



Maintaining and Troubleshooting Avaya Breeze[®] platform

Release 3.9
Issue 4
November 2025

Notices

© 2026 Avaya LLC. All Rights Reserved.

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

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

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

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE). THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/licenseinfo) UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE

TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

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

Copyright

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

Virtualization

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

Third Party Components

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

Service Provider

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

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

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

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Purpose	10
Change history	10
Chapter 2: Avaya Breeze® platform alarm overview	11
Chapter 3: Avaya Aura® System Manager support for alarms	12
Alarm status	12
Alarm severities	13
Chapter 4: SNMP Support for Avaya Breeze® platform	14
Configuring the TrapListener service	15
TrapListener service field descriptions	15
Creating an SNMPv3 user profile	16
Creating an SNMP target profile	17
Configuring the Avaya Breeze® platform Serviceability Agent	18
Downloading the Avaya Breeze® platform SNMP MIB	18
Chapter 5: Operations supported on System Manager for alarming	20
Generating test alarms in System Manager	20
Verifying test alarms in System Manager	21
Viewing alarms	21
Filtering alarms	22
Searching for alarms	22
Exporting alarms	23
Changing the alarm status	24
Alarming field descriptions	24
Chapter 6: Avaya Breeze® platform alarm descriptions	28
AAMS_AUTHERROR	28
AAMS_CONNFAIL	28
AAMS_LOCKED	29
AAMS_OVERLOAD	29
ARBITER_10001	29
ARBITER_10002	29
ARBITER_10003	30
AU_GEMMTC20061	30
AuthorizationService_GENERR1	30
avCEAVDM52603	31
avCECVDM52603	31
BR_MMTC20053	31
CCLRCONNFAIL	31
CCONNFAIL	32
CLR_CONERR2	32
CLR_GENERR1	32

CLR_MBCN_ERR_001.....	32
CLR_PBCN_ERR_001.....	33
CLR_SSLERR3.....	33
CONERR2.....	33
DRS_DBG_0001.....	34
FILEBEATCONNECTIONERROR.....	34
FILEBEATCONNECTIONFINE.....	34
MBCN_ERR_001.....	34
nsNotifyRestart.....	35
nsNotifyShutdown.....	35
nsNotifyStart.....	35
OP_AASL10900.....	35
OP_ANFW11001.....	36
OP_ANFW11002.....	36
OP_APLM10300.....	36
OP_APLM10302.....	36
OP_APLM10304.....	37
OP_AWTC10405.....	37
OP_AWTC10406.....	37
OP_CDAO50001.....	37
OP_CDAO50002.....	38
OP_CDAO50003.....	38
OP_CDAO50111.....	38
OP_CDAO50112.....	38
OP_CEMMTC20033.....	39
OP_CMON55001.....	39
OP_CMON55002.....	39
OP_GEMMTC20033.....	39
OP_GEMMTC20035.....	40
OP_GEMMTC20037.....	40
OP_GEMMTC20039.....	40
OP_MAMA20102.....	41
OP_MMTC200[1-4][13579].....	41
OP_MMTC20019.....	41
OP_MMTC20025.....	41
OP_MMTC20031.....	42
OP_MMTC20047.....	42
OP_MMTC20048.....	42
OP_MMTC20049.....	42
OP_MMTC20050.....	43
OP_MMTC20051.....	43
OP_MMTC20052.....	43
OP_MMTC20054.....	43

OP_MMTC20055.....	44
OP_MMTC20129.....	44
OP_MWD20202.....	44
OP_MWD20204.....	44
OP_TALM00100.....	45
OP_TestAlarm.....	45
OP_TMAG20500.....	45
OP_TMAG20501.....	46
OVERLOAD_100001.....	46
OVERLOAD_100002.....	46
OVERLOAD_100003.....	46
OVERLOAD_100004.....	47
PBCN_ERR_001.....	47
Postgres alarms.....	47
SEC_000421.....	48
SNAPINSCRIPTFAILED.....	48
SSLERR3.....	48
UCAService_UCA_ALARM_1.....	49
Chapter 7: Cluster and server administration.....	50
Cluster administration field descriptions.....	50
Server Administration field descriptions.....	56
Backing up a cluster database.....	59
Restoring the cluster database.....	60
Chapter 8: Data replication	61
Viewing replica groups.....	61
Viewing replica nodes in a replica group.....	62
Repairing a replica node.....	62
Repairing all replica nodes in a replica group.....	62
Viewing replication details for a replica node.....	63
Removing a replica node.....	63
Removing a replica node from queue.....	64
Chapter 9: Maintenance tests.....	65
Avaya Breeze® platform maintenance test descriptions.....	65
Running maintenance tests.....	66
Running Reliable Eventing Framework maintenance tests.....	67
System resource monitor.....	67
Viewing the current usage of a cluster.....	68
Viewing the peak usage of a cluster.....	69
Resetting the peak usage of a cluster.....	69
System Resource Monitoring page field descriptions.....	69
System resource monitor.....	71
Viewing the current usage of a cluster.....	72
Viewing the peak usage of a cluster.....	72

Resetting the peak usage of a cluster.....	72
System Resource Monitoring page field descriptions.....	73
Chapter 10: Maintaining and upgrading ESXi host software.....	75
Checklist for Avaya Breeze® platform ESXi host maintenance for.....	75
Checklist for Avaya Solutions Platform 130 Appliance ESXi upgrades.....	78
Preparing Breeze nodes for ESXi maintenance.....	79
Upgrading the ESXi host.....	80
Adding the new ESXi vSphere license.....	81
Accepting new service after ESXi maintenance.....	81
Rebooting the Breeze clusters after ESXi maintenance.....	82
Chapter 11: Avaya Breeze® platform troubleshooting.....	83
Agent login on Avaya Workspaces fails intermittently.....	84
Alarms are not raised for a node.....	85
Avaya Breeze® platform does not send alarms to System Manager.....	85
A snap-in gets invoked twice.....	86
Auto-switchover has occurred in a cluster database.....	86
Identity certificate change requires Avaya Breeze® platform restart.....	87
Certificate expiration.....	88
Certificate status.....	88
Troubleshooting certificate status alarms.....	88
Avaya Breeze® platform instance resolution failure.....	89
Troubleshooting Avaya Breeze® platform instance resolution failure.....	89
Avaya Breeze® platform in overload.....	89
Avaya Breeze® platform not in overload.....	91
Checking the call processing status of Avaya Breeze® platform.....	92
The Add participant operation in snap-ins fails while using FCLC.....	92
Troubleshooting database connection errors.....	93
Troubleshooting database errors.....	94
Database Query.....	94
Data Replication Service synchronization failure.....	94
Data Replication Service synchronization troubleshooting checklist.....	95
Troubleshooting hard disk drive update errors.....	96
License errors.....	97
Avaya Breeze® platform server license file not installed.....	98
Snap-in license file is not installed.....	98
Avaya Breeze® platform server software version mismatch.....	98
There is a version mismatch in the snap-in software.....	99
Insufficient Avaya Breeze® platform server license capacity.....	100
Snap-in license file has expired.....	100
Avaya Breeze® platform server license file has expired.....	101
Troubleshooting Reliable Eventing maintenance test failures.....	101
Management Instance check failed.....	102
Troubleshooting management instance check failure.....	103

Troubleshooting network configuration errors.....	104
Troubleshooting network firewall critical events.....	104
Troubleshooting network firewall pinholing.....	104
Troubleshooting network firewall stoppages.....	105
Platform Application did not start.....	105
Troubleshooting Postgres database sanity check failures.....	106
Troubleshooting SAL sanity check failures.....	107
DCM sanity check failed.....	109
Maintenance test for Call Processing status fails.....	109
Secondary alarms persist.....	110
Security Module failure.....	110
Security Module Management Agent is not able to configure Security Module.....	111
Troubleshooting Avaya Breeze [®] platform service failures.....	112
Troubleshooting SIP Entity Monitoring alarms.....	112
Snap-in installation issues.....	113
Troubleshooting Avaya Aura [®] Media Server issues.....	114
Verifying the Avaya Aura [®] Media Server status.....	114
Media Server Monitoring page field descriptions.....	115
WebSphere generates Java core files because of connection errors with Media Server.....	116
Troubleshooting when accepting nodes are lesser than the total number of nodes in a cluster...	116
Troubleshooting unexpected data detections.....	117
Resizing the Breeze Virtual Machine Disk on VMware.....	118
Virtual machine hangs after you reboot.....	118
Callable service gets the 404 error while trying to add a participant to a one-party call.....	119
Troubleshooting Filebeat service connection errors.....	119
traceMessage does not display the IP address of Avaya Breeze [®] platform.....	120
CRL download fails when an HTTP proxy is configured on Avaya Breeze [®] platform.....	121
Troubleshooting Cluster Database maintenance test failures.....	121
Cluster Database status log field descriptions.....	122
Troubleshooting certificate validation.....	123
Troubleshooting the Cluster Database status.....	124
Chapter 12: Avaya Breeze[®] platform configuration updates.....	126
Updating the Avaya Breeze [®] platform configuration using CEnetSetup.....	126
HTTP/HTTPS proxy exclusion list.....	128
Configuring Avaya Breeze [®] platform after changing the IP address or FQDN.....	128
Changing the security module IP address.....	129
Setting the ciphers supported by a cluster.....	130
Enabling ciphers suites in WAS.....	131
Chapter 13: Enhanced Access Security Gateway.....	134
EASGManage.....	134
EASGProductCert.....	135
EASGSiteCertManage.....	135
EASGStatus.....	136

Chapter 14: Serviceability tools	137
Collecting logs using the Avaya Breeze® platform report tool	137
Tracing messages using Avaya Breeze® platform traceMessage	138
Start Capture field descriptions	139
Viewing the Avaya Breeze® platform traceMessage results	140
Chapter 15: Log files	141
Log Viewer	141
Viewing log details	141
Searching for logs	142
Filtering logs	142
Avaya Breeze® platform log service	143
Modifying the logging configuration	144
Chapter 16: Log retention	146
logRetention command	146
hardware_info	146
ceconfig	147
Chapter 17: Additional information	149
Documentation	149
Finding documents on the Avaya Support website	152
Avaya Documentation Center navigation	152
Training	153
Viewing Avaya Mentor videos	154
Developer resources	155
Support	155
Using the Avaya InSite Knowledge Base	156

Chapter 1: Purpose

This document describes how to identify and troubleshoot problems for Avaya Breeze® platform. It is intended for anyone who is responsible for maintaining and troubleshooting Avaya Breeze® platform.

This document provides procedures for:

- Running maintenance tests
- Setting up and viewing SIP tracing
- Setting up and viewing HTTP tracing
- Setting up and tracing Collaboration Bus messages
- Monitoring events
- Monitoring system components
- Troubleshooting errors and alarms

Related links

[Change history](#) on page 10

Change history

Issue	Date	Summary of changes
1	December 2023	Updated the document for Avaya Breeze® platform R3.9.
2	January 2024	Corrected the name and details of cipher script. See Setting the ciphers supported by a cluster on page 130.
3	February 2024	Corrected Avaya Breeze® platform documentation links.
4	November 2025	Added the following new sections for Release 3.9.0.3: • Resizing the Breeze Virtual Machine Disk • Troubleshooting certificate validation • Enabling ciphers suites in WAS • Ensuring the server cipher order is preferred during SSL negotiation • Disabling ciphers on WAS

Chapter 2: Avaya Breeze® platform alarm overview

Avaya Breeze® platform provides a virtualized and secure application platform where workflow developers and Java programmers can develop and dynamically deploy advanced collaboration capabilities. These capabilities extend the power of Avaya Aura®, Avaya Oceana®, and Avaya Professional Services custom development. Customers, Business Partners, and Avaya developers can use Avaya Breeze® platform to deploy snap-ins.

Avaya Breeze® platform requires Secure Access Link (SAL) for remote access and for sending alarms to Avaya. A SAL gateway must be installed in the customer's enterprise for Avaya Services remote access. For more information, see [Avaya Aura System Manager support for alarms](#) on page 12. Avaya Breeze® platform also supports SNMP and you can create SNMP user and target profiles and attach the profiles to Serviceability Agent.

For steps on how to troubleshoot issues when alarms are not raised by the Avaya Breeze® platform node, see [Alarms are not raised for a node](#) on page 85.

You can configure alarming on System Manager for Avaya Breeze® platform nodes. After you have completed the configuration, the Cluster Administration and Server Administration pages in System Manager display alarms for the configured Avaya Breeze® platform nodes.

Reliable Eventing Framework provides a new mechanism for delivering messages. The current Eventing Framework uses Collaboration Bus as a point-to-point delivery mode for intra-node asynchronous events with high performance. The Reliable Eventing Framework adopts Apache ActiveMQ, which provides reliability, asynchronous events, inter-node, and inter-cluster capabilities, which are not available in Eventing Framework. For information about configuring Reliable Eventing on System Manager, see [Administering Avaya Breeze® platform](#). For information about Reliable Eventing Framework maintenance tests, see [Running Reliable Eventing Framework maintenance tests](#) on page 67. The process for troubleshooting Reliable Eventing Dashboard errors or warnings is the same as the process of troubleshooting Avaya Breeze® platform alarms.

Related links

[Cluster and server administration](#) on page 50

[Avaya Breeze platform maintenance test descriptions](#) on page 65

[Running Reliable Eventing Framework maintenance tests](#) on page 67

Chapter 3: Avaya Aura® System Manager support for alarms

Avaya Breeze® platform requires Secure Access Link (SAL) for remote access and for sending alarms to Avaya. A SAL gateway must be installed in the customer's enterprise for Avaya Services remote access.

Avaya Breeze® platform generates alarms that reference hardware-related events, lost connections, and Avaya Breeze® platform software events.

The Avaya Aura® System Manager Web interface allows you to perform various operations for alarms. For more information, see “Operations supported on System Manager for alarming”.

Alarm codes identify the system component which generates the alarm. Alarms are classified by their effect on system operation.

Snap-in alarms

- Alarms are now generated for third party as well as licensed snap-ins. However, the third party alarms are filtered by Avaya Aura® System Manager. These alarms are not sent to the Avaya Customer Data Center.

Related links

[Alarm status](#) on page 12

[Alarm severities](#) on page 13

Alarm status

The status of an alarm can be:

- Raised: An alarm has been generated. Software recovery actions cannot correct the problem.
- Acknowledged: The alarm is being investigated. This state is set manually by the customer or technician.
- Cleared: The problem has been resolved and the alarm has been cleared. This state is set by the customer or technician or by Avaya Breeze® platform.

Related links

[Avaya Aura System Manager support for alarms](#) on page 12

Alarm severities

Critical alarms indicate the system or certain components within the system are unusable. These alarms require immediate attention.

Major alarms identify failures that are causing a critical degradation of service. These alarms require immediate attention.

Minor alarms identify failures that are causing service degradation. These failures do not cause the system to be inoperable.

Warning alarms identify failures that cause no significant degradation of service. The system does not report warning alarms to a services organization.

 Note:

You can change the colors of the severities.

Related links

[Avaya Aura System Manager support for alarms](#) on page 12

Chapter 4: SNMP Support for Avaya Breeze[®] platform

This section provides details for creating SNMP User and Target profiles, and attaching the profiles to Serviceability Agents.

Avaya Breeze[®] platform requires Secure Access Link (SAL) for alarming. A SAL Gateway must be installed in the customer's enterprise.

The Serviceability Agent is an enhanced version of the SAL agent for alarming and forwarding logs. The Serviceability Agent sends SNMP v2 and SNMP v3 traps to System Manager, the SAL Gateway, and other configured Network Management System (NMS) destinations.

The **Manage Serviceability Agents** page has four sub-pages:

- **SNMPv3 User Profiles:** Establish and manage SNMP v3 user accounts. These accounts are used for SNMP v3 traps/informs and SNMP v3 queries of the SNMP master agent.
- **SNMP Target Profiles:** SNMP trap/inform destinations for System Manager, SAL Gateway, and customer NMS destinations. The profile setup supports both SNMP v2 and SNMP v3.
- **SNMP Serviceability Agents:** Manage serviceability agents that are registered with the System Manager agent manager. The System Manager hostname is automatically included in the list of agents.
- **Notification Filter Profile:** Manage filter profiles and assign the profiles to the target and serviceability agent pair. See *Administering Avaya Aura[®] System Manager* for more information.

Perform the following procedures in the order that they are presented to set up alarming for Avaya Breeze[®] platform.

Related links

[Configuring the TrapListener service](#) on page 15

[TrapListener service field descriptions](#) on page 15

[Creating an SNMPv3 user profile](#) on page 16

[Creating an SNMP target profile](#) on page 17

[Configuring the Avaya Breeze platform Serviceability Agent](#) on page 18

[Downloading the Avaya Breeze platform SNMP MIB](#) on page 18

Configuring the TrapListener service

The System Manager TrapListener service receives traps/informs from applications and generates alarms according to the severity.

If you change the TrapListener default settings, you need to:

- create a new SNMP Target Profile for the System Manager IP address, and
- create a new SNMPv3 User Profile for the System Manager.

As an alternative, you can edit the System Manager Target Profile and SNMPv3 User Profile to match the setting changes on the System Manager trap listener. The values in these profiles must match the values in the TrapListener settings.

Procedure

1. In System Manager, click **Services > Configuration > Settings > SMGR > TrapListener**.
2. Click **Edit**.
3. Edit the required fields as needed.
4. Click **Commit**.

Related links

[SNMP Support for Avaya Breeze platform](#) on page 14

TrapListener service field descriptions

* Note:

The passwords can contain any printable and non-whitespace characters. The password must contain between 8 and 255 characters. The password cannot be an empty string.

Name	Description
Authentication Password	The password to authenticate the user.
Authentication Protocol	The protocol to authenticate the source of traffic from SNMP V3 users. The values are: • md5 • SHA The default is md5 .
Community	The community for the v2c traps and informs.
Privacy Password	The pass phrase that is used to encrypt the SNMP data.

Table continues...

Privacy Protocol	The encryption policy for an SNMP V3 user. The values are: • DES • AES The default value is AES .
Interval for compare alarm timer (in seconds)	The interval, in seconds, in which alternate database alarms are compared against System Manager database alarms on a secondary standby System Manager server.
TrapListener Port	The port on which the TrapListener service listens. The default is 10162 .
V3 UserName	The SNMP V3 user name. The default is initial .

Related links

[SNMP Support for Avaya Breeze platform](#) on page 14

Creating an SNMPv3 user profile

About this task

Create a user profile to match the System Manager TrapListener settings.

Procedure

1. In System Manager, click **Services > Inventory > Manage Serviceability Agents > SNMPv3 User Profiles**.
2. Click **New**.
3. Enter the following information:
 - a. **User Name:** Enter the same SNMPv3 user name as the TrapListener. The default is **initial**.

*

Note:
 The user name can contain the following characters: alphanumeric, period, underscore, white space, single quote, and hyphen. The user name cannot be an empty string.
 - b. **Authentication Protocol:** Use the Authentication Protocol of the TrapListener service. The default is **md5**.
 - c. **Authentication Password:** Use the Authentication Password of the TrapListener service.
 - d. **Privacy Protocol:** Use the Privacy Protocol of the TrapListener service. The default is **AES**.

- e. **Privacy Password:** Use the Privacy Password of the TrapListener service.
 - f. **Privileges:** Select a privilege from the drop-down menu. Using the **Read/Write** privilege, you can perform both GET and SET operations on MIBs. Using the **Read** privilege, you can perform only the GET operation on MIBs. The default is **None**.
4. Click **Commit**.

Related links

[SNMP Support for Avaya Breeze platform](#) on page 14

Creating an SNMP target profile

About this task

Create a target profile for the System Manager TrapReceiver. The System Manager Serviceability Agent is already configured with a default target profile and default user for the local TrapReceiver. Other target profiles can be set up for the SAL Gateway and NMS destinations to receive alarm traps/informs.

Procedure

1. In System Manager, click **Services > Inventory > Manage Serviceability Agents > SNMP Target Profiles**.
2. Either:
 - Select the default, **SMGR Trap Receiver**, and click **Edit**, or
 - Click **New** to create a new target profile.
3. Enter the following information:
 - a. **Name:** If you are creating a new target profile, enter the SNMP target profile name.
 - b. **Description:** Enter a description of the SNMP target profile. This field is optional.
 - c. **IP Address:** Enter the IP address of the target server.
 - d. **Port:** Enter the port of the target server.
 - e. **Notification Type:** Select a Notification Type from the drop-down menu. The values are **Trap** and **Inform**.
 - f. **Protocol:** Select the appropriate SNMP protocol from the drop-down menu.
4. Click the **Attach/Detach User Profile** tab.
5. Select the appropriate **User Profile**, if applicable.
6. Click **Commit**.

Related links

[SNMP Support for Avaya Breeze platform](#) on page 14

Configuring the Avaya Breeze® platform Serviceability Agent

Procedure

1. Change the **Authentication Password** and the **Privacy Password** according to the specifications of the customer for the System Manager TrapListener. See [Configuring the TrapListener service](#) on page 15.
2. Set up an SNMPv3 User Profile to match the System Manager TrapListener settings. See [Creating an SNMPv3 user profile](#) on page 16.
3. Set up a target profile for the System Manager TrapReceiver. See [Creating an SNMP target profile](#) on page 17.
4. In System Manager, click **Services > Inventory > Manage Serviceability Agents > Serviceability Agents**.
5. Verify the Avaya Breeze® platform Serviceability Agent hostname and IP address appear in the **Agent List**.
6. Verify the status of the Avaya Breeze® platform Serviceability Agent is **Active**.
7. If the status is not **Active**:
 - a. Select the Avaya Breeze® platform Serviceability Agent.
 - b. Click **Activate**.
 - c. Verify the status changes to **Active**.
8. Re-select the agent to enable the **Manage Profiles** button.
9. Click **Manage Profiles**.
10. Using the appropriate tabs, assign the target and user profiles.
11. Click **Commit**.

Related links

[SNMP Support for Avaya Breeze platform](#) on page 14

Downloading the Avaya Breeze® platform SNMP MIB

About this task

Snap-ins define their own alarms. When you load a snap-in on System Manager, Avaya Breeze® platform generates a `ce-mibs-version.zip` or a `ce-services-mib.zip` zip file. You can download this zip file from the SNMP MIB Download page.

Procedure

1. In System Manager, click **Elements > Avaya Breeze® > System Tools and Monitoring > SNMP MIB**.

2. On the SNMP MIB Download page, click **Download** .

 Tip:

If the page gets stuck after you click **Download**, you can reset it by clicking any navigation link on the left side of the screen. You do not need to download the zip file again.

3. Open the file using a utility such as WinZip.
4. Save the file.
5. Expand the downloaded compressed files.
6. Import all the MIB files with the .my extension to a Network Management System (NMS).
7. Download the Avaya_Aura_ServicabilityAgent_Mib.my MIB file from <https://support.avaya.com> and import it onto the NMS.

Related links

[SNMP Support for Avaya Breeze platform](#) on page 14

Chapter 5: Operations supported on System Manager for alarming

The Avaya Aura® System Manager web console provides the following operations for alarms:

- Viewing the Avaya Breeze® platform server and snap-in alarms.
- Filtering and searching for alarms.
- Exporting alarms to a comma separated values (csv) file.
- Changing the alarm status.

Related links

[Generating test alarms in System Manager](#) on page 20

[Verifying test alarms in System Manager](#) on page 21

[Viewing alarms](#) on page 21

[Filtering alarms](#) on page 22

[Searching for alarms](#) on page 22

[Exporting alarms](#) on page 23

[Changing the alarm status](#) on page 24

[Alarming field descriptions](#) on page 24

Generating test alarms in System Manager

About this task

Generate test alarms to verify that Avaya Breeze® platform sends alarms to System Manager.

Procedure

1. In System Manager, click **Services > Inventory > Manage Serviceability Agents > Serviceability Agents**.
2. In the **Agents List** section, select the Avaya Breeze® platform servers to generate the test alarms.
3. Click **Generate Test Alarm**.

Next steps

Verify the test alarms.

Related links

[Operations supported on System Manager for alarming](#) on page 20

Verifying test alarms in System Manager

Before you begin

Generate test alarms.

Procedure

1. On the System Manager web console, click **Services > Events**.
2. On the left navigation pane, click **Events > Alarms**
System Manager displays the Alarming page.
3. Click **Advanced Search**.
4. Search for the following criteria:
 - a. In the first drop-down list, select **Event ID**
 - b. In the second drop-down list, select **Equals**
 - c. In the third field, type the following event ID of the test alarm: `OP_TALM00100`
5. Click **Search**.
System Manager displays the alarm list based on the search criteria.
6. Do the following to clear the alarms:
 - a. Log in to the Avaya Breeze® platform instance as an administrative user.
 - b. Run the following command: `generateTestAlarmCE.sh -c`
7. On the System Manager web console, verify that the status of the alarms changed to **Cleared**.

Related links

[Operations supported on System Manager for alarming](#) on page 20

[Avaya Breeze platform does not send alarms to System Manager](#) on page 85

Viewing alarms

The **Alarms List** page displays the alarms and information about each alarm. The alarm information includes the time the alarm occurred, the severity of the alarm, the current status of the alarm, the Host Name or System Name of where the alarm occurred, and a description.

Procedure

1. In System Manager, click **Elements > Avaya Breeze® > Server Administration**.
2. To view the alarm details, click the link in the **Alarms** column.

