Deploying Avaya Breeze® platform

Release 3.6
Issue 1
December 2018

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 mediums which may include product information, 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. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: 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 You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You 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 SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

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, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note, unless otherwise stated, that 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

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

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

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER’S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

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

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying 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, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

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).

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 Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted 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.

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 Inc.

Contents

Chapter 1: Introduction

Purpose

This document contains installation, configuration, initial administration, and basic maintenance checklist 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.

Chapter 2: Architecture overview

Avaya Breeze® platform overview

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

Avaya products, such as Avaya Oceana® Solution, Presence Services, Engagement Designer, and Context Store 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 Zang.
- Zang SMS connector for snap-ins to interact with Zang to send and receive messages.
- Tools that log and monitor operations and provide troubleshooting support.
- High availability. For information about high availability, see “High Availability”.

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 the 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 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.

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
- Equinox connector
- Eventing Framework connector
- Zang call connector
- Zang SMS connector

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

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

Zang SMS connector

For information about Zang SMS connector, see *Deploying Zang-Enabled Avaya Breeze® platform* and *Zang SMS Connector Snap-in Reference*.

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

Equinox connector

Equinox connector, earlier known as Scopia connector, uses the Conferencing API to access the Equinox Management Server for audio and video conferencing. Equinox connector is still called Scopia connector on the Service Management page of the Avaya Breeze® platform Element Manager. Equinox 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 Equinox 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 Equinox connector include the:

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

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.

Zang Call Connector

Zang Call Connector is an Avaya Breeze® platform snap-in used to interact with Zang. Zang Call Connector takes instructions from Avaya Breeze® platform CMA API through Avaya Breeze® platform Normalized Interaction Protocol to sends http(s) messages to Zang for handling voice call operations and other media operations.

System interactions

Avaya product	Supported releases
Avaya Aura® System Manager	8.0.1
Avaya Aura® Session Manager	6.3.8, 6.3.9, 7.0, 7.0.1, 7.1.x, 8.0, and 8.0.1
Avaya Aura® Communication Manager	6.3.6, 7.0, 7.0.1, 7.1.x, 8.0, and 8.0.1
Avaya Aura® Application Enablement Services	6.3.3, 7.0.x, 7.1.x, and 8.0
Avaya Aura® Media Server	8.0 and 8.0.1
Avaya Aura® Messaging	6.3.5 and 7.0
Avaya Equinox® Conferencing	8.3 to 9.1.2
Engagement Call Control solution	3.5.0.1

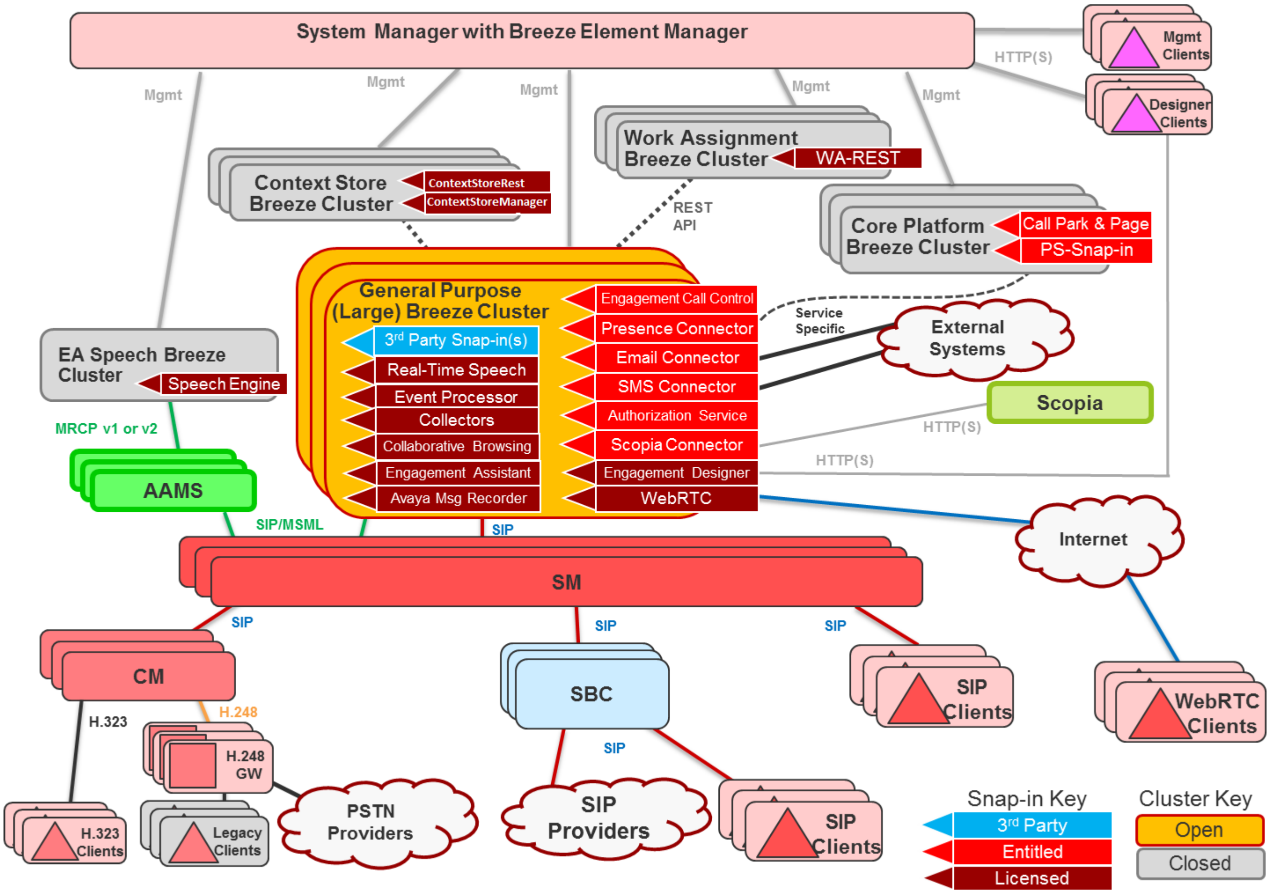
Traditional H.248 gateways provide access to the PSTN and support for H.323 and legacy endpoints. Connection to SIP service provider trunks is provided through Session Border Controller to Session Manager.

Snap-ins

Avaya Breeze® platform snap-ins interoperate with other Avaya products. For example, WebRTC Snap-in interoperates with Avaya Session Border Controller for Enterprise Releases 6.3 to 8.0.

Topology

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



Chapter 3: Deployment process

Avaya Aura® Media Server deployment checklist

The following table lists the procedures required to deploy Avaya Aura® Media Server. You must deploy Avaya Aura® Media Server before deploying Avaya Breeze® platform.

#	Action	Reference/Notes	✔
1	Download software from PLDS. Download the Avaya Aura® Media Server License file from PLDS.	Downloading software from PLDS on page 26	
2	Deploy the Avaya Aura® Media Server OVA.	See *Deploying and Updating Avaya Aura® Media Server Appliance*.	
3	Configure virtual machine automatic startup settings.	Configuring virtual machine automatic startup settings using vSphere desktop client on page 47	
4	License the Avaya Aura® Media Server.	Licensing the Avaya Aura Media Server on page 70 Installing the Avaya Aura Media Server license file on page 70	
5	Enroll Avaya Aura® Media Server on System Manager. Before enrolling, ensure to follow the pre-enrollment checklist included in *Implementing and Administering Avaya Aura® Media Server*.	Refer to the "System Manager enrollment" section in *Implementing and Administering Avaya Aura® Media Server*. **Note:** Note the following during enrolling: • 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	

Table continues…

#	Action	Reference/Notes	✔
		DNS or must have an entry in /etc/hosts. • System Manager and Avaya Aura® Media Server need to be on the same domain.	
6	Administer Avaya Aura® Media Server for REST.	Administering Avaya Aura Media Server for REST on page 68	
7	Assign Avaya Aura® Media Server for use with Avaya Breeze® platform.	Assigning Avaya Aura Media Server for use with Avaya Breeze platform on page 69	
8	Create a new certificate on Avaya Aura® Media Server, or import an existing certificate to establish a trust relationship with Avaya Breeze® platform.	See *Security Configuration* in the *Configuration* chapter of *Implementing and Administering Avaya Aura® Media Server* for additional information.	
9	Add the System Manager IP address.	Adding the System Manager IP address on page 71	
10	Configure name resolution.	Avaya Aura Media Server host name resolution on page 72	
11	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*.	

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.	Key customer configuration information on page 19	
2	Install or upgrade to the latest System Manager.	Verify that System Manager is running on the correct release. For more details on the System Manager version, see the Product Change Notice (PCN) and the *Release Notes for Avaya Breeze® platform*.	

Table continues…

#	Action	Reference/Notes	✔
3	Download software from PLDS. Download the Avaya Breeze® platform License file from PLDS. Download the patch file (if required) from PLDS.	Downloading software from PLDS on page 26	
4	Verify that the **Enrollment Password** is not expired.	Verifying Enrollment Password status on page 26	
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 27 • Deploying Avaya Breeze platform OVA with VMware vSphere Client connected to vCenter on page 32 • Deploying Avaya Breeze platform OVA with VMware vSphere Client connected to ESXi host on page 36 • Deploying Avaya Breeze platform OVA with Solution Deployment Manager on page 43 The Avaya Breeze® platform management FQDN assigned to the management network interface must be registered in DNS. For assistance, contact Avaya Support. **Note:** 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.	

Table continues…

#	Action	Reference/Notes	✔
		Note: 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.	Changing the customer password on first login on page 49	
7	Configure virtual machine automatic startup settings.	Configure virtual machine automatic startup settings on page 47	
8	Install the patch file.	Patching Avaya Breeze platform on page 49	
9	Create multiple privileged user accounts. (optional)	Creating multiple privileged user accounts on page 50	
10	Install the Avaya Breeze® platform license file.	Installing the Avaya Breeze platform license file on page 54	
11	Administer the SIP Entity.	Administering an Avaya Breeze platform SIP Entity on page 54	
12	Administer the SIP Entity Link.	Administering the Avaya Breeze platform Entity Link on page 55	
13	Enable implicit users applications for SIP users.	Enabling implicit users applications for SIP users on page 56	
14	Administer the Avaya Breeze® platform Instance.	Administering an Avaya Breeze platform instance on page 56	
15	Verify the Entity Link connection.	Verifying the Avaya Breeze platform Entity Link connection on page 57	
16	Verify the replication status.	Verifying replication status on page 58	
17	Verify management link.	Verifying the management link on page 59	
18	Assign the server to an Avaya Breeze® platform cluster. If one does not already exists for this server, create the cluster.	Creating a new cluster on page 59	
19	Add a trust certificate to all servers.	Adding a Trust Certificate to all Avaya Breeze platform servers in a cluster on page 78	
20	Add individual trust certificates. **Note:** Step 19 adds the trust certificates to all Avaya Breeze® platform	Adding trusted CA certificates on page 79	

Table continues…

#	Action	Reference/Notes	✔
	server in the cluster. This step is required only if you are provisioning a new server to be added to the cluster or have redeployed an existing server using an OVA.		
21	Replace an identity certificate.	Replacing an identity certificate on page 80	
22	Change the state of the server to accept new service.	Accepting new service on page 61	
23	Configure the Alarming setup. Configure System Manager to receive the Avaya Breeze® platform alarms.	See *SNMP Support for Avaya Breeze® platform* in *Maintaining and Troubleshooting Avaya Breeze® platform.*	
24	If you have cluster database enabled, you setup scheduled backups for cluster database.	See *Administering Avaya Breeze® platform*.	
25	For Communication Manager route inbound ISDN calls.	Routing inbound ISDN calls on page 91	
26	For Communication Manager route outbound ISDN calls.	Routing outbound ISDN calls on page 92	

Chapter 4: Planning and preconfiguration

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 server's IP address`	Management IP address to be assigned to Avaya Breeze® platform.
Short Hostname	`Enter server's hostname`	
Network Domain	`Enter network domain or 'none'`	
Netmask	`Enter netmask`	
Default gateway	`Enter gateway IP address`	Default gateway for Avaya Breeze® platform management network interface.
DNS servers	`Enter the Primary, Secondary, and Tertiary DNS server IP address`	You can have up to three DNS servers.
Cluster IP address	`Enter a unique IP address`	This value is required after deployment.

Proxy settings

Field	Information to enter	Notes
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.`	

Table continues…

Field	Information to enter	Notes
HTTP Proxy exclusion list	Enter the HTTPS proxy severs 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 IP/FQDN of 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 to 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 Login ID to use for the customer account (cust).`	Login ID and password for customer account you will create during OVA deployment.
Enter Password	`Enter the customer account password.`	This password will change after first customer login.

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.	**Note:** You must know the Enrollment Password, and the password must not have expired. The password is set on System Manager at **Security** > **Certificates** > **Enrollment Password**. On this page, verify that the **Time Remaining** is greater than zero. If you do not know the password, create a new one.

Flexi Footprint values

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

Profile	CPU (cores)	Available Memory (GB)	Disk Storage (GB)	Notes
2	4	8	50 GB	Maximum active SIP application sessions: 29,900 sessions. This deployment requires 4 CPUs, 8 GB Memory and 50 GB disk space.
3	6	10	50 GB	This profile is targeted as a migration path for the Presence Services application on Midsize Enterprise to Presence Services

Table continues…

Profile	CPU (cores)	Available Memory (GB)	Disk Storage (GB)	Notes
				with Avaya Breeze® platform. Maximum active SIP application sessions: 44,880 sessions. This deployment requires 6 CPUs, 10 GB Memory and 50 GB Disk space.
4	8	16	50 GB For Solution Deployment Manager deployments this increases to 150 GB.	Maximum active SIP application sessions: 59,840 sessions. This deployment requires 8 CPUs, 16 GB Memory and 150 GB disk space.
5	12	27	50 GB For Solution Deployment Manager deployments this increases to 150 GB.	Presence Services Environment: Dell R610 with: 2 x 6 cores CPU, cpu speed clock > = 2.925 GHz, 32 GB RAM, 3 x 300 GB hard drive configured using RAID 5. 27 GB memory based on CSR1 server with AVP using 5 GB. This deployment requires 12 CPUs, 27 GB Memory and 300 GB disk space.

Virtual Machine

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

Field	Information to enter	Notes
DataStore location	Select the datastore location to store the virtual machine files.	
Host networking assignments		

SIP Entity (Security Module Interface) Networking Information

This information is required for administering Avaya Breeze® platform SIP Entity and Avaya Breeze® platforminstance.

