Upgrading Avaya Breeze™

Release 3.5
Issue 1
July 2018

© 2013-2018, Avaya Inc.
All Rights Reserved.

Notice

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

Documentation disclaimer

“Documentation” means information published in varying 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 G.729 CODEC, 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 G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. 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.

All non-Avaya trademarks are the property of their respective owners.
Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction ... 6
Purpose ... 6
Chapter 2: Upgrade overview and considerations ... 7
Required permissions ... 7
Supported upgrades ... 7
Upgrades licensing ... 8
Password restriction ... 8
Latest software updates and patch information ... 8
Avaya Aura® Media Server selection algorithm ... 9
Chapter 3: Upgrading Avaya Breeze™ ... 10
Supported upgrading paths ... 10
Upgrading with Method 1 ... 10
Upgrading with Method 2 ... 56
Upgrading with Method 3 ... 73
Enhanced Access Security Gateway ... 92
Chapter 4: Patching ... 94
Determining patching sequence ... 94
Patching Avaya Breeze™ ... 95
Patch command options ... 96
Chapter 5: Resources ... 97
Documentation ... 97
Finding documents on the Avaya Support website ... 99
Training ... 100
Avaya Breeze™ videos ... 100
Viewing Avaya Mentor videos ... 100
Support ... 101
Using the Avaya InSite Knowledge Base ... 101
Appendix A: Removing obsolete Avaya Aura® Media Server configuration ... 103
Checklist for removing obsolete Avaya Aura® Media Server configuration in System Manager ... 103
Removing the Avaya Aura® Media Server Routing Pattern ... 103
Removing the SIP Entity Links for Avaya Aura® Media Server ... 104
Removing the SIP Entity for each Avaya Aura® Media Server ... 104
Removing the Avaya Aura® Media Server Host Name Resolution ... 104

Chapter 1: Introduction

Purpose

This document provides procedures for upgrading Avaya Breeze™ from Release 3.0 or later to Release 3.5. The document includes upgrade checklist, upgrade procedures, and verification procedures for each supported upgrade path.

People who perform upgrades can use this document.

Chapter 2: Upgrade overview and considerations

Required permissions

To upgrade Avaya Breeze™, you must have permissions to:

- Log in to a craft or cust account.
- Administer the Avaya Breeze™ Element Manager on System Manager.

Supported upgrades

Due to enhanced security changes in Release 3.5, all upgrades to Release 3.5 are service impacting.

Before upgrading Avaya Breeze™, first upgrade to the latest release of System Manager and then upgrade to the latest release of other Avaya Aura® components. Upgrade Avaya Aura® Media Server first and then upgrade Avaya Breeze™. Avaya Breeze™ Release 3.5 is compatible with Avaya Aura® Media Server Releases 8.0. For information about upgrading Avaya Aura® Media Server, see *Implementing and Administering Avaya Aura® Media Server*.

Avaya Breeze™ Release 3.5 requires:

- System Manager Release 8.0 installed to update the Avaya Breeze™ Element Manager to Release 3.5.

For snap-ins that process calls, Avaya Breeze™ Release 3.5 requires:

- Session Manager Releases 6.3.8 and later.

For snap-ins that use the Avaya Aura® Media Server, Avaya Breeze™ Release 3.5 requires:

- Avaya Aura® Media Server Release 8.0.

Avaya Breeze™ supports Communication Manager 6.3.6 and later releases.

Avaya Breeze™ supports snap-ins built with 3.0 and later SDK. You must contact your snap-in vendor for your specific combination or for any concerns related to your existing snap-in on this new platform release without recompiling with Release 3.5 SDK. You must also refer to Avaya Breeze™ Release 3.5 release notes for any known issues that might impact your snap-in.

For the latest and most accurate upgrade compatibility information, go to https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Note:

It is recommended that you upgrade to the latest releases for all components.

Upgrades licensing

Upgrading Avaya Breeze™ to Release 3.5 does not require a new Avaya Breeze™ license file. However, if you are upgrading System Manager to Release 8.0, a new Avaya Breeze™ license will need to be installed during that upgrade, unless you use SDM client for the System Manager upgrade.

Avaya Breeze™ uses the Avaya Product Licensing and Delivery System (PLDS) to manage license entitlement and generate license files. License files are downloadable from PLDS and are installed on System Manager WebLM. In a network with multiple Avaya Breeze™ servers and clusters, only a single license file installed on System Manager WebLM is needed to license all the Avaya Breeze™ servers.

Password restriction

Password restrictions are enforced on the cust accounts. A cust user is forced to change the password on first login and the password that the user enters must meet the password complexity needs. This restriction is only for new Release 3.5 deployments and when upgrading from Release 3.2 and later to Release 3.5.