Related links

[Operations supported on System Manager for alarming](#) on page 20

Filtering alarms

You can filter alarms based on certain criteria. You can use more than one filter criterion on the selected alarms.

Procedure

1. In System Manager, click **Elements > Avaya Breeze® > Server Administration**.
2. Click the link in the **Alarms** column.
3. On the **Alarming** page, select the alarm to filter.
4. Click **Filter: Enable** at the top right of the alarm table.
5. Select the filter criteria to apply to the selected alarms.

The **Status** and **Severity** fields have drop-down menus.

6. Click **Filter: Apply**.

The page displays the alarms matching the filter criteria. A message is displayed if no alarms match the filter criteria.

Related links

[Operations supported on System Manager for alarming](#) on page 20

Searching for alarms

Use the **Advanced Search** function to find alarms based on certain conditions. The system displays only those alarms which satisfy the search conditions. You can specify multiple search conditions.

Procedure

1. In System Manager, click **Elements > Avaya Breeze® > Server Administration**.
2. Click the link in the **Alarms** column.
3. Click **Advanced Search**.

4. In the **Criteria** section, from the first and second drop-down fields, select one of the following search criteria:
 - Time Stamp
 - Severity
 - Status
 - Host name or system name
 - Identifier
 - M/E Reference number or System OID
 - Event ID
 - Source IP address
 - Notification OID
 - Description
5. Select or enter the search value in the third field.
6. To add another search condition, click the **+** sign and select the AND or OR operator from the drop-down field.

To delete a search condition, click the **-** sign. You can delete a search condition only if you added more than one search condition.
7. To find alarms for the given search conditions, click **Search**.

Related links

[Operations supported on System Manager for alarming](#) on page 20

Exporting alarms

You can export alarms to a Comma Separated Values (.csv) file. You can open the CSV file using a text editor such as Wordpad or a spreadsheet application such as Microsoft Excel.

Procedure

1. In System Manager, click **Elements > Avaya Breeze® > Server Administration**.
2. Click the link in the **Alarms** column.
3. On the Alarming page, perform one of the following steps:
 - To export an alarm to a CSV file, select an alarm and click **More Actions > Export Selected**.
 - To export all the alarms to a CSV file, click **More Actions > Export All**.
4. Click **Save** to save the exported file to the local disk.

Related links

[Operations supported on System Manager for alarming](#) on page 20

Changing the alarm status

You can change the status of an alarm to:

- **Acknowledged:** This state indicates the alarm is under investigation.
- **Cleared:** This state indicates the error condition has been resolved.

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®** > **Server Administration**.
2. Click the link in the **Alarms** column.
3. On the **Alarming** page, select the alarm and click **Change status**. You can select multiple alarms.
4. Select the status to apply to the selected alarm or alarms.

Related links

[Operations supported on System Manager for alarming](#) on page 20

Alarming field descriptions

The Alarming page has two sections.

The upper section displays buttons that you can use to view the details of the selected alarms, change the status of alarms, search for alarms, and set filters to view specific alarms.

The lower section displays alarms in a table. The table provides information such as the status of the alarms and the alarm severity. You can click a column title to sort the information in the table in ascending or descending order.

Field	Description
Time Stamp	Specifies the date and time when the alarm is generated.
Severity	Specifies the severity of the alarm.
Status	Specifies the current status of the alarms.
Host Name / SysName	Specifies the name of the host server that generated the alarm. In case of the trap listener service, this column specifies the system name.
Source IP Address	Specifies the IP address of the system that generated the alarm.

Table continues...

Field	Description
Description	Provides a detailed description of the problem that generated the alarm.
Identifier	Specifies the unique identifier for an alarm.
Event ID	Specifies the log event ID if the alarm is generated from logs or the Event OID if the alarm is generated from the trap listener service.
NotificationOID	Specifies the SNMP OID of the alarm.
M/E Ref Number / SysOID	Specifies the unique identification number assigned to the product, also called the product ID. This number helps in identifying the component that generated the alarm. For alarms that are generated from trap listener, the system displays the System OID.

Button	Description
View	Displays the details of the selected alarms.
Change Status	Changes the status of the selected alarm. The options are: • Acknowledged • Cleared
Auto-Refresh Mode	Changes over to the Auto-Refresh mode. When the Alarming page is set in this mode, it automatically updates the alarms in the table. A toggle button.
More Actions > Export Selected	Exports the selected alarms to a CSV file, which can be viewed with Wordpad or Excel.
More Actions > Export All	Exports all the alarms to a CSV file, which can be viewed with Wordpad or Excel.
Advanced Search	Displays fields that you can use to specify the search criteria for searching an alarm.
Refresh	Refreshes the log information in the table.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. A toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. A toggle button.
Filter: Clear	Clears the filter criteria.
Filter: Apply	Filters alarms based on the filter criteria.
All	Selects all the alarms in the table.
None	Clears the check box selections.
Previous	Displays the logs in the previous page. This button is not available if you are on the first page.
Next	Displays the logs in the next page. This button is not available if you are on the last page.

Criteria section

This section appears when you click **Advanced Search** on the upper right corner of page.

Name	Description																
Criteria	Use this section to specify search conditions. Select the search criteria from the first drop-down list. Select the operator from the second drop-down list. Enter the search value in the text field. Select following search criteria from the first drop-down list: • Time Stamp: Searches all of the alarms that match the specified date and time. The valid format for entering the date is MM/DD/YYYY. The valid format for entering the time is HH:MM. • Severity: Searches all the alarms that match the specified severity level. • Status: Searches all the alarms that match the specified status. • Host Name: Searches all of the alarms that are generated from the specified host. • Identifier: Searches all the alarms that match the specified identifier. • Description: Searches all the alarms that match the specified description. • M/E Ref Number: Searches all the alarms that match the specified M/E Ref Number. The operators available are based on the search criterion that you select in the first drop-down field. The following table lists the operators that are available for a search criterion: <table> <tr> <th>Criterion</th><th>Operators</th></tr> <tr> <td>Time Stamp</td><td>=, >, <, >=, <=, >=, !=</td></tr> <tr> <td>Severity</td><td>Equals, Not Equals</td></tr> <tr> <td>Status</td><td>Equals, Not Equals</td></tr> <tr> <td>Host Name</td><td>Equals, Not Equals, Starts With, Ends With, and Contains</td></tr> <tr> <td>Identifier</td><td>=, >, <, >=, <=, >=, !=</td></tr> <tr> <td>Description</td><td>Equals, Not Equals, Starts With, Ends With, and Contains</td></tr> <tr> <td>M/E Ref Number</td><td>Equals, Not Equals, Starts With, Ends With, and Contains</td></tr> </table> When you select Begin Date and End Date from the first drop-down list, you are prompted to enter the date in the third field.	Criterion	Operators	Time Stamp	=, >, <, >=, <=, >=, !=	Severity	Equals, Not Equals	Status	Equals, Not Equals	Host Name	Equals, Not Equals, Starts With, Ends With, and Contains	Identifier	=, >, <, >=, <=, >=, !=	Description	Equals, Not Equals, Starts With, Ends With, and Contains	M/E Ref Number	Equals, Not Equals, Starts With, Ends With, and Contains
Criterion	Operators																
Time Stamp	=, >, <, >=, <=, >=, !=																
Severity	Equals, Not Equals																
Status	Equals, Not Equals																
Host Name	Equals, Not Equals, Starts With, Ends With, and Contains																
Identifier	=, >, <, >=, <=, >=, !=																
Description	Equals, Not Equals, Starts With, Ends With, and Contains																
M/E Ref Number	Equals, Not Equals, Starts With, Ends With, and Contains																

Button	Description
Clear	Clears the entered search criteria and sets the default search criteria.
Search	Searches the alarms based on the search conditions.
Close/Advanced Search	Hides the search fields.
+	Adds a search condition.
-	Deletes a search condition.

Related links

[Operations supported on System Manager for alarming](#) on page 20

Chapter 6: Avaya Breeze® platform alarm descriptions

The following sections provide information about alarm event IDs, including a description, the severity, and a recovery action.

AAMS_AUTHERROR

An Avaya Breeze® platform server is using the wrong credentials to connect to Avaya Aura® Media Server.

Severity

Warning

Recovery action

Verify that the user ID and password configured in the Avaya Breeze® platform cluster attributes are identical to those configured on Avaya Aura® Media Server for basic authentication in the REST configuration.

See [Troubleshooting Avaya Aura Media Server issues](#) on page 114.

AAMS_CONNFAIL

An Avaya Breeze® platform server is unable to connect to an Avaya Aura® Media Server.

Severity

Warning

Recovery action

Check if Avaya Aura® Media Server is working and can establish connections. Verify the certificate configuration of Avaya Aura® Media Server and the Avaya Breeze® platform server.

See [Troubleshooting Avaya Aura Media Server issues](#) on page 114.

AAMS_LOCKED

The Avaya Aura® Media Server is in a locked state.

Severity

Warning

Recovery action

Configure Avaya Aura® Media Server to an unlocked state.

AAMS_OVERLOAD

Avaya Aura® Media Server is in an overloaded state.

Severity

Warning

Recovery action

Check if any Avaya Aura® Media Server instances are not working. The Avaya Aura® Media Server instances that are not working might cause an overload on other instances.

This overload condition might indicate that the Avaya Aura® Media Server capacity needs to be increased.

ARBITER_10001

Avaya Breeze® platform server switches to a different System Manager.

Severity

Warning

Recovery action

No action required.

ARBITER_10002

Avaya Breeze® platform server does not have a master System Manager.

Severity

Warning

Recovery action

No action required.

ARBITER_10003

In a geographically redundant environment, the System Manager servers are in the active or standby mode after coming back to the sunny day scenario.

Severity

Warning

Recovery action

Manually clear the alarms after the System Manager servers return to the sunny day scenario.

AU_GEMMTC20061

An audit event that indicates that an auto-switchover has occurred in the cluster database.

Severity

Info

Recovery action

See [Auto-switchover has occurred in a cluster database](#) on page 86.

AuthorizationService_GENERR1

Any generic error that occurs when the authorization service tries to connect to an LDAP data source provisioned in System Manager.

Severity

Major

Recovery action

Troubleshoot the issue by checking the appended root cause in the alarm description.

avCEAVDM52603

State of Health Daemon (SOHD) load balancer arbiter failed to ping the default gateway.

Severity

Minor

Recovery action

Network outage detected. Verify network access and connectivity in your environment.

avCECVDM52603

SOHD load balancer arbiter recovered to ping default gateway.

Severity

Minor

Recovery action

No action required.

BR_MMTC20053

The Call Processing database sanity check failed.

Severity

Major

Recovery action

See [Maintenance test for Call Processing status fails](#) on page 109.

CCLRCONNFAIL

Severity

Major

Recovery action

Clear the alarm.

CCONNFAIL

Severity

Major

Recovery action

Check that the Zang Call connector is deployed in the cluster, and at least one snap-in uses the call connector.

For more information, see [Viewing log details](#) on page 141.

CLR_CONERR2

A connection error has been cleared. The connection error was previously raised by the authorization service when trying to connect to an LDAP data source provisioned in System Manager.

Severity

Info

Recovery action

No action required.

CLR_GENERR1

A generic error has been cleared. The generic error was previously raised by the authorization service when trying to connect to an LDAP data source provisioned in System Manager.

Severity

Info

Recovery action

No action required.

CLR_MBCN_ERR_001

The Metric beat service failure alarm cleared.

Severity

Warning

Recovery action

No action required.

CLR_PBCN_ERR_001

The Packet beat service failure alarm cleared.

Severity

Warning

Recovery action

No action required.

CLR_SSLERR3

An SSL error has been cleared. The SSL error was previously raised by the authorization service when trying to connect to an LDAP data source provisioned in System Manager.

Severity

Info

Recovery action

No action required.

CONERR2

A connection error that occurs when the authorization service tries to connect to an LDAP data source provisioned in System Manager.

Severity

Major

Recovery action

Rectify the connection between the LDAP source and the Avaya Breeze® platform nodes.

DRS_DBG_0001

DRS client batch error.

Severity

Major

Recovery action

See [Data Replication Service Synchronization failure](#) on page 94.

FILEBEATCONNECTIONERROR

The Filebeat connection to the centralized logging server failed.

Severity

Major

Recovery action

See [Troubleshooting Filebeat service connection errors](#) on page 119.

FILEBEATCONNECTIONFINE

The Filebeat connection to the centralized logging server is restored.

Severity

Major

Recovery action

See [Troubleshooting Filebeat service connection errors](#) on page 119.

MBCN_ERR_001

The Metric beat service failed.

Severity

Warning

Recovery action

No action required.

nsNotifyRestart

An indication that the SNMP agent restarted.

Severity

Indeterminate

Recovery action

No action required.

nsNotifyShutdown

An indication that the SNMP agent is in the process of shutting down.

Severity

Indeterminate

Recovery action

No action required.

nsNotifyStart

An indication that the SNMP agent is running.

Severity

Indeterminate

Recovery action

No action required.

OP_AASL10900

Certificate load failure.

Severity

Major

Recovery action

See [Certificate status](#) on page 88.

OP_ANFW11001

Network firewall stopped.

Severity

Warning

Recovery action

See [Network firewall stopped](#) on page 105.

OP_ANFW11002

SM100 network firewall critical event.

Severity

Warning

Recovery action

See [Network firewall critical event](#) on page 104.

OP_APLM10300

Failure pinholing network firewall.

Severity

Major

Recovery action

See [Network firewall pinholing](#) on page 104.

OP_APLM10302

Failure configuring network parameters.

Severity

Major

Recovery action

See [Network configuration error](#) on page 104.

OP_APLM10304

Security Module interface is not running.

Severity

Major

Recovery action

See [Network configuration error](#) on page 104.

OP_AWTC10405

An identity certificate is about to expire.

Severity

Warning

Recovery action

See [Certificate expiration](#) on page 88.

OP_AWTC10406

An identity certificate has expired.

Severity

Critical

Recovery action

See [Certificate expiration](#) on page 88.

OP_CDAO50001

The database connection is not working. Administration updates do not function during this update.

Severity

Minor

Recovery action

See [Troubleshooting database connection errors](#) on page 93.

OP_CDAO50002

Administration relating to certain screens might have caused a database query failure (SQL Exception).

Severity

Minor

Recovery action

See [Database Query](#) on page 94.

OP_CDAO50003

Administration relating to certain screens might have recently created an entry in the database, which will not be actualized in the Runtime system due to an error with imposed restrictions.

Severity

Minor

Recovery action

See [Unexpected data](#) on page 117.

OP_CDAO50111

The Avaya Breeze® platform instance cannot be resolved.

Severity

Critical

Recovery action

See [Avaya Breeze platform instance resolution failure](#) on page 89.

OP_CDAO50112

Multiple Avaya Breeze® platform IP addresses map to the local Avaya Breeze® platform instance.

Severity

Minor

Recovery action

See [Avaya Breeze platform instance resolution failure](#) on page 89.

OP_CEMMTC20033

Management instance check failed.

Severity

Minor

Recovery action

See [Management instance check failed](#) on page 102.

OP_CMON55001

The SIP monitoring state for an entity is partially up.

Severity

Warning

Recovery action

See [Troubleshooting SIP Entity Monitoring alarms](#) on page 112.

OP_CMON55002

The SIP monitoring state for an entity is out of service.

Severity

Minor

Recovery action

See [Troubleshooting SIP Entity Monitoring alarms](#) on page 112.

OP_GEMMTC20033

The Avaya Breeze® platform snap-in has no license file or the license file has expired. The snap-in is in error mode.

Severity

Major

Recovery action

See [License errors](#) on page 97.

OP_GEMMTC20035

The Avaya Breeze® platform snap-in goes to the restricted mode and is uninstalled from the clusters.

Severity

Critical

Recovery action

See [License errors](#) on page 97.

OP_GEMMTC20037

The Avaya Breeze® platform server is in the license error mode.

Severity

Major

Recovery action

See [License errors](#) on page 97.

OP_GEMMTC20039

The Avaya Breeze® platform server is in the license restricted mode. The Avaya Breeze® platform server is out of service in the restricted mode.

Severity

Critical

Recovery action

See [License errors](#) on page 97.

OP_MAMA20102

Security Module Management Agent cannot configure the Security Module.

Severity

Major

Recovery action

See [Security Module Management Agent is not able to configure Security Module](#) on page 111.

OP_MMTC200[1-4][13579]

The Postgres database sanity check failed. The database is not accessible.

Severity

Major

Recovery action

See [Troubleshooting Postgres database sanity check failures](#) on page 106.

OP_MMTC20019

The SAL Agent sanity check failed. Alarms cannot be processed.

Severity

Minor

Recovery action

See [Troubleshooting SAL sanity check failures](#) on page 107.

OP_MMTC20025

Security Module sanity check failed. Avaya Breeze® platform is down.

Severity

Major

Recovery action

See [Troubleshooting SAL sanity check failures](#) on page 107 and [Security Module failure](#) on page 110.

OP_MMTC20031

Data distribution/redundancy is down.

Severity

Minor

Recovery action

Clear the alarm.

OP_MMTC20047

Avaya Breeze® platform is using the default authentication file.

Severity

Warning

Recovery action

This alarm code only applies only to Avaya Breeze® platform Release 3.2 and earlier.

OP_MMTC20048

A certificate is nearing its expiration date.

Severity

Warning

Recovery action

See [Certificate expiration](#) on page 88.

OP_MMTC20049

A certificate is nearing its expiration date.

Severity

Major

Recovery action

See [Certificate expiration](#) on page 88.

OP_MMTC20050

A certificate is nearing its expiration date.

Severity

Critical

Recovery action

See [Certificate expiration](#) on page 88.

OP_MMTC20051

The DCM database sanity check failed.

Severity

Major

Recovery action

See [DCM sanity check failed](#) on page 109.

OP_MMTC20052

The DCM sanity check error resolution failed.

Severity

Major

Recovery action

Resolve the OP_MMTC20051 event code.

OP_MMTC20054

The Call Processing database sanity check error resolution failed.

Severity

Major

Recovery action

Resolve the BR_MMTC20053 event code.

OP_MMTC20055

The Reliable Eventing broker group cannot deliver maintenance test events.

Severity

Major

Recovery action

See [Troubleshooting Reliable Eventing maintenance test failures](#) on page 101.

OP_MMTC20129

The platform service SAR is not deployed.

Severity

Major

Recovery action

See [Platform Application did not start](#) on page 105.

OP_MWD20202

The snap-in monitored by Watchdog has failed.

Severity

Minor

Recovery action

See [Troubleshooting Avaya Breeze platform service failures](#) on page 112.

OP_MWD20204

WebSphere does not respond to SIP requests.

Severity

Major

Recovery action

The Avaya Breeze® platform monitoring of WebSphere fails, indicating that WebSphere is no longer functioning. At this point, Watchdog restarts WebSphere in an attempt to clear the condition. If the problem persists, contact Avaya support personnel.

OP_TALM00100

Test alarm only.

Severity

Indeterminate

Recovery action

No action required.

OP_TestAlarm

Clear event for testing only.

Severity

Indeterminate

Recovery action

No action required.

OP_TMAG20500

When you modify a certificate, you see a warning message indicating that Avaya Breeze® platform should be restarted to avoid any potential outages.

Severity

Warning

Recovery action

Renew the MGMT certificate or WAS certificate. Navigate to **System Manager > Services > Manage Elements** to renew the certificate.

See [Certificate change requires WAS restart](#) on page 87.

OP_TMAG20501

When you modify a certificate, you see a warning message indicating that Avaya Breeze® platform should be restarted to avoid any potential outages.

Severity

Warning

Recovery action

See [Certificate change requires WAS restart](#) on page 87.

OVERLOAD_100001

The Avaya Breeze® platform server is in an overload state. This error puts the server in the **Deny New Service** state and prohibits new SIP and HTTP traffic.

Severity

Major

Recovery action

See [Avaya Breeze platform in overload](#) on page 89.

OVERLOAD_100002

The Avaya Breeze® platform is no longer in the overload state. This alarm puts the server back into the **Accept New Service** state.

Severity

Warning

Recovery action

See [Avaya Breeze platform not in overload](#) on page 91.

OVERLOAD_100003

An Avaya Breeze® platform extended overload condition has been reached. Snap-ins are uninstalled and new snap-ins cannot be deployed.

Severity

Critical

Recovery action

See [Avaya Breeze platform in overload](#) on page 89.

OVERLOAD_100004

The Avaya Breeze® platform server is in an overload warning state.

Severity

Minor

Recovery action

See [Avaya Breeze platform in overload](#) on page 89.

PBCN_ERR_001

The Packet beat service failed.

Severity

Warning

Recovery action

No action required.

Postgres alarms

The following Postgres alarms do not have an associated event ID.

Event ID	Severity	Description	Action
N/A	Minor	Postgres connection failure.	See Hard disk drive data save errors on page 96.
N/A	Minor	Postgres integrity or protocol violation.	
N/A	Minor	Postgres invalid transaction failure.	
N/A	Minor	Postgres insufficient resource failure.	
N/A	Minor	Postgres resource issues failure.	
N/A	Minor	Postgres I/O or internal errors.	See Database error on page 94.
N/A	Minor	Postgres connection or indexing issues.	

SEC_000421

The TLS version that the snap-in requested is lower than the minimum supported TLS version configured for System Manager or the cluster.

Severity

Minor

Recovery action

Change the TLS version:

- Increase the TLS version that the snap-in requested to match the minimum supported TLS version configured for System Manager or the cluster.
- Decrease the minimum supported TLS version configured to match the TLS version that the snap-in requested.

SNAPINSCRIPTFAILED

Installation of the snap-in with `setup.sh` failed with unrecoverable errors.

Severity

Major

Recovery action

Check the document of the snap-in that raised the alarm for troubleshooting steps.

SSLERR3

An SSL error that occurs when the authorization service tries to connect to an LDAP data source provisioned in System Manager.

Severity

Major

Recovery action

Verify the certificates that are currently deployed. Check if the LDAP CA certificate is properly installed in the cluster.

For more information, you can also check the appended root cause in the alarm description.

UCAService_UCA_ALARM_1

UCA service alarms

Severity

N/A

Recovery action

See *Engagement Call Control Snap-in Reference* to troubleshoot UCA service alarms.

Chapter 7: Cluster and server administration

In System Manager, from **Elements > Avaya Breeze®**, you can navigate to **Cluster Administration** or **Server Administration**. From the values of the fields present on the Cluster Administration and Server Administration pages, you can determine if there are alarms, service installation issues, security module issues, license issues, or replication issues.

Cluster administration field descriptions

Use this page to:

- Access information about the status of the Avaya Breeze® platform clusters.
- Add or edit an Avaya Breeze® platform cluster.
- Change the status of the Avaya Breeze® platform cluster.
- Assign trust and identity certificates to the Avaya Breeze® platform servers assigned to the cluster.
- Manage cluster database backup and restore operations.

The Cluster Administration page displays failures using the  icon.

On the Cluster Administration page, click **Show** to view the details of the Avaya Breeze® platform instances assigned to the cluster. Click **Hide** to view only the details of the Avaya Breeze® platform cluster.

Name	Description	Troubleshooting procedure
Details	The details of the cluster. You can view the Avaya Breeze® platform instances and services assigned to the cluster.	—
Cluster Name	The unique name of the cluster.	—

Table continues...

Name	Description	Troubleshooting procedure
Cluster Group	The cluster group number that you assign to the cluster. You can enter a value from 1 to 10. This optional field is used only to configure attributes for multiple snap-ins.	—
Cluster IP	The IP address of the cluster. The Cluster IP value is applicable only for HTTP/HTTPS.	If the Avaya Breeze® platform instance does not match the IP address of the configured management interface, then see Avaya Breeze platform instance resolution failure on page 89. To update Avaya Breeze® platform configuration using CEnetSetup, see Updating the Avaya Breeze platform configuration using CEnetSetup on page 126.
Cluster FQDN	The unique FQDN that you assign to the cluster.	—
Cluster Profile	The type of cluster that you want to choose. The options are: • Context Store • Core Platform • Engagement Assistant Speech • General Purpose • General Purpose Large • Work Assignment • Customer Engagement	—
Cluster State	The state of the cluster. The options are: • Accepting state: The cluster can serve service requests. • Denying state: The cluster cannot serve services or calls.	If the number of accepting nodes is lesser than the total number of nodes available in the cluster, then see Troubleshooting when accepting nodes are lesser than the total number of nodes in a cluster on page 116.
Alarms	The number of alarms for the cluster. This value is displayed in the following format: <i><critical + major alarm count>/<minor alarm count>/<warning alarm count></i> .	For Avaya Breeze® platform alarm descriptions, see Avaya Breeze platform alarm descriptions on page 28.

Table continues...

Name	Description	Troubleshooting procedure
Activity	The sum of active Call, HTTP, and other custom-defined sessions of all the snap-ins installed on the Avaya Breeze® platform servers in the cluster.	—
Cluster Database	The High Availability status between the active Avaya Breeze® platform server and the standby Avaya Breeze® platform server in a cluster. • A green background indicates that the connection between the active and the standby servers is up. • A yellow background indicates that the standby server is getting ready to take over if the need arises. • A red background indicates that the connection between the active and the standby server is down. • No background color and the Disabled value indicates that the cluster database is disabled. The Cluster Database displays: • The number of active components and the disk consumption in the following format: <i><number of active connections>/<disk consumption></i>. • - - - - if the server does not report the disk consumption. • Disabled if the cluster database is disabled.	For troubleshooting database connection issues, see Troubleshooting database connection errors on page 93.

