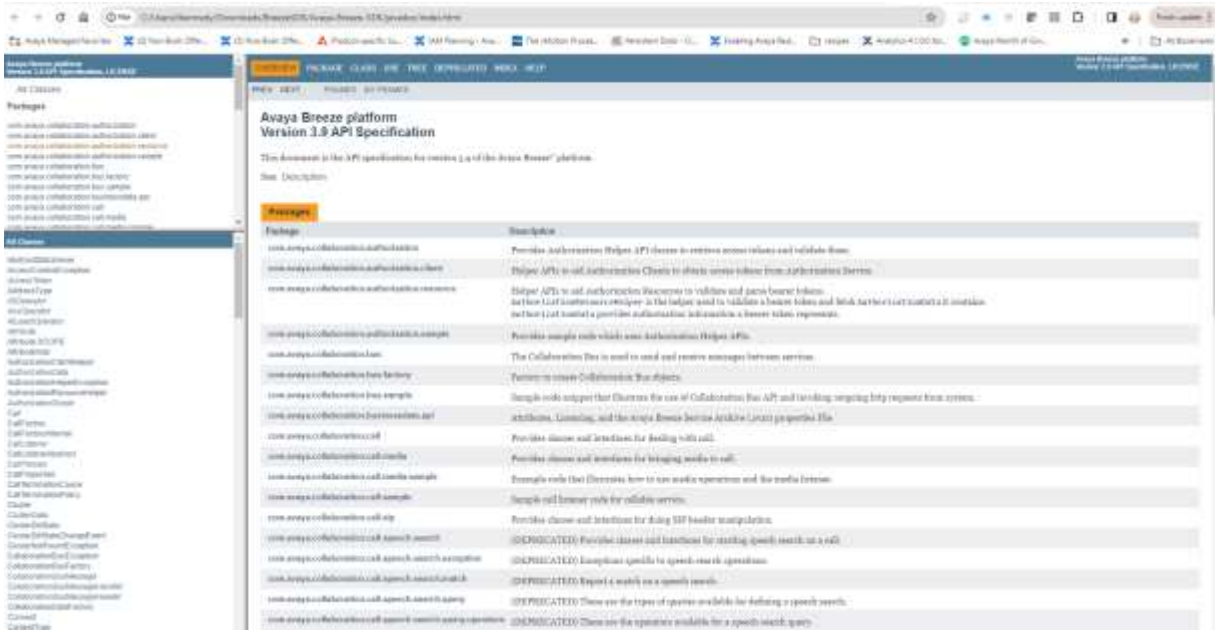
Where do I find Avaya Breeze® platform Javadoc

Procedure

1. Log in to your system where you downloaded and extracted the SDK. Assuming it is a Linux system:

```
drwxr-xr-x.  7 root  root      4096 Oct 31 16:46 Avaya-Breeze-SDK
-rw-------.  1 root  root  40161439 Dec  5 15:08 Avaya-Breeze-SDK-3.9.0.0.390016.zip
```

2. Execute “cd <Avaya-Breeze-SDK>/javadoc”. avaya-aura-collaboration-javadoc-3.9.jar is the Javadoc jar is the Javadoc jar.
3. Execute jar –xvf avaya-aura-collaboration-javadoc-3.9.jar.
4. Open the index.html file using a web browser to see the Javadoc.



5. If you are using Microsoft Windows, unzip the SDK under avaya-aura-collaboration-javadoc-3.9.jar
6. Open the index.html file using a web browser.

   If you use Mozilla Firefox to view documentation, you can put the jar directly in the address bar without extracting the contents. For example, jar:file:///home/dev5/<SDK folder>/javadoc/avaya-aura-collaboration-javadoc-3.9.jar!/.

7. Click `index.html` to look at the Javadoc.
8. To access the Collaboration API Javadocs, click on a class name in Eclipse, press `F2`, and click **Open Attached Javadoc in Browser**.

Why does Eclipse show errors after I import the Helloservice?

Solution

1. From the Eclipse menu, select **Project** > **Clean**, then select either **Clean all projects** or **Clean projects selected below** and select all the helloservice projects.
2. If step 1 does not clear the errors, right-click on the top-level project (that would be helloservice without a suffix), then select **Run As – Maven build…**.
3. In the **Goals** field of the Edit Configuration dialog box, enter `clean package`, and then click **Run**.
4. If errors still exist after the build, right-click on the top-level project and select **Refresh**.
5. To verify that you have configured Eclipse to use JDK 1.8 or later, from the top menu, select **Project** > **Properties** > **Java Compiler**, and check the Compiler compliance level.
6. From the **Eclipse** menu, select **Window** > **Show view** > **Markers** and look at the error text to understand the problem.
7. If you are still unable to resolve the errors within Eclipse, try building from the command line instead of in Eclipse.

   Use the command `mvn clean package`.

8. If this shows errors, and you believe your environment (Java, Maven, etc.) is set up correctly:
   a. Try deleting the Maven repository. To find your local repository, run mvn help:effective-settings

      Near the end of the output, you will see some XML.
   b. Go to the top of the XML and look for the localRepository element:

      <settings xmlns=http://maven.apache.org/POM/4.0.0 xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance xsi:schemaLocation="http://maven.apache.org/SETTINGS/1.1.0 http://maven.apache.org/xsd/settings-1.1.0.xsd">

      <localRepository xmlns="http://maven.apache.org/SETTINGS/1.1.0 /maven/repository</localRepository> <proxies xmlns="http://maven.apache.org/SETTINGS/1.1.0"> <proxy>">/usr/local <port>8000</port>

      …

      </localRepository>

      …

      </settings>

      In this example, the local repository starts at the directory /usr/local/maven/repository.
   c. Go to the /usr/local/maven/ directory and delete everything under this directory.
9. Delete the SDK and then re-install the SDK according to the SDK installation instructions provided in “Getting Started with the Avaya Breeze® platform SDK” doc.

Why does my project build fail with “Unable to locate the Javac Compiler in…”?

You see the following error message on the Eclipse console while building the project:

[INFO] BUILD FAILURE

[INFO] ----------

[INFO] Total time: 1.344s [INFO] Finished at: Wed Sep 11 09:31:08 MDT 2013

[INFO] Final Memory: 5M/15M

[INFO] ----------

[ERROR] Failed to execute goal org.apache.maven.plugins:maven-compiler-plugin: 2.3.2:compile (default-compile) on project testtracy-war: Compilation failure

[ERROR] Unable to locate the Javac Compiler in:

[ERROR] C:\Program Files\Java\jre8\..\lib\tools.jar

[ERROR] Please ensure you are using JDK 1.8 or above and

[ERROR] not a JRE (the com.sun.tools.javac.Main class is required).

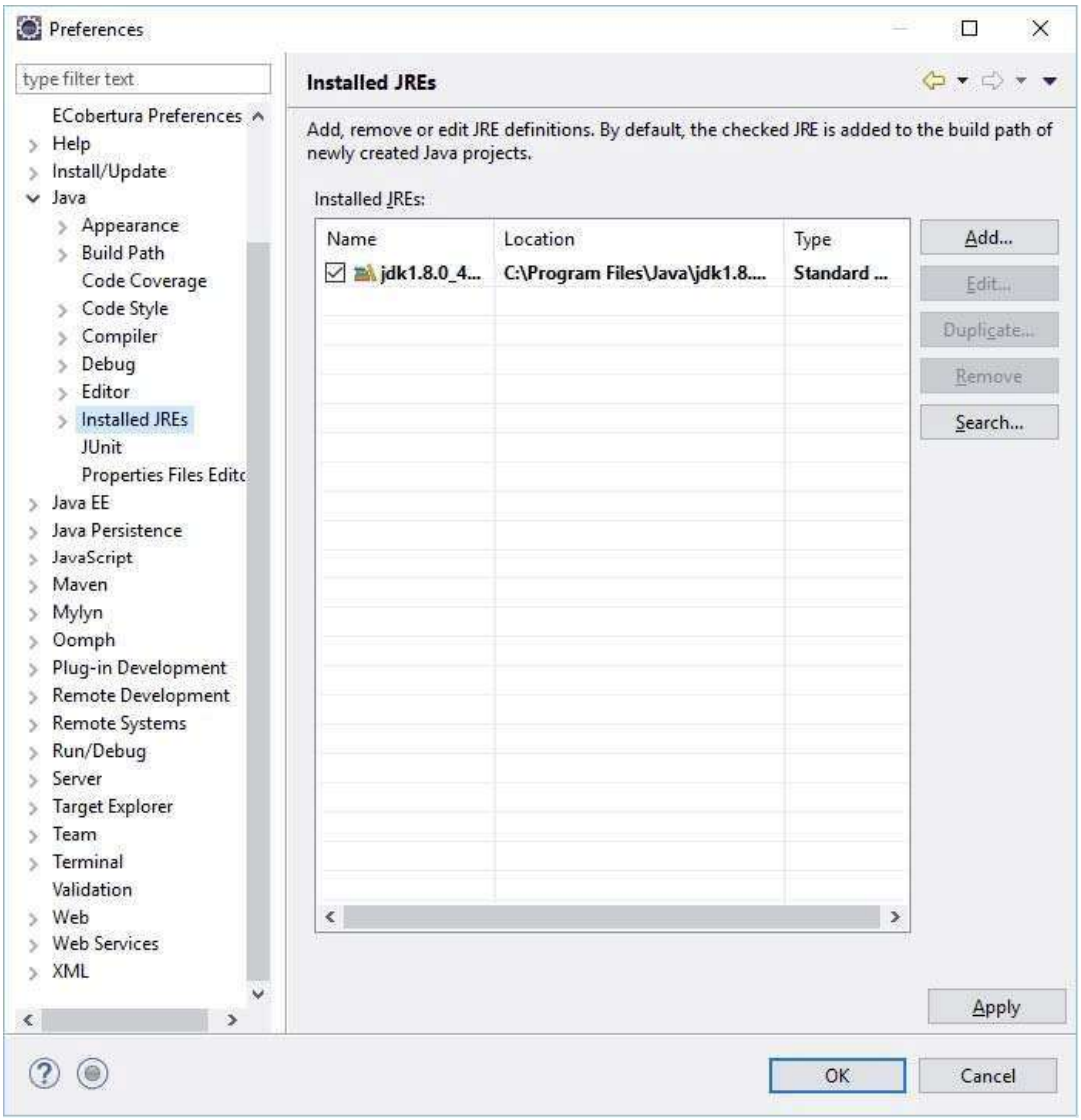
[ERROR] In most cases you can change the location of your Java

[ERROR] installation by setting the JAVA_HOME environment variable.

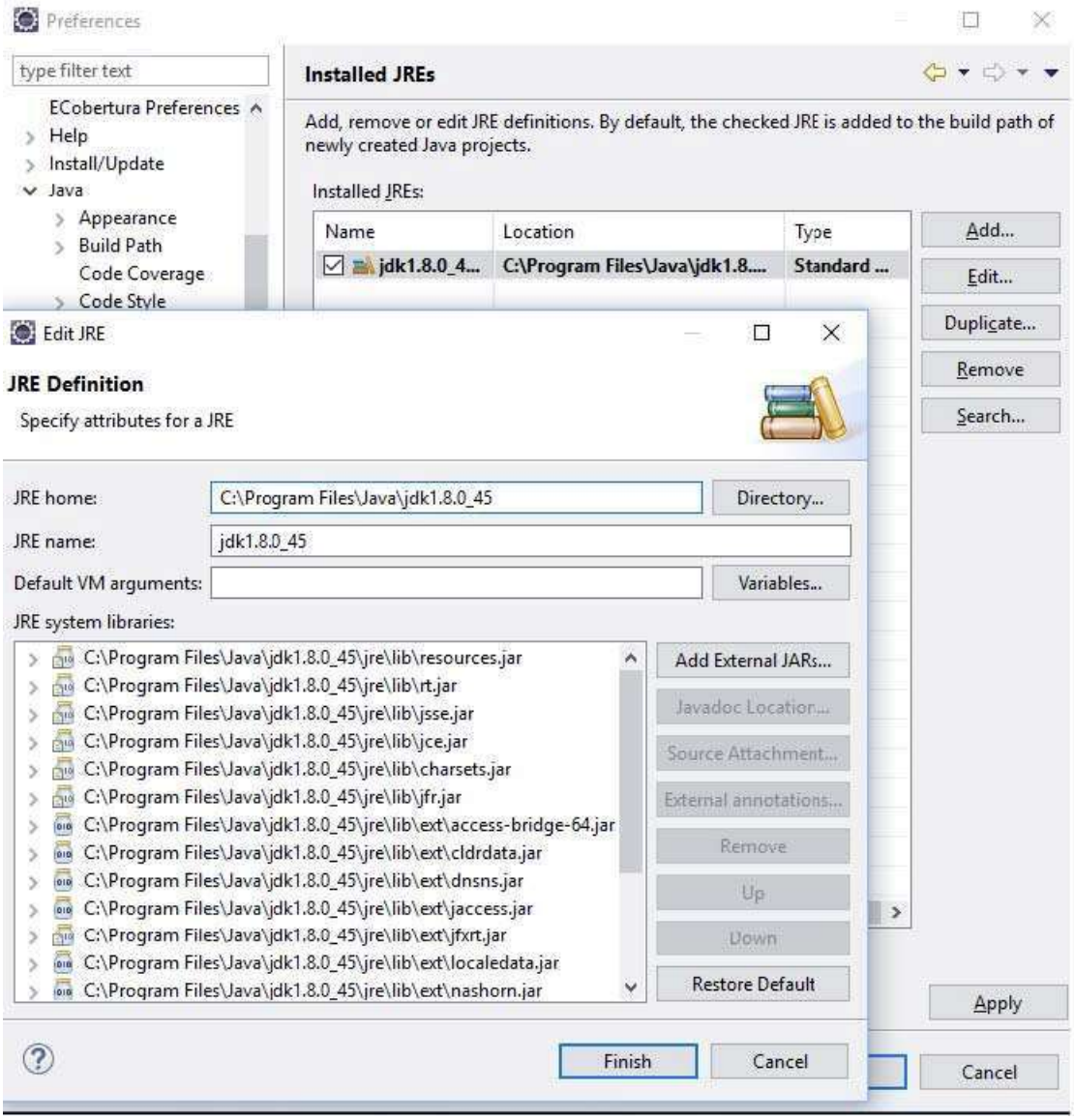
[ERROR] -> [Help 1]

Solution

1. Go to **Eclipse** > **Window** > **Preferences** > **Java** > **Installed JREs**.



2. Make sure that the JDK path is mentioned in the list and selected. If not, select the entry and click **Edit**.



3. Finish and save all the screens and build the project again.

Why does the Eclipse Maven plug-in installation fail

The Eclipse Maven plug-in installation fails.

Solution

Check if Eclipse is installed.

If Eclipse is installed, Eclipse includes the Maven plug-in. You do not need to install the Maven plug-in again. The recommended version of Eclipse is Eclipse 4.29 (2023-09).

Where is the .svar located after the project build is complete?

Procedure

After the build completes, in Eclipse right-click on the top-level project (that would be helloservice without a suffix) and select **Refresh**.

After the build completes, the directory structure will look like this (some directories and files omitted to keep this smaller):

```
|-helloservice
  |---helloservice-ear
  | ----src
  | ----target
  | --helloservice-svar
  | ----src
  | ----- main
  | ------- assembly
  | ------- resources
  | ----target
  |------- HelloWorld-0.0.0.1.5.svar <- this is the svar to install
  | ----- archive-tmp
  | ----- dependency
  | ----- dependency-maven-plugin-markers
  | --helloservice-war
  | ----src
  | ----- main
  |----------java
  | ----- test
  |----------java
  | ----target
```

Why don't I see service-archetype in the list when I try to start my project from within Eclipse?

Solution

1. When starting a new Maven project, verify that the checkbox for **Create a simple project(skip archetype selection)** is unchecked.
2. In the Eclipse Maven archetype selection page, check that the **Catalog** field is set to **All Catalogs**.
3. Verify that the SDK installation completed successfully.
   The SDK install script runs a few separate commands. If any of these commands fail, the SDK install script will exit and indicate a failure. If you scan the last few lines of output and see success, then the install script complete successfully.

4. Verify archetype-catalog.xml is in the .m2 directory.
5. If the file is not present, try deleting everything from the Maven repository and then re-installing the SDK according to the SDK installation instructions in “Getting Started with the Avaya Breeze® platform SDK” doc.

Why do I have different project directories when I create a project from the archetype

Different project directories are different Maven artifacts which together create a service archive file (.svar) for deployment on Avaya Breeze® platform. Taking an example of the Helloservice, Eclipse will show 4 project directories:

```
|-helloservice
|---helloservice-ear
| --- src
| --- target
| --helloservice-svar
| --- src
| ----- main
| ------- assembly
| ------- resources
| --- target
| --helloservice-war
| --- src
| ----- main
|----------java
| ----- test
|----------java
| --- target
```

|-helloservice: This is the base maven project which contains “helloservice-ear”, “helloservicesvar” and “helloservice-war”.

|-helloservice-ear: This is the ear application which gets bundled into the svar for deploying. This contains the application.xml which defines the enterprise application archive.

|-helloservice-svar: This maven project is used to bundle the ear into a svar. It contains the manifest.xml, properties.xml which defines a service archive.

|-helloservice-war: This maven project can contain all the required servlets, REST services and classes along with the core logic of an Avaya Breeze® platform service.

It is also possible to have an ejb jar in your service in case you would like to execute some EJB related operations (session beans, JPA, .etc.). For this, you will need to have an appropriate code structure and modify the pom.xml for the ear to bundle the ejb jar into your project. For example, the email connector has a dependency similar to the following in the pom.xml of the ear project:

```
<dependencies>
   <dependency> <groupId>com.xyz.emailconnector</groupId> <artifactId>emailconnector-
       ejb</artifactId> <version>XYZ</version> <type>ejb</type>
   </dependency>

</dependencies>
```

pom.xml of the ejb project should have lines similar to:

```
<parent>
   <artifactId>emailconnector</artifactId>
   <groupId>com.xyz</groupId>
</parent>
<groupId>com.xyz.emailconnector</groupId>
<artifactId>emailconnector-ejb</artifactId>
<packaging>ejb</packaging>

<name>emailconnector-ejb</name>
```

The build section of pom.xml of the EJB project should have following lines:

```
<build>
     <plugins> …… ……
          <plugin> <groupId>org.apache.maven.plugins</groupId> <artifactId>maven-ejb-
             plugin</artifactId> <version>ejb-plugin-version</version> <configuration>
                <ejbVersion>ejb-plugin-version</ejbVersion>
             </configuration> </plugin> ……. ……
     </plugins>
</build>
```

pom.xml of the project root should have lines similar to:

```
<modules> <module>emailconnector-
     ejb</module> …. ….
</modules>
```

Chapter 2: Avaya Breeze® platform Eclipse plug-in

Why do I see a popup message about the current maven version being lower than the minimal supported version?

Condition

The Eclipse plugin shows a warning pop-up message during snap-in deployment. An example of a message you might see is: *Current maven version 3.2 is lower than minimal maven version supported. Do you want to continue?*

Cause

The snap-in might have been built with an unsupported Maven version.

Solution

Upgrade to Maven version 3.6.3 or higher. Maven 3.9.5 is the latest at the time of this document.

Why is the “Edit System” menu option disabled?

Condition

The **Edit System** menu option is disabled if multiple System Managers are selected. Only a single System Manager can be edited at a time. However, the **Edit System** menu option is enabled even if there are multiple Avaya Breeze® platform servers/clusters within a single System Manager.

Solution

1. Select a single System Manager.
2. Click **Save**.

   After the save operation successfully executes, the **Edit System** menu option will be enabled.

Why are some of the Eclipse plugin actions disabled when I right click?

Cause

All snap-in related Eclipse plugin actions are disabled for snap-in sub-projects. Those actions are only enabled on the main (parent) project for the snap-in.

Solution

The user can select those Eclipse plugin actions by right-clicking on the main (parent) project for the snap-in.

If I have added new nodes and modify cluster name, how does the Eclipse plugin get the updated configuration from System Manager?

About this task

If you have added Avaya Breeze® platform nodes to your cluster or changed your cluster name, you sometimes won't see those changes immediately in the Eclipse Plugin. If that is the case, you need to perform the following steps.

Procedure

1. Select and save the cluster.
2. Right-click on **Cluster** in the Eclipse plug-in.
3. Select **Refresh**.

I have only modified java files with no modification in properties.xml of snap-in. Do I need to re-publish the snap-in to System Manager?

Yes, you need to re-publish snap-in to System Manager. Since the java files modified, you need to build the snap-in and deploy it (you can use Eclipse plugin “Maven clean package followed by (Re) Deploy or (Re)Deploy” action here).

Why can’t I see new functionality provided by a newer Eclipse plugin version?

Cause

It's possible that an older version of the eclipse plugin jar was maintained in a cache in the Eclipse environment.

Solution

1. Close Eclipse.
2. Delete the jar com.avaya.zephyr.eclipse.plugin from the <*Eclipse install path*>/plugins/ directory.
3. Restart Eclipse and verify that no Eclipse plugin UI and button is visible on toolbar.
4. Copy this same jar from <*unzipped SDK location*>/lib/com.avaya.zephyr.eclipse.plugin.jar to the plugins directory above.
5. Copy all the jar files from <*unzipped SDK location*>*/eclipse-bundles* to the plugins directory above.
6. Start Eclipse and verify that the plugin icon is displayed in toolbar.

My cluster list is not getting refreshed in the plugin System Manager Browser

About this task

If a user edits a cluster or adds/deletes clusters in System Manager, those changes are sometimes not refreshed in the plugin UI.

Procedure

1. Select the System Manager, right-click the entry and select **Delete SMGR**.
2. Re-add the System Manager entry, then use the menu options to view the correct, updated cluster information.

The cluster status is Green but there is a Red icon next to some of my Avaya Breeze® platform servers. Why is that?

The icons displayed adjacent to the Avaya Breeze® platform servers in a cluster indicate the availability of the server.

If an Avaya Breeze® platform server icon is red, the particular server is currently unreachable or the user credentials configured for the server are incorrect. If the credentials are incorrect, do following:

1. Select the Avaya Breeze® platform node.
2. Right-click Edit.
3. Enter the correct username and password and ssh port in the pop-up window.
4. Click Save.

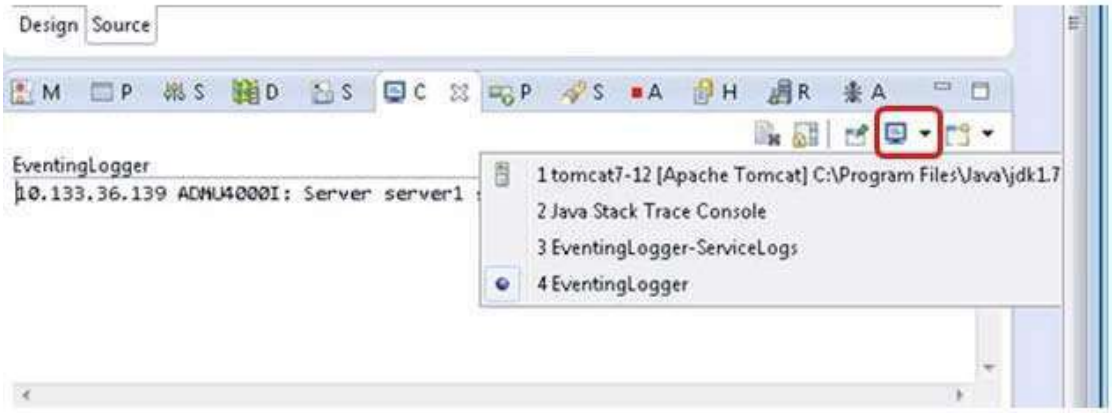
I was building the service and tailing logs, but now I can’t see any logs in the console for my other service

Cause

The Eclipse plugin uses the Standard Eclipse console to display logs, build results and status of any operations. However at times due to Eclipse plugin development limitations, the right instance of the console cannot be auto focused.

Solution

Click on the icon highlighted below to display all the console windows and select the relevant one.



I have multiple Avaya Breeze® platform servers selected in a cluster and now I enabled debug mode. Can I debug my application on multiple Avaya Breeze® platform servers?

No. The eclipse plugin by default selects the first selected Avaya Breeze® platform in the cluster and enables debug mode.

Cannot debug snap-ins on Avaya Breeze® platform node using the Eclipse plugin

Solution

1. In the Eclipse plugin, from the Avaya Breeze® platform menu, select **Enable Debug on selectedserver(s) (container will restart)**.
   This places the selected and saved Avaya Breeze® platform nodes into the debug mode.
2. To create a debug configuration in eclipse, do the following:
   a. Select **Run** > **Debug Configurations...** from the workbench menu bar.

      Or **Debug Configurations...** from the drop-down menu on the **Debug** toolbar button to display the launch configuration dialog.
   b. Select **Remote Java Application**. This is the standard debug configuration for debugging java application in eclipse.
   c. Click **New**. A new remote launch configuration is created.
   d. In the **Name** field, enter the name of the configuration.
   e. In the **Project** field, select the project that you want to debug from the workspace.
   f. In the **Host** field, enter the Avaya Breeze® platform management IP address.
   g. In the **Port** field, enter 8787.
   h. Click **Apply**.
   i. Click **Debug**.

      This opens eclipse in the Debug perspective and displays eclipse connected to the Avaya Breeze® platform node in the debug mode.

Why is the Eclipse plug-in not able to connect to Avaya Breeze® platform 3.9 and System Manager 10?

Cause

Avaya Breeze® platform Release 3.9 does not support the default cust user. System Manager Release 10.1 does not support the default admin user.

Solution

1. Edit the Avaya Breeze® platform node in the System Manager browser window of the Eclipse plug-in.
2. Edit the System Manager node in the System Manager browser window of the Eclipse plug-in.

Chapter 3: Services

Can I create a service that has Call related features and can be invoked through HTTP/REST interface?

Yes, this is possible. When you use service-archetype to create a new service, the archetype creates skeleton code which you can then modify (including renaming):

- MyCallListener.java – This provides a base file to make call related requests using the Call apis.
- MyApplication.java – This is needed if you want your service to be invoked by a REST web service. This class is needed to provide the base application path for your REST webservice.
- MyResource.java – This class contains the GET/POST/PUT/DELETE methods for your REST web service.
- MyServlet.java – This class is needed if you want to invoke a service using a servlet.

The Click to Call sample is an example of this service. More details on how to create a new service can be found in *Deploying Avaya Breeze® platform*. Look at "Trimming the Project" section as well.

How can I replace my service with newer iterations where I did not change the version number? (Lab only)

About this task

During development, you will probably go through cycles of coding and testing. For multiple iterations of your service, you do NOT need to change the service version number. You provided the version number in the Maven service-archetype when first starting development of the service. This version number is kept as the serviceVersion property in the project POM. For the "helloservice" sample service provided in the SDK, for example, the directory structure is trimmed down for context:

```
|-helloservice
|---pom.xml <- project pom
|---helloservice-ear
| --- pom.xml
| --helloservice-svar
| --- pom.xml
| --- src
| ----- main
| ------- assembly
| ------- resources
| ---------- properties.xml
| --helloservice-war
| --- pom.xml
```

This project pom contains this definition:

```
[properties]
    [serviceName]HelloWorld[/serviceName]
    [serviceVersion]0.0.0.1.5[/serviceVersion]
 [/properties]
```

You do NOT need to change the serviceVersion just to progressively add to and test your service. When developing in this mode, you may find it more convenient to replace your service on the Avaya Breeze® platform server, rather than through the System Manager interface.

These instructions assume you are merely iterating your service rather than changing the version. Note that you cannot use this approach if you have changed service attributes (in the properties.xml file) that you want to test on System Manager. You will instead need to re-install your service through System Manager. To do this, copy the SVAR from your build to your Avaya Breeze® platform server.

Procedure

On the Avaya Breeze® platform server, run this command: `deploy_service <path-to-your-svar>`.

For example, if you copied `HelloWorld-0.0.0.1.5.sva` to the `/tmp` directory on your Avaya Breeze® platform server, the command would be: `deploy_service /tmp/HelloWorld-0.0.0.1.5.svar`. The output of this command should indicate whether the service deployed successfully. You can always check using the `deploy_service –lv` command. The command `deploy_service –h` describes the command in general, including how to interpret the output of the `deploy_service –lv` command.

This approach would still require you to install your service once through System Manager. All subsequent replacements can be done with this command, as long as the service name and version remain the same.

How do I replace my service with a newer version where I changed the version number? (For production use)

About this task

If you changed the version number of your service (that is, you changed the serviceVersion property in your project pom), you will need to install the new version on System Manager.

Procedure

1. Log in to System Manager.
2. On the System Manager Home page, select **Avaya Breeze® platform** from the Elements panel.
3. In the Avaya Breeze® platform page, select **Service Management** > **Services** from the menu.
4. Load the newer version of your service. Press the **Load** button and follow the prompts.
5. After the load completes, check the radio button by the newer version of your service and press the **Install** button.

After clicking **Install**, you will be prompted to select the cluster/clusters of Avaya Breeze® platformservers where the service should be installed.

6. Choose the appropriate clusters.

   Note:

   You can also use cluster Administration screens to install services.

   You can run multiple versions of your service concurrently. You might find this useful, for example, to run the newer version with a small subset of users until you feel the service is ready to roll out to a larger community.

7. You can use the **Set Preferred Version** to achieve this. However, if you want to remove an older version of your service, find the older version of your service in the list on Service Management page, check the radio button next to your service, and press the **Uninstall** button.
8. Select the appropriate cluster/clusters from where you would like to uninstall the service.

   Note:

   You can also use cluster administration screens to uninstall services from specific clusters

9. Once uninstall completes, select your service and click **Delete**.

How do I remove/delete my service

About this task

There are 2 distinct operations for removing a service:

1. Uninstall – This step does an un-deploy of the service on all configured Avaya Breeze® platformservers but leaves entries in the database.
2. Delete – This step removes entries from the database. This means that the service will be deleted from any service profiles that included the service; you should configure users with other service profiles or add this service back to the service profiles if you decide to re-install this service.

   Warning:

   On deleting the last remaining version of a service, all the attributes are wiped out. If you want to upgrade your service rather than a true deletion and want to keep old attribute data intact, you must consider adding the new version of the service BEFORE removing the old one.

Procedure

1. Log in to System Manager.
2. On the System Manager Home page, click **Avaya Breeze® platform** from the Elements panel.
3. In the Avaya Breeze® platform page, click **Service Management** > **Services**.
4. Select your service and then click **Uninstall**.

5. When the uninstall completes, select your service and click **Delete**.
6. To verify that your service was removed, log in to the Avaya Breeze® platform server and run this command: `deploy_service -l`

Your service should not appear in the list output by this command. When you uninstall and delete a service from System Manager, System Manager propagates commands to all configured Avaya Breeze® platform servers. The time for the operation to complete will vary depending on the number of configured Avaya Breeze® platform servers, network issues, and so on. You may need to wait a minute or two and then run the `deploy_service –l` command again.

Why don't I see my (re)deployed service?

Cause

If you initially installed your service through System Manager and then later replaced it using the `deploy_service` command, it might be possible that the version changed.

Solution

1. Log in to System Manager.
2. On the System Manager Home page, select **Avaya Breeze® platform** from the Elements panel.
3. In the Avaya Breeze® platform page, select **Service Management** > **Services** from the menu.
4. Find your service and note the version.
5. In the workspace where you build your service (assuming that you used the service archetype to start your project in Maven), find the `pom.xml` file at the project level.