Required information	Value
IP address	
Subnet Mask	
Gateway	

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.

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.

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 web site 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 need to download and install any updates or patches.

Avaya Aura® Media Server selection algorithm

Avaya Breeze® platform supports a rich algorithm for selecting Avaya Aura® Media Server to use for a call. The algorithm depends on the use of locations defined in System Manager routing. Locations can be assigned in one of the following ways:

- Locations can explicitly be assigned to a SIP Entity such as Avaya Breeze® platform.
- IP address patterns can be specified for locations. If an endpoint or SIP Entity IP address matches a pattern for a location, the location is associated with the endpoint or the entity.

The selection algorithm includes the following rules that are evaluated in order, and each of which can be independently enabled or disabled through Cluster Attributes:

1. If enabled, the first rule is to check the location of the caller. If the caller SIP endpoint or SIP Entity, such a a trunk gateway matches an assigned location, Avaya Breeze® platform attempts to assign Avaya Aura® Media Server that is in the same location.
2. If enabled, the second rule is to check the location of Avaya Breeze® platform. If a location has been assigned to the Avaya Breeze® platform server that is handling a call, Avaya Breeze® platform attempts to assign Avaya Aura® Media Server that is in the same location.
3. If enabled, the third rule is to select a lightly-loaded Avaya Aura® Media Server from any location.

If none of these rules match, the call fails. Avaya recommends to enable all the rules. Any new clusters that are created in Release 3.6 have all the rules enabled by default. In order to preserve backward compatible behavior, any existing clusters will not have the first rule enabled by default upon upgrading to Release 3.6. You should enable the rule after upgrade.

Chapter 5: Avaya Breeze® platform OVA deployment

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. See “Deploying Avaya Breeze® platform OVA with VMware vSphere Web Client”.
- Solution Deployment Manager. See “Deploying Avaya Breeze® platform OVA with Solution Deployment Manager”.

Select the procedure that applies to you.

You must have the following to complete a procedure:

- vSphere ESXi 6.0 or later
- 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 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 the “Configuring Avaya Breeze® platform after changing the IP address or FQDN using AvayaNetSetup or CEnetSetup” section.

Related links

Deploying Avaya Breeze platform OVA with VMware vSphere Web Client on page 27

Deploying Avaya Breeze platform OVA with VMware vSphere Client connected to vCenter on page 32

Deploying Avaya Breeze platform OVA with VMware vSphere Client connected to ESXi host on page 36

Deploying Avaya Breeze platform OVA with Solution Deployment Manager on page 43

Downloading software 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, select **Assets**.
4. Select **View Downloads**.
5. If you are a customer, skip this step.
    a. In the **%Name** field, either Enter **Avaya** or the Partner company name, or click on the search icon (magnifying glass) and select the appropriate company from the drop-down menu.
    b. Click on **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** dialogue box, click the appropriate download link.

    Note:

    The first link, **Click to download your file now**, uses the Download Manager to download the file. The Download Manager provides features to manage the download (stop, resume, 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 on the **install ActiveX** message at the top of the page and continue with the download.
13. Select a location where you want to save the file and click **Save** .
14. If you used the Download Manager, click **Details** to view the download progress.

Verifying Enrollment Password status

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** is not zero, the password is valid. Verify that the time remaining is sufficient.

Procedure

1. On 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.

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.

Get the Avaya Breeze® platform OVA file, and save it on the workstation where you will be running the vSphere web client to configure the new virtual machine (VM).

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.

If you are redeploying an instance of Avaya Breeze® platform, ensure that you deny new service to and power off the instance that is being redeployed.

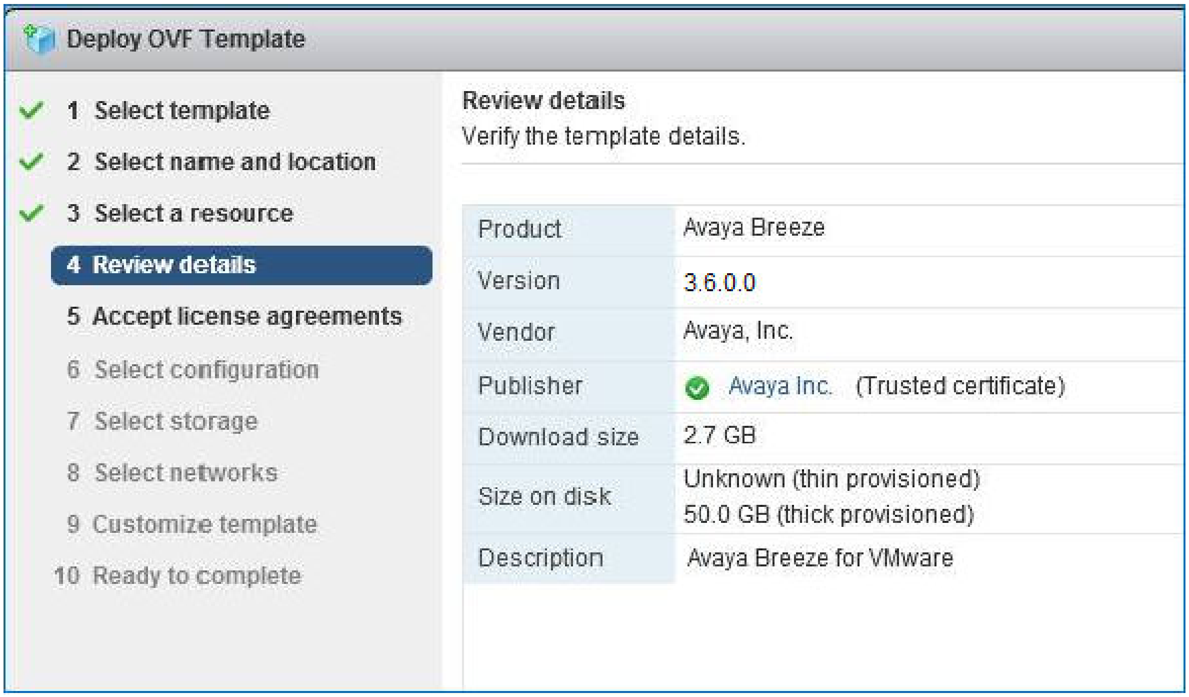
Verify that the Enrollment Password is administered and not expired.

Procedure

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

   The format is `https://<IP Address:9443>/vsphere-client`
2. In the navigation pane, click **vCenter**.
3. Click **Inventory Trees** > **Hosts and Clusters**.
4. Expand **Hosts and Clusters** to locate and select the target deployment host.
5. Right-click the on the host and select **Deploy OVF Template**.
6. On the Select Source page, enter the **URL** or path for installing the OVA, and click **Next**.

7. On the Review Details page, confirm the properties of the OVA file you selected and click **Next**.



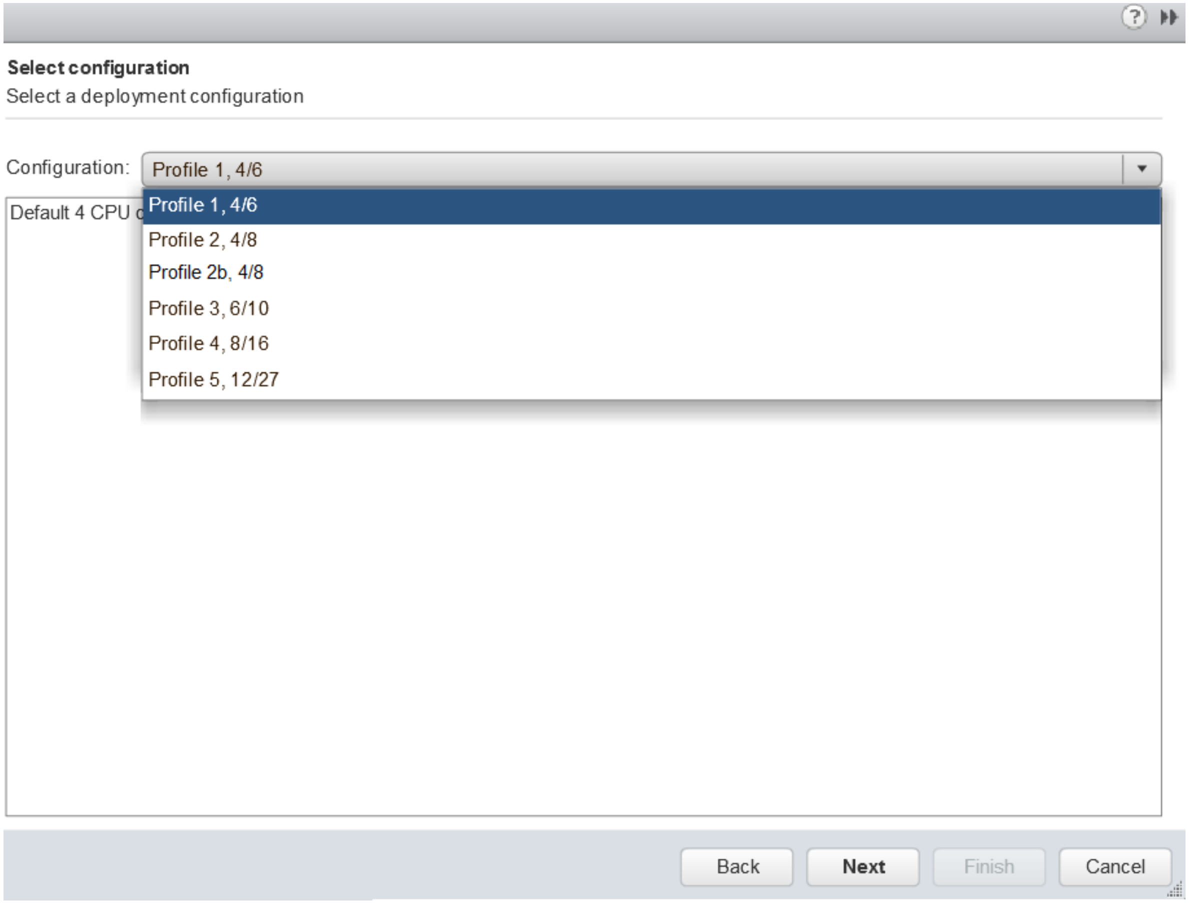
Review details

Verify the template details.

Product	Avaya Breeze
Version	3.6.0.0
Vendor	Avaya, Inc.
Publisher	✓ Avaya Inc. (Trusted certificate)
Download size	2.7 GB
Size on disk	Unknown (thin provisioned) 50.0 GB (thick provisioned)
Description	Avaya Breeze for VMware

8. To accept the End User License Agreement, click **Accept**.
9. Click **Next**.
10. Enter a name for the Avaya Breeze® platform VM and select the required datacenter folder for the VM.
11. Click **Next**.
12. On the Select a resource page, select the location to run the deployed template and click **Next**.

13. Select the configuration profile that best fits the deployment, and click **Next**.



Select configuration

Select a deployment configuration

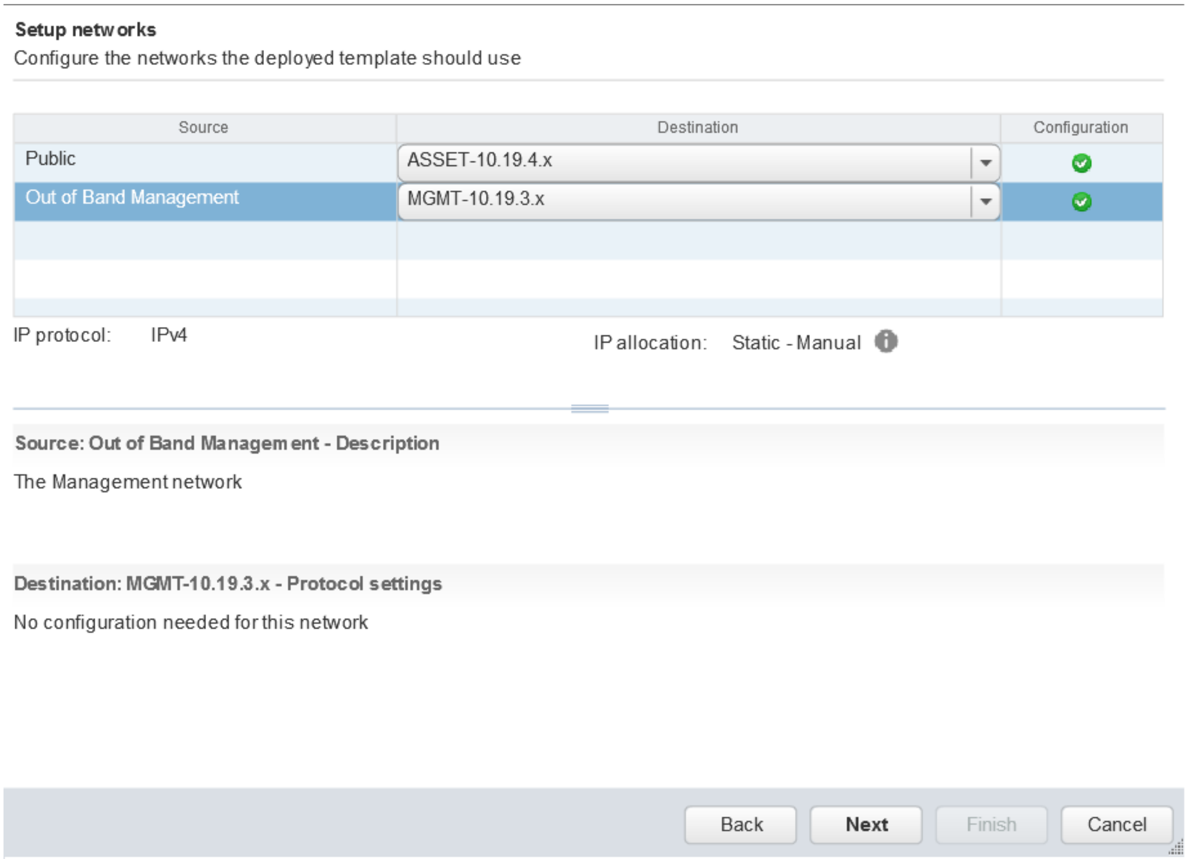
Configuration: Profile 1, 4/6

Default 4 CPU c

14. Select the virtual disk format you want and click **Next**.

15. Select the destination network for each Avaya Breeze® platform interface and click **Next**.

16. On the Setup networks page, configure the network settings for your VM and click **Next**.



Setup networks

Configure the networks the deployed template should use

Source	Destination	Configuration
Public	ASSET-10.19.4.x	✓
Out of Band Management	MGMT-10.19.3.x	✓

