Deploying 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.

© 2013-2025, Avaya LLC
All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

Copyright

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

Virtualization

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

Third Party Components

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

Service Provider

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

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

Compliance with Laws

You acknowledge and agree that it is Your responsibility 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 8
Change history 8
Chapter 2: The Avaya Breeze® platform 9
Avaya Breeze® platform overview 9
Snap-in types 10
Connector snap-ins 11
Email connector 12
Scopia connector 12
Eventing Framework connector 12
Zang Call connector 13
Zang SMS connector 13
System interactions 13
Avaya Breeze® platform compatibility 14
Topology 14
Chapter 3: Deployment process checklists 15
Avaya Aura® Media Server deployment checklist 15
Avaya Breeze® platform deployment checklist 16
Chapter 4: Planning and preconfiguration 21
Deployments that require Avaya Aura® Media Server 21
Downloading software from PLDS 22
Key customer configuration information 23
Out of Band Management in Avaya Breeze® platform 27
Network latency 27
Latest software updates and patch information 28
Avaya Aura® Media Server selection algorithm 28
Running the upgradeSolution script for System Manager 29
Chapter 5: Avaya Aura® Media Server OVA deployment 31
Administering Avaya Aura® Media Server for REST 31
Assigning Avaya Aura® Media Server for use with Avaya Breeze® platform 33
Licensing the Avaya Aura® Media Server 33
Installing the Avaya Aura® Media Server license file 34
Adding the System Manager IP address 34
SIPS and SRTP on Avaya Aura® Media Server 35
Avaya Aura® Media Server host name resolution 37
Configuring Avaya Aura® Media Server name resolution (alternative 1) 37
Configuring connection security options (alternative 2) 38
Avaya Aura® Media Server trust configuration 38
Exporting an Avaya Aura® Media Server certificate 39
Enabling and configuring digit relay settings 39

Chapter 6: Deploying the Avaya Breeze® platform OVA 41
OVA deployment requirements 41
Verifying the enrollment password status 42
Deploying Avaya Breeze® platform OVA with VMware vSphere Web Client 43
Deploying Avaya Breeze® platform OVA with VMware vSphere Client connected to vCenter 45
Deploying Avaya Breeze® platform OVA with VMware vSphere Client connected to ESXi host 47
Deploying Avaya Breeze® platform OVA with Solution Deployment Manager 50
Configuring Avaya Breeze® platform after changing the IP address or FQDN 53
Changing the System Manager configuration for an Avaya Breeze® platform node 54
Configure the new server automatic startup settings 54
Configuring startup settings using the vSphere desktop client 54
Configuring startup settings using the vSphere Web Client 56
Changing the customer password on first login 56
Patching the Avaya Breeze® platform 57
Creating multiple privileged user accounts 58
Enhanced Access Security Gateway 58
Enabling and disabling EASG 59
Viewing the EASG certificate information 59
EASG site certificate 60
Chapter 7: Avaya Breeze® platform System Manager administration 61
Installing the Avaya Breeze® platform license file 61
Administering an Avaya Breeze® platform SIP Entity 62
Administering the Avaya Breeze® platform Entity Link 62
Enabling implicit users applications for SIP users 63
Administering an Avaya Breeze® platform instance 64
Enabling IPv6 on the management interface of an Avaya Breeze® platform server 65
Verifying the Avaya Breeze® platform entity link connection 67
Verifying replication status 67
Verifying the management link 68
Creating a new cluster 68
Accepting new service 71
Cluster backup and restore 71
Backing up a cluster database 72
Restoring the cluster database 73
Cancelling a pending job 73
Purging a backup 73
Reliable eventing administration 74
Creating a Reliable Eventing group 74
Editing a Reliable Eventing group 75
Deleting a Reliable Eventing group 75
Viewing the status of Reliable Eventing destinations 76
Deleting a Reliable Eventing destination 76
Running a maintenance test for a broker 76

Chapter 8: Certificate administration 78
Trust and Identity Certificate administration 78
Viewing Identity Certificate details 79
Adding a trusted certificate to all Avaya Breeze® platform servers in a cluster 80
Adding trusted CA certificates 81
Replacing an identity certificate 82
Chapter 9: Avaya Breeze® platform HA administration 84
SIP High Availability 84
Avaya Breeze® platform SIP HA deployment checklist 85
Creating an FQDN SIP entity 85
Creating an FQDN entity link 86
Creating an application and application sequence for HA 87
Determining active and standby database servers 88
Resolving the local host name for HA 88
HTTP High Availability 90
HTTP load balancing in an Avaya Breeze® platform cluster 90
Enabling HTTP load balancing in an Avaya Breeze® platform cluster 91
External load balancer for HTTP Geo-redundancy 92
Chapter 10: Communication Manager call routing 94
Routing inbound ISDN calls 94
Routing outbound ISDN calls 95
Chapter 11: FIPS configuration 96
Enabling FIPS 96
Disabling FIPS 96
Appendix A: VMware snapshots 98
VMware snapshots 98
Appendix B: Sending Avaya Breeze® platform logs to rsyslog 100
Configuring rsyslog on the Avaya Breeze® platform 100
Appendix C: Avaya Aura® Media Server configuration for Avaya Engagement Assistant Snap-in 102
Administering an Avaya Aura® Media Server SIP Entity 102
Administering the Avaya Aura® Media Server Entity Link 103
Creating the Avaya Aura® Media Server Routing Pattern 104
Verifying the Avaya Aura® Media Server Entity Link connection 105
Configuring Avaya Aura® Media Server Host Name Resolution 106
Administering Avaya Aura® Media Server URI 106
Appendix D: Additional information 108
Documentation 108
Finding documents on the Avaya Support website 110
Avaya Documentation Center navigation 111
Training 112
Viewing Avaya Mentor videos 113

Developer resources..... 113
Support..... 114
Using the Avaya InSite Knowledge Base..... 114

Chapter 1: Purpose

This document contains planning, installation, configuration, and initial administration checklists and procedures for Avaya Breeze® platform.

Administrators can use this document to install and configure a verified Avaya Breeze® platform reference configuration at a customer site.

Related links

Change history on page 8

Change history

Issue	Date	Summary of changes
1	December 2023	Updated for Avaya Breeze® platform R3.9.
2	January 2024	Added separate maximum SIP application sessions value for profile 5.
3	February 2024	Corrected the web links to other Avaya Breeze® platform documents.
4	November 2025	Updated the following sections for Release 3.9.0.3: • Avaya Aura® Media Server OVA deployment • Administering Avaya Aura® Media Server for REST • SIPS and SRTP on Avaya Aura® Media Server • Enabling and configuring digit relay settings • OVA deployment requirements • Trust and Identity Certificate administration

Chapter 2: The Avaya Breeze® platform

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.

Related links

Avaya Breeze platform overview on page 9
Snap-in types on page 10
Connector snap-ins on page 11
System interactions on page 13
Avaya Breeze platform compatibility on page 14
Topology on page 14

Avaya Breeze® platform overview

Avaya products are powered by Avaya Breeze® platform. It enables the user to do the following:

- Develop the snap-ins, without developing the platform to deploy and invoke snap-ins.
- Perform the following operations:
  - Intercept calls to and from the enterprise.
  - Redirect calls to an alternate destination.
  - Block calls and optionally play an announcement to the caller.
  - Change the caller ID of the calling or called party.
- Place an outbound call for playing announcements and collecting digits.
- Use web services for added functionality.
- Make webpages and web services available for remote browsers and applications.
- Add or replace trust and identity certificates for increased security.
- Create custom connectors that provide access to an external application or service.

Avaya Breeze® platform provides:

- Unified Communications and Contact Center customers and Business Partners the ability to deliver capabilities using the skill sets of enterprise and cloud application developers.
- A robust Software Development Kit (SDK) with an easy-to-use API. Developers need not understand the details of call processing to develop new capabilities.
- A Collaboration Bus that snap-ins can use to leverage capabilities through a point-to-point model and publish or subscribe to messaging patterns.
- A Common Data Manager framework that snap-ins can use to access common information stored on System Manager.
- Connector snap-ins that provide access to email and conferencing host applications.

  For the list of third-party developed snap-ins, go to https://www.devconnectmarketplace.com/marketplace/ and navigate to **Avaya Snapp Store**.
- Zang Call connector to interact with Avaya Communications APIs.
- Zang SMS connector for snap-ins to interact with Avaya Communications APIs to send and receive messages.
- Tools that log and monitor operations and provide troubleshooting support.

Related links

The Avaya Breeze platform on page 9

Snap-in types

For the list of third-party developed snap-ins, go to https://www.devconnectmarketplace.com/marketplace/ and navigate to **Avaya Snapp Store**.

Call Intercept snap-ins

All incoming and outgoing calls between the PSTN and the enterprise can use Call Intercept snap-ins that run on Avaya Breeze® platform. Call Intercept snap-ins can be used regardless of the type of endpoint or trunk being used, but not on station-to-station calls within the enterprise.

Call Intercept snap-ins are based on the called party or the calling party. The called party snap-in or the calling party snap-in refers to the configuration data to determine the call handling.

Hello World Snap-in that is delivered with the standard product software image is an example of a Call Intercept snap-in.

Outbound Calling snap-ins

Outbound Calling snap-ins can start calls to play prerecorded announcements and detect button presses from the called phone. Multi-channel Broadcast Snap-in is an example of an Outbound Calling snap-in.

Outbound Calling snap-ins can also start two-party calls to connect two participants in a call. The calling party is called first and after receiving an answer, a call is initiated to the called party. After the called party answers, both participants can talk to each other. The Click to Call application

that is delivered with the standard product software image is an example of a two-party Outbound Calling snap-in.

Callable snap-ins

Callable snap-ins can receive calls. For information about administering Callable snap-ins, see Administering Avaya Breeze® platform.

HTTP-invoked snap-ins

HTTP-invoked snap-ins perform an action on receipt of an incoming HTTP request. For example, when the HTTP-invoked snap-ins receive an incoming HTTP request, Dynamic Team Formation Snap-in creates a Scopia or Avaya Equinox® Conferencing video conference. The snap-in also sends the conference URL to the email and SMS recipients.

Multi-channel Broadcast Snap-in that is delivered with the standard product software image is an example of an HTTP-invoked service.

Related links

The Avaya Breeze platform on page 9

Connector snap-ins

Connector snap-ins provide access to external host applications. The built-in connector snap-ins communicate over the Collaboration bus with snap-ins that request them.

The following are connector snap-ins:

- Email connector
- Scopia connector
- Eventing Framework connector
- Zang Call connector
- Zang SMS connector

  Other vendors, such as WebText, provide similar connector snap-ins for SMS services.

Related links

The Avaya Breeze platform on page 9
Email connector on page 12
Scopia connector on page 12
Eventing Framework connector on page 12
Zang Call connector on page 13
Zang SMS connector on page 13

Email connector

Email connector enables snap-ins to send emails. It is a send-only email client that sends SMTP requests to one or more email hosts, which in turn send the email. Snap-ins use the Email API of the Collaboration bus framework to communicate with the email connector.

The Email API can handle 10000 recipients for a request, which can be a combination of primary, carbon-copy, and blind-copy recipients.

Email connector supports the following multipart body content types:

- HTML
- Plain Text
- XML
- Rich Text Format
- Vcard

Related links

Connector snap-ins on page 11

Scopia connector

The Scopia connector, which provides Avaya Equinox® Conferencing integration, uses the Conferencing API to access the Avaya Equinox® Conferencing Management Server for audio and video conferencing. The Scopia connector can schedule a conference, cancel a conference, and retrieve a list of active and scheduled conferences.

The ScopiaRequest class enables a snap-in to send and receive raw XML messages to the Conferencing server. This mode of operation works with both TE and OTT. The higher level Scheduled Conference (SchedConf) API works only in OTT mode.

Video conferences can include video participants and audio-only participants. Conference requests from the Scopia connector include the:

- Participant URL
- Host URL
- Dial-in phone number
- Meeting ID
- Host code
- Participant code

Related links

Connector snap-ins on page 11

Eventing Framework connector

Eventing Framework connector enables remote systems to publish events in the Avaya Breeze® platform Eventing Framework using REST web services. The publisher specifies the event family,

type, metadata, and message body. The Eventing Framework connector delivers the event to all subscribers and provides the easiest way to publish events to Engagement Designer workflows.

Remote applications can also subscribe to events by using the Eventing Framework connector. These applications must be able to receive the incoming HTTP POST messages when the events are generated.

Related links

Connector snap-ins on page 11

Zang Call connector

Zang Call connector facilitates communication between Avaya Communications APIs and Avaya Breeze® platform using HTTPS.

Related links

Connector snap-ins on page 11

Zang SMS connector

For information about the Zang SMS connector, see Deploying Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform and *Zang SMS connector Snap-in Reference*.

Related links

Connector snap-ins on page 11

System interactions

For information about Avaya product compatibility, see https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml.

Traditional H.248 gateways provide access to the PSTN and support for H.323 and legacy endpoints. Connection to SIP service provider trunks is provided through Avaya SBC to Session Manager.

Snap-ins

Avaya Breeze® platform snap-ins interoperate with other Avaya products. For example, WebRTC Connect interoperates with Avaya SBC.

Conferencing API

Avaya Equinox® Conferencing and the Avaya Breeze® platform Scheduled Conference API support Over-the -Top (OTT) Conferencing configurations. The Avaya Breeze® platform API to Conferencing is the same API as the Scopia API.

Related links

The Avaya Breeze platform on page 9

Avaya Breeze® platform compatibility

You can deploy Avaya Breeze® platform with the latest System Manager R10.1.2.x (Avaya Breeze® platform 3.9.0.0 only), R10.1.3.x or R10.2.

For information about Avaya product compatibility, see https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml.

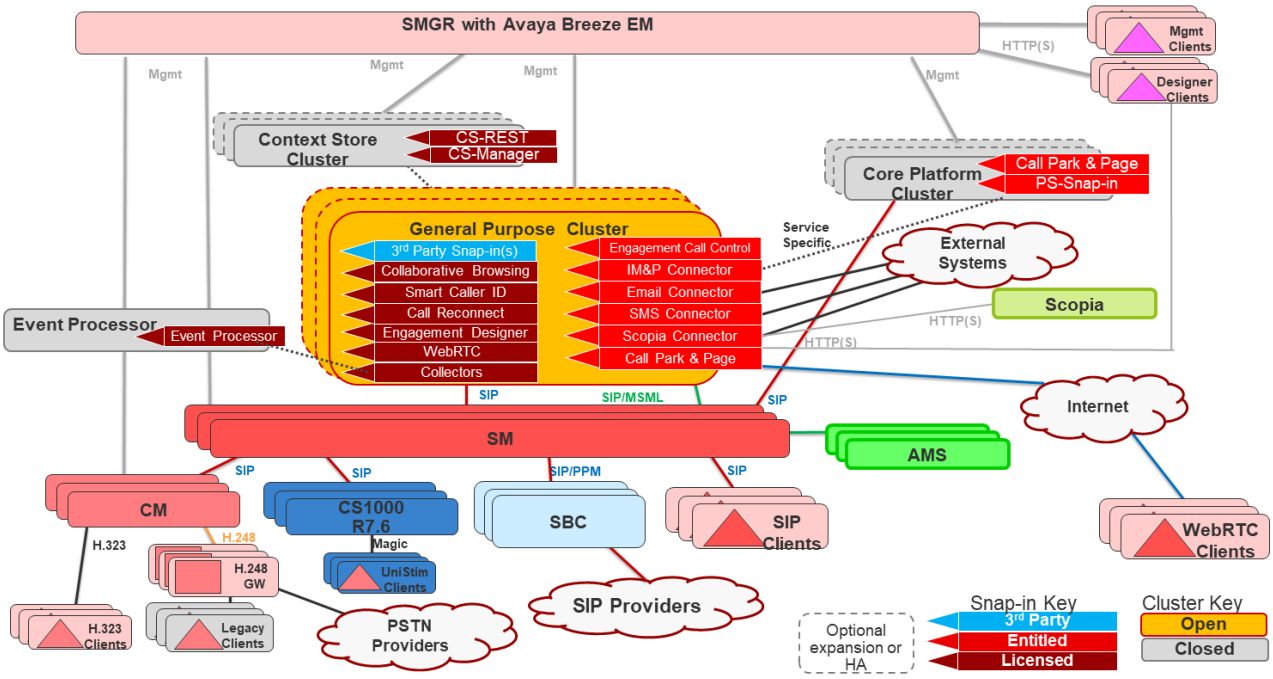
System Manager	Notes
pre-R10.13.6	• Install the latest Avaya Breeze® platform 3.9.0.x Element Manager that is approved for the corresponding platform release by using the `upgradeSolution` utility available in Avaya Aura® System Manager.

Related links

The Avaya Breeze platform on page 9

Topology

The following diagram provides a high-level illustration of the components of an Avaya Breeze® platform solution:



Related links

The Avaya Breeze platform on page 9

Chapter 3: Deployment process checklists

Use the following checklists to guide the Avaya Breeze® platform deployment process.

Related links

Avaya Aura Media Server deployment checklist on page 15
Avaya Breeze platform deployment checklist on page 16

Avaya Aura® Media Server deployment checklist

The following table lists the procedures for deploying Avaya Aura® Media Server. If you are using Avaya Aura® Media Server, deploy it before Avaya Breeze® platform.

#	Action	Reference/Notes	✔
1.	Determine whether you need to deploy Avaya Aura® Media Server.	See Deployments that require Avaya Aura Media Server on page 21	
2.	Download software from PLDS. Download the Avaya Aura® Media Server license file from PLDS.	See Downloading software from PLDS on page 22	
3.	Deploy the Avaya Aura® Media Server OVA.	See *Deploying and Updating Avaya Aura® Media Server Appliance*.	
4.	Configure virtual machine automatic startup settings.	See Configuring startup settings using the vSphere desktop client on page 54	
5.	License the Avaya Aura® Media Server.	See Licensing the Avaya Aura Media Server on page 33 and Installing the Avaya Aura Media Server license file on page 34	

Table continues…

#	Action	Reference/Notes	✔
6.	Enroll Avaya Aura® Media Server on System Manager. Before enrolling, follow the pre-enrollment checklist in *Implementing and Administering Avaya Aura® Media Server*.	See the “System Manager enrollment” section in *Implementing and Administering Avaya Aura® Media Server*. During enrollment: • The element and cluster names must not contain the following special characters: "[^<>\\^%$@*#]*"). • The Avaya Aura® Media Server FQDN and the System Manager FQDN must be registered in DNS or must have an entry in `/etc/hosts`. • System Manager and Avaya Aura® Media Server need to be on the same domain.	
7.	Administer Avaya Aura® Media Server for REST.	See Administering Avaya Aura Media Server for REST on page 31	
8.	Assign Avaya Aura® Media Server for use with Avaya Breeze® platform.	See Assigning Avaya Aura Media Server for use with Avaya Breeze platform on page 33	
9.	Create a new certificate on Avaya Aura® Media Server, or import an existing certificate to establish a trust relationship with Avaya Breeze® platform.	For more information, see “Security Configuration” in *Implementing and Administering Avaya Aura® Media Server*.	
10.	Add the System Manager IP address.	See Adding the System Manager IP address on page 34	
11.	Configure name resolution.	See Avaya Aura Media Server host name resolution on page 37	
12.	Configure MRCP server on Avaya Aura® Media Server to support Automatic Speech Recognition (ASR) and to stream Text-To-Speech (TTS).	See *Implementing and Administering Avaya Aura® Media Server*.	

Related links

Deployment process checklists on page 15

Avaya Breeze® platform deployment checklist

The following table lists the procedures required to deploy Avaya Breeze® platform.