   Here is the directory structure of an example service (with many files and directories removed to make this explanation concise):

   ```
   |-helloservice
   |---pom.xml <- this one
   |---helloservice-ear
   | ----pom.xml
   | --helloservice-svar
   | ----pom.xml
   | --helloservice-war
   | ----pom.xml
   ```
6. Look for the serviceVersion property in this pom file. If this version differs from the version shown on System Manager, you will need to either change the serviceVersion property or install your service on System Manager.

Why do attributes defined by my service not appear under Service Globals?

Attributes provided in properties.xml of the "-svar" project must conform to the XSD. XSD is part of archive-xsd.jar in the lib directory of the Avaya Breeze® platform SDK.

If the xml is created as per XSD, it is possible that you are trying to install the same service with a new version and the following should be kept in mind while doing this:

- You cannot modify the attribute values in the new version of the service. Please add an attribute or uninstall the old version of service and delete the old version of the service before installing the new version of the service.
- Make sure to verify the “admin_visible” flag is set to “true” and “global” flag is set to “false”.
- You cannot modify the validation type “<validation name=“anyString”><type>STRING</type></ validation>”

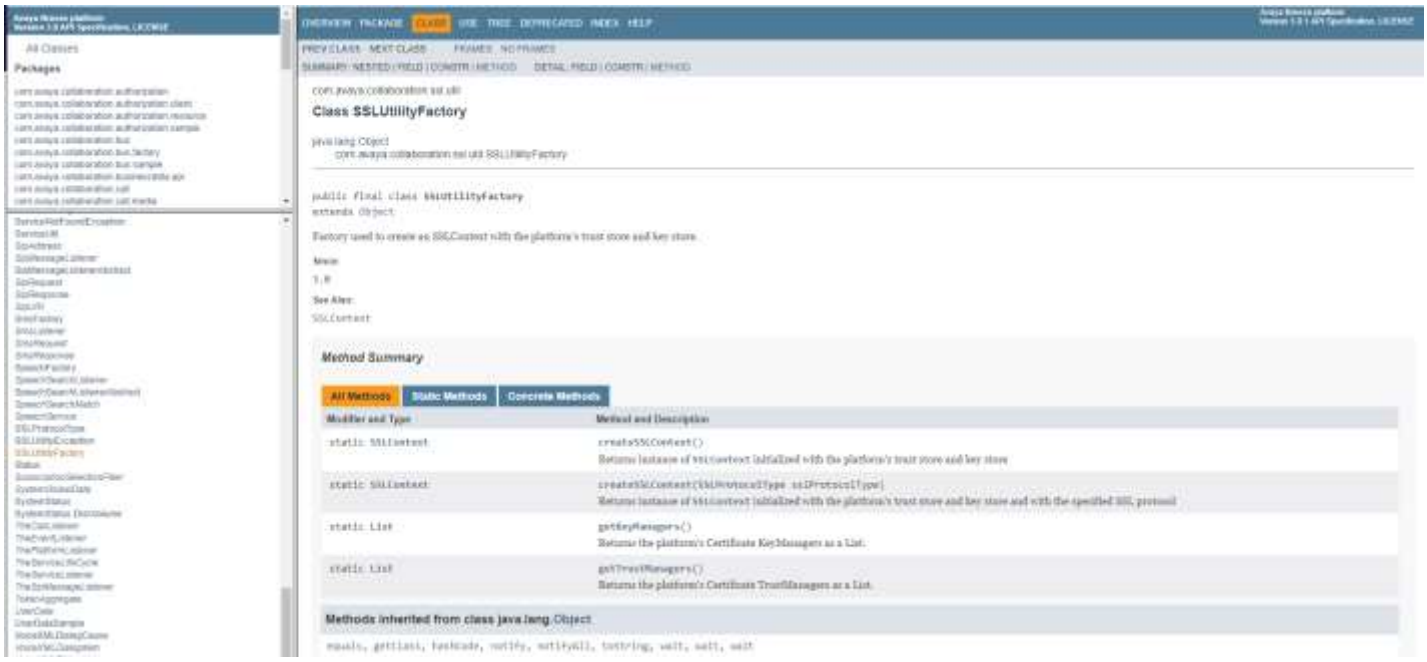
In the above, validation name of “anyString” could be used in other fields of a deployed service. So, if you change the type from “STRING” to “ENCRYPTED_STRING”, the service would not show the encrypted string. You can add a new attribute to work around this or uninstall the old version of service and delete the old version of the service before installing the new version of the service.

How can I make HTTPS requests using the WebSphere certificate from my service?

Procedure

Look at SSLUtility APIs provided in the Avaya Breeze® platform Javadoc on how to get the required certificate for making SSL connection from your service.

For more information, see the OutboundHttps Sample snap-in.



How can I define alarms in my service?

The alarms are defined in an alarms.xml file which needs to be bundled in the service archive.

```
|-helloservice
  |---pom.xml
  |---helloservice-ear
  | ----pom.xml
  | --helloservice-svar
  | ----src
  | -----  main
  | -------- resources
  | ----------- alarms.xml <- this one
  | --helloservice-war
  | ----pom.xml
```

Example

```
<?xml version="1.0" encoding="UTF-8"?>
<p:alarms xmlns:p="http://archiveschemas.aus.avaya.com/snapinalarms"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="http://archiveschemas.aus.avaya.com/snapinalarms alarms.xsd "> <p:alarm>
            <p:eventcode>EVENT_01</p:eventcode>
             <p:alarmDisplayText>Service couldn't connect to the DB.</p:alarmDisplayText>
            <p:severity>major</p:severity>
            <notificationOid>.1.3.6.1.4.1.6889.2.68.10.1</notificationOid>
  <clearFlag>true</clearFlag>
   <clearNotificationOid>.1.3.6.1.4.1.6889.2.68.10.2</clearNotificationOid>
      </p:alarm>
</p:alarms>
```

How do I define notification OID?

The SNMP Notification OID is the unique identifier for a trap/alarm. Alarms usually have two notifications OIDs: one for setting the alarm and one for resolving the alarm. Setting this field is typically not required. The only reason to set the OID would be if:

- You are not an Avaya developer and need to represent your snap-in to the SNMP manager under your enterprise/product IDs.
- You are an Avaya developer and need to represent your snap-in to the SNMP manager under your product ID.

If you do not define the Notification OID, your alarm will automatically be represented under the Avaya enterprise and the Avaya Breeze® platform (CE) product ID. If you do define a Notification OID, ensure that it is unique for your enterprise / product.

For more information on Notification OIDs, see https://en.wikipedia.org/wiki/Object_identifier

How do I define the enterprise ID and product identifier?

The SNMP Notification OID contains the enterprise ID and product ID for a trap/alarm.

“enterpriseToProductId” – Identifier starting from enterprise to product.

“enterpriseToProductIdentifier” – Identifier starting from enterprise to product. For example,

```
<enterpriseToProductId>6889.2.63</enterpriseToProductId>  <enterpriseToProductIdentifier
>avaya.products.ce</enterpriseToProductIdentifier>
<notificationOid>.1.3.6.1.4.1.6889.2.63.10.1</notificationOid>
```

This step is only required if you want to override the notificationOid value. The following is an example of how to define these fields in alarms.xml.

```
<p:organization> <p:enterpriseToProductId>123456.5.20</p:enterpriseToProductId>123456.5.20>
      <p:enterpriseToProductIdentifier>mycompany.products.sample</
p:enterpriseToProductIdentifier>
</p:organization>
```

In this example, 123456 is the enterprise number assigned to "mycompany" by IANA. 5 corresponds to "products" and 20 corresponds to "sample".

How do I define event codes?

The event code specified in the alarms.xml file must be greater or equal to 2 characters and less than or equal to 12 characters. Avaya Breeze® platform automatically prefixes the event code with the snap-in name and uses the CLR_ prefix to denote a clear event. The total string formed by combining the snap-in name and the CLR_ prefix must not exceed 32 characters.

How do I enable clearing of a defined alarm?

About this task

Alarms usually have two notifications OIDs - one for setting the alarm and one for resolving the alarm.

Procedure

If you are setting clear flag to true, make sure clearNotificationOid is uniquely defined in alarms.xml.

For example:

```
<clearFlag>true</clearFlag>
<clearNotificationOid>.1.3.6.1.4.1.6889.2.68.10.2</clearNotificationOid>
```

How do I raise defined alarms?

Procedure

1. Get the instance of Collaboration Logger (com.avaya.collaboration.util.logger.Logger).
2. Log the event using logger's logEvent API. For example, `logger.logEvent("EVENT_CODE");`.

How do I convert my Avaya Breeze® platform 3.8 service to a 3.9 service?

Before you begin

- SDK is successfully installed
- JDK 1.8 is installed.

Procedure

1. In the pom.xml present in war project, replace dependency below :

```
<dependency>
    <groupId>com.avaya.collaboration.api</groupId>
     <artifactId>avaya-aura-collaboration-api-3.8</artifactId>
     <version>3.8.1.0.381005</version>
            <scope>provided</scope>
</dependency>
```

   with

```
<dependency>
    <groupId>com.avaya.collaboration.api</groupId>
    <artifactId>avaya-aura-collaboration-api-3.9</artifactId>
    <version> 3.9.0.0.390016</version>
    <scope>provided</scope>
</dependency>
```

   The new <version> value should correspond to the latest version of the SDK that is installed on your system.

2. Replace the JRE system Library 1.7 dependency with 1.8 JRE System libraries. (if the version is prior to Breeze 3.8.x)
3. In the pom.xml for service svar project , replace the <artifactID> and <version>.

```
<artifactItem>
     <groupId>com.avaya.collaboration.api</groupId>
     <artifactId>avaya-aura-collaboration-api-3.8</artifactId>
     <version>3.8.1.0.381005</version>
```

```
<type>jar</type>
<overWrite>true</overWrite>
<outputDirectory>${project.build.directory}/tmp</outputDirectory>
<destFileName>sdk.properties</destFileName>
    <includes>META-INF/MANIFEST.MF</includes></artifactItem>
```

with

```
<artifactId>avaya-aura-collaboration-api-3.9</  artifactId>
<version> 3.9.0.0.390016</version>
```

The new <version> value should correspond to the latest version of the SDK that is installed on your system.

4. Replace the <version>.

```
<dependency>
    <groupId>com.avaya.zephyr.zephyrCommon.xsds</groupId>
    <artifactId>archive-xsd</artifactId>
    <version>2.0.2.1.202105</version>
    <exclusions>
    <exclusion>
    <artifactId>smc-api</artifactId>
    <groupId>com.avaya.zephyr.services.smc</groupId>
    </exclusion>
    </exclusions>
</dependency>
```

with

```
<version> 3.9.0.0.390016</version>
```

The new <version> value should correspond to the latest version of the SDK that is installed on your system.

5. Also need to add snippet below to the pom.xml for service svar project:

```
<validationSet>
    <dir>${basedir}</dir>
    <systemId>${basedir}/target/dependency/alarms.xsd</systemId>
    <includes>
    <include>src/main/resources/alarms.xml</include>
    </includes>
</validationSet>
```

You can add an alarms.xml file under \<workspace>\<servicename>\<servicename>-svar\sra\main\resources\alarms.xml to add dynamic snap-in alarming capability.

6. Add snippet below to dist.xml located at /<svcname>-svar/src/main/assembly/dist.xml

```
    <file>
    <source>src/main/resources/alarms.xml</source>
    <outputDirectory>/</outputDirectory>
    <filtered>true</filtered>
```

```
</file>
```

7. CARRules.xml should contain TerminatingServiceRule similar to the following
```
<TerminatingServiceRule desc="for callback to CMATestService">
    <FeatureURI>CMATestService</FeatureURI>
</TerminatingServiceRule>
```

   CMATestService is an example and it should be replaced with your service name
8. See the service archetype for Avaya Breeze® platform 3.9 for the appropriate sip.xml and web.xml files.
   There are new servlets, which are required for services to function correctly. You can also refer to Multichannel Broadcast sample application to see how the sip.xml and web.xml look as of Release 3.9.

How do I access third-party services and APIs that require a secure (i.e., HTTPS or TLS) connection?

About this task

When connecting to services that require a secure connection, you will need to import the proper trust certificates into the Avaya Breeze® platform trust store. This applies to any external services, such as REST APIs over HTTPS, email servers using TLS, etc. The exact procedure to obtain the required trust certificates will vary.

Procedure

1. Log in to System Manager and navigate to the Avaya Breeze® platform page.
2. Select the cluster where your service is deployed and click on the **Certificate Management** dropdown.
3. Click **Install Trust Certificate (All Avaya Breeze® platform Instances)**.
4. In the **Select Store Type to install certificate** dropdown, select **WEBSPHERE**.
5. Click **Browse** and navigate to the saved copy of the trust certificate.
6. Click **Retrieve Certificate** to upload the certificate to System Manager.
7. Verify the details of the trust certificate displayed, then click **Commit** to upload the trust certificate to each Avaya Breeze® platform in the selected cluster.

Do I need an extra attribute in properties.xml to mark my snap-in as a callable service?

No extra attribute is needed in properties.xml, Callable service can be written like any other snap-in.

What is trusted hosts per cluster?

“Trusted Host” is the authentication mechanism currently supported for HTTP requests. There are two aspects to trusted host validation. A “whitelist” of trusted IP addresses of IP network addresses can be provisioned by the administrator on the Avaya Breeze® platform Element Manager. For example, valid configuration values can be 10.10. 1.10 or 192.168.10.0/24. Also, this whitelist can be enabled or disabled. A disabled whitelist means that requests from all servers will be allowed. Client Certificate Challenge/Validation (Mutual TLS) – If configured to do so Nginx will challenge an incoming request to open a TLS session. Upon receiving the challenge, the client machine must provide a valid certificate that has been signed by a trusted Certificate Authority. Mutual TLS is a requirement for certificate-based whitelist enforcement and is optional for IP address-based whitelist enforcement. Similarly, under the HTTP CORS, the administrator can specify a source server IP or hostname (with or without port as needed) for Cross-origin resource sharing. The functionality is now extended at the cluster level, so the administrator can make a cluster-specific trusted hosts assignment. A trusted host can access HTTP(S) resources on clusters where it has been configured as a trusted host.

Can the administrator assign trusted hosts to a legacy cluster?

Yes. The Cluster drop-down will list all the 3.8, 3.9 (or later versions) of clusters along with a “Legacy” option. Any Trusted hosts assigned to the “Legacy” cluster option, will implicitly assign the Trusted hosts to all pre-3.8 clusters. The administrator will not be able to assign separate Trusted hosts for each of the Legacy clusters. For instance, if there are Cluster A and B having pre-3.8 clusters, the administrator will not be able to assign say Trusted host X and Y to Cluster A and B, respectively.

The administrator will have to select the “Legacy” cluster option, and assign Trusted host X and Y, which will implicitly assign it to Cluster A and B.

Why does my snap-in encounter "SSLUtilityException (TLS version for Service cannot be lower than Default version)" when it calls createSSLContext API?

Starting Avaya Breeze® platform Release 3.3, when a snap-in invokes `createSSLContext(SSLProtocolType sslProtocolType)` API, platform checks that if the SSLContext version requested by the snap-in is not lower than that of minimum TLS version set by administrator.

For example, if a snap-in invokes `com.avaya.collaboration.ssl.util.SSLUtility.createSSLContext(SSLProtocolType.TLS)` and the minimum allowed TLS version is set to TLSv1.2 by administrator then snap-in will encounter `"SSLUtilityException (TLS version for Service cannot be lower than Default version)"`

To get rid of this exception, use one of the following methods:

- Snap-in code needs to make sure that it is requesting TLS version which is equal or higher than minimum allowed TLS version set for the snap-in.
- Administrator can reconfigure minimum allowed TLS version for the snap-in from the Cluster editor page.

When my snap-in sends an HTTP response, Avaya Breeze® platform adds security headers. How can one customize the value of the headers?

Avaya Breeze® platform adds the following security headers with pre-defined values to every HTTP response from snap-ins:

- Strict-Transport-Security
- X-Content-Type-Options
- X-XSS-Protection
- Cache-Control
- Pragma
- Expires

Snap-ins must not override the default values.

If the snap-in has a reason to override one of the above headers with its own value, it can do so. The platform will leave the contents of these headers intact if the snap-in already populated them.

As an ISV, how can I configure snap-ins to efficiently process customers' varying dial plans?

In Avaya Aura®, that the format of calling and called party numbers depend on the type of endpoint and the administration of the elements. The number reported as the alerting or answering party might be different than the number of the called party.

The mitigation of the problems because of the different calling and called party number formats can be done by using one of the following two methods:

- Using the E.164 format universally, which might be an impractical option for some customers.
- Using Session Manager Adaptation Modules. Administrator can define an adaptation modules to convert all calling and called party numbers in messages to and from Avaya Breeze® platform to the E.164 format.

Why cannot a snap-in gain access to UCIDs of a call created by another snap-in?

Most snap-ins the use the Avaya Breeze® platform Call Manipulation API are native SIP applications of Avaya Breeze® platform. The SIP applications process SIP signaling paths in the following ways:
- Snap-ins can be invoked as a Call Intercept application for calls destined for a different person or application
- Snap-ins can be invoked as a Callable application for calls that are explicitly addressed to the snap-in
- Snap-ins can initiate outbound calls

Snap-ins can perform call and media operations on calls in which they were not directly involved using SIP signaling. Avaya Breeze® platform provides a snap-in called CallEventControl. The CallEventControl snap-in is invoked before Call Intercept snap-ins. The snap-in:

- Sends asynchronous call events that snap-ins can monitor.
- Receives call control requests from other snap-ins.

Snap-ins can be explicitly sequenced to initiation action on a call the call reaches its intended destination. Avaya Breeze® platform has the following limitations on sequencing snap-ins:

- CallEventControl is not sequenced on outbound calls from Avaya Breeze® platform
- CallEventControl is not sequenced on calls to Callable services
- CallEventControl does not support media operations

You can mitigate these Avaya Breeze® platform limitations by:

- Configuring snap-in A to send requests to snap-in B to initiate actions on calls.
- Configuring snap-in A as a sequenced Call Intercept snap-in for calls initiated by snap-in B.

Why is my service being invoked again after I call removeServiceFromCall?

Condition
A Call Intercept snap-in invokes ServiceManager.removeServiceFromCall. The snap-in immediately sees callIntercepted invoked again for the same call.
Cause
The following two conditions can cause the invocation of the service:

- The snap-in is a Calling Party Call Intercept snap-in
- Such snap-ins cannot currently use removeServiceFromCall.
- The snap-in is a Called Party Call Intercept snap-in and the Implicit User administration for Session Manager is too general

Solution
Ensure that no Calling Party Call Intercept snap-ins are invoking the removeServiceFromCall operation. If there are Called Party Call Intercept snap-ins, ensure that a specific domain is specified in the Implicit User pattern in Session Manager administration rather than using the default of -ANY-.

Chapter 4: Service debugging

Why did I get “Invalid Class Name, the Class Name does not exist in the Jar File.” error message?

Cause

The error “Invalid Class Name, the Class Name does not exist in the Jar File” usually occurs when an incorrect JDBC driver implementation class name has been provided.

Solution

The user needs to input correct JDBC driver implementation class which exists in jar file in order to avoid this kind of error.

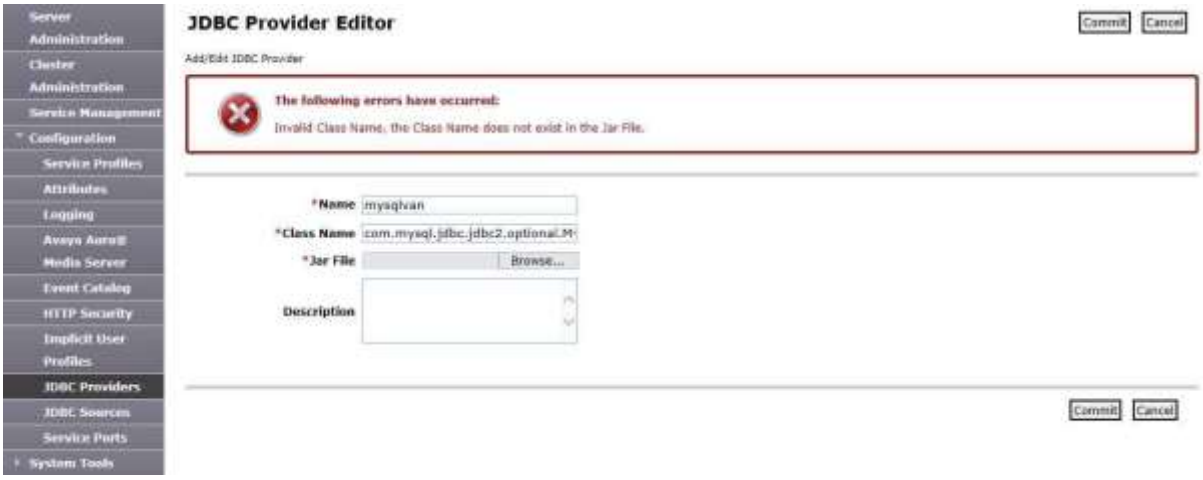
The name of the class file in the driver jar that implements the javax.sql.DataSource interface. The actual class name might differ per the uploaded driver jar.

For example:

For Postgres, you can enter org.postgresql.xa.PGXADataSource.

For MySQL, you can enter com.mysql.jdbc.jdbc2.optional.MysqlXADataSource or com.microsoft.sqlserver.jdbc.SQLServerXADataSource.

For Oracle, you can enter oracle.jdbc.xa.client.OracleXADataSource or oracle.jdbc.pool.OracleConnectionPoolDataSource.



Why aren't my JDBC Providers in the drop-down on the data source editor page?

Cause

There is a two-step process to create a JDBC provider:

1. You first need to create a JDBC provider with appropriate input.
2. As soon as you click on the Commit button, a JDBC provider snap-in will be created and loaded.

Create JDBC provider and install JDBC provider snap-in from the Service Management page. After successful creation of JDBC provider, you will see that the JDBC provider snap-in will be loaded on the Service Management page.

In order to see the created JDBC provider in the drop-down on the JDBC data source page, you need to follow the steps below.

Solution

1. Find the JDBC provider snap-in created on the Service Management page.
2. Select the JDBC provider snap-in on the Service Management page.
3. Click **Install**. After successful installation, you will see the created JDBC provider in the drop-down.

Can I create two JDBC providers with the same name?

Solution

No, the user cannot create JDBC providers with the same name.

Can I create two JDBC data sources with same JNDI name on the same cluster?

Solution

No. the user cannot create two JDBC data sources with the same JNDI name. The JNDI name of the data source should be unique for the cluster.

Can I create multiple JDBC data sources for a single JDBC provider?

Solution

Yes, the user can create multiple JDBC data sources associated with single JDBC provider.

Where do I check JDBC Data source Test Connection result?

Solution

Click the **Status** icon that appeared on JDBC Data Sources after Test connection successful.

Why is the JDBC Source setting not reflected? Even after I changed the JDBC data source attributes, it is giving same error/result

Condition

Sometimes the changes made in JDBC data source will be not reflected.

Cause

This type of problem occurs when the changes made in the JDBC data source attributes are not reflected in the backend Avaya Breeze® platform server.

Solution

Restart Avaya Breeze® platform servers after committing any changes in JDBC data source to avoid this kind of error.

Why am I unable to uninstall/delete JDBC providers from the Service Management page?

Cause

Before uninstalling JDBC provider, the user needs to remove all associated JDBC data sources from JDBC sources page. After successfully remove data sources, user can uninstall JDBC provider.

The JDBC provider snap-in will be deleted directly from the Service Management page. The user can delete JDBC provider from the JDBC providers page, which will delete/unload JDBC provider snap-in from the Service Management page.

Solution

1. On the System Manager Home page, select **Avaya Breeze® platform** from the Elements panel.
2. Select the **Service Management - Services** button, then click the **Filter Enable** tab .
3. Select the required file and click the **Uninstall** button.
4. Click the **Delete** button to delete the file.

Why am I getting the error “com.mysql.jdbc.Driver incompatible with javax.sql.ConnectionPoolDataSource” on the Test connection?

Condition

Even if JDBC provider and data sources are created successfully, the user is not able to see Test connection success.

Cause

Sometimes user get above error if user provides wrong JDBC driver implementation class.

Solution

To avoid this kind of error, user can modify JDBC provider to input correct JDBC driver implementation class name.

1. Select the JDBC provider which you want to edit and click on the **Edit** button on that page.
2. You will be redirected to the JDBC provider editor page where you can edit and specify the appropriate driver implementation class.
3. Click on the **commit** button.
4. Click on the **JDBC Sources** button and select a JDBC data source having the JDBC provider you specified.
5. Click on the **Test Connection** button to check the status.

Why am I getting simply “ERROR” error message on Test Connection?

Condition

A simple “ERROR” message is displayed while creating the JDBC Data Source.

Cause

It is due to the inappropriate url specified while creating the JDBC Data Source.

Solution

To avoid it, user can provide appropriate JDBC data source URL.

Why does my data source not work even with the correct configuration?

Condition

The data source does not work.

Cause

Sometimes attributes cannot be fetched by drivers. If that isn't the problem, the database is either not reachable or the database firewall configuration does not allow it to accept connection from Avaya Breeze® platform host.

Solution

Add following explicit custom properties (sometimes these attributes could not be fetched by drivers.)

- Property name: serverName Property Value:*<Server IP>*
- Property name: databaseName Property Value:*<Server IP>*
- Property name: portNumber Property Value:*<DB port>*
- Property name: user Property Value:*<DB user id>*
- Property name: password Property Value:*<DB password>*

How can I tell if my service got installed properly?

About this task

A service is installed from System Manager. System Manager will propagate the service to all configured Avaya Breeze® platform servers, and an audit running on a Avaya Breeze® platform server will deploy the service. On each Avaya Breeze® platform server, the service is deployed.

Note that some time is required for System Manager to propagate the service to all Avaya Breeze® platform servers, so this operation takes longer in larger systems with more Avaya Breeze® platform servers. But, in general, the service should deploy within a couple minutes of installing it on System Manager.

Procedure

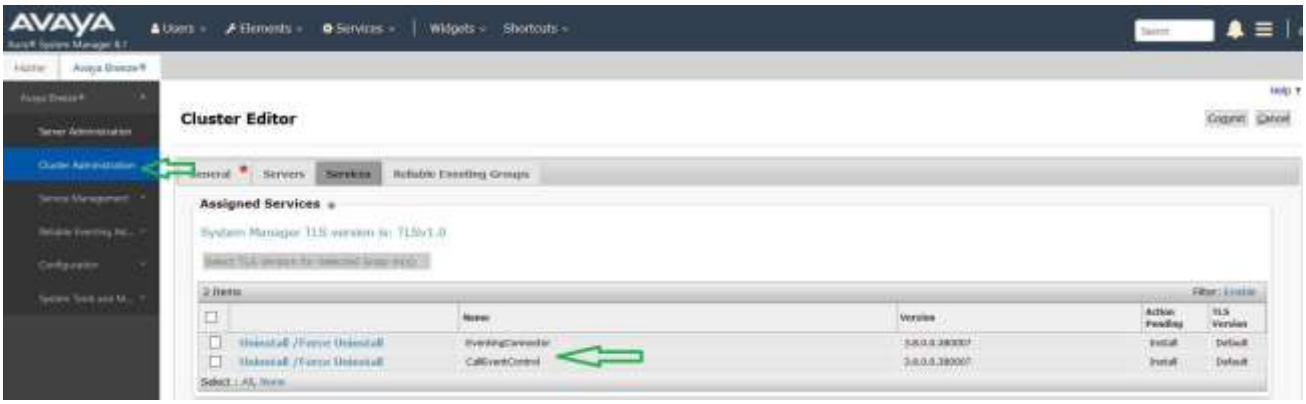
1. Log in to System Manager.
2. On the System Manager Home page, select **Avaya Breeze® platform** from the Elements panel.
3. In the Avaya Breeze® platform page, select **Server Administration** from the left menu.

   You will see a red cross in the Service Install Status column.

4. Click on the red cross and you will be taken to the Service status page for the server.

   The Service install status column on this screen will provide information on which service failed to install on Avaya Breeze® platform.

5. If you are using cluster administration to install the services, as in screen below, make sure that your service is shown in the installed services list and appropriate servers are selected in the Servers tab.



6. If your service is in the Installed state according to System Manager, log in to your Avaya Breeze® platform server and run this command: `deploy_service -lv`

   The output will look something like this:

   `load: + deploy: + run: + car: N HelloWorld-0.0.0.1.3`

   `load: + deploy: + run: + car: + basicSipCall-1.0.0.0.0`

   In this example, the service basicSipCall shows a plus (+) for each step of the deployment, so is installed and ready to go. The service HelloWorld deployed but failed the “car” step of the deployment (“N” indicates the step failed), which means that the service will not be invoked.

   You can get an explanation of the `deploy_service` command by asking for help: `deploy_service -h`

7. If your service is in the list produced by the deploy_service –lv command, but has an “N” for any step, try manually redeploying the service – the output of that may provide a clue as to why the service failed a step: deploy_service <SVAR file>

   When you installed the service from System Manager, the service archive (SVAR) was propagated to all configured Avaya Breeze® platform servers. The copy of the SVAR resides in /var/avaya/aus_svars. You can find your SVAR by running this command:

   ls /var/avaya/aus_svars/

   The output will be something like this:

   basicSipCall-svar-1.0.0.0.0-SNAPSHOT.svar helloservice-svar-0.0.1-SNAPSHOT.svar

Why my service is not installed even after I created a cluster and added my service in the cluster?

Procedure

1. Select the cluster that was created and click **edit**.
2. Go to Servers tab and make sure that Avaya Breeze® platform servers are added in cluster.

Why do I have to manually select my service for installation while creating a cluster especially since I can see some services which are already selected for installation?

Services that appear to be added automatically are all mandatory services defined for that particular cluster. There is no mechanism to define your service as a mandatory service so it needs to be added manually to get it installed.

How can I find why my service installation failed?

Solution

1. Logon to your Avaya Breeze® platform server and try manually redeploying the service through command line – the output of that may provide a clue as to why the service failed a step:

   deploy_service <SVAR file>

   When you installed the service from System Manager, the service archive (SVAR) was propagated to all configured Avaya Breeze® platform servers. The copy of the SVAR resides in /var/avaya/aus_svars.

2. You can find your SVAR by running this command: ls /var/avaya/aus_svars/

   The output will be something like this: basicSipCall-svar-1.0.0.0.0SNAPSHOT.svar helloservice-svar-0.0.1-SNAPSHOT.svar
3. In-order to redeploy a command similar to this can be executed: deploy_service /var/avaya/aus_svars/helloservice-svar-0.0.1-SNAPSHOT.svar
4. If the re-deploying of service from command line does not provide obvious hints on deploy failure, run this command: ce dlogv
   This will open the debug log using the vi editor.
5. Search for your service name.
   This should provide you with information if there were any exceptions that lead to failure in installing your service.
6. If you added logging statements in your service code, you should be able to spot your log statements in the debug log.
7. If you used the Logger class in the Avaya Breeze® platform API (highly recommended), you can view the service log using the command ce dlogv <servicename>.
   For example, to view the logs for the basicSipCall service, run the following command -ce dlogv basicSipCall.
   The logs for different versions of a service all go to the same log file, and each log message contains the service name and version.
   When running in normal mode, logs at level INFO and higher priority (FATAL, ERROR, WARN) will be added to the log file; logs at lower priority (FINE, FINER, FINEST) will not be added to the log. The log level can be changed on the fly to provide more verbose logging.
8. Enter this command while logged in to your Avaya Breeze® platform server to enable all log levels: ce dlogon <servicename>
9. When you are finished debugging, you should return logging to the default using this command: ce dlogoff <servicename>

   Default logging (sysout or syserr) goes to a different log. If you are using Java "system.out.println (not recommended)", the text will be written to the default log.
10. Enter this command to view the log in the vi editor: ce alogv

How can I tell if my service is running or gets invoked?