IP protocol: IPv4

IP allocation: Static - Manual

Source: Out of Band Management - Description

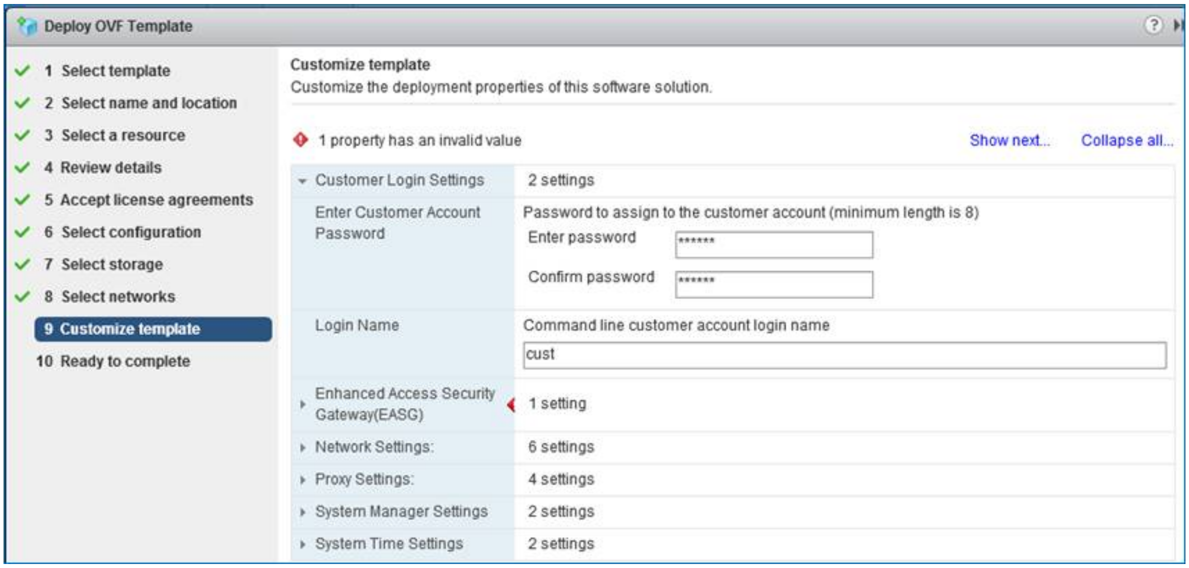
The Management network

Destination: MGMT-10.19.3.x - Protocol settings

No configuration needed for this network

See the *Customer Configuration Information* you collected for the network configuration values.

17. On the Customize template page, enter the configuration details for your VM and click **Next**.



Deploy OVF Template

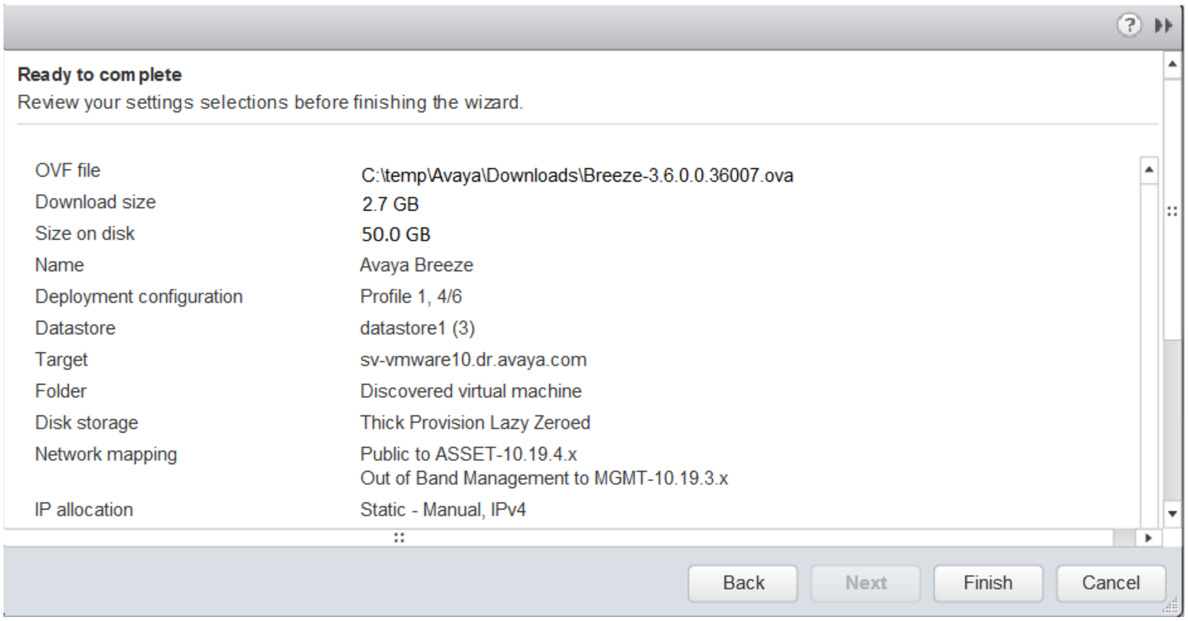
✓ 1 Select template
✓ 2 Select name and location
✓ 3 Select a resource
✓ 4 Review details
✓ 5 Accept license agreements
✓ 6 Select configuration
✓ 7 Select storage
✓ 8 Select networks
9 Customize template
10 Ready to complete

Customize template
Customize the deployment properties of this software solution.

1 property has an invalid value — Show next... Collapse all...

Customer Login Settings	2 settings
Enter Customer Account Password	Password to assign to the customer account (minimum length is 8) Enter password ****** Confirm password ******
Login Name	Command line customer account login name cust
Enhanced Access Security Gateway(EASG)	1 setting
Network Settings:	6 settings
Proxy Settings:	4 settings
System Manager Settings	2 settings
System Time Settings	2 settings

18. On the Ready to Complete page, verify the options for the VM:



Ready to complete
Review your settings selections before finishing the wizard.

OVF file	C:\temp\Avaya\Downloads\Breeze-3.6.0.0.36007.ova
Download size	2.7 GB
Size on disk	50.0 GB
Name	Avaya Breeze
Deployment configuration	Profile 1, 4/6
Datastore	datastore1 (3)
Target	sv-vmware10.dr.avaya.com
Folder	Discovered virtual machine
Disk storage	Thick Provision Lazy Zeroed
Network mapping	Public to ASSET-10.19.4.x Out of Band Management to MGMT-10.19.3.x
IP allocation	Static - Manual, IPv4

- 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 VM.

19. Select the new VM and click the **Summary** tab.
20. Click **Actions** > **Power On**.
21. Click **Summary** > **Launch Console** to open a new console.

    The system displays the progress of the VM system initialization.
22. After the VM initialization is complete, log in by using the customer account that you set up earlier.

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.

Get the Avaya Breeze® platform OVA file, and save it on the workstation where you will be running the vSphere Client to configure the new virtual machine (VM).

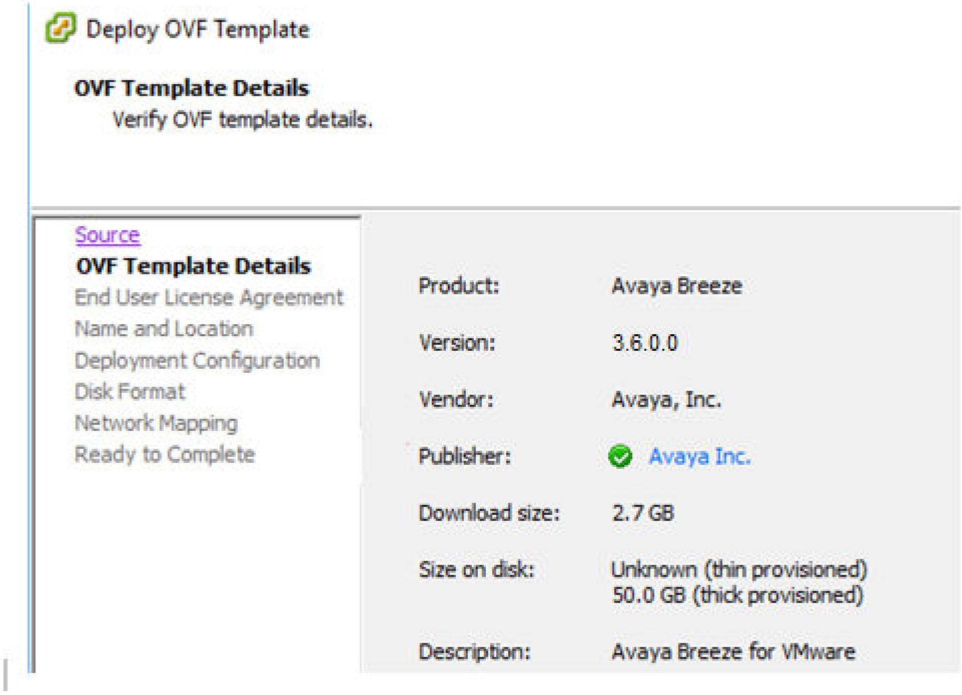
Use the *Customer Configuration Information* to get the required network settings for deployment. You can obtain the settings from an existing system if you are redeploying the OVA.

Verify that the Enrollment Password is administered and not expired.

If you are redeploying an instance of Avaya Breeze® platform, ensure that you deny new service to and power off the instance that is being redeployed.

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**.



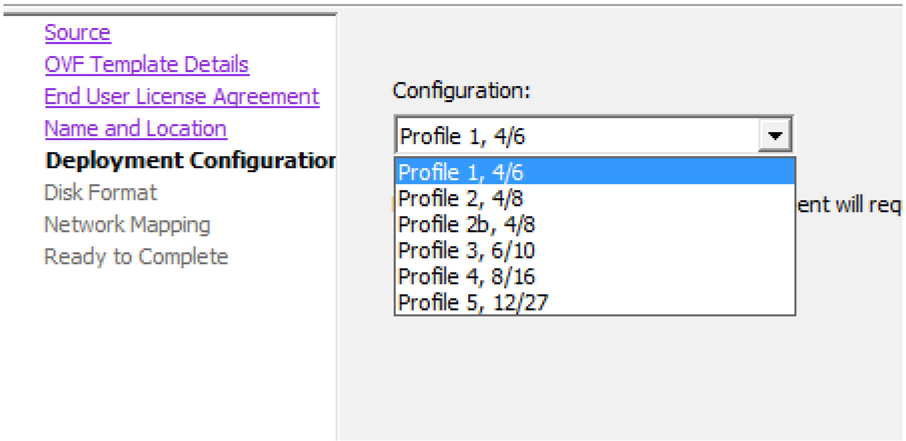
Deploy OVF Template

OVF Template Details

Verify OVF template details.

Product:	Avaya Breeze
Version:	3.6.0.0
Vendor:	Avaya, Inc.
Publisher:	✓ Avaya Inc.
Download size:	2.7 GB
Size on disk:	Unknown (thin provisioned) 50.0 GB (thick provisioned)
Description:	Avaya Breeze for VMware

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 (VM). Select the inventory location for your VM , then click **Next**.
7. On the Deployment Configuration page, select the configuration profile that best fits the deployment, then click **Next**.



Configuration:

Profile 1, 4/6

Profile 1, 4/6
Profile 2, 4/8
Profile 2b, 4/8
Profile 3, 6/10
Profile 4, 8/16
Profile 5, 12/27

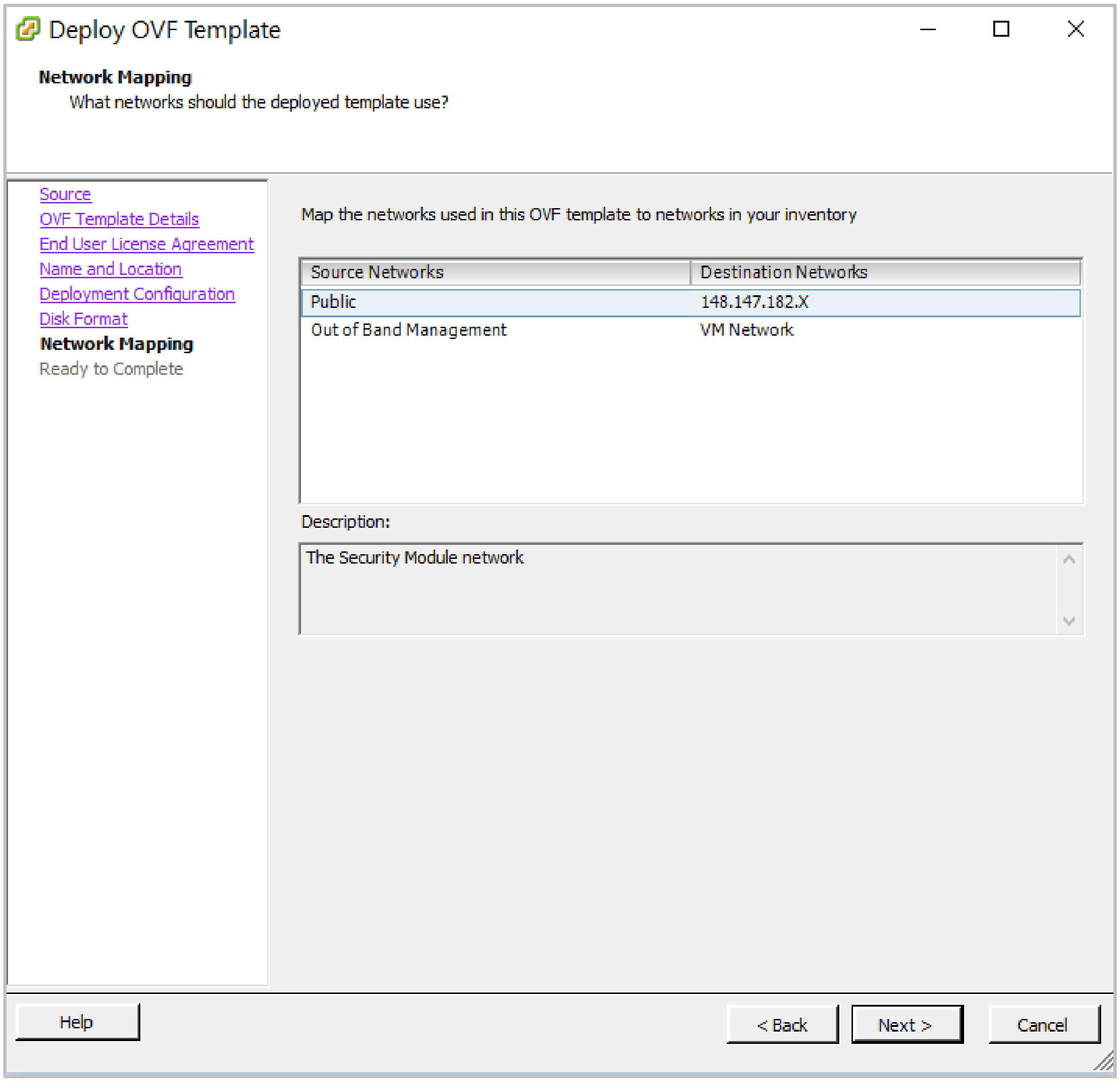
ent will req

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**.