Table continues...

Name	Description	Troubleshooting procedure
Data Replication	The aggregated data replication status between all Avaya Breeze® platform servers in a cluster and System Manager. The options are: •  indicates that the replication is successful. •  indicates that one or more nodes have failed replication.	For troubleshooting database connection issues, see Data Replication Service synchronization failure on page 94.
Service Install Status	The aggregated service installation status of all the Avaya Breeze® platform servers in a cluster. The options are: •  indicates that all snap-ins are installed. •  indicates that the snap-in is either queued for installation or for downloading to Avaya Breeze® platform. If downloading to Avaya Breeze® platform fails, the column displays a red cross with the <code>Transfer has failed</code> message. •  indicates that one or more snap-ins have failed to initialize, run, or deploy.	—
Tests Pass	The aggregated maintenance test result for all Avaya Breeze® platform servers in the cluster.  indicates that all Avaya Breeze® platform servers in the cluster have passed the maintenance tests.	For more information, see Maintenance tests on page 65.

Table continues...

Name	Description	Troubleshooting procedure
Data Grid Status	The aggregate status of the data grid in the cluster. The options are: ✓ indicates that the data grid status is up. ⚠ indicates that the status of one or more servers in the cluster is down. ✗ indicates that the data grid status is down.	For troubleshooting connection problems with the Avaya Breeze® platform instances, see Management Instance check failed on page 102.
Overload Status	The overload status of the Avaya Breeze® platform cluster. The options are: ✓ indicates that none of the servers in the cluster are in the overloaded state. ✗ indicates that one or more servers are in the overloaded state.	For troubleshooting when an Avaya Breeze® platform instance is in overload, see Avaya Breeze platform in overload on page 89.
Last Reboot Status	The status of the last cluster restart operation.	—
Service URL	The list of cut-through URLs for the services installed on the Avaya Breeze® platform cluster. If you have administered the cluster IP, that IP is used as the host for the URL. If not, one of the Avaya Breeze® platform server IP is used as the host for the URL.	—

Server details

On the Cluster Administration page, click **Show** for a cluster to view the details of each server in the cluster.

Name	Description
Server Name	The name of the Avaya Breeze® platform server.
Security Module	The status of the security module for the server.
Server Version	The version of the Avaya Breeze® platform server.
Server State	Indicates whether the server is in the accepting or the denying state.
Alarms	The number of alarms for the server. This value is displayed in the following format: <i><critical + major alarm count>/<minor alarm count>/<warning alarm count></i> .

Table continues...

Name	Description
Activity	The sum of active Call, HTTP, and other custom-defined sessions of all the snap-ins installed on the Avaya Breeze® platform server.
Cluster Database	The state of the server in a High Availability database setup. This column is highlighted in: • Green when the active server, standby server, and the idle server are ready. • Yellow when the standby server is preparing. • Red when the active server and the standby server fail. • No background color and displays --- when cluster database is disabled.
Cluster Database Connection	The status of the connection between the active server and the standby server in a high availability database scenario. •  indicates that the connection between the active and the standby servers is up. •  indicates that the standby server is getting ready to take over if the active server goes down. •  indicates that the connection between the active and standby servers is down. • No background color with the value --- indicates that the cluster database is disabled.
Data Replication	The status of data replication between the Avaya Breeze® platform server and System Manager. •  indicates that the replication is successful. •  indicates that the replication failed.
Service Install Status	The service install status for the Avaya Breeze® platform server. •  indicates that all the snap-ins are installed. •  indicates that the snap-in downloading to Avaya Breeze® platform is in progress. If downloading fails, the column displays the  with the Transfer has failed message. •  indicates that one or more snap-ins failed to initialize, run, or deploy.
Tests Pass	The maintenance test result for the Avaya Breeze® platform server.
Data Grid Status	The data grid status of the Avaya Breeze® platform server. The status of the server is either Up or Down for the server.

Table continues...

Name	Description
Overload Status	The overload status of the Avaya Breeze® platform server: •  indicates that the server is not overloaded. •  indicates that the server is in an overloaded state.

Server Administration field descriptions

Use this page to:

- Add or edit an Avaya Breeze® platform server.
- Shutdown or restart an Avaya Breeze® platform server.
- Access information about the service status and maintenance tests for each Avaya Breeze® platform server.

Name	Description	Troubleshooting procedure
Name	The name of the Avaya Breeze® platform server. Click the Name to navigate to the Avaya Breeze® platform Instance Editor page.	—
Cluster Name	The name of the cluster to which the Avaya Breeze® platform server belongs.	—
Service Install Status	The status of the installed services. •  indicates all services have been installed. •  indicates the service is in the process of installing or uninstalling. •  indicates a service has not downloaded properly or is not installed. Under Details, click Show and then click on the icon under Service Install Status.	—

Table continues...

Name	Description	Troubleshooting procedure
Tests pass	Maintenance test result.  indicates the test or tests passed.  indicates a test failed. Click the  or  to navigate to the Maintenance Tests page.	For more information, see Maintenance tests on page 65.
Alarms	The number of alarms raised for the Avaya Breeze [®] platform server. This value is in the format <critical + major alarm count>/<minor alarm count>/<warning alarm count>.	For Avaya Breeze [®] platform alarm descriptions, see Avaya Breeze platform alarm descriptions on page 28.
System State	The current state of the Avaya Breeze [®] platform server. The system states are: • Accepting • Denying	—
Security Module	The state of the Security Module. The states are Up and Down.	To troubleshoot a Security Module failure, see Security Module Management Agent is not able to configure Security Module on page 111.
Activity	The sum of active Call, HTTP, and other custom defined sessions of all the snap-ins installed on the Avaya Breeze [®] platform server.	—

Table continues...

Name	Description	Troubleshooting procedure
License mode	The license mode of the Avaya Breeze® platform server. It is mandatory that all the Avaya Breeze® platform servers be in compliance with the license file, including the major release and the total number of Avaya Breeze® platform servers. The possible license modes are: •  License Normal Mode: A valid license file is installed. License errors are not found. The complete functionality is present for the Avaya Breeze® platform instance. •  License Error Mode: A license error is displayed in this mode. The Avaya Breeze® platform instance is in a 30 day grace period during this mode. Complete functionality is available during the grace period. The system displays the warning icon along with the date and time of the grace period expiration in the License Mode column. •  License Restricted Mode: The Avaya Breeze® platform instance goes in to the restricted mode after the 30 day grace period expires. The Avaya Breeze® platform server goes in to the Deny New Service mode. The server automatically returns to service when the server returns to the License Normal mode.	To troubleshoot licensing errors, see License errors on page 97.
Overload Status	The overload status of the Avaya Breeze® platform server. •  indicates that the server is not in an overloaded state. •  indicates that the server is in an overloaded state.	For troubleshooting when an Avaya Breeze® platform instance is in overload, see Avaya Breeze platform in overload on page 89.

Table continues...

Name	Description	Troubleshooting procedure
Version	The version of the Avaya Breeze® platform software that is installed on the Avaya Breeze® platform server.	For troubleshooting a version mismatch between Avaya Breeze® platform server and the major version in the license file, see Avaya Breeze platform server software version mismatch on page 98.
Last Reboot Status	The status of the last cluster restart operation.	—

Backing up a cluster database

About this task

The backup feature allows databases in the cluster database to be backed up. The cluster database contains different databases defined by the snap-ins that are installed on the cluster.

You can perform a backup on one cluster and restore on another.

Before you begin

- If backing up a cluster from an earlier release of Breeze (for example 3.8.1.1 or earlier) before an upgrade to Breeze 3.9, you must verify the clusterDBMigrationService-3.9.0.0 service is installed on the cluster before proceeding.
- You cannot use a Windows server as the backup destination. Windows servers are incompatible with the Cluster Backup and Restore feature.

Procedure

1. In System Manager, click **Elements > Avaya Breeze® > Cluster Administration**.
2. Click **Backup and Restore > Configure**.
3. Enter the backup server details.
4. Click **Test Connection** to verify the connection of the backup server.
5. Click **Commit**.
6. Select the cluster that you want to backup and click **Backup and Restore > Backup**.
The system displays the Cluster DB Backup page.
7. In the **Backup** section, select the services to back up.
8. In the **Job schedule** section, enter the following details:
 - In the **Backup password** field, enter a password.
 - In the **Schedule Job** field, to run an immediate backup select **Run immediately**. Otherwise, select **Schedule later** and enter the required details in the **Task Time**, **Recurrence**, and **Range** fields.

9. Click **Backup**.

- To monitor the status of the backup, click **Backup and Restore > Job Status**.
- To cancel a backup operation, click **Backup and Restore > Cancel**.

Restoring the cluster database

About this task

You can perform the restore process on any cluster which has the cluster database enabled.

Before you begin

- Enable the cluster database.
- You cannot use a Windows server as the backup destination. Windows servers are incompatible with the Cluster Backup and Restore feature.

Procedure

1. In System Manager, click **Elements > Avaya Breeze® > Cluster Administration**.
2. Click **Backup and Restore > Restore**. The system lists the backup and restore jobs.
3. Select a completed backup and then click **Restore**.
4. Select the cluster on which you want to restore the backup and then click **Continue**.

Chapter 8: Data replication

The DRS replicates data and configuration from System Manager to the Avaya Breeze® platform nodes.

DRS sends the data in batches from the master database to the replica node. DRS creates replication batches when the data in the master database is added, modified, and deleted.

On the DRS Replication page, you can:

- View replica nodes in a replica group.
- Replicate requested data from the System Manager master database to the database of the replica nodes if the databases are not synchronized.

The replica group for Avaya Breeze® platform displays as AvayaBreeze_<release> on the Replica Groups page.

Related links

[Viewing replica groups](#) on page 61

[Viewing replica nodes in a replica group](#) on page 62

[Repairing a replica node](#) on page 62

[Repairing all replica nodes in a replica group](#) on page 62

[Viewing replication details for a replica node](#) on page 63

[Removing a replica node](#) on page 63

[Removing a replica node from queue](#) on page 64

Viewing replica groups

Procedure

On the System Manager web console, click **Services > Replication**.

Result

The system displays the Replica Groups page with the groups in a table.

Related links

[Data replication](#) on page 61

Viewing replica nodes in a replica group

Procedure

1. In System Manager, click **Services > Replication**.
2. On the Replica Groups page, select a replica group.
3. Click **View Replica Nodes**.

The Replica Nodes page displays the replica nodes for the selected group.

Related links

[Data replication](#) on page 61

Repairing a replica node

Procedure

1. In System Manager, click **Services > Replication**.
2. On the Replica Groups page, perform one of the following:
 - Select a replica group for which you want to repair the replica nodes from the table displaying replica groups and click **View Replica Nodes**.
 - Click the name of the replica node under the **Replica Group** column.
3. On the Replica Nodes page, select a replica node and click **Repair**.

The **Synchronization Status** column displays the data replication status for the replica node.

Related links

[Data replication](#) on page 61

Repairing all replica nodes in a replica group

About this task

You can replicate data for all the replica nodes that are in a group. You can perform this operation if replica nodes in a group are not synchronized with the System Manager database.

Procedure

1. On the System Manager web console, click **Services > Replication**.
2. On the Replica Groups page, select a replica group for which you want repair the replica nodes from the table displaying replica groups.
3. Click **Repair**.

The **Synchronization Status** column displays the data replication status for the replica group.

Related links

[Data replication](#) on page 61

Viewing replication details for a replica node

You can view the batch-related information such as total number of batches received, processed, and skipped for a replica node. The master database sends the requested data in batches to the replica node.

Procedure

1. On the System Manager web console, click **Services > Replication**.
2. On the Replica Groups page, select a replica group and click **View Replica Nodes**.

The Replica Nodes page displays the replica nodes for the selected replica group in a table.

3. Select a replica node and click **View Details**.

The Data Replication page displays the replication details for the selected replica node.

Related links

[Data replication](#) on page 61

Removing a replica node

About this task



Warning:

Removing replica nodes or groups can cause problems with systems that use the configuration data for active call processing. These operations should be done with care to avoid unwanted service disruptions.

Procedure

1. On the System Manager web console, click **Services > Replication**.
2. On the **Replica Groups** page, select the replica group in which you want to remove a node.
3. Select **View Replica Nodes**.
4. Select the **Replica Node Host Name** you want to remove.
5. Select **Remove**.

Related links

[Data replication](#) on page 61

Removing a replica node from queue

About this task



Warning:

Removing replica nodes or groups can cause problems with systems that use the configuration data for active call processing. These operations should be done with care to avoid unwanted service disruptions.

Procedure

1. On the System Manager web console, click **Services > Replication**.
2. On the **Replica Groups** page, select the replica group you want to remove the node from queue.
3. Select **View Replica Nodes**.
4. Select the **Replica Node Host Name** you want to remove.
5. Select **Remove from Queue**.

Related links

[Data replication](#) on page 61

Chapter 9: Maintenance tests

The Avaya Breeze® platform maintenance tests perform functionality and administrative tests on the Avaya Breeze® platform instance. These tests include checking network connectivity and database functionality. The tests are run periodically by the system and can be run on demand.

Tests can fail to execute if the Avaya Breeze® platform instance being tested is down or not responding.

Related links

[Avaya Breeze platform maintenance test descriptions](#) on page 65

[Running maintenance tests](#) on page 66

[Running Reliable Eventing Framework maintenance tests](#) on page 67

[System resource monitor](#) on page 67

[System resource monitor](#) on page 67

Avaya Breeze® platform maintenance test descriptions

Test Alarm Status

This test checks the alarm status of a particular Avaya Breeze® platform server. If the alarm functionality is working correctly, the test passes. An alarm is raised to check if the Avaya Breeze® platform server can raise an alarm to the System Manager database.

Note:

You must configure the Serviceability Agent before you run the alarm test.

Test Cluster Database

This test monitors the connection between Avaya Breeze® platform and the active cluster database.

Test Datagrid Cluster Manager

This test monitors the DataGrid Cluster Manager (DCM) process and Datagrid on the Avaya Breeze® platform server. The test fails and an alarm is raised if DCM is not running or when the Avaya Breeze® platform server is in a cluster and Datagrid is not running.

Test management link status

This test checks the administrative link to Avaya Breeze® platform. If this test fails, administrative changes cannot take effect on Avaya Breeze® platform.

Test Postgres database sanity

This test checks if the master database is corrupted.

Test Reliable Eventing Framework

This test verifies the reliable message delivery by the participating broker group. If the test fails, verify the following on the selected node:

- Server status
- Broker status
- Network status
- Deny New Service state

For more information, see [Running Reliable Eventing Framework maintenance tests](#) on page 67. For information on how to configure Reliable Eventing, see [Administering Avaya Breeze® platform](#).

Test sanity of the Secure Access Link (SAL) agent

This tests checks if the Secure Access Link agent is running on the server. If the link is up and running, the test passes.

If the test fails, run the `statapp` command in the server that had the failure.

Test Call Processing status

This test is a call processing test for a particular Avaya Breeze® platform server. If call processing is working correctly, the test passes. If the test fails, troubleshoot the problem.

If the maintenance tests fail and the troubleshooting steps for the failed maintenance tests do not solve the problem, contact Avaya support personnel.

Test Alarm status

This test triggers the Avaya Breeze® platform node to send a test alarm to the provisioned destination. If the test alarm fails, check the serviceability agent configuration.

Test webSphere Hung Thread status

This test raises an alarm when it detects a hung thread in webSphere. If the problem persists, contact Avaya support personnel.

Related links

[Maintenance tests](#) on page 65

[Maintenance test for Call Processing status fails](#) on page 109

Running maintenance tests

Procedure

1. In System Manager, click **Elements > Avaya Breeze®**.
2. In the navigation pane, click **System Tools And Monitoring > Maintenance Tests**.

3. In the **Select Avaya Breeze® to test** field, select an Avaya Breeze® platform server from the drop-down menu.
 - a. To run all the tests, click **Execute All Tests**.
 - b. To run specific tests: Select the test or tests that you want to run and then click **Execute Selected Tests**.

Related links

[Maintenance tests](#) on page 65

Running Reliable Eventing Framework maintenance tests

Procedure

1. In System Manager, click **Elements > Avaya Breeze®**.
2. In the navigation pane, click **System Tools And Monitoring > Maintenance Tests**.
3. From the **Select Avaya Breeze to test** drop-down list, select an Avaya Breeze® platform server.
4. Select **Test Reliable Eventing Framework**.
5. Click **Execute Selected Tests**. If the test fails, verify the following:
 - a. The Avaya Breeze® platform node server status on the Server Administration page. If the Avaya Breeze® platform node is not running restart the Avaya Breeze® platform node.
 - b. The broker status on the Reliable Eventing Administration page. A high-availability (HA) broker group must have a minimum of two running brokers in a cluster. By design, a broker is not in the running state when the Avaya Breeze® platform node is moved to the **Deny New Service** state.
 - c. Network connection between clients both producer and consumer, and the broker.
 - d. Network connection in a HA broker group.

Related links

[Maintenance tests](#) on page 65

System resource monitor

The System Resource Monitoring tool is used to determine the amount of resources that a service uses. For example, you can view the current resource usage on a cluster before running the service and after running the service. The difference observed in the usage can help determine the resources that the service uses.

Avaya Breeze® platform servers calculate the current and peak usage of the following system resources on the platform. You can view the usage information on System Manager:

- CPU
- Disk
- WebSphere memory
- Cluster database connection count
- SIP sessions
- SIP request rate
- HTTP connections
- HTTP request rate

The system resource data that is collected on Avaya Breeze® platform servers is recorded in the `srdata.log` file located at `/var/log/Avaya/jboss/SessionManager`.

Related links

[Maintenance tests](#) on page 65

[Viewing the current usage of a cluster](#) on page 68

[Viewing the peak usage of a cluster](#) on page 69

[Resetting the peak usage of a cluster](#) on page 69

[System Resource Monitoring page field descriptions](#) on page 69

[Maintenance tests](#) on page 65

[Viewing the current usage of a cluster](#) on page 68

[Viewing the peak usage of a cluster](#) on page 69

[Resetting the peak usage of a cluster](#) on page 69

[System Resource Monitoring page field descriptions](#) on page 69

Viewing the current usage of a cluster

Procedure

1. In System Manager, click **Elements > Avaya Breeze® > System Tools and Monitoring > System Resource Monitor**.
2. In the **Cluster** field, select the cluster for which you want to view the current usage.
3. In the **Time Period** field, select **Today**.
4. Click **View Current Usage**.

The system displays the information in the **Current Resource Usage** table.

Related links

[System resource monitor](#) on page 67

[System resource monitor](#) on page 67

Viewing the peak usage of a cluster

Procedure

1. In System Manager, click **Elements > Avaya Breeze®**.
2. Click **System Tools And Monitoring > System Resource Monitor**.
3. In the **Cluster** field, select the cluster for which you want to view the peak usage.
4. In the **Time Period** field, select one of the following:
 - **Today**
 - **Yesterday**
 - **2 Days Ago**
 - **3 Days Ago**
 - **4 Days Ago**
 - **5 Days Ago**
 - **6 Days Ago**
5. Click **View Peak Usage**.

The system displays the information in the **Peak Resource Usage** table.

Related links

[System resource monitor](#) on page 67

[System resource monitor](#) on page 67

Resetting the peak usage of a cluster

Procedure

1. In System Manager, click **Elements > Avaya Breeze®**.
2. Click **System Tools And Monitoring > System Resource Monitor**.
3. In the **Cluster** field, select the cluster for which you want to reset the peak usage.
4. In the **Time Period** field, select **Today**.
5. Click **Reset Peak Usage**.

Related links

[System resource monitor](#) on page 67

[System resource monitor](#) on page 67

System Resource Monitoring page field descriptions

You can access the System Resource Monitoring page on System Manager by navigating to **Elements > Avaya Breeze® > System Tools and Monitoring > System Resource Monitor**. Use this page to view the current resource usage and peak usage for Avaya Breeze® platform servers in the selected cluster.

Name	Description
Cluster	The cluster for which you want to view usage details.
Time Period	The time period for which you want to view usage details.
Server Name	The name of the Avaya Breeze® platform server.
CPU % Used	The percentage of the CPU processing power that the Avaya Breeze® platform server uses.
WebSphere Memory (MB)	The WebSphere memory use information. This column displays the following information: • Used: The memory that the server uses. • Total: The total memory available to the server. • % Used: The percentage of the total memory that the server uses.
Cluster Database Connections	The status of the connection between the active server and the standby server in a high availability database scenario. •  indicates that the connection between the active and the standby servers is up. •  indicates that the standby server is getting ready to take over if the active server goes down. •  indicates that the connection between the active and standby servers is down. • No background color with the value --- indicates that the cluster database is disabled.
SIP	The details of the SIP sessions active on the server. The column displays the following information: • Sessions: The number of SIP sessions. • Request Rate
HTTP	The details of the HTTP connections active on the server. The column displays the following information: • Connections: The number of HTTP connections. • Request Rate
Disk (MB)	The disk space allocated to the server.

Button	Description
View Current Usage	Displays the current usage details for all nodes in the selected cluster. This button is disabled if the Time Period field is not set to Today.
View Peak Usage	Displays the peak usage details of the selected cluster for the specified day.
Reset Peak Usage	Resets the peak usage values to 0 for all nodes in the selected cluster. This button is disabled if the Time Period field is not set to Today.

Related links

[System resource monitor](#) on page 67

[System resource monitor](#) on page 67

System resource monitor

The System Resource Monitoring tool is used to determine the amount of resources that a service uses. For example, you can view the current resource usage on a cluster before running the service and after running the service. The difference observed in the usage can help determine the resources that the service uses.

Avaya Breeze® platform servers calculate the current and peak usage of the following system resources on the platform. You can view the usage information on System Manager:

- CPU
- Disk
- WebSphere memory
- Cluster database connection count
- SIP sessions
- SIP request rate
- HTTP connections
- HTTP request rate

The system resource data that is collected on Avaya Breeze® platform servers is recorded in the `srdata.log` file located at `/var/log/Avaya/jboss/SessionManager`.

Related links

[Maintenance tests](#) on page 65

[Viewing the current usage of a cluster](#) on page 68

[Viewing the peak usage of a cluster](#) on page 69

[Resetting the peak usage of a cluster](#) on page 69

[System Resource Monitoring page field descriptions](#) on page 69

[Maintenance tests](#) on page 65

[Viewing the current usage of a cluster](#) on page 68

[Viewing the peak usage of a cluster](#) on page 69

[Resetting the peak usage of a cluster](#) on page 69

[System Resource Monitoring page field descriptions](#) on page 69

Viewing the current usage of a cluster

Procedure

1. In System Manager, click **Elements > Avaya Breeze® > System Tools and Monitoring > System Resource Monitor**.
2. In the **Cluster** field, select the cluster for which you want to view the current usage.
3. In the **Time Period** field, select **Today**.
4. Click **View Current Usage**.

The system displays the information in the **Current Resource Usage** table.

Related links

[System resource monitor](#) on page 67

[System resource monitor](#) on page 67

Viewing the peak usage of a cluster

Procedure

1. In System Manager, click **Elements > Avaya Breeze®**.
2. Click **System Tools And Monitoring > System Resource Monitor**.
3. In the **Cluster** field, select the cluster for which you want to view the peak usage.
4. In the **Time Period** field, select one of the following:
 - **Today**
 - **Yesterday**
 - **2 Days Ago**
 - **3 Days Ago**
 - **4 Days Ago**
 - **5 Days Ago**
 - **6 Days Ago**
5. Click **View Peak Usage**.

The system displays the information in the **Peak Resource Usage** table.

Related links

[System resource monitor](#) on page 67

[System resource monitor](#) on page 67

Resetting the peak usage of a cluster

Procedure

1. In System Manager, click **Elements > Avaya Breeze®**.

2. Click **System Tools And Monitoring > System Resource Monitor**.
3. In the **Cluster** field, select the cluster for which you want to reset the peak usage.
4. In the **Time Period** field, select **Today**.
5. Click **Reset Peak Usage**.

Related links

[System resource monitor](#) on page 67

[System resource monitor](#) on page 67

System Resource Monitoring page field descriptions

You can access the System Resource Monitoring page on System Manager by navigating to **Elements > Avaya Breeze® > System Tools and Monitoring > System Resource Monitor**. Use this page to view the current resource usage and peak usage for Avaya Breeze® platform servers in the selected cluster.

Name	Description
Cluster	The cluster for which you want to view usage details.
Time Period	The time period for which you want to view usage details.
Server Name	The name of the Avaya Breeze® platform server.
CPU % Used	The percentage of the CPU processing power that the Avaya Breeze® platform server uses.
WebSphere Memory (MB)	The WebSphere memory use information. This column displays the following information: • Used: The memory that the server uses. • Total: The total memory available to the server. • % Used: The percentage of the total memory that the server uses.
Cluster Database Connections	The status of the connection between the active server and the standby server in a high availability database scenario. •  indicates that the connection between the active and the standby servers is up. •  indicates that the standby server is getting ready to take over if the active server goes down. •  indicates that the connection between the active and standby servers is down. • No background color with the value --- indicates that the cluster database is disabled.

Table continues...