Procedure

1. Log in to your Avaya Breeze® platform server and run this command: deploy_service

   -lv The output will look something like this:

   load: + deploy: + run: + car: N HelloWorld-0.0.0.1.3

   load: + deploy: + run: + car: + basicSipCall-1.0.0.0.0

If your service is in the list and shows a plus (+) for each step, it is installed and ready to go. You can run the command deploy_service –h to get more detail about the output of the deploy_service –lv command.

If the car is “N” for a call related service, make sure that the service name and service version is exactly same in sip.xml as well as web.xml. Also, make sure the sip servlets match in both sip.xml and web.xml.

2. The framework will log that it has deployed, registered, and initialized your service. On your Avaya Breeze® platform server, run this command: ce dlogv

   This will open the debug log using the vi editor. Search for the string “initialization complete for”. The full log string will include your service name and version, so as an alternative you could search for your service name.

   If you added logging statements in your service code, you should be able to spot your log statements in the debug log. If you used the Logger class in the Avaya Breeze® platform API (highly recommended), you can tail/watch the service log using the command ce dlogw<servicename>

   For example, to tail the logs for the basicSipCall service, run the following command: ce dlogw basicSipCall.

Why is my service not getting invoked

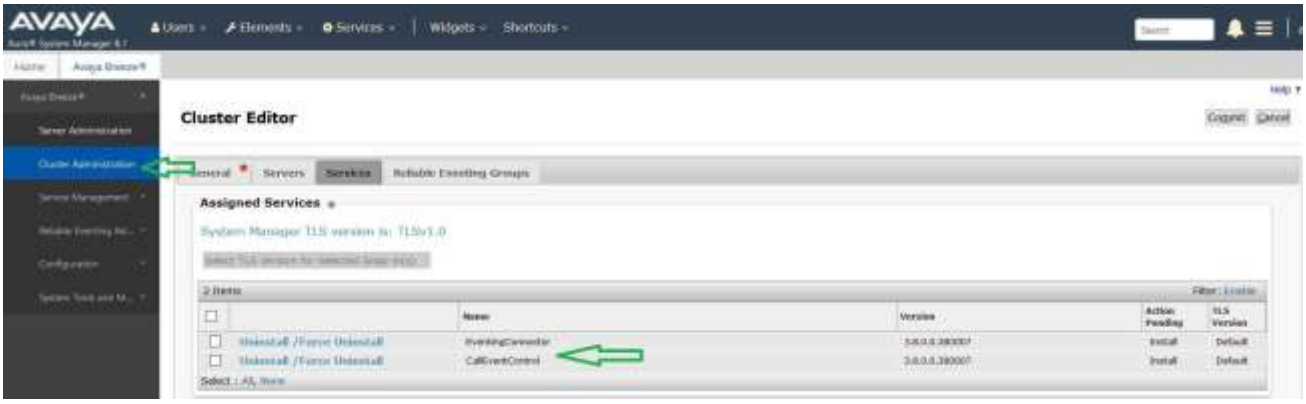
Cause

Your Avaya Breeze® platform server might not be in the state to accept service.

Solution

1. On the System Manager Home page, select **Avaya Breeze® platform** from the Elements panel.
2. Pick the radio button next to your Avaya Breeze® platform server.
3. Click the **System State** button to pull down the menu, and then select **Accept New Service** from the drop-down menu.
4. Verify that your service is installed.
5. Log in to System Manager.
6. On the System Manager Home page, select **Avaya Breeze® platform** from the Elements panel.
7. In the Avaya Breeze® platform page, select **Service Management** > **Services** from the menu.
8. Find your service.
9. If your service does not appear in the table, press the **Load** button to load the SVAR you created when building your service.
10. If the State for your service is Loaded, select the checkbox and press the **Install** button.

11. If you are using cluster administration to install the services, as shown in screen below, make sure that your service is shown in the installed services list and appropriate servers are selected in the servers tab.



12. Also, verify that the preferred version is set for your cluster and the service is installed in the cluster.
13. Click the **General** tab on the Cluster Editor page.
14. Verify that the Cluster attributes for **HTTP or HTTPS traffic rate limit in bytes/sec** and **HTTP or HTTPS limit on connections** are set up appropriately to handle load for your service.
15. If your service is in the Installed state, log in to your Avaya Breeze® platform server and run this command: `deploy_service -lv`

    The output will look something like this:

    `load: + deploy: + run: + car: N HelloWorld-0.0.0.1.3`

    `load: + deploy: + run: + car: + basicSipCall-1.0.0.0.0`

    Service with call related features:

    - If your service is in this list and shows a plus (+) for each step, it is installed and ready to go.
    - If the car is “N” for a call related service, make sure that the service name and service version is exactly same in sip.xml as well as web.xml. Also, make sure the sip servlets match in both sip.xml and web.xml.

    HTTP service with no call features:

    - If your service is in this list and shows a plus (+) for load, deploy and run step, it is installed and ready to go.
16. To verify that replication is working, from the Home tab on System Manager, select **Replication** from the Services panel to display the Replication tab.
17. Look for a Avaya Breeze® platform Replica group in the table.
18. If the Synchronization Status is not “Synchronized”, check the checkbox for the row and press the **View Replica Nodes** button.

    It takes about 1 minute a maximum to replicate data once it is changed in System Manager.

    Note that you could press the **Repair** button here to attempt to repair all servers in the replica group, rather than go to the next page to repair a specific server. Be aware that the

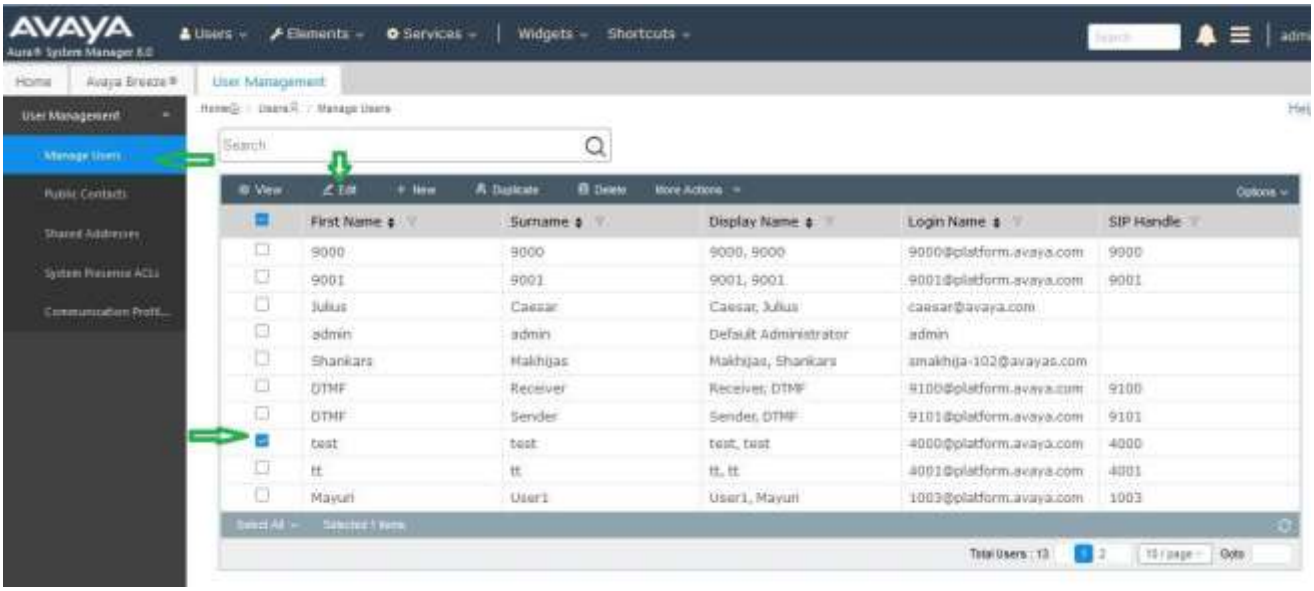
Repair operation is service affecting, which means that calls will fail until the operation completes (usually just a few minutes).

If you pressed the **View Replica Groups** button, you will be in a page that lists the nodes within that Replica Group.

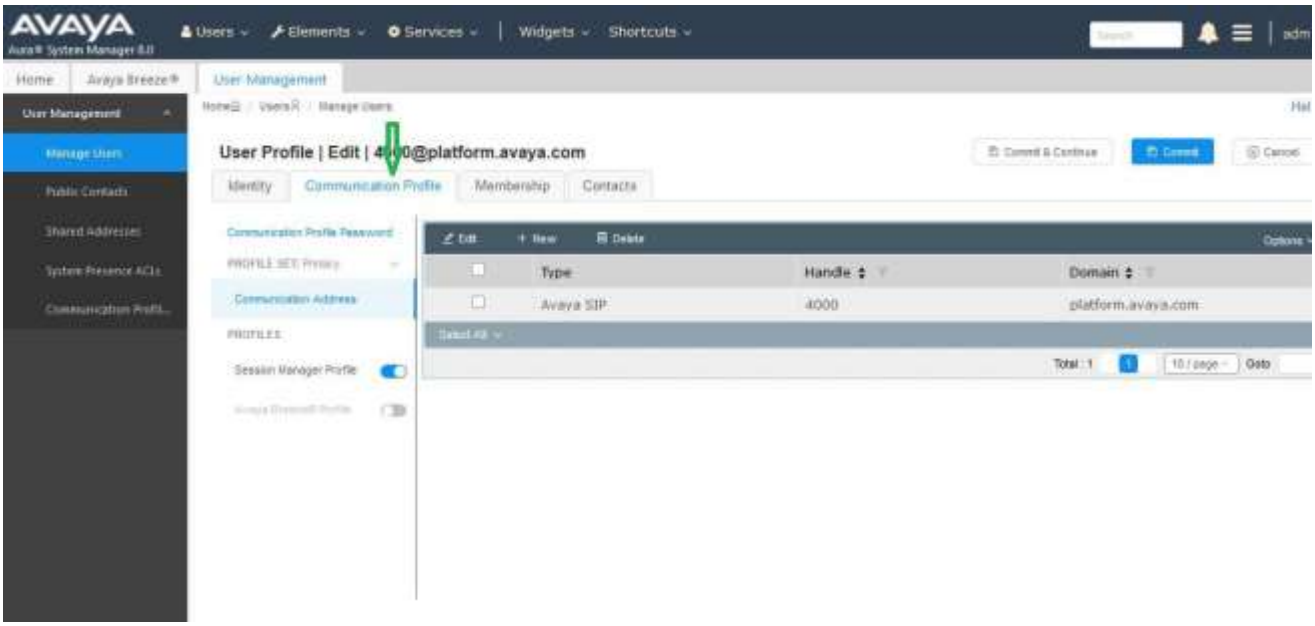
19. Check the checkbox next to your server and press the **Repair** button.

    Be aware that the Repair operation is service affecting, which means that calls will fail until the operation completes (usually just a few minutes).

20. For a Service with Call related features check the following as well:
    a. To check the service profile definition, on System Manager, in **Elements**, click **AvayaBreeze® > Configuration > Service Profiles**.
    b. If you do not see the profile for your service, press the **New** button to define a new service profile. Otherwise, select the radio button next to your service profile and press the **Edit** button (as a shortcut, you could simply click the link for your service profile).
    c. If you do not recognize any of the service profile names, you may need to view each service profile until you find one that includes your service. You might also find it easier to look at a target user's service profile configuration first (instructions just below here) to find the service profile name.
21. The Service Profile Editor page shows the profile at the top, and the list of installed services at the bottom:
    - To add a service to the profile, click the plus (+) icon next to the service in the bottom table; you should then see the service in the profile in the top table.
    - To remove a service, click the X icon next to the service in the top table.
22. To check the user's application sequence and service profile configuration, on System Manager in **Users**, click **User Management > Manage Users**.
23. Each user to which the service is to be applied must have the service profile assigned to it. Find a user from the list, click the checkbox for that user, then press the **Edit** button.



24. In the User Profile Edit page, select the **Communication Profile** tab.



25. If you made changes to this user that you want to keep, press the **Commit** button at the top or bottom of the page. Otherwise, press the **Cancel** button at the top or bottom of the page.
26. Make sure sequencing is administered on the Session Manager Implicit User Rule Editor page for an individual or group of users.

    As a best practice, select both sequences, in which case Avaya Breeze® platform is invoked when the user either makes a call or receives a call. At a minimum, if you have a Calling Party service, ensure that there is an Origination Application Sequence that includes Avaya Breeze® platform. If you have a Called Party service, ensure that there is a Termination Application Sequence that includes Avaya Breeze® platform.

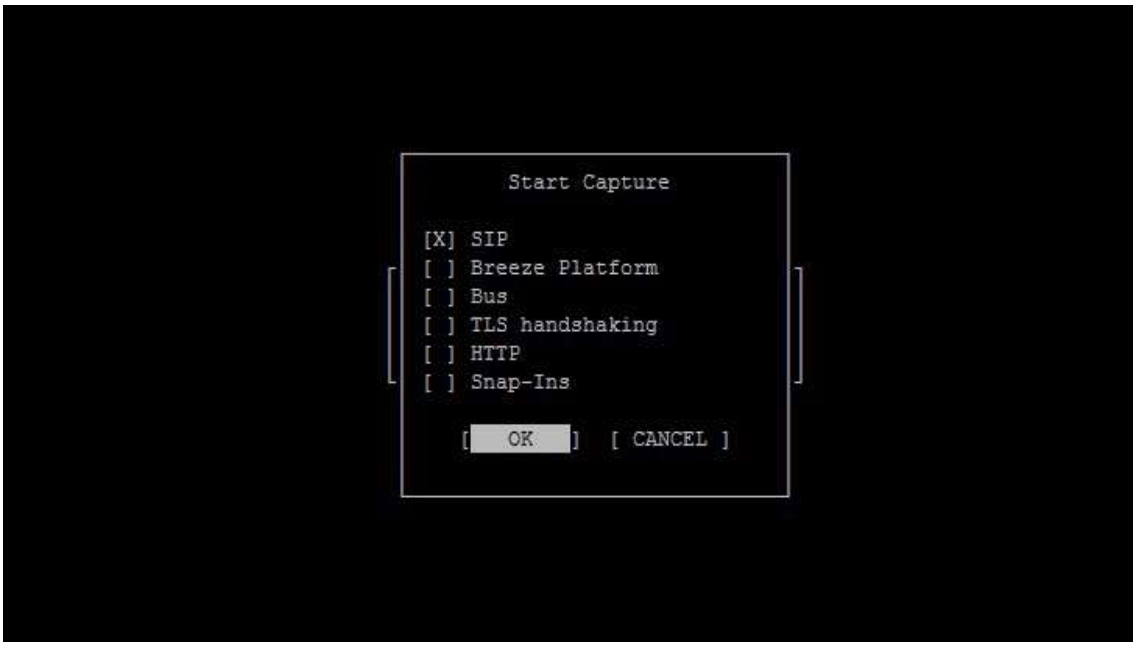
27. Navigate to **Home > Elements > Session Manager > Application Configuration > Implicit Users** and click the user or group you want to set up to receive Avaya Breeze® platform services.

    Enable implicit users applications for sip users should be enabled from session manager administrator.

28. Select your Avaya Breeze® platform Application Sequence for both Origination Application Sequence and Termination Application Sequence.
29. To save your changes, click Commit.

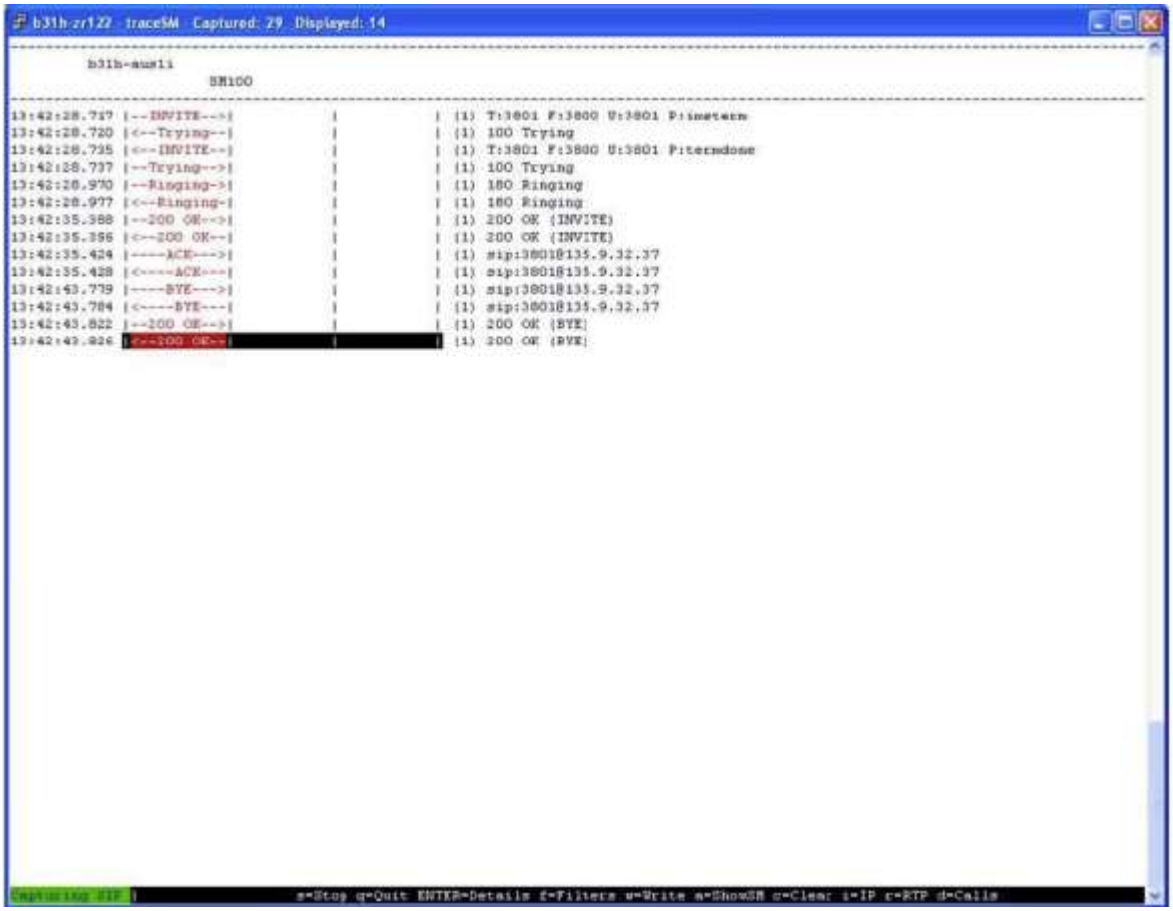
    For more details, refer to the document *How to Install, Configure, and Test an Avaya Breeze® platform Service*.

30. Verify that traffic is hitting your Avaya Breeze® platform server. For this edition of Avaya Breeze® platform 2.0, the supported underlying communication protocol is the Session Initiation Protocol (SIP), as defined in IETF RFC 3261 and associated RFCs. Avaya Breeze® platform has a tool to capture and analyze traffic. Run this command: `traceMsg`
31. When prompted, press `s` to start the capture.
32. You will then be prompted to select the type of traffic – just hit `Return` at this point to take the default.



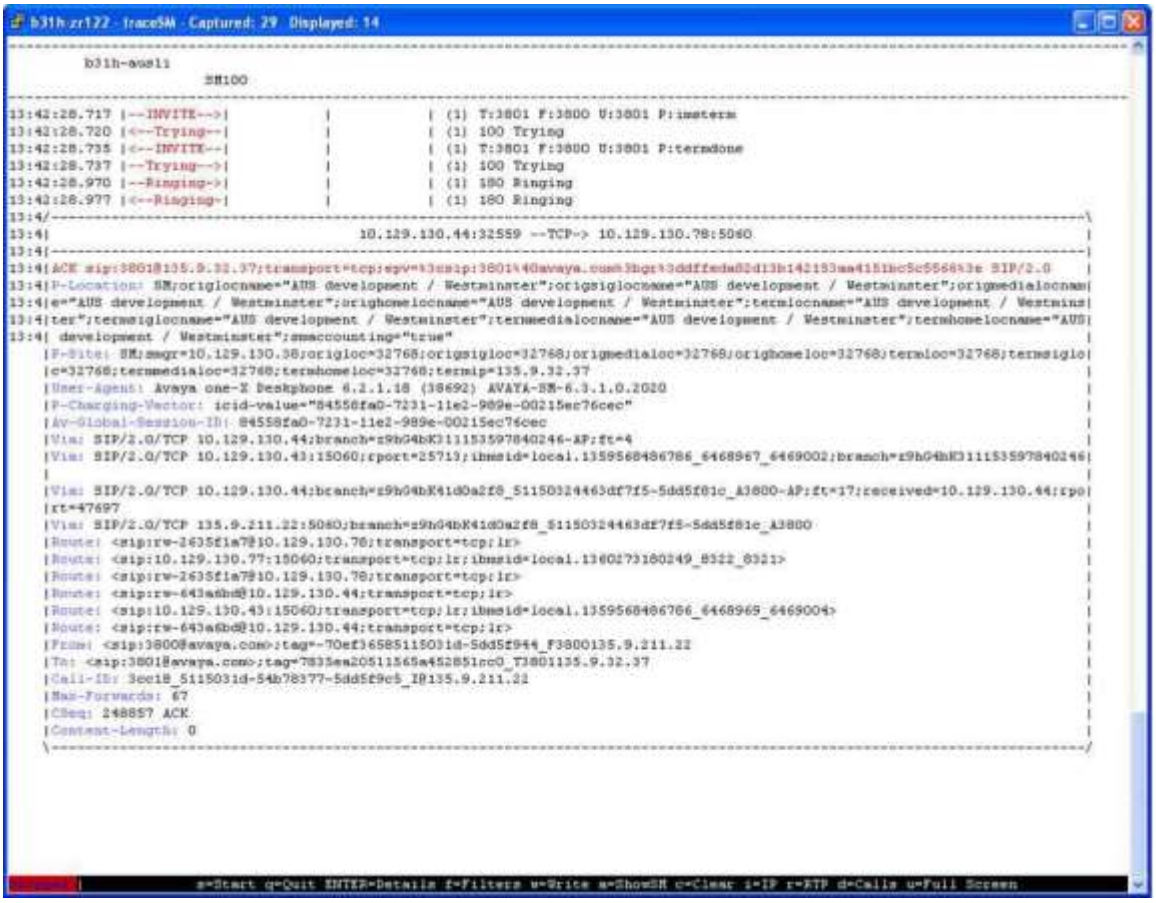
33. Place a call.

    You should see a fencepost diagram develop that shows the messages exchanged between the Avaya Breeze® platform server and other entities. Here is an example of a simple call, where user A called user B, user B answered and then user A dropped:



Note the menu along the bottom – you may want to stop the trace collection after you have made your test call to limit the amount of data captured.

This trace shows 2 entities involved in the signaling: b31h-ausl1 is a Session Manager, and SM100 represents the Avaya Breeze® platform server. Signaling is usually routed from Session Manager to Avaya Breeze® platform and then back to Session Manager. You can use the arrow keys to move up and down through the message sequence. If you press the Enter key, the highlighted message will be expanded.



If you start traceMsg and do not see any traffic from your test call, and the Origination/ Termination Sequences that we checked above are correct and you placed your Avaya Breeze® platform server into the “Accept New Service” state as described above, then you will need to check other configuration on System Manager. Refer to the document *Quick Start to deploying the HelloWorld Snap-in*.

If the trace shows traffic, then check that the users in the call have the correct service profile, as described above.

Both Avaya Breeze® platform and Session Manager monitor the signaling pipes between each other.

34. To check the link monitoring status, on System Manager in **Elements**, click **Session Manager > System Status > SIP Entity Monitoring**.
35. Click the Session Manager.

    If the Session Manager in your environment shows any entities in the Down or Deny state, further inspection is warranted. In this example, the Session Manager named vf-zr120 shows an entity link as down. Clicking the link on the name opens a page that shows the status of the individual entity links.

The Reason Code column provides the clue. Refer to Session Manager documentation for resolution instructions. A tip: a Reason Code of 503 on the link to the Avaya Breeze® platform server probably indicates that the Avaya Breeze® platform server is not in the state to Accept New Service.

More troubleshooting for a Service invoked through HTTP

1. Verify that the URL used to access the service is of the form:

   http://[Breeze_FQDN_or_IP]/services/servicename/[Service_Specified_Pattern] or

   https://[Breeze_FQDN_or_IP]/services/servicename/[Service_Specified_Pattern] or

   http://[Breeze_FQDN_or_IP]/services/servicename-serviceversion/

   [Service_Specified_Pattern] or

   https://[Breeze_FQDN_or_IP]/services/servicename-serviceversion/

   [Service_Specified_Pattern]

   - Breeze FQDN or IP is the Security Module hostname or IP address as configured on System Manager. For example, if you have Multichannel Broadcast Sample service installed on Breeze, it can be invoked as:

     http://10.10.10.100/services/MultiChanBroadcastService /

     MultiChanBroadcastServlet or

     https://10.10.10.100/services/MultiChanBroadcastService /

     MultiChanBroadcastServlet

   - MultiChanBroadcastService – this is the service name
   - The above URLs for Multi-Channel broadcast will invoke the preferred version of the service installed on Avaya Breeze® platform. For example, if you have 2.0.0.0.13002 installed and also 2.0.0.0.13003 on Breeze, the above example URL will invoke 2.0.0.0.13003 version of the application.
   - If you wish to invoke 2.0.0.0.13002 specific version of the example service above, the URL would look like:

     http://10.10.10.100/services/MultiChanBroadcastService-2.0.0.0.13002/

     MultiChanBroadcastServlet or

https://10.10.10.100/services/MultiChanBroadcastService-2.0.0.0.13002/MultiChanBroadcastServlet

- The preferred version of service can also be invoked using the format of servicenameserviceversion in the URL, e.g.:

  http://10.10.10.100/services/MultiChanBroadcastService-2.0.0.0.13003/MultiChanBroadcastServlet or

  https://10.10.10.100/services/MultiChanBroadcastService-2.0.0.0.13003/MultiChanBroadcastServlet

2. Login to Avaya Breeze® platform server and run this command on command line: `ce dlogv`

   This will open the debug log using the vi editor.

3. Search for your service name.

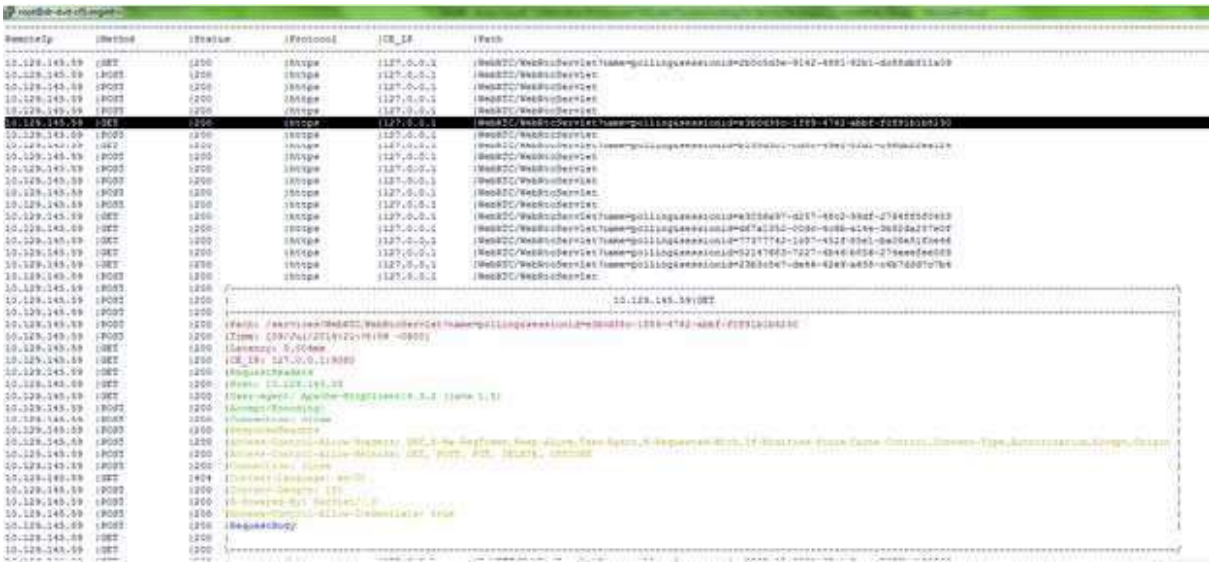
   This should provide you with information if there were any exceptions that lead to issues with invoking the service.

4. If you added logging statements in your service code, and if you used the Logger class in the Avaya Breeze® platform API (highly recommended), you can view the service log using the command `ce dlogv <serviceName>`.

   For example, to view the logs for the basicSipCall service, run the following command -`ce dlogv basicSipCall`. The logs for different versions of a service all go to the same log file, and each log message contains the service name and version.

5. When running in normal mode, logs at level INFO and higher priority (FATAL, ERROR, WARN) will be added to the log file; logs at lower priority (FINE, FINER, FINEST) will not be added to the log. The log level can be changed on the fly to provide more verbose logging. Enter this command while logged in to your Avaya Breeze® platform server to enable all log levels: `ce dlogon`.
6. To enable all log levels for a specific service use `ce dlogon <serviceName>`
7. When you are finished debugging, you should return logging to the default using this command: `ce dlogoff` or `ce dlogoff <serviceName>` for a specific service.
8. Default logging (sysout or syserr) goes to a different log. If you are using Java "system.out.println (not recommended)", the text will be written to the default log. Enter this command to view the log in the vi editor: `ce alogv`
9. Look at logs under `/var/log/nginx/`, if the above errors do not provide sufficient information.
10. You can also run traceMessage to look at the HTTP requests to your service and responses from your service. Type traceMessage.
11. Once you hit `Enter` on command line, you will be able to see the http trace messages.

    By default the trace is started and it you want to stop press s. Help is available in the tool. You can also see details of a message by selecting the message in the trace.

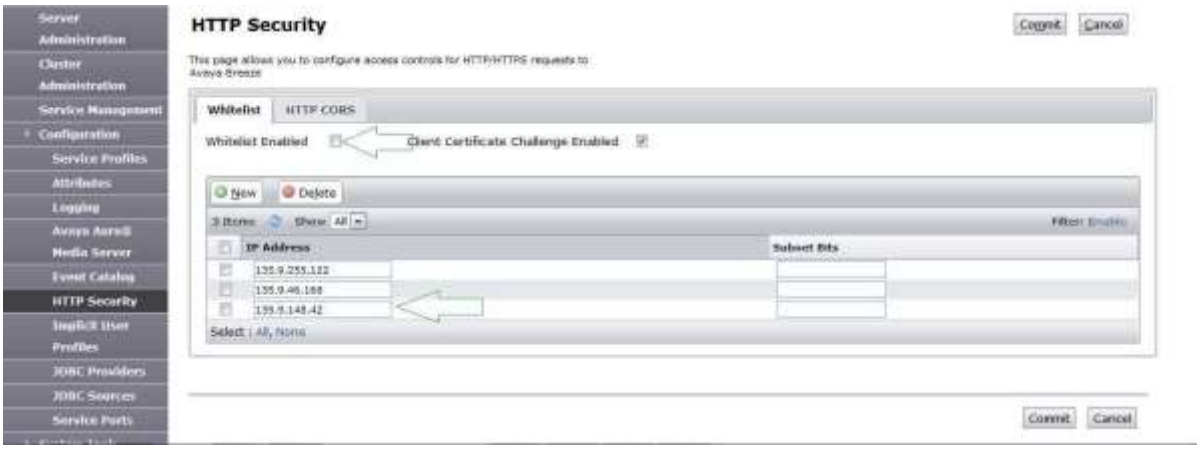


12. Make sure you are passing all the parameters required to execute your service when invoked through HTTP. In case of Multi-Channel Broadcast Sample Service bundled in SDK, you can look at – MultiChanBroadcastServlet.java class.