#	Action	Reference/Notes	✔
1.	Record information that you will require for the deployment.	See Key customer configuration information on page 23	
2.	Install or upgrade System Manager if required and download the latest System Manager hot fix.	You can use System Manager Release 10.1.2 or later. See Avaya Breeze platform compatibility on page 14 **Note:** Avaya Breeze® platform 3.9 and later releases require Avaya Aura® System Manager 10.1.2 or later, with higher Breeze patch versions requiring later System Manager updates. Refer to the corresponding Breeze Release Notes for version-specific System Manager requirements.	
3.	Download Avaya Breeze® platform software and license files from PLDS. Download patch files (if required) from PLDS.	See Downloading software from PLDS on page 22	
4.	Verify that the enrollment password is not expired.	See Verifying the enrollment password status on page 42	

Table continues…

#	Action	Reference/Notes	✔
5.	Deploy the Avaya Breeze® platform OVA. Choose the procedure that corresponds to your OVA deployment method. • Deploying Avaya Breeze platform OVA with VMware vSphere Web Client on page 43 • Deploying Avaya Breeze platform OVA with VMware vSphere Client connected to vCenter on page 45 • Deploying Avaya Breeze platform OVA with VMware vSphere Client connected to ESXi host on page 47 • Deploying Avaya Breeze platform OVA with Solution Deployment Manager on page 50	The Avaya Breeze® platform management FQDN assigned to the management network interface must be registered in DNS. For assistance, contact Avaya Support. **Important:** • Avoid installing multiple OVAs on the same LAN simultaneously unless you are using VCenter or Solution Deployment Manager for the installation. If you install an OVA with vSphere, it boots with a static, fixed IP address associated with eth0. If you load a second OVA on the same network before running CEnetSetup on the first, an address conflict occurs. One or both VMs will not be configurable. • The Avaya Breeze® platform node where Engagement Designer is installed and System Manager must be in the same domain.	
6.	Change the customer password on first login.	See Changing the customer password on first login on page 56	
7.	Configure virtual machine automatic startup settings.	See Configure the new server automatic startup settings on page 54	
8.	Install the patch file.	See Patching the Avaya Breeze platform on page 57	
9.	Create multiple privileged user accounts (optional).	See Creating multiple privileged user accounts on page 58	
10.	Install the Avaya Breeze® platform license file.	See Installing the Avaya Breeze platform license file on page 61	
11.	Administer the SIP entity.	See Administering an Avaya Breeze platform SIP Entity on page 62	
12.	Administer the SIP entity link.	See Administering the Avaya Breeze platform Entity Link on page 62	
13.	Enable implicit user applications for SIP users.	See Enabling implicit users applications for SIP users on page 63	

Table continues…

#	Action	Reference/Notes	✔
14.	Administer the Avaya Breeze® platform instance.	See Administering an Avaya Breeze platform instance on page 64	
15.	Verify the entity link connection.	See Verifying the Avaya Breeze platform entity link connection on page 67	
16.	Verify the replication status.	See Verifying replication status on page 67	
17.	Verify the management link.	See Verifying the management link on page 68	
18.	Assign the server to an Avaya Breeze® platform cluster. If one does not already exist for this server, create the cluster.	See Creating a new cluster on page 68	
19.	Add a trust certificate to all servers.	See Adding a trusted certificate to all Avaya Breeze platform servers in a cluster on page 80	
20.	Add individual trust certificates.	See Adding trusted CA certificates on page 81	
21.	Replace an identity certificate.	See Replacing an identity certificate on page 82	
22.	Change the state of the server to accept new service.	See Accepting new service on page 71	
23.	Configure the alarming setup. Configure System Manager to receive Avaya Breeze® platform alarms.	See SNMP support information in Maintaining and Troubleshooting Avaya Breeze® platform.	
24.	If you have cluster databases enabled, set up scheduled backups for the cluster database.	See Administering Avaya Breeze® platform.	
25.	For Communication Manager, route inbound ISDN calls.	See Routing inbound ISDN calls on page 94	
26.	For Communication Manager, route outbound ISDN calls.	See Routing outbound ISDN calls on page 95	
27.	Enable FIPS (optional).	FIPS is a cryptographic security standard. If FIPS is not already enabled by default for your deployment, you can enable it manually. For more information, see Enabling FIPS on page 96. If you want to disable FIPS when you no longer need it, see Disabling FIPS on page 96.	

Related links

Deployment process checklists on page 15

Chapter 4: Planning and preconfiguration

The following sections cover planning and preconfiguration for Avaya Breeze® platform deployment.

Related links

Deployments that require Avaya Aura Media Server on page 21
Downloading software from PLDS on page 22
Key customer configuration information on page 23
Out of Band Management in Avaya Breeze platform on page 27
Network latency on page 27
Latest software updates and patch information on page 28
Avaya Aura Media Server selection algorithm on page 28
Running the upgradeSolution script for System Manager on page 29

Deployments that require Avaya Aura® Media Server

Use the following guidelines to determine whether you need to deploy Avaya Aura® Media Server. These sections are intended for guidance only, and do not provide an exhaustive list of every scenario that requires Avaya Aura® Media Server.

When you need Avaya Aura® Media Server

You need Avaya Aura® Media Server in the following scenarios:

- With Avaya Workplace Attendant
- With Park and Page
- When using WebRTC with Avaya Oceana®
- When media operations, such as “play announcement” or “play and collect”, are involved in snap-ins

When you do not need Avaya Aura® Media Server

You do *not* need Avaya Aura® Media Server with the following:

- Avaya Oceana® unless you have WebRTC
- Presence Services
- Avaya Device Adapter
- Engagement Call Control

- Whitelist
- Dynamic Team Formation
- Smart Caller ID

Related links

Planning and preconfiguration on page 21
Avaya Aura Media Server deployment checklist on page 15
Avaya Aura Media Server selection algorithm on page 28

Downloading software from PLDS

About this task

Before starting the deployment process, download software and license files from PLDS.

Procedure

1. Enter http://plds.avaya.com in your web browser to access the Avaya PLDS website.
2. Enter your login ID and password.
3. On the PLDS Home page, click **Assets**.
4. Click **View Downloads**.
5. If you are a customer, skip this step.
   a. In the **%Name** field, either enter `Avaya` or your Partner company name.
   b. Click **Apply Company**.
6. Click the **Search by Download** tab.
7. Enter any information specific to the download, or leave the fields blank to view all downloads.
8. Click **Search Downloads**.
9. Locate the appropriate download.
10. Click the **Download** link in the left-most column of the download row.
11. In the Download Manager dialog box, click the appropriate download link.

    Note:

    The first link, **Click to download your file now**, uses Download Manager to download the file. Download Manager provides features to manage the download, such as stop, resume, and auto checksum. The **click here** link uses your standard browser download and does not provide the download integrity features.
12. If you receive an error message, click the **install ActiveX** message at the top of the page and continue with the download.

13. Select the location where you want to save the file and click **Save**.
14. **(Optional)** If you used Download Manager, click **Details** to view the download progress.

Related links

Planning and preconfiguration on page 21

Key customer configuration information

You require the following information to install and configure Avaya Breeze® platform. Have this information before you begin the installation.

Network Settings

Field	Information to enter	Notes
IP Address	Enter the server's IPv4 address.	Management IP address to be assigned to Avaya Breeze® platform.
Short Hostname	Enter the server's host name.	The hostname must match the one for the server that is being upgraded.
Network Domain	Enter the network domain.	The network domain must match the one for the server that is being upgraded.
Netmask	Enter IPv4 netmask information.	—
Default gateway	Enter the IP address for the IPv4 gateway.	Default IPv4 gateway for Avaya Breeze® platform management network interface.
IPv6 Address	(Optional) Enter the IPv6 address for the management interface.	Set the **IPv6 Address**, **IPv6 Prefix**, and **IPv6 Gateway** to prepopulate the IPv6 address on the management (eth0) interface. The IPV4 fields are required even if administering IPv6 addresses.
IPv6 Prefix	(Optional) Enter the IPv6 prefix for the management interface.	The IPv4 **Netmask** is still required.
IPv6 Gateway	(Optional) Enter the IPv6 gateway for the management interface.	The IPv6 gateway address that can route the IPv6 addresses. The **Default gateway** IPv4 address is still required.
DNS servers	Enter the primary, secondary, and tertiary DNS server IP address.	You can have up to three DNS servers. Avaya recommends provisioning at least two DNS servers that are resilient in case of power or network failure.
Cluster IP address	Enter a unique IP address.	This value is required after deployment.

Proxy settings

Field	Information to enter
HTTP Proxy Server	Enter the IP address or FQDN of the HTTP proxy server.
HTTP Proxy Port	Enter the HTTP proxy port.
HTTPS Proxy Server	Enter the IP address or FQDN of the HTTPS proxy server.
HTTPS Proxy Port	Enter the HTTPS proxy port.
HTTP Proxy exclusion list	Enter the HTTPS proxy servers with a delimiter of "|". For example: `*ca.avaya.com|*.us.avaya.com|135.9.95.*` By default, the customer domain will be added to the proxy exclusion list. The proxy exclusion list can be added with the **`CEnetSetup`** command or using the OVA properties during deployment. If the destination for the HTTP request matches any address in the exclusion list, the HTTP request will be sent directly to the destination instead of the proxy.

System Time Settings

Field	Information to enter	Notes
Timezone	Select the timezone from this field.	This configuration is mandatory for Avaya Breeze® platform to function. The timezone configured on Avaya Breeze® platform must match the timezone on System Manager.
NTP Servers	Enter the IP address or FQDN of the primary NTP server.	You can have up to three NTP servers. Enter a value in this field only when the VMware host does not synchronize on its own.

User access

Field	Information to enter	Notes
Enhanced Access Security Gateway (EASG)	Enter one of the following: • `1` to enable EASG. • `2` to disable EASG. Avaya recommends that you enable EASG.	By disabling EASG, you are denying Avaya access to the system. This setting is not recommended as it can impact Avaya's ability to provide support for the product. Unless the customer can manage the product, Avaya Services Logins should not be disabled.

Customer Login Settings

Field	Information to enter	Notes
Login Name	Enter the login ID to use for the customer account (cust).	Login ID and password for customer account you will create during OVA deployment.
Password	Enter the customer account password.	This password will change after first customer login.
Customer Root Password	Enter the customer account root password.	Optional. Available only with SDM upgrades.
Additional user accounts		Record information here that is required to recreate additional user accounts. **Note:** Only one customer account can be created during OVA deployment. These additional accounts may be created post deployment using the `custAccounts` script.

System Manager Settings

Field	Information to enter	Notes
Primary System Manager IP	Enter the IP address of the primary System Manager that will be used to manage this Avaya Breeze® platform server.	
Enrollment Password	Enter the enrollment password that matches the value in System Manager administration.	You must know the enrollment password, and the password must not have expired. The password is set on System Manager at **Services** > **Security** > **Certificates** > **Enrollment Password**. On this page, verify that the **Time Remaining** value is greater than zero. If you do not know the password, create a new one.

Footprint values

Consult your Avaya Breeze® platform snap-in reference documents for specific profile and disk sizing requirements for the snap-ins you intend to install. Some snap-ins require higher disk space provisioning than the default of 50 GB. You must make this modification manually in the VM settings.

- Breeze 3.9 requires an additional 2 GB of memory per profile, as reflected in the table below.

Profile	CPU (cores)	Available Memory (GB)	Disk Storage (GB)	Maximum active SIP application sessions
1	4	8	50GB	29,900 sessions.
2	4	10		
3	6	12		44,880 sessions.
4	8	18	50 GB	59,840 sessions.
5	12	29	For Solution Deployment Manager deployments, this increases to 150 GB.	90,000 sessions.

Virtual machine

The Avaya Breeze® platform profile you select has default values, which can be adjusted, for these settings.

Setting	Information to enter
CPU/Memory allocation and reservations	Consult your snap-in reference document for specific sizing requirements.
DataStore location	Select the datastore location to store the virtual machine files.
Host networking assignments	

vCenter and ESXi Host

Field	Notes
vCenter Host Name	If the chosen OVA deployment method is without vCenter, the vCenter information is not needed.
vCenter IP Address	
vCenter Login	
vCenter Password	
ESXi Host Name	If the chosen OVA deployment method uses vCenter, the host name is the only field needed from this table.
ESXi IP Address	Host IP address.
ESXi host user name	
ESXi host password	

SIP entity (security module interface) networking information

You require the following information for administering the Avaya Breeze® platform instance and SIP entity:

Field	Information to enter	Notes
IP address	Enter the IP address of Avaya Breeze® platform SIP entity.	
Subnet mask	Enter the subnet mask of Avaya Breeze® platform SIP entity.	
Gateway	Enter the gateway of Avaya Breeze® platform SIP entity.	

Related links

Planning and preconfiguration on page 21

Out of Band Management in Avaya Breeze® platform

Avaya Breeze® platform always has two IP addresses that reside on the same or different IP networks depending on the Out of Band Management network.

The IP addresses for the security and management interface must be on:

- Same IP network if Out of Band Management is disabled.
- Different IP networks if Out of Band Management is enabled.

Related links

Planning and preconfiguration on page 21

Network latency

Avaya Breeze® platform tolerates the following maximum network latencies without call failures under load:

- 150ms for the WAN connection between the endpoint and the data center (one way delay).
- 42ms for the LAN connection among components in the data center, such as Avaya Breeze® platform to Session Manager and Avaya Breeze® platform to Avaya Breeze® platform.

Related links

Planning and preconfiguration on page 21

Latest software updates and patch information

Before you start the deployment or upgrade of an Avaya product or solution, download the latest software updates or patches for the product or solution. For more information, see the latest release notes, Product Support Notices (PSNs), and Product Correction Notices (PCNs) for the product or solution on the Avaya Support website at https://support.avaya.com/.

After deploying or upgrading a product or solution, use the instructions in the release notes, PSNs, or PCNs to install any required software updates or patches.

For third-party products used with an Avaya product or solution, see the latest release notes for the third-party products to determine if you must download and install any updates or patches.

Related links

Planning and preconfiguration on page 21

Avaya Aura® Media Server selection algorithm

Avaya Breeze® platform supports a rich algorithm for selecting which Avaya Aura® Media Server to use for each call. The algorithm uses the locations defined in the System Manager routing. You can assign locations as follows:

- You can assign locations explicitly to a SIP entity such as the Avaya Breeze® platform.
- You can specify IP address patterns for locations. Avaya Breeze® platform uses the address patterns to match the IP address of endpoints and SIP entities to locations.

The selection algorithm can also include optional rules which Avaya Breeze® platform uses in the following order:

1. Check the location of the caller

   If the caller's SIP endpoint or SIP entity, such as a trunk gateway, matches an assigned location, Avaya Breeze® platform attempts to assign the Avaya Aura® Media Server that is in the same location.

2. Check the location of the Avaya Breeze® platform server

   If the Avaya Breeze® platform server handling a call has an assigned location, Avaya Breeze® platform attempts to assign the Avaya Aura® Media Server in the same location.

3. Select a lightly-loaded Avaya Aura® Media Server from any location.

If none of these rules match, the call fails. New clusters have all the rules enabled by default. To preserve backward compatible behavior, any existing clusters do not have the first rule enabled by default. If required, you can enable the rule after upgrading.

You can select which rules on the Cluster Editor screen displayed when you click **New** or **Edit** on the Cluster Administration page. For more information, see “Cluster Editor field descriptions” in Administering Avaya Breeze® platform.

Related links

Planning and preconfiguration on page 21

Running the upgradeSolution script for System Manager

About this task

You only need to run this script is deploying or upgrading with Avaya Breeze® platform with System Manager Release 8.0.1.2. You do not need to run it you are using System Manager Release 8.1.3 or 10.1. See Avaya Breeze platform compatibility on page 14.

You must run the **`upgradeSolution`** script before you can access the Avaya Breeze® platform Release 3.8 or higher Element Manager. After performing this procedure, you can deploy or upgrade to Avaya Breeze® platform Release 3.8.1 or later.

Before you begin

Download the latest System Manager hot fix from https://support.avaya.com. This applies for all System Manager releases.

Procedure

1. Log in to System Manager and run the `cd /swlibrary` command to go to the software directory library.
2. Run the `df -h /swlibrary` command to ensure adequate space is available.

   You need approximately 600 MB of space.

   The following is an example of the command output:

   ```
   cust >df -h /swlibrary
   Filesystem      Size  Used Avail Use% Mounted on
   /dev/sdd         21G  7.6G   14G  37% /swlibrary
   ```

3. Create a new directory and navigate to that directory.
4. Download `BreezeEMInstall-<version>.zip` from https://support.avaya.com and transfer it to the directory you created in the previous step.

   You can use a tool, such as WinSCP, to transfer the zip file to the directory.

5. On System Manager, run the `upgradeSolution <path to installation zip>/BreezeEMInstall-<version>.zip` command.
6. When prompted, accept the license agreement.

   The installation of Element Manager runs in the background. The installation process takes approximately 30 minutes to complete.

7. **(Optional)** Use `/var/log/Avaya/breeze-em-upgrade.log` to monitor the progress of the installation process.

Related links

Planning and preconfiguration on page 21

Chapter 5: Avaya Aura® Media Server OVA deployment

There are several different ways to deploy the Avaya Aura® Media Server. For a high-level list of Avaya Aura® Media Server deployment tasks, see Avaya Aura Media Server deployment checklist on page 15. For more detailed information about deploying the Avaya Aura® Media Server Open Virtual Appliance (OVA), see *Deploying and Updating Avaya Media Server using VMware® in the Virtualized Environment*.

Do not configure Avaya Aura® Media Server associated to the Avaya Breeze® platform application in an N+1 Load Sharing cluster. If redundancy or High Availability of Avaya Aura® Media Server is required, use the 1+1 High Availability cluster configuration.

The following sections lead you through the steps to configure Avaya Aura® Media Server for use with Avaya Breeze® platform after the Avaya Aura® Media Server OVA is deployed.

You must clear the **Convert Recordings to Base64** check box on Avaya Aura® Media Server. This setting enables files to be stored unencoded on the remote HTTP location. You can find this check box by navigating to **Home** > **System Configuration** > **Media Processing** > **Advanced Settings**. This setting also helps in file transfer performance.

Related links

Administering Avaya Aura Media Server for REST on page 31
Assigning Avaya Aura Media Server for use with Avaya Breeze platform on page 33
Licensing the Avaya Aura Media Server on page 33
Installing the Avaya Aura Media Server license file on page 34
Adding the System Manager IP address on page 34
SIPS and SRTP on Avaya Aura Media Server on page 35
Avaya Aura Media Server host name resolution on page 37
Avaya Aura Media Server trust configuration on page 38
Exporting an Avaya Aura Media Server certificate on page 39
Enabling and configuring digit relay settings on page 39

Administering Avaya Aura® Media Server for REST

About this task

Use this procedure to configure Avaya Aura® Media Server to allow REST access using HTTP.

For more information, see *Implementing and Administering Avaya Aura® Media Server*.

Procedure

1. Log on to the Avaya Aura® Media Server web console.
2. Navigate to **System Configuration** > **Signaling Protocols** > **REST** > **General Settings**.
3. To enable TLS for REST services, select the **Enable TLS Transport** check box.
4. To enable two-way authentication for an extra level of security, select the **Enable TLS Mutual Authentication** check box.
5. To use plaintext usernames and passwords, select **Basic Authentication**. Alternatively, to include an authentication realm and encrypt the credentials before sending them over the network, select **Digest Authentication**.
    a. Enter the required username and password credentials in the **Authentication Username** and **Authentication Password** fields.
    b. If you selected **Digest Authentication**, then enter the name of the required authentication realm in the **Authentication Realm** field.
6. Click **Save**.

    Changes to the transport settings require a restart to take effect.
7. Navigate to **System Configuration** > **Network Settings** > **General Settings** > **Connection Security**.
8. Select the **Verify Host Name of TLS Client Connections** check box.
9. Change the **Minimum TLS Version** from **TLSv1.3** to **TLSv1.2**.
10. Click **Save**.
11. Navigate to **Security** > **Certificate Management** > **Key Store**.
12. Assign System Manager signed certificate to all service profiles.
13. Click **Save**.
14. Restart Avaya Aura® Media Server:
    a. Navigate to **System Status** > **Element Status**.
    b. Click **Restart**.

Related links

Avaya Aura Media Server OVA deployment on page 31

Assigning Avaya Aura® Media Server for use with Avaya Breeze® platform

Procedure

1. In System Manager, click **Elements** > **Media Server** > **Application Assignment**.
2. Select the check box next to Avaya Breeze® platform and click **Edit**.
3. Select the check box next to Avaya Aura® Media Server and click **Commit**.
   - The system takes up to two minutes to update the Avaya Breeze® platform.
   - You cannot assign Avaya Aura® Media Server to multiple applications.