Name	Description
SIP	The details of the SIP sessions active on the server. The column displays the following information: • Sessions: The number of SIP sessions. • Request Rate
HTTP	The details of the HTTP connections active on the server. The column displays the following information: • Connections: The number of HTTP connections. • Request Rate
Disk (MB)	The disk space allocated to the server.

Button	Description
View Current Usage	Displays the current usage details for all nodes in the selected cluster. This button is disabled if the Time Period field is not set to Today .
View Peak Usage	Displays the peak usage details of the selected cluster for the specified day.
Reset Peak Usage	Resets the peak usage values to 0 for all nodes in the selected cluster. This button is disabled if the Time Period field is not set to Today .

Related links

[System resource monitor](#) on page 67

[System resource monitor](#) on page 67

Chapter 10: Maintaining and upgrading ESXi host software

This section contains notes relating to maintenance of the VMware ESXi software of the servers hosting Avaya Breeze® platform nodes. That includes upgrading the ESXi software.

Important:

- Upgrading requires a maintenance window. Consult your solution documentation for additional guidance.
- Follow the upgrade checklist for the server platform hosting ESXi:
 - **For Avaya Solutions Platform 130 Appliance:** Use the [Checklist for Avaya Solutions Platform 130 Appliance ESXi upgrades](#) on page 78.
 - **For other server platforms:** Use the [Checklist for Avaya Breeze platform ESXi host maintenance for](#) on page 75.

Related links

[Checklist for Avaya Breeze platform ESXi host maintenance for](#) on page 75

[Checklist for Avaya Solutions Platform 130 Appliance ESXi upgrades](#) on page 78

Checklist for Avaya Breeze® platform ESXi host maintenance for

- For Avaya Solutions Platform 130 Appliance, use the [Checklist for Avaya Solutions Platform 130 Appliance ESXi upgrades](#) on page 78.

#	Action	Link/Notes	✓
1.	Plan when to perform the ESXi maintenance or upgrade.	• If the ESXi server hosts all the nodes in a Breeze cluster, you must perform the maintenance during a maintenance window. • If the ESXi server is host to a single node from a multi-node Breeze cluster, you can perform the upgrade during a maintenance window or during a period of low activity. • NOTE: In some solutions with multiple Breeze clusters, nodes from different Breeze clusters can be present on the same ESXi host. For example: Nodes from Breeze cluster 1 and cluster 2 can reside on the same ESXi host. Be aware that for clusters with 2+ nodes, Breeze supports a single node failure for each cluster. Refer to solution documentation for specific recommendations regarding actions requiring a maintenance window.	
2.	Obtain the materials required for the ESXi upgrade or patch.	For an ESXi upgrade, you require: • An upgrade ESXi image. • A license for the updated version of ESXi.	
3.	Back up the cluster database.	If the cluster database is enabled, take a backup. See Backing up a cluster database on page 59.	
4.	Set the cluster or nodes affected to deny new services.	See Preparing Breeze nodes for ESXi maintenance on page 79. • Putting a Breeze node in a 2+ node cluster into deny new service can degrade overall performance as the activity load shifts to the cluster's remaining in-service nodes. Consult the solution documentation for more information. • For some solutions, a maintenance window is required, and the entire cluster must be placed in deny new service. Consult the solution documentation for more information.	

Table continues...

#	Action	Link/Notes	✓
5.	Move the nodes to another ESXi host.	If the solution supports vMotion: 1. If used, disable DRS/vSphere HA. 2. Using vMotion with high priority, move the node(s) to another available ESXi host. 3. Wait until the vMotion is complete. If the solution requires a node power down: 1. If used, disable DRS/vSphere HA. 2. Migrate the breeze node(s) to another ESXi host. 3. Wait until the migration is complete.	
6.	Perform the ESXi maintenance.	See Upgrading the ESXi host on page 80.	
7.	Add the ESXi license.	If upgrading ESXi, add a license for the updated version. See Adding the new ESXi vSphere license on page 81.	
8.	Move the nodes back to their original ESXi host.	If the solution supports vMotion: 1. Using vMotion with high priority, move the node(s) back to their original ESXi host. 2. If previously used, re-enable DRS/vSphere HA. 3. Wait until all maintenance tests pass and all services are running. See Running maintenance tests on page 66. If the solution requires a node power down: 1. Migrate the Breeze node(s) back to their previous ESXi host. 2. If previously used, re-enable DRS/vSphere HA. 3. Power on the nodes. 4. Wait until all maintenance tests pass and all services are running. See Running maintenance tests on page 66.	
9.	Set the nodes back to accept new service	• If only doing maintenance on one ESXi host: Set the node(s) back to accept new service. • If doing maintenance on multiple ESXi hosts: If required by the solution, keep the cluster in deny new service until you have completed maintenance on all ESXi hosts. See Accepting new service after ESXi maintenance on page 81.	

Table continues...

#	Action	Link/Notes	✓
10.	Reboot the Breeze cluster	Some solutions require a cluster reboot after all Breeze nodes are back online. Consult the solution documentation for more information. • This can apply even if you have only restarted one Breeze node.	
11.	Set the nodes and clusters back to accepting new services.	See Accepting new service after ESXi maintenance on page 81.	

Related links

[Maintaining and upgrading ESXi host software](#) on page 75

Checklist for Avaya Solutions Platform 130 Appliance ESXi upgrades

Use the following procedure to upgrade the Avaya Solutions Platform 130 Appliance (ASP130) from Release 4.0 (ESXi 6.5, Update 3) to Release 5.x (ESXi 7.x) that has Avaya Breeze® platform Release 3.9.x installed.

ESXi

#	Action	Link/Notes	✓
1.	Plan when to perform the Avaya Solutions Platform upgrade.	A full maintenance window is required to complete this upgrade of the ASP130.	
2.	Back up the cluster database.	If the cluster database is enabled, take a backup. See Backing up a cluster database on page 59.	
3.	Set the Breeze cluster or nodes affected to deny new services and gracefully power off each node.	See Preparing Breeze nodes for ESXi maintenance on page 79.	
4.	Upgrade the ASP130.	For the ASP130 servers, Avaya provides ESXi upgrade files and instructions which you must use. Refer to the Avaya Solutions Platform files and documentation available from https://support.avaya.com .	
5.	Power on the Breeze nodes and confirm their condition.	Power on each node using the vSphere Web Client. • Wait until all maintenance tests pass and services are running. See Running maintenance tests on page 66.	

Table continues...

#	Action	Link/Notes	✓
6.	Reboot the Breeze cluster	Some solutions require a cluster reboot after all Breeze nodes are back online. Consult the solution documentation for more information. • This can apply even if you have only restarted one Breeze node.	
7.	Set the nodes back to accept new service.	See Accepting new service after ESXi maintenance on page 81.	
8.	(Optional) If the Breeze virtual machine is not up and running.	Perform a fresh deployment of Avaya Breeze [®] platform, using the same version as installed before the Avaya Solutions Platform 130 Appliance upgrade. After Breeze initializes and completes replication: 1. Restore any required System Manager signed or third-party certificates. 2. Restore the cluster database backup taken at step 2. See Restoring the cluster database on page 60. 3. A reboot of the Breeze cluster is recommended after certification installation and cluster database restoration is complete. See Rebooting the Breeze clusters after ESXi maintenance on page 82.	

Related links

[Maintaining and upgrading ESXi host software](#) on page 75

[Preparing Breeze nodes for ESXi maintenance](#) on page 79

[Upgrading the ESXi host](#) on page 80

[Adding the new ESXi vSphere license](#) on page 81

[Accepting new service after ESXi maintenance](#) on page 81

[Rebooting the Breeze clusters after ESXi maintenance](#) on page 82

Preparing Breeze nodes for ESXi maintenance**Procedure**

1. If all the nodes in the cluster are on the ESXi host:
 - a. In System Manager, click **Elements > Avaya Breeze > Cluster Administration**.
 - b. Select the cluster.
 - c. From the **Cluster State** drop-down menu, select **Deny New Service**.
 - d. Verify that the **Cluster State** column for the cluster changes to *Denying*.
2. Otherwise, for individual Breeze nodes on the ESXi host:
 - a. In System Manager, click **Elements > Avaya Breeze > Server Administration**.
 - b. Click the checkbox in front of the server.

- c. From the **System State** drop-down menu, select **Deny New Service**.
 - d. Verify that the **System State** column for the server changes to `Denying`.
3. Shut down the nodes on the ESXi host. For each node:
 - a. In System Manager, click **Elements** > **Avaya Breeze** > **Server Administration**.
 - b. Click the checkbox in front of the server.
 - c. From the **Shutdown System** drop-down menu, select **Shutdown**.

Related links

[Checklist for Avaya Solutions Platform 130 Appliance ESXi upgrades](#) on page 78

Upgrading the ESXi host

About this task

The following is an example for upgrading a host to an updated version of ESXi using a `.iso` file burnt to DVD. However, you can use the other methods of upgraded supported by the customer's vCenter. Refer to the VMware documentation.

- For Avaya ASP130 servers, you must use the files provided by Avaya. Refer to the Avaya Solutions Platform files and documentation available from <https://support.avaya.com>.

Before you begin

1. Complete the preceding steps in the ESXi maintenance checklist. See [Checklist for Avaya Breeze platform ESXi host maintenance for](#) on page 75.
2. Burn the ESXi upgrade `.iso` file to DVD.
3. Obtain a license for the updated version of ESXi.

Procedure

1. Put the ESXi host into maintenance mode:
 - a. Open a web browser and connect to the ESXi web host client.
 - b. Login using the existing root credentials or temporary admin account if applicable.
 - c. Right-click on **Host** and select **Enter maintenance mode**.
 - d. When a `Confirm maintenance mode change` window opens, click **Yes**.
 - e. Right-click on **Host** and select **Shut down**. Your browser session ends.
2. Follow the VMware instructions for installing the new ESXi version from DVD,

Warning:

- When prompted, ensure that you select the upgrade option. Selecting any of the install options will erase the existing ESXi and all its virtual machines with no chance of recovery.
3. After the ESXi host has upgraded, take the ESXi out of maintenance mode:
 - a. Open a web browser and connect to the ESXi web host client.

- b. Login using the existing root credentials or temporary admin account if applicable.
- c. Right-click on **Host** and select **Exit maintenance mode**.

Next steps

- Complete the following steps in the ESXi maintenance checklist. See [Checklist for Avaya Breeze platform ESXi host maintenance for](#) on page 75.

Related links

[Checklist for Avaya Solutions Platform 130 Appliance ESXi upgrades](#) on page 78

Adding the new ESXi vSphere license

About this task

Upgraded ESXi servers run in evaluation mode until licensed. Before the 60-day evaluation period expires, use this process to add a vSphere license for the updated version of ESXi.

Procedure

1. Open a web browser and connect to the ESXi web host client.
2. Login using the existing root credentials or temporary admin account if applicable.
3. Open a web browser and connect to the ESXi Web host client.
4. Login using the existing root credentials or temporary admin account if applicable.
5. Navigate to **Host > Licensing > Assign license**.
6. Enter the new license and click **Check license**.
7. After the host confirms the license as valid, click **Assign license**.

Related links

[Checklist for Avaya Solutions Platform 130 Appliance ESXi upgrades](#) on page 78

Accepting new service after ESXi maintenance

About this task

After moving a node or nodes back to their original ESXi host following the hosts maintenance or upgrade, you need to set the nodes back to accepting new services.

- **If only doing maintenance on one ESXi host:**

Set the node(s) back to accept new service.

- **If doing maintenance on multiple ESXi hosts:**

If required by the solution, keep the cluster in deny new service until you have completed maintenance on all ESXi hosts.

Procedure

Set the Breeze node back into service:

- If all the nodes hosted on the ESXi server are in the same cluster:
 - a. In System Manager, click **Elements > Avaya Breeze > Cluster Administration**.
 - b. Select the cluster.
 - c. From the **Cluster State** drop-down menu, select **Accept New Service**.
 - d. Verify that the **Cluster State** column for the cluster changes to *Accepting*.
- For individual Breeze nodes hosted on the ESXi server:
 - a. In System Manager, click **Elements > Avaya Breeze > Server Administration**.
 - b. Click the checkbox in front of the server.
 - c. From the **System State** drop-down menu, select **Accept New Service**.
 - d. Verify that the **System State** column for the server changes to *Accepting*.

Related links

[Checklist for Avaya Solutions Platform 130 Appliance ESXi upgrades](#) on page 78

Rebooting the Breeze clusters after ESXi maintenance

About this task

Some solutions require a cluster reboot after all Breeze nodes are back online. Consult the solution documentation for more information.

- This can apply even if you have only restarted one Breeze node.

Procedure

1. In System Manager, click **Elements > Avaya Breeze > Cluster Administration**.
2. Select the cluster.
3. From the **Cluster State** drop-down menu, select **Deny New Service**.
4. Verify that the **Cluster State** column for the cluster changes to *Denying*.
5. Select the cluster and click **Reboot**.

Related links

[Checklist for Avaya Solutions Platform 130 Appliance ESXi upgrades](#) on page 78

Chapter 11: Avaya Breeze® platform troubleshooting

This section covers procedures that you can use to troubleshoot Avaya Breeze® platform issues such as certificate issues, database connection issues, licensing issues, and snap-in installation issues.

Related links

[Agent login on Avaya Workspaces fails intermittently](#) on page 84
[Alarms are not raised for a node](#) on page 85
[Avaya Breeze platform does not send alarms to System Manager](#) on page 85
[A snap-in gets invoked twice](#) on page 86
[Auto-switchover has occurred in a cluster database](#) on page 86
[Identity certificate change requires Avaya Breeze platform restart](#) on page 87
[Certificate expiration](#) on page 88
[Certificate status](#) on page 88
[Avaya Breeze platform instance resolution failure](#) on page 89
[Avaya Breeze platform in overload](#) on page 89
[Avaya Breeze platform not in overload](#) on page 91
[Checking the call processing status of Avaya Breeze platform](#) on page 92
[The Add participant operation in snap-ins fails while using FCLC](#) on page 92
[Troubleshooting database connection errors](#) on page 93
[Troubleshooting database errors](#) on page 94
[Database Query](#) on page 94
[Data Replication Service synchronization failure](#) on page 94
[Troubleshooting hard disk drive update errors](#) on page 96
[License errors](#) on page 97
[Troubleshooting Reliable Eventing maintenance test failures](#) on page 101
[Management Instance check failed](#) on page 102
[Troubleshooting network configuration errors](#) on page 104
[Troubleshooting network firewall critical events](#) on page 104
[Troubleshooting network firewall pinholing](#) on page 104
[Troubleshooting network firewall stoppages](#) on page 105
[Platform Application did not start](#) on page 105
[Troubleshooting Postgres database sanity check failures](#) on page 106

[Troubleshooting SAL sanity check failures](#) on page 107
[DCM sanity check failed](#) on page 109
[Maintenance test for Call Processing status fails](#) on page 109
[Secondary alarms persist](#) on page 110
[Security Module failure](#) on page 110
[Security Module Management Agent is not able to configure Security Module](#) on page 111
[Troubleshooting Avaya Breeze platform service failures](#) on page 112
[Troubleshooting SIP Entity Monitoring alarms](#) on page 112
[Snap-in installation issues](#) on page 113
[Troubleshooting Avaya Aura Media Server issues](#) on page 114
[Troubleshooting when accepting nodes are lesser than the total number of nodes in a cluster](#) on page 116
[Troubleshooting unexpected data detections](#) on page 117
[Resizing the Breeze Virtual Machine Disk on VMware](#) on page 118
[Virtual machine hangs after you reboot](#) on page 118
[Callable service gets the 404 error while trying to add a participant to a one-party call](#) on page 119
[Troubleshooting Filebeat service connection errors](#) on page 119
[traceMessage does not display the IP address of Avaya Breeze platform](#) on page 120
[CRL download fails when an HTTP proxy is configured on Avaya Breeze platform](#) on page 121
[Troubleshooting Cluster Database maintenance test failures](#) on page 121
[Cluster Database status log field descriptions](#) on page 122
[Troubleshooting certificate validation](#) on page 123
[Troubleshooting the Cluster Database status](#) on page 124

Agent login on Avaya Workspaces fails intermittently

Condition

The agent login for Avaya Workspaces fails intermittently. The cluster IP is used instead of the cluster FQDN.

Cause

The Avaya Breeze® platform authorization service tries to resolve the cluster IP configured to an FQDN. For the DNS query, if the platform operating system does not return a value or if it returns a non-authoritative answer, the IP is not resolved to an FQDN. This results in the agent login failing.

Solution

Do one of the following:

- Rectify the DNS in `/etc/resolv.conf` to point to a server where the cluster FQDN is resolvable.

- Change the order of DNS server entries in `//etc/resolv.conf` so that the first entry always returns an authoritative answer.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Alarms are not raised for a node

Condition

The Avaya Breeze® platform node does not raise alarms.

Cause

The configuration of serviceability agents is a possible cause. For more information about managing serviceability agents, see *Administering Avaya Aura® System Manager*.

Solution

1. In System Manager, click **Services > Inventory > Manage Serviceability Agents > Serviceability Agents**.
2. Reassign the SNMP user profiles and target profiles to serviceability agents.
3. Select the Avaya Breeze® platform node and click **Repair Serviceability Agent**.
4. Wait for 20 minutes.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Avaya Breeze® platform does not send alarms to System Manager

Condition

Avaya Breeze® platform does not send alarms to System Manager. Attempts to generate a test alarm from System Manager to Avaya Breeze® platform fail to display the Indeterminate test alarm.

Cause

The Avaya Breeze® platform Serviceability Agents in System Manager might not have a target profile assigned.

Solution

1. In System Manager, click **Services > Inventory > Manage Serviceability Agents > Serviceability Agents**.
2. In the **Agents List** section, verify that all Avaya Breeze® platform servers are active.

3. Select the Avaya Breeze® platform servers, and click **Manage Profiles**.
4. Click the **SNMP Target Profiles** tab.
5. In the **Assignable Profiles** section, select the target profiles to assign.
6. Click **Assign**.
7. Click **Commit** to assign the profiles to the Avaya Breeze® platform servers.
8. Generate test alarms for all Avaya Breeze® platform servers to verify that Avaya Breeze® platform servers send alarms to System Manager.
9. Verify that the test alarms are generated in System Manager.
10. Do the following to clear the alarms:
 - a. Log in to the Avaya Breeze® platform instance as an administrative user.
 - b. Run the following command: `generateTestAlarmCE.sh -c`
11. On the System Manager web console, verify that the status of the alarms changed to **Cleared**.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

A snap-in gets invoked twice

Condition

A snap-in gets invoked twice for the same call.

This issue could occur if the called endpoint rejects a SIP invite that has specified that SIPS must be used.

Solution

You can avoid an automatic re-invite from endpoints in case of SIPS rejection by configuring all the devices in your network to allow SIPS. Configure SIPS for all the devices involved in the call path up to Avaya Session Border Controller (Avaya SBC).

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Auto-switchover has occurred in a cluster database

Condition

Alarm message text Auto-switchover has occurred in a cluster database.

Alarm level Info

Cause

This alarm is an audit event that indicates that an auto-switchover between the active and standby servers has occurred. This also implies that the Avaya Breeze® platform servers are not able to connect to the cluster database active server.

The connection to the active server could be down due to a network outage, server failure, or process failure.

Solution

1. Verify whether the active server VM is running, and try to connect to the VM.
2. Verify whether the hadb service is active.
3. Verify whether the other Avaya Breeze® platform servers can reach the active server.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Identity certificate change requires Avaya Breeze® platform restart

Condition

Alarm message text A certificate change has been made that requires a restart

Alarm level Warning

Cause

Avaya Breeze® platform displays this alarm when you change or renew the identity certificate on the application server.

Solution

1. Restart the Avaya Breeze® platform server from Element Manager.
2. If the problem persists, contact Avaya Support: <https://support.avaya.com>.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Certificate expiration

Avaya Breeze® platform requires certificates for securing SIP and HTTP connections, and for communication between Avaya Breeze® platform and System Manager. If a certificate has expired, the Avaya Breeze® platform instance might not be able to establish any new connections and security may be compromised.

A warning message is logged periodically if the certificate is within 60 days of expiring.

A major alarm is logged daily if the certificate is within 30 days of expiring.

A critical alarm is generated when the certificate is within 15 days of expiring.

Important:

The Security Module only raises the critical expiration alarm when the security certificate expires. You must resolve warning expiration alarms without delay before the major and critical alarms are raised.

Install new certificates to resolve this problem. See [Administering Avaya Breeze® platform](#) for the certificate installation procedure.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Certificate status

The Security Module identity certificate and CA (trusted) certificate must be present for SIP TLS. An alarm is raised if one of the certificates cannot be loaded because it is invalid, expired, or revoked.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

[Troubleshooting certificate status alarms](#) on page 88

Troubleshooting certificate status alarms

Procedure

1. Verify that valid identity certificates are installed on the system.
2. Verify that valid CA certificates are installed on the system.
3. See [Administering Avaya Breeze® platform](#) for certificate installation information.

Related links

[Certificate status](#) on page 88

Avaya Breeze® platform instance resolution failure

This alarm occurs when the administration for the Avaya Breeze® platform instance does not match the IP address of the configured management interface.

Possible causes include:

- The IP address of the Avaya Breeze® platform instance is incorrect.
- The IP address of the Security Module was entered instead of the IP address of the Avaya Breeze® platform instance.
- The DNS name resolves to multiple IP addresses or no IP address.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

[Troubleshooting Avaya Breeze platform instance resolution failure](#) on page 89

Troubleshooting Avaya Breeze® platform instance resolution failure

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®** > **Server Administration**.
2. Select the appropriate Avaya Breeze® platform server.
3. Click **Edit**.
4. Verify whether the information is correct for the Avaya Breeze® platform server.

Related links

[Avaya Breeze platform instance resolution failure](#) on page 89

Avaya Breeze® platform in overload

About this task

The Avaya Breeze® platform generates various alarms for elevated CPU use, WebSphere memory use, or disk use on specific monitored disks. Each type of alarm has a specific alarm thresholds.

Condition and Alarm	Description
Overload Warning OVERLOAD_100004	The system generates a overload warning alarm when the warning threshold is reached and maintained for over 60 seconds.

Table continues...

Condition and Alarm	Description
Overload OVERLOAD_100001	The system generates an overload alarm when the overload threshold is reached and maintained for over 60 seconds. When an overload alarm occurs: - The server is put into Deny New Service state and prohibits new SIP and HTTP traffic to the server. - Based on the overload type, the system generates a diagnostic file or files. The system only does this first instance of the overload issue that day.
Extended Overload OVERLOAD_100003	If a CPU or memory overload extends beyond 10 minutes, or the disk usage rises to 95%, an extended overload occurs. This is indicated by an alarm. When in extended overload: - Snap-ins with multiple active sessions are removed. - You cannot deploy new snap-ins. - Snap-ins can be reinstalled by an audit after the alarm is cleared. If the audit fails to install a snap-in after three attempts, you must manually restart the Avaya Breeze® platform server to restore the service.
Overload Cleared OVERLOAD_100002	The system clears overload warning and overload alarms when all three monitored levels drop below the alarm clearing thresholds. This is indicated by an OVERLOAD_100002 alarm.

Overload type	Alarm Threshold (%)			Diagnostic file
	Overload	Warning	Clearing	
CPU	80	70	60	/var/avaya/cpuovl.<DateTime> /var/log/Avaya/sm/javacore.<DateTime>.txt
Memory	90	80	75	/var/log/Avaya/sm/heapdump.<DateTime>.phd
Disk	90	87	85	/var/avaya/diskovl.<DateTime>

! Important:

When you delete logs, ensure that you keep the latest versions of the logs.

Before you begin

Back up the old logs and trace files for debugging.

Procedure

- Using PuTTY, start an SSH session with Avaya Breeze® platform.
Log in using your customer account credentials.
- Perform the following steps to delete all Session Manager logs:
 - Use the following command to delete the logs at /var/log/Avaya/sm: **ce dlogclear**
 - Use the following command to delete the WebSphere TextLogs at /var/log/Avaya/sm: **ce logclear -a**

3. Use the following command to delete all the Java core files: `rm -rf /var/log/Avaya/sm/javacore*`
4. Use the following command to delete all WAS memory heap data: `was dump rm`
Use the `was dump ls` command to list the WAS memory heap data files.
5. Use the following commands to delete old logs and trace files:
 - `ce tlogclear`
 - `rm -rf /var/log/Avaya/trace/snapins2*`
6. Perform the following steps to delete old logs and trace files at `/var/log/Avaya/dcm/pu`:
 - a. Navigate to `/var/log/Avaya/dcm/pu`.
 - b. Use the following command to delete the files: `find <filename pattern> -mtime +<number of days> -exec rm {} \;`
7. Use the following command to delete all output files generated using the `ce-report` command in the Avaya Breeze® platform report tool: `rm -rf /var/tmp/ce-report*`
8. Perform the following steps to delete all installed snap-in logs:
 - a. Log in to System Manager.
 - b. Click **Elements** > **Avaya Breeze** > **Configuration** > **Logging**.
 - c. Select the cluster and the Avaya Breeze® platform server.
 - d. Select the snap-ins.
 - e. Click **Clear logs**.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Avaya Breeze® platform not in overload

An `OVERLOAD_100002` alarm indicates that the Avaya Breeze® platform is no longer in an overload or overload warning state. See [Avaya Breeze platform in overload](#) on page 89.