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 (PSN), and Product Correction Notices (PCN) 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™ 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™.
- 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™ 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™. If a location has been assigned to the Avaya Breeze™ server that is handling a call, Avaya Breeze™ 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 3.5 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 3.5. You shoud enable the rule after upgrade.

Chapter 3: Upgrading Avaya Breeze™

Supported upgrading paths

Select your upgrade method from the following table.

Release	Upgrade procedure
3.0.x to 3.5	See Method 1 overview on page 10.
3.1.x to 3.5	See Method 1 overview on page 10.
3.2.x to 3.5	See Method 1 overview on page 10.
3.3.x to 3.5	See Method 2 overview on page 56.
3.4.x to 3.5	See Method 2 overview on page 56.

Note:

Before upgrading, you must disable CRL on the System Manager instance. On the **Security** > **Configuration** > **Security Configuration** page, set the **Certification Revocation Validation** field to **NONE**.

Note:

Do not add Release 3.3 or earlier nodes to an upgraded Release 3.5 cluster.

Upgrading with Method 1

Method 1 overview

The OVA upgrade requires the reinstallation of the Avaya Breeze™ OVA on each server in the cluster after all nodes are removed from the cluster. Cluster database and data grid data are not preserved. The upgrade is service impacting. Complete upgrades during a maintenance window.

After upgrading and using Avaya Aura® Media Server, you must configure the new REST-based configuration. If not using Avaya Engagement Assistant Snap-in, then remove the existing Avaya Aura® Media Server SIP version of configuration. If using Avaya Engagement Assistant Snap-in, then leave the existing Avaya Aura® Media Server SIP version configuration.

Avaya Aura® Media Server that are supporting the cluster must be upgraded to Release 8.0.

Checklist for Method 1 upgrades

Caution:

Upgrades using OVA file are service impacting. Complete upgrades during a maintenance window.

Snap-ins may have pre-requisite activity and post-upgrade activity that needs consideration before proceeding with the Platform upgrade. For more information, refer to the snap-in documentation.

#	Action	Link/Notes	✔
1	Access and record information for the existing Avaya Breeze™ servers that you will require for OVA deployment. Run the **`ceconfig`** command and record the information.	Customer configuration information for OVA upgrades on page 15. Recording configuration information on page 15.	
2	Before upgrading Avaya Breeze™, upgrade the following in this order to the required release: 1. System Manager 2. Session Manager	Refer to the *Upgrading Avaya Aura® System Manager* and *Upgrading Avaya Aura® Session Manager* documents.	
3	Upgrade Avaya Aura® Media Server.	Refer to *Deploying and Updating Avaya Aura® Media Server Appliance*. Upgrade Avaya Aura® Media Server within the same maintenance window if your Avaya Breeze™ is Release 3.0.	
4	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 DNS or must have an entry in /etc/hosts.	

Table continues…

#	Action	Link/Notes	✔
		• System Manager and Avaya Aura® Media Server need to be on the same domain.	
5	Administer Avaya Aura® Media Server for REST.	Administering Avaya Aura Media Server for REST on page 19	
6	Assign Avaya Aura® Media Server for use with Avaya Breeze™.	Assigning Avaya Aura Media Server for use with Avaya Breeze on page 20	
7	If the cluster database is enabled and you want to keep the data that is stored in the cluster database, take a backup.	Refer to *Administering Avaya Breeze™*. This step is not applicable for Release 3.0.	
8	Download the Avaya Breeze™ OVA and patch file (if required) from PLDS. Place the OVA on a network share connected to vCenter or vSphere. After deploying the OVA, copy the patch file to each server you will be upgrading.	Downloading software from PLDS on page 20.	
9	Verify that the **Enrollment Password** is not expired.	Verifying Enrollment Password status on page 21.	
10	Change the state of the cluster you are upgrading to **Deny New Service**.	Denying new service on page 21.	
11	Verify that the cluster **Activity** field is zero.	Verifying activity on page 22.	
12	Clear the **Enable Database Auto Switchover** field on the **Elements** > **Avaya Breeze™** > **Cluster Administration** general page.	—	This step is only required for multi-node clusters with Cluster database.
13	Remove all Avaya Breeze™ servers from the cluster.	Removing Avaya Breeze servers from the cluster for upgrading on page 22	
14	Shut down all the servers in the cluster before deploying the OVA on the first server.	Shutting down servers on page 23. **Note:** Rename and retain the original image if resources allow until the upgrade is complete.	