Related links

Avaya Aura Media Server OVA deployment on page 31

Licensing the Avaya Aura® Media Server

About this task

The license file installed on the System Manager WebLM and Avaya Aura® Media Server gets the license from System Manager WebLM.

Note:

- In accordance with the Avaya End User License Agreement (EULA) you can only administer the number of Avaya Aura® Media Server instances allowed by your Media Server license. For more information, see *Implementing and Administering Avaya Aura® Media Server*.

Procedure

1. Get the Avaya Aura® Media Server license from PLDS.
2. Install the Avaya Aura® Media Server license file on System Manager WebLM.
3. To configure Avaya Aura® Media Server with the System Manager WebLM IP address, perform the following steps:
   a. Navigate to **Licensing** > **General Settings**.
   b. From the **Licensing** drop-down list, select **WebLM Server**.
   c. Enter the address of the **WebLM Server** that you plan to use in the **Server Host Name or IP Address** field.
   d. Enter the port to use with the **WebLM Server** in the **Server Port** field.
   e. Enter the URL suffix used to identify the **WebLM Server**. The default URL suffix is `/WebLM/LicenseServer`.
   f. In the **License Details** , set the **Maximum Number** and **Minimum Number** based on the number of sessions the cluster supports.

g. Click **Save**.

Related links

Avaya Aura Media Server OVA deployment on page 31

Installing the Avaya Aura® Media Server license file

Procedure

1. On the System Manager web console, click **Services** > **Licenses**.
2. Click **Install license** and **Browse** to the location of the Avaya Breeze® platform license file on your computer.
3. Click **Install**.

Related links

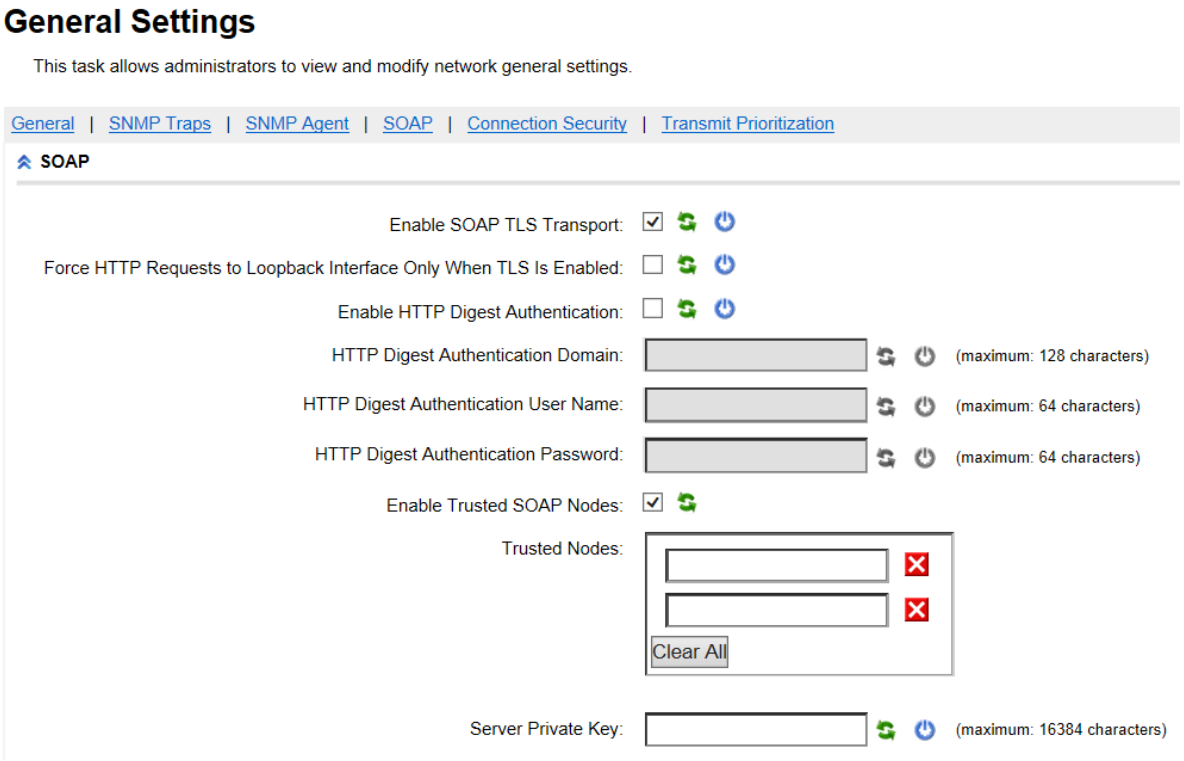
Avaya Aura Media Server OVA deployment on page 31

Adding the System Manager IP address

Procedure

1. Type `https://<fqdn>:8443/emlogin` in a Web browser.
2. Log on to the Avaya Aura® Media Server Element Manager interface using the customer login ID and password created when you deployed the OVA.

3. Navigate to **System Configuration** > **Network Settings** > **General Settings**.



4. In the **SOAP** section, **Trusted Nodes** field, type the IP address of the primary System Manager that is used to manage Avaya Breeze® platform. If this is a geo-redundant deployment, type the secondary System Manager IP addresses in the second text field in the Trusted Nodes box.
5. Click **Save** .
6. Repeat this procedure for each Avaya Aura® Media Server.

Next steps

Configure announcements for services on each Avaya Aura® Media Server. For additional information, see *Media File Provisioning* in *Implementing and Administering Avaya Aura® Media Server*. All Media Servers must be configured with the same announcement files.

Related links

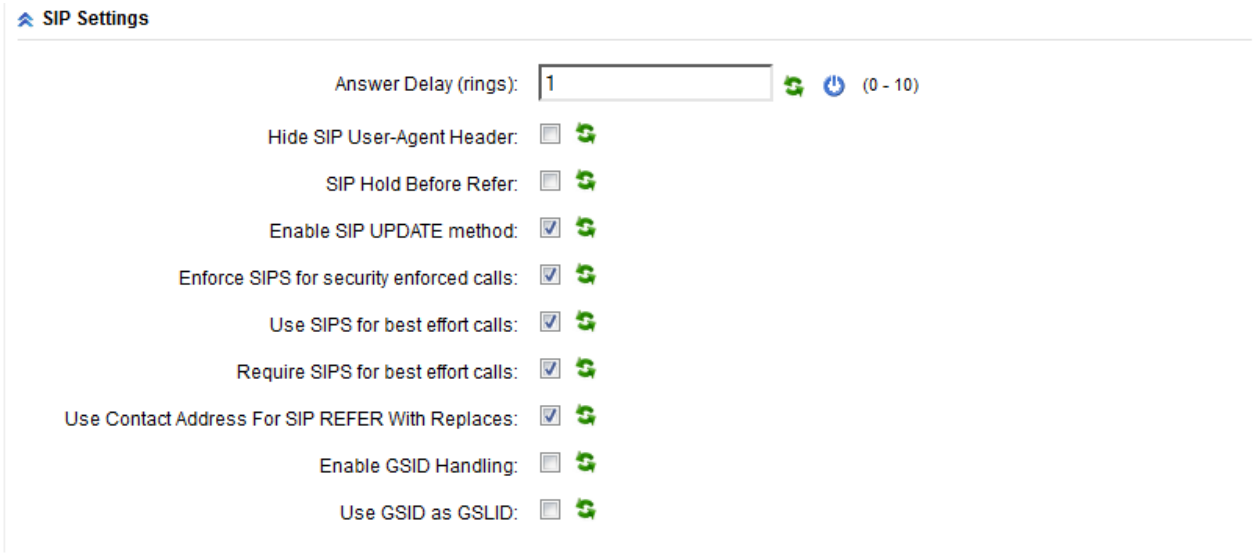
Avaya Aura Media Server OVA deployment on page 31

SIPS and SRTP on Avaya Aura® Media Server

The Secure Real Time Protocol (SRTP) administration is described in detail in the *Implementation and Administering Avaya Aura Media Server* document, specifically the topics on Configuring

SIP general settings and Media security configuration. Refer to the Avaya Aura® Media Server Element Manager example below for interoperability with Avaya Aura.

The SIPS settings are found under **Home** > **System Configuration** > **Signaling Protocols** > **SIP** > **General Settings**.



Note:

The following configuration is not applicable to Avaya Aura® Media Server 10.2 and later. However, it remains valid for versions prior to 10.2.

The SRTP settings are found under **Home** > **System Configuration** > **Media Processing** > **Media Security**.

If you set the **Security Policy** field to **BEST EFFORT**, you must select the following fields in the SIP Settings section:

- **Enforce SIPS for security enforced calls**
- **Require SIPS for best effort calls**

Related links

Avaya Aura Media Server OVA deployment on page 31

Avaya Aura® Media Server host name resolution

This section is applicable only to snap-ins using SIP to communicate with Avaya Aura® Media Server.

In cases where the Avaya Aura® Media Server is retrieving announcements or storing recordings for an Avaya Breeze® platform snap-in via HTTPS, you must ensure that the Media Server can communicate with the Avaya Breeze® platform server. You can accomplish this in several ways:

- Map the FQDN of each Avaya Breeze® platform server on your DNS server.
- Enter the IP Address and Hostname of each Avaya Breeze® platform server in the Avaya Aura® Media Server Network Settings.
- Disable host name verification in the Avaya Aura® Media Server Network Settings. This is a less secure option. It is acceptable for a lab deployment, but is not recommended for a production environment.

Related links

Avaya Aura Media Server OVA deployment on page 31
Configuring Avaya Aura Media Server name resolution (alternative 1) on page 37
Configuring connection security options (alternative 2) on page 38

Configuring Avaya Aura® Media Server name resolution (alternative 1)

About this task

Complete this procedure to allow communication between the Avaya Aura® Media Server and required Avaya Breeze® platform servers. You must enter a mapping for each Avaya Breeze® platform that the Avaya Aura® Media Server accesses. The mappings are preserved in the local hosts file on the Avaya Aura® Media Server. This procedure is not necessary if you have mapped the FQDN of each Avaya Breeze® platform server on your DNS server or if you have disabled host name verification (alternative 2).

Procedure

1. On the Avaya Aura® Media Server web console, click **System Configuration** > **Network Settings** > **Name Resolution**.
2. Click **Add**.
3. Add the **IP Address** and the **Hostname** of an Avaya Breeze® platform server.

   The **Hostname** must match the one specified in the identity certificate for the Avaya Breeze® platform server.

   IP Address is the management IP address of Avaya Breeze® platform server.
4. Continue adding the **IP Address** and the **Hostname** for each additional Avaya Breeze® platform server.
5. Click **Save**.

Related links

Avaya Aura Media Server host name resolution on page 37

Configuring connection security options (alternative 2)

About this task

This procedure is recommended only in a lab deployment. It is not recommended for a production environment. This procedure is not necessary if you have mapped the FQDN of each Avaya Breeze® platform server on your DNS server or if you have configured host name resolution (alternative 1).

Procedure

1. On the Avaya Aura® Media Server web console, click **System Configuration** > **Network Settings** > **General Settings** > **Connection Security**.
2. Clear **Verify Host Name**.
3. Click **Save**.
4. Restart the Avaya Aura® Media Server for the changes to take effect.
5. On the web console, click **System Status** > **Element Status**.
6. Click **Restart**.
7. Click **Confirm**.

Related links

Avaya Aura Media Server host name resolution on page 37

Avaya Aura® Media Server trust configuration

Only secure (https) connection is supported between Avaya Breeze® platform and Avaya Aura® Media Server. The Subject Name or Subject Alternate Name in the certificate must be valid, and the security options for the connection must be appropriately configured. Refer to the following sections of the *Implementing and Administering Avaya Media Server* document:

- “Configuring connection security options”
- “Security configuration”

Related links

Avaya Aura Media Server OVA deployment on page 31

Exporting an Avaya Aura® Media Server certificate

Procedure

1. In System Manager, click **Services** > **Inventory** > **Manage Elements**.
2. Select an Avaya Aura® Media Server instance.
3. Click **More Actions** > **Configure Trusted Certificates**.
4. Select the appropriate certificate to export.
5. Click **Export**.

Related links

Avaya Aura Media Server OVA deployment on page 31

Enabling and configuring digit relay settings

About this task

Note:

The following configuration is not applicable to Avaya Aura® Media Server 10.2 and later. However, it remains valid for versions prior to 10.2.

Note:

Controlling applications typically override AAMS configuration using templates and template control modifiers. Digit relay configuration changes and preferences must be configured first on the controlling application and not on Avaya Aura® MS. See documentation for the controlling application to determine if any Avaya Aura® MS changes are required.

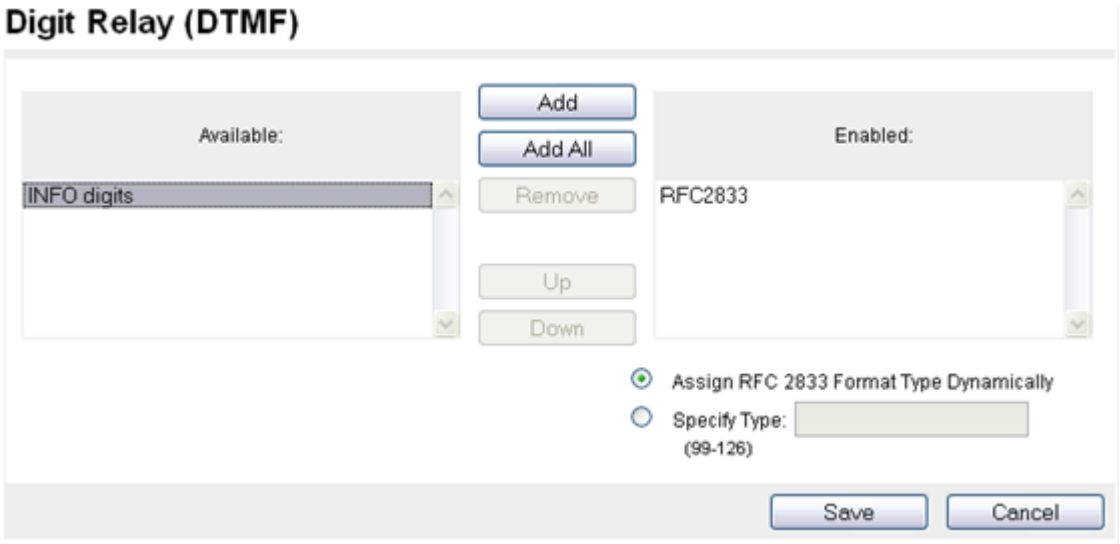
Avaya Aura® MS uses digit relay settings and the order of the enabled relay methods when negotiating digit relay with a client endpoint. These settings apply for inbound or outbound sessions.

Avaya Aura® MS also supports in-band DTMF. The system defaults to this option if no other option is configured or negotiated by Avaya Aura® MS. The preferred method of digit transmission is RFC 2833.

Perform the following procedure to enable and configure the digit relay support on Avaya Aura® MS.

Procedure

1. Navigate to **EM** > **System Configuration** > **Media Processing** > **Digit Relay (DTMF)**.



2. On the Digit Relay (DTMF) page, select one or more methods from the **Available** list.
3. Click **Add** to move the methods to the **Enabled** list.
4. To change the priority rank of a method within the **Enabled** list, select a method and use the **Up** or **Down** buttons to move it within the list.
5. Choose the required payload type option:
   - If a dynamic payload type is required, select **Assign RFC 2833 Format Type Dynamically**.
   - If a fixed payload type is required, select **Specify Type**. In the **Specify Type** field, enter the value to use in the payload type field of the RTP header when transmitting RFC2833 encoded digits.
6. Click **Save**.

Related links

Avaya Aura Media Server OVA deployment on page 31

Chapter 6: Deploying the Avaya Breeze® platform OVA

Related links

OVA deployment requirements on page 41
Verifying the enrollment password status on page 42
Deploying Avaya Breeze platform OVA with VMware vSphere Web Client on page 43
Deploying Avaya Breeze platform OVA with VMware vSphere Client connected to vCenter on page 45
Deploying Avaya Breeze platform OVA with VMware vSphere Client connected to ESXi host on page 47
Deploying Avaya Breeze platform OVA with Solution Deployment Manager on page 50
Configuring Avaya Breeze platform after changing the IP address or FQDN on page 53
Changing the System Manager configuration for an Avaya Breeze platform node on page 54
Configure the new server automatic startup settings on page 54
Changing the customer password on first login on page 56
Patching the Avaya Breeze platform on page 57
Creating multiple privileged user accounts on page 58
Enhanced Access Security Gateway on page 58

OVA deployment requirements

This section leads you through the steps to deploy the Avaya Breeze® platform Open Virtual Appliance (OVA). You can deploy it with:

- The VMware vSphere Web Client
- Solution Deployment Manager

Select the procedure that applies to you.

You must have the following to complete a procedure:

- vSphere ESXi 7.0 or later

  For more information, see: https://support.avaya.com/CompatibilityMatrix/Index.aspx
- A downloaded copy of the Avaya Breeze® platform OVA

- The information recorded in the Customer Configuration Information Worksheet

For a description of required resources, see Avaya Breeze® platform Overview and Specification.

After deploying the Avaya Breeze® platform OVA, you can run the **CEnetSetup** command to change the value of any OVA property specified during deployment.

If you change the IP address or FQDN of Avaya Breeze® platform using the **CEnetSetup** or the **AvayaNetSetup** script, you must follow the steps in Configuring Avaya Breeze platform after changing the IP address or FQDN on page 53.

GDPR compliance

All the data to and from Avaya Breeze® platform nodes is encrypted using TLS in transit.

When deploying Avaya Breeze® platform you can choose to encrypt your virtual machine (VM) for General Data Protection Regulation (GDPR) compliance using VMware provided encryption. The procedure requires a Key Management Server (KMS). Follow the vCenter virtual machine encryption instructions in your VMware documentation.

Encrypting your VM will reduce the capacity of your server. How much depends on the resources used by the installed snap-ins. Snap-ins that use the system storage, including the local cluster database, will notice a greater capacity decrease.

For additional information about GDPR compliance, see Avaya Breeze® platform Overview and Specification.

Related links

Deploying the Avaya Breeze platform OVA on page 41

Verifying the enrollment password status

The Avaya Breeze® platform requires an Enrollment Password during the initial installation and deployment process. Enrolling a password establishes trust between System Manager and Avaya Breeze® platform. The enrollment password is also known as the 'certificate enrollment password'.

- If the enrollment password has expired, renew the existing password.
- If the **Time Remaining** value is not zero, the password is valid. Verify that the time remaining is sufficient.

Procedure

1. In System Manager, click **Services** > **Security** > **Certificates** > **Enrollment Password**.
2. If the value of the **Time Remaining** field is zero, renew the password:
   a. In the **Password expires in** field, select a value from the drop-down menu for the time when the password must expire.
   b. Enter the password in the **Password** field.
   c. Reenter the password in the **Confirm Password** field.

d. Click **Commit**.

The system updates the **Time Remaining** field.

Related links

Deploying the Avaya Breeze platform OVA on page 41

Deploying Avaya Breeze® platform OVA with VMware vSphere Web Client

Before you begin

The steps in this procedure use vSphere Web Client connected to vCenter. It runs in a web browser.

- Save the Avaya Breeze® platform OVA file onto the workstation running the vSphere web client.
- Verify that the Enrollment Password is administered and not expired.
- Use the *Customer Configuration Information* to get the required network settings for deployment. You can obtain the settings from an existing system if you are redeploying the OVA.

Procedure

1. If using vCenter 7.0 U2 or later, do the following.

   a. Download the OVF/OVA signing certificate chain from https://web.entrust.com/root-certificates/entrust_g2_ca.cer?_ga=2.204957712.1460439918.1633458407-705405935.1632328263. For more information, see the VMware article at https://kb.vmware.com/s/article/84240.

   b. Log in to vCenter as administrator.

   c. Click **Administration** > **Certificates** > **Certificate Management**.

   d. Click **Add** next to **Trusted Root Certificates**.

   e. Browse and select the certificates file downloaded in the first sub-step.

   f. Select the **Start Root certificate push to vCenter Hosts** check box.