To prevent further service outages, determine the root cause of why the snap-in or the system process was utilizing the system resources.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Checking the call processing status of Avaya Breeze® platform

Procedure

1. In System Manager, click **Elements > Avaya Breeze®**.
2. Check the status for each administered Avaya Breeze® platform instance.
3. Note which Avaya Breeze® platform instances are failing tests, if any.
4. In the navigation pane, click **System Tools And Monitoring > Maintenance Tests**.
5. Select the affected Avaya Breeze® platform instance from the **Select Target** drop-down menu.
6. Select the **Test Call Processing status** test.
7. Click **Execute Selected Tests**.
8. If the test passes, clear the alarm.

Next steps

1. If the maintenance test for the Calls Processing status fails:
 - Check the network connections.
 - Check the network administration.
 - Rerun the **Test Call Processing status** test.
2. If the problem persists:
 - Troubleshoot the problem.
 - If the troubleshooting steps fail, contact Avaya Support: <https://support.avaya.com>.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

The Add participant operation in snap-ins fails while using FCLC

Cause

When Avaya Breeze® platform gets an initial invite without SDP from Communication Manager, the add participant operation in snap-ins fails. This happens only when Communication Manager is enabled with media encryption over IP.

Solution

1. Log in to the Communication Manager SAT interface.
2. Type the `change system-parameters features` command.

The system displays the FEATURE-RELATED SYSTEM PARAMETERS screen.

3. In the **Initial INVITE with SDP for secure calls** field, type `y`.

 Note:

The **Initial INVITE with SDP for secure calls** field might change in different Communication Manager releases. For more information, see *Avaya Aura® Communication Manager Screen Reference*.

4. Save the changes.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Troubleshooting database connection errors

Condition

This alarm indicates that there might be a problem with the connection to the database that contains the administration data for establishing call routes and users. The connection to the database is either disconnecting after a timeout period or is lost. During the connection failure, you cannot perform new administration tasks.

The possible causes include:

- The database might not be running.
- The connection to the database was lost or is experiencing timeouts between queries.
- The user name or password that the system uses may not match the user name or password in the database.
- The database process might not be running on the Avaya Breeze® platform instance or is on a different IP address than expected.

Solution

1. Ensure the database process is running on the Avaya Breeze® platform instance by logging on to the Avaya Breeze® platform system and running any of the following commands:
 - a. Type `statapp -s postgres-db`.
The output should be similar to `postgres-db 18/ 18 UP`.
 - b. Type `systemctl status postgres`.
The output should be similar to:
`Active: active (running) since Tue 2017-05-02 09:58:36 MDT ...`
`Main PID: 29514 (postgres)`
 - c. If none of these conditions are true, type `start -s postgres-db`.
2. Ensure there is a connection to the database. Verify that the connection is stable and is not experiencing outages

3. Ensure that the Avaya Breeze® platform instance is reachable by pinging the Avaya Breeze® platform instance from another machine that is capable of reaching the Avaya Breeze® platform instance.
4. If the problem persists, contact Avaya Support: <https://support.avaya.com>.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Troubleshooting database errors

About this task

This alarm indicates a connection or indexing error with the postgres database.

For Avaya Breeze® platform, a reinstallation might be required. For System Manager servers, a backup restoration might be required.

Procedure

Contact Avaya Support: <https://support.avaya.com>.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Database Query

This event occurs when a database query cannot complete or fails, usually after an upgrade indicating that the upgrade had problems. As a result, Avaya Breeze® platform might not operate correctly.

This event can occur if the database schemas do not match, indicating that variable types are different or fields are nonexistent.

Verify that the releases of Avaya Breeze® platform and System Manager are compatible.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Data Replication Service synchronization failure

Data Replication Service (DRS) replication error. The Avaya Breeze® platform is not synchronized with the System Manager database.

Procedure

1. In System Manager, click **Services > Replication**.
2. Select the appropriate Avaya Breeze® platform **Replica Group**.
3. Click **View Replica Nodes**.
4. Select the affected **Replica Node Host Name**.
5. Click **Repair**.
6. Resolve any inconsistencies.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

[Data Replication Service synchronization troubleshooting checklist](#) on page 95

Data Replication Service synchronization troubleshooting checklist

The following checklist provides steps to troubleshoot a Data Replication Service (DRS) synchronization error.

No.	Task	Notes	✓
1	Check if the versions of System Manager and Avaya Breeze® platform are compatible.	—	
2	Check the network connectivity between System Manager and Avaya Breeze® platform using the ping command.	• Check if any of the IPs that are assigned to System Manager or Avaya Breeze® platform are already in use by some other entity. • Check if the VM Network selected for VMs is correct. • Is the DNS able to resolve the FQDNs for both System Manager or Avaya Breeze® platform servers?	
3	Is NTP set to the same NTP server?	Check if the effective time on the Avaya Breeze® platform node is same as the time on System Manager.	

Table continues...

No.	Task	Notes	✓
4	Is trust management successful?	• If trust management is successful then log on to the Avaya Breeze® platform node and run the <code>initDRS</code> command on the command prompt. Wait for the <code>initDRS</code> command to complete before exiting. Check if the <code>initDRS</code> command completes successfully. - If the <code>initDRS</code> command completes successfully wait for a few minutes for replication to complete. - If the <code>initDRS</code> command does not complete successfully then check if the virtual FQN of System Manager has been updated. If the virtual FQN has been updated then run the <code>CEnetsetup</code> command on the Avaya Breeze® platform node again. • If trust management is not successful, run the <code>initTM</code> command. After the <code>initTM</code> completes successfully, run the <code>initDRS</code> command. If the <code>initTM</code> command does not complete successfully and contains errors, run the <code>initTM -f</code> command to reconfigure the trust settings on Avaya Breeze® platform node.	

Related links

[Data Replication Service synchronization failure](#) on page 94

Troubleshooting hard disk drive update errors

About this task

The database software cannot read or write data to the hard disk drive.

Procedure

1. Verify that sufficient space exists on the disk drive.
2. If there's not enough space on the disk drive, remove old and unnecessary files.

Next steps

If the problem persists, contact Avaya Support: <https://support.avaya.com>.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

License errors

Avaya Breeze® platform servers and some snap-ins require license files. A properly licensed Avaya Breeze® platform server or a snap-in is in the License Normal Mode. A major alarm is raised if a Avaya Breeze® platform server or a licensed snap-in has a license error. The server or the snap-in enters License Error Mode with the 30-day license grace period. While in License Error Mode, the Avaya Breeze® platform servers and the licensed snap-ins provide full functionality.

If the license error has not been corrected before the 30-day license grace expires, a critical alarm is raised and the server or the snap-in enters License Restricted Mode. In the case of an Avaya Breeze® platform server in License Restricted Mode, the server goes to the Deny New Service state. The server automatically returns to service when the license error is resolved. In the case of a snap-in in License Restricted Mode, the snap-in is uninstalled from all the clusters. You cannot reinstall the snap-in before the license error is resolved. You must manually install the snap-in after the license error is resolved, and the snap-in returns to License Normal Mode.

The possible causes of license error include:

- There is no Avaya Breeze® platform or snap-in license file installed in System Manager WebLM.
- The major release of the Avaya Breeze® platform server or the snap-in is higher than the major release specified in the license file.
- There are more Avaya Breeze® platform servers administered than allowed by the Avaya Breeze® platform license file.
- The license file of the server or the snap-in has expired.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

[Avaya Breeze platform server license file not installed](#) on page 98

[Snap-in license file is not installed](#) on page 98

[Avaya Breeze platform server software version mismatch](#) on page 98

[There is a version mismatch in the snap-in software](#) on page 99

[Insufficient Avaya Breeze platform server license capacity](#) on page 100

[Snap-in license file has expired](#) on page 100

[Avaya Breeze platform server license file has expired](#) on page 101

Avaya Breeze® platform server license file not installed

Condition

You have not installed a license file. The `debug.log` file displays the following message in the logs: *The server license file is not present. All the servers have gone to the ERROR MODE.*

Solution

Obtain and install Avaya Breeze® platform license file from PLDS.

To purchase a Avaya Breeze® platform license file, contact an Avaya sales representative or an authorized Avaya reseller.

Related links

[License errors](#) on page 97

Snap-in license file is not installed

Condition

You have not installed the snap-in license file. The `debug.log` file displays the following error message: *Snap-in license file is not present; the licensed snap-ins XXX are in ERROR MODE.*

Solution

1. In System Manager, click **Services > Licenses**.
2. In the left navigation pane, click **Products > <Snap-in license name>**.
3. Check whether a license file is present for the snap-in.

If you have not installed a license file, obtain and install the snap-in license file from PLDS.

4. To purchase a new snap-in license file, contact an Avaya sales representative or an authorized Avaya reseller.

Related links

[License errors](#) on page 97

Avaya Breeze® platform server software version mismatch

Condition

There is a version mismatch between the Avaya Breeze® platform server and the major version in the license file. The `debug.log` file displays the following error message: *The release version in the license file is not compatible with the Avaya Breeze® platform server's major release version. The Avaya Breeze® platform server goes to ERROR MODE.*

Cause

The Avaya Breeze® platform server version in the license file is not compatible with the Avaya Breeze® platform version of the server you installed.

Solution

1. On the System Manager web console, click **Services > Licenses**.

2. In the left navigation pane, click **Collaboration Environment > View License Capacity**.
3. Check the Avaya Breeze® platform software version of the license file.
4. Click **Elements > Avaya Breeze**.
5. On the Server Administration page, in the **Version** column, check the release of the server.

If this Avaya Breeze® platform software version is greater than the version specified in the license file, upgrade your license. You can also downgrade the Avaya Breeze® platform server to a version that is supported by the license file. A Avaya Breeze® platform license file with a software version N supports any dot release of version N, and any prior major release. For example N-1.

 Note:

If you are not entitled to a Avaya Breeze® platform upgrade to the higher, major release, contact an Avaya sales representative or an authorized Avaya reseller to purchase an upgrade.

Related links

[License errors](#) on page 97

There is a version mismatch in the snap-in software

Condition

There is a mismatch between the version that the snap-in license file supports and the version of the installed snap-in.

The `debug.log` file displays the following error message:

```
The snap-in version in the license file is not compatible with the major
release version of the snap-in. The licensed snap-in XXX is in the ERROR
MODE.
```

Cause

The release version that the snap-in license supports is older than the installed snap-in version.

Solution

1. In System Manager, click **Services > Licenses**.
2. In the left navigation pane, click **Products > <Snap-in license name>**.

On the snap-in license page, the header displays the snap-in release supported by the license file. The major release version of the license file must be greater than or equal to the snap-in major release version.

3. If the license file supports an older snap-in version, purchase an upgraded license file.

If you are not entitled to an upgrade to a higher, major release, contact an Avaya sales representative or an authorized Avaya reseller to purchase an upgrade. You can also downgrade the snap-in to a version that is supported by the license file.

Related links

[License errors](#) on page 97

Insufficient Avaya Breeze® platform server license capacity

Condition

The license file has insufficient capacity. The `debug.log` file displays the following error message: *VALUE_CE_SERVER license acquired failed, so <Avaya Breeze_NAME> has gone to ERROR MODE due to insufficient license.*

Cause

Your license file supports fewer Avaya Breeze® platform servers than what you have installed.

Solution

1. In System Manager, click **Services > Licenses**.
2. In the left navigation pane, click **Collaboration Environment > View License Capacity**.
3. Check the value in the **VALUE_CE_SERVER** field.
4. Click **Elements > Avaya Breeze**.
5. On the Server Administration page, check the number of servers that are administered.

The value in the **VALUE_CE_SERVER** field must be greater than or equal to the number of Avaya Breeze® platform servers administered.

If the license quantity is less than the number of Avaya Breeze® platform servers, you must either increase the license capacity, or you must delete the Avaya Breeze® platform servers above the license limit.

Note:

It is not mandatory to delete the Avaya Breeze® platform server with the license error. For example, if you have a license for one Avaya Breeze® platform server, and you have two servers administered, one of the Avaya Breeze® platform servers has the license error. You can delete either of the servers. The remaining Avaya Breeze® platform server gets the single server license and the license capacity error is cleared.

6. To purchase additional Avaya Breeze® platform licenses, contact an Avaya sales representative or an authorized Avaya reseller.

Related links

[License errors](#) on page 97

Snap-in license file has expired

Condition

The snap-in license file has expired. The `debug.log` file displays the following error message: *The FEAT_XXX_EXPIRATION snap-in license feature has expired. The licensed snap-in XXX has gone to the ERROR MODE.*

Cause

You must install another license file.

Solution

1. In System Manager, click **Services > Licenses**.
2. In the left navigation pane, click **Products > <Snap-in license name>**.
3. Check the expiration date of the license file on this page.
4. If the license file has expired, install a new license file.

To purchase a new license file, contact an Avaya sales representative or an authorized Avaya reseller.

Related links

[License errors](#) on page 97

Avaya Breeze® platform server license file has expired

Condition

The Avaya Breeze® platform server license file has expired. The `debug.log` file displays the following message: *The server license feature has expired due to the expiration of the license file. The licensed server has gone to ERROR MODE.*

Solution

1. In System Manager, click **Services > Licenses**.
2. In the left navigation pane, click **Avaya Breeze > View License Capacity**.
3. Check the expiration date of the license file on this page.

If the license file has expired, you must install a new, unexpired license file. To purchase a new license file, contact an Avaya Sales representative or an authorized Avaya reseller.

Related links

[License errors](#) on page 97

Troubleshooting Reliable Eventing maintenance test failures

Condition

The Reliable Eventing broker group cannot deliver maintenance test events.

Solution

1. In System Manager, click **Elements > Avaya Breeze®**.
2. In the navigation pane, click **System Tools And Monitoring > Maintenance Tests**.
3. From the **Select Avaya Breeze to test** drop-down list, select the affected Avaya Breeze® platform instance.
4. Select **Test Reliable Eventing Framework**.

5. Click **Execute Selected Tests**.

If the test passes, clear the alarm. The problem no longer exists and you do not need to continue with this procedure.

If the test fails, continue with this procedure and perform the following steps.

6. Go to Server Administration page and verify the following on the affected Avaya Breeze® platform node:

a. The **Security Module** is **Up**.

If the **Security Module** is not **Up**, then do the following:

- a. Establish an SSH connection to the Avaya Breeze® platform instance using either the craft login (Avaya) or an established customer login.
- b. Run the `statapp` command to verify the status of secmod.
- c. If secmod is not in service, restart the Avaya Breeze® platform server using **Shutdown System** > **Reboot** on the Avaya Breeze® platform Server Administration page.

b. The **System State** is **Accepting**.

If the **System State** is not **Accepting**, then move the node to **Accept New State** from the **System State** drop-down list.

7. Click **Reliable Eventing Administration** > **Dashboard**.

8. Click **Show Details** on each of the Reliable Eventing groups to locate the affected Avaya Breeze® platform node.

9. Once you locate the Reliable Eventing group, click the **Status** icon and examine the broker status in detail.

10. Check the network connection between the affected Avaya Breeze® platform node and the Reliable Eventing broker.

11. If the problem persists, contact Avaya Support: <https://support.avaya.com>.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Management Instance check failed

The periodic maintenance test that runs on System Manager detects connection problems with the listed Avaya Breeze® platform instance or instances.

The possible causes include:

- The management service running on the Avaya Breeze® platform server could be down.
- The network connectivity between the Avaya Breeze® platform instance and System Manager might be faulty.
- The Avaya Breeze® platform server might not be running.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

[Troubleshooting management instance check failure](#) on page 103

Troubleshooting management instance check failure**Procedure**

1. In System Manager, click **Elements** > **Avaya Breeze®**.
2. On the Avaya Breeze® platform Server Administration page, check if a Avaya Breeze® platform instance has — listed in the **Version** column instead of the correct version.

If the system displays the correct version for all the Avaya Breeze® platform instances, manually clear the alarm.
3. Establish an SSH session with the Avaya Breeze® platform instance that did not have a version displayed in the Server Administration page.
4. Check if this Avaya Breeze® platform instance is up and running.
 - If the Avaya Breeze® platform instance is down, **Power On** the Avaya Breeze® platform server.
 - If the Avaya Breeze® platform instance is running, type the **statapp** command to determine whether the management service is running. The status of the management instance should display **UP**.
5. If the application is not running, type the **start -s mgmt** command to start the management service.

Wait until the status changes to **UP**.
6. After the status of the application status is **UP**, go to the Server Administration page. Check if the page displays the version of the Avaya Breeze® platform instance.
7. If the Avaya Breeze® platform version remains unchanged, login to the System Manager shell.
8. Ping the Avaya Breeze® platform server to check if you can reach the server from System Manager.
9. If you cannot reach the Avaya Breeze® platform server from System Manager, fix the network connectivity.
10. After the network connectivity is restored, go to the Avaya Breeze® platform Server Administration page, and check if the page displays the correct Avaya Breeze® platform version.

Related links

[Management Instance check failed](#) on page 102

Troubleshooting network configuration errors

About this task

The Security Module network parameters are configured during the installation and administration. Avaya Breeze® platform raises an alarm if the Security Module is not configured or if the module is not configured correctly. This alarm indicates there might be a problem with:

- a NIC.
- the network.
- the network configuration.
- the virtual machine configuration.

Procedure

1. Check the Security Module configuration information.
2. Check if a problem exists in the network.
3. Check the network configuration information.
4. Check the virtual machine configuration information.

Next steps

If the problem persists, contact Avaya Support: <https://support.avaya.com>.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Troubleshooting network firewall critical events

This alarm indicates there is a problem with the Linux network firewall iptables.

Contact Avaya Support: <http://support.avaya.com/>.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Troubleshooting network firewall pinholing

The Security Module network firewall restricts access to all interfaces except for the interfaces and ports defined in *Avaya Breeze® platform: Port Matrix*.

You can make on-demand requests using the pinhole mechanism to open or close temporary pinholes through the network firewall.

If an application fails to open a pinhole, there might be an internal Avaya Breeze® platform problem. If the problem persists, contact Avaya Support: <https://support.avaya.com>.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Troubleshooting network firewall stoppages

This alarm indicates that the network firewall has been manually turned off.

Contact Avaya Support: <http://support.avaya.com/>.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Platform Application did not start

Condition

Platform Application does not start along with the Avaya Breeze® platform deployment.

When you deploy Avaya Breeze® platform using CLI, the system displays notification to manually run CEnetSetup to clear the issue. The system does not display this notification if you use vCenter or Solution Deployment Manager to deploy Avaya Breeze® platform.

Cause

Avaya Breeze® platform might not be able to validate the SSL certificate chain upon deployment. If Avaya Breeze® platform cannot get the SSL certificates, Platform Application does not start.

Solution

1. Log in to the Avaya Breeze® platform instance as an administrative user.
2. View `/var/log/Avaya/SMnetSetup.log` to verify the initialization errors.
Search for the Trust Management Initialization records in the log. You can view the log by using the vi editor or the `cat` command.
3. **(Optional)** View `/var/log/Avaya/mgmt/drs/symmetric.log` to verify the trust management initialization errors.

Search for the error with the following message:

```
The server does not support SSL.
```

4. Verify that System Manager is configured to support SSL.
5. If System Manager is not configured to support SSL, do the following:
 - a. Type `initTM`.

- b. Enter the System Manager enrollment password.

System Manager displays a confirmation that the Platform Application started.

6. If the manual initialization of Platform Application fails, do the following to restart Avaya Breeze® platform:
 - a. On the System Manager web console, click **Element** > **Avaya Breeze**.
 - b. From the Server Administration page, select the affected Avaya Breeze® platform server.
 - c. Click **Shutdown System** > **Reboot**.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Troubleshooting Postgres database sanity check failures

About this task

The periodic maintenance test of the Postgres database failure might indicate that the Postgres service might not be running.

To troubleshoot the database failure, you must perform the troubleshooting steps for Avaya Breeze® platform and System Manager. You must have root user privileges to perform the troubleshooting steps on System Manager.

Procedure

1. Perform the following steps for Avaya Breeze® platform:
 - a. On the System Manager **Home** page, under **Elements**, select Avaya Breeze® platform.
 - b. Select **System Tools and Monitoring** > **Maintenance Tests**.
 - c. Select the affected Avaya Breeze® platform instance from the **Select Target** list.
 - d. Select the **Test Postgres database sanity** test.
 - e. Click **Execute Selected Tests**.
 - f. If the test passes, clear the alarm. The problem no longer exists, and you do not need to continue with this procedure.
 - g. If the test fails, establish an SSH connection to the Avaya Breeze® platform instance using either the craft login (Avaya) or an established customer login.
 - h. Run the **statapp** command to verify the status of **postgres-db**.
 - i. If the status of **postgres-db** is **Down**, run the command **restart postgres-db** and wait for the Postgres service to restart.
 - j. If the status of **postgres-db** is **Partially UP**, wait for the status to change to **Up**.

- k. Run the **statapp** command to verify the status of **postgres-db**.
 - l. Run the **Test Postgres database sanity** test again.
 - m. If the test still fails, reboot the Avaya Breeze® platform server using the **Shutdown System > Reboot** option on the Avaya Breeze® platform Server Administration page.
2. Perform the following steps for System Manager:
- a. On the System Manager **Home** page, under **Elements**, select Session Manager.
 - b. Select **System Tools and Monitoring > Maintenance Tests**.
 - c. Select **System Manager** from the **Select Target** list.
 - d. Select the **Test Postgres database sanity** test.
 - e. Click **Execute Selected Tests**.
 - f. If the test passes, clear the alarm. The problem no longer exists, and you do not need to continue with this procedure.
 - g. Run the **systemctl status postgresql** command to verify the Postgres service is running.
 - h. If the Postgres service is **up**, the problem no longer exists and you do not need to continue with this procedure.
 - i. If the services is **down**, run the **systemctl restart postgresql** command.
 - j. Wait for the Postgres service to restart.
 - k. Run the **systemctl status postgresql** command to verify the Postgres service is running.
 - l. If the Postgres service is still down, check the available disk space in the /var partition.
 - m. If enough disk space exists, reboot the server.

Next steps

If the problem persists, contact Avaya Support: <https://support.avaya.com>.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Troubleshooting SAL sanity check failures

About this task

The periodic maintenance test of SAL Agent failure might indicate that the Avaya Breeze® platform alarm service might not be running.

To troubleshoot the database failure, you must perform the troubleshooting steps for Avaya Breeze® platform and System Manager. You must have root user privileges to perform the troubleshooting steps on System Manager.

Procedure

1. Perform the following steps for Avaya Breeze® platform:
 - a. On the System Manager web console, click **Elements > Avaya Breeze**.
 - b. Select **System Tools and Monitoring > Maintenance Tests**.
 - c. Select the affected Avaya Breeze® platform instance from the **Select Target** list.
 - d. Select the **Test sanity of Secure Access Link (SAL) Agent** test.
 - e. Click **Execute Selected Tests**.
 - f. If the test passes, clear the alarm. The problem no longer exists, and you do not need to continue with this procedure.
 - g. If the test fails, establish an SSH connection to the Avaya Breeze® platform instance using either the craft login (Avaya) or an established customer login.
 - h. Run the **statapp** command to verify the status of **sal-agent**.
 - i. If the status of **sal-agent** is **Down**, run **restart sal-agent** and wait for the sal-agent service to restart.
 - j. If the status of **sal-agent** is **Partially UP**, wait for the status to change to **Up**.
 - k. Run the **statapp** command to verify the status of **sal-agent**.
 - l. Run the **Test sanity of Secure Access Link (SAL) Agent** test again.
 - m. If the test still fails, reboot the Avaya Breeze® platform server using the **Shutdown System > Reboot** option on the Avaya Breeze® platform Server Administration page.
2. Perform the following steps for System Manager:
 - a. On the System Manager **Home** page, under **Elements**, select Session Manager.
 - b. Select **System Tools and Monitoring > Maintenance Tests**.
 - c. Select **System Manager** from the **Select Target** list.
 - d. Select the **Test sanity of Secure Access Link (SAL) Agent** test.
 - e. Click **Execute Selected Tests**.
 - f. If the test passes, clear the alarm. The problem no longer exists, and you do not need to continue with this procedure.
 - g. Run the **systemctl status spiritAgent** command to verify the SAL agent service is running.
 - h. If the sal-agent service is **up**, nothing further needs to be done.
 - i. If the sal-agent service is **down**, run the **service spritAgent restart** command.
 - j. Wait for the sal-agent service to restart.
 - k. Run the **systemctl status spiritAgent** command to verify the sal-agent service is running.

- I. Run the **Test sanity of Secure Access Link (SAL) Agent** test.

Next steps

If the problem persists, contact Avaya Support: <https://support.avaya.com>.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

DCM sanity check failed

Condition

Maintenance test for DCM sanity check failed.

Solution

1. Establish an SSH session with the Avaya Breeze® platform instance for which the maintenance test is failing.
2. Run the `statapp` command and verify the status of the dcm application.
3. If the status of the dcm application is DOWN then type the `start -s dcm` command to start the dcm service.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Maintenance test for Call Processing status fails

The maintenance test for Call Processing status might fail because of the following reasons:

- PfA is not deployed.
- Configuration errors while installing or upgrading the Avaya Breeze® platform server.
- WebSphere or Secmod is not running.

Solution

1. Establish an SSH session with the Avaya Breeze® platform server.
2. If the maintenance test fails after installing or upgrading the Avaya Breeze® platform server, verify the AvayaNetSetup logs for configuration-related errors.