    MultichanbroadcastCollection directory in the sample service provides the Postman collections which is a skeleton for Postman requests to be sent to Multi-Channel Broadcast Sample Service.

    Also look at “How do I import collections bundled with Sample Services to Postman client in Chrome?”, if you want to know how to import the collections and use them.

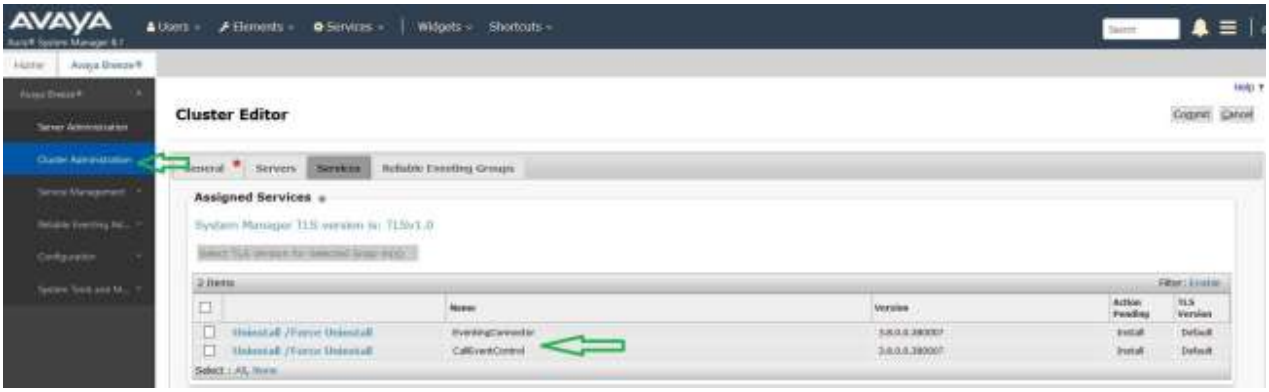
13. Make sure Avaya Breeze® platform shows “Accepting” in System State as per the steps mentioned at the start of this question.
14. Check that the HTTP Security either:
    - Does not have Whitelist Enabled.
    - Has Whitelist Enabled and the IP address of the connecting client is in the Whitelist. If the checkbox **Whitelist Enabled** is checked, please make sure the IP address or subnet from which you are trying to connect is in the Whitelist.
15. Verify the following if your application depends on CORS (for example, WebRTC does need CORS):
    - Check that the IP address of the service which serves your JavaScript and tries to make HTTP call to Avaya Breeze® platform is administered in the HTTP CORS page.
    - Alternatively use the checkbox in the screen. But this can have security issues, so please consider those before using this option.



Why are the changes from System Manager to service attributes of my service not reflected during execution or runtime?

Procedure

1. Verify that your service is installed.
2. Log in to System Manager.
3. On the System Manager Home page, select **Avaya Breeze® platform** from the Elements panel.
4. In the Avaya Breeze® platform page, select **Service Management > Services** from the menu.
5. Find your service.
6. If your service does not appear in the table, press the **Load** button to load the SVAR you created when building your service.
7. If the State for your service is Loaded, select the checkbox and press the **Install** button.
8. If you are using cluster administration to install the services as in the screen below, make sure that your service is shown in the installed services list and appropriate servers are selected in the servers tab. Also, verify that the preferred version is set for your cluster and the service is installed in the cluster.



9. If your service is in the Installed state, log in to your Avaya Breeze® platform server and run this command: `deploy_service -lv`.

   The output will look something like this:

   `load: + deploy: + run: + car: N HelloWorld-0.0.0.1.3`

   `load: + deploy: + run: + car: + basicSipCall-1.0.0.0.0`

   Service with call related features:

   If your service is in this list and shows a plus (+) for each step, it is installed and ready to go.

   If the car is “N” for a call related service, make sure that the service name and service version is exactly same in `sip.xml` as well as `web.xml`. Also, make sure the sip servlets match in both `sip.xml` and `web.xml`.

   HTTP service with no call features:

   If your service is in this list and shows a plus (+) for load, deploy and run step, it is installed and ready to go.

10. To verify that replication is working, from the Home tab on System Manager, select **Replication** from the Services panel.

    This will open the Replication tab.

11. Look for a AvayaBreeze_3.9 Replica group in the table.
12. If the **Synchronization Status** is not **Synchronized**, check the checkbox for the row and press the **View Replica Nodes** button.

    It takes about 1 minute a maximum to replicate data once it is changed in System Manager.

    Note that you could press the **Repair** button here to attempt to repair all servers in the replica group, rather than go to the next page to repair a specific server. Be aware that the Repair operation is service affecting, which means that calls will fail until the operation completes (usually just a few minutes).

Why is my service not accessible over http but accessible over https?

About this task

Avaya Breeze® platform has http access disabled by default. Only https is allowed by default. If you want to have http access as well as https access:

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze® platform > Cluster Administration**.
2. Click the checkbox in front of the cluster.
3. From the **Cluster State** drop-down menu, select **Deny New Service**.

4. Verify that the system displays **Denying** in the **Cluster State** column.
5. Click **Edit**.
6. Uncheck **Only Allow HTTPS traffic** and click **Commit**.
7. Put your cluster back in service. Now you will be able to have both http and https to your service.

How to use postman for https invocation to my service?

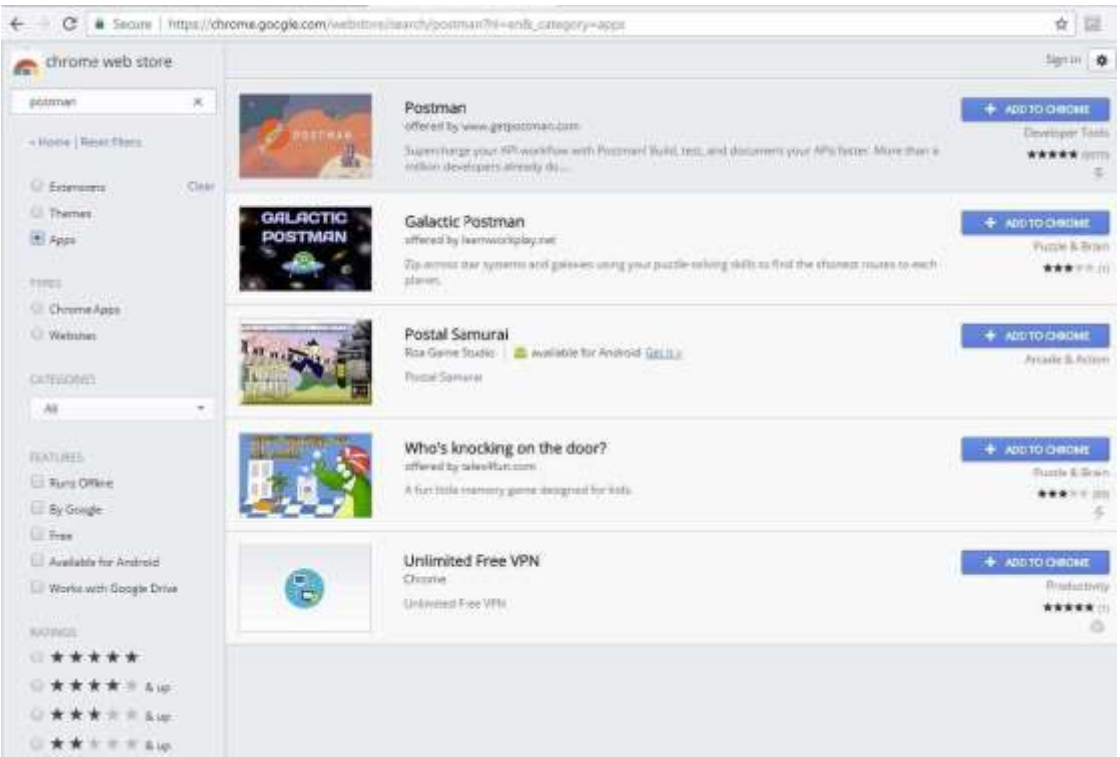
In order to use postman to do https invocation to your service, you need to accept the certificate of your Avaya Breeze® platform server in Chrome. For example, if you want to execute https to 10.10.10.10

Avaya Breeze® platform server and you are using default certificates – Launch Chrome and execute https://10.10.10.10 as the URL. You will be prompted to accept the certificate. Once accepted, you can use postman to point to your service.

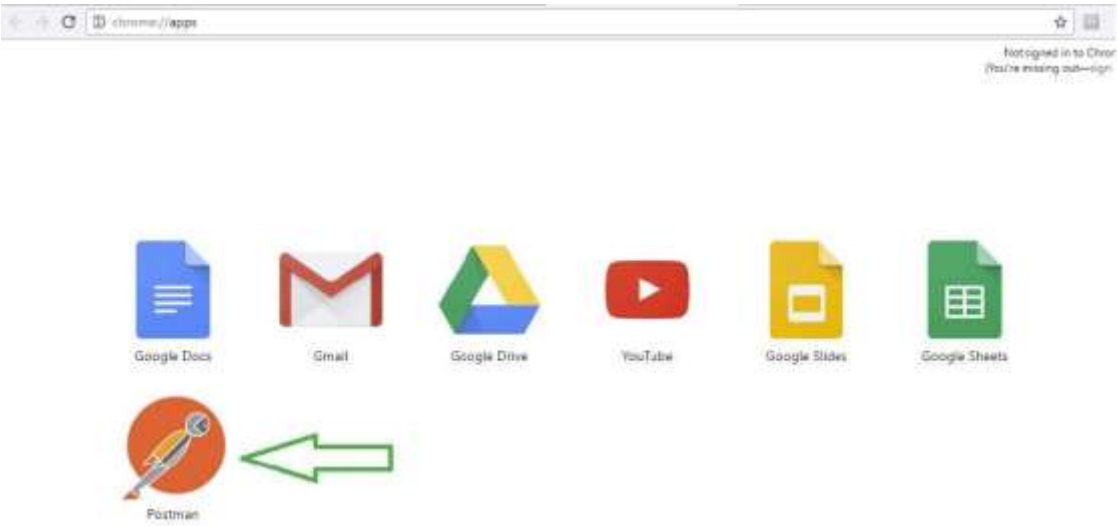
How do I import collections bundled with Sample Services to Postman client in Chrome?

Procedure

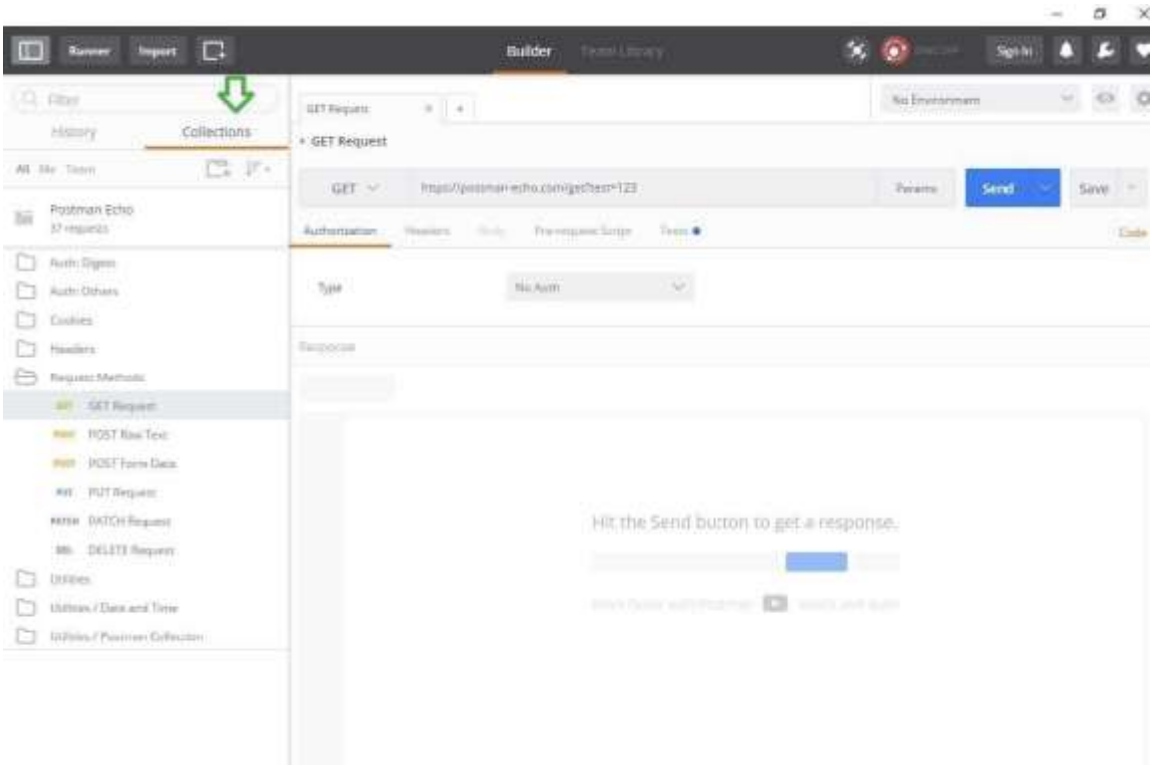
1. The first step is to make sure you have Postman Client installed in Chrome. Go to Chrome Web Store and Search for “postman app”..



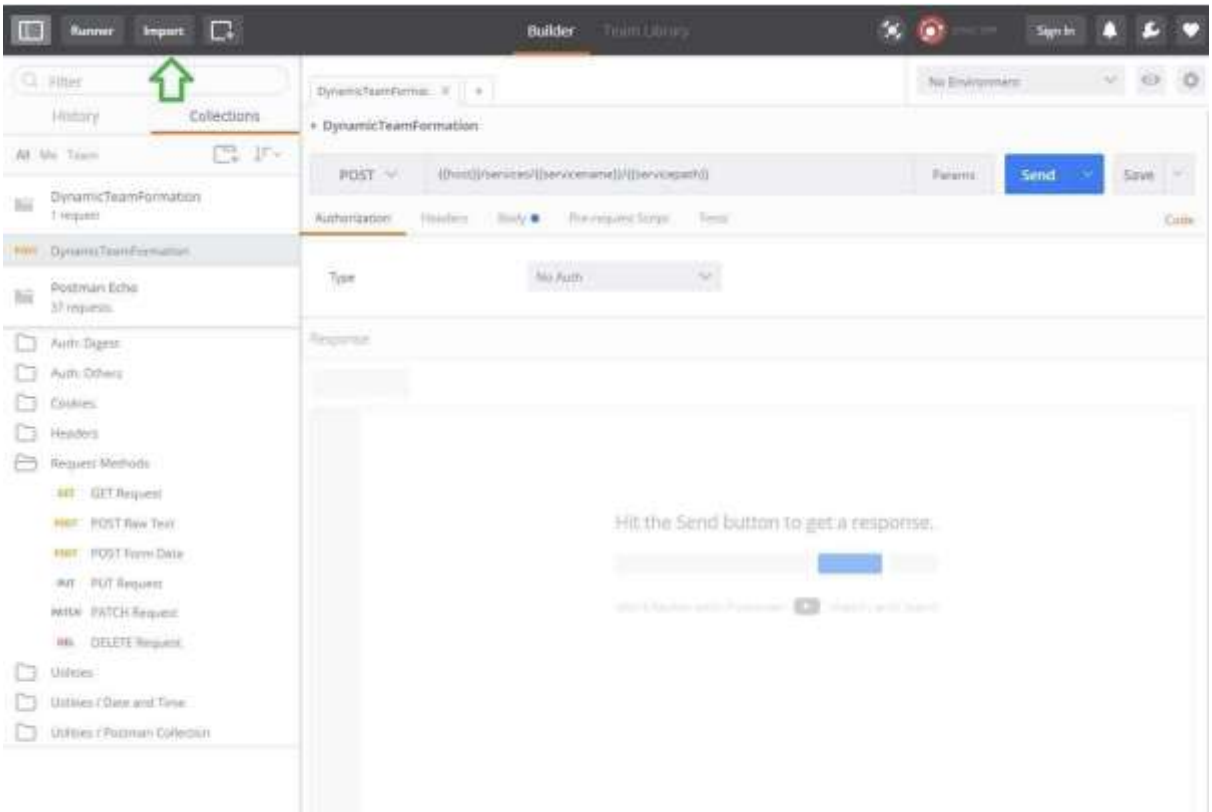
2. Install the client and you should be able to see the client when you launch chrome.



3. Launch the Postman Client.

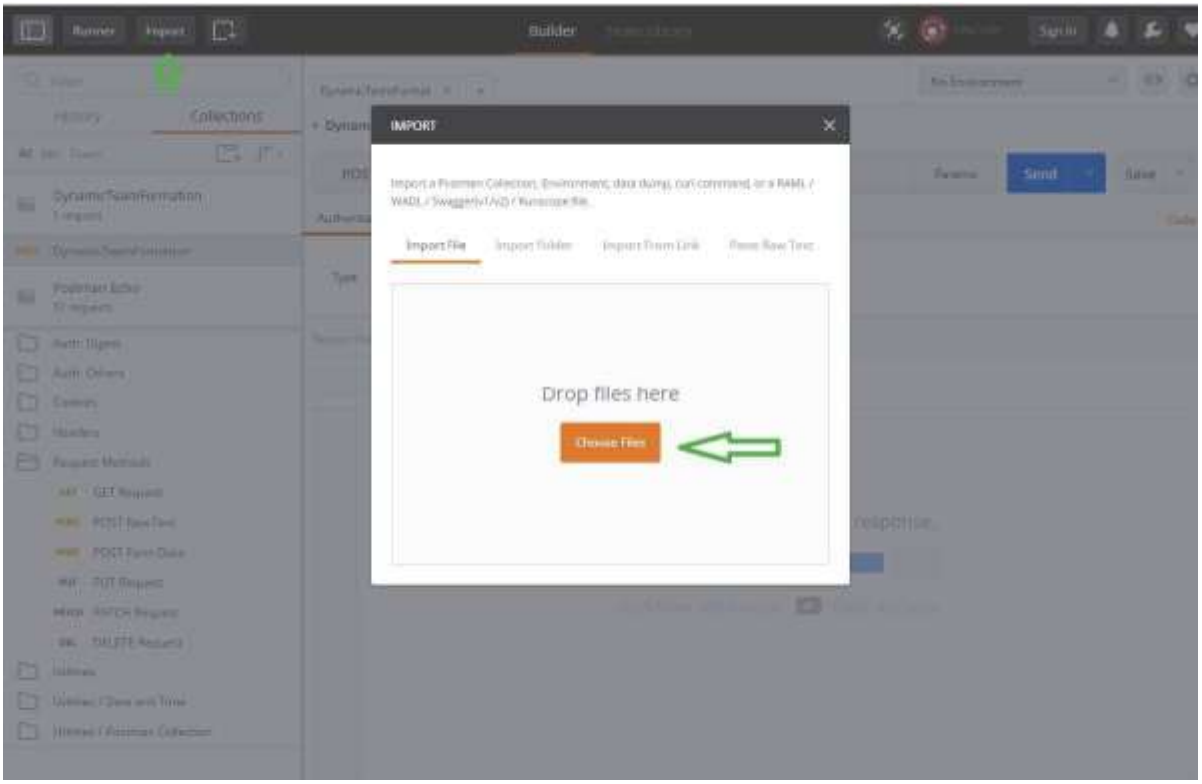


4. Click **Import** button.

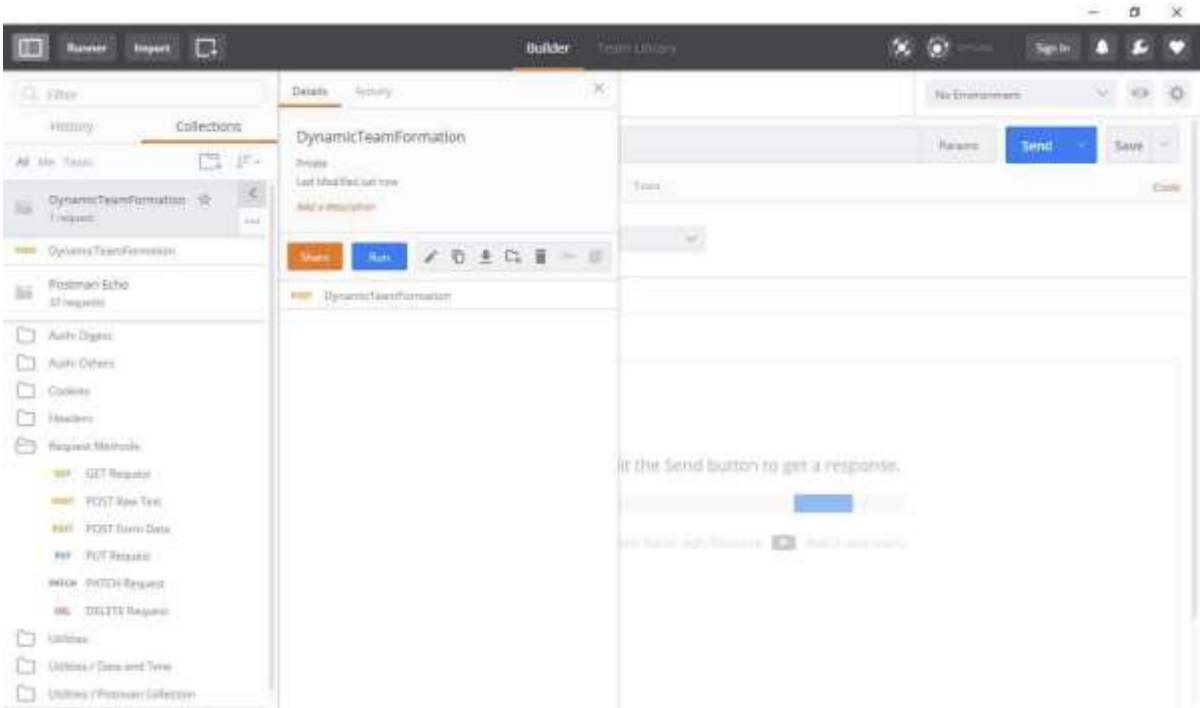


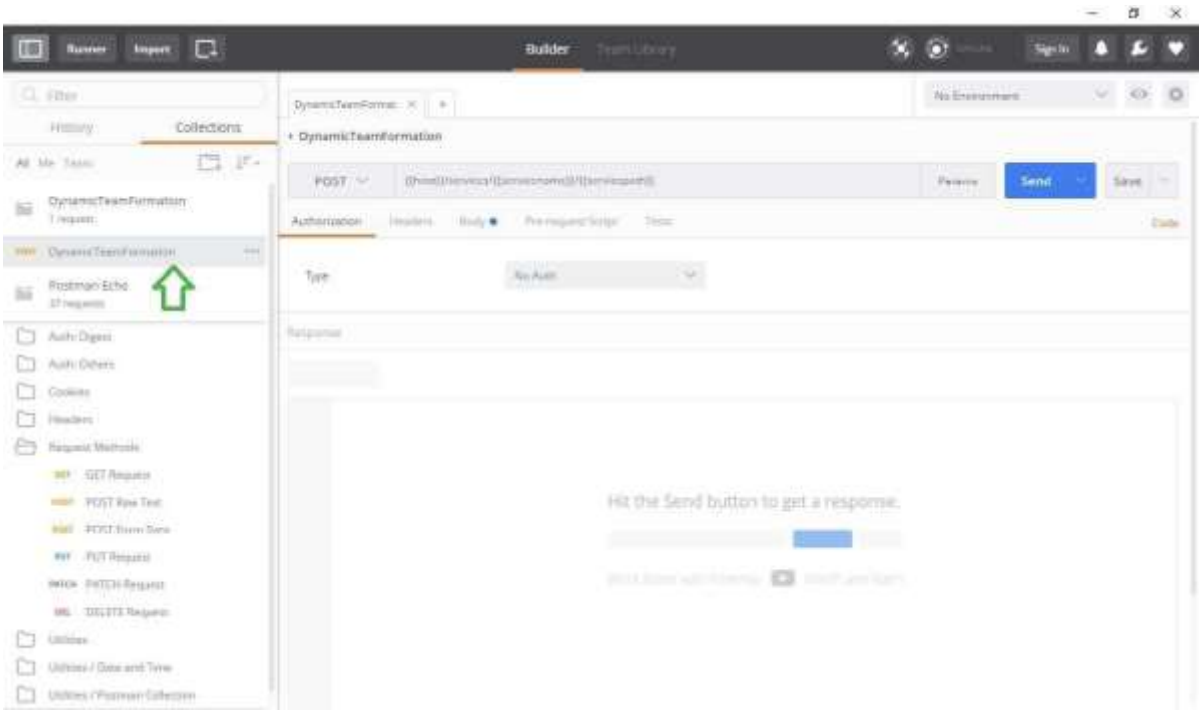
5. Click **Choose files** and select the json file from the SDK zip sample service directory.

We are taking an example of Dynamic Team Formation Collection here. The collection can be found in following location in the SDK – \samples 7 \dynamicteamformation\DynamicTeamFormationCollection.

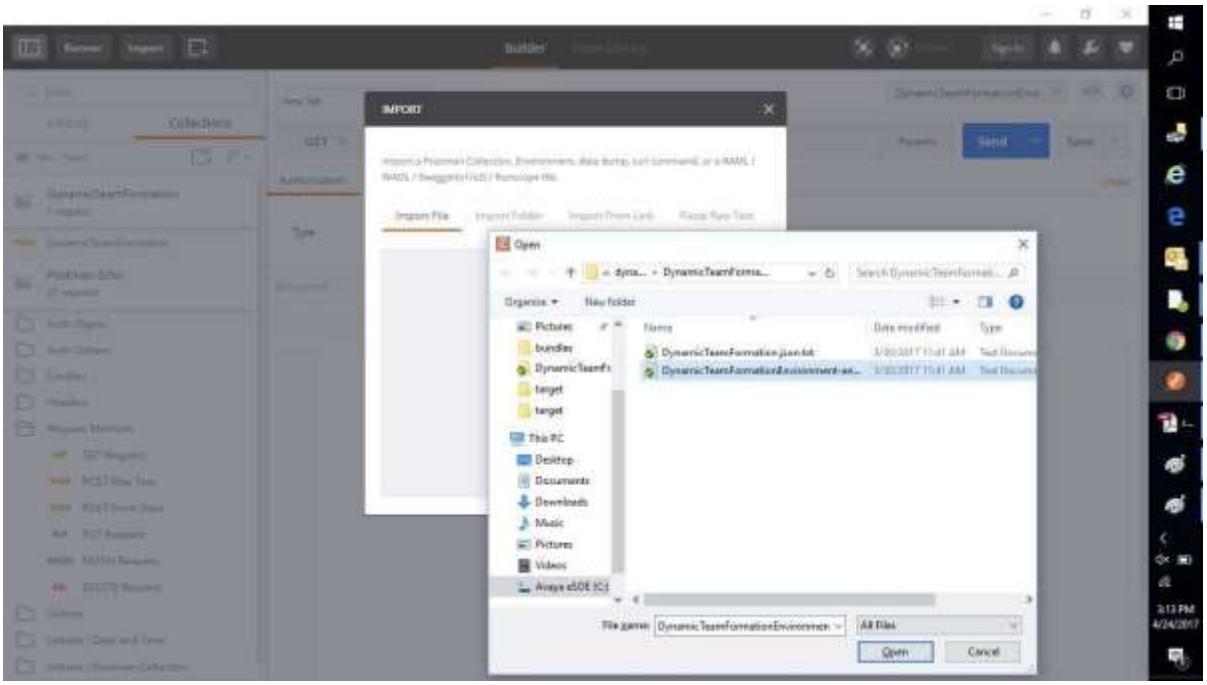


6. Check the collection by selecting the left navigation.

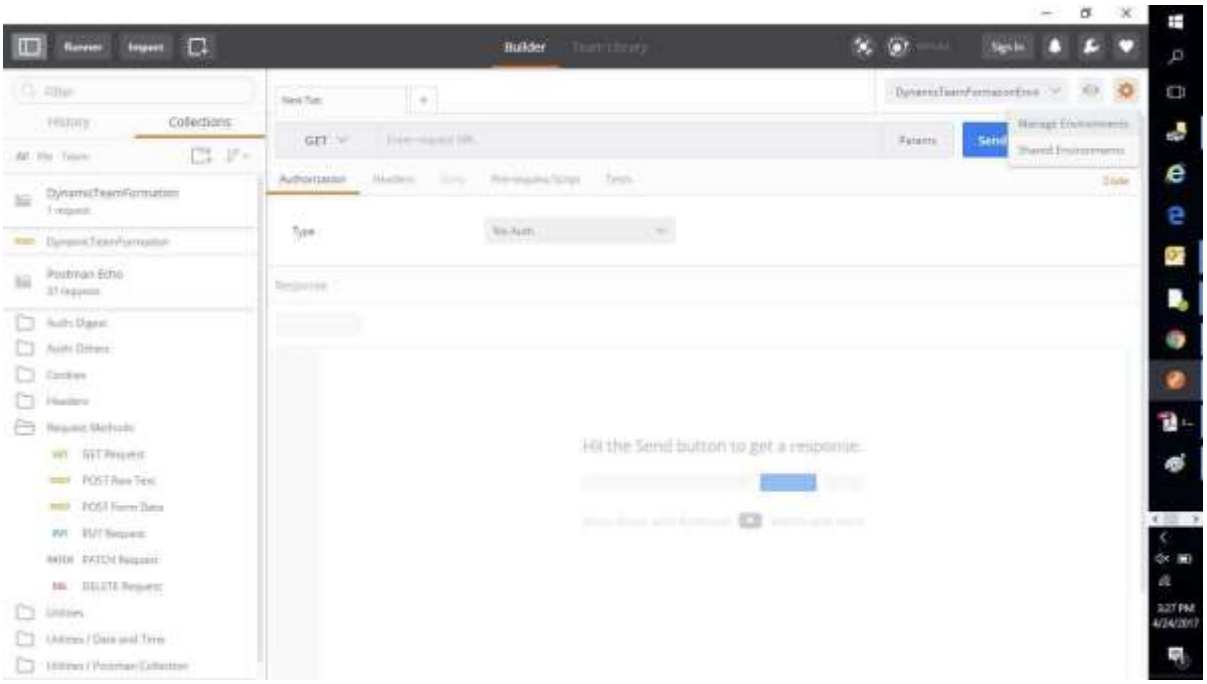




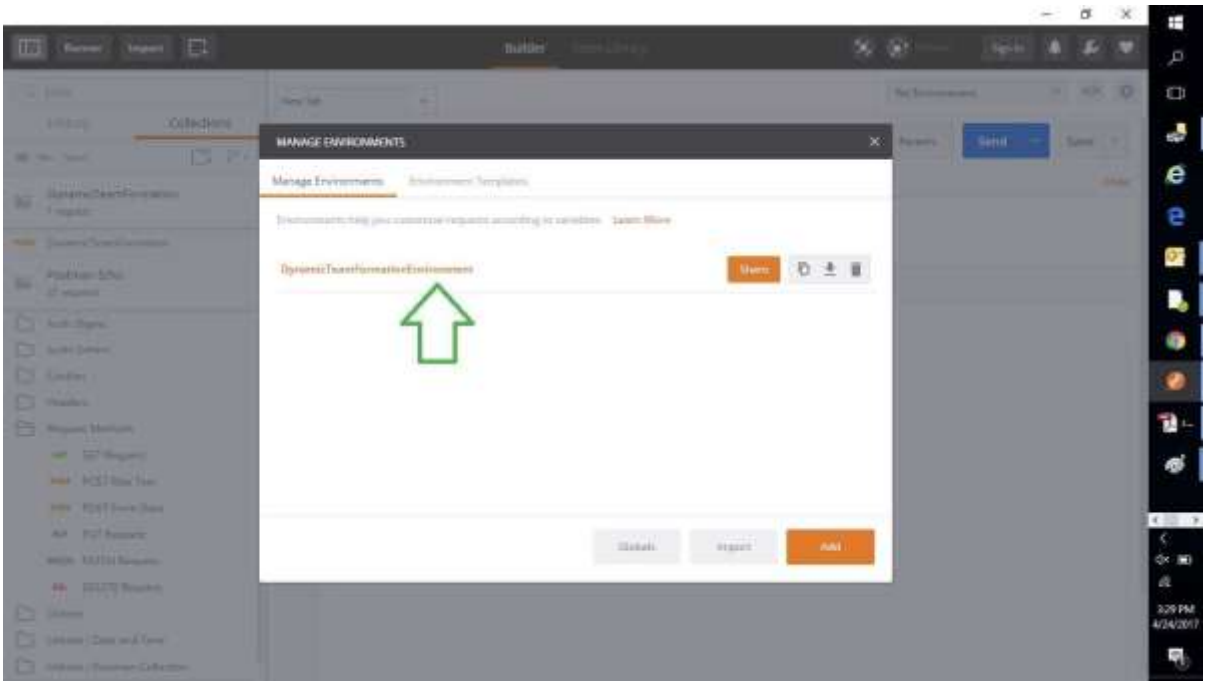
7. The next step is to import the Environment Collection.
8. Click **Import** and then click **Choose Files**.