2. Log in to the vCenter using the VMware vSphere Web Client.

   The format is `https://<IP Address:9443>/vsphere-client`

3. In the navigation pane, click **vCenter**.
4. Click **Inventory Trees** > **Hosts and Clusters**.
5. Expand **Hosts and Clusters** to locate and select the target deployment host.
6. Right-click the on the host and select **Deploy OVF Template**.

7. On the **Select Source** page, enter the **URL** or path for installing the OVA, and click **Next**.
8. On the **Review Details** page, confirm the properties of the OVA file you selected and click **Next**.
9. If using vCenter 7.0 U2 or later:
   - If you performed step 1: Ignore the “invalid certificate” warning in the **Publisher** field.
   - If you performed step 1: Click **Ignore** next to the warning “The certificate is not trusted”.
10. To accept the End User License Agreement, click **Accept**.
11. Click **Next**.
12. Enter a name for the Avaya Breeze® platform VM and select the required datacenter folder for the VM.
13. Click **Next**.
14. On the **Select a resource** page, select the location to run the deployed template and click **Next**.
15. Select the configuration profile that best fits the deployment and click **Next**.
16. Select the virtual disk format you want and click **Next**.
17. Select the destination network for each Avaya Breeze® platform interface and click **Next**.
18. On the **Setup networks** page, configure the network settings for your VM and click **Next**.

    Important:

    During OVA deployments do not enter the IPv6 address, IPv6 network prefix, or IPv6 gateway for eth0 unless the latest Avaya Breeze® platform patches already have been applied. For more information about configuring IPv6, see “Enabling IPv6 on the management interface of an Avaya Breeze platform server” in Deploying Avaya Breeze® platform.
19. On the **Customize template** page, enter the configuration details for your VM and click **Next**.
20. On the **Ready to Complete** page, verify the options for the VM:
    - If the values are incorrect, click **Back** to make the changes.
    - If the values are correct, click **Finish**.

    Tip:

    To alter the configuration settings later, see Maintaining and Troubleshooting Avaya Breeze® platform.

    Wait for the deployment to complete. The time taken depends on the speed of your network connection.

    After the deployment is complete, the system updates the **Inventory list** and displays the new virtual machine.

21. Select the new VM and click the **Summary** tab.
22. Click **Actions** > **Power On**.

    Important:

    - If installing multiple servers, allow at least 5 minutes between starting each of the new virtual machines.

23. Click **Summary** > **Launch Console** to open a new console.

    The system displays the progress of the VM system initialization.

24. After the VM initialization is complete, log in by using the customer account that you set up earlier.

Related links

Deploying the Avaya Breeze platform OVA on page 41

Deploying Avaya Breeze® platform OVA with VMware vSphere Client connected to vCenter

Before you begin

The steps in this procedure use the vSphere Client connected to VMware vCenter. This method of deployment is available if vCenter version is 6.0 or earlier.

- Save the Avaya Breeze® platform OVA file onto the workstation running the vSphere Client.
- Verify that the Enrollment Password is administered and not expired.
- Use the *Customer Configuration Information* to get the required network settings for deployment. You can obtain the settings from an existing system if you are redeploying the OVA.

Procedure

1. Log in to the vCenter using the VMware vSphere Client.
2. Click **File** > **Deploy OVF Template**
3. Click **Browse** and find the Avaya Breeze® platform OVA. Click **Next**.
4. Verify that the details displayed match the version of the Avaya Breeze® platform that you are expecting to deploy.
   - If the details do not match, you may have chosen the wrong OVA. Click **Back** and choose the correct OVA.
   - If the details match, click **Next**.
5. If you wish to accept the End User License Agreement click **Accept**, then click **Next**.
6. On the **Name and Location** page, enter a name for the Avaya Breeze® platform virtual machine. Select the inventory location for your virtual machine, then click **Next**.

7. On the **Deployment Configuration** page, select the configuration profile that best fits the deployment, then click **Next**.
8. On the **Host/Cluster** page, select the specific host on which you want to deploy this VM, and click **Next**.
9. On the **Disk Format** page, select the disk provisioning format you want, then click **Next**.
10. On the **Network Mapping** page, select the destination network for each Avaya Breeze® platform interface, and click **Next**.

    Important:

    During OVA deployments do not enter the IPv6 address, IPv6 network prefix, or IPv6 gateway for eth0 unless the latest Avaya Breeze® platform patches have been applied. For more information about configuring IPv6, see “Enabling IPv6 on the management interface of an Avaya Breeze platform server” in Deploying Avaya Breeze® platform.

    We recommend that you use different physical networks for each of the Avaya Breeze® platform interfaces.

    - Public (eth1) - Asset/security module
    - Out of band management (eth0) - management NIC
11. On the **Properties** page, enter the configuration details for your new server. See the *Customer Configuration Information* you collected for the values to enter in these fields. Click **Next**.
12. On the **Ready to Complete** page, verify the listed properties.
    - If the values are incorrect, click **Back** to modify the values.
    - If the values are correct, click **Finish**.

    Tip:

    To alter the configuration settings later, see Maintaining and Troubleshooting Avaya Breeze® platform.

    A status window pops up after clicking **Finish**. Wait for the deployment to complete. The time this takes depends on the speed of your network connection. Once completed, you can close the window.
13. Locate your new VM in the inventory list in the **vSphere Client** window, right click and click **Virtual Machine** > **Power** > **Power On**.

    Important:

    - If installing multiple servers, allow at least 5 minutes between starting each of the new virtual machines.
14. (Optional) To open a **console** window to your VM, right-click the VM and click **Open Console**.

Related links

Deploying the Avaya Breeze platform OVA on page 41

Deploying Avaya Breeze® platform OVA with VMware vSphere Client connected to ESXi host

Before you begin

The steps in this procedure use the VMware vSphere Client connected to the ESXi host.

- Save the Avaya Breeze® platform OVA file onto the workstation running the vSphere Client.
- Use the *Customer Configuration Information* to get the required network settings for deployment. You can obtain the settings from an existing system if you are redeploying the OVA.
- Verify that the Enrollment Password is administered and not expired.

Procedure

1. Log in to the VMware host using the VMware vSphere client.
2. Click **File** > **Deploy OVF Template**
3. Click **Browse** and find the Avaya Breeze® platform OVA.
4. Click **Next**.
5. Verify that the details displayed match the version of the Avaya Breeze® platform that you are expecting to deploy.
   - If the details do not match, you may have chosen the wrong OVA. Click **Back** and find the correct OVA.
   - If the details do match, click **Next**.
6. If you accept the End User License Agreement, click **Accept** and then click **Next**.
7. Enter a name for the Avaya Breeze® platform Virtual Machine (VM) on the **Name and Location** page and click **Next**.
8. On the **Deployment Configuration** page, select the configuration profile that best fits the deployment and click **Next**.
9. On the **Disk Format** page, select the disk provisioning format you want and click **Next**.

   While Avaya Breeze® platform works with either thick or thin provisioned disk, Avaya recommends using a **Thick Provision Lazy Zeroed** disk.
10. On the **Network Mapping** page, select the destination network for each Avaya Breeze® platform interface, then click **Next**.

    We recommend that you use different physical networks for each of the Avaya Breeze® platform interfaces.
    - Public (eth1) - Asset/security module
    - Out of band management (eth0) - management NIC

11. On the **Ready to Complete** page, verify the options listed.
    - If the values are incorrect, click **Back** to modify the values.
    - If the values are correct, click **Finish**.
12. A status window pops up after clicking **Finish**. Wait for the deployment to complete. The time this takes depends on the speed of your network connection. After completing, close the window.
13. Locate your new VM in the **inventory list** in the **vSphere Client** window.
14. Right-click to go to **Power** > **Power On**.
15. To open a **console** window to your VM, right-click the VM and click **Open Console**.
16. During the boot, you will see the **End User License Agreement**. Scroll down through this document using the spacebar. At the bottom, enter `yes` if you agree to the terms.
17. When prompted to configure the virtual machine enter `y`.
18. Enter the management interface network parameters, date and time information, customer user information, and System Manager information.

    Important:

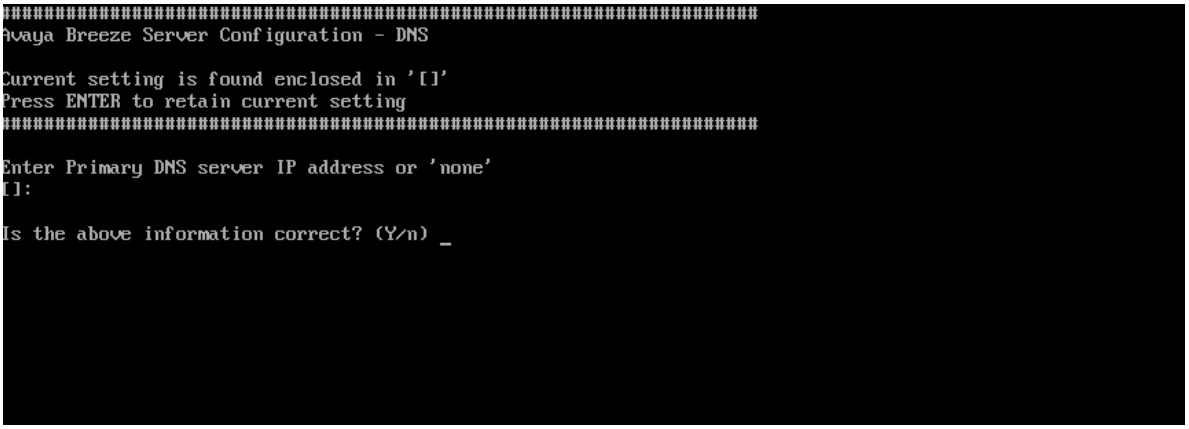
    During OVA deployments do not enter the IPv6 address, IPv6 network prefix, or IPv6 gateway for eth0 unless the latest Avaya Breeze® platform patches already have been applied. For more information about configuring IPv6, see “Enabling IPv6 on the management interface of an Avaya Breeze platform server” in Deploying Avaya Breeze® platform.

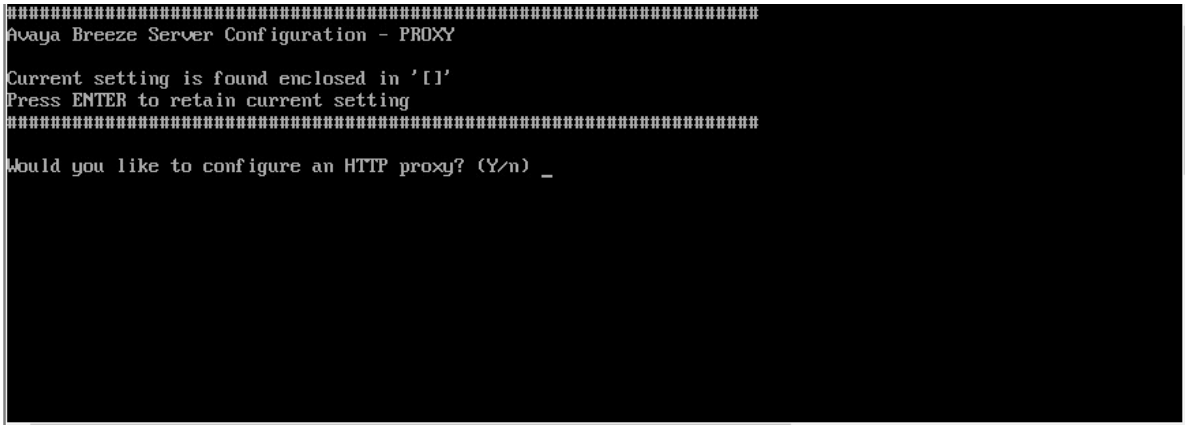
    See the *Customer Configuration Information* you collected for the values to enter in these fields.

    Tip:

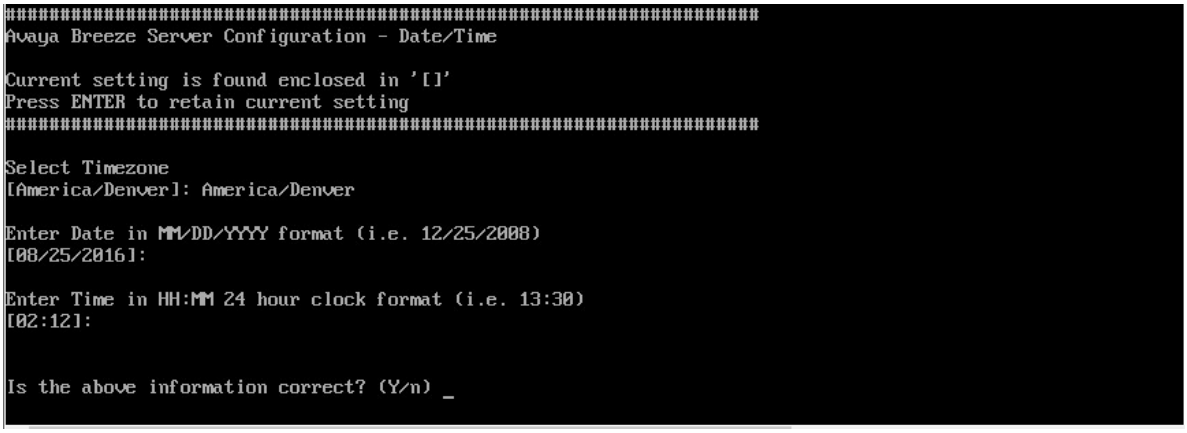
    To alter the configuration settings later, see Maintaining and Troubleshooting Avaya Breeze® platform.

    Refer to the following screenshots.


Avaya Breeze Server Configuration - DNS
Current setting is found enclosed in '[]'
Press ENTER to retain current setting
Enter Primary DNS server IP address or 'none'
[]:
Is the above information correct? (Y/n)


Avaya Breeze Server Configuration - PROXY
Current setting is found enclosed in '[]'
Press ENTER to retain current setting
Would you like to configure an HTTP proxy? (Y/n)

Avaya Timezone Selection
America/Belem
America/Belize
America/Blanc-Sablon
America/Boa_Vista
America/Bogota
America/Boise
America/Buenos_Aires
America/Cambridge_Bay
America/Campo_Grande
America/Cancun
America/Caracas
America/Catamarca
America/Cayenne
America/Cayman
America/Chicago
America/Chihuahua
America/Coral_Harbour



19. Run the `CEnetSetup` command to change the value of any OVA property specified during deployment.

Important:

During OVA deployments do not enter the IPv6 address, IPv6 network prefix, or IPv6 gateway for eth0 unless the latest Avaya Breeze® platform patches already have been applied. For more information about configuring IPv6, see “Enabling IPv6 on the management interface of an Avaya Breeze platform server” in Deploying Avaya Breeze® platform.

Related links

Deploying the Avaya Breeze platform OVA on page 41

Deploying Avaya Breeze® platform OVA with Solution Deployment Manager

This procedure uses the Solution Deployment Manager.

Before you begin

- Install the Avaya Aura® Appliance Virtualization Platform if necessary.
- Download the Avaya Breeze® platform OVA file.
- Use the *Customer Configuration Information* to get the required network settings for deployment. You can obtain the settings from an existing system if you are redeploying the OVA.
- Verify that the Enrollment Password is administered and not expired.

Procedure

1. Copy the previously downloaded Avaya Breeze® platform OVA file to the System Manager `/swlibrary/staging/sync/` directory. If necessary, add the `staging/sync` folders to the directory structure.
2. In System Manager, click **Services** > **Solution Deployment Manager** > **Software Library Management**.
3. Click **Manage Files**.
4. In the list of **Sync Files from directory**, enter the SHA256 checksum and select a software library.
5. In **Product Family**, select **Avaya Breeze**.
6. In **Device Type** and **Software Type**, select **OVA**.
7. Click **Sync** and wait for the operation to complete.
8. Verify completion of the file sync to the library.
    a. Navigate to **Home** > **Services** > **Scheduler** > **Completed Jobs**.
    b. Check for `Job Name = IUM_syncFiles`, and `Job Status = SUCCESSFUL`.
9. Navigate to **Home** > **Services** > **Solution Deployment Manager** > **Software Library Management**.
10. Check SMGR_DEFAULT_LOCAL, click **Manage Files**, and confirm that the OVA file is in the list of files under **Software Library Files**.
11. Add a location to Solution Deployment Manager. There might be an existing location if adding a second or later virtual machine.
    a. On System Manager, click **Services** > **Solution Deployment Manager**.
    b. Click **Application Management**.
    c. Select **New** under **Locations**.
    d. Populate the location properties and click **Save**.
12. Add a host to a location. The VMware host or AVP must be accessible to the System Manager to perform this step.
    a. In the **Application Management Tree**, select the location to add the host to.
    b. Click the **Platforms** tab.

c. Click **Add**.

d. Populate the **Host Name**, **Host FQDN or IP**, **User Name**, and **Password** fields using the same information used for the Appliance Virtualization Platform.

For the **Host FQDN or IP** field, use the FQDN of the VMware host or the FQDN of the Appliance Virtual Platform.

13. Navigate to **Home** > **Services** > **Solution Deployment Manager** > **Application Management**.
14. Expand the **Application Management Tree** and expand the **Location**. Click the platform on which you want to deploy the Avaya Breeze instance.
15. On the **Applications** tab click **New**.
16. In the **Select Location and Platform** section, perform the following steps:

Alternatively, in Step 12a, you can pre-select the location and platform in the **Application Management Tree**.

a. In **Select Location**, select a location.

b. In **Select Host**, select a host.

c. Select a data store.

17. Click **Next**.
18. In the **Deploy OVA** section, perform the following steps:

a. Select the **Select from software library** field.

b. In the **Select Software Library** field, select the local and remote library where the OVA file is available. To deploy the OVA file using the Solution Deployment Manager client, use the default software library that is set during client installation.

c. In **Select OVAs**, select the OVA file that you want to deploy.

d. In **Flexi Footprint**, select a footprint.

For more information, refer to the **Flexi Footprint** values in the “Key customer configuration information” section.

19. Click the **Network Parameters** tab and select appropriate networks.

- Select the network that provides the subnet that Avaya Breeze® platform needs for SIP traffic (security module).
- Select the network that provides the subnet that Avaya Breeze® platform needs for the management interface (Avaya Breeze® platform instance).

20. Click the **Configuration Parameters** tab and populate the Configuration Parameters fields.

Note:

The SIP entity name must match the VM name when deploying with Solution Deployment Manager.

21. Optionally on the **Configuration Parameters** tab, set up a customer root access account.
    a. Click the box to **Enable Customer Root Account for this Application**.
    b. Click **Accept** to accept the **Root Access Acceptance Statement**.
    c. Enter the **Customer Root Password**.
22. Click **Deploy** to begin the OVA deployment.
23. Click **Accept** to accept the license terms.
24. Click the **Virtual Machines** tab.
25. Click the **Status Details** link to display the **VM deploy Status** window. The deployment is complete when all status checks display green check marks.

Related links

Deploying the Avaya Breeze platform OVA on page 41

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

Deploying the Avaya Breeze platform OVA on page 41

Changing the System Manager configuration for an Avaya Breeze® platform node

Procedure

1. Remove Avaya Breeze® platform node from the cluster on the old System Manager.
2. Ensure that the node is not part of any cluster on the new System Manager.
3. Wait for the system to complete the replication.
4. Run the `CEnetSetup` command to change the System Manager details.
5. Once trust is established with the new System Manager and the replication is complete, run the **`statapp`** command to verify that all services are up.
6. Add the node to a cluster on the new System Manager.

Related links

Deploying the Avaya Breeze platform OVA on page 41

Configure the new server automatic startup settings

You must configure all the Avaya Breeze® platform virtual machines to start automatically after the vSphere ESXi host starts.

- You do not need to configure the virtual machine automatic startup settings if using Solution Deployment Manager. For Solution Deployment Manager deployments, automatic startup configuration is part of the VM deployment.
- In high availability (HA) clusters, the VMware HA software ignores the startup selections.
- Avaya recommends a 5 minute delay between the startup of each server.