The AvayaNetSetup logs are located at:

- Configuration information: `/var/log/Avaya/SMnetSetup.log`
- Installation summary: `/var/log/Avaya/install-summary.log`
- Upgrade summary: `/var/log/Avaya/asm-install.log`

3. Verify the status of the WebSphere and Secmod applications using the following command: **statapp**
4. If the status of the WebSphere or Secmod application is DOWN, start the service using the following command: **restart <app name>**
5. Check if PfA and the platformApp are deployed using the following command:
deploy_service -cb.
Avaya Breeze® platform displays the activity count of the services in the following format:

```
0 0 0 pfa
0 0 0 platformApp
```
6. If the troubleshooting steps fail to solve the problem, perform the configuration update procedure without changing the values using the following command: **AvayaNetSetup**
7. If performing the configuration update procedure fails to resolve the problem, download the ISO and run the following command: **upgradeCE <iso-file>**

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Secondary alarms persist

Condition

Secondary alarm persists even after Avaya Breeze® platform goes to the Normal License mode.

Cause

This issue is seen in a Geo-Redundancy set up, when the primary server goes down.

Solution

If the alarm is already raised, manually clear the alarm.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Security Module failure

Procedure

1. Verify the status of the security module:
 - a. On the System Manager web console, click **Elements > Avaya Breeze**.
 - b. Click **Server Administration**.
 - c. Verify that the status of the Avaya Breeze® platform security module is **Up**.

2. Verify that the data replication status of the Avaya Breeze® platform instance is **Synchronized**.
 - a. On the System Manager web console, click **Services > Replication**.
 - b. Verify that the **Synchronization Status** of the Avaya Breeze® platform instance is **Synchronized**.
3. Verify the status of the Avaya Breeze® platform server:
 - a. Establish an SSH session with the Avaya Breeze® platform server.
 - b. To check the status, run the following command: **statapp**
 - c. To verify the configuration, run the following command: **ceconfig**
 - d. To verify the network status, run the following command: **ifconfig**

Next steps

If all troubleshooting steps fail, restart the security module using the following command: **restart secmod**.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Security Module Management Agent is not able to configure Security Module

The management configuration of the Security Module is failing. Without the configuration, the Security Module cannot set up the network configuration for accepting SIP connections. In this case, you must restart the security module as specified in the following procedure.

About this task

If the management configuration of the security module fails, the security module cannot set up the network configuration to accept SIP connections. You must restart the security module.

Note:

The Avaya Breeze® platform server cannot process calls while you restart the security module.

Procedure

1. In System Manager, click **Elements > Avaya Breeze® > Server Administration**.
2. Verify that the status of the Avaya Breeze® platform security module is **Up**.
3. If the status of the security module is not **Up**, establish an SSH session with the Avaya Breeze® platform server.
4. Restart the security module using the following command: **restart secmod**.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Troubleshooting Avaya Breeze® platform service failures

About this task

The Avaya Breeze® platform watchdog service cannot start the service specified in the alarm message. The alarm might be temporary. If the alarm is not temporary, you might need to restart the Avaya Breeze® platform server.

Note:

The Avaya Breeze® platform instance cannot process calls during a restart operation.

Before you begin

Verify the Avaya Breeze® platform server configuration for the failed service.

Procedure

1. Establish an SSH session with the Avaya Breeze® platform server.
2. Run the following command to view the running services: **statapp**

The **statapp** command results do not display all the monitored services.
3. Using root privileges, run the following command to verify if the service is running: **/sbin/systemctl status <failed service name>**
4. If the service is not running, run the following command to start the service: **start -s <failed service name>**
5. If the problem persists, restart the Avaya Breeze® platform server.

Next steps

If restarting the Avaya Breeze® platform does not solve the issue, contact Avaya Support: <https://support.avaya.com>..

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Troubleshooting SIP Entity Monitoring alarms

About this task

The alarmed SIP entity is not successfully responding to SIP OPTIONS requests. SIP entities are reachable through multiple addresses, which depends on the Local Host Name Resolution administration and the DNS address resolution.

If the state of the entity is Down, none of the entity addresses respond to OPTIONS requests successfully. If the state of the entity is Partially Up, minimum one of the entity addresses responds successfully and minimum one address does not respond successfully.

Before you begin

Verify the details of the SIP entity, such as the status of the multiple addresses of the SIP entity and the response codes returned by the addresses. The response codes are the standard SIP responses based on RFC 3261, Section 21. View the details of the SIP entity on the SIP Entity Link Monitoring Status Summary page of System Manager at **Elements > Session Manager > System Status > SIP Entity Monitoring**.

Procedure

1. Check the network connections of the SIP entity.
2. Run the following command to check the network connection between Avaya Breeze® platform and the SIP entity: `ping`
3. Using the SIP Tracer tool or a network protocol analyzer, such as Wireshark, verify that:
 - An OPTIONS request can be sent from the Avaya Breeze® platform to the SIP entity.
 - The SIP entity send the following response: 200 OK
4. Check the Avaya Breeze® platform configuration.
5. Check the network configuration.
6. Check the local host name resolution configuration.

Next steps

If the problem persists, contact Avaya Support: <https://support.avaya.com>.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Snap-in installation issues

Verify whether you properly installed the snap-in. Try to install the snap-in again.

For more information about the snap-in installation and configuration, specifically the HelloWorld call-intercept snap-in, see:

- [Quick Start to deploying the HelloWorld Snap-in](#)
- [Deploying Avaya Breeze® platform](#)
- [Administering Avaya Breeze® platform](#)

If the problem persists, see *Avaya Breeze® platform FAQ and Troubleshooting for Snap-in Developers*.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Troubleshooting Avaya Aura® Media Server issues

To troubleshoot issues when you configure Avaya Aura® Media Server, see *Avaya Breeze® platform FAQ and Troubleshooting for Snap-in Developers*.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

[Verifying the Avaya Aura Media Server status](#) on page 114

[Media Server Monitoring page field descriptions](#) on page 115

[WebSphere generates Java core files because of connection errors with Media Server](#) on page 116

Verifying the Avaya Aura® Media Server status

About this task

Verify the status of Avaya Aura® Media Server instances using a CLI command combined with a variable. The variable can contain the full name of the Avaya Aura® Media Server instance or a pattern that matches multiple Avaya Aura® Media Server names.

You can verify the status of multiple Avaya Aura® Media Server instances using a variable pattern that matches the Avaya Aura® Media Server instance names. For example, if you type `ams`, the system displays the status of Avaya Aura® Media Server instances with the `amsToledo` and `amsLA` names.

Procedure

1. Establish an SSH connection.
2. Type the following command:

```
mscc <variable pattern that matches the Avaya Aura® Media Server names>
```

Result

The system displays the following status information of the Avaya Aura® Media Server instances

- Media Server Host Name
- Media Server
- Location
- Operation State
- Load Factor
- CPU Usage
- Detailed Result

Example

```
mscc ams
```

The system displays the status of the following Avaya Aura® Media Server instances with names that begin with the ams variable:

- amsToledo
- amsLA

Related links

[Troubleshooting Avaya Aura Media Server issues](#) on page 114

Media Server Monitoring page field descriptions

Use the Media Server Monitoring page to monitor the status of Avaya Aura® Media Server. This page displays the connection status only when Avaya Breeze® platform nodes and Avaya Aura® Media Server nodes are in the same administered location. You can access this page on System Manager by navigating to **Elements > Avaya Breeze® > System Tools and Monitoring > Media Server Monitoring**.

Name	Description
Media Server	The name of the Avaya Aura® Media Server instance.
Overload Status	The status of Avaya Aura® Media Server. This column displays: •  when Avaya Aura® Media Server is not overloaded. •  when Avaya Aura® Media Server is overloaded.
License Mode	The license mode of the Avaya Aura® Media Server instance: • licensed • unlicensed
Lock Mode	The operational state of Avaya Aura® Media Server: • locked • unlocked
Authentication	This column indicates whether Avaya Breeze® platform is able to authenticate with Avaya Aura® Media Server.
Avaya Breeze Server	The name of the Avaya Breeze® platform server. The system will not display the value for: • The Avaya Breeze® platform servers prior to Release 3.3. • The Avaya Breeze® platform servers that are not reachable.

Table continues...

Name	Description
Connection Status	The connection status of Avaya Breeze® platform with Avaya Aura® Media Server. This column displays: •  when Avaya Breeze® platform is able to connect with Avaya Aura® Media Server. •  when Avaya Breeze® platform is unable to connect with Avaya Aura® Media Server. Connection Disabled is displayed when the Select AAMS by Breeze server Location - Priority 2 cluster attribute is selected and the location of the Avaya Breeze® platform server is different than the location of Avaya Aura® Media Server.

Related links

[Troubleshooting Avaya Aura Media Server issues](#) on page 114

WebSphere generates Java core files because of connection errors with Media Server

Condition

WebSphere might generate Java core files when multiple Media Server instances that are configured with Avaya Breeze® platform have connection problems.

Cause

WebSphere generates Java core files when the thread for the health check that monitors connections to Media Server instances takes too long to complete. When there are multiple Media Server instances configured with Avaya Breeze® platform, and the connections to multiple Media Server instances have problems, the health check thread takes much longer to complete.

The connection failures might be because of problems with the enterprise network, the connection between Media Server and Avaya Breeze® platform, or configuration errors.

Solution

Resolve the connection errors between Avaya Breeze® platform and Media Server.

Related links

[Troubleshooting Avaya Aura Media Server issues](#) on page 114

Troubleshooting when accepting nodes are lesser than the total number of nodes in a cluster

Condition

Number of accepting nodes lesser than the total number of nodes available in the cluster. For example, Accepting [0/1]:

Solution

1. In System Manager, click **Elements > Avaya Breeze®**.
2. Click **Cluster Administration** and click **Show** on the cluster that displays the number of accepting nodes lesser than the total number of nodes available in the cluster.
3. Verify the state of the remaining nodes in the cluster if the remaining nodes are not under scheduled maintenance.
4. If the status displayed is --- for multiple fields on the dashboard for a given node then verify node connectivity, network connectivity and power state using vSphere. To troubleshoot these issues, see “Network configuration error”..
5. If the status displayed is --- for only the Security Module for a given node – run the maintenance tests to verify failure, check network connectivity for this interface using vSphere. To troubleshoot these issues, see “Running maintenance tests” and “Security Module failure”.
6. If the Server State is **Denying** for a particular node and the node is not undergoing scheduled maintenance, verify that all maintenance tests pass, replication is green, the data grid is up and the overload status is green before releasing into service. To troubleshoot Avaya Breeze® platform in an Overload state, see “Avaya Breeze® platform in overload”.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Troubleshooting unexpected data detections

The system detects unexpected data in the database. During this period, the invalid data will not be actualized in the running Avaya Breeze® platform .

Possible causes are:

- Administration data that was not properly checked for errors by the system.
- Incorrect data that was written directly into the database. For example, if you enter a digit pattern that is 5555 and set the minimum and maximum limits to 3. The limit must be set to at least 4.

To correct the problem:

1. Check any recent administration relating to the suggested configuration pages of the alarm.
2. If the problem persists, contact Avaya Support: <http://support.avaya.com/>.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Resizing the Breeze Virtual Machine Disk on VMware

Condition

If you increase the disk size of a powered-on Avaya Breeze® platform 3.9 virtual machine, the VM will be corrupted after the next reboot. This issue does not occur with Avaya Breeze® platform 3.8.

Solution

Ensure that the VM is powered off before you expand the disk. Ensure all snapshots are removed from the Avaya Breeze® platform VMs before the resize operation and subsequent power on.

For more information, see: <https://knowledge.broadcom.com/external/article/344854/increasing-the-disk-size-on-a-virtual-ma.html>

* Note:

PVSCSI controller allows hot extend disk from vSphere 7.0.

NVMe controller allows hot extend disk from vSphere 8.0.1.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Virtual machine hangs after you reboot

The virtual machine hangs when you start the virtual machine. The system displays an error message that a route table cannot be found.

Cause

Issues with library time synchronization causes the virtual machine to hang on initial reboot.

Solution

Rename `libtimeSync.so` to a name of your choice.

You can locate the `libtimeSync.co` file at:

- `/usr/lib/vmware-tools/plugins32/vmsvc/libtimeSync.so`
- `/usr/lib/vmware-tools/plugins64/vmsvc/libtimeSync.so`

* Note:

This action does not affect the NTP settings as NTP starts and synchronizes after the reboot.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Callable service gets the 404 error while trying to add a participant to a one-party call

Condition

A callable service gets the 404 error when sends an INVITE to Session Manager to add a participant to a one-party call. The callable service get this error because it sends the original Request URI in the INVITE.

The callable service number might be associated with a Session Manager application sequence.

Solution

Associate the callable service number with a route pattern.

The callable service number must be associated with a route pattern even if the service profile is configured with both Call Intercept and Call Services features.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Troubleshooting Filebeat service connection errors

Condition

The connection between the Filebeat service and Centralized Logging Service failed.

Cause

The Filebeat service continuously sends the logs from the configured log locations to Centralized Logging Service.

If the connection between the Filebeat service and Central Logging Service fails, the system records a connection failure error in the `filebeat.log` file. The probable causes of connection errors can be physical connection failures, TLS connection failures, or incorrect configurations in the `filebeat.yml` file.

The system raises the FILEBEATCONNECTIONERROR alarm when it detects a Filebeat service connection failure.

Solution

1. Check the Filebeat log to determine the cause of the connection failure.

The Filebeat log is located at `/var/log/Avaya/filebeat/filebeat.log` on the Avaya Breeze® platform server.

2. Check the physical connection between the Filebeat service cluster and the Centralized Logging Service cluster.

The physical connection failure can occur when the destination host is restarted or shut down.

3. Check the connection between the Filebeat service cluster and the Centralized Logging Service cluster.
 - If both the source host and the destination host are configured for secure communication, a secure TLS connection is established.
 - If both the source host and the destination host are similarly not configured for secure communication, an insecure connection is established.
 - If the source host and the destination host have different configurations, a connection is not established.

The Filebeat service tries to connect to the `logstash` destination at `/etc/filebeat/filebeat.yml`.

4. Check the Websphere certificate configuration of the destination host.

For secure communication, the Websphere certificate must have the management IP added as Subject Alternative Name (SAN).

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

traceMessage does not display the IP address of Avaya Breeze® platform

Condition

`traceMessage` displays the `/etc/profile.d/proxy.sh` file path instead of the IP address or FQDN of Avaya Breeze® platform.

Cause

The HTTP proxy exclusion list contains multiple values in `HTTP_PROXY_EXCLUSION` separated by the OR symbol (`|`). The symbol (`|`) that represents the OR symbol also represents the command line pipe symbol, so `traceMessage` does not display the IP address or FQDN of Avaya Breeze® platform.

You must manually edit the `proxy.sh` file at `/etc/profile.d/` and add double quotation marks (" ") around the value of `HTTP_PROXY_EXCLUSION` to correct the error.

Solution

1. Using PuTTY, start an SSH session with Avaya Breeze® platform.
Log in using your customer account credentials.
2. Using vi Editor, open the `proxy.sh` file at `/etc/profile.d/`.
3. Add double quotation marks (" ") around the value of `HTTP_PROXY_EXCLUSION`.
4. Save the changes in the file.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

[Tracing messages using Avaya Breeze platform traceMessage](#) on page 138

CRL download fails when an HTTP proxy is configured on Avaya Breeze® platform

Cause

When you configure an HTTP proxy in Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform, the CRL check fails. The CRL check fails because of a failure to establish a secure HTTP connection in WAS.

Solution

1. Click the following URL to download CRL manually to the local enterprise network:

<http://crl3.digicert.com/CloudFlareIncECCA2.crl>

Ensure that you can gain access to the network through System Manager.

2. Add the CRL download job in System Manager.

For more information, see *Administering Avaya Aura® System Manager* at the Avaya Support website: <https://support.avaya.com>

Avaya Breeze® platform receives the CRL file through System Manager and the CRL check successfully completes.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Troubleshooting Cluster Database maintenance test failures

Condition

The maintenance test for Cluster Database reports a node failure even though the status of the node is Green.

Solution

1. Log in to the Avaya Breeze® platform instance as an administrator.
2. Do the following to verify the connectivity to the host:
 - a. Ping virtualHaDbMaster from all the nodes in the cluster.
 - b. Ping EdpHaDbMaster from all the nodes in the cluster.
 - c. Correct all network connectivity issues.

The DNAT address of virtualHaDbMaster is 192.11.13.200. If virtualHaDbMaster or EdpHaDbMaster is unknown to the host, contact Avaya Support: <https://support.avaya.com>

3. Check the `/var/log/Avaya/sm/clusterdb.log` on all the nodes for errors.

The `/var/log/Avaya/sm/clusterdb.log` contains periodic records of the cluster database process status. Records in the log have the following format:

```
Oct 3 09:21:04 dr-dvit-cf1-mgmt root: CLUSTERDB: slave up 0 na ready 0
```

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Cluster Database status log field descriptions

Name	Description
DB role	The status of the Avaya Breeze® platform instance. The different Avaya Breeze® platform statuses indicate the following: • slave: Standby • master: Active • other: Idle
Connection status with master	The connection status of the Avaya Breeze® platform instance with the master instance. The status of all Avaya Breeze® platform instances must be up.
Number of active connections	The number of socket connections to the active cluster database. The number of connections is determined by the status of the Avaya Breeze® platform instance. If the status of an Avaya Breeze® platform instance is: • slave or other, this field displays 0. • master, this field displays the number of connections to the cluster database. If an Avaya Breeze® platform instance is connected to the cluster database, this field must not display 0.
Status with slave	This field is not used and displays NA.
HADB status	The status of the cluster database. This field displays the following based on the cluster database status: • active: Ready or Failed • standby: In-progress, Ready, or Failed

Table continues...

Name	Description
Amount of disk used in DB db directory	The total disk space that the cluster database uses. If the status of the Avaya Breeze® platform instance is: • slave or other, this field displays 0. • master, this field displays the size of the cluster database at <code>/var/avaya/hadb</code>. The size includes the disk space used by the configuration files, replication backlog, and the database.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Troubleshooting certificate validation

Starting with Avaya Breeze® platform version 3.9.0.3, hostname validation is enhanced to require Subject Alternative Name (SAN) entries in all Identity Certificates. Subject Alternative Name (SAN) entries are now mandatory in all Identity Certificates. The Common Name (CN) alone is no longer sufficient when SAN is missing. Ensure that FQDN is resolvable from all systems accessing the Avaya Breeze® platform. The OVA deployment of Avaya Breeze® platform 3.9.0.3 and higher automatically includes the minimum required SAN fields. For servers upgraded from earlier releases (for example, 3.9.0.2), the existing certificates are typically retained. In most cases, no action is required unless the existing Websphere Identity Certificate does not include Avaya Breeze® platform Management FQDN (mgmt-fqdn) and its corresponding IP address in SAN field.

If the certificate in use does not include the required SAN entries, it must be replaced using System Manager (SMGR).

To replace the certificate

1. Place the Avaya Breeze® platform cluster in the **Deny New Service** state.
2. On the System Manager web console, click **Services > Inventory**.
3. In the navigation pane, click **Manage Elements**.
4. On the **Manage Elements** page, select an element and click **More Actions > Manage Identity Certificates**.
5. On the Manage Identity Certificates page, select the **Websphere** certificate that you want to replace.
6. Click **Replace**.
7. On the Replace Identity Certificate page, select **Replace this Certificate with Internal CA Signed Certificate**.
8. Click Replace this Certificate with Internal CA Signed Certificate, and do the following:
 - a. Select the Common Name (CN) check box and type the common name that is defined in the existing certificate.

- b. Select the key algorithm and key size from the respective fields. System Manager uses the SHA2 algorithm for generating certificates.
 - c. In Subject Alternative Name, select the relevant options and enter the **Breeze Management FQDN** as **DNS Name** and its corresponding IP addresses.
 - d. To replace the identity certificate with the internal CA signed certificate, click **Commit**.
9. Repeat this process for each node in the cluster.
10. After all nodes have been updated, restart the entire Avaya Breeze® platform cluster to apply the new certificates.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Troubleshooting the Cluster Database status

Condition

The Cluster Administration page displays the cluster database status as Red, which indicates that the database failed.

Solution

1. Log in to the Avaya Breeze® platform instance as an administrator.
2. Do the following to verify the connectivity to the host:
 - a. Ping virtualHaDbMaster from all the nodes in the cluster.
 - b. Ping EdpHaDbMaster from all the nodes in the cluster.
 - c. Correct all network connectivity issues.

The DNAT address of virtualHaDbMaster is 192.11.13.200.

Contact Avaya Support: <https://support.avaya.com> if:

- virtualHaDbMaster or EdpHaDbMaster is unknown to the host.
- the cluster database status does not revert to Green.

3. Check the following logs for errors:

- `/var/log/Avaya/sm/clusterdb.log`: Contains the cluster database control, backup, and restore scripts and periodic records of the cluster database status.
- `/var/log/Avaya/db/postgresql-*.log`: Contains records of the cluster database postgres process.
- `/var/avaya/hadb/update.log` and `pgstartup.log`: Contains the update and start up records of the cluster database process.
- `/var/log/Avaya/jboss/SessionManager/hadbarbiter.log`: Contains records of the cluster database arbiter.

Related links

[Avaya Breeze platform troubleshooting](#) on page 83

Chapter 12: Avaya Breeze® platform configuration updates

Related links

[HTTP/HTTPS proxy exclusion list](#) on page 128

[Configuring Avaya Breeze platform after changing the IP address or FQDN](#) on page 128

[Changing the security module IP address](#) on page 129

[Setting the ciphers supported by a cluster](#) on page 130

Updating the Avaya Breeze® platform configuration using CEnetSetup

About this task

After you deploy Avaya Breeze® platform, if you want to change the default configuration values, use the **CEnetSetup** command.

If your Avaya Breeze® platform server is not registered in the DNS, and if you modify the host name or IP address, you must update the System Manager `/etc/hosts` file with the appropriate information.

Important:

Before you change the Avaya Breeze® platform host name or IP address using **CEnetSetup** or before you re-deploy the Avaya Breeze® platform OVA, you must remove the targeted Avaya Breeze® platform node from the cluster. For information about deploying the OVA or changing the Avaya Breeze® platform host name and IP address, see [Deploying Avaya Breeze® platform](#).

Before you begin

Connect to the host server or vCenter using the vSphere client or the vSphere web-based client.

Before you proceed with the configuration, verify each entry.

Procedure

1. Open the vSphere client in the hierarchy view.
2. Select the Avaya Breeze® platform server and click the **Console** tab in the tab view.

3. Log in to the Avaya Breeze® platform server using your credentials.
4. Type the `CEnetSetup` command.
5. On the console, enter the IP Configuration details.
Enter the Avaya Breeze® platform server host name, Avaya Breeze® platform management IP address, netmask, gateway IP address, and network domain if applicable.
6. For the DNS configuration, enter the secondary and tertiary DNS if applicable.
7. **(Optional)** If HTTP proxy configuration is required, enter `y` and then provide the HTTP proxy IP address, host name, and port details.
Otherwise, if HTTP proxy configuration is not required, enter `n`.
8. If you do not want to use the same details for the HTTPS configuration, enter the HTTPS proxy, IP address, host name, and port details.
You can configure a proxy exclusion list for HTTP and HTTPS.
9. Configure the timezone and day and time details.
10. When the system prompts you to disable NTP, enter `No`.
11. Enter the NTP server details.
Enter the secondary and tertiary NTP server details if applicable.
12. Confirm the configuration details in the Summary page before you continue.
13. When prompted, create a customer account and password.
14. Enter the primary System Manager IP address.
15. If the System Manager is unreachable, enter the following information when prompted:
 - a. If the System Manager is set up with geographic redundancy, enter `Y`.
 - b. Enter the FQDN of the primary System Manager.
 - c. Enter the IP address of the secondary System Manager, if applicable.
 - d. Enter the FQDN of the secondary System Manager, if applicable.
 - e. Enter the FQDN of the virtual System Manager.
16. Verify your settings.
17. Enter the enrollment password.
The configuration script runs automatically. The configuration takes about 10 minutes to complete. If required, the system performs an automatic reboot.

HTTP/HTTPS proxy exclusion list

You can configure a proxy exclusion list for HTTP and HTTPS. Use the proxy exclusion list to define domains, or IP addresses where outgoing HTTP requests go directly to the destination address without first going through a proxy.

For Avaya Breeze® platform, the following HTTP traffic must not go through a proxy:

- Traffic between Avaya Breeze® platform and System Manager,
- Traffic between two or more Avaya Breeze® platform nodes
- Traffic between Avaya Breeze® platform and any other Avaya Aura® server.

To add a proxy exclusion list for outgoing HTTP(S) requests, use either the OVA template during the OVA install process or the CLI **CEnetSetup** command. See [Updating the Avaya Breeze platform configuration using CEnetSetup](#) on page 126.

By default, the proxy exclusion list displays the detected local subnet configuration and the local network domain if administered through the **CEnetSetup** command. The inclusion of the local subnet on the proxy exclusion list enables the cluster data grid to bypass the routing of internal communications through a configured proxy server.

The HTTP proxy exclusion list supports both domains and IP addresses as well as wild cards. Entries in the exclusion list are separated by a | character. An example of a proxy exclusion list is 10.134.34.0/24|*.wf.aura.com.