    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



Network Mapping

What networks should the deployed template use?

Map the networks used in this OVF template to networks in your inventory

Source Networks	Destination Networks
Public	148.147.182.X
Out of Band Management	VM Network

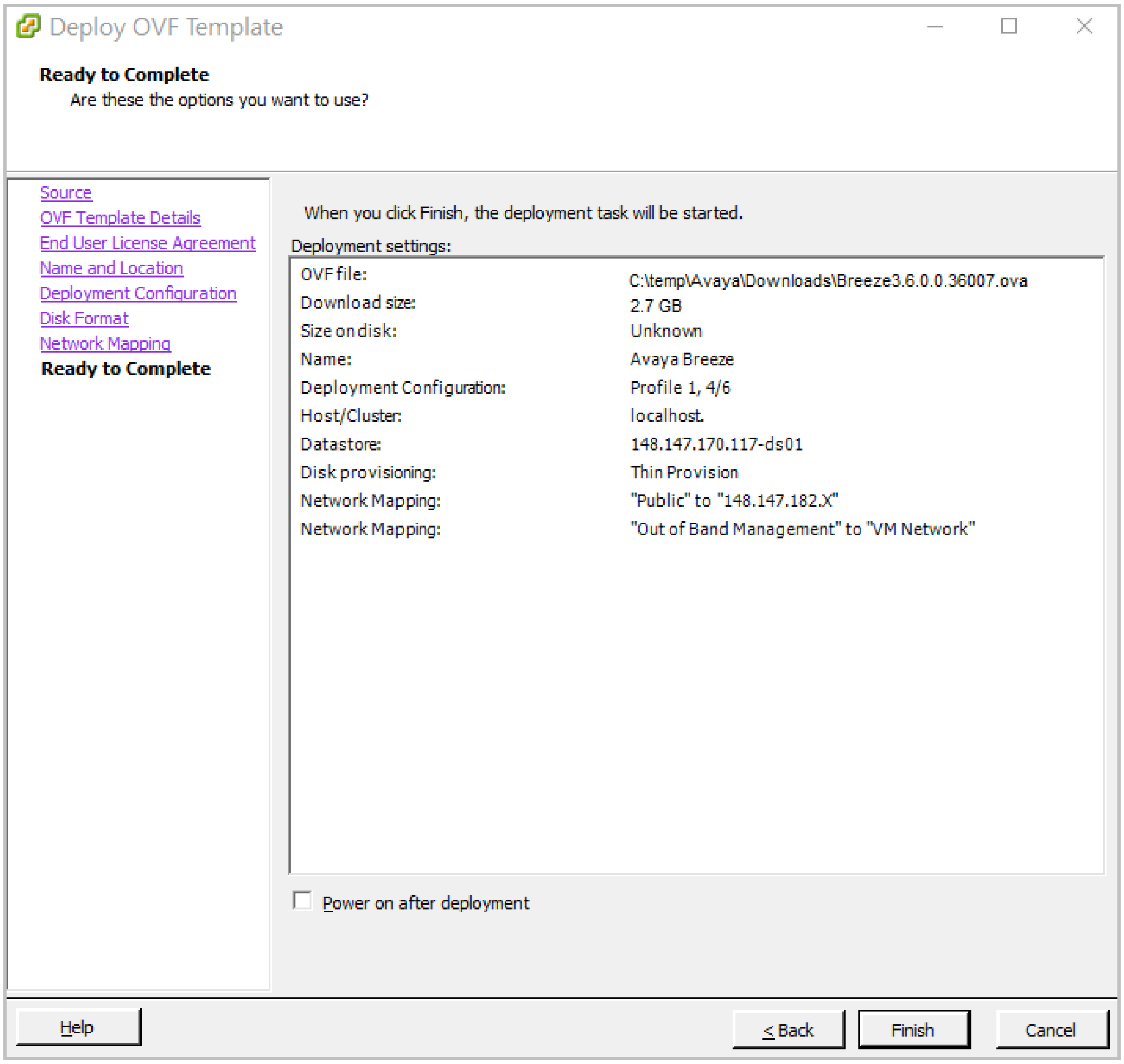
Description:

The Security Module network

11. On the Properties page, enter the configuration details for your VM. Click **Next**.

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

12. On the Ready to Complete page, verify the listed properties.



Ready to Complete

Are these the options you want to use?

When you click Finish, the deployment task will be started.

Deployment settings:

OVF file:	C:\temp\Avaya\Downloads\Breeze3.6.0.0.36007.ova
Download size:	2.7 GB
Size on disk:	Unknown
Name:	Avaya Breeze
Deployment Configuration:	Profile 1, 4/6
Host/Cluster:	localhost.
Datastore:	148.147.170.117-ds01
Disk provisioning:	Thin Provision
Network Mapping:	"Public" to "148.147.182.X"
Network Mapping:	"Out of Band Management" to "VM Network"

□ Power on after deployment

- 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**.

14. (Optional) To open a console window to your VM, right-click the VM and click **Open Console**.

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.

Get the Avaya Breeze® platform OVA file, and save it on the workstation where you will be running the VMware vSphere client to configure the new virtual machine (VM).

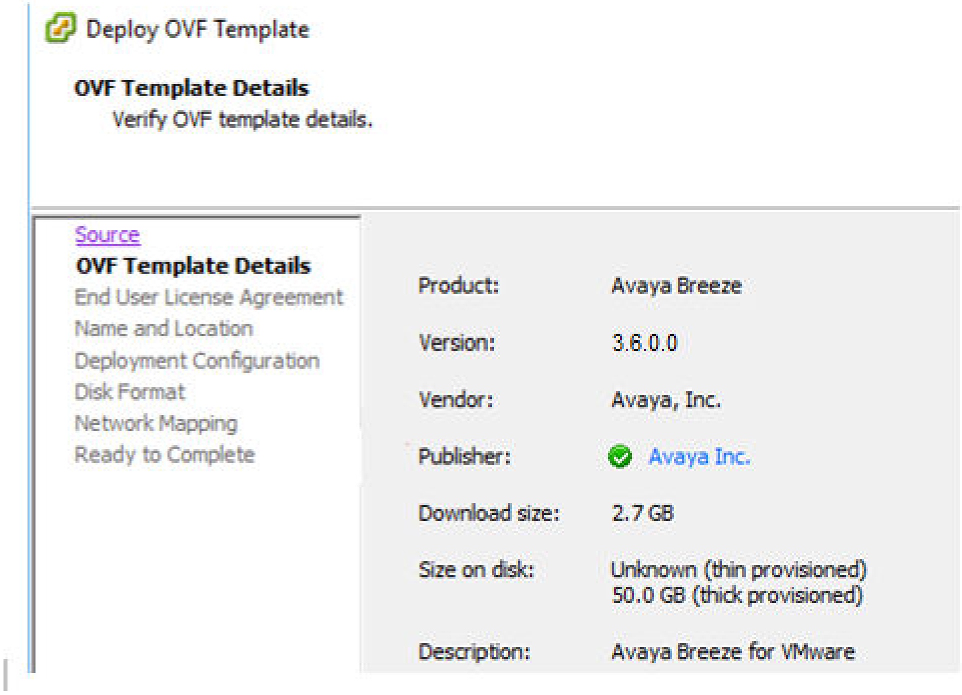
Use the *Customer Configuration Information* to get the required network settings for deployment. You can obtain the settings from an existing system if you are redeploying the OVA.

Verify that the Enrollment Password is administered and not expired.

If you are redeploying an instance of Avaya Breeze® platform, ensure that you deny new service to and power off the instance that is being redeployed.

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**.


Deploy OVF Template

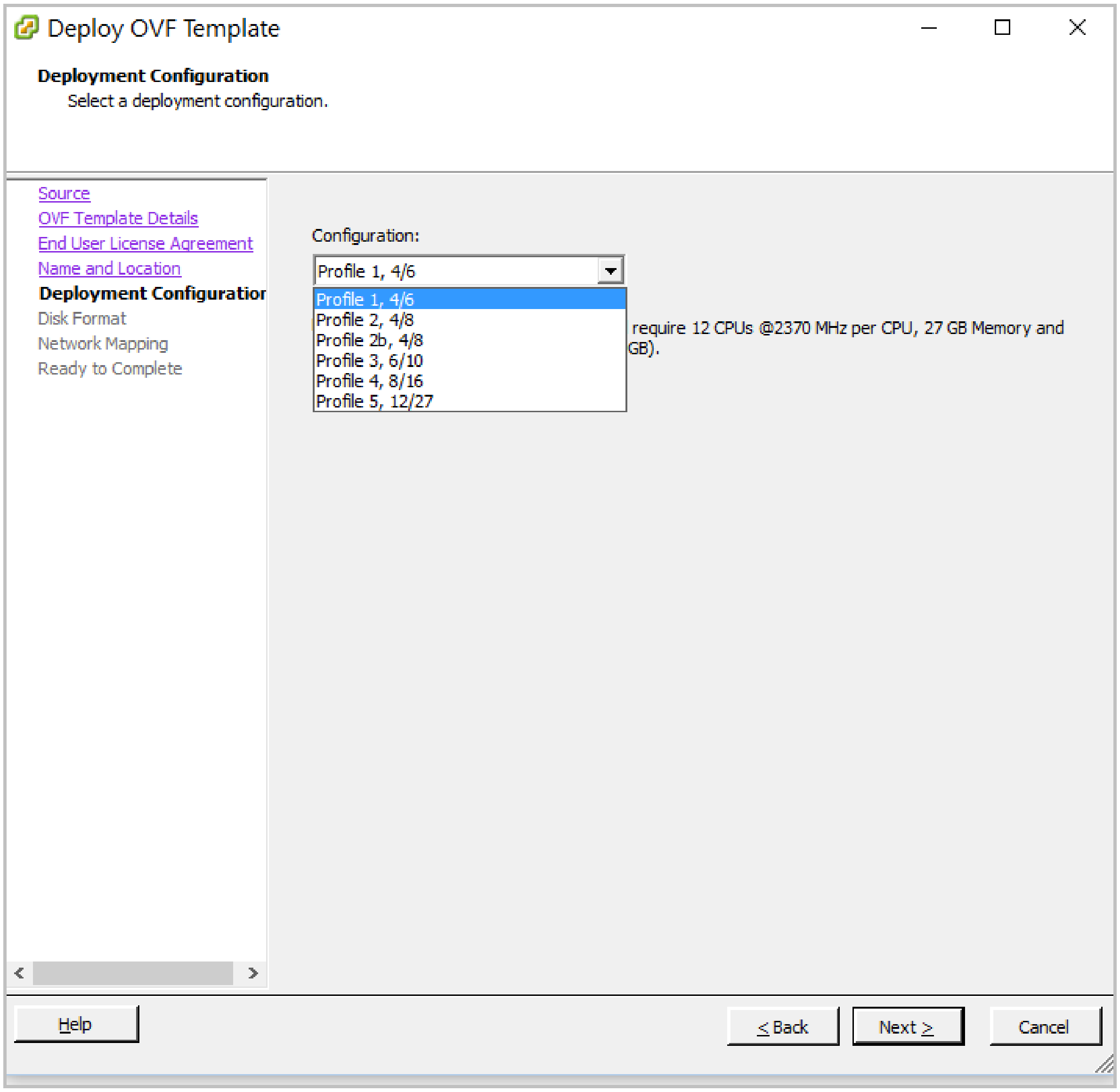
OVF Template Details

Verify OVF template details.

Product:	Avaya Breeze
Version:	3.6.0.0
Vendor:	Avaya, Inc.
Publisher:	✓ Avaya Inc.
Download size:	2.7 GB
Size on disk:	Unknown (thin provisioned) 50.0 GB (thick provisioned)
Description:	Avaya Breeze for VMware

6. If you accept the End User License Agreement click **Accept**, and 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, then click **Next**.



9. On the Disk Format page, select the disk provisioning format you want, then click **Next**.

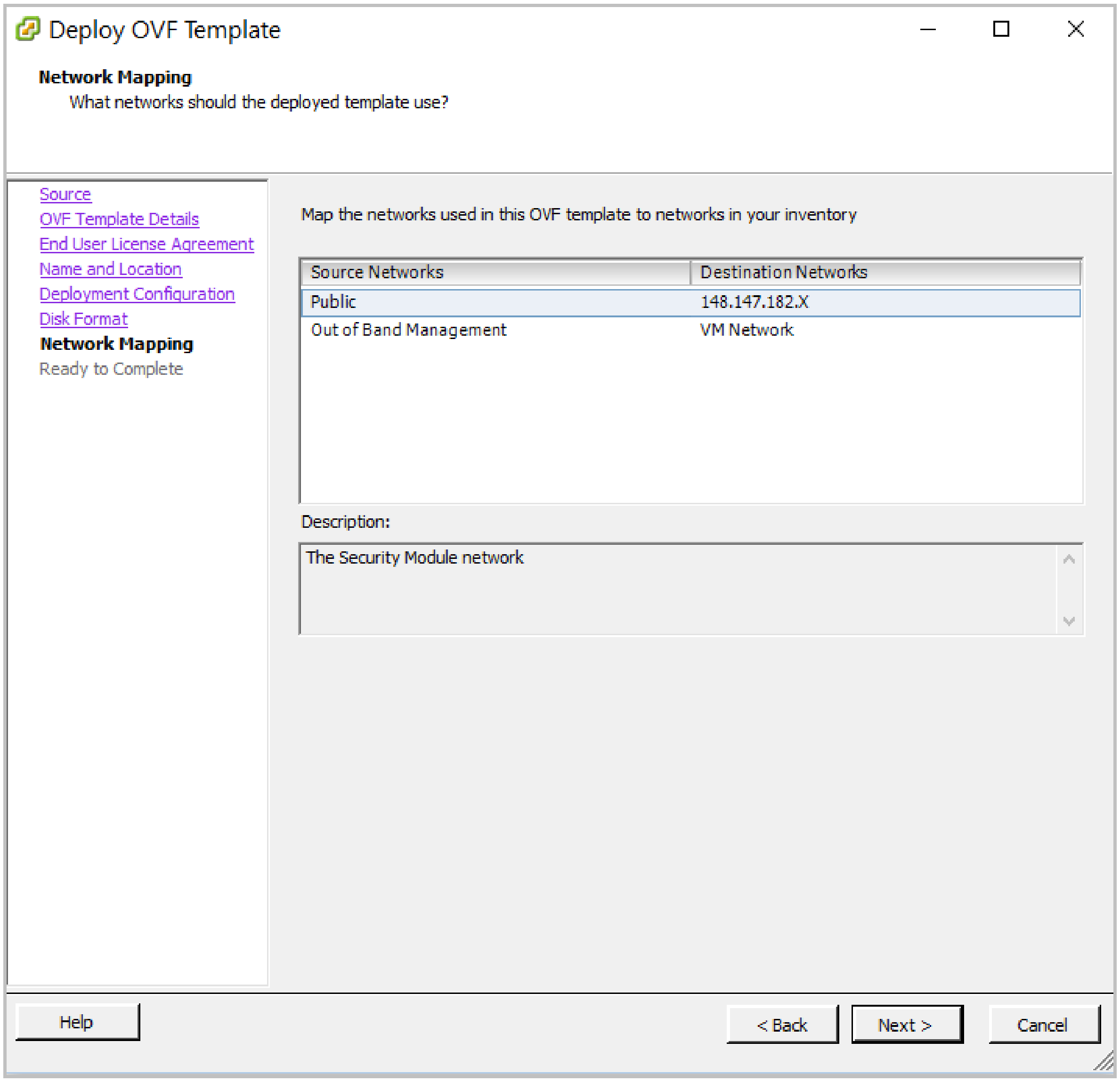
   While Avaya Breeze® platform works with either thick or thin provisioned disk, Avaya recommends using a **Thick Provision Lazy Zeroed** disk.