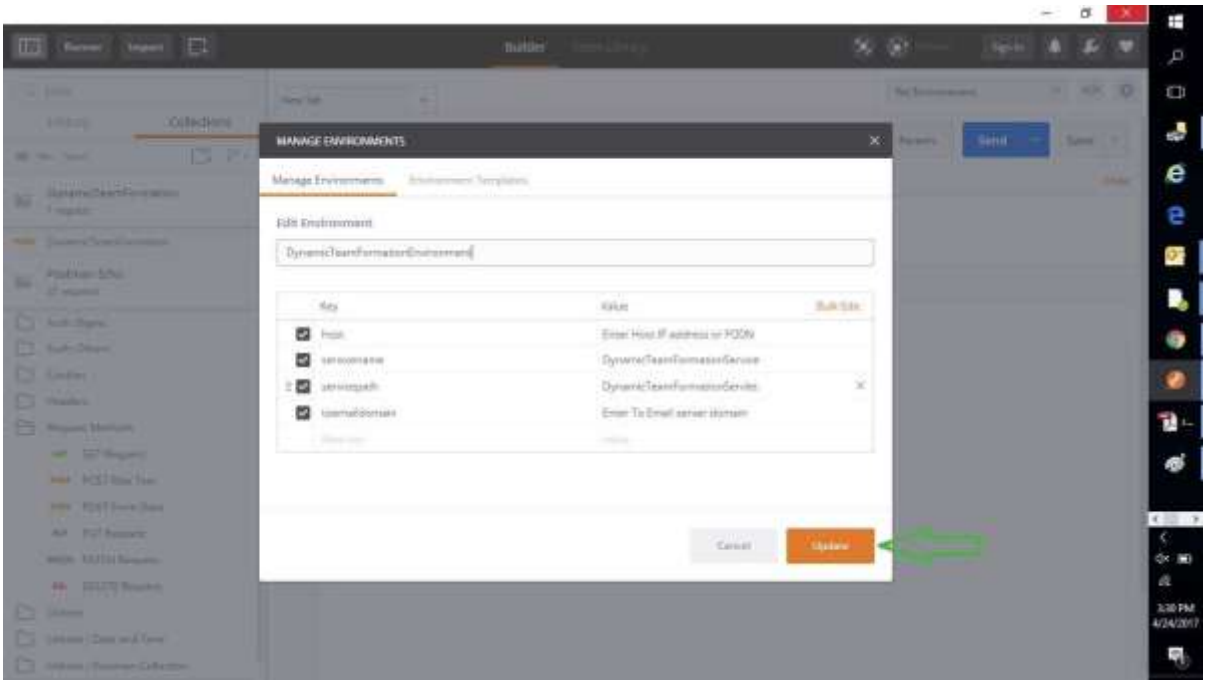
9. Now you can edit the skeleton data as needed to invoke your service by selecting the specific environment.
10. Go to Setting, Click on **Manage Environments**.



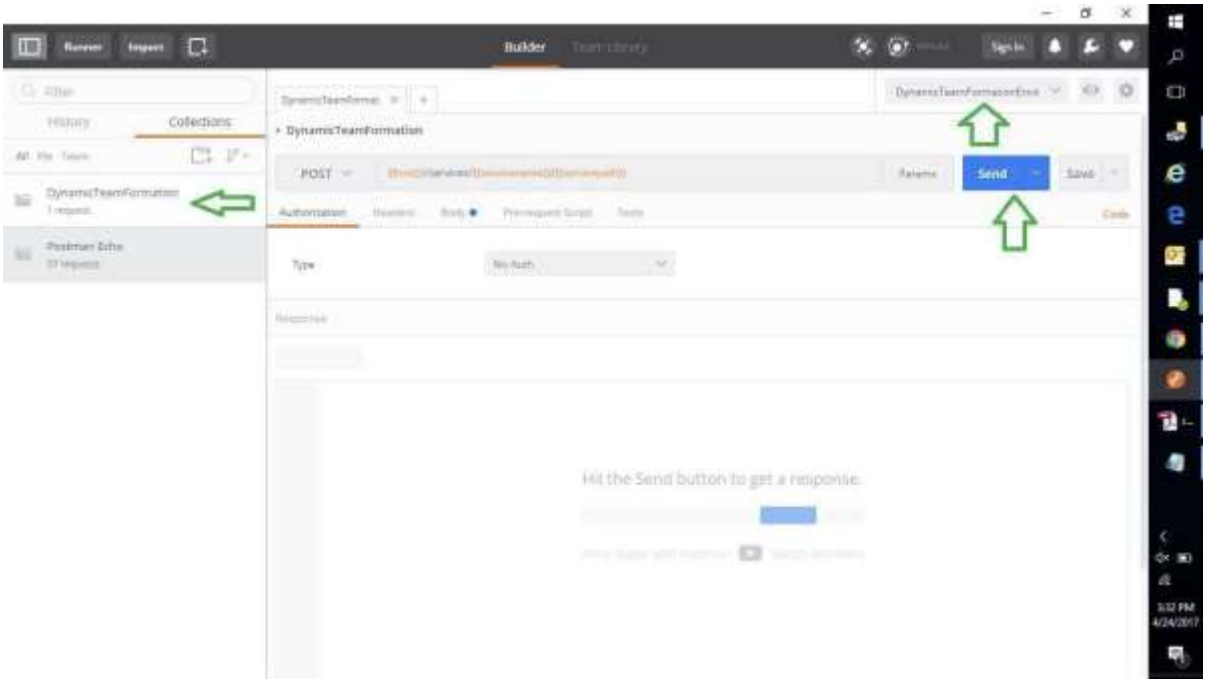
11. Click on **Environment** for editing.



12. Click on **Update** to save changes.



13. After saving is successful, submit this and select the Environment to be used by your collection.



14. Edit the fields in the screen and you are ready to test the Dynamic Team Formation Service assuming that the service is already installed on Avaya Breeze® platform.
15. Click **Send** button to see your request sent to Avaya Breeze® platform.

How do I invoke Multi-Channel Broadcast service and Dynamic Team Formation Service for my testing

Procedure

- You can write an external application which can send GET and POST HTTP requests to Multi-Channel Broadcast or Dynamic Team formation service to test your service. URL to invoke the service would look like:

  Multichannel Broadcast Sample service installed on Avaya Breeze® platform, it can be invoked as:

  http://10.10.10.100/services/MultiChanBroadcastService/MultiChanBroadcastServlet

  OR

  https://10.10.10.100/services/MultiChanBroadcastService/MultiChanBroadcastServlet

  MultiChanBroadcastService – this is the service name

  The above URLs for Multi-Channel broadcast will invoke the preferred version of the service installed on Avaya Breeze® platform. For example, if you have 2.0.0.0.13002 installed and also 2.0.0.0.13003 on Avaya Breeze® platform, the above example URL will invoke 2.0.0.0.13003 version of the application.

- If you wish to invoke 2.0.0.0.13002 specific version of the example service above, the URL would look like:

  http://10.10.10.100/services/MultiChanBroadcastService-2.0.0.0.13002/MultiChanBroadcastServlet

  OR

  https://10.10.10.100/services/MultiChanBroadcastService-2.0.0.0.13002/MultiChanBroadcastServlet

  The preferred version of service can also be invoked using the format of servicenameserviceversion in the URL. i.e.:

  http://10.10.10.100/services/MultiChanBroadcastService-2.0.0.0.13003/MultiChanBroadcastServlet

  OR

  https://10.10.10.100/services/MultiChanBroadcastService-2.0.0.0.13003/MultiChanBroadcastServlet

- Dynamic Team formation Service on Collaboration Environment can be invoked as:

  http://10.10.10.100/services/DynamicTeamFormationService/DynamicTeamFormationServlet

  OR

  https://10.10.10.100/services/DynamicTeamFormationService/DynamicTeamFormationServlet

  Alternatively, you can use Postman client and use the Collections provided with the sample services to send the requests to the services. Details on how to import the

Collections can be found in the previous question “How do I import collections bundled with Sample Services to Postman client in Chrome?”

More details about the sample services can be found in documents *Multi-Channel Broadcast Sample Service* and *Dynamic Team Formation Sample Service*.

How do I invoke ClickToCall Sample service for my testing?

Procedure

Open a well-known browser and type http://*<Avaya Breeze® platform Cluster IP>*/services/ClickToCall/index.jsp.

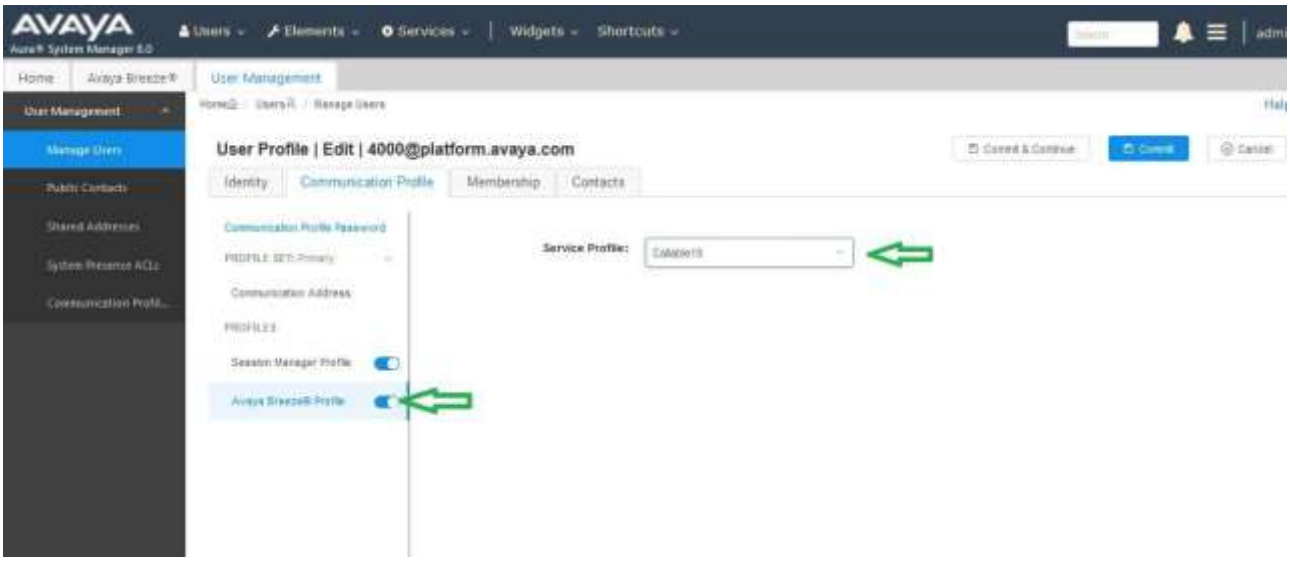
For example: http://10.129.177.214/services/ClickToCall/index.jsp.

What are the prerequisites for the Callingpolicies Sample service?

Procedure

1. Configure the service profile and add the Callingpolicies preferred version to the Service profile:

2. On System Manager, in **Users**, click **User Management > Manage Users**.



3. Click the checkbox by the user that you want to have the service profile and click **Edit**.
4. From the **Service Profile** menu , under **Avaya Breeze Profile**, select the service profile for the selected extension:
5. On System Manager, in **Elements**, click **Avaya Breeze® platform > Configuration > Attributes**.
6. Under Attributes Configuration , set the Service profile attributes by selecting the **Profile** and the **Service**:

How do I test the Callingpolicies Sample service?

Procedure

Since this is a term side called service, call a number example: 3401@avaya.com from another extension. This would be the called extension.

- Called extension rings.
- The announcement is played.

- Based on the dtmf input , call is either forked or, redirected or, allowed to continue or dropped.
- For 1= Fork, it forks to the extensions provided in the service attributes. Please refer the screen shot above.
- For 2 = redirect, it redirects to the extension provided in the service attribute. Please refer the screen shot above.
- For 3= allow, the called extension (in the above example 3401@avaya.com) rings.
- For 4=drop, the call is dropped and the respective tone is heard on the extension.

My service is installed and I see logs from my service, but things are not behaving like I expected. What should I check?

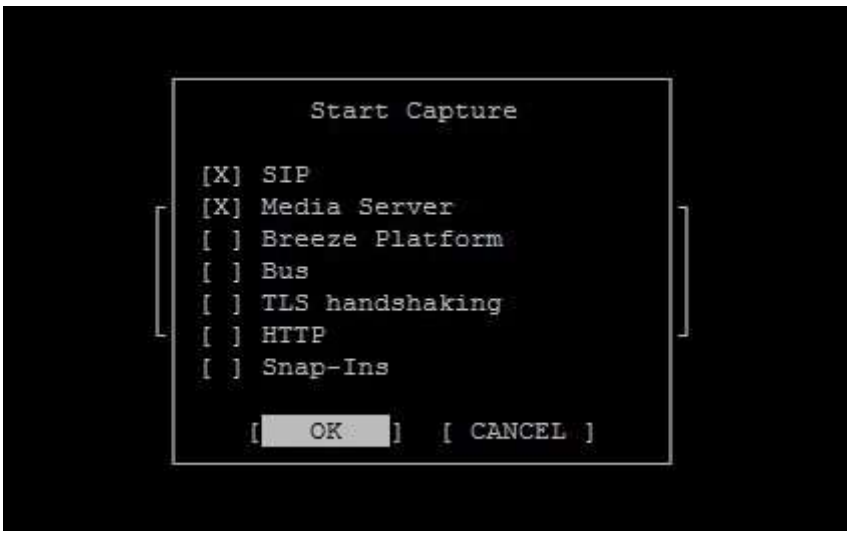
Condition

If your application makes use of collaboration bus and think that messages are not passed correctly, you can run a traceMessage command to check the messages to and from the collaboration bus.

For this edition of Avaya Breeze® platform, the supported underlying communication protocol is the Session Initiation Protocol (SIP) for call intercept/call control services, as defined in IETF RFC 3261 and associated RFCs. Avaya Breeze® platform has a tool to capture and analyze traffic.

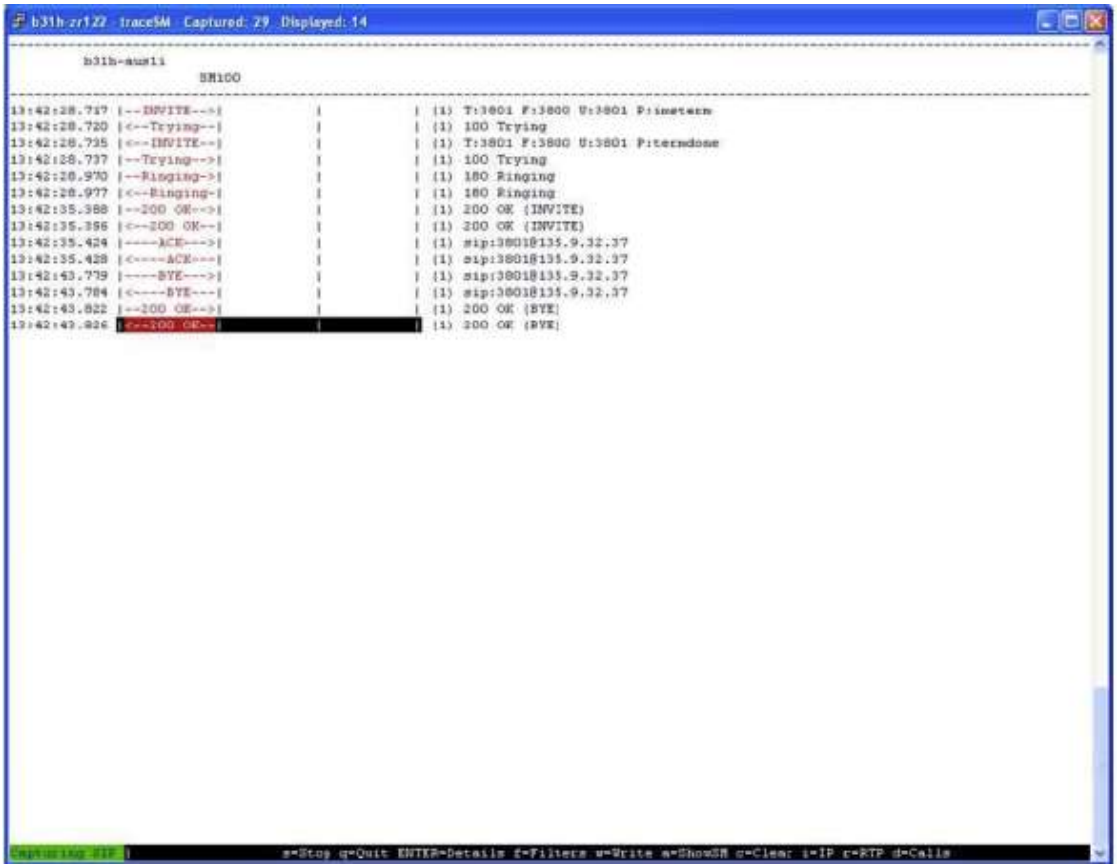
Solution

1. Run this command on the Avaya Breeze® platform server: traceMessage.
2. When prompted, press `s` to start the capture.
3. You will then be prompted to select the type of traffic – just hit `Return` at this point to take the default.



4. Place a call.

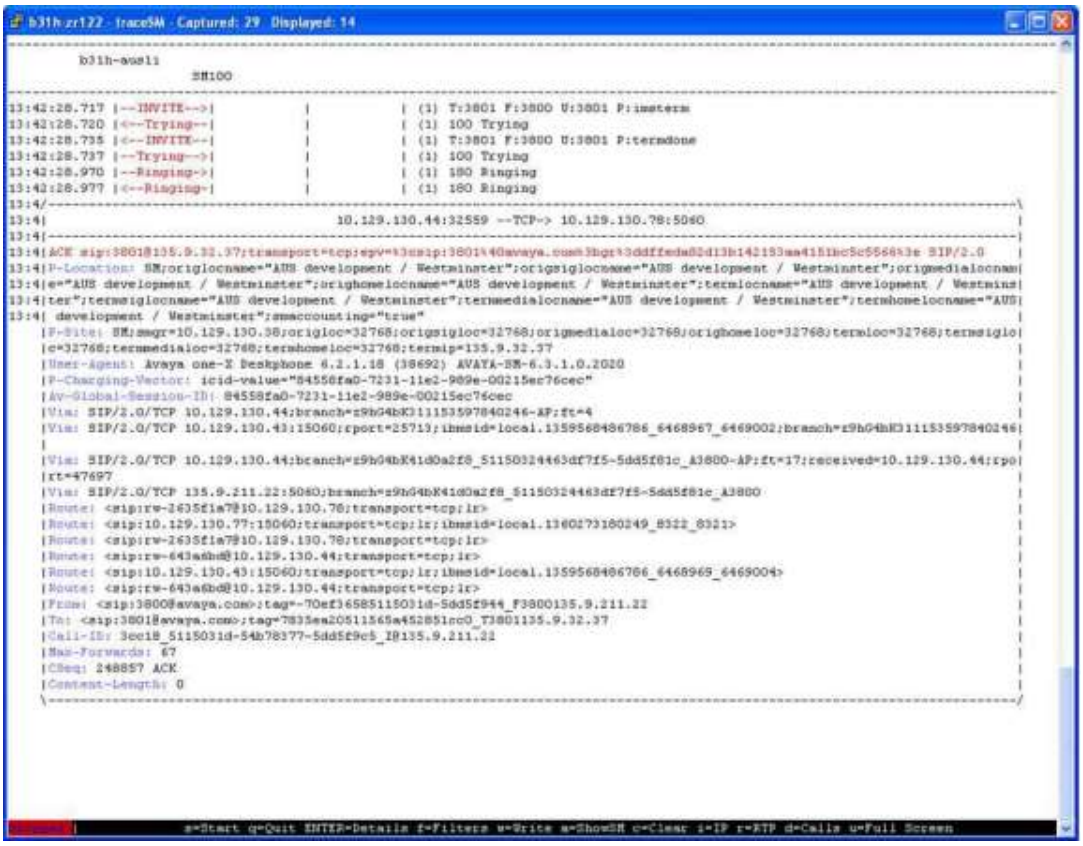
You should see a fencepost diagram develop that shows the messages exchanged between the Avaya Breeze® platform server and other entities. Here is an example of a simple call, where user A called user B, user B answered and then user A dropped:



Note the menu along the bottom – you may want to stop the trace collection after you have made your test call to limit the amount of data captured.

This trace shows 2 entities involved in the signaling: b31h-ausl1 is a Session Manager, and SM100 represents the Avaya Breeze® platform server. Signaling is generally routed from Session Manager to Avaya Breeze® platform and then back to Session Manager.

5. You can use the arrow keys to move up and down through the message sequence. If you press the Enter key, the highlighted message will be expanded.



You can inspect the various messages to see if your service has any effect.

6. You can get a view of application status on Avaya Breeze® platform Server Administration screen by looking at the activity column.
7. You can get a view of application status by running this command on your Avaya Breeze® platform server: metget =sipapp.

   The output will look something like this:

   0
   SipContainerModule.ApplicationModule.SessionModule.WhiteList-1.0.0.0.0.Active_SIP_Sessions
   1
   SipContainerModule.ApplicationModule.SessionModule.basicSipCall-1.0.0.0.0.Active_SIP_Sessions
   2 SipContainerModule.ApplicationModule.SessionModule.pfa.Active_SIP_Sessions
   0
   SipContainerModule.ApplicationModule.SessionModule.testingLogger-0.0.0.0.1.Active_S
   IP_Sessions
   3 SipContainerModule.Active_SIP_Sessions

   The clue here is that the basicSipCall service shows 1 active session.

   Sometimes debugging can be a bit easier by starting with simpler configurations or simpler scenarios. For example, you might want to start with all signaling going over TCP rather than TLS. At a minimum, this would allow you to use network sniffers like wireshark to analyze

traffic at different points in your infrastructure. After resolving your problem, you could try switching back to TCP.

Make sure you use same protocol across all your systems: Avaya Breeze® platform, Session Manager, and Communication Manager.

8. If you use TCP, use TCP on all these servers. If TLS, then configure TLS on all of these servers.

For Service invoked through HTTP

1. Verify that the URL used to access the service is of the form:

   http://[Breeze_FQDN_or_IP]/services/servicename/[Service_Specified_Pattern] or
   https://[Breeze_FQDN_or_IP]/services/servicename/[Service_Specified_Pattern] or
   http://[Breeze_FQDN_or_IP]/services/servicename-serviceversion/
   [Service_Specified_Pattern] or
   https://[Breeze_FQDN_or_IP]/services/servicename-serviceversion/
   [Service_Specified_Pattern]

   Breeze FQDN or IP is the Security Module hostname or IP address as configured on System Manager. For example, if you have Multichannel Broadcast Sample service installed on Avaya Breeze® platform, it can be invoked as –

   http://10.10.10.100/services/MultiChanBroadcastService/MultiChanBroadcastServlet
   or
   https://10.10.10.100/services/MultiChanBroadcastService/MultiChanBroadcastServlet

   MultiChanBroadcastService – this is the service name

   The above URLs for Multi-Channel broadcast will invoke the preferred version of the service installed on Avaya Breeze® platform. For example, if you have 3.8.0.320005 installed and also 3.8.0.320006 on Avaya Breeze® platform, the above example URL will invoke 3.8.0.320006 version of the application.

2. Login to Avaya Breeze® platform server and run this command on command line: `ce dlogv`.

   This will open the debug log using the vi editor.

3. Search for your service name.

   This should provide you with information if there were any exceptions that lead to issues with invoking the service.

4. If you added logging statements in your service code, and if you used the Logger class in the Avaya Breeze® platform API (highly recommended), you can view the service log using the command `ce dlogv <serviceName>`.

   For example, to view the logs for the basicSipCall service, run the command `ce dlogvbasicSipCall`.

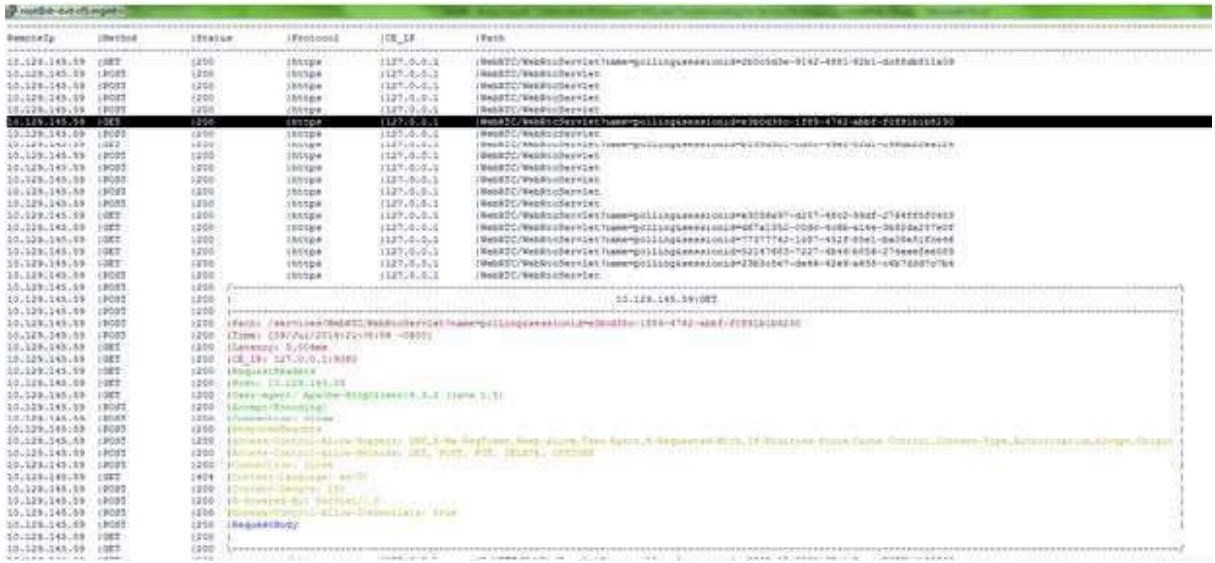
   The logs for different versions of a service all go to the same log file, and each log message contains the service name and version.

   When running in normal mode, logs at level INFO and higher priority (FATAL, ERROR, WARN) will be added to the log file; logs at lower priority (FINE, FINER, FINEST) will not be added to the log. The log level can be changed on the fly to provide more verbose logging.

5. Enter this command while logged in to your Avaya Breeze® platform `ce dlogon`
6. To enable all log levels for a specific service use `ce dlogon <serviceName>`.
7. When you are finished debugging, you should return logging to the default using this command: `ce dlogoff` or `ce dlogoff <serviceName>` for a specific service.
8. When you are finished debugging, you should return logging to the default using this command: `ce dlogoff`

   Default logging (sysout or syserr) goes to a different log. If you are using Java "system.out.println (not recommended)", the text will be written to the default log.
9. Enter this command to view the log in the vi editor: `ce alogv`
10. Look at logs under `/var/log/nginx/`, if the above errors do not provide sufficient information.
11. You can also run traceMessage to look at the HTTP requests to your service and responses from your service by typing `traceMessage`.

    When you press Enter on the command line, press S to start the capture when prompted. When the system prompts you to select the type of traffic, you will be able to see the http trace messages. By default, the trace is started and it you want to stop press S. Help is available in the tool. You can also see details of a message by selecting the message in the trace.



    Make sure you are passing all the parameters required to execute your service when invoked through HTTP. In case of Multi-Channel Broadcast Sample Service bundled in SDK, you can look at MultiChanBroadcastServlet.java class.

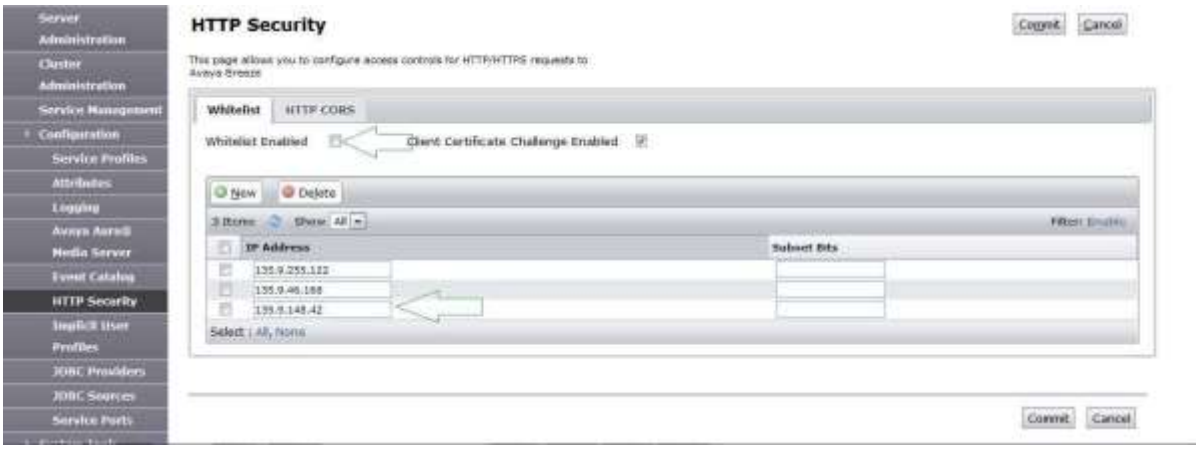
    `MultichanbroadcastCollection` directory in the sample service provides the Postman collections which is a skeleton for Postman requests to be sent to Multi-Channel Broadcast Sample Service.