Related links

Deploying the Avaya Breeze platform OVA on page 41
Configuring startup settings using the vSphere desktop client on page 54
Configuring startup settings using the vSphere Web Client on page 56

Configuring startup settings using the vSphere desktop client

Before you begin

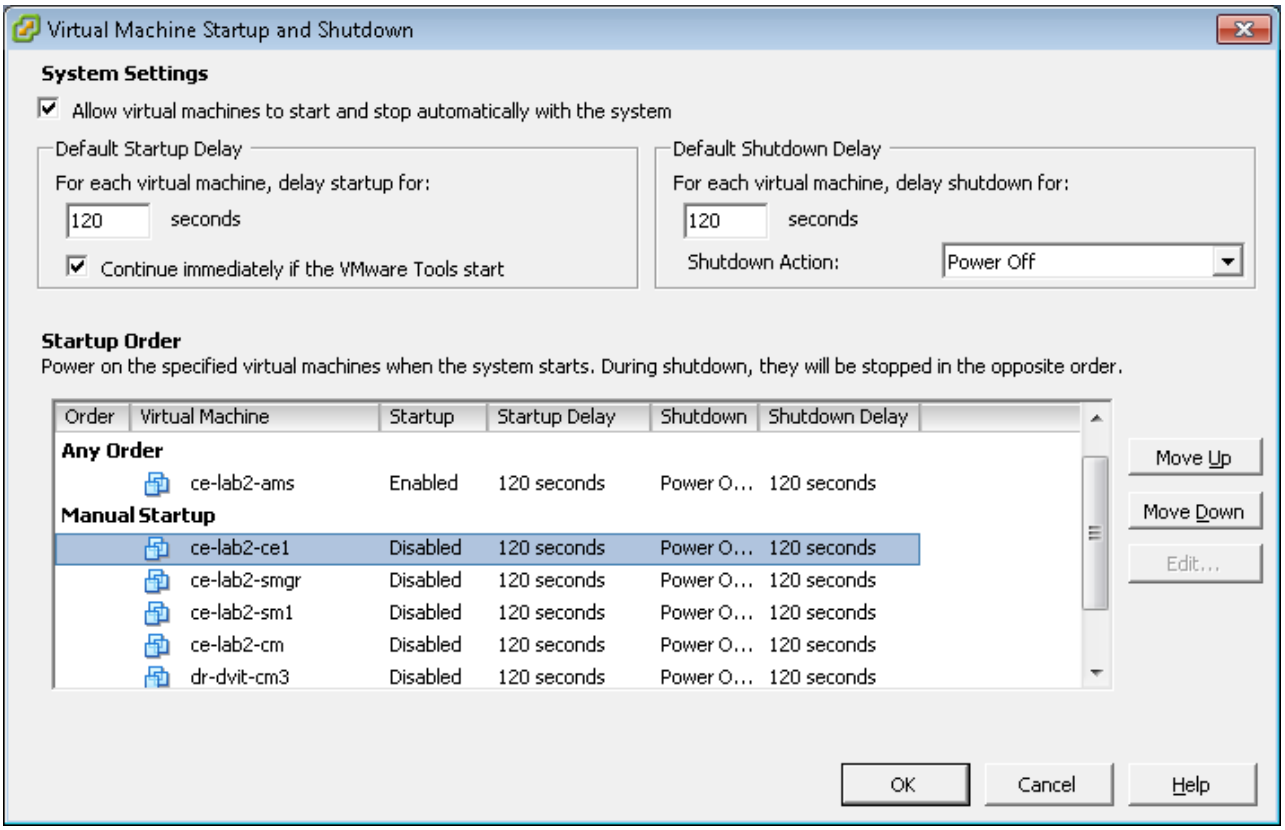
Confirm that you have the proper level of permissions to configure the automatic startup settings. If you do not have the proper level of permissions, contact your system administrator.

Procedure

1. In the vSphere Client inventory, select the host where the virtual machine is located.
2. Click the **Configuration** tab.
3. In the **Software** section, click **Virtual Machine Startup/Shutdown**.
4. Click **Properties** in the upper right corner of the screen.
5. In the **System Settings** section, select **Allow virtual machines to start and stop automatically with the system**.
6. In the **Default Startup Delay** section, set the **For each virtual machine, delay startup for** setting to 300 seconds. The hosting platform applies this setting to the start time between each virtual machine set for automatic startup.
7. In the **Manual Startup** section, select the virtual machine.
8. Use the **Move up** button to move the virtual machine under **Automatic Startup**.
9. Click **OK**.

Example

The following is an example of the **Virtual Machine Startup/Shutdown** screen.



Related links

Configure the new server automatic startup settings on page 54

Configuring startup settings using the vSphere Web Client

Before you begin

Confirm that you have the proper level of permissions to configure the automatic startup settings. If you do not have the proper level of permissions, contact your system administrator.

Procedure

1. Select the host where the virtual machine is located.
2. Click **Manage** > **Settings**.
3. Click **Virtual Machine Startup/Shutdown**.
4. Click **Edit**.
5. In the **System Settings** section, select **Allow virtual machines to start and stop automatically with the system**.
6. In the **Default Startup Delay** section, set the **For each virtual machine, delay startup for** setting to 300 seconds. The hosting platform applies this setting to the start time between each virtual machine set for automatic startup.
7. In the **Manual Startup** section, select the virtual machine.
8. Move the Avaya Breeze® platform virtual machine to **Automatic Startup** section.

Related links

Configure the new server automatic startup settings on page 54

Changing the customer password on first login

Before you begin

Set a temporary password while deploying the Avaya Breeze® platform OVA:

- If using vCenter, the temporary customer password is set during initial deployment. Regardless of what you set there, you will be prompted to change it upon first login
- If using the Standalone client, a temporary customer password is set during the first boot when you are prompted to configure the Avaya Breeze® platform node.

Procedure

1. Log in to the deployed and configured Avaya Breeze® platform node.
2. Enter the customer login.
3. Enter the temporary customer password created while deploying the OVA.
4. When the system prompts to change the password for the customer login, enter the new password. The new password:
   - Must have at least eight characters.

- Should not be based on a dictionary word or username.
- Must contain a mix of numbers, letters, and at least one special character.
- Must have a mix of upper and lower case letters.
- Cannot be the same as the temporary password.

5. When the system prompts to confirm the password, reenter the same password that you entered above.

Related links

Deploying the Avaya Breeze platform OVA on page 41

Patching the Avaya Breeze® platform

About this task

This procedure provides general patching steps. For more information about specific patches, see *Avaya Breeze® platform Release Notes*.

Caution:

You cannot remove a patch after it is installed. This includes recovery from a patch install failing due to intermittent network issues. To enable recovery, you must take a snapshot of Avaya Breeze® platform before installing the patch. Verify that the system is running correctly after the patch is installed. When verified, remove the snapshot within 12–24 hours. See VMware snapshots on page 98 for special considerations when using snapshots.

Before you begin

- The server must be in the Deny New Service state.
- Ensure that the activity count is 0 for a cluster database.
- Download the patch file and copy it to the Avaya Breeze® platform server.
- The patch should have the following Linux permissions: `rw-r--r--`.

Procedure

1. Log in to Avaya Breeze® platform using the customer account.
2. Execute the `patchCE` command.

   For example: `$ patchCE –i /home/cust/<patchname>.bin`

3. When prompted that the patch is service interrupting, answer **Yes** and press `Enter`.

   The patch installs. Wait for the patch installation to complete. Depending on the patch, Avaya Breeze® platform may reboot.

4. Verify the version of the installed patch. The version can be viewed in one of the following ways:
   - Log in to Avaya Breeze® platform and execute the command `patchCE -s`.

- Log in to Avaya Breeze® platform and execute the command `swversion`.
- On System Manager, click **Elements** > **Avaya Breeze®** > **Server Administration**.

5. In System Manager, click **Elements** > **Avaya Breeze®** > **Server Administration**.
6. Identify the row for the Avaya Breeze® platform server you are patching and verify the following:
   - The **Service Install Status** is a green checkmark.
   - The **Security Module** is Up.
   - The **License mode** is a green checkmark.
   - The **Version** displays the new release.

Related links

Deploying the Avaya Breeze platform OVA on page 41

Creating multiple privileged user accounts

Procedure

1. Log in to Avaya Breeze® platform with the login credentials created during the OVA deployment.
2. Type the following command: **`custAccounts -a`**
3. When prompted to add this user as an EASG administrator, type **`y`** to enable the user to run EASG commands.
4. Enter the username and a temporary password for the new customer user account you are creating.

   The password is temporary. The server prompts the user to set a new password when they first login.

Related links

Deploying the Avaya Breeze platform OVA on page 41

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

Deploying the Avaya Breeze platform OVA on page 41
Enabling and disabling EASG on page 59
Viewing the EASG certificate information on page 59
EASG site certificate on page 60

Enabling and disabling EASG

About this task

By enabling Avaya Services logins, you are granting Avaya access to your system. This allows Avaya to resolve product issues in a timely manner.

Before you begin

- You must registered the product using the Avaya Global Registration Tool (GRT) at https://grt.avaya.com. See https://support.avaya.com/registration for additional information on registering products for remote access and alarming.

Procedure

1. Log in to the Avaya Breeze® platform CLI interface using your customer account.
2. To check the status of EASG, run the command: `EASGStatus`.
3. To enable EASG, run the command: `EASGManage --enableEASG`.
4. To disable EASG, run the command: `EASGManage --disableEASG`.

Related links

Enhanced Access Security Gateway on page 58

Viewing the EASG certificate information

About this task

Use this procedure to view information about the product certificate, which includes information about when the certificate expires.

Procedure

1. Log in to the Avaya Breeze® platform CLI interface using customer account.
2. Run the following command: `EASGProductCert --certInfo`.

Related links

Enhanced Access Security Gateway on page 58

EASG site certificate

Onsite Avaya technicians use the EASG site certificates to respond to EASG challenges when accessing a server. The technician generates and provides the EASG site certificate to the customer. The customer loads the EASG site certificate onto each Avaya Breeze® platform server to which they want to grant the technician access.

The EASG site certificate only allows access for the Avaya technician. Other users, including other Avaya technicians cannot use it. After the technician completes their work, the customer can remove the EASG site certificate from the server or it is automatically removed by the EASG software when the site certificate expires.

Related links

Enhanced Access Security Gateway on page 58
Managing site certificates on page 60

Managing site certificates

Before you begin

Obtain the site certificate from the Avaya support technician and install it to Avaya Breeze® platform. Note the location of this file and use it in place of *installed_pkcs7_name* in the following commands.

Procedure

1. Log in to the Avaya Breeze® platform CLI interface using customer account.
2. To install the site certificate:
   a. Run the following command: `EASGSiteCertManage -add <installed_pkcs7_name>`.
   b. Save the Site Authentication Factor to share with the technician once on site.
3. To view information about a particular certificate: run the following command:
   - To list the site certificates installed on the system: `EASGSiteCertManage --list`
   - To display detailed information about a specified site certificate: `EASGSiteCertManage --show <installed_pkcs7_name>`
4. To delete the site certificate, run the following command:
   - To delete the specified site certificate: `EASGSiteCertManage --delete <installed_pkcs7_name>`
   - To delete all site certificates installed on the system: `EASGSiteCertManage --delete all`

Related links

EASG site certificate on page 60

Chapter 7: Avaya Breeze® platform System Manager administration

Related links

Installing the Avaya Breeze platform license file on page 61
Administering an Avaya Breeze platform SIP Entity on page 62
Administering the Avaya Breeze platform Entity Link on page 62
Enabling implicit users applications for SIP users on page 63
Administering an Avaya Breeze platform instance on page 64
Enabling IPv6 on the management interface of an Avaya Breeze platform server on page 65
Verifying the Avaya Breeze platform entity link connection on page 67
Verifying replication status on page 67
Verifying the management link on page 68
Creating a new cluster on page 68
Accepting new service on page 71
Cluster backup and restore on page 71
Reliable eventing administration on page 74

Installing the Avaya Breeze® platform license file

Procedure

1. On the System Manager web console, click **Services** > **Licenses**.
2. Click **Install license** and **Browse** to the location of the Avaya Breeze® platform license file on your computer.
3. Click **Install**.

Related links

Avaya Breeze platform System Manager administration on page 61

Administering an Avaya Breeze® platform SIP Entity

Before you begin

To complete this task, you will need the IP address of the Avaya Breeze® platform Security Module interface and the SIP Entity name.

About this task

Administer Avaya Breeze® platform as a SIP Entity so that you can configure Session Manager to route traffic through Avaya Breeze® platform.

Procedure

1. In System Manager, click **Elements** > **Routing** > **SIP Entities**.
2. Click **New**.
3. In the **Name** field, type the name of your SIP Entity.

   The SIP Entity name is automatically used as your Avaya Breeze® platform instance name when you create the Avaya Breeze® platform instance.
4. In the **FQDN or IP Address** field, type the IP address of your Avaya Breeze® platform Security Module.

   You must only enter the IP address.
5. From the **Type** drop-down menu, select `Avaya Breeze`.
6. From the **SIP Link Monitoring** drop-down menu, select `Link Monitoring Enabled`.
7. Click **Commit** to save your changes.

Next steps

Administer an Entity Link to connect Session Manager and Avaya Breeze® platform.

Related links

Avaya Breeze platform System Manager administration on page 61
Creating an FQDN SIP entity on page 85

Administering the Avaya Breeze® platform Entity Link

Before you begin

Administer Avaya Breeze® platform as a SIP Entity.

About this task

Create an Entity Link to connect Session Manager to Avaya Breeze® platform. You must administer separate Entity links for Avaya Breeze® platform servers in order to open SIP listeners on the designated ports.

Note:

You must use a common protocol for the entity links between Avaya Breeze® platform and Session Manager, and between Session Manager and Avaya Aura® Media Server. If you have multiple Avaya Aura® Media Servers with different protocols, configure two Entity Links between Avaya Breeze® platform and Session Manager for TLS and TCP.

Note:

TLS is the recommended protocol for production environments since it is secure and encrypted. Should the need arise to take a network trace between Session Manager and Avaya Breeze® platform, change the protocol to TCP. If this is a production environment, change the protocol back to TLS as soon as the trace is complete.

Procedure

1. In System Manager, click **Elements** > **Routing** > **Entity Links**.
2. Click **New**.
3. In the **Name** field, type a name for the Avaya Breeze® platform SIP Entity Link.
4. For the **SIP Entity 1** select the Session Manager.
5. For the **SIP Entity 2** select the Avaya Breeze® platform SIP Entity that you created.
6. Edit **Protocol** and **Connection policy** fields if necessary.
7. Press **Commit** to save your changes.

Related links

Avaya Breeze platform System Manager administration on page 61

Enabling implicit users applications for SIP users

About this task

This procedure is required for calling-party and called-party snap-ins.

Note:

You must perform this procedure only once.

Procedure

1. On System Manager, click **Elements** > **Session Manager** > **Global Settings**.
2. Select **Enable Implicit Users Applications for SIP users**.
3. Click **Commit**.

Related links

Avaya Breeze platform System Manager administration on page 61

Administering an Avaya Breeze® platform instance

About this task

You can create and administer the number of Avaya Breeze® platform instances allowed by the Avaya Breeze® platform license.

You set the FQDN of the Avaya Breeze® platform **Management Network Interface** to the same IP address you used when deploying the virtual machine.

System Manager supports HTTP Cookie based Single Sign On (SSO). To facilitate SSO between System Manager and Avaya Breeze® platform, the domain name component of Avaya Breeze® platform FQDN must match all or at least a part of the domain name of System Manager FQDN.

Before you begin

Ensure that you have the following:

- The IPv4 address or the FQDN of the Avaya Breeze® platform **Management Network Interface**.
- (Optional) The IPv6 address or the FQDN of the Avaya Breeze® platform **Management Network Interface**. You must enter the IPv4 address even if administering an IPv6 address.

  Important:

  During OVA deployments do not enter the IPv6 address, IPv6 network prefix, or IPv6 gateway for eth0 unless the latest Avaya Breeze® platform patches already have been applied. For more information about configuring IPv6, see “Enabling IPv6 on the management interface of an Avaya Breeze platform server” in Deploying Avaya Breeze® platform.
- An Avaya Breeze® platform management FQDN that is registered in DNS.
- The IPv4 or IPv6 address including the IPv4 network mask or IPv6 Network prefix length, and IPv4 or IPv6 default gateway for the Avaya Breeze® platform **Security Module**.
- The SIP entity name associated to the Avaya Breeze® platform **Security Module**.

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®** > **Server Administration**.
2. In the Avaya Breeze® Server Instances list, click **New**.
3. In the **SIP Entity** field, click the SIP Entity that you created.
4. Ensure that the value in the **UCID Network Node ID** field is unique across the solution deployment so that it does not conflict with other UCID-generating entities such as Avaya Aura® Communication Manager or Avaya Experience Portal.

   UCID Network Node ID is a unique, numeric node ID that is assigned to each Avaya Breeze® platform server provisioned.
5. In the Management Network Interface **FQDN or IPv4 Address** field, type the IP address or FQDN of the Avaya Breeze® platform **Management Network Interface**.
6. **(Optional)** In the Management Network Interface **FQDN or IPv6 Address** field, type the IPv6 address or FQDN of the Avaya Breeze® platform **Management Network Interface**.

7. In the Security Module fields, type the required addresses for the IPv4 or IPv6 SIP Entity Address, Network Mask or Network prefix length, and Default Gateway used for the SIP (Security Module) network.
8. Click **Commit** to save your changes.

   The Commit fails if the Avaya Breeze® platform license file on WebLM does not have the sufficient capacity to allow addition of another Avaya Breeze® platform server.
9. To put the Avaya Breeze® platform instance in service, do the following:
   a. If an in-service cluster does not exist, create a new cluster.
   b. On System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
   c. Select a cluster and assign your Avaya Breeze® platform server to the cluster.

      For more information, see “Creating a new cluster”.
   d. Click **Cluster State** > **Accept New Service**.

      For more information, see “Accepting new service”.

Related links

Avaya Breeze platform System Manager administration on page 61

Enabling IPv6 on the management interface of an Avaya Breeze® platform server

About this task

Complete this task to enable IPv6 addresses for the management interface (eth0) on an existing Avaya Breeze® platform server.

Important:

This task is service affecting. Perform these steps during a Service Maintenance window.

Before you begin

- On System Manager update Avaya Breeze® platform Element Manager to the latest Element Manager release.
- In the cluster upgrade all Avaya Breeze® platform nodes to Avaya Breeze® platform Release 3.8.1.
- Have unique IPV6 addresses for all nodes in the cluster. All IP addresses must be in the same subnet.
- Have the IPV6 address prefix and IPV6 gateway address that can route the IPv6 addresses.

Procedure

1. Log in to System Manager as admin.

2. In System Manager, click **Elements** > **Avaya Breeze®** > **Server Administration**.
3. Select the Avaya Breeze® platform node where you want to assign the IPv6 address to the management interface and click **Edit**.
4. In the **FQDN or IPv6 Address** field under Management Network Interface, enter a unique IPv6 address and click **Commit**.

   When configuring an IPv6 address, an IPv4 address is also required.
5. Repeat steps 3 and 4 for all Avaya Breeze® platform nodes in the cluster.

   When an IPv6 address is configured on the management interface of an Avaya Breeze® platform node, all Avaya Breeze® platform nodes in the cluster must also have IPv6 addresses.
6. In System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
7. Select the cluster and click **Cluster State** > **Deny New Service** to put the cluster in a Deny New Service state.
8. Remove the Avaya Breeze® platform node from the cluster.
   a. If the node being removed is the Cluster Database active server, it must switch over to standby. Click **Show** to list the servers in the cluster, and click **Standby** to promote the standby server to active.
   b. If a Reliable Eventing Group is assigned to the node being removed, edit the group to unassign the node.