Table continues…

#	Action	Link/Notes	✔
15	Deploy the Avaya Breeze™ OVA. Upgrade the mandatory snap-ins and connector snap-ins. For more information, refer to the snap-in documentation.	You can deploy the OVA sequentially for each server in the cluster, or for all servers simultaneously. Deploying Avaya Breeze OVA with VMware vSphere Client connected to vCenter on page 23. Deploying Avaya Breeze OVA with VMware vSphere Web Client on page 28. Deploying Avaya Breeze OVA with VMware vSphere Client connected to ESXi host on page 33. Deploying Avaya Breeze OVA with Solution Deployment Manager on page 40. **Note:** You must configure all customized disk sizes again after you install the Avaya Breeze™ OVA. If you use the cluster database, ensure that the disk size configuration is appropriate for the snap-in that uses the database.	
16	Configure the virtual machine automatic startup settings.	Configure virtual machine automatic startup settings on page 42.	
17	Change the customer password on first login.	—	
18	Create multiple privileged user accounts.	Creating multiple privileged user accounts on page 44.	
19	Install the patch file if required.	Patching Avaya Breeze on page 95.	
20	Add all Avaya Breeze™ servers to the cluster.	Adding Avaya Breeze servers to the cluster after upgrading on page 44	
21	Select the **Enable Database Auto Switchover** field on the **Elements** > **Avaya Breeze™** > **Cluster Administration** general page.	—	This step is only required for multi-node clusters with

Table continues…

#	Action	Link/Notes	✔
			Cluster database.
22	Verify data replication between System Manager and Avaya Breeze™.	Verifying replication status on page 45.	
23	Run Avaya Breeze™ maintenance tests for each server in the cluster.	Running maintenance tests on page 44. Resolve errors before proceeding. For information, see *Maintaining and Troubleshooting Avaya Breeze™*.	
24	On the **Server Administration** page verify the following for each upgraded server: • The **Service Install Status** is a green checkmark • The **Security Module** is Up • The **License mode** is a green checkmark • The **Version** displays Release 3.5	Verifying server status on page 45.	
25	Add trust certificates.	For information, see *Certificate administration* in *Deploying Avaya Breeze™*.	
26	Edit cluster attributes.	Editing cluster attributes on page 45.	
27	Install new snap-ins.	Installing new snap-ins on page 54.	
28	Set the preferred version for each snap-in.	Setting preferred snap-in version on page 54.	
29	Change the state to **Accept New Service** for the upgraded Avaya Breeze™ cluster.	Accepting new service on page 55.	
30	Verify the Avaya Breeze™ SIP Entity Link with Session Manager.	Verifying the Avaya Breeze Entity Link connection on page 55.	
31	Test Avaya Breeze™ snap-ins to verify that they are functioning correctly.		
32	After the successful upgrade operation, delete the previous Avaya Breeze™ 3.0 or later VMware image.		
33	If not using Engagement Assistant, but using Avaya Aura® Media Server before upgrading to Release 3.5, remove obsolete Avaya Aura® Media Server configuration.	Checklist for removing obsolete Avaya Aura Media Server configuration in System Manager on page 103.	
34	Configure the Alarming setup. Configure System Manager to receive the Avaya Breeze™ alarms.	See *SNMP Support for Avaya Breeze™* in *Maintaining and Troubleshooting Avaya Breeze™*.	

Recording configuration information

About this task

Use the procedures in this task to access the system information to record for configuring the Avaya Breeze™ OVA upgrade. Record this information in the *Customer configuration information for OVA upgrades* section.

Procedure

1. Log in to Avaya Breeze™ CLI interface.
2. Run the `ceconfig` command.

   The `ceconfig` command displays the following information:

   - IP address
   - Short Hostname
   - Network Domain
   - Netmask
   - Default gateway
   - DNS servers
   - Time zone
   - NTP servers
   - Primary System Manager IP address
   - Primary System Manager FQDN
3. Record this information.
4. Record the HTTP Proxy settings for the server on vCenter.

   Alternatively, you run the `CEnetSetup` command to record the HTTP Proxy settings.

Customer configuration information for OVA upgrades

You require the following information to upgrade Avaya Breeze™ with an OVA. Have this information before you begin the upgrade.

Network Settings

Field	Information to enter	Notes
IP Address	`Enter server's IP address`	The IP Address must match the one for the server that is being upgraded.
Short Hostname	`Enter server's hostname`	The hostname must match the one for the server that is being upgraded.

Table continues…

Field	Information to enter	Notes
Network Domain	`Enter network domain or 'none'`	The network domain must match the one for the server that is being upgraded.
Netmask	`Enter netmask`	
Default gateway	`Enter gateway IP address`	Default gateway for Avaya Breeze™ management network interface
DNS servers	`Enter the Primary, Secondary, and Tertiary DNS server IP address`	You can have up to three DNS servers.