Related links

[Avaya Breeze platform configuration updates](#) on page 126

Configuring Avaya Breeze® platform after changing the IP address or FQDN

About this task

Complete the configuration of Avaya Breeze® platform after changing the IP address or FQDN using the AvayaNetSetup or CEnetSetup scripts. Perform additional steps such as starting the WebSphere service and the trust initialization with System Manager.

Before you begin

Ensure that:

- The Avaya Breeze® platform server is running.
- All services on the Avaya Breeze® platform server are running.

Procedure

1. To verify that all services on the Avaya Breeze® platform server are running, run the **statapp** command.

2. If WebSphere is not running, run the **was start** command.
3. To start the trust initialization with System Manager, run the **initTM -f** command.
4. Add the Avaya Breeze® platform server to the cluster.
5. Import certificates to the Avaya Breeze® platform cluster.
6. If the following steps fail, restart the Avaya Breeze® platform server and cluster.
 - The trust initialization with System Manager
 - The certificate import to the Avaya Breeze® platform cluster

Related links

[Avaya Breeze platform configuration updates](#) on page 126

Changing the security module IP address

Before you begin

Get web login access to the System Manager that is managing the Avaya Breeze® platform server.

Caution:

The security module IP address must be on the same subnet as the Avaya Breeze® platform cluster IP address in support of HTTP Load Balancing, if applicable.

Note:

If you are using Session Manager Local Host Name Resolution for SIP Load Balancing or High Availability, ensure that the entry for the corresponding Avaya Breeze® platform security module IP address has been updated with the changes.

Procedure

1. Change the state of the target Avaya Breeze® platform server to **Deny New Service**.
For more information on changing the state of a cluster, see [Administering Avaya Breeze® platform](#).
2. Remove the target Avaya Breeze® platform server from the associated cluster.
3. If you want to relocate the server, do the following:
 - a. Power off the server.

Note:

Verify that all the services are removed from the server before you power off the server.
 - b. Relocate the server.
 - c. Power up the server.

4. To change the security module address of the Avaya Breeze® platform server, on the System Manager web console, click **Elements > Routing > SIP Entities**.
5. Select the appropriate Avaya Breeze® platform entity and click **Edit**.
6. In the **FQDN or IP Address** field, type the new IP address of the security module.

 Note:

This IP address is not the management address.

7. Click **Commit**.
8. To update the security module information, on the System Manager web console, click **Elements > Avaya Breeze > Server Administration**.
9. Select the Avaya Breeze® platform server and click **Edit**.
10. Edit parameters, such as Default Gateway and QoS, for the security module.
11. Click **Commit**.
12. Make the appropriate changes to the DNS server for Avaya Breeze® platform, if required.
13. On the Avaya Breeze® platform Server Administration page, ensure that the **Status** of the Avaya Breeze® platform Security Module is up.
14. Add the Avaya Breeze® platform server back to the cluster.
15. Click **System Tools and Monitoring > Maintenance Tests**.
16. In the **Select Target** field, select the Avaya Breeze® platform server.
17. Click **Execute All Tests**.
18. Click **Avaya Breeze > Server Administration**.
19. Ensure that the **Service Install Status** of the Avaya Breeze® platform server displays a green check mark. Else, wait till all the snap-ins are installed before proceeding.
20. Change the state of the Avaya Breeze® platform server to **Accept New Service**.
21. On the Confirmation page, click **Confirm**.

Related links

[Avaya Breeze platform configuration updates](#) on page 126

Setting the ciphers supported by a cluster

You can set the ciphers supported by an Avaya Breeze® platform cluster using the `asset-ciphers.sh` script. This

- To run the script, you must have root privileges.
- You must reboot the cluster after running the script.

Script options and parameters

The `asset-ciphers.sh` script can use the following options and parameters:

```
asset-ciphers [-l|--list] [-y|--yes] [-c|--set-ciphers '<new cipher string>'] [-f|--use-fips-ciphers] [-d|--use-default-ciphers]
```

where:

- `-l|--list` = List the current cipher string use for SIP(S) and HTTP(S).
- `-y|--yes` = Assume yes for service restart confirmation prompt.
- `-c|--set-ciphers` = Set the new ciphers string using the values in the parameter '`<new cipher string>`' as follows:
 - Enclose the list of ciphers in ' ' marks (single-quote marks).
 - Separate each cipher in the string with a : (colon).
 - You can prefix each cipher with one of the following:
 - `!` = Permanently deleted the cipher from the supported ciphers. You cannot re-add a permanently deleted cipher.
 - `-` = Delete the cipher from the supported ciphers. You can add the cipher again by using the cipher name with no prefix.
 - `+` = Move the cipher to the end of the supported ciphers.
 - No prefix = Add the cipher. You cannot use this to add a cipher that was permanently deleted using the `!` prefix.
- `-f|--use-fips-ciphers` = Set FIPS compliant ciphers for both FIPS & non-FIPS mode.
- `-d|--use-default-ciphers` = Set the out-of-the-box cipher string for both FIPS and non-FIPS mode.
- `-h|--help` = Show the script help.

Examples

- `asset-ciphers -c 'ALL:!aNULL:!eNULL:!ADH:!3DES:!IDEA:!SEED:!CAMELLIA:!EXP:!RC4:!KRB5:+HIGH:+MEDIUM:-LOW:-SSLv2'`
- `asset-ciphers -y -c 'FIPS:!3DES:!DSS:!kDH:!DHE:!PSK:!eNULL:!aNULL'`
- `asset-ciphers -d`
- `asset-ciphers -f -y`
- `asset-ciphers -l`

Related links

[Avaya Breeze platform configuration updates](#) on page 126

[Enabling ciphers suites in WAS](#) on page 131

Enabling ciphers suites in WAS

About this task

This task involves enabling the cipher suites in WAS

Procedure

1. Login to Avaya Breeze® platform node and su to root user.
2. Run the following command as root to enable the WebSphere Administrative Console:

```
was set console on
```
3. From a browser, navigate to the WebSphere Administrative Console: `http://<breeze-mgmt-fqdn>:9060/ibm/console`
4. Enter user ID `admin` and click on **Log in**.
5. Go to **Security > SSL certificate and key management > SSL Configuration > your node SSL configuration > Quality of protection(QoP) settings**.
6. Under **Cipher suite settings**, set **Cipher suite groups** to **Custom**
7. In the **Cipher suites** list, select the required ciphers (for example, GCM suites).
8. Click **Add >>** to move them to the **Selected ciphers** list.
9. Click **Apply**, then **Save** to apply the changes directly to the master configuration.

Note:

The property `com.ibm.websphere.tls.disabledAlgorithms` defines globally restricted algorithms and ciphers.

Even if a cipher is enabled in the SSL configuration (QoP settings), it will not be used if it matches an entry in this list. Review and adjust this property before enabling specific ciphers.

10. Run the following command using root access to turn the IBM console off:

```
was set console off
```

Related links

[Setting the ciphers supported by a cluster](#) on page 130

[Ensuring the server's cipher order is preferred during SSL negotiation](#) on page 132

[Disabling ciphers on WAS](#) on page 133

Ensuring the server's cipher order is preferred during SSL negotiation

About this task

To ensure the server's cipher order is preferred during SSL negotiation, perform the following steps.

Procedure

1. From the Console, go to **Security > Global Security > Custom properties**.
2. Click **new**.
3. Enter the name: `ibm.websphere.ssl.enforceCipherOrder` and set the value to be **true**.

4. Click **Apply**, then **Save** to apply the changes directly to the **master configuration**.

Related links

[Enabling ciphers suites in WAS](#) on page 131

Disabling ciphers on WAS

About this task

The following steps will help you to disable specific algorithms or cipher suites in WAS:

Procedure

1. Login to Avaya Breeze® platform node and su to root user.
2. Run the following command as root to enable the WebSphere Administrative Console:
`was set console on`
3. From a browser, navigate to the WebSphere Administrative Console: `http://<breeze-mgmt-fqdn>:9060/ibm/console`
4. Enter user ID `admin` and click on **Log in**.
5. **Security > Global Security > Custom properties.**
6. Locate the existing property named: `com.ibm.websphere.tls.disabledAlgorithms`
7. If the **property** exists, click the property name to edit it.
 - Update the **Value** field with a comma-separated list of algorithms or cipher suites to disable.

For example, `SSLv3, RC4, DES, MD5withRSA, DH keySize < 2048, DESede, EC keySize < 224, 3DES_EDE_CBC, anon, NULL`
8. If the **property** does not exist, click **New** and create it.
 - **Name:** `com.ibm.websphere.tls.disabledAlgorithms`
 - **Value:** `SSLv3, RC4, DES, MD5withRSA, DH keySize < 2048, DESede, EC keySize < 224, 3DES_EDE_CBC, anon, NULL`
9. Click **Apply**, then **Save** to apply the changes directly to the master configuration.
10. Restart the WebSphere Application Server or Avaya Breeze® platform node for the changes to take effect.
11. Run the following command using root access to turn the IBM console off:

`was set console off`

Related links

[Enabling ciphers suites in WAS](#) on page 131

Chapter 13: Enhanced Access Security Gateway

Avaya Breeze® platform supports Enhanced Access Security Gateway (EASG). EASG is a certificate-based, challenge-response authentication and authorization solution.

EASG provides a secure method for Avaya services personnel to:

- Access Avaya Breeze® platform remotely and onsite. As the customer, you can enable or disable access at any time.
- Perform tasks necessary for the ongoing support, management, and optimization of the solution.
- Enable remote proactive support tools such as Avaya Expert Systems® and Avaya HealthCheck.
- Perform the required maintenance tasks.

EASG only supports Avaya services logins, such as init, inads, and craft.

Related links

[EASGManage](#) on page 134

[EASGProductCert](#) on page 135

[EASGSiteCertManage](#) on page 135

[EASGStatus](#) on page 136

EASGManage

Use **EASGManage** to enable or disable the EASG authentication, check the status of EASG feature for the specified users, and display information about the available EASG users.

Syntax

```
EASGManage [--enableEASG] [--disableEASG] [--enable user] [--disable user] [--userStatus user] [--listUsers] [--printDisableWarning] [--printEnableWarning]
```

- | | |
|----------------------|---|
| --enableEASG | Enables Enhanced Access Security Gateway (EASG) authentication. |
| --disableEASG | Disables EASG authentication. |

--enable	Enables EASG authentication only for the Avaya Services logins specified in the <i>user</i> variable. If the main EASG enable/disable switch is disabled, no Avaya Services logins will have access, no matter what this setting reflects for an individual Avaya Services Login. EASG supports only Avaya services logins, such as init, inads, and craft.
--disable	Disables EASG authentication only for the Avaya Services logins specified in the <i>user</i> variable.
--userStatus	Displays the EASG status of the user specified in the <i>user</i> variable.
--listUsers	Lists the available EASG users.
--f	Forces the enable or disable action to run without prompts.
--printDisableWarning	Displays the warning message for disabling EASG on the system.
--printEnableWarning	Displays the warning message for enabling EASG on the system.

Related links

[Enhanced Access Security Gateway](#) on page 134

EASGProductCert

Use **EASGProductCert** to determine whether the EASG product certificate expires within the specified days and to check the information about the EASG product certificate.

Syntax

```
EASGProductCert [--lessThanDays number_of_days] [--certInfo]
```

--lessThanDays	Determines whether the certificate expires within the number of days indicated by <i>number_of_days</i> .
--certInfo	Displays information about the Enhanced Access Security Gateway (EASG) product certificate.

Related links

[Enhanced Access Security Gateway](#) on page 134

EASGSiteCertManage

Use **EASGSiteCertManage** to manage the Enhanced Access Security Gateway (EASG) site certificate.

Syntax

```
EASGSiteCertManage [--add pkcs7_file_path] [--saf SAF_string] [--list] [--show  
installed_pkcs7_name] [--delete installed_pkcs7_name | all]
```

- add** Adds the specified file to the site certificate repository. If you do not use the **--saf** option, the system prompts you to confirm the certificate details and enter a site authentication factor.
- saf** Provides the site authentication factor in the **--add** option, which enables the system to run the command in a noninteractive mode.
- list** Lists all the site certificates that are installed on the system.
- show** Displays information about the specified site certificate.
- delete** Deletes the specified site certificate from the system. You can use the **all** option to remove all site certificates.

Related links

[Enhanced Access Security Gateway](#) on page 134

EASGStatus

Use the **EASGStatus** command to check the status of the Enhanced Access Security Gateway (EASG) feature.

Syntax

```
EASGStatus
```

Related links

[Enhanced Access Security Gateway](#) on page 134

Chapter 14: Serviceability tools

Collecting logs using the Avaya Breeze® platform report tool

About this task

Use the Avaya Breeze® platform report tool to collect logs, configuration data, and system statistics data. You can customize the logs to include:

- Specific number of days of data to collect.
- Specific types of data.
- List of files

Procedure

1. Log in to the Avaya Breeze® platform console as a cust user.
2. Run the **ce-report** command.

Use the following options to customize the log:

- **-d**: Includes latest Java core files and WAS memory heap data.
- **-p**: Includes the performance data.
- **-n**: Generates logs at normal priority. By default, the report tool collects the logs at a lower priority. If you collect logs at a normal priority, the system performance might be impacted. Use this option only during scheduled maintenance times.
- **-c**: Specifies the number of days to collect logs. The default value is 7 days.
- **-l**: Includes the list of open files. This option might considerably increase the size of the log.
- **-b**: Includes the Avaya Breeze® platform database.
- **-s**: Includes the snap-in service logs.
- **-g**: Includes data grid logs.

Result

Avaya Breeze® platform generates the output file containing logs, configuration data, and system statistics.

Tracing messages using Avaya Breeze® platform traceMessage

About this task

Avaya Breeze® platform traceMessage supports tracing messages of multiple protocols and components. You can customize the display of the trace message results using the display filter options that traceMessage provides.

traceMessage displays a maximum of 10000 messages.

* Note:

While configuring the HTTP proxy exclusion list using CEnetSetup, if you used the OR symbol (|) to separate multiple values in HTTP_PROXY_EXCLUSION, traceMessage does not display the IP address or FQDN of Avaya Breeze® platform. You must manually edit the `proxy.sh` file at `/etc/profile.d/` and add double quotation marks (") around the value of HTTP_PROXY_EXCLUSION to correct the error.

Procedure

1. Using PuTTY, start an SSH session with Avaya Breeze® platform.
2. Run the **traceMessage** command.

Use the **traceMessage -?** command to view the optional filters to use with the command.

3. Press **s** to start the message trace.

traceMessage displays the Start Capture window.

4. Select one or more of the following options to customize the message trace:

- **SIP**
- **Media Server**
- **Breeze Platform**
- **Bus**
- **TLS handshaking**
- **HTTP**
- **Snap-Ins**

Use the arrow keys to scroll to the option and the spacebar to select the option.

5. Use the arrow keys to select **OK** to start the trace.
6. Press **s** to stop the message trace.
7. **(Optional)** Press **f** to customize the display of the message trace results.
8. Press **q** to quit Avaya Breeze® platform traceMessage.

Result

traceMessage displays the output file containing the traced messages. After you quit, traceMessage saves the file at `/var/log/Avaya/trace`.

Related links

[traceMessage does not display the IP address of Avaya Breeze platform](#) on page 120

Start Capture field descriptions

Name	Description
SIP	Captures bidirectional SIP messages exchanged between Avaya Breeze[®] platform and remote SIP entities. The captured SIP messages include: • Messages from security components, such as the SIP firewall. • Messages from users or call IDs for calls. Use the captured SIP messages to troubleshoot or monitor an Avaya Breeze[®] platform server.
Media Server	Captures Media Server HTTP messages separately from other HTTP messages. Combine the capture of Media Server HTTP messages and SIP messages to establish context for the Media Server messages for calls.
Breeze Platform	Captures the Avaya Breeze[®] platform platform messages, such as DEBUG-level trace messages for calls and HTTP requests. Combine the capture of Avaya Breeze[®] platform platform messages with the desired protocol messages, such as SIP or HTTP, to identify logic errors. traceMessage might use high CPU processing power and memory to capture the Avaya Breeze[®] platform platform messages, which might impact the performance of a busy Avaya Breeze[®] platform server.
Bus	Capture the Collaboration Bus messages of snap-ins that use Collaboration Bus. traceMessage captures the internal messages of snap-ins, such as email, SMS, and events from Collaboration Bus.
TLS handshaking	Captures the TLS handshake messages using SIP and HTTPS. Use the TLS handshake messages to identify certificate-related issues between Avaya Breeze[®] platform and Session Manager, Media Server, and snaps-in.

Table continues...

Name	Description
HTTP	Captures HTTPS requests and responses. The HTTP messages captured include: • Request and response headers • HTTP method • Response status • Upstream Avaya Breeze® platform IP address • Response time • Snap-in name
Snap-Ins	Embeds snap-in logs with the results of the traceMessage captured messages. All snap-in log levels, such as WARN, ERROR, INFO, and DEBUG, can be embedded with the captured messages. Use the combined captured messages and snap-in logs to troubleshoot snap-in problems.

Viewing the Avaya Breeze® platform traceMessage results

About this task

traceMessage saves the trace message results at `/var/log/Avaya/trace`.

You can view the trace results live during capture or view the saved file offline by using traceMessage.

Before you begin

Capture messages using Avaya Breeze® platform traceMessage.

Procedure

1. Using PuTTY, start an SSH session with Avaya Breeze® platform.
2. Run the `traceMessage <output file path and file name>` command.

For example, use the following command syntax to view specific traceMessage results of:

- SIP messages: `traceMessage /var/log/Avaya/trace/tracer_asset.log`
- SIP messages and Media Server
HTTP messages: `traceMessage /var/log/Avaya/trace/tracer_asset.log /var/log/Avaya/trace/mediaServer_http.log`

Result

traceMessage displays the output file containing the traced messages.

Chapter 15: Log files

Use **Log Viewer** for viewing audit logs, including Avaya Breeze® platform administration changes.

Related links

[Log Viewer](#) on page 141

[Avaya Breeze platform log service](#) on page 143

Log Viewer

Log Viewer displays all the logs generated by System Manager and its adopters.

The **Log List** displays a list of all the logs. You can view the details of each log, perform a search for logs, and filter specific logs. Log details include the time the log was generated, information on the severity level of the log, and the message associated with the log. You can search logs based on conditions and filters to view logs that match the filter criteria.

Log Viewer displays logs that are of type **AUDIT** only.

Note:

The viewing, filtering, and searching logs described in this section are applicable only for System Manager logs. These sections are not relevant for the service logs or for the platform logs.

Related links

[Log files](#) on page 141

[Viewing log details](#) on page 141

[Searching for logs](#) on page 142

[Filtering logs](#) on page 142

Viewing log details

Procedure

1. In System Manager, click **Services > Events > Logs**.
2. Select **Log Viewer**.
3. On the Logging page, select a log.
4. Click **View**.

Related links

[Log Viewer](#) on page 141

Searching for logs

Use the advanced search function to find logs based on specified conditions. The system displays only those logs that satisfy the search conditions. You can specify multiple search conditions.

Procedure

1. In System Manager, click **Services > Events > Logs**.
2. Click **Log Viewer**.
3. On the Logging page, click **Advanced Search**.
4. In the **Criteria** section, from the first and second drop-down fields, select the search criterion and the operator.
5. Select or enter the search value in the third field.
6. If you want to add another search condition, click the **+** sign and repeat the steps 3 and 4.
Click the **-** sign to delete a search condition. You can delete a search condition only if you added more than one search condition.
7. Select the **AND** or **OR** operator from the drop-down field.
This field appears when you specify more than one search condition.
8. Click **Search** to find the logs for the given search conditions.

Related links

[Log Viewer](#) on page 141

Filtering logs

You can filter and view logs that meet the specified filter criteria. To apply the filters, you need to specify the filter criteria in the fields provided under certain columns in the log list table . The column titles are the filter criteria. You can filter logs on multiple filter criteria.

Procedure

1. In System Manager, click **Services > Events > Logs**.
2. Click **Log Viewer**.
3. On the Logging page, click **Filter: Enable** at the top right corner of the log table.
4. Enter or select the filter criteria.
5. Click **Filter: Apply**.

The page displays the logs that match the specified filter criteria.

 **Note:**

If no records match the filter criteria, a message is displayed indicating that no records matching the search criteria are found.

Related links

[Log Viewer](#) on page 141

Avaya Breeze® platform log service

Avaya Breeze® platform provides the following log service enhancements:

- The logs for snap-ins are available in the `/var/log/Avaya/services/<ServiceName>/<ServiceName>.log` file. The log files of all the versions of the snap-in are available in the `<ServiceName>` directories. The logs are present on the Avaya Breeze® platform node and not on System Manager.
- The maximum size of the service logs is controlled by the snap-in. You can view the maximum log size for a snap-in on the Service Management page for that snap-in.
- Each log message contains the full class name from where the log was generated, the snap-in name, and the snap-in version details.
- The log files from the 3.0 version of the EmailConnector, the SMSConnector, and the ScopiaConnector use the Avaya Breeze® platform logger instead of the Avaya common logger. The connector and the mandatory services provided by Avaya Breeze® platform use the Avaya common logger.

Log levels

Avaya Breeze® platform logger provides various log levels to indicate the severity of the log messages. The following table specifies the possible log levels in Avaya Breeze® platform:

Log level	Description
Fatal	Indicates a very severe event that might cause a service to fail.
Error	Indicates a serious error, but the service might continue to function.
Warn	Indicates the possibility of a harmful problem, but the service continues to function.
Info	Indicates an information message.
Fine	Indicates a message of finer granularity than an information message.
Finer	Indicates a message of finer granularity than Fine.
Finest	Indicates a message of finest level of granularity.

Log service commands

Use the `/opt/Avaya/contrib/bin/ce` tool that is present on the Avaya Breeze® platform node, to enter commands for viewing logs and changing logs configuration. The commands have been enhanced to take a snap-in name as an argument so that the action is only on the log files of that particular snap-in. For example, `ce dlogstat <snap-in name>`.

⚠ Caution:

Use the `ce dlog` command with caution. This command is performance impacting. You must view the logs on the server if you are using the log service commands tool.

Command	Description
<code>dlogstat <snap-in name></code>	Displays the status of the log including the files and the size.
<code>dlogc <snap-in name></code>	Displays all the snap-in's log files
<code>dlogt <snap-in name></code>	Displays the reverse line snap-in's log files
<code>dlogv <snap-in name></code>	Displays the snap-in log files in the vi editor.
<code>dlogw <snap-in name></code>	Watches or tails a snap-in's log files. New contents in the log file are printed on the screen.
<code>dlogwi <snap-in name></code>	Watches or tails a snap-in's log files immediately.
<code>dlogwf <snap-in name></code>	Tails a snap-in's log file into X.log as well.
<code>dlog4j <snap-in name></code>	Displays the snap-in's log4j.properties file and the definitions of the properties.
<code>dlog4jc <snap-in name></code>	Displays the snap-in's master file, the file used after restart.
<code>dlog4jm <snap-in name></code>	Displays the snap-in's master file.
<code>dlogclear <snap-in name></code>	Clears the rolled-over logs, except the active log.
<code>dlogon <snap-in name> <arg></code>	Turns on the finest debug level for the snap-in logs. You can add the logging level as the argument. The debug level will be enabled for the log level you set.
<code>dlogoff <snap-in name> <arg></code>	Reverts to the default debug level for the snap-in logs. You can add the logging level as the argument. The debug level will be disabled for the log level you set.

Related links

[Log files](#) on page 141

[Modifying the logging configuration](#) on page 144

Modifying the logging configuration

About this task

Use the Logging Configuration page to change the logging level of an installed server on Avaya Breeze® platform servers or a cluster. You can also clear the logs for an installed service.

The log level for a snap-in does not persist when you:

- Upgrade the Avaya Breeze® platform servers on which you installed the snap-in.
- Reinstall the snap-in.

Procedure

1. On the System Manager web interface, click **Elements > Avaya Breeze® > Configuration > Logging**.

2. On the Logging Configuration page, do the following:
3. In the **Cluster** field, select the cluster to which you want to apply the log level.
4. In the **Server** field, select the server to which you want to apply the log level.
5. In the **Service** field, select the snap-in whose logging level you want to change.
6. In the **Log Level** field, select the logging level of the snap-in that you selected.
The system displays the clusters and instances where the snap-in is loaded.
7. Click **Set Log Level**.
8. To clear the logs of the selected snap-in, click **Clear Logs**.

Related links

[Avaya Breeze platform log service](#) on page 143

Chapter 16: Log retention

You can view the number of days Session Manager has been administered to retain application and system logs.

For more information, see *Administering Avaya Aura® Session Manager* and *Avaya Aura® Session Manager Data Privacy Guidelines* from the Avaya Support website at <https://support.avaya.com>.

logRetention command

The **logRetention** utility displays the currently administered log retention time.

Syntax

```
logRetention [-a] [-c] [-d] [-h -g -l -v -h | ? ]
```

- a** Displays all log retention time settings.
- c** Displays current log retention time from database.
- d** Displays default log retention time.
- g** Displays global log retention time (blank if unavailable).
- l** Displays local log retention time (blank if unavailable).
- v** Verify current log retention configuration.
- h | ?** Displays help options.

hardware_info

The **hardware_info** command is used to display the original deployment configuration and current runtime configuration information regarding resource reservations and network.