      On the **Reliable Eventing Administration** page, click **Dashboard**. Edit the reliable eventing group, remove the node from Assigned Brokers, and click **Commit**.
   c. From the **Cluster Administration** page, select the cluster, click **Edit**, and click the **Servers** tab. Click **X** to remove the node from the cluster and click **Commit**.
9. Log in to the Avaya Breeze® platform node using its IPv4 management IP address and run the **`CEnetSetup`** command.
   a. When **`CEnetSetup`** shows the option to configure IPv6 addressses, enter the IPv6 address for the eth0 interface.
   b. When prompted by **`CEnetSetup`**, provide the IPv6 address network prefix and IPv6 gateway address.

      You also can configure other options that **`CEnetSetup`** presents.

   `CEnetSetup` makes the necessary configuration changes and reboots the Avaya Breeze® platform node.
10. After the Avaya Breeze® platform node reboots, log in to System Manager and add the node back into the cluster.

    Wait for all services to deploy on the node.

Related links

Avaya Breeze platform System Manager administration on page 61

Verifying the Avaya Breeze® platform entity link connection

About this task

Complete this task to verify that Session Manager can connect with Avaya Breeze® platform using the SIP entity link. To do this you must first verify the status of SIP link monitoring on the Session Manager instance.

Procedure

1. Modify the Session Manager Instance.
   a. On System Manager, click **Elements** > **Session Manager** > **Session Manager Administration**.
   b. Select the Session Manager instance that you linked to Avaya Breeze® platform. Click **Edit**.
   c. Check **Enable Monitoring** in the **Monitoring** section.
   d. Click **Commit**.
2. Test the entity link.
   a. On System Manager, click **Elements** > **Session Manager** > **System Status** > **SIP Entity Monitoring**.
   b. Click the name of the Session Manager instance that you linked to Avaya Breeze® platform.

      The system displays a list with the status of all the entity links for the selected Session Manager.
   c. Locate the Avaya Breeze® platform SIP entity and check the **Conn. Status** column.
      - If you see `UP`, the link to Session Manager is successful.
      - If you do not see `UP`, for additional information, see *Avaya Breeze® platform FAQ and Troubleshooting for Service Developers*.

Related links

Avaya Breeze platform System Manager administration on page 61

Verifying replication status

About this task

Complete this task to verify that the System Manager database has replicated to Avaya Breeze® platform.

Procedure

1. In System Manager, click **Services** > **Replication**.
2. Locate the Avaya Breeze® platform in the **Replica Group** list.
3. In the **Synchronization Status** column, verify that the Avaya Breeze® platform status is `Synchronized`.
   - Depending on the amount of data, the replication takes time to complete. Refresh the page periodically to check the status.
   - If the status is not `Synchronized`, for more information, see Maintaining and Troubleshooting Avaya Breeze® platform.

Related links

Avaya Breeze platform System Manager administration on page 61

Verifying the management link

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®** > **Server Administration**.
2. Check the **Tests Pass** column.
   - A green check mark indicates that the management link is up and healthy.
   - Dashes indicate that the management link is still initializing and is not up yet.
   - A red cross indicates that the management link is down.

   For more information, see Maintaining and Troubleshooting Avaya Breeze® platform.

Related links

Avaya Breeze platform System Manager administration on page 61

Creating a new cluster

Before you begin

Load the required services or bundles for your cluster on the Service Management page.

About this task

Use the Cluster Editor page to:

- Select a cluster profile.
- Configure the cluster attributes.
- Add Avaya Breeze® platform servers to a cluster.

- Install snap-ins on a cluster.
- Subscribe to Reliable Eventing groups that are already created.

You must set up user name and password for Avaya Aura® Media Server if basic authentication is used in Avaya Aura® Media Server administration.

Warning:

Avaya Breeze® platform supports VMware HA, but different applications running on Avaya Breeze® platform may not. Refer to the application deployment guide before deploying Avaya Breeze® platform into an HA-enabled data center. For applications that do not support VMware HA, Avaya Breeze® platform itself can provide an HA solution if each node in a cluster is deployed on a different VMware host.

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, click **New**.
3. On the Cluster Editor page, select the cluster profile of your choice.

   Note:

   You must select a cluster profile to view the appropriate cluster attributes.

   For example, select the general purpose cluster profile or a product specific cluster profile.

   Refer to the snap-in reference documentation for the cluster profile appropriate for the use case being deployed.
4. Enter the cluster attributes for your cluster. You can edit the default cluster attributes the system displays.

   The name and the IP address of a cluster must be unique.

   You cannot edit all the cluster attributes. Some attributes are read-only.

   Note:

   Do not assign a **Cluster IP** for a single-node cluster.
5. If you will be installing snap-ins that use the cluster database, select the **Enable Cluster Database** check box.

   Note:

   If you attempt to install a snap-in using the cluster database on a cluster that has the **Enable Cluster Database** feature disabled, the installation will be blocked.
6. In the **Minimum TLS Version for SIP Call Traffic** field, specify the TLS version which will be used for SIP calls intercepting Avaya Breeze® platform.
7. In the **Minimum TLS Version for Non-SIP Call Traffic** field, specify the TLS version which will be applied for HTTP requests to Avaya Breeze® platform.
8. (Optional) Click the **Servers** tab to assign Avaya Breeze® platform servers to the cluster.

Important:

Do not assign servers with different releases to the same cluster. All servers in the cluster should be running the same Avaya Breeze® platform version.

For more information on upgrading clusters, see Upgrading Avaya Breeze® platform.

9. **(Optional)** Click the **Services** tab to assign snap-ins to this cluster.

   When you assign snap-ins to a cluster, the highest version of the required snap-ins are automatically assigned to the cluster for installation. For the product specific cluster profiles, you must load the required snap-ins from the Service Management page before you install the snap-in.

   In the **Select TLS Version for Selected Snap-in** field, select the TLS version of the snap-in:

   - **Default**

     If you select **Default**, the Avaya Breeze® platform uses the **Minimum TLS Version** field value set in the System Manager global configuration.

   - **TLS v1.0**
   - **TLS v1.2**
   - **TLS v1.3**

     Avaya recommends using TLS v1.3.

10. **(Optional)** Click the **Reliable Eventing Groups** tab to add the Reliable Eventing Groups that you have already created.

    In the **Available Reliable Eventing Groups** table, click the **+** icon adjacent to a group.

    Selecting a Reliable Eventing Group would enable the snap-ins installed in the cluster to get connection details to the eventing group and use that to send/receive inter-cluster events.

11. Click **Commit** to create the cluster.

    The **Service Install Status** in the Cluster Administration page displays a green tick symbol after all the assigned snap-ins are successfully installed on all the servers in the cluster.

    To view the Avaya Breeze® platform servers in the cluster, click **Show** in the **Details** column of the cluster. The system displays the members of the cluster, and the status of each instance in the cluster.

    Click a specific Avaya Breeze® platform server to go to the Avaya Breeze® Instance Editor page. You can view and edit the properties of the Avaya Breeze® platform server from this page.

Note:

When you administer a new Avaya Breeze® platform server, you must add the server to a cluster. If you do not add the Avaya Breeze® platform server to a cluster, you cannot install snap-ins on that server.

Related links

Avaya Breeze platform System Manager administration on page 61

Accepting new service

About this task

The steps for returning the server to service are different depending on if the server is being added to an existing in-service cluster or if it is being added as part of a new cluster. Follow the steps appropriate to your situation.

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. Select a cluster and assign your Avaya Breeze® platform server to the cluster.
3. If this is a new cluster, put the cluster in service.
   a. From the **Cluster State** drop-down menu, select **Accept New Service**.
   b. Verify that the **Cluster State** column for the cluster changed to **Accepting**.
4. If you are adding the server to an existing cluster that is in service, accept service for the server.
   a. On System Manager, click **Elements** > **Avaya Breeze®** > **Server Administration**.
   b. Click the checkbox in front of the new server.
   c. From the **System State** drop-down menu, select **Accept New Service**.
   d. Verify that the **System State** column for the server changed to **Accepting**.

Related links

Avaya Breeze platform System Manager administration on page 61

Cluster backup and restore

The following sections cover cluster backup and restoration.

Related links

Avaya Breeze platform System Manager administration on page 61
Backing up a cluster database on page 72

Restoring the cluster database on page 73
Cancelling a pending job on page 73
Purging a backup on page 73

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**.

Related links

Cluster backup and restore on page 71

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**.

Related links

Cluster backup and restore on page 71

Cancelling a pending job

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. Click **Backup and Restore** > **Cancel**

   The system displays the Backup and Restore Status page.
3. Select the pending job to be cancelled, and click **Cancel**.
4. Click **Continue**.

Related links

Cluster backup and restore on page 71

Purging a backup

Before you begin

The backup to be purged must be complete.

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. Click **Backup and Restore** > **Purge**.

   The system displays the Backup and Restore Status page.
3. Select the backup and click **Purge**.

The system displays `Warning: Purged backups will no longer be available for restore.`

4. Click **Confirm**.

Related links

Cluster backup and restore on page 71

Reliable eventing administration

The 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 a richer set of capabilities like reliability, asynchronous events, inter-node, and inter-cluster which are not available in Eventing Framework.

Reliable eventing framework provides the following additional features beyond what a standard eventing framework provides:

- Enables delivery of events across servers and clusters.
- Guarantees event delivery with event persistence, acknowledgement, and durable subscriptions.
- High availability of nodes with replicated persistent messages.

Related links

Avaya Breeze platform System Manager administration on page 61
Creating a Reliable Eventing group on page 74
Editing a Reliable Eventing group on page 75
Deleting a Reliable Eventing group on page 75
Viewing the status of Reliable Eventing destinations on page 76
Deleting a Reliable Eventing destination on page 76
Running a maintenance test for a broker on page 76

Creating a Reliable Eventing group

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®** > **Reliable Eventing Administration** > **Dashboard**.
2. Click **New**.
3. Enter the following details:
   - **Cluster**: Select the cluster on which you want to create the Reliable Eventing group.
   - **Group Name**: Assign a name to the Reliable Eventing group.

- **Description**: Enter a brief description.
- **Type**: Select **HA** or **Standalone**.
  - If you select **HA**, you must select at least three Avaya Breeze® platform nodes or brokers.
  - If you select **Standalone**, you must select at least one Avaya Breeze® platform node or broker.

4. In the Unassigned Brokers table, click **+** to assign the Avaya Breeze® platform nodes or brokers to the Reliable Eventing group.
5. Click the Associated clusters tab:
   a. In the **Unassigned associated clusters** table, click **+** to add an associated cluster.
   b. In the **Assigned associated clusters** table, click **X** to remove an associated cluster.
6. Click **Commit**.

   The **Status** column displays one of the following:

   - ✔: Indicates that the status of the broker is up and running for subscription and event transfers.
   - ⛔: Indicates that the status of the broker is down.

Related links

Reliable eventing administration on page 74

Editing a Reliable Eventing group

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®** > **Reliable Eventing Administration** > **Dashboard**.
2. Select the **Reliable Eventing group** and click **Edit**.
3. Assign new brokers or remove existing brokers.
4. Click the Associated clusters tab:
   a. In the **Unassigned associated clusters** table, click **+** to add an associated cluster.
   b. In the **Assigned associated clusters** table, click **X** to remove an associated cluster.
5. Click **Commit**.

Related links

Reliable eventing administration on page 74

Deleting a Reliable Eventing group

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®** > **Reliable Eventing Administration** > **Dashboard**.

2. Select the **Reliable Eventing group** and click **Delete**.
3. In the Confirm Delete window, click **Continue**.

Related links

Reliable eventing administration on page 74

Viewing the status of Reliable Eventing destinations

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Reliable Eventing Administration** > **Destination Status**.

   The Broker Destination Status page is displayed.
2. To view the destination status, from **Group**, select the Reliable Eventing group.

Related links

Reliable eventing administration on page 74

Deleting a Reliable Eventing destination

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®** > **Reliable Eventing Administration** > **Destination Status**.
2. In the **Group** field, select the **Reliable Eventing group**.

   The system displays the destination status.
3. Select a **Destination** and click **Delete**.
4. Click **Commit**.

   The system purges the messages and deletes the destination.

Related links

Reliable eventing administration on page 74

Running a maintenance test for a broker

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®** > **System Tools and Monitoring** > **Maintenance Tests**.
2. In the **Select Avaya Breeze to test** field, click the Avaya Breeze® platform instance that you want to test.
3. Select the **Test Reliable Eventing Framework** check box.
4. Click **Execute Selected Tests**.

Avaya Breeze® platform displays one of the following statuses:

- `Failure` when Reliable Eventing is down. That is, publishing and receiving messages by Reliable Eventing is failing.
- `Success` when Reliable Eventing is functional. That is, publishing and receiving messages by Reliable Eventing is working.

Related links

Reliable eventing administration on page 74

Chapter 8: Certificate administration

Related links

Trust and Identity Certificate administration on page 78
Viewing Identity Certificate details on page 79
Adding a trusted certificate to all Avaya Breeze platform servers in a cluster on page 80
Adding trusted CA certificates on page 81
Replacing an identity certificate on page 82

Trust and Identity Certificate administration

You can administer both Trust Certificates and Identity Certificates for Avaya Breeze® platform.

Identity Certificates are administered individually for Avaya Breeze® platform clusters. Five default Identity Certificates are generated as part of the Avaya Breeze® platform OVA deployment process. You can replace a default certificate with a certificate from a well-known certificate authority.

The Security Module (ASSET) HTTP certificate is the one that is visible to applications and endpoints. If using HTTPS with hostname validation checks, you will need to replace the default ASSET HTTP certificate. When replacing the certificate, edit the Subject Alternative Name field to include both the FQDN assigned to the Avaya Breeze® platform server and the FQDN assigned to the cluster.

For instructions for replacing a certificate and changing the Subject Alternative Name (SAN), see “Replacing an identity certificate”.

Note:

Starting with Avaya Breeze® platform 3.9.0.3, hostname validation behavior has changed. 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.

Entities that access Avaya Breeze® platform via HTTPS must be able to resolve the Subject Alternative Name (SAN) entries in the certificate with the Fully Qualified Domain Names (FQDNs) of the Avaya Breeze® platform nodes. If you use the default certificates generated by System Manager, the CN in the certificate will look like: `<serverHostName>-sm100.<domain>`, where host and domain are those specified when you installed the server (or specified during

CEnetSetup). If a different certificate has been installed, the FQDN is whatever was specified in CN and/or SAN when generating that certificate.

If you change the Avaya Breeze® platform hostname or domain name, you need to re-create and install the certificates with updated CN and SAN. For more information, see *Managing Certificates*.

To view the Security Module HTTPS Certificate details, including the CN, for the Avaya Breeze® platform server, see “Viewing Identity Certificate details”.

To resolve the certificate CN or SAN fields with the FQDN, take one of the following actions:

- Enter the FQDN of each Avaya Breeze® platform node in your DNS server.
- Populate the host file of each entity with the FQDN of each Avaya Breeze® platform node that it will access.

Note:

You can edit the Avaya Aura® Media Server host files through the Avaya Aura® MS Element Manager. For more information, see “Configuring Avaya Aura® Media Server name resolution (alternative 1)”.

You can administer the Trust Certificates for each Avaya Breeze® platform cluster or a single Trust Certificate can be assigned simultaneously to all the clusters.

For more information about Trust and Identify Certificates, click **Help** on the System Manager interface and select **Managing Certificates**. For detailed information about migrating from the Avaya Certificate Authority to a Well-known Certificate Authority, see *Avaya Aura® Certificate Migration*.

About WebSphere Identity Certificate:

The OVA deployment of Avaya Breeze® platform 3.9.0.3 and higher automatically includes the minimum required SAN fields. For systems 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 Identity Certificate does not include Avaya Breeze® platform Management FQDN (mgmt-fqdn) and its corresponding IP address in SAN field. The WebSphere identity certificates that do not contain this SAN value will not function correctly. When replacing the certificate, edit the Subject Alternative Name field to include the Breeze Management FQDN assigned to the Avaya Breeze® platform server.

Related links

Certificate administration on page 78

Viewing Identity Certificate details

Procedure

1. In System Manager, click **Services** > **Inventory** > **Manage Elements**.
2. Click the checkbox in front of the Avaya Breeze® platform server.

3. From the **More Actions** menu, select **Configure Identity Certificates**.
4. In the list of certificate, click the Security Module HTTPS certificate.

   Certificate Details for the Security Module HTTPS certificate display below the certificate list.
5. To exit the screen, click **Done**.

Related links

Certificate administration on page 78

Adding a trusted certificate to all Avaya Breeze® platform servers in a cluster

Before you begin

Certificates that you intend to add as trusted certificates must be accessible in System Manager.

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. Select the cluster for which you want to administer the trusted certificates.
3. Click **Certificate Management** > **Install Trust Certificate (All Avaya Breeze® Instances)** to download the trusted certificates to all the servers in the cluster.
   - The trusted certificates that you add apply to all Avaya Breeze® platform servers assigned to the cluster.
4. From the **Select Store Type to install trusted certificate** menu, select the appropriate store type.
5. Click **Choose file** to navigate to the location of your trusted certificate, and then select the certificate.
6. Click **Retrieve Certificate** and review the details of the trusted certificate.
7. Click **Commit**.

Related links

Certificate administration on page 78

Adding trusted CA certificates

About this task

Use this procedure to import a trusted CA certificate. You can import trusted CA certificate using one of the following options:

- from a file.
- by copying the contents of a PEM file.
- from a list of an existing certificates.
- from a remote location using a TLS connection.

Procedure

1. In System Manager, click **Services** > **Inventory** > **Manage Elements**.
2. Select an Avaya Breeze® platform instance.
3. Click **More Actions** > **Configure Trusted Certificates** .
4. On the Trusted Certificates page, click **Add**.
5. To import a certificate from a file:
   a. Click **Import from file**.
   b. Click **Browse** and locate the file.
   c. Click **Retrieve Certificate**.
   d. Click **Commit**.
6. To import a certificate in the PEM format:
   a. Select **Import as PEM Certificate**.
   b. Locate the PEM certificate.
   c. Open the certificate using Notepad.
   d. Copy the entire contents of the file. You must include the start and end tags:

      -----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE----.
   e. Paste the contents of the file in the box provided at the bottom of the page.
   f. Click **Commit**.
7. To import certificates from existing certificates:
   a. Click **Import from existing**.
   b. Select the certificate from the Global Trusted Certificate section.
   c. Click **Commit**.
8. To import certificates using TLS:
   a. Click **Import using TLS**.

b. Enter the IP Address of the location in the **IP Address** field.
c. Enter the port of the location in the **Port** field.
d. Click **Retrieve Certificate**.

9. Click **Commit**.

Related links

Certificate administration on page 78

Replacing an identity certificate

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an element and click **More Actions** > **Manage Identity Certificates**.
4. On the Manage Identity Certificates page, select the certificate that you want to replace.
5. Click **Replace**.

   On the Replace Identity Certificate page, select one of the following:

   - **Replace this Certificate with Internal CA Signed Certificate**
   - **Import third party certificate**
   - **Generate Certificate Signing Request (CSR) for third party certificate**

6. 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. **(Optional)** In **Subject Alternative Name**, select the relevant options and enter the details.
   d. **(Optional)** In **OtherName**, type the other name for the certificate signing request.
   e. To replace the identity certificate with the internal CA signed certificate, click **Commit**.
7. Click **Import third party certificate**, and do the following:
   a. In the **Please select a file** field, choose the file from your local computer.
   b. In the **Password** field, type the password.
   c. Click **Retrieve Certificate**.

      The Certificate Details section displays the details of the certificate.

d. Review the details of the uploaded certificate.

e. To replace the certificate with the third-party certificate that you imported, click **Commit**.

8. Click **Generate Certificate Signing Request (CSR) for third party 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. **(Optional)** In **Subject Alternative Name**, select the relevant options and enter the details.

   d. In **OtherName**, type the other name for the certificate signing request.

   e. Click **Generate CSR**.

   f. Ensure that the downloaded CSR is third-party signed.

   g. Import the signed certificate using the **Import third party certificate** option.

9. For the newly generated certificates to take effect, restart the System Manager Application server.

Related links

Certificate administration on page 78

Chapter 9: Avaya Breeze® platform HA administration

High Availability (HA) is achieved for Avaya Breeze® platform by sending traffic to a cluster with multiple servers. Load balancing determines what percentage of traffic each server receives. Clusters are auto-configured with the datagrid and the HTTP load balancing functionality.