Proxy settings

This information is only required if a proxy is in use.

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.`	
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 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
Time zone	`Select the timezone from this field.`	

Table continues…

Field	Information to enter	Notes
NTP Servers	`Enter IP/FQDN of Primary NTP Server`	You can have up to three NTP servers.
EASG Enable/Disable	Select the checkbox to enable EASG or clear the checkbox to disable EASG.	

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.	

Customer Login Settings

Field	Information to enter	Notes
Login Name	`Enter Login ID to use for the customer account.`	Login ID and password for customer account you will create during OVA deployment.
Enter Password	`Enter the customer account password.`	
Additional user accounts		Record information here that is required to recreate additional user accounts. **Note:** Only one customer account can be created during OVA deployment. These additional accounts may be created post deployment using the `custAccounts` script.

System Manager Settings

Field	Information to enter	Notes
Primary System Manager IP	Enter the `IP Address` of the Primary System Manager that will be used to manage this Avaya Breeze™ 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.

Table continues…

Field	Information to enter	Notes
		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.

Avaya Breeze™ Profile

Consult your Avaya Breeze™ Snap-in Reference documents for specific profile requirements for snap-ins you intend to install.

Selected profile	Options
	• Avaya Breeze™ default 4 CPU configuration. Requires 4 CPUs, 6 GB Memory and 50 GB Disk space. • Avaya Breeze™ General Purpose Large Cluster 4 CPU configuration. Requires 4 CPUs, 8 GB Memory and 50 GB Disk space. • Avaya Breeze™ 6 CPU configuration. Requires 6 CPUs, 10 GB Memory and 50 GB Disk space. This profile is targeted as a migration path for the Presence Services application on Midsize Enterprise to Presence Services 8.0 with Avaya Breeze™. • Avaya Breeze™ 8 CPU configuration. Requires 8 CPUs, 16 GB Memory and 50 GB Disk space. • Avaya Breeze™ 12 CPU configuration. Requires 12 CPUs, 27 GB Memory and 50 GB Disk space.

Virtual Machine

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

Field	Information to enter	Notes
CPU/Memory allocation and reservations		
DataStore location		
Host networking assignments		

vCenter and ESXi Host

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

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. Navigate to **Security** > **Certificate Management** > **Key Store**.
11. Assign System Manager signed certificate to all service profiles.
12. Click **Save**.
13. 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™

Procedure

1. On System Manager, click **Elements** > **Media Server** > **Application Assignment**.
2. Select the check box next to Avaya Breeze™, 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™.

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

Downloading software from PLDS

Procedure

1. In your web browser, type http://plds.avaya.com to go to the Avaya PLDS website.
2. On the PLDS website, enter your Login ID and password.
3. On the Home page, select **Assets**.
4. Select **View Downloads**.
5. Click the search icon ( ) for Company Name.
6. In the Search Companies dialog box, do the following:
   a. In the **%Name** field, type `Avaya` or the Partner company name.
   b. Click **Search Companies**.
   c. Locate the correct entry and click the **Select** link.
7. Search for the available downloads by using one of the following:
   - In **Download Pub ID**, type the download pub ID.
   - In the **Application** field, click the application name.
8. Click **Search Downloads**.
9. Scroll down to the entry for the download file, and click the **Download** link.

10. Select a location where you want to save the file, and click **Save**.
11. **(Optional)** If you receive an error message, click the message, install Active X, and continue with the download.
12. **(Optional)** When the system displays the security warning, click **Install**.

    When the installation is complete, PLDS displays the downloads again with a check mark next to the downloads that have completed successfully.

Verifying Enrollment Password status

Avaya Breeze™ requires an Enrollment Password during the initial installation and deployment process. Enrolling a password establishes trust between System Manager and Avaya Breeze™. 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.

Denying new service

About this task

Place the cluster in the Denying New Service state before you edit the cluster attributes.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Cluster Administration**.
3. Select the cluster that you want to upgrade.
4. From the **Cluster State** drop-down menu, select **Deny New Service**.
5. Verify that the system displays **Denying** in the **Cluster State** column.

Verifying activity

About this task

Verify that currently there is no activity on the Avaya Breeze™ servers in the cluster you are upgrading.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Cluster Administration**.
3. In the row for the cluster you are upgrading, look at the **Activity** column.
4. Verify that the **Activity** is 0.

   You can view the **Activity** for individual servers in the cluster by clicking **Show** in the **Details** column.