    Also look at "How do I import collections bundled with Sample Services to Postman client in Chrome?", if you want to know how to import the collections and use them.

12. Make sure Avaya Breeze® platform shows "Accepting" in System State as per the steps mentioned at the start of this question.

13. Check that the HTTP Security either:
    - Does not have Whitelist Enabled.
    - Has Whitelist Enabled and the IP address of the connecting client is in the Whitelist. .
14. If the checkbox **Whitelist Enabled** is checked, please make sure the IP address or subnet from which you are trying to connect is in the Whitelist
15. Verify the following if your application depends on CORS (for example, WebRTC does need CORS).
16. Check that the IP address of the service which serves your JavaScript and tries to make HTTP call to Avaya Breeze® platform is administered in the HTTP CORS page.

    Alternatively use the checkbox in the screen. But this can have security issues, so please consider those before using this option.



Where do I look for the debug logs I added to my service?

About this task

Assuming you added logging statement in your service code using the Logger class in the Avaya Breeze® platform API (highly recommended), the debug logs are text files. The default location for log files for a particular service on Avaya Breeze® platform is `/var/log/Avaya/services/<servicename>`. The logs for different versions of a service all go to the same log file, and each log message contains the service name and version.

Procedure

1. Log in to the Avaya Breeze® platform server and run this command: `ce dlogv <serviceName>`.

   This opens the service log using the vi editor. Take a look at the Javadoc for the Logger class in the Avaya Breeze® platform API. When running in normal mode, logs at level INFO and higher priority (FATAL, ERROR, WARN) will be added to the log file; logs at lower priority (FINE, FINER, FINEST) will not be added to the log.

   The log level can be changed on the fly to provide more verbose logging.

2. Enter this command while logged in to your Avaya Breeze® platform server to enable all log levels: `ce dlogon <serviceName>`.

3. When you are finished debugging, you should return logging to the default using this command: `ce dlogoff <serviceName>`.

   Default logging (sysout or syserr) goes to a different log. If you are using Java "System.out.println (not recommended)", the text will be written to the default log.

4. Enter this command to view the log in the vi editor: `ce alogv`.

Why does my outgoing HTTP request from my service not use the security module IP?

Cause

By default the outgoing HTTP requests from Avaya Breeze® platform use the management IP address. For more information, see the OutboundHttps Sample snap-in.

Solution

1. In-order to make sure security module IP address is used in outgoing HTTP requests, please look at sample code from Javadoc. `Package:com.avaya.collaboration.bus.sample Class: SampleLotteryHttpClient`
2. If you would like to make https requests from your snap-in look at sample code in Javadoc for SSLUtility APIs.

   Please note that this does not use proxy configuration by default. Write the service such that you can use a proxy in your snap-in while making the http request.

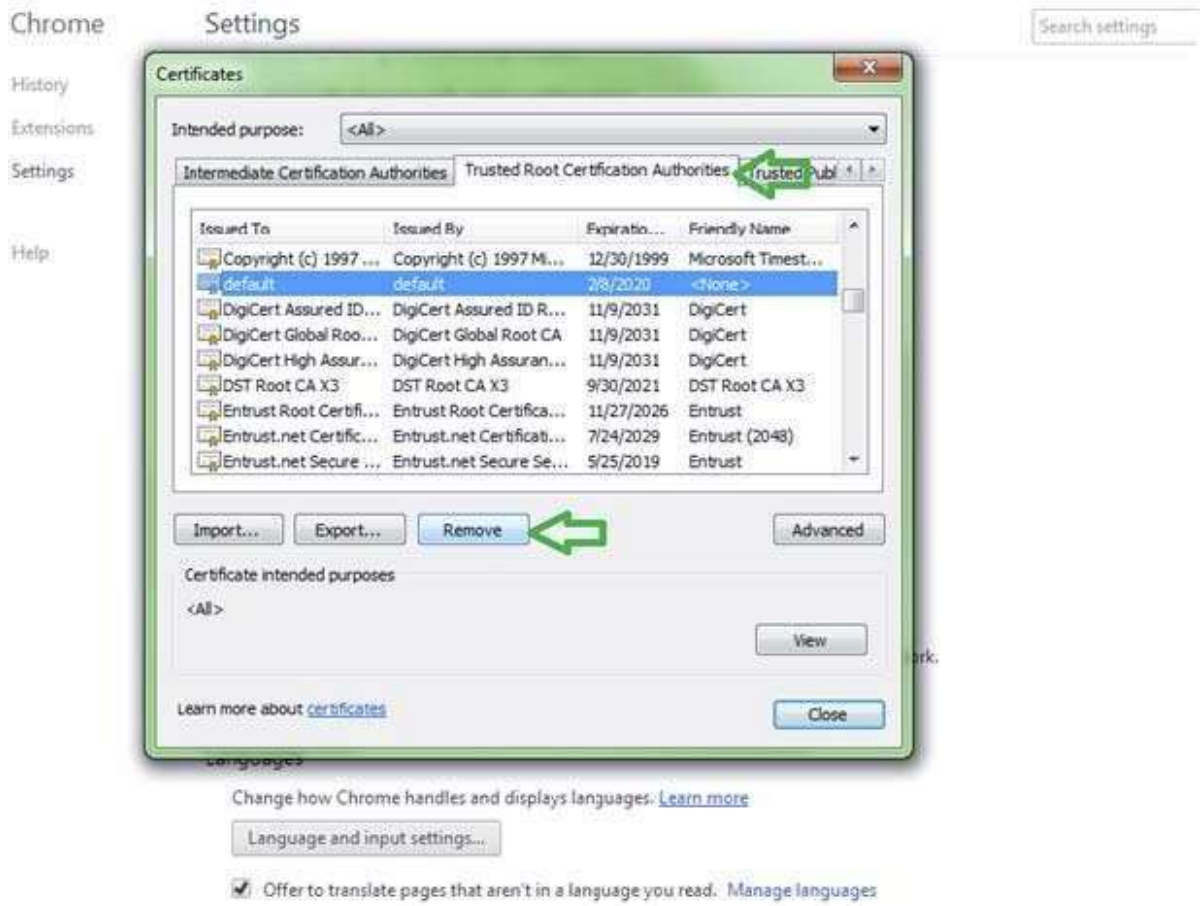
Why does HTTPS access to my services give error like "Cannot connect to real <IP address>"?

Cause

This happens if you are using default certificates on your Avaya Breeze® platform. The default certificate would not be valid. You can clear the default cert and then access your application over https again.

Solution

1. To remove the incorrect certificate, launch chrome as "administrator".
2. Go to **Settings > Show Advanced Settings > Manage Certificates > trusted Root Certification Authorities**.
3. Now select the Default certificate and remove.



4. Close the browser and launch again.
5. Now access your service using HTTPS. You should be able to accept the certificate and proceed with testing your snap-in.

How do I debug media-related issues?

Solution

1. Make sure the administration is done as per the Deploying Avaya Breeze® platform document.
   Look specifically at the chapter with details about Avaya Aura® Media Server Deployment.

2. Do you see an exception in the logs “mediaService play throws illegalStateException”?

   This indicates that an unsupported scenario is being executed using the Avaya Aura® Media Server. The scenarios in which the operations are supported are:

- An Outbound Calling service that plays announcements for notification purposes.
- A Call Intercept service that 1) Plays a message then 2) Drops the call.

Refer to the details about developing applications with announcements from the .

Refer to the Sample Service – Multi-Channel Broadcast sample service (which is part of the SDK) on how announcements can be played for an outgoing call.

3. Login to Avaya Breeze® platform server and run this command on command line: `ce dlogv <serviceName>`

   This will open the debug log using the vi editor.

4. Search for your service name.

   This should provide you with information if there were any exceptions that lead to issues with invoking the service.

5. If you added logging statements in your service code, and if you used the Logger class in the Avaya Breeze® platform API (highly recommended), you can view the service log using the command: `ce dlogv <serviceName>`

   For example, to view the logs for the basicSipCall service, run the following command: `ce dlogv basicSipCall`

   When running in normal mode, logs at level INFO and higher priority (FATAL, ERROR, WARN) will be added to the log file; logs at lower priority (FINE, FINER, FINEST) will not be added to the log. The log level can be changed on the fly to provide more verbose logging.

6. Enter this command while logged in to your Avaya Breeze® platform server to enable all log levels: `ce dlogon <serviceName`

7. When you are finished debugging, you should return logging to the default using this command: `ce dlogoff <serviceName>`

   Default logging (sysout or syserr) goes to a different log. If you are using Java "system.out.println (not recommended)"", the text will be written to the default log.

8. Enter this command to view the log in the vi editor: `ce alogv`.

9. In order to debug and look for ce platform logs, enable logging by running: `ce dlogon`.

10. Then look at server by running: `ce dlogv`.

11. Once you are done disable logging by executing: `ce dlogoff`.

Additional information

1. When using "http://" or "https://" for the recording file URI, the recording failed with a record.failed.post.

The snap-in is responsible to provide an implementation of an HTTP service to receive the recording file from Avaya Aura® Media Server. Avaya Aura® Media Server does an HTTP post when the recording is completed. If the HTTP service is running on an Avaya Breeze® platform snap-in, the recording must be smaller than the NGINX size limit of 10MB for HTTP. If the recording file exceeds this limit, the recording will fail with a record.failed.post. In this situation, you may see a 413 status with "traceMessage".

2. What kind of file format did Avaya Aura® Media Server use to post the record file?

   It is multipart/form-data format. The recoded file is under the “rec_data” part. By default the recording file is posted with base64 encoded data. The base64 encoding for http recording files can be disabled through the media server element manager. Please check the current Avaya Aura® Media Server documentation for the detailed procedure. For example, Avaya Aura® Media Server 7.8 it may be done through **System Configuration > Media Processing > Advanced settings > Convert Recording to Based64**. This procedure may be changed through releases, so verify the current Avaya Aura® Media Server documentation for the proper procedures.

3. I am unable to record to a http location but the same http location worked for play announcement.

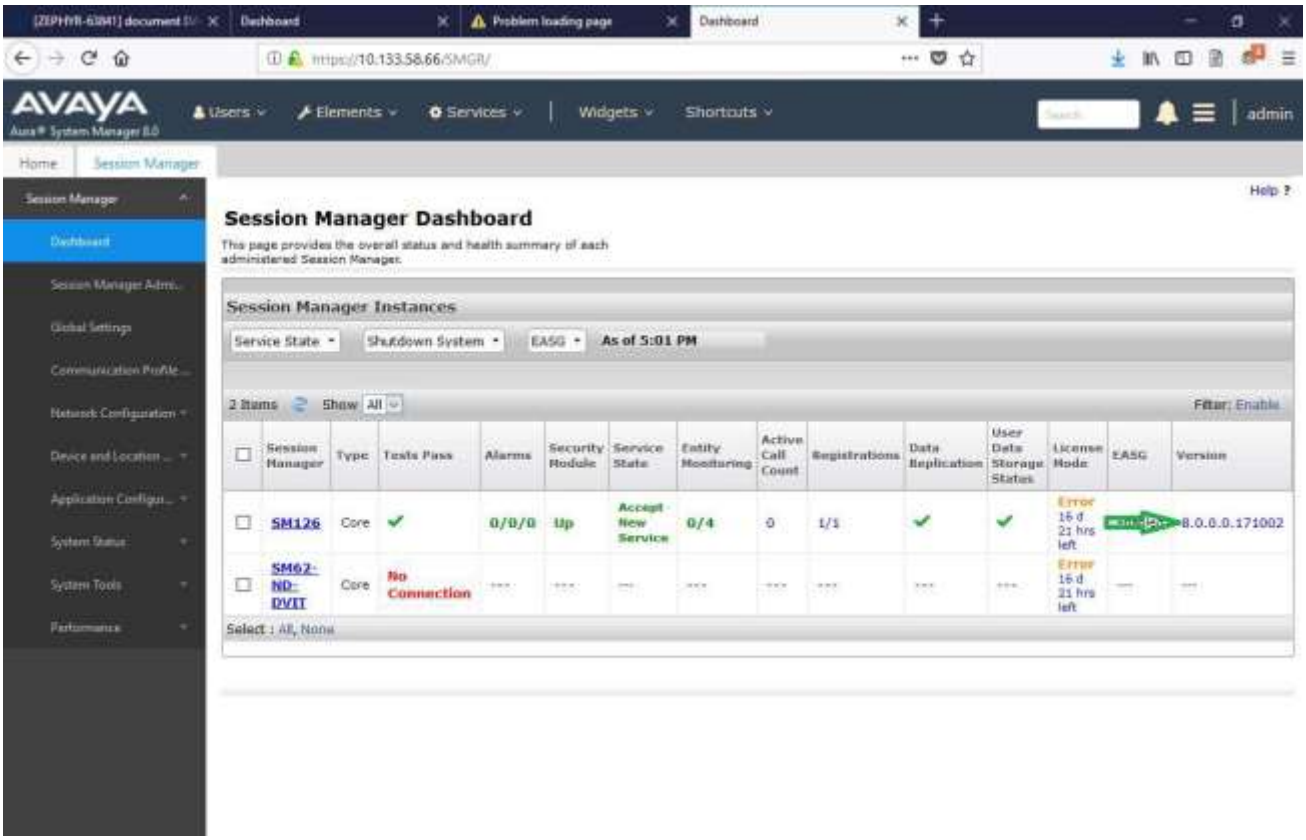
   The snap-in is responsible to provide the implementation for the HTTP service that receive the HTTP POST requests from Avaya Aura® Media Server. It is relatively easy to configure httpd (running on a non-Avaya Breeze® platform server) to serve up announcement files. This same simple configuration cannot be used to store incoming files, however.

4. If the Announcement/Recording URL is `https://`, Avaya Aura® Media Server must be configured to trust the certificate that is presented by the fileserver/snap-in. Please see Deploying Avaya Breeze® platform for details on how to properly configure trust for the media server.

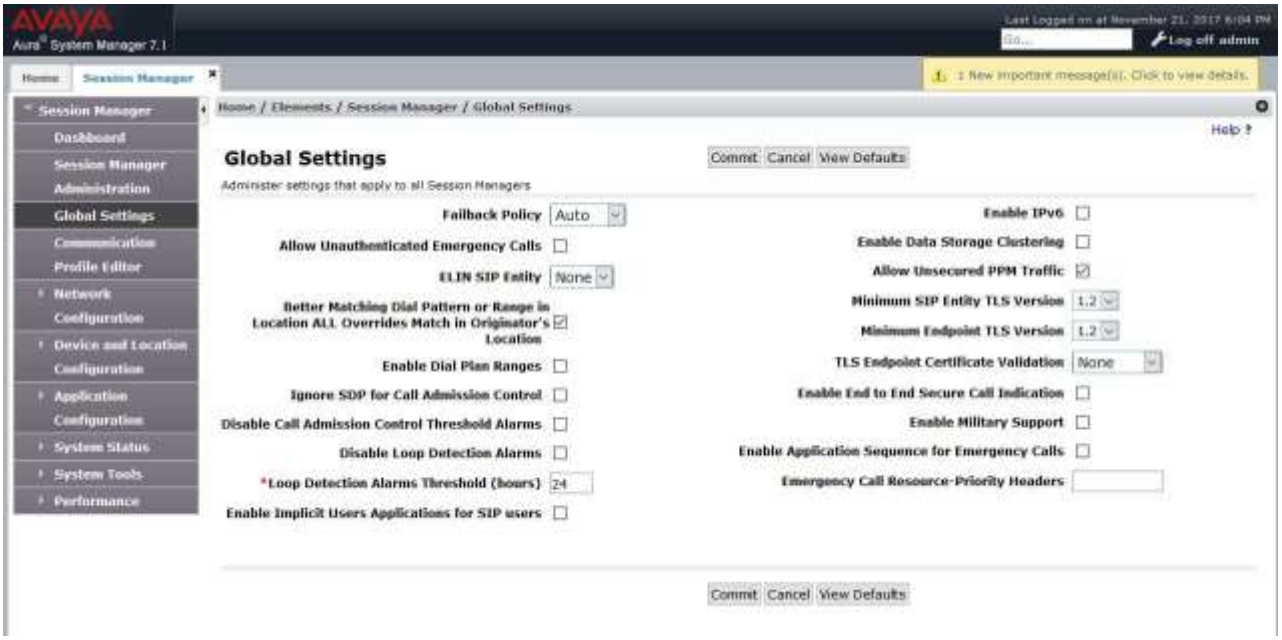
I've set up an implicit sequence pattern so that Session Manager routes calls to Avaya Breeze® platform, but some calls that match my pattern are not sent to Avaya Breeze® platform. What might cause this?

Solution

1. Login to System Manager and go to **Home > Session Manager**



2. Go to "**Global Settings**" page and verify that the **Enable Implicit Users Applications for SIP users** configuration is selected.



How can I stop Avaya Breeze® platform from logging me out of an SSH session?

About this task

This is actually a security feature that will log you out after a few minutes of inactivity.

Procedure

1. While logged in to your Avaya Breeze® platform server, you can disable the timer by entering this command: `unset TMOUT`
2. Or, you can set it to a longer interval with this command: `export TMOUT=<number of seconds>`

Why don't I see my service alarm on System Manager or Data Center?

Solution

1. Verify Avaya Breeze® platform Serviceability Agent's configuration for User and Target profiles.
2. If not configured properly, reconfigure correctly. Refer to appropriate section for alarming configuration section in Administering Avaya Breeze® platform.
3. Verify Serviceability agent is running on the Avaya Breeze® platform instance using the `command service spiritAgent status`.
4. If the service is down start the service. The `command is "service spiritAgent start"`.
5. Verify the event is logged in the `/var/log/Avaya/services/event.log` file.
6. If the event is not logged check server logs for exceptions.

Why is access to my service so slow or sometimes not accessible?

Look at other FAQs, such as "Why is my service not accessible" and "Why is my service not getting invoked"

Avaya Breeze® platform changes the system state to the Overload state when CPU, the WebSphere memory, or the disk usage exceeds a set threshold. The system exits the Overload state when all the three usage levels drop below the clearing thresholds. In Avaya Breeze® platform Release 3.9, the thresholds are:

- **CPU use**: The Avaya Breeze® platform, system would enters the Overload state when CPU usage is 80%. The system exits the Overload state when the usage of CPU drops to 60%.
- **WebSphere memory use**: The Avaya Breeze® platform system memory enters the Overload state when the memory usage is 90%. The system exits the Overload state when the memory usage drops to 85%.

- **Disk use**: The Avaya Breeze® platform system disk use enters the Overload state when usage is 90%. The system exits the Overload state when the disk use drops to 70%. The system monitors the root(/), /var, and /data partitions for overload. Look at the activity status on Avaya Breeze® platform Server Administration screen. If there is excess activity on Avaya Breeze® platform, the service access might be slow.

How can I have my service not show “Not Applicable” for my service?

You cannot create a licensed service. Licensed services are only provided by Avaya. Some of these services are – WebRTC, Avaya Breeze® platform, etc.

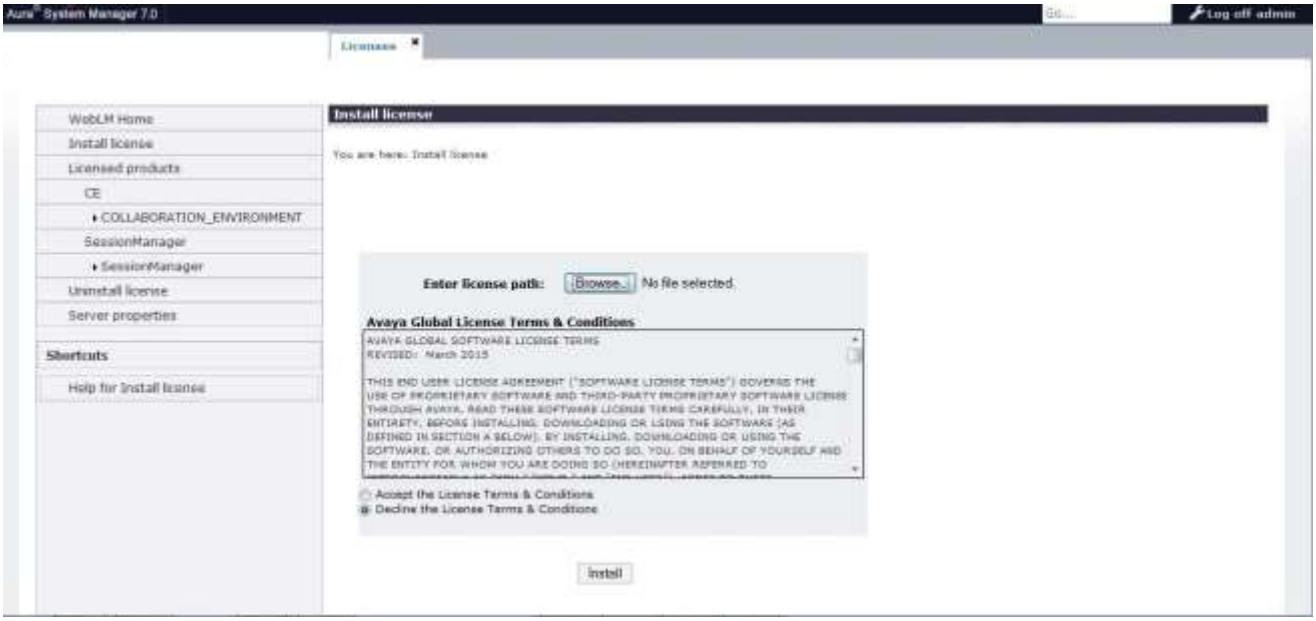
Why does my service show a warning icon with a date?

Cause

This means that you have not installed a license file for the licensed service. It is very important that you see a green checkmark for your service.

Solution

To make sure you install appropriate license for your service, on System Manager, from **Services**, click **Licenses**.



Once you install the license, it takes a maximum 9 minutes for the License mode to update with a green check mark.

When the grace period is expires, the license state changes to restricted mode and the snap-in is uninstalled from the cluster.

Why do I have call failures when using APIs which use Avaya Aura® Media Server?

Cause

Avaya Aura® Media Server may not be configured properly.

Solution

Check with your administrator to confirm that the configuration of Avaya Aura® Media Server has been performed as described in *Deploying Avaya Breeze® platform*. Also ask your administrator to confirm that Avaya Aura® Media Server is licensed.

My service is invoked and it runs media operations, or indicates that it might run media operations. Why does the call seem to stall?

If your service invokes Call.enableMediaBeforeAnswer() or runs a media operation within the callIntercepted callback in your class that implements CallListener and is annotated with @TheCallListener, then Avaya Breeze® platform will attempt to include the Avaya Aura® Media Server in the call. As part of the call setup, Avaya Breeze® platform will instruct the Avaya Aura® Media Server to initiate a call to your service. Your service must be configured to accept this call. Check the CARRule.xml file (if you used the service archetype to start writing your service, the CARRule.xml file can be found under yourService-war/src/main/resources) – it should include a TerminatingServiceRule element. Here is an example:

```
<?xml version="1.0" encoding="UTF-8"?>

<ServiceRules name="${serviceName}" version="${serviceVersion}"

xmlns:xs="http://www.w3.org/2001/XMLSchema-instance">

<!-- Following section is needed for call related applications. Refer HelloWorld Sample service for
more clarifications. If your application is HTTP only, please remove the SequencedServiceRule
tags. You can refer DynamicTeamFormation Sample service in SDK for help on http only service
-->

<SequencedServiceRule phase="imsterm" order='125'

desc="Interested in imsterm phase">

</SequencedServiceRule>

<SequencedServiceRule phase="imsorig" order='25'
```

```
            desc="Interested in imsorig phase">
        </SequencedServiceRule>
        <TerminatingServiceRule desc="for callback to CMATestService">
            <FeatureURI>CMATestService</FeatureURI>
        </TerminatingServiceRule>
    </ServiceRules>
```

The TerminatingServiceRule element contains a child FeatureURI element, the value of which must be the same as the service name.

How do I know if the attribute was changed at the global level, cluster level, or service profile level?

The call back method objectChanged(object,object) will get invoked with arguments of different types on attribute change notification. If the arguments are of type “DefaultAttribute” then attribute was changed at the global level. If they are of type “ClusterDefaultAttribute” then at Cluster level and if “AusAttribute” then at Service profile level.

Why do I get the attribute change notification with “newObject = null” when I change the cluster level value of an attribute to its default by doing an uncheck from the GUI?

An attribute change notification only tells you which attribute got changed and at what level. To get the attribute value you should always use the apis “serviceData.getServiceAttribute(attributeName)” or “serviceData.getServiceAttribute(useraddress, attributeName)”.

My callable service is not invoked and an error is received

– ERR104 No callable service was found for <user@domain>

Solution

The service profile assigned against the implicit user pattern does not contain your snap-in. Make sure to follow callable service administration guide and make sure to add your callable snap-in to service profile against desired implicit user pattern.

If I do an addParticipant() operation from my Callable Service, I see an INVITE sent back to Session Manager with the original Request URI, resulting in a 404 error.

Solution

The Callable Service number might be associated with a Session Manager Application Sequence. This number must be associated with a Route Pattern even if the Service Profile is configured with both Call Intercept and Callable Services features.

Identifying if my snap-in is invoked as a sequenced snap-in or is invoked as a callable service

About this task

Call.wasServiceCalled() API can be used to distinguish between both the above scenarios. Refer to SDK Javadocs for more details.

How can I debug Out of Memory issues on the server?

To debug Out of Memory problems on Avaya Breeze® platform, take the heapdump from the location /var/log/Avaya/sm/. The file has an extension .hprof. Look for the one you want to debug. Open this heapdump with Eclipse Memory Analyzer Tool (MAT) and analyze the dump. You can also look at it using the HeapAnalyzer from IBM, available on the IBM HeapAnalyzer web page.

How can I debug threading issues on the server?

The core files for analysis are available at /var/log/Avaya/sm/ . The file name is in the format javacore.*. Open this file using the IBM Thread Analyzer Tool and look for any deadlocks or blocked threads for analysis.

You can also go through the javacore* files to look at reasons why core was created. Also, match this with Text* files during the time when core was created.

How do I list snap-in attributes?

list_snapin_attr.sh – lists the attribute value for a given snap-in, if specified, and all services if no snap-in is specified. Log in to the Avaya Breeze® platform console and execute.

It will list the values at the global, cluster and service profile levels.

Example

```
$ list_snapin_attr.sh HelloWorld
-----------------------------------------------------------------------------------------------------------
              Attribute values for Snapin HelloWorld
        Name          | Factory default | Override
----------------------+-----------------+----------
 com.avaya.supplierId | 10000000        |
 displayString        | Hello from EDP  |
(2 rows)

              Attribute value overrides by cluster for Snapin HelloWorld
 Cluster  |     Name      |       Value
----------+---------------+-------------------
 GPSanity | displayString | Hello from Breeze
(1 row)

              Attribute values by profile for Snap-in HelloWorld
 Profile |     Name      |      Value
---------+---------------+-----------------
 Hello   | displayString | Hello from Abcd
(1 row)

              End of Attribute Snapin HelloWorld
-----------------------------------------------------------------------------------------------------------
```

Why do responses to my MessageReceiver, EmailListener, SmsListener arrive late or not at all

Condition

Responses to my MessageReceiver (Collaboration Bus API) / EmailListener (Email API) / SmsListener (SMS API) arrive only after a many second delay or never arrive.

Cause

If you are using the Collaboration Bus (or the Email and SMS APIs, which use the Collaboration Bus) from an Enterprise Java Bean (EJB), a certain coding pattern can result in this behavior. Examples of this type of coding pattern are:

- A method on the EJB called "sendMyMessage" sends a message to a channel. The sendMyMessage method then waits for a response from the channel to arrive at the MessageReceiver before returning control to the invoking software.
- A method on the EJB called "sendMyMessage" creates an EmailRequest and then invokes "EmailRequest.send()". The sendMyMessage method then waits for a response to arrive at the EmailListener before returning control to the invoking software.
- A method on the EJB called "sendMyMessage" creates an SmsRequest and then invokes "SmsRequest.send()". The sendMyMessage method then waits for a response to arrive at the SmsListener before returning control to the invoking software.

With this coding pattern the response may not be delivered to the listener as long as control remains in the sendMyMessage method. This condition is a result of the EJB framework attempting to enforce a transaction.

Solution

Since the Collaboration Bus has been designed not to participate in transactions, it is necessary to disable transaction processing in the EJB when a coding pattern is used that leads to this

condition. To disable transaction processing, add the following annotation at the class level to the definition of the EJB:

```
@TransactionAttribute(value = TransactionAttributeType.NOT_SUPPORTED)
```

When I do a play announcement or a prompt and collect media operation, why is the announcement/prompt not heard?

Condition

When I do a play announcement or a prompt and collect media operation, the announcement/prompt is not heard.

Solution

1. Double check that the announcement/prompt is being played to the intended participant. For example, if the announcement has been played only to the caller (as opposed to the call), the announcement cannot also be heard by the callee.
2. Consider the possibility that the file format of the recording is not a supported format. For best performance, the recommended format is a 16 bit, 8 kHz, single channel (mono), PCM WAV file. Additional information about other supported formats can be found in *Implementing and Administering Avaya Aura® Media Server*.

Why does log_space in properties.xml not reserve the same log space for my snap-in?

Condition

The *log_space* specified in properties.xml does not reserve the same log space for my snap-in on Avaya Breeze® platform though I see the specified value on the Service Management page on Avaya Aura® System Manager.

Cause

The log space is usually reserved once when a snap-in is first installed. When a version of a snap-in is already installed, the log space is not altered when another version of the same snap-in with a different *log_space* value is installed.

Solution

Uninstall all versions of the same snap-in and reinstall the snap-in version with the modified *log_space* value.

Test Connection action for TLS supported JDBC Datasource does not succeed even after all the correct configurations

Test connection can fail for multiple reasons:

1. Please check that you installed third-party certificates (Trust certificates for database server) on the required Avaya Breeze® platform cluster.
2. Please check that all the correct custom properties for TLS support as required by DB driver are set for JDBC data source. For example, few DB drivers need a property "ssl" with value as "true" to be passed as a custom property.
3. Please check that the DB server is configured to listen and accept TLS connections.

Why was an IllegalStateException with a detail message of "AMS is not configured" thrown?

Cause

Avaya Aura® Media Server is not configured properly, and your snap-in is attempting to perform an operation that requires a media server to be included in the call.

Solution

Check with your administrator to confirm that the configuration of Avaya Aura® Media Server has been performed as described in *Deploying Avaya Breeze® platform* .

Why does a call that performs a media operation not work? I see that the asm logs complain of invalid credentials.

Cause

The Avaya Aura® Media Server Rest Configuration is configured for Basic Authentication but Avaya Breeze® platform is not presenting valid credentials.

Solution

Check with your administrator to confirm that the cluster attributes of **Avaya Aura® Media Server User Id for RESTful TLS authentication** and **Avaya Aura® Media Server - Password for RESTful TLS authentication** have been configured with a user ID and password that match those configured in the REST configuration of Avaya Aura® Media Server.

See *Deploying Avaya Breeze® platform* for more information.

Why does a call that performs a media operation not work? I see that the asm logs complain of SSL and/or TLS and/or certificate issues.