- You must enable HTTP load balancing for a cluster; by default load balancing is not enabled.
- SIP load balancers are not configured in the servers and clusters. For SIP high availability, you must manually configure load balancing.

Related links

SIP High Availability on page 84
HTTP High Availability on page 90

SIP High Availability

SIP HA is possible with Avaya Breeze® platform by administering a cluster of Avaya Breeze® platform servers and connecting each member of the cluster to each Session Manager. You can then route users of a service to the cluster rather than to a specific Avaya Breeze® platform server so it is likely that at least one will be available.

When you administer an Avaya Breeze® platform cluster, each Avaya Breeze® platform server is entered in a table of local host names, along with a priority and weight for each.

When the cluster database is enabled with three or more servers, assign weights to servers for load balancing in the recommended percentages.

The cluster load balancer is only used for HTTP, not for SIP. Session Manager acts as the load balancer for SIP traffic. To enable Session Manager to fulfill this function, an FQDN must be populated in the **Local Host Name Resolution** table, and each Avaya Breeze® platform security IP address must be associated with this FQDN. This FQDN must be used when creating the FQDN SIP entity.

Related links

Avaya Breeze platform HA administration on page 84
Avaya Breeze platform SIP HA deployment checklist on page 85
Creating an FQDN SIP entity on page 85
Creating an FQDN entity link on page 86

Creating an application and application sequence for HA on page 87
Determining active and standby database servers on page 88
Resolving the local host name for HA on page 88
Local load balancing recommendation on page 89

Avaya Breeze® platform SIP HA deployment checklist

The following checklist lists the procedures required to deploy Avaya Breeze® platform in a SIP HA configuration:

#	Action	Reference/Notes	✔
1	Create an FQDN SIP entity.	Creating an FQDN SIP entity on page 85	
2	Create the FQDN entity link.	Creating an FQDN entity link on page 86	
3	Create a high availability application and application sequence.	Creating an application and application sequence for HA on page 87	
4	Resolve the local host name.	Resolving the local host name for HA on page 88	
5	Enable load balancing for the cluster.	Enabling HTTP load balancing in an Avaya Breeze platform cluster on page 91	

Related links

SIP High Availability on page 84

Creating an FQDN SIP entity

Before you begin

To complete this task, you will need the FQDN of the Avaya Breeze® platform cluster. In addition to creating this FQDN SIP entity for the cluster, you must also create a separate SIP entity for each Avaya Breeze® platform instance in the cluster.

Procedure

1. In System Manager, click **Elements** > **Routing** > **SIP Entities**.
2. Click **New**.
3. In the **Name** field, type the name of your SIP entity.
4. In the **FQDN or IP Address** field, type the FQDN of your Avaya Breeze® platform cluster.

   Caution:

   Do not use the load balancer IP address for the FQDN SIP entity. The cluster load balancer is only used for HTTP traffic, not SIP traffic.
5. In the **Type** field select `Other`.

6. Click **Commit** to save your changes.

Related links

SIP High Availability on page 84
Administering an Avaya Breeze platform SIP Entity on page 62

Creating an FQDN entity link

About this task

For an Avaya Breeze® platform cluster, create a single entity link for the FQDN SIP entity. You must create an entity link for each Avaya Breeze® platform server in the cluster using the HA configuration. Do not use the default port 5061 on Session Manager for the entity link between the cluster and the Session Manager server.

Note:

TLS is the recommended protocol since it is secure and encrypted. Should the need arise to take a network trace between Session Manager and Avaya Breeze® platform, change the protocol to TCP and then change it back to TLS as soon as the trace is complete.

Before you begin

Create the FQDN SIP Entity.

Procedure

1. In System Manager, click **Elements** > **Routing** > **Entity Links**.
2. Click **New**.
3. In the **Name** field, type a name for the SIP entity link.
4. In the **SIP Entity 1** field, select the Session Manager.
5. In the **Protocol** field, select the desired protocol.
6. In the **Port** field, enter a unique port number.

   Do not use the Session Manager port number that is administered for the entity link connecting Session Manager and Avaya Breeze® platform. For example, if you used 5061 as the Session Manager port in the entity link administration representing your Session Manager to your specific Avaya Breeze® platform server, use a different port value here, such as 5091. This represents the Session Manager side of the HA FQDN entity link.

   Caution:

   The consequences for using a non-unique port can be severe. If you use the same port number, the system will generate the error message “500 Server Internal Error (Indeterminate originating entity).” This error causes Session Manager to try to alternate route to another server in the cluster.
7. In the **SIP Entity 2** field, select the Avaya Breeze® platform HA FQDN SIP Entity that you created.

8. In the **Port** field, enter the same port that you specified in Administering the Avaya Breeze platform Entity Link on page 62.

   For example if you used 5061 as the Avaya Breeze® platform port of the Session Manager to your specific Avaya Breeze® platform entity link, then use 5061 as the Avaya Breeze® platform port in the HA FQDN entity link as well.

9. Click **Commit** to save your changes.
10. In System Manager, click **Elements** > **Routing** > **SIP Entities**.
11. Select the Session Manager SIP entity that you created a link to and click **Edit**.

    Repeat these steps for each SIP entity that you created a link to.

12. Under Listen Port, click **Add**.
13. Enter the port number and protocol that you selected for the entity link above.
14. From **Default Domain**, select the root domain used for call routing.
15. Click **Commit**.

Related links

SIP High Availability on page 84

Creating an application and application sequence for HA

By administering the Avaya Breeze® platform cluster as an application you can add it to an application sequence.

About this task

By administering the Avaya Breeze® platform cluster as an application you can add it to an application sequence. You can then add this application sequence to the implicit user table so that called and caller application requests route to a cluster of Avaya Breeze® platform servers rather than an individual Avaya Breeze® platform server.

Procedure

1. In System Manager, click **Elements** > **Session Manager** > **Application Configuration** > **Applications**.
2. Click **New**.
3. Type a name for the application.
4. For the **SIP Entity**, select the Avaya Breeze® platform cluster.
5. To save your changes, click **Commit**.
6. On the **Session Manager** menu under **Application Configuration** click **Application Sequences** and click **New**.
7. Type the name of your new application sequence.
8. In the list of **Available Applications** click **+** by the Avaya Breeze® platform application that you created.

9. **(Optional)** Deselect the **Mandatory** check box..

   Session Manager stops processing a call if it cannot reach a mandatory application.

10. To save your application sequence, click **Commit**.

Related links

SIP High Availability on page 84

Determining active and standby database servers

About this task

For load balancing configuration, you must be able to identify your active and standby cluster database servers. Use this information to determine what weight you will specify for each server for load balancing.

The servers that host the cluster database are selected when the servers are added to a cluster. If the active database server fails, Avaya Breeze® platform promotes the standby server to active. If the standby database server fails, no action is taken. The only occurrence that causes another server in the cluster to be selected as a replacement active or standby database is when one of the current database hosts is removed from the cluster.

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. Click **Show** in front of the cluster you are administering to see the servers in the cluster.
3. In the Cluster Database column, identify the active and standby database servers.

   Active is the primary server
   Standby is the secondary server
   All additional servers in the cluster are marked as Idle

Related links

SIP High Availability on page 84

Resolving the local host name for HA

Procedure

1. Verify that at least one entity link has been defined for each FQDN and Transport entry.
2. In System Manager, click **Elements** > **Session Manager** > **Network Configuration** > **Local Host Name Resolution**.
3. Click **New**.
4. Enter the host information on the New Local Host Name Entries page.

   You can enter a maximum of ten host names.

   a. For the **Host Name (FQDN)**, enter the FQDN or IP address of the host. The host name entries override the information provided by DNS.

b. Enter the IP address that the host name is mapped to. A host can be mapped to more than one IP addresses and each of these mappings are a separate entry.
c. Enter the port number that the host should use for routing using the particular IP address.
d. Enter a value in **Priority**. If there are multiple IP address entries for a given host, Session Manager tries the administered IP addresses in the order of the priority.
e. Enter a value in **Weight**. If there are multiple IP address entries for a given host, and if some entries have the same priority, then for each priority level, Session Manager chooses a host according to the specified weights.

   For systems with the cluster database enabled, see the local load balancing recommendations. For systems with geographical redundancy, see the geo-redundancy example configuration for **Priority** and **Weight** suggestions.
f. Select the transport type.

   The default is TLS.

5. Click **Commit**.

Related links

SIP High Availability on page 84
Local load balancing recommendation on page 89
Geo-redundancy load balancing example configuration on page 89

Local load balancing recommendation

When the cluster database is enabled, use the following table to determine the load balancing weight to assign to each server in the cluster. Use this table only for local load balancing, not for geographic redundancy clusters.

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

Related links

Resolving the local host name for HA on page 88

Geo-redundancy load balancing example configuration

The following is an example of cluster provisioning for a North American cluster and a European cluster that are providing geo-redundancy for each other.

Avaya Breeze® platform high availability is not call preserving but it is connection preserving. This example assumes that the Cluster Database and Load Balancer are running on these clusters and that they are assigned to the first two nodes ((NA-CE1-IP-Addr, NA-CE2-Addr for the North America cluster and EU-CE1-IP-Addr, EU-CE2-IP-Addr for the European cluster).

Host Name	IP Address	Priority	Weight
NA-CE.example.com	<NA-CE1-IP-Addr>	1	25
NA-CE.example.com	<NA-CE2-IP-Addr>	1	25
NA-CE.example.com	<NA-CE3-IP-Addr>	1	50
NA-CE.example.com	<EU-CE1-IP-Addr>	2	25
NA-CE.example.com	<EU-CE2-IP-Addr>	2	25
NA-CE.example.com	<EU-CE3-IP-Addr>	2	50
EU-CE.example.com	<EU-CE1-IP-Addr>	1	25
EU-CE.example.com	<EU-CE2-IP-Addr>	1	25
EU-CE.example.com	<EU-CE3-IP-Addr>	1	50
EU-CE.example.com	<NA-CE1-IP-Addr>	2	25
EU-CE.example.com	<NA-CE2-IP-Addr>	2	25
EU-CE.example.com	<NA-CE3-IP-Addr>	2	50

Related links

Resolving the local host name for HA on page 88

HTTP High Availability

Related links

Avaya Breeze platform HA administration on page 84
HTTP load balancing in an Avaya Breeze platform cluster on page 90
Enabling HTTP load balancing in an Avaya Breeze platform cluster on page 91
External load balancer for HTTP Geo-redundancy on page 92

HTTP load balancing in an Avaya Breeze® platform cluster

Enable load balancing for a cluster if you want to scale the HTTP services without targeting a particular Avaya Breeze® platform server. All the requests are sent to the cluster IP address. When you enable load balancing, two Avaya Breeze® platform servers are chosen as the active and standby load balancing servers. The active load balancer distributes the HTTP requests to all the other servers in the cluster in a round robin fashion.

The following cluster attributes must be configured for HTTP load balancing:

Name	Description
HTTP Load Balancer backend server max failure response timeout period (seconds)	The maximum timeout period of the failure response of the HTTP Load Balancer backend server. The default value is 15.

Table continues…

Name	Description
Max number of failure responses from HTTP Load Balancer backend server	The maximum number of failure responses from the HTTP Load Balancer backend server. The default value is 2.
Network connection timeout to HTTP Load Balancer backend server (seconds)	The network connection timeout period from the HTTP Load Balancer backend server. The default value is 10.

Load balancing validations

The following are the validations when you enable load balancing in a cluster:

- Load balancing is not supported in a single server cluster.
- By default the load balancing check box is not selected.
- For load balancing to function, the cluster must have two Avaya Breeze® platform servers that have the SIP Entity IP addresses in the same subnet as the cluster IP address. The active server starts a network alias using the cluster IP address. If the active server is down, the standby starts a network alias with the cluster IP address. The standby server takes over as the active load balancer.
- With load balancing, you cannot remove the active or the standby Avaya Breeze® platform server from the cluster unless another server in the cluster meets the subnet validation.

Session affinity

Session affinity ensures that all the requests from the same client are directed to the same back end Avaya Breeze® platform server in a cluster. Session affinity is mandatory for snap-ins like the WebRTC Connect.

To enable session affinity, select the **Is session affinity** cluster attribute.

Use the Trusted addresses for converting to use X-Real-IP for session affinity cluster attribute to enter trusted addresses that are known to send correct replacement addresses so thatAvaya Breeze® platform load balancer can use the real client IP when an HTTP request traverses through reverse proxies like Avaya Session Border Controller. The header which is used to identify the real client IP address is X-Real-IP

Related links

HTTP High Availability on page 90

Enabling HTTP load balancing in an Avaya Breeze® platform cluster

About this task

You do not need to enable load balancing if you are using an external load balancer or if you are running a single server cluster.

Procedure

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

2. **(Optional)** To enable load balancing for an existing cluster, on the Cluster Administration page, do the following:
   a. Select the check box in front of the cluster.
   b. In the **Cluster State** field, click **Deny New Service**.
   c. Verify that the **Cluster State** column for the cluster is changed to **Denying**.
   d. Click **Edit**.
3. **(Optional)** To create a new cluster with load balancing enabled, on the Cluster Administration page, do the following:
   a. Click **New**.
   b. Specify the attributes of the cluster.
4. In the Cluster Attributes section, select the **Is Load Balancer enabled** check box to enable load balancing.
5. In the Basic section **Cluster IP** field, type the IP address of the cluster.

   The cluster IP address used for load balancing must be unique. The security module IP address must be on the same subnet as the cluster IP address.
6. Click **Commit**.

   Two Avaya Breeze® platform servers are automatically designated as active and standby to perform the load balancing functionality.
7. On the Cluster Administration page, in the **Cluster State** field, click **Accept New Service**.

Related links

HTTP High Availability on page 90

External load balancer for HTTP Geo-redundancy

Session Manager can be used to achieve geo-redundancy for SIP signaling across Avaya Breeze® platform clusters. Similarly, an external HTTP load balancer or Application Gateway can be used. Multiple Avaya Breeze® platform clusters are configured exactly the same and deployed in different regions. An FQDN is defined for each region. The external load balancer is configured with both of these FQDNs. Each FQDN includes the cluster IP address for both Breeze clusters, but in a different preferential order. Each FQDN prefers the local cluster's IP address, with the other cluster's IP address being the second choice.

Browsers or other clients that access Avaya Breeze® platform HTTP services can use the FQDN associated with their local Avaya Breeze® platform cluster. When the load balancer receives this request, the load balancer routes the request to the local Avaya Breeze® platform cluster if available. If the local cluster is not available, the load balancer routes to the remote cluster. In either case, the local Avaya Breeze® platform load balancer distributes the request to one of the Avaya Breeze® platform machines in the cluster.

Some Avaya Breeze® platform snap-ins use a Avaya Breeze® platform-specific affinity mechanism that is not supported by external load balancers. Therefore, this configuration is not a supported

configuration to use an external HTTP load balancer to distribute HTTP requests to individual Avaya Breeze® platform servers in the cluster as opposed to addressing the cluster IP address.

Related links

HTTP High Availability on page 90

Chapter 10: Communication Manager call routing

Calls to or from non-SIP endpoints on Communication Manager over ISDN trunks are not routed by default through Session Manager and so do not have access to Avaya Breeze® platform Call Intercept services. However, you can administer Communication Manager to route Public Switched Telephone Network (PSTN) ISDN calls through Session Manager for Avaya Breeze® platform processing.

This procedure is necessary only when Call Intercept services are used on calls between stations and ISDN trunks on the same Communication Manager instance.

For detailed instructions for any of the procedures described in this section, see your Communication Manager documentation.

Related links

Routing inbound ISDN calls on page 94
Routing outbound ISDN calls on page 95

Routing inbound ISDN calls

To route incoming Communication Manager ISDN PSTN calls to Avaya Breeze® platform for services, divert all inbound calls to Session Manager using already configured SIP trunks. In this way, the calls route to Session Manager and from there to Avaya Breeze® platform.

Before you begin

To complete this task you must have:

- An administered Automatic Alternate Routing (AAR) and Feature Access Code (FAC)
- A SIP trunk group between Communication Manager and Session Manager
- A route pattern administered to route calls to this SIP trunk group

Procedure

1. Using the Incoming Call Handling Treatment table, prepend your AAR FAC to the received digits of your ISDN trunk group.

   This will route calls from your ISDN trunk group to AAR treatment.

2. Use AAR analysis to route ISDN trunk group inbound calls to a route pattern that routes calls to your SIP trunk group.

Related links

Communication Manager call routing on page 94

Routing outbound ISDN calls

Route outbound calls to Session Manager instead of routing them to the PSTN ISDN trunk. Calls route to Session Manager and from there to Avaya Breeze® platform. Then the calls are routed back to the Communication Manager ISDN trunk group with digits added to prevent the calls from looping back to Session Manager.

Before you begin

To complete this task you must have:

- An administered Automatic Route Selection (ARS) and Feature Access Code (FAC)
- A route pattern administered to route calls to your SIP trunk group
- A route pattern administered to route calls to your ISDN trunk group

About this task

Procedure

1. Set up your ARS digit analysis so that all outbound ISDN calls that do not route to a specific dialed string use a route pattern that directs them to your SIP trunk group.

   You can use a dialed string value of `x`.

2. In Session Manager create a digit conversion adapter for the Communication Manager entity .
3. In the **Insert Digits** field, add ARS FAC and steering digits (such as 999) that will not be confused with an area code.

   In Communication Manager set up your AAR digit analysis so that calls with a dialed string of your administered steering digits are directed to a route pattern that directs calls to the ISDN trunk group.

4. Edit the route pattern for your ISDN trunk group to remove the steering digits you added.

Related links

Communication Manager call routing on page 94

Chapter 11: FIPS configuration

You can enable FIPS if your enterprise requires full FIPS compliance. In some deployments, FIPS is enabled by default.

Related links

Enabling FIPS on page 96
Disabling FIPS on page 96

Enabling FIPS

About this task

This procedure describes how to enable FIPS.

Important:

- This process will cause the Avaya Breeze® platform server to reboot.

Procedure

1. To check the current status of FIPS, enter the following command:
   - `fips_mode.sh`
2. To enable FIPS, enter the following command:
   - `fips_mode.sh enable`

   Avaya Breeze® platform reboots for the changes to take effect.

Related links

FIPS configuration on page 96

Disabling FIPS

About this task

This procedure describes how to disable FIPS.

Important:

- This process will cause the Avaya Breeze® platform server to reboot.

Procedure

1. To check the current status of FIPS, enter the following command:
   - `fips_mode.sh`
2. To disable FIPS, enter the following command:
   - `fips_mode.sh disable`

   Avaya Breeze® platform reboots for the changes to take effect.

Related links

FIPS configuration on page 96

Appendix A: VMware snapshots

VMware snapshots

A snapshot preserves the state and data of a virtual machine at a specific point in time. You can create a snapshot before upgrading or installing a patch.

The best time to take a snapshot is when no applications in the virtual machine are communicating with other computers. The potential for problems is greatest if the virtual machine is communicating with another computer. For example, if you take a snapshot while the virtual machine is downloading a file from a server on the network, the virtual machine continues downloading the file and communicating its progress to the server. If you revert to the snapshot, communications between the virtual machine and the server are confused and the file transfer fails.

Caution:

Snapshot operations can adversely affect service. Before performing a snapshot operation, you must stop the application that is running on the virtual machine or place the application out-of-service. When the snapshot operation is complete, start or bring the application back into service.

Only take snapshots during a maintenance window.

Snapshots can:

- Consume large amounts of data resources.
- Increase CPU loads on the host.
- Affect performance.
- Affect service.

To prevent adverse behaviors, consider the following recommendations when using the Snapshot feature:

- Do not rely on VMware snapshots as a robust backup and recovery method. Snapshots are not backups. The snapshot file is only a change log of the original virtual disk.
- Do not run a virtual machine from a snapshot. Do not use a single snapshot for more than 24 to 72 hours.

  If your virtual machine contains snapshots that are more than 72 hours old, system performance might be impacted. When you no longer need a snapshot, remember to delete it.