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



Deploy OVF Template

Network Mapping

What networks should the deployed template use?

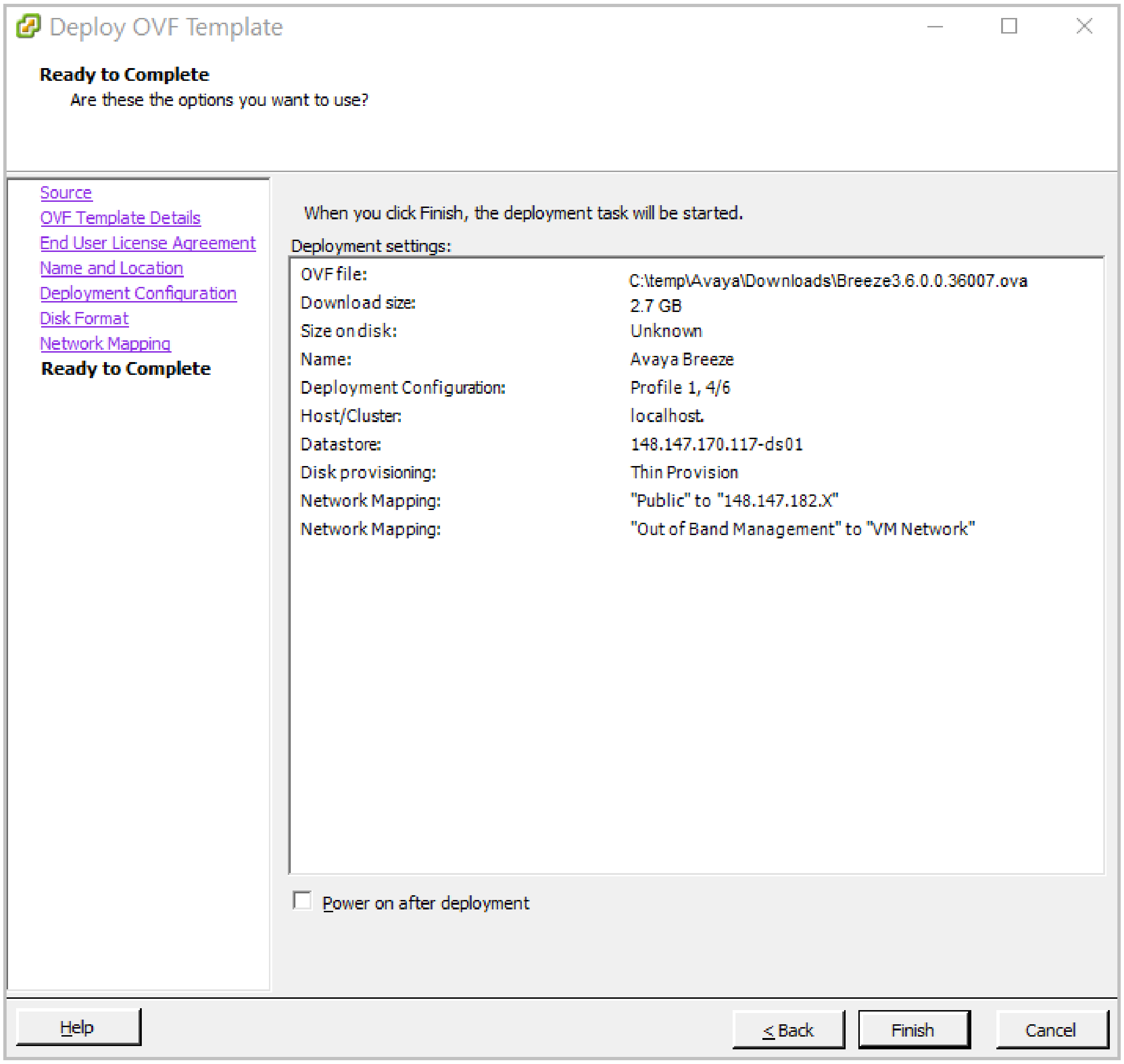
Map the networks used in this OVF template to networks in your inventory

Source Networks	Destination Networks
Public	148.147.182.X
Out of Band Management	VM Network

Description:

The Security Module network

11. On the Ready to Complete page, verify the options listed.



Ready to Complete

Are these the options you want to use?

When you click Finish, the deployment task will be started.

Deployment settings:

OVF file:	C:\temp\Avaya\Downloads\Breeze3.6.0.0.36007.ova
Download size:	2.7 GB
Size on disk:	Unknown
Name:	Avaya Breeze
Deployment Configuration:	Profile 1, 4/6
Host/Cluster:	localhost.
Datastore:	148.147.170.117-ds01
Disk provisioning:	Thin Provision
Network Mapping:	"Public" to "148.147.182.X"
Network Mapping:	"Out of Band Management" to "VM Network"

☐ Power on after deployment

Important:

Do not check the **Power on after deployment** box.

- If the values are incorrect, click **Back** to modify the values.
- If the values are correct, click **Finish**.

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.

12. Locate your new VM in the **inventory list** in the vSphere Client window.
13. Right-click to go to **Power** > **Power On**.

14. To open a console window to your VM, right-click the VM and click **Open Console**.
15. 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.

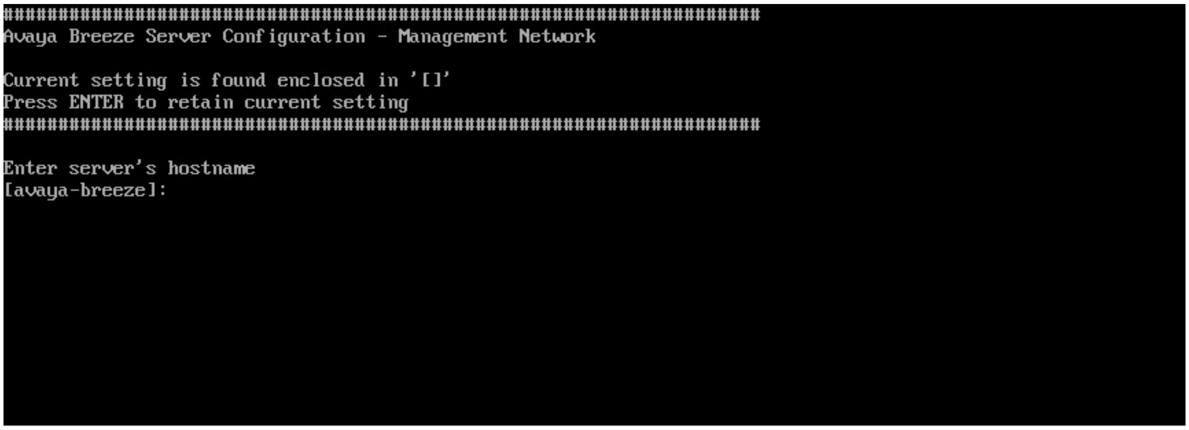
    The VM continues to boot.
16. Towards the end of the boot sequence you are prompted to configure the VM. Enter `y` to proceed.
17. When the system prompts, enter the management interface network parameters, date and time information, customer user information, and System Manager information.

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

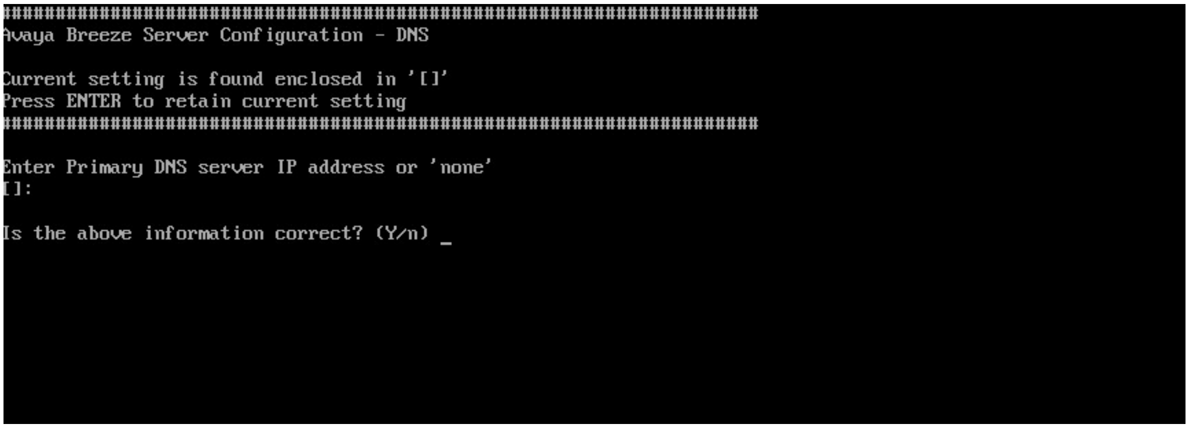
    ⊕ **Tip:**

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

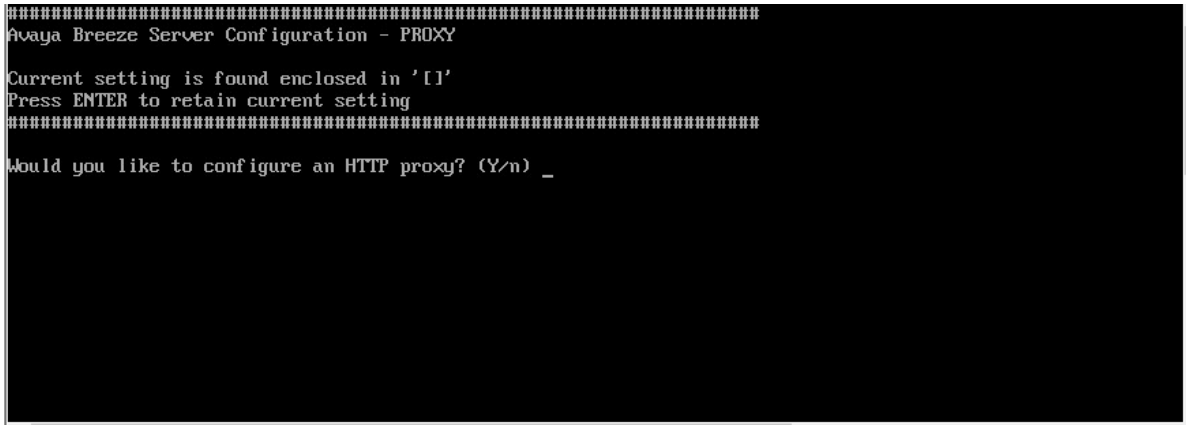
    Refer to the following screenshots.



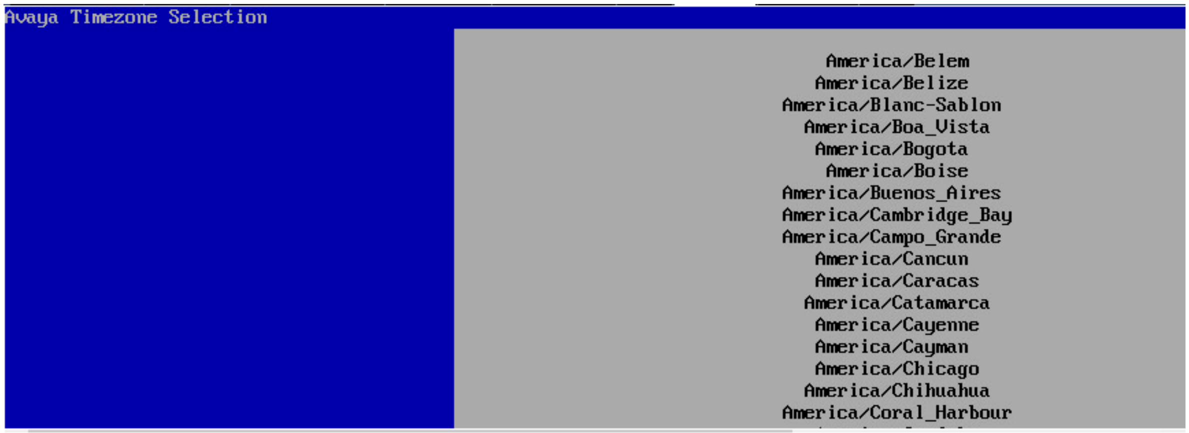
```
##########################################################################
Avaya Breeze Server Configuration - Management Network

Current setting is found enclosed in '[]'
Press ENTER to retain current setting
##########################################################################

Enter server's hostname
[avaya-breeze]:
```