Cause

The configuration of TLS for communication with Avaya Aura® Media Server through its REST interface is incorrect. This error can sometimes indicate a problem where a certificate on Avaya Breeze® platform used to communicate with Avaya Aura® Media Server is incompatible with the certificate on Avaya Aura® Media Server used for the communication.

Solution

1. Check with your administrator to confirm that the configuration of Avaya Aura® Media Server has been performed as described in Deploying Avaya Breeze® platform. One area to double check is that the proper certificate has been assigned to the service profiles on Avaya Aura® Media Server (**Security > Certificate > Management > Key Store**).
2. Additionally, if the error refers to the version of TLS that is in use, try configuring a higher version of TLS on Avaya Aura® Media Server (**System Configuration > Network Settings > General Settings**).
1.

Why does the PlatformListener class not getting the notification

Solution

Check whether the class annotated with @ThePlatformListener has either default constructor (i.e., no constructors defined) or a public constructor with no arguments. Because platform will be initializing an instance of the class at runtime and it expects a public constructor with no arguments.

Why does a service declaring dependencies on the cluster database, the reliable eventing group, or the datagrid show a yellow triangle when a cluster is selected for installation from the Service Management or Bundles page or when it is assigned to the cluster from Cluster Editor?

Cause

The service might have declared a dependency on the cluster database, the reliable eventing group, or the datagrid when one of the dependencies is unavailable. You can view the dependency with problems in the tooltip which is displayed by hovering your cursor on the yellow triangle.

If one or more snap-in dependencies are unavailable or become erroneous, the snap-in might be stopped based on the rules specified by the snap-in developer.

Resolve this problem to automatically start the snap-in.

Solution

1. On the Server administration page, click the service install status icon for a node in the cluster.
2. Select the stopped snap-in, and click Start Service.
3. Repeat the process for each node in the cluster

What are the trace tools available for debugging environment/snap-in issues on Avaya Breeze® platform?

There are a variety of Serviceability tools available for Avaya Breeze® platform.

traceMsg is the main tool using which you can trace various service of Avaya Breeze® platform – HTTP, SIP, Collaboration Bus, Snap-ins, TLS handshake.

Please refer to “Chapter 9 : Serviceability Tools” of the “Maintaining and Troubleshooting Avaya Breeze® platform” guide for details.

Why are the trusted certificates bundled in my snap-in not getting installed when I install my snap-in?

See *Avaya Breeze® platform Snap-in Development Guide* for the procedure to include certificates in the snap-in. Check the following aspects:

1. Ensure the trusted certificates are correctly included in the snap-in.

2. Unzip the snap-in and check that there is a certs directory in the svar file.
3. Confirm that the snap-in is an Avaya Signed snap-in.
4. Check that the certificates are of the correct format, such as .pem, and .crt.
5. Avaya Breeze® platform nodes in the cluster where snap-in is being installed are accessible.

Outgoing Requests from my snap-in do not work, even though certificates are part of my snap-in and the trusted certificates are installed on Avaya Breeze® platform servers?

Outgoing Requests might not work when you need more certificates if the enterprise network where the snap-in is being installed is connected to a proxy server. All the requests might be transmitted through the proxy server.

If the enterprise network is connected to a proxy server, see *Administering Avaya Breeze® platform* to add a certificate to the Avaya Breeze® platform trust store.

Why does loading the snap-in fail with the "Properties" file is missing the mandatory smgr element" error message?

Condition

The snap-in loading fails with the error message: Properties file is missing the mandatory smgr element.

Cause

The properties.xml does not include the "smgr" element.

Solution

Add <smgr></smgr> in properties.xml.

For more information, see *Avaya Breeze® platform Snap-in Developer Guide*.

Why does loading the snap-in fail with the “The Factory_Override missing one or more elements: name, type or factory sub element” error message?

Condition

The snap-in loading fails with the error message: The Factory_Override missing one or more elements: name, type or actory sub element

Cause

The snap-in loading fails with the error message: Factory_Overrive element must include name, type and factory

Solution

Check whether the Factory_Override element includes the following parts: name, type, and factory

Why does loading the snap-in fail with the “The Factory_Override type must be STRING,INTEGER or BOOLEAN” error message?

Condition

The snap-in loading fails with the error message: The Factory_Override type must be STRING, INTEGER or BOOLEAN

Cause

The type of Factory_Override is not STRING, INTEGER, or BOOLEAN.

Solution

Change the type of Factory_Override to the required type.

Why does loading the snap-in fail with the “Attribute_override must include at least one factory_Override element” error message?

Condition

The snap-in loading fails with the error message: Attribute_override must include at least one factory_Override element

Cause

Attribute_override does not include the factory_Override element

Solution

Add factory_Override element under Attribute_override

Why does loading the snap-in fail with the “Attribute_override must include at least one override_SnapinAttribute element” error message?

Condition

The snap-in loading fails with the error message: Attribute_override must include at least one override_SnapinAttribute element

Cause

Attribute_override does not include the override_SnapinAttribute element

Solution

Add the override_SnapinAttribute element under Attribute_override.

Why does loading the snap-in fail with the “factory_override element type must match snapin element type” error message?

Condition

The snap-in loading fails with the error message: factory_override element type must match snap-in element type

Cause

The type of the factory_override element and the snapin attribute do not match.

Solution

Ensure that the type of the factory_override element and the snapin attribute match.

Why does loading the snap-in fail with the “no match Attribute in snapin” error message?

Condition

The snap-in loading fails with the error message: no match Attribute in snapin

Cause

Cannot find the matched snap-in

Solution

Ensure that the attribute name of the snap-in is correct.

Why do asm.log and server.log contain DAO WARN message?

Condition

asm.log shows WARN message – “2018-04-11 12:33:31,955 [SoapConnectorThreadPool : 0] asm.datamgr.DMFactory WARN - Calling component not registered with the DMFactory: ClassLoader Name=null(-20141473_1453608023). Not tracking 'ZephyrDM' against this Class loader. Requested DataMgr is NOT currently tracked under a different Class Loader, so this will cause a performance problem due to frequent reinitializations. Class loader IDs stored in appMap: 150919542_-1356920990”

server.log shows WARN message – “2018-04-11 12:35:14,775 WARN [com.avaya.asm.datamgr.DMFactory] Calling component not registered with the DMFactory: ClassLoader Name=null(978764392_1984697014). Not tracking 'AsmInstanceDAO' against this Class loader. Requested DataMgr is NOT currently tracked under a different Class Loader, so this will cause a performance problem due to frequent reinitializations. Class loader IDs stored in appMap:: java.lang.Throwable”

Cause

DAO is loaded by some other class loader. If the application goes away, DAO might collect garbage collected. DAO restarts when you gain access to it next time.

Solution

- If the WARN message is from Avaya Breeze® platform classes, ignore the warning.
- If the WARN message is from the snap-in classes, you can prevent the warning by doing a DMFactory.getInstance().register(‘some_object’) from the init() method of the ServiceLifeCycle class or from postConstruct() method of a startup bean.

  ‘some_object’ is an object that is available throughout the snap-in lifecycle. This ensures that the DAO does not collect garbage throughout the snap-in lifecycle.

Why do some calls through Avaya Breeze® platform fail immediately?

Cause

Calls are initiated with an INVITE that contains an SDP offer, which contains the media connection information of the call initiator. However, some far end implementations, including some older versions of earlier than Communication Manager Release 5.0 initiate calls with an INVITE that does not contain an SDP offer. Avaya Breeze® platform is not capable of processing these INVITEs causing the calls to fail immediately.

Solution

Modify the initiator of the call to send INVITEs that contain an SDP offer or remove Avaya Breeze® platform from the signaling path.

Why is Avaya Breeze® platform in system overload for disk space?

Cause

Avaya Breeze® platform system could be in overload state if log files have filled up the disk.

Solution

1. Log in to the Avaya Breeze® platform server using CLI.
2. Go to the log directory: /var/log/Avaya
3. Run the “ls -l” command in the log directory or its subdirectories to check which files are consuming a large amount of disk space
4. Clear the log files using the “ce logclear <service name>” command on services whose log files are consuming a large amount of disk space. This will delete all the specified service logs except the latest log.
5. Clear the log files using “ce logclear -a” command if the /var/log/Avaya/sm logs are consuming a large amount of disk space. This will delete all the asm and TextLog files except latest log files.

Chapter 5: Connector debugging

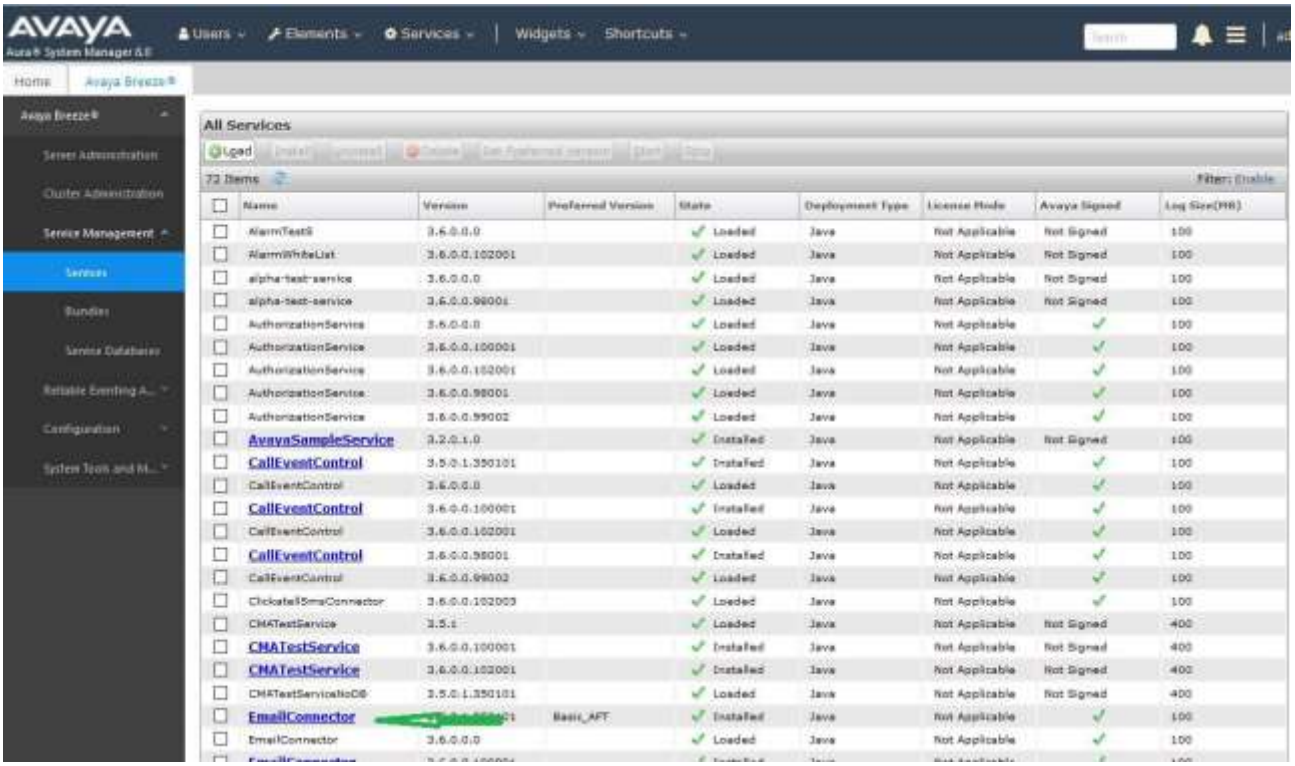
Why was email not sent from my service?

Solution

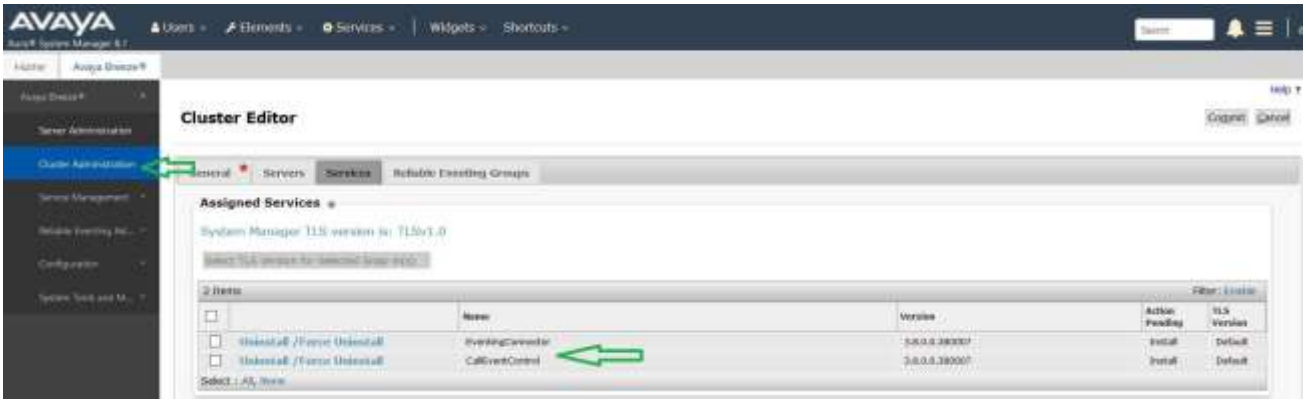
1. Please check that the email connector is installed on the Avaya Breeze® platform Server.

   By default when you get set up a system, the EmailConnector is only Loaded and not installed.

2. Log in to System Manager.
3. On the System Manager Home page, select **Avaya Breeze® platform** from the Elements panel.
4. In the Avaya Breeze® platform page, select **Service Management > Services** from the menu.
5. Check if the EmailConnector is installed.



6. To check if Email connector is installed for your cluster, go to **Cluster Administration**.
7. Select your cluster and **Edit**.
8. Go to Services tab to verify that the connector is installed.



9. Go to **Configuration > Attributes** in left navigation and select the **Service Globals and Service Clusters** tab.
10. From the **Service** menu, select **EmailConnector**.
11. Make sure the details provided for email server, host are correct.
12. Based on the burst of emails that your server is sending, please configure the setting for **Maximum Number of Emails to Send per Run, Maximum Age of an Email Request inOutbox, and Maximum Memory Usage for the Outbox**.

    Details about all the parameters are available in *Avaya Breeze® platform Snap-in Development Guide*.

13. Set **Test mode enabled?** to true and check if the request-response is working fine without actually sending an email.
14. Refer to the Multi-channel Broadcast Sample Service which is part of the SDK as it shows how to send an Email using the Avaya Breeze® platform APIs.

    This can be found in the SDK at <SDK-3.9 Folder>\samples\multichanbroadcast.

    Test using the multi-channel broadcast sample service once. Look at the question “How do I invoke Multi-Channel Broadcast service and Dynamic Team Formation Service for my testing?” if you need details on how to do this.

15. 15. Log in to Avaya Breeze® platform server and run this command on command line: ce dlogv EmailConnector

    This will open the debug log using the vi editor.

16. Search for your service name.

    This should provide you with information if there were any exceptions that lead to issues with invoking the service.

17. If you added logging statements in your service code, and if you used the Logger class in the Avaya Breeze® platform API (highly recommended), you can view the service log using the command `ce dlogv <serviceName>`.

    For example, to view the logs for the basicSipCall service, run the following command `ce dlogv basicSipCall`.

    The logs for different versions of a service all go to the same log file, and each log message contains the service name and version.

    When running in normal mode, logs at level INFO and higher priority (FATAL, ERROR, WARN) will be added to the log file; logs at lower priority (FINE, FINER, FINEST) will not be added to the log. The log level can be changed on the fly to provide more verbose logging.

18. Enter this command while logged in to your Avaya Breeze® platform server to enable all log levels for the Email connector: `ce dlogon EmailConnector`.
19. When you are finished debugging, you should return logging to the default using this command: `ce dlogoff EmailConnector`.

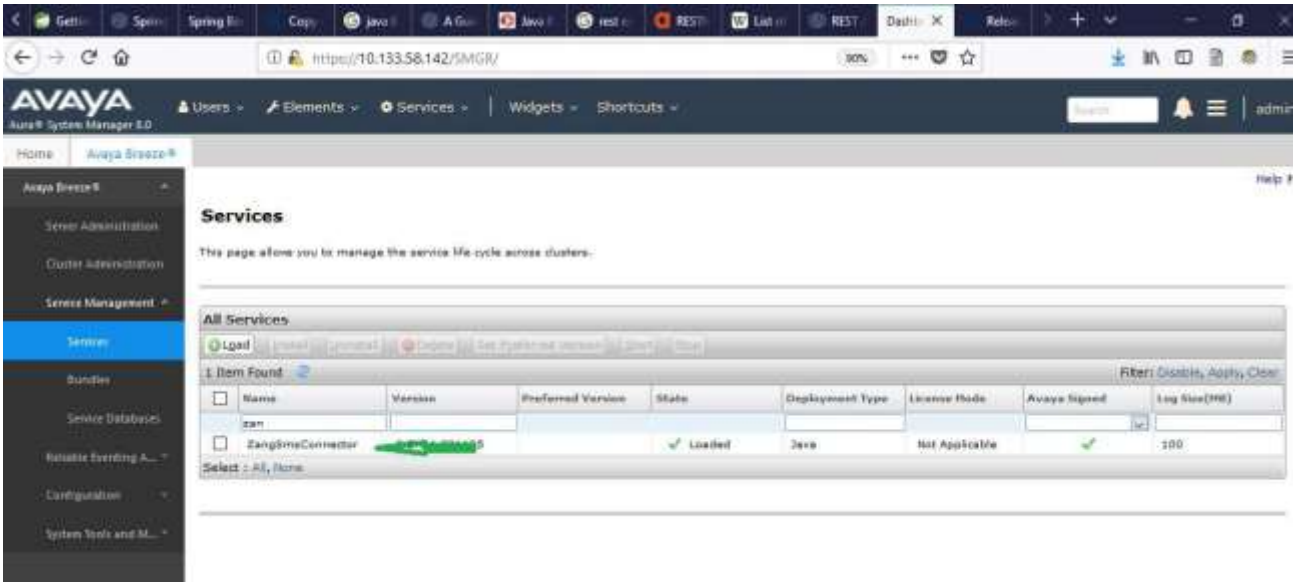
Why was SMS not sent from my service

Solution

1. Please check that the Zang SMS connector is installed on the Avaya Breeze® platform Server.

   By default when you get set up a system, the Zang Sms Connector is only Loaded and not installed. Log in to System Manager.

2. On the System Manager Home page, select **Avaya Breeze® platform** from the Elements panel.
3. In the Avaya Breeze® platform page, select **Service Management > Services** from the menu.
4. Check if the Zang Sms Connector is installed.



5. Check if Zang Sms Connector is installed for your cluster by going to **Cluster Administration**, selecting a cluster, and click **Edit**.
6. Go to **Services** tab to verify that the connector is installed.
7. If there are additional SMS connectors installed in this cluster, verify that the right connector is set as default SMS connector

   In the cluster Editor, on the General tab, ensure that value of Default SMS Connector Service attribute is set to ZangSmsConnector.
8. Go to **Configuration > Attributes** in left navigation and select the **Service Globals** tab.
9. Select **Zang Sms Connector**.
10. Ensure that the details are provided to access the Zang server is https://api.zang.io and https://pubsub.zang.io. For more details, see *Zang SMS Connector Snap-in Reference*.
11. Set the **Test mode enabled?, attribute value** to true and check if the request-response is working fine without actually sending an SMS.

    Refer to the Multi-channel Broadcast Sample Service which is part of the SDK as it shows how to send an SMS using the Avaya Breeze® platform APIs. This can be found in the SDK at <SDK-3.9 Folder>\samples\multichanbroadcast Test using the multi-channel broadcast sample service once. Look at the question “How do I invoke Multi-Channel Broadcast service and Dynamic Team Formation Service for my testing?” if you need details on how to do this.

12. Login to Avaya Breeze® platform and run this command on command line: ce dlogvZangSmsConnector.

    This will open the SMS connector log using the vi editor.

13. Search for your service name. This should provide you with information if there were any exceptions that lead to issues with sending the SMS.
14. If you added logging statements in your service code, and if you used the Logger class in the Avaya Breeze® platform API (highly recommended), you can view the service log using the command `ce dlogv <serviceName>`.

    For example, to view the logs for the ZangSMSConnector service, run the following command `ce dlogv ZangSMSConnector`.

    The logs for different versions of a service all go to the same log file, and each log message contains the service name and version.

    When running in normal mode, logs at level INFO and higher priority (FATAL, ERROR, WARN) will be added to the log file; logs at lower priority (FINE, FINER, FINEST) will not be added to the log.

15. The log level can be changed on the fly to provide more verbose logging by entering this command while logged in to your Avaya Breeze® platform server to enable all log levels for the SMS connector: `ce dlogon ZangSmsConnector`
16. When you are finished debugging, you should return logging to the default using this command: `ce dlogoff ZangSmsConnector`
17. Ensure that the SMS request has the valid Zang SMS enabled number being set as the From number
    Ensure that a valid SMS To number is being set in the request.

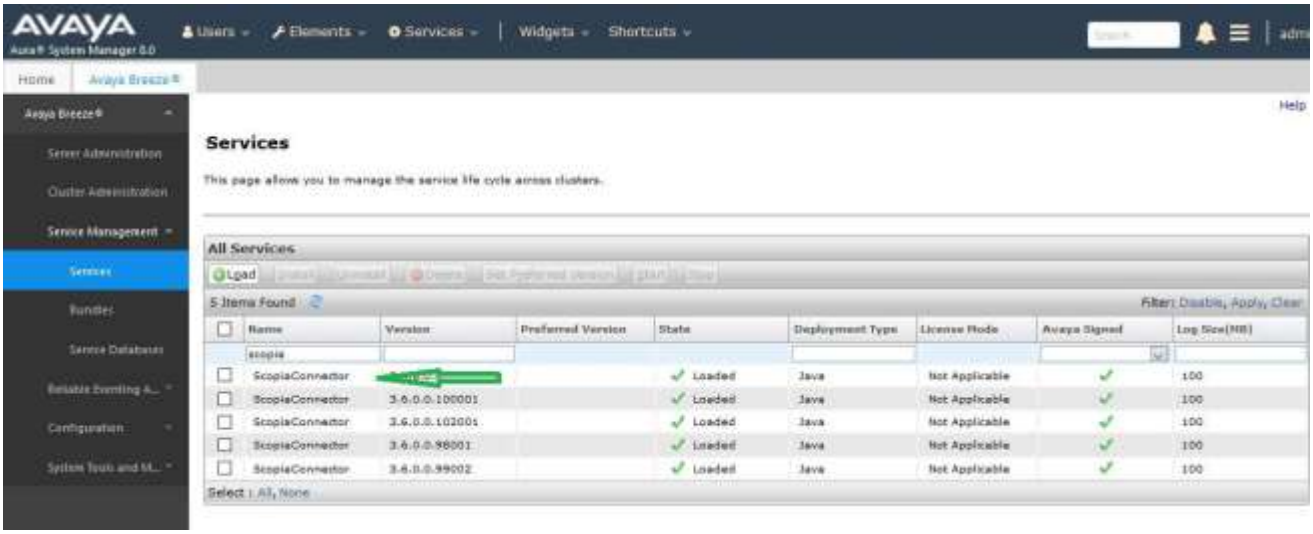
Why was Scopia conference not scheduled from my service?

Solution

1. Please check that the Scopia connector is installed on the Avaya Breeze® platform Server.

   By default when you get set up a system, the ScopiaConnector is only Loaded and not installed. Log in to System Manager.

2. On the System Manager Home page, select **Avaya Breeze® platform** from the Elements panel.
3. In the Avaya Breeze® platform page, select **Service Management > Services** from the menu.
4. Check if the ScopiaConnector is installed.



5. To check if ScopiaConnector is installed for your cluster, go to **Cluster Administration**, select your cluster and click **Edit**.
6. Go to Services tab to verify that the connector is installed.
7. Go to **Configuration > Attributes** in left navigation and select the **Service Globals** tab. Then select **ScopiaConnector** from the drop down for Service.
8. Make sure the details provided for Scopia server address and port is correct. Also, you must have a valid login on the server which you use in User name and password field. Details about all the parameters are available in.
9. Try to launch the URI that you provide in **URI for Conference Access**– You should be able to get to the Scopia Desktop.
10. If you try to call the number specified in **Dial-in Number for Conference Access**– You should hear the attendant announcement.
11. Set **Test mode enabled?** to true and check if the request-response is working fine without actually scheduling a conference on your scopia server.
12. Refer to the Dynamic Team Formation Sample Service which is part of the SDK as it shows how to schedule a Scopia conference using the Avaya Breeze® platform APIs. This can be found in the SDK at <SDK-3.9 Folder>\samples\ dynamicteamformation.
13. Test using the dynamic team formation sample service once to verify Scopia server set up is correct. Look at the question “How do I invoke Multi-Channel Broadcast service and Dynamic Team Formation Service for my testing?” if you need details on how to do this.
14. Log in to Avaya Breeze® platform server and run this command on command line: ce dlogvScopiaConnector
    This will open the debug log using the vi editor.

15. Search for your service name.

    This should provide you with information if there were any exceptions that lead to issues with scheduling the conference.

16. If you added logging statements in your service code, and if you used the Logger class in the Avaya Breeze® platform API (highly recommended), you can view the service log using the command `ce dlogv <serviceName>`.

    For example, to view the logs for the basicSipCall service, run the following command `ce dlogv basicSipCall`

    The logs for different versions of a service all go to the same log file, and each log message contains the service name and version.

    When running in normal mode, logs at level INFO and higher priority (FATAL, ERROR, WARN) will be added to the log file; logs at lower priority (FINE, FINER, FINEST) will not be added to the log. The log level can be changed on the fly to provide more verbose logging.

17. Enter this command while logged in to your Avaya Breeze® platform server to enable all log levels for the SMS connector: `ce dlogon ScopiaConnector`

18. When you are finished debugging, you should return logging to the default using this command: `ce dlogoff ScopiaConnector`

Why do I see the following services – EventingConnector and CallEventControl installed on most cluster types?

These are default services from Avaya Breeze® platform and are needed for functioning of Avaya Breeze® platform. These cannot be removed as long as the Avaya Breeze® platform server is part of the cluster and is needed to be functional.

Chapter 6: HTTP Load Balancing and High Availability

How to enable/disable HTTP load balancer in a cluster?

About this task

By default, the HTTP load balancer is set to disabled when creating a new cluster.

Procedure

1. To change the HTTP load balancer state, go to the Cluster Administration page,
2. Select and edit the cluster.
3. Click the Is load balancer enabled check box.
4. Click **Commit**.

How to locate the HTTP load balancer nodes in a cluster?

After you have enabled the HTTP load balancer and added at least two or more servers into the cluster, the System Manager will automatically pick up two Avaya Breeze® platform servers in the cluster to serve the load balancing roles. You can find out the HTTP load balancer state on Cluster Administration page. The colored icon indicates the active load balancer node and the grayed-out icon indicates the standby load balancer.

You also can verify the load balancer status from the command line on the server. For example: $ sohctl –dls

curr=ST_HA_ACTIVE new=ST_HA_ACTIVE prev=ST_HA_ACTDISC ACTIVEfor=00000:03:08:14:905.

How is the cluster IP address used on the load balancer?

The cluster IP address will be assigned as an IP alias to eth1:0 interface on active load balancer server. The client should send the HTTP/s request to this IP address and load balancer will distribute the request to one of the upstream servers. The standby load balancer will take over this cluster IP address to become active when failover occurs.

Why hasn't the cluster IP address been assigned to any of the servers?

Cause

This condition should not happen unless both active and standby load balancer servers are down or the load balancer was disabled at this time.

Solution

1. Make sure load balancer is enabled.
2. Locate the active and standby load balancer servers.
3. Ping management and secure module interfaces on each server
4. Make sure secmod is running (by running the statapp command).

5. Has cluster administration page been “Commit”ed properly?
6. Make sure the cluster IP address is of the same subnet as the Avaya Breeze® platform servers.

What if planned maintenance needs to be done on active load balancer node?

If you have to manually bring down the server with active load balancer running for any reasons (e.g.,. software upgrade, hardware replacement,…), you must put this server into Deny New Service state from Server Administration page. That triggers a failover and the standby load balancer will take over the active role within several seconds. By doing this, the server downtime will be minimal with less service affecting.

What if an unplanned failover happened?

In the cases of power outage, network outage, and hardware failure, the standby load balancer will be promoted to active if the failure condition only affected the active load balancer. If both active and standby load balancer servers are affected, the load balancer will be re-established as in previous status once the failure conditions are cleared.

Why do I see both load balancers are in active state?

Cause

This condition is called “Split Brain” that is usually caused by the network connection issues. When standby load balancer cannot reach to the active load balancer server thru both management and security module interfaces, it believes itself is the only active server. The standby load balancer will promote itself to become the active load balancer. In the meantime, the previous active load balancer is still up and running, but most likely the server might have lost the network connection.

Solution

No action is required in this case. The high availability arbiter will resolve this tie break once the network issue is cleared and both load balancers are able to resume the keepalives between them.

How can I tell when the HTTP Load Balancer failed over?

The easiest way is to check on the load balancing icons on Server Administration or Cluster Administration page. You can also use command line command to list the most recent histories of load balancer on the servers. For example:

```
$ sohctl -lh
!!! Listing only 3 most recent entries for each HealthObject !!!
Resource=replication:
    HealthObject:
    ce_failover :
        INFO 2014:07:09-15:06:47:844 O_IVDM52413 "DEMOTED took=001340 ms "
        CLEARED 2012:07:09-10:48:59:000 O_CVDM52606 "reconnected to farend"
        ALARM 2012:07:09-10:48:58:000 O_AVDM52606 "farend NOT reachable SPLIT BRAIN may have
        occurred"
Resource=keepalive:
    HealthObject:
    kapath_0 :
        CLEARED 2012:07:09-10:48:59:000 O_CVDM52502 "path established 10.129.176.147
>10.129.176.145"
        ALARM 2012:07:09-10:48:58:000 O_AVDM52502 "path not up ne=10.129.176.147
fe=10.129.176.145"
        ERROR 2012:07:09-10:48:57:000 O_EVDM52502 "path not up ne=10.129.176.147
fe=10.129.176.145"
    kapath_1 :
        CLEARED 2012:07:09-10:48:59:000 O_CVDM52502 "path established 10.129.176.148
>10.129.176.146"
        ALARM 2012:07:09-10:48:58:000 O_AVDM52502 "path not up ne=10.129.176.148
fe=10.129.176.146"
        ERROR 2012:07:09-10:48:57:000 O_EVDM52502 "path not up ne=10.129.176.148
fe=10.129.176.146"
```

How does the load balancer distribute requests in a cluster?

After the load balancer is enabled, all servers in the cluster will be put into the upstream server list, including active and standby load balancers. By default, requests are distributed to all the upstream servers by using a weighted round-robin balancing method.

The load balancer supports failure detection. It will retry the request against the next available upstream server if a server failed to respond to a request with timeout or 5xx error in the response.

How can I tell whether the load balancer distributes the traffic evenly in cluster?

Load balancer uses round-robin to spread traffic evenly between servers in the cluster. For the traffic monitoring, there is no centralized management reporting tool for the traffic and throughput today. You can get details from logs in the following areas if the dive-in investigation is needed:

- Load balancer (/var/log/Avaya/asset/nginx_error.log)

- WebSphere (/var/log/Avaya/sm/TextLog*)
- Snap-in (/var/log/Avaya/services/<*snap-in service name*>)

How do I redirect Http Request with Load Balancer ?