Example output

```
[cust@dr-dvit-cfl-mgmt ~]$ hardware_info  
[System Information]
```

```

Configuration: Profile 2, 4/10
Manufacturer: VMware, Inc.
Product Name: VMware7,1

[CPU Information]
CPU #0
  Model: Intel(R) Xeon(R) Gold 6226R CPU @ 2.90GHz
  MHZ: 2893.202
  Cores: 1
CPU #2
  Model: Intel(R) Xeon(R) Gold 6226R CPU @ 2.90GHz
  MHZ: 2893.202
  Cores: 1
CPU #4
  Model: Intel(R) Xeon(R) Gold 6226R CPU @ 2.90GHz
  MHZ: 2893.202
  Cores: 1
CPU #6
  Model: Intel(R) Xeon(R) Gold 6226R CPU @ 2.90GHz
  MHZ: 2893.202
  Cores: 1
CPU Reservation: 0 MHz

[Memory Information]
Total RAM: 10485760 kB
Memory Reservation: 0 MB

[Disk Information]
KNAME MOUNTPOINT TYPE FSTYPE      SIZE RO
sda      disk      55G  0
sda1  /boot/efi  part vfat      200M  0
sda2  /boot      part xfs       1G    0
sda3  [SWAP]     part swap      8G    0
sda4      part LVM2_member 45.8G  0
sr0      rom      1024M  0
dm-0  /          lvm  xfs      16.6G  0
dm-1  /tmp       lvm  xfs       4G    0
dm-2  /data      lvm  xfs       5G    0
dm-3  /var       lvm  xfs     16.1G  0
dm-4  /home      lvm  xfs       4G    0

[Network Information]
eth0:
  IPv4: 10.x.x.x
  Link detected: yes
eth1:
  IPv4: 10.x.x.x
  Link detected: yes

```

ceconfig

The **ceconfig** command is used to display Avaya Breeze® platform cluster information and certificate information.

Example output

```

[root@dr-dvit-cfl-mgmt ~]# ceconfig
postgres version is 13.22 postgresql-13.22
System Manager: 10.x.x.x (dr-dvit-smgr1.dr.avaya.com)

```

Certificates:

SIP: Using SIP CA issued certificate
HTTP: Using SIP CA issued certificate
POSTGRES: CN = dr-dvit-cf1-mgmt.dr.avaya.com, O = Avaya, C = US
CLUSTER DB: CN = dr-dvit-cf1-mgmt.dr.avaya.com, O = Avaya, C = US
MGMT: C=US, O=Avaya, CN=dr-dvit-cf1-mgmt.dr.avaya.com
SPIRIT: C=US, O=Avaya, CN=dr-dvit-cf1-mgmt.dr.avaya.com
AUTHORIZATION: C=US, O=Avaya, CN=dr-dvit-cf1-mgmt.dr.avaya.com
WEBSPPHERE: C=US, O=Avaya, CN=dr-dvit-cf1-mgmt.dr.avaya.com

Local Instance Name: dr-dvit-cf1
Local Cluster Name: Breeze 3.9.x Cluster
Local Cluster Profile: General Purpose
Local Management Host: 10.x.x.x
Local Security Module: 10.x.x.x
Local SIP State: Allow New SIP
Local FQDN: dr-dvit-cf1-mgmt.dr.avaya.com
Local Netmask: 255.x.x.x
Local Gateway: 10.x.x.x
Local Timezone: America/Denver (MST, -0700)
Local Date/Time: Thu Nov 6 18:27:31 MST 2025
Local NTP Servers: 198.x.x.x
Local DNS Servers: 198.x.x.x

Other Avaya Breeze(R) platform Servers:

ECC-EDP1 Management Host: 10.x.x.x
ECC-EDP1 Security Module: 10.x.x.x
ECC-EDP1 Cluster Name: ECC Cluster

ECC-EDP2 Management Host: 10.x.x.x
ECC-EDP2 Security Module: 10.x.x.x
ECC-EDP2 Cluster Name: ECC Cluster

dr-dvit-cf3 Management Host: 10.x.x.x
dr-dvit-cf3 Security Module: 10.x.x.x
dr-dvit-cf3 Cluster Name: Breeze 3.9.x Cluster

dr-dvit-cf2 Management Host: 10.x.x.x
dr-dvit-cf2 Security Module: 10.x.x.x
dr-dvit-cf2 Cluster Name: Breeze 3.9.x Cluster

Chapter 17: Additional information

The following resources provide additional information.

Documentation

See the following related documents at <https://support.avaya.com>. Many documents are also available at <https://documentation.avaya.com>.

Overview

Title	Use this document to:	Audience
Avaya Breeze® platform Overview and Specification	Understand the Avaya Breeze® platform, customer requirements, and design considerations.	Sales engineers Programmers System administrators Services and support personnel
<i>Avaya Aura® System Manager Overview and Specification</i>	Understand System Manager customer requirements and design considerations.	Sales engineers Programmers System administrators Services and support personnel
<i>Avaya Aura® Media Server Overview and Specification</i>	Understand Avaya Aura® Media Server customer requirements and design considerations.	Sales engineers Programmers System administrators Services and support personnel
<i>Avaya Solutions Platform 130 Overview and Specification</i>	Understand Avaya Solutions Platform 130 customer requirements and design considerations.	Sales engineers Programmers System administrators Services and support personnel

Deploying

Title	Use this document to:	Audience
Deploying Avaya Breeze® platform	Deploy and configure Avaya Breeze® platform. This is the main deployment document for Avaya Breeze® platform. The deployment documents for other environments are listed below.	Implementation engineers Support personnel System administrators
<i>Installing the Avaya Solutions Platform 130 Series 6.0.x</i>	Deploy Avaya Solutions Platform 130 Series 6.0.x.	Implementation engineers Support personnel System administrators
Deploying Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform	Deploy Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform.	Implementation engineers Support personnel System administrators
Quick Start to deploying the HelloWorld Snap-in	Install, configure, and test an Avaya Breeze® platform snap-in service, specifically the HelloWorld call intercept snap-in.	Programmers System administrators
<i>Planning for Deploying Avaya Aura® applications</i>	Understand deployment options for various Avaya Aura® applications.	Services and support personnel System administrators
<i>Deploying and Updating Avaya Aura® Media Server Appliance</i>	Deploy and configure Avaya Aura® Media Server when it is installed on customer-provided servers.	System administrators Services and support personnel
<i>Deploying Avaya Aura® System Manager in Infrastructure as a Service Environment</i>	Deploy and configure Avaya Aura® System Manager in an IaaS environment. A separate document is also available for deploying System Manager in a virtualized environment.	System administrators Services and support personnel

Administering

Title	Use this document to:	Audience
Administering Avaya Breeze® platform	Administer Avaya Breeze® platform and snap-ins.	System Administrators Services and Support personnel
<i>Implementing and Administering Avaya Aura® Media Server</i>	Deploy and configure Avaya Aura® Media Server.	System administrators Services and support personnel

Table continues...

Title	Use this document to:	Audience
<i>Administering Avaya Aura® System Manager</i>	Administer Avaya Aura® System Manager.	System Administrators Services and support personnel
<i>Administering Avaya Aura® Session Manager</i>	Administer Avaya Aura® Session Manager.	System Administrators Services and support personnel
<i>Administering Avaya Session Border Controller</i>	Administer Avaya SBC.	System Administrators Services and support personnel

Maintaining and troubleshooting

Title	Use this document to:	Audience
Upgrading Avaya Breeze® platform	Upgrade Avaya Breeze® platform.	Services and support personnel
Maintaining and Troubleshooting Avaya Breeze® platform	Troubleshoot Avaya Breeze® platform.	Services and support personnel System administrators
<i>Troubleshooting Avaya Aura® System Manager</i>	Troubleshoot System Manager.	Services and support personnel
<i>Troubleshooting Avaya Aura® Session Manager</i>	Troubleshoot Avaya Aura® Session Manager.	Services and support personnel
<i>Maintaining and Troubleshooting Avaya Solutions Platform 130 Series</i>	Troubleshoot Avaya Solutions Platform 130.	Services and support personnel

Programming

The following developer documents are available on [Avaya DevConnect](#) .

Title	Use this document to:	Audience
<i>Getting Started with the Avaya Breeze® platform SDK</i>	Deploy and configure the Eclipse IDE, Apache Maven, and the Avaya Breeze® platform SDK.	Programmers
<i>Avaya Breeze® platform Snap-in Development Guide</i>	Understand the key concepts needed to develop the different types of Avaya Breeze® platform snap-ins.	Programmers
<i>Avaya Breeze® platform FAQ and Troubleshooting for Snap-in Developers</i>	Troubleshoot Avaya Breeze® platform snap-in developer issues.	Programmers
<i>Avaya Breeze® platform API Javadocs</i>	Understand API classes and uses.	Programmers

Finding documents on the Avaya Support website

Procedure

1. Go to <https://support.avaya.com>.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support > Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.
This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.
For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click  to display the search results.

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at <https://documentation.avaya.com>. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the [Avaya Support website](#).

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.
- Click **Languages** () in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.
You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.

- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click < or > next to the document title to navigate to the previous topic or the next topic.
- Click **Share** (🔗) to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** (📁). You can add the topic and its subtopics or add the entire publication.
- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

You can do the following:

- Create, rename, and delete a collection.
- Set a collection as the default or favorite collection.
- Save a PDF of the selected content in a collection and download it to your computer.
- Share content in a collection with others through email.
- Receive collections that others have shared with you.
- Click **Watch** (👁) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

You can do the following:

- Enable **Email notifications** to receive email alerts.
- Unwatch the selected content or all topics.
- Send feedback for a topic.

Training

The following courses are available on the Avaya Learning website at <https://www.avaya-learning.com>. After logging in to the website, enter the course code or the course title in the **Search** field, and click **Go** to search for the course.

Course code	Course title
43750W	Selling Avaya Custom and Integration Solutions

Table continues...

Course code	Course title
30210W	Avaya Breeze® platform Overview for Design
30810W	Designing the Avaya Breeze® Solution Part 1 of 2
30820W	Designing the Avaya Breeze® Solution Part 2 of 2
39220W	Avaya Breeze® Release 3.8 Details for Pre-Sales
39240W	Avaya Breeze® UC Snap-ins Release 3.8 Details for Pre-Sales
2016W	Avaya Breeze® platform Fundamentals
20240W	Programming Avaya Breeze® platform Snap-ins Using Java SDK
20250W	Creating Avaya Breeze® platform Workflows Using Engagement Designer
20260W	Creating Advanced Avaya Breeze® platform Workflows Using Engagement Designer
7016W	Avaya Breeze® platform Implementation and Support
71300V	Integrating Avaya Aura® Communication Applications
72300V	Supporting Avaya Aura® Communication Applications

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to <https://support.avaya.com/> and do one of the following:
 - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Select Content Type**.
 - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select Content Type**.

The **Video** content type is displayed only when videos are available for that product.

In the right pane, the page displays a list of available videos.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
 - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
 - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

 Note:

Videos are not available for all products.

Developer resources

Avaya DevConnect provides resources for Avaya Breeze® platform developers.

You must register to access the DevConnect website.

Basic DevConnect membership is free and gives you access to the following information and resources:

- Programming and product documentation
- Sample applications
- Videos
- Webinar recordings
- Forums

Upgraded membership options offer developer-oriented technical support and other program services.

Use a browser to navigate to the Avaya Breeze® platform DevConnect website at <https://www.avaya.com/breezedevconnect>.

Support

Platform support

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

Product documentation is also available on the Avaya Documentation Center at <https://documentation.avaya.com>.

Developer support

Go to the Avaya DevConnect website at <http://www.avaya.com/breezedevconnect> to access the Avaya Breeze® platform API, SDK, sample applications, developer-oriented technical documentation, and training materials.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips.
- Information about service packs.
- Access to customer and technical documentation.
- Information about training and certification programs.
- Links to other pertinent information.

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to <https://support.avaya.com>.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support > Products**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. Select the release number, if applicable.
6. Click the **Technical Solutions** tab to view articles for resolving technical issues.

Index

Numerics

404 error	
adding participant to a call	119

A

AAMS_AUTHERROR	28
AAMS_CONFAIL	28
AAMS_LOCKED	29
AAMS_OVERLOAD	29
active server not reachable	86
add participant operation	92
alarm	
overload	89
alarm descriptions	28 , 83
OP_MMTC200[1-4][13579]	41
AAMS_AUTHERROR	28
AAMS_CONNFALL	28
AAMS_LOCKED	29
AAMS_OVERLOAD	29
ARBITER_10001	29
ARBITER_10002	29
ARBITER_10003	30
AU_GEMMTC20061	30
AuthorizationService_GENERR1	30
avCEAVDM52603	31
avCECVDM52603	31
BR_MMTC20053	31
CCLRCONNFAIL	31
CCONNFALL	32
CLR_CONERR2	32
CLR_GENERR1	32
CLR_MBCN_ERR_001	32
CLR_PBCN_ERR_001	33
CLR_SSLERR3	33
CONERR2	33
DRS_DBG_0001	34
FILEBEATCONNECTIONERROR	34
FILEBEATCONNECTIONFINE	34
MBCN_ERR_001	34
nsNotifyRestart	35
nsNotifyShutdown	35
nsNotifyStart	35
OP_AASL10900	35
OP_ANFW11001	36
OP_ANFW11002	36
OP_APLM10300	36
OP_APLM10302	36
OP_APLM10304	37
OP_AWTC10405	37
OP_AWTC10406	37
OP_CDAO50001	37

alarm descriptions (*continued*)

OP_CDAO50002	38
OP_CDAO50003	38
OP_CDAO50111	38
OP_CDAO50112	38
OP_CEMMTC20033	39
OP_CMONT55001	39
OP_CMONT55002	39
OP_GEMMTC20033	39
OP_GEMMTC20035	40
OP_GEMMTC20037	40
OP_GEMMTC20039	40
OP_MAMA20102	41
OP_MMTC20019	41
OP_MMTC20025	41
OP_MMTC20031	42
OP_MMTC20047	42
OP_MMTC20048	42
OP_MMTC20049	42
OP_MMTC20050	43
OP_MMTC20051	43
OP_MMTC20052	43
OP_MMTC20054	43
OP_MMTC20055	44
OP_MMTC20129	44
OP_MWD20202	44
OP_MWD20204	44
OP_TALM00100	45
OP_TestAlarm	45
OP_TMAG20500	45
OP_TMAG20501	46
OVERLOAD_100001	46
OVERLOAD_100002	46
OVERLOAD_100003	46
OVERLOAD_100004	47
PBCN_ERR_001	47
postgres alarms	47
SEC_000421	48
SNAPINSCRIPTFAILED	48
SSLERR3	48
UCAService_UCA_ALARM_1	49
alarms	11
alarms not sent to System Manager	85
changing status	24
exporting	23
field descriptions	24
filtering	22
generating test alarms	20
identity certificate change	87
searching for	22
system manager	12
verifying test alarms	21
viewing	21

alarms for a Breeze node	85	CLR_GENERR1	32
ARBITER_10001	29	CLR_MBCN_ERR_001	32
ARBITER_10002	29	CLR_PBCN_ERR_001	33
ARBITER_10003	30	CLR_SSLERR3	33
ASP130	78	cluster	
asset-ciphers.sh	130	restore	60
AU_GEMMTC20061	30	cluster administration	50
AuthorizationService_GENERR1	30	field descriptions	50
Auto-switchover in a cluster database	86	cluster database	
Avaya Aura® Media Server		backup	59
verifying status	114	log field descriptions	122
Avaya Breeze		troubleshooting maintenance test failures	121
insufficient license capacity	100	troubleshooting status	124
license file expired	101	cluster state	
software version mismatch	98	troubleshooting	116
Avaya Breeze 3.2		clusters	
proxy exclusion list	128	accepting nodes are lesser than the total number of	
Avaya Breeze alarms	86	nodes	116
Avaya Breeze server license file has expired	101	Collaboration Environment	
Avaya Breeze server license file not installed	98	configuring with CEnetSetup	126
Avaya Breeze server version mismatch	98	logs	143
Avaya InSite Knowledge Base	156	collecting logs	137
Avaya Media Server		collection	
troubleshooting	114	delete	152
AvayaNetSetup		edit	152
configuring after changing IP address or FQDN	128	generating PDF	152
avCEAVDM52603	31	sharing content	152
avCECVD52603	31	command	
		logRetention	146
		CONERR2	33
		configuration	
		proxy exclusion list	128
		configuring	
		after changing IP address or FQDN	128
		Avaya Breeze Serviceability Agent	18
		TrapListener service	15
		Configuring AMS	
		troubleshooting	114
		configuring asset IP	126
		Configuring the Collaboration Environment server	126
		content	
		publishing PDF output	152
		searching	152
		sharing	152
		sort by last updated	152
		watching for updates	152
		correcting IP address display errors in traceMessage	120
		CPU alarm	89
		creating	
		SNMP target profile	17
		SNMPv3 user profile	16
		CRL download fails when configuring http proxy	121
		current usage	68, 72
		D	
		Data Replication Service synchronization	
B			
backup			
cluster database	59		
BR_MMTC20053	31		
C			
CCLRCONNFAIL	31		
CCONNFAIL	32		
ceconfig	147		
CEnetSetup			
configuring after changing IP address or FQDN	128		
certificate expiration	88		
Certificate Status	88		
certificate status alarms			
troubleshooting	88		
Certificate validation	123		
changes	10		
changing alarm status	24		
changing IP address or FQDN			
configuring after changes	128		
Changing the security module IP address	129		
checklist			
DRS synchronization	95		
ESXi maintenance	75, 78		
ciphers	130		
CLR_CONERR2	32		

Data Replication Service synchronization (<i>continued</i>)	finding content on documentation center	152
troubleshooting checklist	FIPS	
database error description	ciphers	130
Database Query	FQDN change	
default SIP CA	configuring after changes	128
DevConnect	G	
disabling	generating test alarms	20
disk resize	generation of excessive Java core files troubleshooting	116
disk space alarm	Geo-Redundancy	
document changes	secondary alarms	110
documentation center	H	
finding content	hardware_info	146
navigation	http	
documentation portal	CRL download fails when configuring proxy	121
downloading	proxy exclusion list	128
SNMP MIB	https	
DRS synchronization	proxy exclusion list	128
troubleshooting checklist	I	
DRS_DBG_0001	IBM console	131
E	identity certificate change alarm	87
EASG	install status	
EASGManage	service	56
EASGProductCert	Installation issues	
EASGSiteCertManage	snap-ins	113
EASGStatus	instance resolution	
enabling	alarm troubleshooting	89
enabling WAS UI	Insufficient server license capacity	100
Enhanced Access Security Gateway	IP address change	
error	configuring after changes	128
database connection	K	
errors	KB	
troubleshooting Filebeat connection	Support site	156
ESXi	L	
license	license	
maintenance	vSphere	81
excessive Java core files troubleshooting	License errors	97
exporting alarms	license file expired	101
F	license file not available	98
failure	license file not installed	98
DCM sanity check	log collection	137
FCLC	log details; view	141
field descriptions	log files	141
alarms	log retention	146
cluster database log	log services	143
Server Administration	Log Viewer	141
Start Capture	logging configuration	144
TrapListener		
Filebeat service		
troubleshooting connection errors		
FILEBEATCONNECTIONERROR		
FILEBEATCONNECTIONFINE		
filtering alarms		
filtering logs		

logging improvements	143
logs	143
searching	142

M

maintain	
ESXI	75
VMware	75
maintenance test descriptions	65
maintenance test failure	
Reliable Eventing	101
maintenance tests	56 , 65
cluster database log field descriptions	122
on-demand	66
Reliable Eventing Framework	67
system resource monitor	67 , 71
troubleshooting cluster database status	124
troubleshooting failures in cluster database	121
Management Instance failure	102
manually clear alarms	110
MBCN_ERR_001	34
media server	
verifying status	114
Media Server Monitoring, field descriptions	115
memory alarm	89
MIB download	18

N

network configuration error	
troubleshooting	104
network firewall critical event	104
network firewall pinholing	104
network firewall stopped	105
nodes; remove	63
nsNotifyRestart	35
nsNotifyShutdown	35
nsNotifyStart	35

O

OP_AASL10900	35
OP_ANFW11001	36
OP_ANFW11002	36
OP_APLM10300	36
OP_APLM10302	36
OP_APLM10304	37
OP_AWTC10405	37
OP_AWTC10406	37
OP_CDAO50001	37
OP_CDAO50002	38
OP_CDAO50003	38
OP_CDAO50111	38
OP_CDAO50112	38
OP_CEMMTC20033	39

OP_CM0N55001	39
OP_CM0N55002	39
OP_GEMMTC20033	39
OP_GEMMTC20035	40
OP_GEMMTC20037	40
OP_GEMMTC20039	40
OP_MAMA20102	41
OP_MMTC200[1-4][13579]	41
OP_MMTC20019	41
OP_MMTC20025	41
OP_MMTC20031	42
OP_MMTC20047	42
OP_MMTC20048	42
OP_MMTC20049	42
OP_MMTC20050	43
OP_MMTC20051	43
OP_MMTC20052	43
OP_MMTC20054	43
OP_MMTC20055	44
OP_MMTC20129	44
OP_MWD20202	44
OP_MWD20204	44
OP_TALM00100	45
OP_TestAlarm	45
OP_TMAG20500	45
OP_TMAG20501	46
operations supported for alarms	
system manager	20
overload alarm	89
OVERLOAD_100001	46
OVERLOAD_100002	46
OVERLOAD_100003	46
OVERLOAD_100004	47

P

PBCN_ERR_001	47
peak usage	69 , 72
reset	69 , 72
Platform Application troubleshooting	105
postgres alarms	47
proxy exclusion list	128

R

reboot system	56
REF maintenance tests	
on-demand	67
Reliable Eventing	
maintenance test failure	101
removing a node	63
removing replica node from queue	64
repairing	
replica nodes	62
replica group; remove nodes	63
replica group; removing replica node from queue	64
replica groups; view	61

replica node		status	
repair	62	verifying for Avaya Aura® Media Server	114
report tool	137	support	155
restore	60	synchronizing System Manager master database and	
		replica computer database	62
S		system resource monitor	67 , 71
searching for alarms	22	System Resource Monitoring	
searching for content	152	field descriptions	69 , 73
searching logs	142	system state	56
SEC_000421	48		
Secondary alarms persist	110	T	
security		test alarms	
trusted certificates	56	generating	20
security certificates		verifying	21
identity certificate change alarm	87	Test Call Processing status failure troubleshooting	109
security module		trace tools	
sanity failure	111	tracing messages using traceMessage	138
sanity test failure	110	viewing traceMessage results	140
security module agent		traceMessage	
unable to configure	111	correcting IP address display errors	120
security module IP address		field descriptions	139
security module	129	tracing messages	138
server administration	50	viewing traceMessage results	140
Server Administration page description	56	tracing messages using traceMessage	138
serviceability agent	14	training	153
Serviceability Agent		TrapListener	
configuring for Avaya Breeze	18	configuring	15
serviceability tools		field descriptions	15
report tools	137	troubleshooting	83 , 123
tracing messages using traceMessage	138	404 error while trying to add a participant to a call	119
viewing traceMessage results	140	accepting nodes are lesser than the total number of	
sharing content	152	nodes	116
shutdown system	56	agent login fails intermittently	84
snap-in		alarms are not raised	85
license errors	97	alarms not sent to System Manager	85
version mismatch	99	Avaya Breeze server resolution failure	89
Snap-in installation issues	113	Breeze node does not raise alarms	85
snap-in invoked twice		certificate status alarms	88
troubleshooting	86	cluster database maintenance test failures	121
snap-in license file		cluster database status	124
expired	100	correcting IP address display errors in traceMessage	120
not installed	98	CRL download fails when configuring proxy	121
snap-in license file is not installed	98	data distribution down	92
snap-in license has expired	100	database connection error	93
snap-in software version mismatch	99	database error	94
SNAPINSCRIPTFAILED	48	DRS synchronization failure	94
SNMP MIB		Filebeat service connection errors	119
downloading	18	generation of excessive Java core files	116
SNMP support	14	hard disk drive data save error	96
SNMP target profile		identity certificate change	87
creating	17	instance resolution alarms	89
SNMPv3 user profile		management instance failure	103
creating	16	network configuration alarms	104
sort documents	152	overload condition	89
SSLERR3	48	Platform Application did not start	105
Start Capture field descriptions	139	Postgres database sanity	106

troubleshooting (<i>continued</i>)	
redundancy down	92
Reliable Eventing maintenance test failure	101
SAL Agent sanity failure	107
service has failed	112
SIP Entity Monitoring alarms	112
snap-in invoked twice	86
Test Call Processing status failure	109
troubleshooting alarms	11
Troubleshooting AMS	114
trusted certificates	56

U

UCAServic_UCA_ALARM_1	49
unexpected data	117
upgrade	
ESXi	75

V

verifying	
Avaya Aura® Media Server status	114
verifying test alarms	21
videos	154
view log details	141
view replica groups	61
viewing	
replica nodes	62
viewing alarms	21
viewing log details	141
viewing replica groups	61
viewing replica node details	63
viewing replication details for a replica node	63
viewing traceMessage results	140
Virtual Machine hangs	118
VMware	
maintenance	75
vSphere	
license	81

W

warning	
overload warning	89
watchlist	152