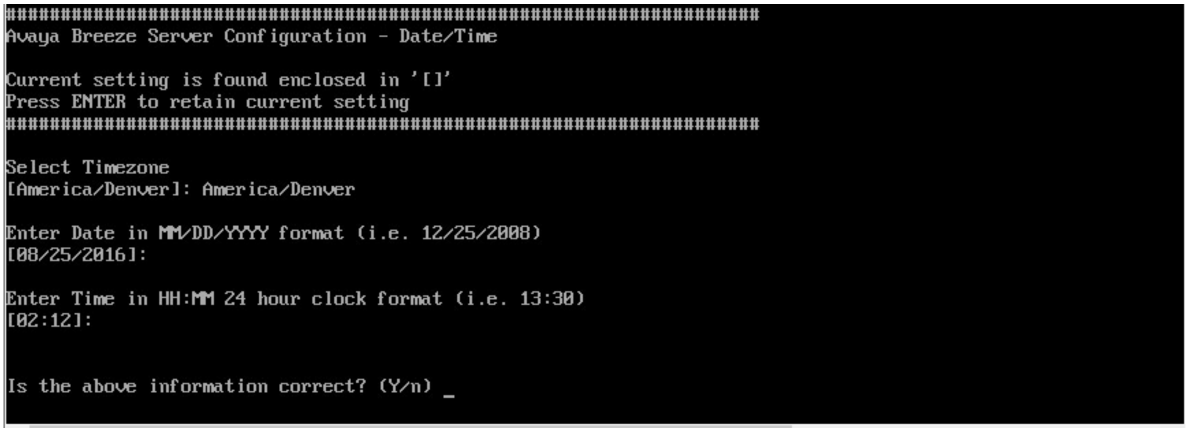
```
##########################################################################
Avaya Breeze Server Configuration - DNS

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) _
```



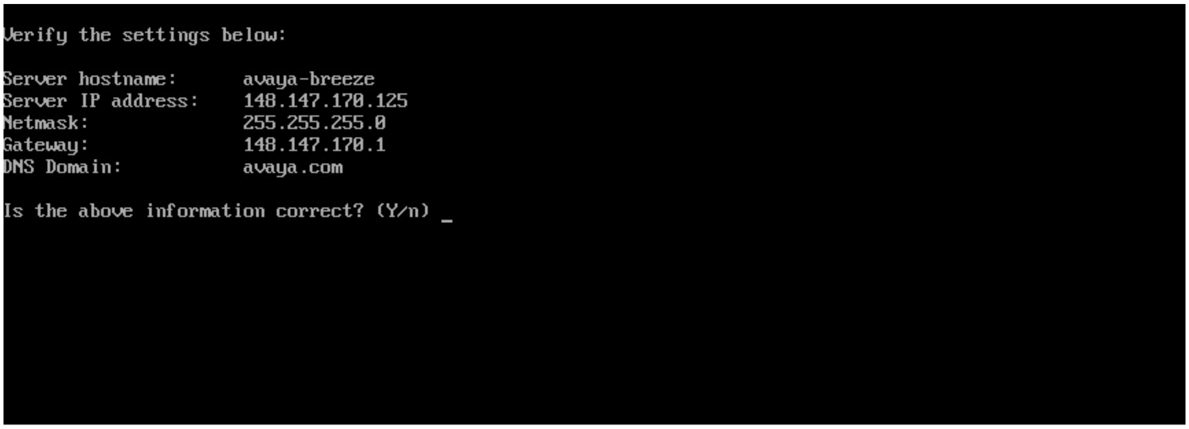
```
#####################################################################
Avaya Breeze Server Configuration - PROXY

Current setting is found enclosed in '[]'
Press ENTER to retain current setting
#####################################################################

Would you like to configure an HTTP proxy? (Y/n) _
```



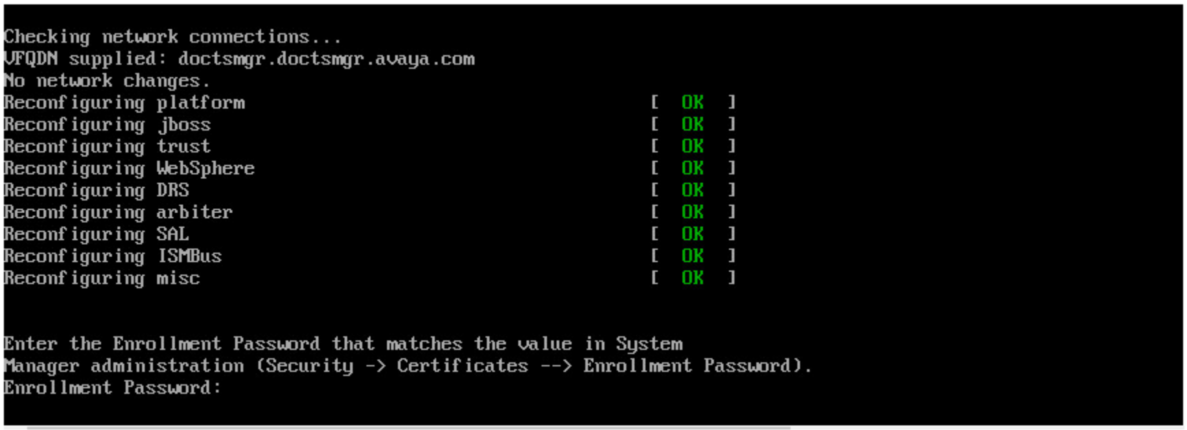
```
Avaya Timezone Selection
                                        America/Belem
                                       America/Belize
                                    America/Blanc-Sablon
                                      America/Boa_Vista
                                       America/Bogota
                                        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
```



```
#####################################################################
Avaya Breeze Server Configuration - Date/Time

Current setting is found enclosed in '[]'
Press ENTER to retain current setting
#####################################################################

Select Timezone
[America/Denver]: America/Denver

Enter Date in MM/DD/YYYY format (i.e. 12/25/2008)
[08/25/2016]:

Enter Time in HH:MM 24 hour clock format (i.e. 13:30)
[02:12]:


Is the above information correct? (Y/n) _
```



```
Verify the settings below:

Server hostname:       avaya-breeze
Server IP address:     148.147.170.125
Netmask:               255.255.255.0
Gateway:               148.147.170.1
DNS Domain:            avaya.com

Is the above information correct? (Y/n) _
```



```
Checking network connections...
VFQDN supplied: doctsmgr.doctsmgr.avaya.com
No network changes.
Reconfiguring platform                                      [  OK  ]
Reconfiguring jboss                                         [  OK  ]
Reconfiguring trust                                         [  OK  ]
Reconfiguring WebSphere                                     [  OK  ]
Reconfiguring DRS                                           [  OK  ]
Reconfiguring arbiter                                       [  OK  ]
Reconfiguring SAL                                           [  OK  ]
Reconfiguring ISMBus                                        [  OK  ]
Reconfiguring misc                                          [  OK  ]


Enter the Enrollment Password that matches the value in System
Manager administration (Security -> Certificates --> Enrollment Password).
Enrollment Password:
```

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

Deploying Avaya Breeze® platform OVA with Solution Deployment Manager

Before you begin

Install the Avaya Aura® Appliance Virtualization Platform if necessary.

The steps in this procedure use the Solution Deployment Manager.

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.

Download the Avaya Breeze® platform Open Virtual Appliance (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. On 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. Observe 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 appears 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. Use the same information that was used during installation of the Appliance Virtualization Platform.

> ✱ **Note:**
>
> 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, and click **New**.
16. In the Select Location and Platform section, perform the following steps:
    a. In **Select Location**, select a location.
    b. In **Select Host**, select a host.
    c. Select a data store.

    Alternatively, in Step 12a, you can pre-select the location and platform in the **Application Management Tree**.
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 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.
21. Click **Deploy** to begin the OVA deployment.
22. Click **Accept** to accept the license terms.
23. Click the Virtual Machines tab.
24. Click the Status Details link to display the VM deploy Status window.

When all status points display green check marks, deployment is complete and the VM is started.

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 AvayNetSetup 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

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.

Configure virtual machine automatic startup settings

You do not need to configure the virtual machine automatic startup settings if you deploy the OVA using Solution Deployment Manager. With Solution Deployment Manager the automatic startup configuration is part of the VM deployment.

With other OVA deployment methods, all virtual machines must be configured to start automatically when the vSphere ESXi host starts. Complete the procedure that corresponds to your OVA deployment method.

In high availability (HA) clusters, the VMware HA software ignores the startup selections.

Configuring virtual machine automatic startup settings using vSphere desktop client

Before you begin

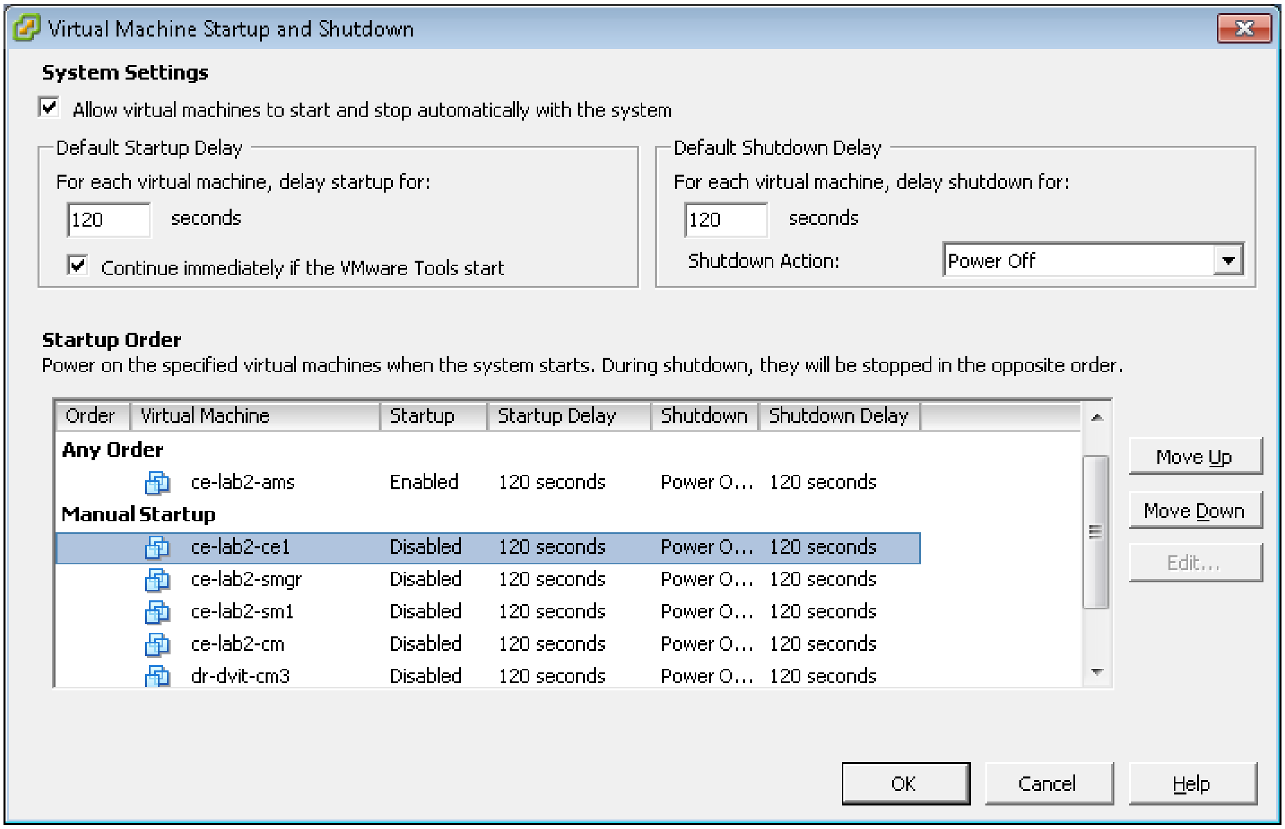
Confirm that you have the proper level of permissions to configure the automatic startup settings. If you do not have the proper level of permissions, contact your system administrator.

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 **Manual Startup** section, select the virtual machine.
7. Use the **Move up** button to move the virtual machine under **Automatic Startup**.
8. Click **OK**.

Example

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



Virtual Machine Startup and Shutdown

System Settings

☑ Allow virtual machines to start and stop automatically with the system

Default Startup Delay

For each virtual machine, delay startup for:

120 seconds

☑ Continue immediately if the VMware Tools start

Default Shutdown Delay

For each virtual machine, delay shutdown for:

120 seconds

Shutdown Action: Power Off

Startup Order

Power on the specified virtual machines when the system starts. During shutdown, they will be stopped in the opposite order.

Order	Virtual Machine	Startup	Startup Delay	Shutdown	Shutdown Delay
Any Order					
	ce-lab2-ams	Enabled	120 seconds	Power O...	120 seconds
Manual Startup					
	ce-lab2-ce1	Disabled	120 seconds	Power O...	120 seconds
	ce-lab2-smgr	Disabled	120 seconds	Power O...	120 seconds
	ce-lab2-sm1	Disabled	120 seconds	Power O...	120 seconds
	ce-lab2-cm	Disabled	120 seconds	Power O...	120 seconds
	dr-dvit-cm3	Disabled	120 seconds	Power O...	120 seconds

Configuring virtual machine automatic startup settings using 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 **Manual Startup** section, select the virtual machine.
7. Move the Avaya Breeze® platform VM to be included for Automatic Startup.

Changing the customer password on first login

Before you begin

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

- If using vCenter, set a temporary customer password during initial deployment. Regardless what you set here, you will be prompted to change it upon first login
- If using the Standalone client, set a temporary customer password post deployment during the first boot where 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 in Step 4

Patching Avaya Breeze® platform

About this task

This procedure provides general patching steps. Refer to the Release Notes and PSN to determine if there are patch-specific installation instructions.

⚠ **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.

Note:

If using Cluster Database, before upgrading the active node:

- Place the active node into Deny New Service.
- Ensure that the activity count is 0.
- Manually switchover the newly upgraded standby node and the targeted to be upgraded active node.

Before you begin

The server must be in a deny service state. You must have downloaded the patch file and copied 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. On System Manager, click **Elements** > **Avaya Breeze®** > **Server Administration**.
6. Identify the row for the Avaya Breeze® platform server you are patching. Verify the following information:
   - 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.

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 **`custAccounts -a`** command.

   The system prompts you to add this user as an EASG administrator. Accept the default value, or enter `y`. Selecting y enables the user to run the EASG commands. The system prompts you to enter the login credentials for a new customer user account you are creating.

3. Enter the user name and password for the new customer user account you are creating.

   This password is a temporary password that you must change at the first login attempt for the new account.

4. Reenter the password for confirmation.

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. Customers can enable or disable the 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.