- Take the snapshot, make the changes to the virtual machine, and delete or commit the snapshot after you verify the virtual machine is working properly. These actions prevent snapshots from growing so large as to cause issues when deleting or committing the snapshots to the original virtual machine disks.
- When taking a snapshot, do not save the memory of the virtual machine. The time that the host takes to write the memory to the disk is relative to the amount of memory that the virtual machine is configured to use. Saving the memory can add several minutes to the time taken to complete the operation. If the snapshot is active, saving memory can make calls appear to be active or in progress and can cause confusion to the user. To create a clean snapshot image from which to boot, do the following when you create a snapshot:
  - In the Take Snapshot window, clear the **Include virtual machine's memory** check box.
  - Select the **Quiesce guest file system (Needs VMware Tools installed)** check box to ensure that all write instructions to the disks are complete. You have a better chance of creating a clean snapshot image from which to boot.
- If you are going to use snapshots for a long time, you must consolidate the snapshot files regularly to improve performance and reduce disk usage. Before merging the snapshot delta disks back into the base disk of the virtual machine, you must first delete stored snapshots.

  Note:

  If a consolidation failure occurs, end-users can use the actual Consolidate option without opening a service request with VMware. If a commit or delete operation does not merge the snapshot deltas into the base disk of the virtual machine, the system displays a warning on the user interface.

Related resources

Title	Link
Best practices for virtual machine snapshots in the VMware environment	Best Practices for virtual machine snapshots in the VMware environment
Understanding virtual machine snapshots in VMware ESXi and ESX	Understanding virtual machine snapshots in VMware ESXi and ESX
Working with snapshots	Working with snapshots
Configuring VMware vCenter Server to send alarms when virtual machines are running from snapshots	Send alarms when virtual machines are running from snapshots

Appendix B: Sending Avaya Breeze® platform logs to rsyslog

You can configure the Avaya Breeze® platform server to send log files to a remote rsyslog server.

- This method of logging is not supported if Avaya Breeze® platform is configured for FIPS (see FIPS configuration on page 96).

Related links

Configuring rsyslog on the Avaya Breeze platform on page 100

Configuring rsyslog on the Avaya Breeze® platform

About this task

You can use the following process to enable the sending of logs from an Avaya Breeze® platform server to a remote rsyslog server.

- This process assumes that Avaya Breeze® platform send the logs to UDP port 514.

Before you begin

- Check that rsyslog is installed and operating on the server to which the Avaya Breeze® platform will send logs.

Procedure

1. Check if rsyslog is already installed on the Avaya Breeze® platform by entering the following command:

   ```
   rsyslogd -v
   ```

2. If not installed, enter the following command to install rsyslog:

   ```
   dnf install rsyslog
   ```

3. Open the rsyslog configuration file using the following command:

   ```
   vi /etc/rsyslog.conf
   ```

4. Locate the `# remote host` is section and add the address of the rsyslog server:

```
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
*.* @<rsyslog server IP address>:514
```

   - Where `<rsyslog server IP address>` is the address of the rsyslog server.

5. Close the rsyslog configuration file, saving the changes.
6. Enter the following command to open the ports the Avaya Breeze® platform client will use to send logs to the remote rsyslog server:

```
sh /etc/snfw/snfw-nft.sh --nft-custom-add inet filter output oif "eth0" udp dport
514 ct state { established, new } counter accept
```

7. Check the status of rsyslog by entering the following commands:

```
systemctl restart rsyslog
systemctl enable rsyslog
systemctl status rsyslog
```

8. On the remote rsyslog server:
   a. Under the `/var/log/` path, locate the folder with the hostname of the Avaya Breeze® platform server.
   b. Enter the folder.
   c. Use the `tail` command to view the most recent logs from the Avaya Breeze® platform.

Related links

Sending Avaya Breeze platform logs to rsyslog on page 100

Appendix C: Avaya Aura® Media Server configuration for Avaya Engagement Assistant Snap-in

The procedures in this section are only required if Avaya Engagement Assistant Snap-in is one of the deployed snap-ins. If a particular Avaya Breeze® platform deployment does not include Avaya Engagement Assistant Snap-in, these procedures may be omitted.

Related links

Administering an Avaya Aura Media Server SIP Entity on page 102
Administering the Avaya Aura Media Server Entity Link on page 103
Creating the Avaya Aura Media Server Routing Pattern on page 104
Configuring Avaya Aura Media Server Host Name Resolution on page 106
Administering Avaya Aura Media Server URI on page 106

Administering an Avaya Aura® Media Server SIP Entity

Before you begin

To complete this task, you need the FQDN of the Avaya Aura® Media Server pool you set up when configuring network connections.

Procedure

1. In System Manager, click **Elements** > **Routing** > **SIP Entities**.
2. Click **New**.
3. In the **Name** field, type the name of your SIP Entity. For example, type `ams-cluster1`.
4. In the **FQDN or IP Address** field, type the FQDN of your Avaya Aura® Media Server pool.

Note:

If you leverage Avaya Aura® Media Server high availability through the use of Local Host Name resolution on System Manager, use the FQDN representing those Avaya Aura® Media Server set of servers here, or use the FQDN or IP address of a single Avaya Aura® Media Server server traffic interface.

5. In the **Type** field, select `Media Server`.
6. In the **Location** field, select an assigned location.

   For

7. Click **Commit** to save your changes.

Related links

Avaya Aura Media Server configuration for Avaya Engagement Assistant Snap-in on page 102

Administering the Avaya Aura® Media Server Entity Link

Before you begin

Administer Avaya Aura® Media Server as a SIP Entity.

About this task

Create an Entity Link to connect Session Manager to Avaya Aura® Media Server.

Note:

You must use a common protocol for the entity links between Avaya Breeze® platform and Session Manager, and between Session Manager and Avaya Aura® Media Server. If you have multiple Avaya Aura® Media Servers with different protocols, configure two Entity Links between Avaya Breeze® platform and Session Manager for TLS and TCP.

Note:

TLS is the recommended protocol for production environments since it is secure and encrypted. Should the need arise to take a network trace between Session Manager and Avaya Aura® Media Server, change the protocol to TCP. If this is a production environment, change the protocol back to TLS as soon as the trace is complete.

Procedure

1. In System Manager, click **Elements** > **Routing** > **Entity Links**.
2. Click **New**.
3. In the **Name** field, type a name for the Avaya Aura® Media Server SIP Entity Link.
4. For the **SIP Entity 1** select the Session Manager.
5. For the **SIP Entity 2** select the Avaya Aura® Media Server SIP Entity that you created.
6. Press **Commit** to save your changes.

Next steps

Create a Routing Pattern for Avaya Aura® Media Server.

Related links

Avaya Aura Media Server configuration for Avaya Engagement Assistant Snap-in on page 102

Creating the Avaya Aura® Media Server Routing Pattern

About this task

This section is applicable only to snap-ins using SIP to communicate with Avaya Aura® Media Server.

Procedure

1. On System Manager, click **Elements** > **Routing** > **Routing Policies** .
2. Click **New**.
3. Type a **Name** for the Routing Policy.
4. From the **SIP Entity as Destination** field, click **Select**.
5. Select the Avaya Aura® Media Server SIP Entity that you created.

   Select the Local Host Name FQDN SIP Entity if you are using High Availability for the Avaya Aura® Media Server routing.
6. Click **Commit** .
7. Navigate to **Home** > **Elements** > **Routing** > **Regular Expressions** and click **New**.
8. In the **Pattern** field, type `ce-msml.*`
9. Click **Commit**.

Next steps

Verify the Avaya Aura® Media Server entity link with Session Manager.

Related links

Avaya Aura Media Server configuration for Avaya Engagement Assistant Snap-in on page 102

Verifying the Avaya Aura® Media Server Entity Link connection

About this task

Complete this task to verify that Session Manager can connect with Avaya Aura® Media Server using the SIP Entity Link. To do this you must make a couple of minor changes to the Avaya Aura® Media Server SIP entity, and the administered Session Manager instance.

Procedure

1. Enable SIP Link Monitoring on the Avaya Aura® Media Server SIP Entity.
   a. On System Manager, click **Elements** > **Routing** > **SIP Entities**.
   b. Select the Avaya Aura® Media Server SIP Entity.
   c. Click **Edit**.
   d. From the **SIP Link Monitoring** drop-down menu select **Link Monitoring Enabled**.
   e. Click **Commit**.
2. Modify the Session Manager Instance.
   a. Navigate to **Home** > **Elements** > **Session Manager** > **Session Manager Administration**.
   b. Select the Session Manager Instance that you linked to Avaya Aura® Media Server. Click **Edit**.
   c. Check **Enable Monitoring** in the **Monitoring** section.
   d. Click **Commit**.
3. Test the Entity Link.
   a. Navigate to **Home** > **Elements** > **Session Manager** > **System Status** > **SIP Entity Monitoring**.
   b. Click the name of the Session Manager Instance that you linked to Avaya Aura® Media Server.

      The system displays a list with the status of all the Entity Links for the selected Session Manager.
   c. Located the Avaya Aura® Media Server SIP Entity and check the **Conn. Status** column.
      - If you see `UP`, congratulations! You have successfully configured your Avaya Aura® Media Server link.
      - If you do not see `UP`, for additional information, see *Avaya Breeze® platform FAQ and Troubleshooting for Service Developers*.

Configuring Avaya Aura® Media Server Host Name Resolution

About this task

In this task you are creating an FQDN Host Name for the pool of Avaya Aura® Media Server servers that will be used by Avaya Breeze® platform. The pool can contain one to five servers. Add information for each server as part of this task.

This section is applicable only to snap-ins using SIP to communicate with Avaya Aura® Media Server.

Procedure

1. In System Manager navigate to **Home** > **Elements** > **Session Manager** > **Network Configuration** > **Local Host Name Resolution** and click **New**.
2. In **New Local Host Name Entries**, on each line type the **Host Name (FQDN)**, **IP Address** and **Port** for each Avaya Aura® Media Server.

   The **Host Name** is the same for each server in the pool.
3. Select a **Priority**, **Weight**, and **Transport** protocol for each server.
   - **Priority**: If there are multiple Avaya Media Servers for the single host, Session Manager tries the administered IP addresses in the order of the priority.
   - **Weight**: If there are multiple Avaya Media Servers for the single host, and if some entries have the same priority, then for each priority level, Session Manager picks a host according to the specified weights.
4. Click **Commit** to save your changes.

   For additional information about administering Local Host Names, see *Administering Avaya Aura® Session Manager*.

Related links

Avaya Aura Media Server configuration for Avaya Engagement Assistant Snap-in on page 102

Administering Avaya Aura® Media Server URI

Before you begin

Check the snap-in documentation and Release Notes to confirm if this configuration is required.

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®**.
2. In the navigation pane, click **Configuration** > **Avaya Aura® Media Server**.
3. In the **Avaya Aura® Media Server URI** field, enter the URI.

Related links

Avaya Aura Media Server configuration for Avaya Engagement Assistant Snap-in on page 102

Appendix D: 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
Avaya Aura® System Manager Overview and Specification	Understand System Manager customer requirements and design considerations.	Sales engineers Programmers System administrators Services and support personnel
Avaya Aura® Media Server Overview and Specification	Understand Avaya Aura® Media Server 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
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
Planning for Deploying Avaya Aura® applications	Understand deployment options for various Avaya Aura® applications.	Services and support personnel System administrators
Deploying and Updating Avaya Aura® Media Server Appliance	Deploy and configure Avaya Aura® Media Server when it is installed on customer-provided servers.	System administrators Services and support personnel
Deploying Avaya Aura® System Manager in Infrastructure as a Service Environment	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
Implementing and Administering Avaya Aura® Media Server	Deploy and configure Avaya Aura® Media Server.	System administrators Services and support personnel
Administering Avaya Aura® System Manager	Administer Avaya Aura® System Manager.	System Administrators Services and support personnel
Administering Avaya Aura® Session Manager	Administer Avaya Aura® Session Manager.	System Administrators Services and support personnel

Table continues…

Title	Use this document to:	Audience
Administering Avaya Session Border Controller	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
Troubleshooting Avaya Aura® System Manager	Troubleshoot System Manager.	Services and support personnel
Troubleshooting Avaya Aura® Session Manager	Troubleshoot Avaya Aura® Session Manager.	Services and support personnel

Programming

The following developer documents are available on Avaya DevConnect .

Title	Use this document to:	Audience
Getting Started with the Avaya Breeze® platform SDK	Deploy and configure the Eclipse IDE, Apache Maven, and the Avaya Breeze® platform SDK.	Programmers
Avaya Breeze® platform Snap-in Development Guide	Understand the key concepts needed to develop the different types of Avaya Breeze® platform snap-ins.	Programmers
Avaya Breeze® platform FAQ and Troubleshooting for Snap-in Developers	Troubleshoot Avaya Breeze® platform snap-in developer issues.	Programmers
Avaya Breeze® platform API Javadocs	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
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

Table continues…

Course code	Course title
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/breezedeveloper.

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/breezedeveloper 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

A

accepting new service ... 71
add
  trusted CA certificates ... 81
administering
  Avaya Breeze® platform ... 64
application for high availability ... 87
application sequence for high availability ... 87
assigning
  media server ... 33
automatic restart
  virtual machine ... 54, 56
Avaya Aura Media Server
  adding the System Manager IP address ... 34
  deployment checklist ... 15
  entity link ... 103
  host name resolution ... 106
  licensing ... 33
  network connections ... 106
  routing pattern ... 104
  SIP entity ... 102
  when required ... 21
Avaya Aura Media Server OVA deployment ... 31
Avaya Aura Media Server selection algorithm ... 28
Avaya InSite Knowledge Base ... 114
Avaya SIP CA certificate ... 78
AvayaNetSetup
  configuring after changing IP address or FQDN ... 53

B

backup ... 71
  cluster database ... 72

C

call intercept snap-in ... 10
call interrupt services call routing ... 94
callable snap-in ... 10
cancel ... 73
CEnetSetup
  configuring after changing IP address or FQDN ... 53
certificate administration ... 78
certificate enrollment password ... 42
certificates ... 16
changes ... 8
changing IP address or FQDN
  configuring after changes ... 53
checklist ... 15
cluster
  accepting new service ... 71
  backup ... 71
cluster *(continued)*
  restore ... 71, 73
cluster database
  backup ... 72
cluster database servers
  identifying ... 88
clusters
  create ... 68
  load balancing ... 91
  new ... 68
  view ... 68
  view attributes ... 68
collaboration bus-invoked snap-in ... 10
collection
  delete ... 111
  edit ... 111
  generating PDF ... 111
  sharing content ... 111
Communication Manager
  call routing ... 94
configuration information ... 23
configuring
  after changing IP address or FQDN ... 53
  IPv6 ... 65
  VM automatic restart ... 54, 56
configuring connection security options ... 38
connection security options
  configuring ... 38
connector for conferencing ... 12
connector snap-ins ... 11, 13
  email connector ... 12
  Eventing Framework connector ... 12
  Scopia connector ... 12
content
  publishing PDF output ... 111
  searching ... 111
  sharing ... 111
  sort by last updated ... 111
  watching for updates ... 111
creating a new cluster ... 68
Creating multiple privileged user accounts ... 58
customer configuration information ... 23
customer password ... 56

D

Deleting a Reliable Eventing destination
  Eventing destination ... 76
Deleting a Reliable Eventing group
  Eventing group ... 75
deploying using SDM ... 50
deploying using vSphere client ... 45
Deploying using web-based client ... 43

deployment checklist
Avaya Aura Media Server ... 15
Avaya Breeze® platform ... 16
high availability ... 85
deployments that require Avaya Aura Media Server ... 21
determine if you need AAMS ... 21
DevConnect ... 113
disable
FIPS ... 96
document changes ... 8
documentation center ... 111
finding content ... 111
navigation ... 111
documentation portal ... 111
downloading software ... 22

E

EASG ... 58
certificate information ... 59
disabling ... 59
enabling ... 59
site certificates ... 60
EASG site certificate ... 60
Editing a Reliable Eventing group
Eventing group ... 75
email connector ... 12
enable
FIPS ... 96
Enhanced Access Security Gateway ... 58
enrollment password status ... 42
entity link
Avaya Aura Media Server ... 103
for high availability ... 86
FQDN ... 86
verification ... 67
Entity link
Avaya Breeze® platform ... 62
Equinox connector ... 12
eth0 ... 65
eventing ... 74
Eventing Framework connector ... 12
exporting certificate ... 39
External load balancer ... 92

F

finding content on documentation center ... 111
FIPS ... 96
disable ... 96
enable ... 96
status ... 96
FQDN change
configuring after changes ... 53

H

high availability
administration ... 84
application ... 87
application sequence ... 87
deployment checklist ... 85
planning ... 84
SIP ... 84
traffic distribution ... 84
host name resolution for high availability ... 88
HTTP Geo-redundancy ... 92
HTTP high availability ... 90
HTTP load balancing ... 90
HTTP-invoked snap-in ... 10

I

identify certificates ... 79
identity certificates ... 78
replacing ... 82
implicit users applications for SIP users ... 63
install ... 16
trust certificates ... 80
IP address change
configuring after changes ... 53
IPv6 ... 65
ISDN call routing
inbound ... 94
outbound ... 95
ISDN trunk routing ... 94

K

KB
Support site ... 114

L

latency ... 27
latest software patches ... 28
license file install
Avaya Aura Media Server ... 34
Avaya Breeze® platform ... 61
licensing ... 16
Avaya Aura Media Server ... 33
file install ... 33
load balancing ... 91
restrictions ... 90
validations ... 90

M

maintenance test
broker ... 76
management interface ... 65

management link verification ... 68
Media Server
configuration ... 102
when required ... 21
multiple user accounts
configure ... 58
create ... 58

N

name resolution ... 37
network connections for Avaya Aura Media Server ... 106
network latency ... 27
networking
IPv6 ... 65

O

Out of Band Management ... 27
outbound calling snap-in ... 10
OVA ... 16
OVA deployment ... 41
Avaya Aura Media Server ... 31
vSphere client connected to ESXi host ... 47
with SDM ... 50
with vCenter ... 45
with VMware vSphere web client ... 43
OVA requirements ... 41
overview ... 9

P

patch information ... 28
patching the server ... 57
PCN ... 28
planning ... 21
PLDS ... 16
downloading software ... 22
preconfiguration ... 21
PSN ... 28
purge ... 73

R

release notes for latest software patches ... 28
reliable eventing ... 74
Reliable Eventing group
creating ... 74
Reliable Eventing status ... 76
replacing identity certificates ... 82
replication status verification ... 67
requirements
OVA ... 41
REST ... 31
restore ... 71, 73
routing pattern for Avaya Aura Media Server ... 104
rsyslog ... 100
enable ... 100
running upgradeSolution script ... 29

S

Scopia connector ... 12
SDM OVA deployment ... 50
searching for content ... 111
security ... 78
trust certificates ... 78, 80
setting up load balancing ... 91
sharing content ... 111
SIP entity ... 16
Avaya Aura Media Server ... 102
Avaya Breeze® platform ... 62
for high availability ... 85
FQDN ... 85
SIP load balancing ... 84
geo-redundancy ... 89
local ... 89
SIPS ... 35
snap-in types
call intercept snap-in ... 10
callable snap-in ... 10
collaboration bus-invoked snap-in ... 10
HTTP-invoked snap-in ... 10
outbound calling snap-in ... 10
snapshots ... 98
software patches ... 28
sort documents ... 111
SRTP ... 35
status
enrollment password ... 42
FIPS ... 96
support ... 114
system interactions ... 13
system manager administration ... 61
System Manager compatibility ... 14
System Manager configuration
changing ... 54
System Manager IP address for AAMS ... 34

T

Topology ... 14
training ... 112
trust certificates ... 78, 80
trust configuration ... 38

U

upgradeSolution
System Manager ... 29
upgradeSolution script
System Manager ... 14

URI
administering 106

V

verification
Avaya Aura Media Server entity link 105
entity link 67
management link 68
replication status 67
videos 113
viewing cluster attributes 68
virtual machine
automatic restart 54, 56
vSphere client connected to ESXi host 47
vSphere client OVA deployment 45
vSphere web client OVA deployment 43

W

watchlist 111