Condition

There appears to be a different way that WebSphere handles relative URLs for servlet redirect. If we send a relative URL like "../../Something.html" to HttpServletResponse#sendRedirect, the relative path should be relative to the requested URI. WebSphere seems like not implementing this behavior correctly. Instead, it appears to interpret it as relative to the app context and servlet mapping. Here are the alternatives to resolve the case:

Solution

1. (1) Use request.forward() to relative path, or (2) sendRedirect() to absolute path.
2. The cluster IP address for absolute URL can be retrieved by couple different ways if HTTP load balancer is enabled:
   - "Host" from request header that contains the cluster IP
   - SDK API ClusterData.getClusterIP() returns cluster IP

How does Session Affinity work on load balancer?

You can enable the Session Affinity on load balancer if session persistence is required. The client's IP address will be used as a hashing key to determine which upstream server should be selected for this request. The method ensures that requests from the same client will always be passed to the same server except when this server is unavailable. In the latter case client requests will be passed to another server in round-robin fashion. Most probably, it will always be the same server as well.

Alternatively, snap-ins may override the hashing algorithm by specifying the IP address of a specific Avaya Breeze® platform instance in an "affinity" query parameter. For example, https://myClusterFqdn/services/mySnapIn?affinity=192.168.0.10.

If you would like the client IP address to be used for load balancing instead of the last hop IP address in a series of reverse proxies being traversed, please work with your administrator to configure the Cluster Attribute **Trusted addresses for converting to use X-Real-IP for session affinity**. This will make sure that when a client makes a HTTP request to Avaya Breeze® platform via Reverse proxies like Avaya Session Border Controller for Enterprise, the X-Real-IP header gets used for load balancing instead of the Avaya Session Border Controller for Enterprise IP address for load balancing.

Chapter 7: Eventing Framework

Why do I stop receiving events after 8-9 hours?

Cause

Subscriptions have an expiration time associated with them. This expiration time is currently set to 8 hours. Your service will receive an event "EventFamilyEventing.EVENT_SUBSCRIPTION_EXPIRING_QUALIFIED" when its subscription is about to expire.

Solution

When you receive this event, invoke the "renewSubscription" method on the Eventing Service, passing the payload that was in the received event.

How can I tell which subscriptions were matched when an event is sent?

Procedure

1. Turn debug logging on with the command `ce dlogon`.
2. If you then watch the logs with "`ce dlogw`" or view them after events have been sent with ce dlogv, you will see log statements like the following. These statements tell you which subscriptions were matched.

```
2014-07-14 13:47:04,597
[WorkManager.WebSphere_EJB_Container_AsynchMethods_Internal_WorkManager : 2]
ejb.singleton.PublisherImpl FINEST - sendEvents Sent the following events:
subscriptionId='EventConsumerTester-3.9.0-5188298e18263886397c1ed620e41d938f3651773df
27ff6f1ceca6a0639cc38'; consumer version to deliver to='3.9.0'<=>
subscriptionId='EventConsumerTester-3.9.0-
ec7c68b90748882794a3b6e968a7e06a742b4669f460a555ce7f63af803bbae7'; consumer version to
deliver to='3.9.0'<=>
```

Why am I getting multiple event notifications for a single event?

Cause

It's likely that you have multiple subscriptions for the same event family/type. The Eventing Framework has a mechanism to treat subscriptions as being duplicates of each other and ensures that only one event will be sent to a subscriber. This is to handle a case where a service subscribes to events on startup and will therefore subscribe on each server in a cluster. In such cases, it is desirable to treat those multiple subscriptions as a single subscription. However,

there are very specific criteria to determine if a subscription is a duplicate and your subscriptions may not have met those criteria.

Solution

Please check the Javadoc for the com.avaya.collaboration.eventing package for a detailed description of what qualifies as a duplicate subscription.

One thing in particular to check is to ensure that you do not have server-specific Consumer Private Data in your subscriptions.The Consumer Private Data must match exactly for the subscriptions to be considered duplicates and to therefore only receive a single copy of an event.

Why am I not getting my expected events?

Cause

There are several things to consider here. One important point is that a snap-in will not receive any events on a given server until that snap-in has performed at least one subscription. If your snap-in subscribes for events on startup, this is not an issue.

Solution

1. If your snap-in subscribes for events based on some stimulus which may arrive at one particular server, you'll want to ensure that all servers are equipped to handle that event (it may be published on a different server).

   One way to do this would be to always subscribe for the Eventing family of events. These events are sent by default anyway, but this subscription will allow you to receive any other events as a result of a subscription on another server.

2. Another thing to watch out for is the use of subscriptions based on preferred version. You'll want to ensure that if one version of your snap-in follows this model, they all do.

Why are there log statements saying the Eventing System is still initializing?

Condition

You may occasionally see log statements such as the following after startup:

```
com.avaya.collaboration.eventing.EventingException [result=EVENTING_SYSTEM_NOT_READY - The eventing system is still initializing and cannot yet be used.
```

Cause

This is caused by the datagrid component not initializing soon enough after the system starts.

Solution

The condition should clear itself after a few minutes. If it doesn't, do the following:

1. Log in to System Manager.
2. Click Home > Elements > Avaya Breeze® platform > Server Administration.
3. Select the Avaya Breeze® platform node, and click Reboot.

Why does my subscription not seem to activate?

Cause

You may not have defined your event listener properly.

Solution

Check the log file for your snap-in (ce dlogv <snap-in name>). If everything is OK, you should see the following log statement:

2014-07-14 13:27:16,656 [WebContainer : 2] EventConsumerTester INFO - EventConsumerTester-3.9.0 - findEventListener Listener class "com.avaya.zephyr.tester.event.consumer.MyEventListener" found implementing interface "EventListener" and specified by the properties XML file.

You will see the following are error statements if you've done something incorrect.

You haven't specified an event listener in your properties.xml file:

2014-07-14 08:45:11,872 [WebContainer : 1] EventConsumerTester ERROR - EventConsumerTester-3.9.0 - findEventListener No Event Listener found. See documentation regarding the annotation "TheEventListener".

The class name specified as the event listener in properties.xml doesn't exist:

2014-07-14 08:45:11,872 [WebContainer : 1] EventConsumerTester ERROR - EventConsumerTester-3.9.0 - findEventListener No Event Listener found. See documentation regarding the annotation "TheEventListener".

You haven't annotated your event listener class with "@Stateless"

2014-07-14 13:30:03,496 [WebContainer : 3] EventConsumerTester ERROR - EventConsumerTester-3.9.0 - confirmClassDefinition There is an error in the definition of the class implementing interface "EventListener" and specified by the properties XML file. Class must be annotated with @Stateless.

Your event listener class doesn't implement the EventListener interface

2014-07-14 13:33:24,826 [WebContainer : 2] EventConsumerTester ERROR - EventConsumerTester-3.9.0 - confirmClassDefinition There is an error in the definition of the class implementing interface "EventListener" and specified by the properties XML file. Class does not implement interface.

Why don’t I get an acknowledgement for an event?

Cause

There are several things to consider here. One important point is that a producer snap-in has to include the ackId in metadata form (callbackURL is required for an EFC snap-in) when publishing event in order to receive the acknowledgement.

Solution

1. As a producer, application is responsible to use the EventMetaData to signal EF that an ack is required when publishing an event;
    a. For EFC producer that requires an ACK for an event, its PUBLISH request should contain two form-data in its MIME body: “metadata-callbackUrl” and “metadata-ackId”
    b. For non-EFC producer (i.e. snap-in directly using EF) that requires an ACK for an event, it should add “ackId” in event metadata valueMap before invoking publish() method.
2. Upon receiving any event, the application should:
    a. If incoming event is EVENTING:EVENT_RECEIVED (i.e. ACK for a previously published event), use the “ackId” value to associate with previously published event, and do necessary processing;
    b. If incoming event is any other explicitly subscribed events, then exam EventMetaData to see if an ACK is required before processing the event normally:
        i. If “ackId” is not blank, implies ACK is required;
            - Java application should Invoke eventingService.ack(Event event, String eventBodyForExtraInfo) API to send back application acknowledgement.
            - EFC application should compose a new HTTP request to <EventingConnector_ServicePath>/ack. The request parameter should contain the following mandatory parts: producer name and version (i.e. the acker name/ version), original event's producer name and version (i.e. the publisher's name/ version), everything copied from the original event metadata (including valueMap()), and an optional eventBody.
        ii. If “ackId” is blank, proceed normally with event handling.
3. Other things to verify and consider if producer and consumer have above implemented:
    - ACK will not be received if there is no consumer at the time event is published.
    - A new EventType (EVENT_RECEIVED) will be added to EVENTING family, this is the event type to be used by consumers when sending an application acknowledgement.
    - If there are multiple consumers at the time event is published, multiple ACKs will be delivered back to initial producer
    - Application (producer) is responsible for the creation of the unique ackId and mapping it between the published event and ACK.
    - Application (producer) is responsible for the logic whether to resend the event if expected ACK is not received within certain period of time
    - Application (consumer) is responsible for the logic when to respond the ACK after received the event
    - Applications (producer and consumer) should be on the same contract of the content/ format in ACK message body.

Chapter 8: Snap-in bundle and dependencies debugging

What does the 'Load' operation of a bundle mean?

Using the Load operation, one or more services packaged in the bundle can be loaded at a time.

Is partial bundle load supported?

Partial loading of a bundle is not supported. Either all or none of the services within a bundle will be loaded.

Does the bundle load fail if services within the bundle are loaded?

No, the bundle load will not fail if the services within the bundle are already loaded. The bundle load operation will be skipped for the services that are loaded.

Does the bundle load fail if the service dependencies are not loaded?

No, the bundle load will not fail if the service dependencies are not loaded. The service dependency will be loaded after the bundle is loaded from the Services page. The bundle installation is blocked.

Does bundle load fail if the service within the bundle was loaded by another bundle?

No, the bundle load will not fail if the service within the bundle was loaded by another bundle. Such a service will be skipped during the bundle load.

Why my bundle load fail?

If bundle size is more than 3GB then it might fail in load operation.

To fix the problem, split the bundle in multiple bundles so that individual bundle size is not more than 3 GB.

What does the Install operation of a bundle mean?

Using the Install operation, services packaged in the bundle or their dependencies will be installed on the cluster.

Can I install more than one bundle at a time?

No, only one bundle can be installed at a time.

Can I install a bundle on multiple clusters?

Yes, a bundle can be installed on multiple clusters.

What is the meaning of ‘n of m’ in the state column?

n is the number of clusters where the bundle is installed. *m* is the total number of clusters available on System Manager.

Why is the Partial status displayed for a cluster when the n of m state link is clicked? Are there any other status legends used?

The Partial status indicates:

- That one of more services in the selected bundle are already installed through another bundle.
- If the current bundle is in the Installing state on one cluster and it allows an administrators to install the same bundle on another cluster.
- If the status is Unknown when the bundle is installed on a cluster without nodes assigned to it.

Does the installation of a bundle automatically install the dependency services?

Yes, if it meets below conditions

- Dependency services are defined explicitly on bundle.xml and loaded onto System Manager through the Services page or loaded through another bundle.
- Dependency services are defined implicitly on bundle.xml and loaded with the same bundle.

What happens when a dependency service in a bundle is not loaded on System Manager and triggers the bundle installation?

The bundle installation will be failed with the following error:

Missing dependencies are preventing the following list of services from being installed. Please load the required services and retry the installation

What happens when some services of a bundle are already installed on a cluster and trigger the bundle installation?

The bundle installation is successful.

What happens when a service is part of multiple bundles and one of the bundle is installed?

The bundle installation is successful. Same services are installed in all bundles.

What happens when a service which is part of a bundle is selected from the Services page and installed? Does it install the whole bundle?

No, it will be installed with selected services only. The status of the services displays as Installed on Bundles/Services page.

What happens when a service, which is a part of an installed bundle, is uninstalled from the Services page? Does it uninstall other services of the bundle? Does it affect the functions of a bundle?

The service will be uninstalled successfully from the Services page, irrespective of it being a part of bundle. This does not affect the functions of a bundle.

If the selected service is defined as dependency on another service in bundle.xml, the bundle may be in an error state. To recover from error state, do the following:

1. Uninstall the bundle.
2. Reinstall the dependency.
3. Reinstall the bundle.

What happens when a bundle is installed on a cluster without Avaya Breeze® platform instances?

The bundle state displays 1 of total number of clusters. The installation of services within the bundle is triggered when an Avaya Breeze® platform node is added to the cluster.

What happens when a bundle is installed on a cluster with Avaya Breeze® platform instances that are not working?

The bundle installation fails for that cluster with an error message.

What happens when Avaya Breeze® platform instances of a cluster stop working during installation?

The bundle installation will be in error state till the Avaya Breeze® platform instances are not working.

What happens when a service fails to install on an Avaya Breeze® platform instance in a cluster during bundle installation?

The bundle installation fails with the following error message:

Failed to install

How do I reinstall a bundle whose installation failed?

To reinstall the bundle whose installation failed, uninstall the bundle. Wait for the operation to complete and reinstall the bundle.

How do I see the installation status of services of a bundle?

To see the installation status of services of a bundle, click the bundle name on the Bundles page. The system navigates to the Bundle Details and Installation Status page.
On the new page that is displayed, click the state of each service to view the detailed status of each Breeze node.

Can I install a service which is part of a bundle from the Cluster add edit page? Does it install the entire bundle?

The service which is part of a bundle can be installed from the Cluster editor page. It will not install the entire bundle.

WFDs as SVARs

Why are my Bundle WFDs and Tasks services not listed on Service Management page?

Avaya Breeze® platform Release 3.9 supports the WFDs and Tasks services management through the Bundle Management page only, and not through service management.

The page lists WFDs SVAR from only Avaya Breeze® platform Release 3.2 or earlier.

Why doesn’t the Cluster Editor page display my Bundle WFDs and Tasks services to be assigned/unassigned?

Avaya Breeze® platform Release 3.9 supports the WFDs and Tasks services management through the Bundle Management page only, and using cluster editor.

The page lists WFDs SVAR from only Avaya Breeze® platform Release 3.2 or earlier.

Why does not the Service Profile page for assign/un-assign services display my Bundle WFDs and Tasks services?

Avaya Breeze® platform Release 3.9 supports the WFDs and Tasks services management through the Bundle Management page only, and not through service management.

The page lists WFDs SVAR from only Avaya Breeze® platform Release 3.2 or earlier to support backward compatibility.

Why don't I see service attributes after uninstalling Engagement Designer Release 3.2 or earlier?

Avaya Breeze® platform Release 3.9 supports the WFDs attribute changes through Engagement Designer Console only.

If Engagement Designer Console Release 3.2 or earlier is installed on the cluster, the console lists WFDs SVAR attributes from only Avaya Breeze® platform Release 3.2 or earlier to support backward compatibility.

Why do the cluster attributes not display after installing Engagement Designer Release 3.8+ on the same cluster that has Engagement Designer Release 3.2 installed?

Avaya Breeze® platform Release 3.9 supports service attribute changes through Avaya Breeze® platform Element Manager.

If Engagement Designer Console Release 3.2 or earlier is installed on the cluster, the service-level and system-level attributes can be changed through Avaya Breeze® platform Element Manager. Cluster-level attributes can be changed only through Engagement Designer Console.

Why don't we see the service, cluster, and system attributes for WFDs if only Engagement Designer Release 3.8 or later is installed?

Avaya Breeze® platform Release 3.8+ supports the services attribute changes only through Avaya Breeze® platform Element Manager.

If Engagement Designer Console Release 3.2 or earlier is installed on the cluster, the service-level and system-level attributes can be changed through Avaya Breeze® platform Element Manager. Cluster-level attributes can be changed only through Engagement Designer Console.

Why does the Bundle allow installation of WFDs and Tasks even though dependency of Engagement Designer Release 3.8 or later not defined in the metadata?

Dependencies on the services need to be defined explicitly during bundle creation. Avaya Breeze® platform Element Manager can only know about dependency through bundle metadata. If no dependency has been defined bundle will allow installation as Avaya Breeze® platform Element Manager has no way to detect the dependencies.

Why can’t we load WFDs and Tasks services from the Service Management page?

Avaya Breeze® platform Release 3.9 supports the WFDs and Tasks services management only through the Bundle Management page, not through service management.

Why does Engagement Designer Console display the WFDs status as deployed when the WFDs are in the installing state?

Workflow might be using some of the tasks which are not deployed on Engagement Designer. Installing those tasks will make the Engagement Designer status API to return status as deployed and Avaya Breeze® platform Element Manager will in turn show the status installed.

Chapter 9: Authorization debugging

Authorization key not updated after ISO upgrade

If the authorization service snap-in is installed on a particular cluster and if the Avaya Breeze® platform node is upgraded using the ISO or a patch is applied, or a new OVA is installed then the administrator must update the Authorization Certificate by performing the following steps

Solution

1. Log on to System Manager
2. On the System Manager Web console, click **Elements** > **Avaya Breeze® platform**.
3. Click **Cluster Administration** and select the particular cluster on which Authorization Service is installed.
4. Click the **Certificate Management** drop-down and select **Update/Install Identity Certificate (Authorization Service)**.

Connection Exception when using APIs to fetch access tokens

Condition

Authorization Client snap-in log shows statement such as: AuthorizationHelperException:Caught exception while executing request ... Connect to host failed:Connection refused.

Cause

One of the following configuration is missing or incorrect:

- Cluster attribute **Authorization Service Address**. This attribute is found on System Manager in **Elements** > **Avaya Breeze® platform** > **Cluster Administration**. Select the cluster when it is in Deny mode and click **Edit.**
- Enter a valid value, which is the URL using which authorization service can be accessed.
- Click commit.
- Service attribute **Authorization Service Address**. This attribute is found on System Manager in **Elements** > **Avaya Breeze® platform** > **Configuration** > **Attributes**. Select the Service Clusters or Service Globals tab. Select the client snap-in.
- Enter a valid value, which is the URL using which authorization service can be accessed.
- Click commit.

Solution

Modify the cluster or service attribute to point to the node where the Authorization Service is installed using above steps.

AuthorizationHelperException when using APIs to fetch access tokens

Condition

Authorization Client snap-in log shows statement such as: Unable to determine signer key for client. Check if a service attribute to detect this snap-in as an Authorization Client has been provisioned.

Cause

A service attribute by name *com.avaya.authorization.client* has not been included in the client snap-in properties.xml file.

Solution

Include an attribute by name *com.avaya.authorization.client* in the snap-in properties.xml file. Refer to *Avaya Breeze® platform Snap-in Development Guide* for details.

Authorization Helper APIs respond with “403 Forbidden. No associated scope found”

Condition

Helper API call to get access token results in a HttpResponseException with status “403 Forbidden” and a message “No associated scope found for Client with Id <>”

Cause

The client snap-in has not been provisioned with any grants by the administrator. Therefore the Authorization Service is unable to generate an access token for a client with no scope.

Solution

Request that the administrator assign grants to the client snap-in by going to System Manager in **Elements** > **Avaya Breeze® platform** > **Configuration** > **Authorization**.

How do I change the token validity time?

Procedure

1. On System Manager go to **Elements** > **Avaya Breeze® platform** > **Configuration** > **Attributes**.
2. Select the Service Clusters or Service Globals tab.
3. Select the AuthorizationService service.
4. Modify the value of **Token validity time**.
5. Click **Commit**.

How do I change the client JWT validity time?

Procedure

1. On System Manager go to **Elements** > **Avaya Breeze® platform** > **Configuration** > **Attributes**.
2. Select the Service Clusters or Service Globals tab.
3. Select the AuthorizationService service.
4. Modify the value of **Client JWT validity time**.
5. Click **Commit**.

Unable to edit grants on Authorization Client

You cannot edit grants on the Authorization Client, if you have added "( )" in the cluster name while creating the cluster.

Solution

1. Update the cluster name to not include "( )".
2. To verify if you can edit grants, do the following:
   a. Log on to System Manager.
   b. On the System Manager web console, click **Elements** > **Avaya Breeze® platform** > **Configuration** > **Authorization**.
   c. On the **Clients** tab, click **Edit Grants**.

What user scopes are supported?

For release 3.2 and 3.3 the following scopes relating to a user's System Manager communication profile are available to be queried:

- CommunicationAddress
- MailboxNumber
- StationExtension
- AgentId

When an access token request is made for any of these scopes, the value associated in System Manager is retrieved by AuthorizationService and provided as a user scope in the token.

How do I configure SAML Authentication?

Procedure

1. Navigate to **System Manager** > **Avaya Breeze®** > **Configuration** > **Authorization** > **Authentication Mechanism**.
2. Select Current Authentication Mechanism.
3. Click **Change Authentication Mechanism**.
4. Select **SAML** and complete the other form fields.

How do I configure LDAP authentication on the Authorization Service provided login screen?

Procedure

1. Navigate to **System Manager** > **Avaya Breeze®** > **Configuration** > **Authorization** > **Authentication Mechanism**.
2. Select Current Authentication Mechanism.
3. Click **Change Authentication Mechanism**.
4. Select **LDAP** and commit.

How do I resolve the ‘SAML profile is not deployed’ error?

Procedure

1. Navigate to **System Manager > Avaya Breeze® > Configuration > Authorization > Authentication Mechanism**.
2. Select the cluster where Authorization Service is installed.
3. Select **Service as AuthorizationService**.
4. For the attribute SAML Profile, select **Override Default**, and set the effective value as **Deploy**.
5. Click **Commit**.

When logging an agent to Workspaces, an error : “Invalid claims in token” is seen

Cause

When logging an agent to Workspaces, the following error is displayed:

Invalid claims in token

Procedure

1. The Invalid claims in error is displayed when an agent logs in to a Workspaces session. This happens if the token granted by Authorization Service does not indicate the subject(username) of the token. Refer to the respective IDP configuration and ensure that:
   a. The user's identity is sent in an SAML assertion attribute statement.
   b. The identifier of the SAML attribute sent is specified in the Attribute Used as UserID field when configuring SAML under: System Manager > Avaya Breeze® > Configuration > Authorization > Authentication Mechanism.
2. The authenticated user might not be configured in UCA. Check if the user's identity provided in the subject of the access token granted by the Authorization Service is properly configured in Oceana UCAStoreService.

When authenticating a user on the browser, an error: "502 : Bad gateway error" is seen.

Cause

When authenticating a user on the browser, the following error is displayed:

502 : Bad gateway error

Procedure

1. Verify that Authorization Service is installed.
2. Verify that the cluster and all the servers are in the Accepting state.
3. Log in to Avaya Breeze® platform as an sroot user, and run the flowing command:

```
[root@breeze165 ~]# netstat –anp | grep 9050
```

4. If there is no output, the Authorization Service SAML profile is not running.
5. This may happen if there's insufficient memory available for the Gigaspaces components to start. Try allocating more memory to the virtual machine and check if it solves the issue. If sufficient memory is already allocated, try to restart Gigaspace:

```
[root@breeze165 ~]# stop –s dcm
Wait for 2 minutes for all processes to stop.
[root @breeze165 ~]$ statapp | grep dcm
dcm            1/  1 DOWN
[root@breeze165 ~]# start –s dcm
[root@breeze165 ~]# statapp | grep dcm
dcm            1/  1 UP
```

Verify that the 9050 port is in the LISTEN state. Run the following command:

```
[root@breeze165 ~]# netstat –anp | grep 9050
tcp6       0      0 127.0.0.1:9050          :::*                    LISTEN      18766/java
```

6. If there is no output, run below commands

```
[root@breeze165 ~]# stop –s dcm
Wait for 2 minutes for all processes to stop.
[root @breeze165 ~]$ statapp | grep dcm
dcm              1/  1 DOWN
[root@breeze165 ~]# systemctl start dcm
[root@breeze165 ~]# statapp | grep dcm
dcm              1/  1 UP
```

Verify that the 9050 port is in the LISTEN state. Run the following command:

```
[root@breeze165 ~]# netstat –anp | grep 9050
tcp6       0      0 127.0.0.1:9050          :::*                    LISTEN      18766/java
```

7. If there is no output, reboot all the Avaya Breeze® platform nodes in the cluster at the same time.

LDAP Authentication is failing

Cause

The authorization.log contains the following error:

Ex : 2017-06-19 10:57:49,407 [WebContainer : 3] AuthorizationService ERROR - AuthorizationService-3.9.0.390016 - LDAPAuthenticationFilter doFilter : LDAP exception com.avaya.zephyr.services.production.AuthorizationService.exception.AuthenticationSystemException: Caught exception while trying to establish secure session with data source: sv-exchange AD cn=510

Procedure

1. Import the LDAP certificate to Avaya Breeze® platform nodes on the Avaya Breeze® platform cluster where the Authorization Service is installed.
2. Navigate to System Manager -> Avaya Breeze® ->Cluster Administration -><select the cluster where AS is installed> ->certificate management -> Update /Install Identity certificate (Authorization Service).
3. Click Update /Install Identity certificate (Authorization Service).

Chapter 10: Cluster Database debugging

How to enable cluster DB?

If you enable the cluster database during cluster Commit operation, the first Commit operation enables the cluster database in the cluster. One of the nodes is marked as a master while another, if present, is marked as the slave. Other nodes are marked as Idle nodes.

You must perform the cluster Commit operation again to enable the cluster database in another node.

Snap-in installed successfully, DB is created but schema upgrade scripts are not run

Solution

1. Check whether the upgrade SQL scripts are in proper naming convention.

   For more information, see Avaya Breeze® platform Snap-in Development Guide.

2. Ensure that the properties.xml file has the EoL characters in UNIX format.

Errors seen in logs related to connections exhausted

Solution

Check the maximum number of connection parameters configured in properties.xml and customize the parameters.

The maximum number of connections, inclusive of all snap-ins from all nodes, allowed is 300.

Where do I see the cluster db back up jobs that are scheduled to run immediately?

Solution

Scheduled back jobs and their status can be viewed on the same screen where they get scheduled. The jobs which are scheduled to run immediately can be viewed with below step:

On cluster administration page, click **Backup and Restore > Job Status**.

Cluster db backup is failing with message – Error: Auth fail

Solution

The Avaya Breeze® platform made changes in the way the backup server password was stored in Release 3.3. After upgrading to Release 3.3, you need to administer the backup server password again.

Chapter 11: Cluster and node management

Why aren't the certificate management and Cluster State buttons not enabled when I select a cluster on Cluster Administration page?

1. Is this System Manager a standalone system?
    a. If yes, check if the replication of the Avaya Breeze® platform node is complete.
    b. Ensure that the node is reachable from System Manager.
    c. Check the IP address and FQDN configured in SIP entity and Server Administration for Avaya Breeze® platform on System Manager.
2. Is this System Manager a part of a Geo-redundant System Manager environment?
    a. Ensure that the Geo R health is green and the replication is enabled and healthy between the two System Managers.
    b. Ensure that the current System Manager is aware that it is managing the Avaya Breeze® platform nodes in this cluster
    c. This can be validated from the page Home / Services / Inventory / Manage Elements

The Managed status of the nodes should indicate the current System Manager.

- If the status is unknown, select each node on this page, and click **e**.
- The issue might resolve after the status shows the current System Manager
- If the status is returned as Unmanaged/Managed by other System Manager, select each node on this page and click More Actions > Manage.
- The issue might resolve after the status shows the current System Manager

Why do I see --- instead of values when I select an older time period, for example, 4 days ago for a cluster to view Peak Usage on System Resource Monitor page?

This is since the System Manager was restarted in the last 4 days.

Restarting the System Manager clears the saved monitoring data for the nodes.

Reliable eventing group status shows Error on the Dashboard

1. Ensure that the cluster and the nodes in cluster which form the reliable eventing group are in the Accepting state
2. If a node was redeployed using the OVA in the cluster while the reliable eventing group still in place, do the following:

a. Change the state of the cluster to the Deny state.
b. Delete the reliable eventing group.
c. Recreate the group.
d. Change the state of the cluster to the Accept state.

These steps are service impacting.

Chapter 12: IPv6 management in JITC mode

How do I enable general IPv6 settings?

1. IPv6 can only be enabled in a JITC-hardened lab.Log in to System Manager.
2. Click Elements->Session Manager->Global Settings.
3. Select “Enable IPv6”.

How do I configure IPv6 addresses on Avaya Breeze® platform?

1. Log in to System Manager.
2. Click Element->Routing->SIP Entities.
3. Select the Avaya Breeze® platform server, and click “Edit”.
4. Configure the Avaya Breeze® platform IPv6 address in “IPv6 Address”.
5. Add the associated Entity Links.
6. Click Element->Avaya Breeze®->Server Administration.
7. Select the Avaya Breeze® platform server, and click “Edit”.
8. In “SIP Entity IPv6 Address”, configure IPv6 Network prefix length and IPv6 Default Gateway.

How do I configure IPv6 address on Avaya Breeze® platform clusters?

1. Log in to System Manager.
2. Click Element-> Avaya Breeze®->Cluster Administration.
3. Select Avaya Breeze® platform cluster, and click “Edit”.
4. Configure the cluster IPv6 address in “Cluster IPv6”.

How do I verify IPv6 addresses on Avaya Breeze® platform servers?

Verify the IPv4 and IPv6 addresses on Avaya Breeze® platform using the “ifconfig” command.

```
[root@ce135-ra-dvit ~]# ifconfig
dummy0: flags=195<UP,BROADCAST,RUNNING,NOARP>  mtu 1500
        inet 127.0.0.2  netmask 255.0.0.0  broadcast 127.255.255.255
        inet6 fe80::cc1f:88ff:fe61:2f25  prefixlen 64  scopeid 0x20<link>
        ether ce:1f:88:61:2f:25  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7  bytes 610 (610.0 B)
```

```
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
dummy1: flags=195<UP,BROADCAST,RUNNING,NOARP>  mtu 1500
        inet6 ::2  prefixlen 64  scopeid 0x80<compat,global>
        inet6 fe80::44b5:e9ff:fe8c:6291  prefixlen 64  scopeid 0x20<link>
        ether 46:b5:e9:8c:62:91  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7  bytes 610 (610.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.133.45.135  netmask 255.255.255.0  broadcast 10.133.45.255
        inet6 fe80::250:56ff:feb3:e28d  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:b3:e2:8d  txqueuelen 1000  (Ethernet)
        RX packets 116634042  bytes 64178402485 (59.7 GiB)
        RX errors 0  dropped 1516  overruns 0  frame 0
        TX packets 113425867  bytes 41737621522 (38.8 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.133.45.136  netmask 255.255.255.0  broadcast 10.133.45.255
        inet6 2a07:2a42:adc0:100::67  prefixlen 64  scopeid 0x0<global>
        inet6 2a07:2a42:adc0:100::61  prefixlen 64  scopeid 0x0<global>
        ether 00:50:56:b3:94:a2  txqueuelen 1000  (Ethernet)
        RX packets 11378546  bytes 1381930849 (1.2 GiB)
        RX errors 0  dropped 1403  overruns 0  frame 0
        TX packets 9922637  bytes 1288834586 (1.2 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1:0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.133.45.8  netmask 255.255.255.0  broadcast 10.133.45.255
        ether 00:50:56:b3:94:a2  txqueuelen 1000  (Ethernet)

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 116489053  bytes 113321254827 (105.5 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 116489053  bytes 113321254827 (105.5 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

In the example, the IP addresses represent the following assets:

- 10.133.45.136 is the Avaya Breeze® platform asset IPv4 address

- 2a07:2a42:adc0:100::67 is the Avaya Breeze® platform asset IPv6 address
- 10.133.45.8 is the cluster IPv4 address
- 2a07:2a42:adc0:100::61 is the cluster IPv6 address.