Enabling and disabling EASG

About this task

By enabling Avaya Services Logins, you are granting Avaya access to your system. This setting is required to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner. The product must be registered using the Avaya Global Registration Tool (GRT) at https://grt.avaya.com for Avaya remote connectivity. See the Avaya support site https://support.avaya.com/registration for additional information for registering products and establishing remote access and alarming. By disabling Avaya Services Logins, you are denying Avaya access to your 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.

Procedure

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

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`.

EASG site certificate

EASG site certificates are used by the onsite Avaya technicians who do not have access to the Avaya network to generate a response to the EASG challenge. The technician will generate and provide the EASG site certificate to the customer. The customer loads this EASG site certificate on each Avaya Breeze® platform server to which the customer has granted the technician access. The EASG site certificate will only allow access to systems on which it has been installed, and will only allow access to the given Avaya technician and cannot be used by anyone else to access the system including other Avaya technicians. Once this is done, the technician logs in with the EASG challenge and response. After the technician is done, the customer can remove the EASG site certificate from the server or it will be removed by the EASG software after the site certificate expires.

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:
    - `EASGSiteCertManage --list`: To list all the site certificates that are currently installed on the system.
    - `EASGSiteCertManage --show` *`<installed_pkcs7_name>`*: To display detailed information about the specified site certificate.
4. To delete the site certificate, run the following command:
    - `EASGSiteCertManage --delete` *`<installed_pkcs7_name>`*: To delete the specified site certificate.
    - `EASGSiteCertManage --delete all`: To delete all the site certificates that are currently installed on the system.

Chapter 6: Avaya Breeze® platform System Manager Administration

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**.

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. On 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

Creating an FQDN SIP Entity on page 82

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. On 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.

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** > **Session Manager Administration**.
2. Under **Global Settings**, select **Enable Implicit Users Applications for SIP users**.
3. Click **Save**.

Administering an Avaya Breeze® platform instance

Before you begin

Get:

- The IP address or the FQDN of the Avaya Breeze® platform **Management Network Interface**.

  This is the same IP address you used when deploying the virtual machine.

  The Avaya Breeze® platform management FQDN assigned to the management network interface must be registered in DNS.

  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.
- The IP address including the network mask, and default gateway for the Avaya Breeze® platform **Security Module**.
- The SIP entity name associated to the Avaya Breeze® platform **Security Module**.

Note:

In accordance with the Avaya End User License Agreement (EULA), you can administer only the number of Avaya Breeze® platform instances allowed by the Avaya Breeze® platform license.

Procedure

1. On 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 Aura® 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 IP Address** field, type the IP address or FQDN of the Avaya Breeze® platform **Management Network Interface**.
6. In the Security Module **IPv4 Network Mask** field, type the network mask used for the SIP (Security Module) network.
7. In the Security Module **IPv4 Default Gateway** field, type the default gateway used for the SIP (Security Module) network.
8. Click **Commit** to save your changes.

   Note:

   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:

   Note:

   If an in-service cluster does not exist, you must create a new cluster.

   a. On System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
   b. Select a cluster and assign your Avaya Breeze® platform server to the cluster.

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

      For more information, see “Accepting new service”.

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*.

Verifying replication status

About this task

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

Procedure

1. On 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 might take some time to complete. Refresh the page or periodically recheck the status.

   If the status is not `Synchronized`, for more information, see *Maintaining and Troubleshooting Avaya Breeze® platform*.

Verifying the management link

Procedure

1. On 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*.

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. On 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. Use the **Context Store** profile for the Context Store snap-in, **Work Assignment** profile for the Work Assignment snap-ins, **Customer Engagement** profile for Avaya Oceana® Solution, **Core Platform** profile for Presence Services, **General Purpose Large** profile for the Engagement Call Control snap-in and the **General Purpose** profile for other snap-ins.

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

Avaya recommends using TLS v1.2.

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

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.

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. On 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**.

Cluster Database backup and restore

Backing up a cluster

About this task

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

You can backup on one cluster and restore on another.

Note:

Windows CoreFTP server is incompatible with the Cluster Backup and Restore feature and should not be used as an archive server.

Procedure

1. On 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, select **Run immediately** or **Schedule later**.

     If you select **Schedule later**, enter the appropriate details in the **Task Time**, **Recurrence**, and **Range** fields.
9. Click **Backup**.
10. To monitor the status of the backup, click **Backup and Restore** > **Job Status**.
11. To cancel the backup operation, click **Backup and Restore** > **Cancel**.

Restoring a cluster

About this task

Restore can be performed on any cluster where Cluster database is enabled.

Note:

Windows CoreFTP server is incompatible with the Cluster Backup and Restore feature and should not be used as an archive server.

Before you begin

Cluster database must be enabled.

Procedure

1. On 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 click **Restore**.
4. Select the cluster on which you want to restore the backup, and click **Continue**.

Cancelling a pending job

Procedure

1. On 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**.

Purging a backup

Before you begin

The backup to be purged must be complete.

Procedure

1. On 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**.

Reliable Eventing administration

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 that 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 features beyond what Eventing Framework provides:

- Enables delivery of events across servers and clusters.
- Guarantees event delivery with event persistence, acknowledgement, and durable subscriptions.
- Master/Slave high availability with replicated persistent messages.

Related links

Creating a Reliable Eventing group on page 65
Editing a Reliable Eventing group on page 65
Deleting a Reliable Eventing group on page 66
Viewing the status of Reliable Eventing destinations on page 66
Deleting a Reliable Eventing destination on page 67
Running a maintenance test for a broker on page 67

Creating a Reliable Eventing group

Procedure

1. On 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 the **+** icon to add an associated cluster.
   b. In the **Assigned associated clusters** table, click the **X** icon to remove an associated cluster.
6. Click **Commit**.

   The **Status** column shows one of the following:
   - Green checkmark: Indicates that the status of the broker is up and running for subscription and event transfers.
   - Red cross icon: Indicates that the status of the broker is down.
7. To view the status of the brokers, click the green checkmark.

Related links

Reliable Eventing administration on page 64

Editing a Reliable Eventing group

Procedure

1. On 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 the **+** icon to add an associated cluster.
    b. In the **Assigned associated clusters** table, click the **X** icon to remove an associated cluster.
5. Click **Commit**.

Related links

Reliable Eventing administration on page 64

Deleting a Reliable Eventing group

Procedure

1. On 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 64

Viewing the status of Reliable Eventing destinations

Procedure

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

    The system displays Broker Destination Status Page.
2. In the **Group** field, select the **Reliable Eventing group**.

    The system displays the destination status.

Related links

Reliable Eventing administration on page 64

Deleting a Reliable Eventing destination

Procedure

1. On 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 will purge the messages and delete the destination.

Related links

Reliable Eventing administration on page 64

Running a maintenance test for a broker

Procedure

1. On 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 64

Chapter 7: Avaya Aura Media Server Deployment

Avaya Aura® Media Server OVA deployment

The *Avaya Aura® Media Server deployment checklist* contains the high level deployment procedure. There are several different ways to deploy the Avaya Aura® Media Server. The detailed procedure used to deploy the Avaya Aura® Media Server Open Virtual Appliance (OVA) can be found in the *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 will enable the files to be stored unencoded on the remote HTTP location. The check box is on the **Home** > **System Configuration** > **Media Processing** > **Advanced Settings** page. This setting also helps in file transfer performance

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. Click **Save**.
10.
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**.

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

Procedure

1. On 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 can take up to two minutes to update Avaya Breeze® platform.

    You cannot assign Avaya Aura® Media Server to multiple applications.

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 administer only 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**.

Installing the Avaya Aura® Media Server license file

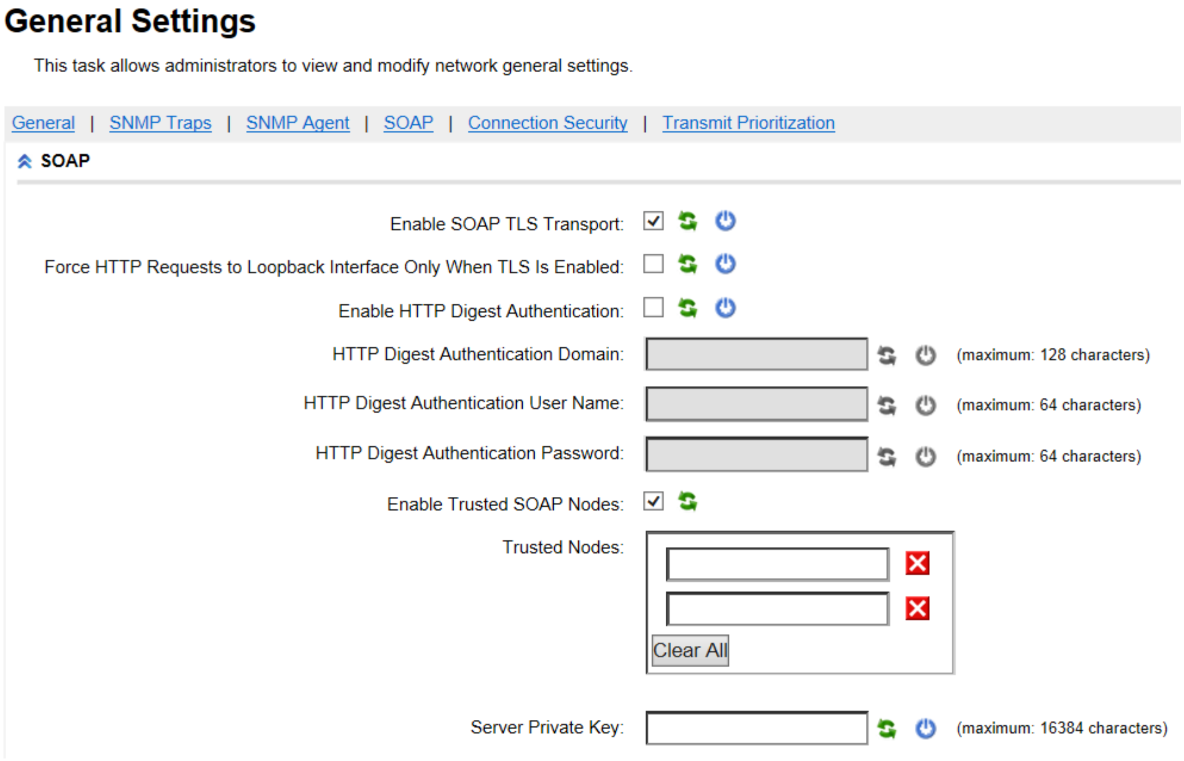
Procedure

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**.

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**.



General Settings

This task allows administrators to view and modify network general settings.

General | SNMP Traps | SNMP Agent | SOAP | Connection Security | Transmit Prioritization

SOAP

Enable SOAP TLS Transport: ☑

Force HTTP Requests to Loopback Interface Only When TLS Is Enabled: □

Enable HTTP Digest Authentication: □

HTTP Digest Authentication Domain: (maximum: 128 characters)

HTTP Digest Authentication User Name: (maximum: 64 characters)

HTTP Digest Authentication Password: (maximum: 64 characters)

Enable Trusted SOAP Nodes: ☑

Trusted Nodes: ☒ ☒ Clear All

Server Private Key: (maximum: 16384 characters)

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.

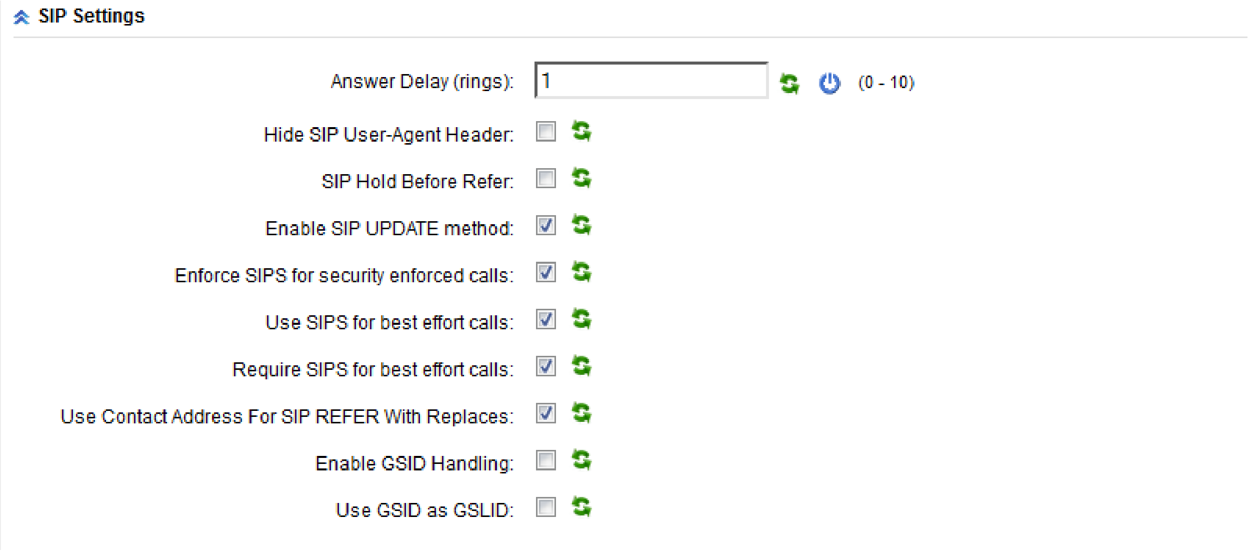
Next steps

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.

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**.



SIP Settings

Answer Delay (rings): 1 (0 - 10)

Hide SIP User-Agent Header: □

SIP Hold Before Refer: □

Enable SIP UPDATE method: ☑

Enforce SIPS for security enforced calls: ☑

Use SIPS for best effort calls: ☑

Require SIPS for best effort calls: ☑

Use Contact Address For SIP REFER With Replaces: ☑

Enable GSID Handling: □

Use GSID as GSLID: □

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**

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

Configuring Avaya Aura Media Server name resolution (alternative 1) on page 73

Configuring connection security options (alternative 2) on page 74

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 72

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 72

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”

Exporting an Avaya Aura® Media Server certificate

Procedure

1. On 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**.

Enabling and configuring digit relay settings

About this task

Note:

Digit relay configuration changes and preferences must be configured on the controlling application and not Avaya Aura® MS. Please refer to controlling application documentation since these configuration changes will be typically ignored, but may be required in certain cases.

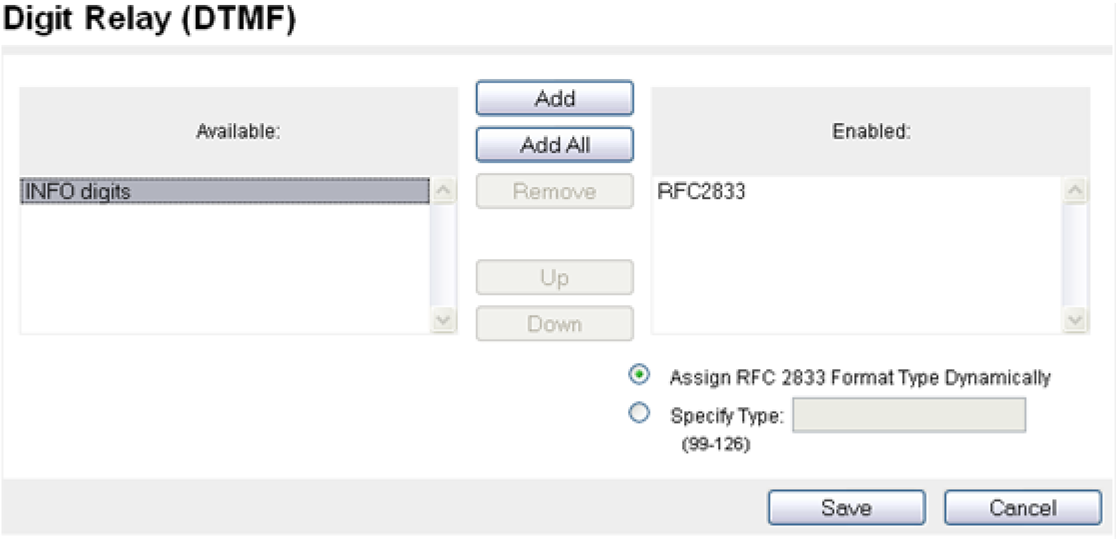
Avaya Aura® MS uses digit relay settings and the order of the enabled relay methods when negotiating digit relay with a client endpoint. These settings apply for inbound or outbound sessions.

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)**.



Digit Relay (DTMF)

Available: INFO digits

Enabled: RFC2833

● Assign RFC 2833 Format Type Dynamically

○ Specify Type: (99-126)

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**.

Chapter 8: Certificate administration

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”.

Entities that access Avaya Breeze® platform via HTTPS must be able to resolve the Common Name (CN) or SAN fields in the certificate with the FQDN of the Avaya Breeze® platform node. 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 theAvaya Breeze® platform 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 host name 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*.

Viewing Identity Certificate details

Procedure

1. On 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**.

Adding a Trust 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 to System Manager.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. Select the cluster to which you want to administer the trusted certificates.
3. Click **Certificate Management** > **Install Trust Certificate (All Avaya Breeze® Instances)** to download the trusted certificate for all the servers in the cluster.

✱ **Note:**

The Trust Certificate that you are about to add will apply to all the 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 **Browse** to the location of your Trust Certificate, and select the certificate.
6. Click **Retrieve Certificate**, and review the details of the Trusted Certificate.
7. Click **Commit** .

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. On 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**.

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**.

    The system displays the Replace Identity Certificate page.

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 JBoss on System Manager.

Chapter 9: High Availability Administration

Avaya Breeze® platform high availability administration

High availability is achieved for Avaya Breeze® platform by sending traffic to a cluster with multiple servers. Load balancing determines what percentage of traffic each server will receive. Clusters are auto configured with the datagrid and the HTTP load balancing functionality. The SIP load balancers are not configured in these servers and clusters. Therefore, for SIP high availability, you must manually configure load balancing. You must enable HTTP load balancing for a cluster; by default load balancing is not enabled.

SIP high availability

SIP high availability 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 a 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. In order 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 in the following procedure.

Related links

Local load balancing recommendation on page 86

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. On 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

Administering an Avaya Breeze platform SIP Entity on page 54

Creating the FQDN Entity Link

Before you begin

Create the FQDN SIP Entity.

About this task

For a 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 high availability 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 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. On 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. See Administering the Avaya Breeze platform Entity Link on page 55 for information about the Session Manager and Avaya Breeze® platform Entity Link.

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, like 5091. This represents the Session Manager side of the High Availability 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 High Availability 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 55.

   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 High Availability FQDN entity link as well.
9. Click **Commit** to save your changes.
10. On 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 the Default Domain, select the root domain used for call routing.
15. Click **Commit**.

Creating an Application and Application Sequence for high availability

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. On 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. Uncheck the **Mandatory** box if necessary.

   Session Manager stops processing a call if it cannot reach a mandatory application.
10. To save your Application Sequence, click **Commit**.

Determining active and standby database servers

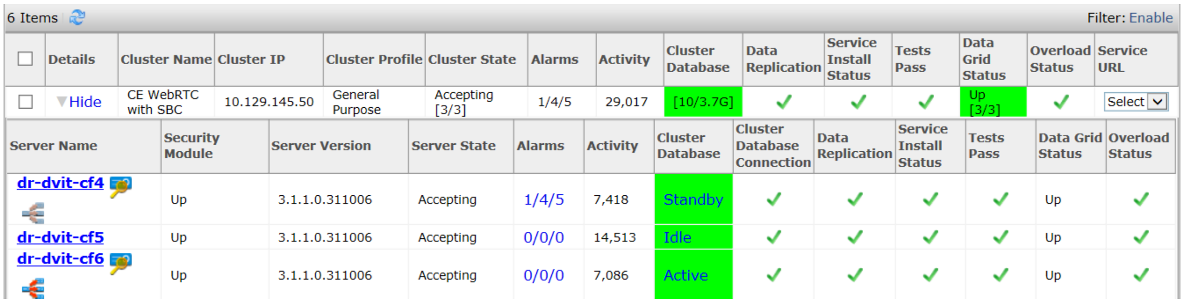
About this task

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. On 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.



6 Items

Filter: Enable

□	Details	Cluster Name	Cluster IP	Cluster Profile	Cluster State	Alarms	Activity	Cluster Database	Data Replication	Service Install Status	Tests Pass	Data Grid Status	Overload Status	Service URL
□	▼Hide	CE WebRTC with SBC	10.129.145.50	General Purpose	Accepting [3/3]	1/4/5	29,017	[10/3.7G]	✓	✓	✓	Up [3/3]	✓	Select

Server Name	Security Module	Server Version	Server State	Alarms	Activity	Cluster Database	Cluster Database Connection	Data Replication	Service Install Status	Tests Pass	Data Grid Status	Overload Status
dr-dvit-cf4	Up	3.1.1.0.311006	Accepting	1/4/5	7,418	Standby	✓	✓	✓	✓	Up	✓
dr-dvit-cf5	Up	3.1.1.0.311006	Accepting	0/0/0	14,513	Idle	✓	✓	✓	✓	Up	✓
dr-dvit-cf6	Up	3.1.1.0.311006	Accepting	0/0/0	7,086	Active	✓	✓	✓	✓	Up	✓

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

Resolving the local host name for high availability

Procedure

1. Verify that at least one entity link has been defined for each FQDN and Transport entry.
2. On 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 Fully Qualified Domain Name 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** that the host should use for routing using the particular IP address.
    d. Enter a value for the **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 for the **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, the 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 a **Transport**. The default is TLS.
5. Click **Commit**.

Related links

Local load balancing recommendation on page 86
Geo-redundancy load balancing example configuration on page 87

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

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

Avaya Breeze® platform SIP high availability deployment checklist

The following table lists the procedures required to deploy Avaya Breeze® platform in a SIP high availability configuration.

#	Action	Reference/Notes	✔
1	Create an FQDN SIP Entity.	Creating an FQDN SIP Entity on page 82	
2	Create the FQDN Entity Link.	Creating the FQDN Entity Link on page 83	
3	Create a high availability Application and Application Sequence.	Creating an Application and Application Sequence for high availability on page 84	
4	Resolve the local host name.	Resolving the local host name for high availability on page 86	
5	Enable load balancing for the cluster.	Enabling HTTP load balancing in an Avaya Breeze platform cluster on page 89	

HTTP high availability

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.
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 Snap-in.

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 for Enterprise. The header which is used to identify the real client IP address is X-Real-IP

Enabling HTTP load balancing in an Avaya Breeze® platform cluster

About this task

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

Before you begin

1. When you select the load balancing option during **Edit** operation, change the state of the cluster to **Deny New Service**. 2. After enabling the load balancing functionality, change the state of the cluster back to **Accept New Service**.

Procedure

1. On 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.

   If the **Is Load Balancer enabled** check box is selected and the load balancer node in the cluster is in the Accepting state, the **Cluster State** field displays **Accepting**. If the **Is Load Balancer enabled** check box is cleared and at least one of the node in the cluster is in the Accepting state, the **Cluster State** field displays **Accepting**. discuss
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. It must not match the Security Module IP address or the management IP address. The Security Module IP address must be on the same subnet as the Avaya Breeze® platform **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, select **Accept New Service**.

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.

Chapter 10: Communication Manager Administration

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.

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.

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 route these calls 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 don't route to a specific Dialed String use a Route Pattern that directs them to your SIP trunk group. (This can be done using a Dialed String value of "x.")
2. In Session Manager create a Digit Conversion Adapter for the Communication Manager entity . In the **Insert Digits** field, add the ARS FAC and steering digits, (999 for example) that will not be confused with an area code.
3. In Communication Manager set up your AAR Digit Analysis so that calls with a dialed string of your administered steering digits (999 for example) 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.

Chapter 11: Resources

Documentation

See the following related documents at http://support.avaya.com.

Title	Use this document to:	Audience
Understanding		
Avaya Breeze® platform Overview and Specification	Understand the Avaya Breeze® platform 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
Implementing		
Deploying Avaya Breeze® platform	Deploy and configure Avaya Breeze® platform.	Services and support personnel System administrators
Deploying Zang-Enabled Avaya Breeze® platform	Deploy and configure Zang-enabled Avaya Breeze® platform.	Services and support personnel System administrators
Upgrading Avaya Breeze® platform	Upgrade Avaya Breeze® platform.	Services and support personnel
Implementing and Administering Avaya Aura® Media Server	Deploy and configure Avaya Aura® Media Server.	System administrators

Table continues…

Title	Use this document to:	Audience
		Services and support personnel
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	Deploy and configure Avaya Aura® System Manager in a virtualized environment using VMware.	System administrators Services and support personnel
Avaya Aura® System Manager Solution Deployment Manager Job-Aid	Use Solution Deployment Manager.	System administrators Services and support personnel
Migrating and Installing Avaya Aura® Appliance Virtualization Platform	Deploy and configure Avaya Aura® Appliance Virtualization Platform.	System administrators Services and support personnel
Deploying Avaya Session Border Controller for Enterprise	Deploy and configure Avaya Aura® Session Border Controller.	System administrators Services and support personnel
Customizing		
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.	Programmers
Avaya Breeze® platform API Javadocs	Understand API classes and uses.	Programmers
Supporting		
Maintaining and Troubleshooting Avaya Breeze® platform	Troubleshoot Avaya Breeze® platform.	Services and support personnel System administrators
Troubleshooting Avaya Aura® Session Manager	Troubleshoot Avaya Aura® Session Manager.	Services and support personnel

Table continues…

Title	Use this document to:	Audience
Troubleshooting Avaya Aura® System Manager	Troubleshoot System Manager.	Services and support personnel
Using		
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
Administering Avaya Breeze® platform	Administer Avaya Breeze® platform and snap-ins.	System Administrators Services and Support personnel
Administering Avaya Aura® Session Manager	Administer Avaya Aura® Session Manager.	System Administrators Services and support personnel
Administering Avaya Aura® System Manager	Administer Avaya Aura® System Manager.	System Administrators Services and support personnel
Administering Avaya Session Border Controller for Enterprise	Administer Avaya Aura® Session Border Controller.	System Administrators Services and support personnel

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com/.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.
7. Click **Enter**.

Avaya Documentation Portal navigation

Customer documentation for some programs is now available on the Avaya Documentation Portal at https://documentation.avaya.com/.

Important:

For documents that are not available on the Avaya Documentation Portal, click **Support** on the top menu to open https://support.avaya.com/.

Using the Avaya Documentation Portal, you can:

- Search for content in one of the following ways:
  - Type a keyword in the **Search** field.
  - Type a keyword in **Search**, and click **Filters** to search for content by product, release, and document type.
  - Select a product or solution and then select the appropriate document from the list.
- Find a document from the **Publications** menu.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** (☆).

  Navigate to the **My Content** > **My Docs** menu, and do any of the following:

  - Create, rename, and delete a collection.
  - Add content from various documents to a collection.
  - Save a PDF of selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive content that others have shared with you.
- Add yourself as a watcher by using the **Watch** icon (👁).

  Navigate to the **My Content** > **Watch list** menu, and do the following:

  - Set how frequently you want to be notified, starting from every day to every 60 days.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

  As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the portal.
- Share a section on social media platforms, such as Facebook, LinkedIn, Twitter, and Google +.
- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log in to the portal. The available functionality depends on the role with which you are logged in.

Training

The following courses are available on the Avaya Learning website at http://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
2016W	Fundamentals of Avaya Breeze® platform
2316W	Avaya Breeze® platform Client SDK Fundamentals
2024V	Programming Avaya Breeze® platform Snap-ins using Java SDK Bootcamp
2024T	Programming Avaya Breeze® platform Snap-ins using Java SDK Online Test
20250V	Programming Avaya Breeze® platform Snap-ins using Engagement Designer
20250T	Programming Avaya Breeze® platform R3 Snap-ins using Engagement Designer Online Test
5105	Avaya Breeze® platform Implementation and Support Test
7016W	Avaya Breeze® platform Implementation and Support

Avaya Breeze® platform videos

Avaya Breeze® platform provides the following videos to help in the development and deployment of snap-ins. Access these videos at http://www.avaya.com/breezedeveloper.

Title	Audience
Getting Started with the Avaya Breeze® platform SDK: Windows	Programmers
Getting Started with the Avaya Breeze® platform SDK: Linux	Programmers
Creating Your First Service — Part 1	Programmers
Creating Your First Service — Part 2	Programmers
Server Installation and Configuration with vCenter	System Administrators, Services and Support personnel
Server Installation and Configuration without vCenter	System Administrators, Services and Support personnel

Table continues…

Service Installation, Configuration, and Test	Programmers
Understanding the Hello Sample Service	Programmers
Understanding the Multi-Channel Broadcast Sample Service	Programmers
Understanding the Whitelist Sample Service	Programmers

Support

Platform support

Go to the Avaya Support website at www.avaya.com/Support for the most up-to-date product documentation, and product notices. 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.

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.

Appendix A: 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.

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. On 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.

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. On 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.

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.

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*.

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. On 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.

Index