   Even after new service is stopped, it can take a couple of hours for activity to reach zero. If activity has not stopped in a reasonable time, you can choose to proceed with the upgrade. Active calls will continue, but Avaya Breeze™ snap-in call control for those calls will be lost.

Removing Avaya Breeze™ servers from the cluster for upgrading

About this task

You can skip this procedure when upgrading from Release 3.0.x, 3.1.x, or 3.2.x to Release 3.5 for a Presence cluster that only runs Presence Services Snap-in.

This procedure is service impacting for the targeted cluster and scheduling a maintenance window will be required.

Before you begin

Change the state of the cluster to Deny New Service.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. Click **Cluster Administration**.
3. Select the targeted cluster and click **Edit**.
4. Navigate to the Servers tab.
5. For a single node cluster, select the Avaya Breeze™ server by selecting the blue **X** next to the assigned server and click **Commit**.
6. For a two-node cluster:
   a. Verify that the load balancer is disabled (if applicable) on the General tab.
   b. If using the cluster database feature:
      a. On the General tab, disable **Database Auto Switchover** (if applicable).
      b. Remove the Standby server instance first by choosing the blue **X** next to the assigned server.

c. Remove the Active server instance next by choosing the blue **X** next to the assigned server

d. Click **Commit**.

7. For a cluster with more than three nodes:

   a. Verify that the load balancer is disabled (if applicable) on the General tab.

   b. If using the cluster database feature:

      a. On the General tab, disable **Database Auto Switchover** (if applicable).

      b. Remove the assigned server instances without an **A** or **S** designation by choosing the blue **X** next to the assigned server.

      c. Remove the Standby server instance first by choosing the blue **X** next to the assigned server.

      d. Remove the Active server instance next by choosing the blue **X** next to the assigned server

      e. Click **Commit**.

8. Confirm the warnings presented regarding the service disrupting actions that will follow.

9. Wait until all services are successfully uninstalled.

Next steps

Shut down the servers.

Shutting down servers

About this task

You must shut down all the servers in the cluster before beginning the OVA deployment on any single server.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Server Administration**.
2. Click the button in front of a server in the cluster.
3. From the **Shutdown System** drop-down menu, select **Shutdown**.
4. Repeat for every server in the cluster.

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

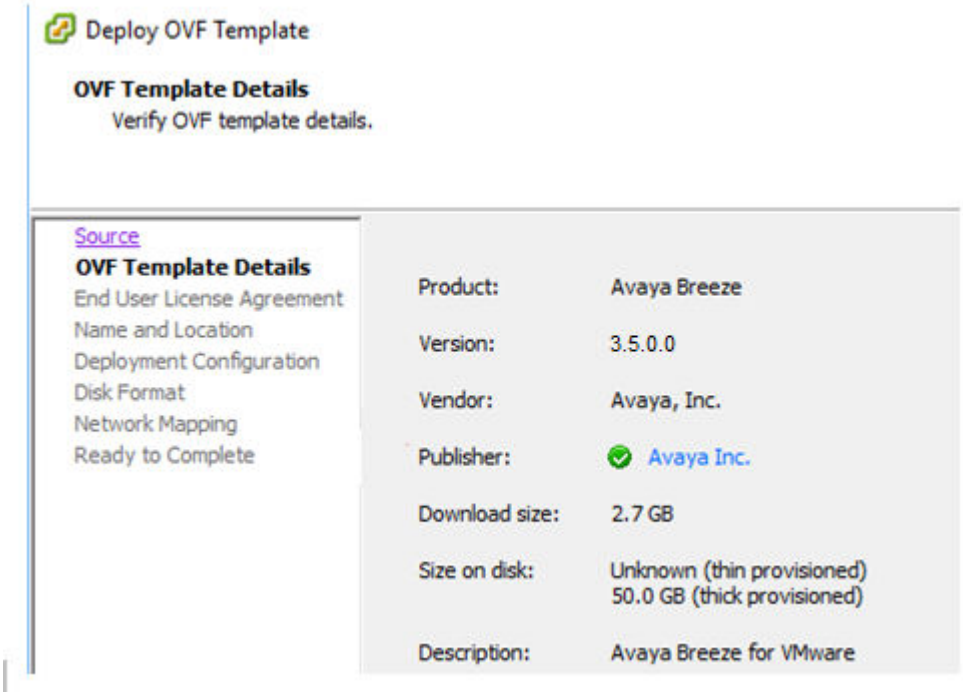
Use the *Customer Configuration Information* to get the required network settings for deployment. You can obtain the settings from an existing system if you are redeploying the OVA.

Verify that the Enrollment Password is administered and not expired.

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

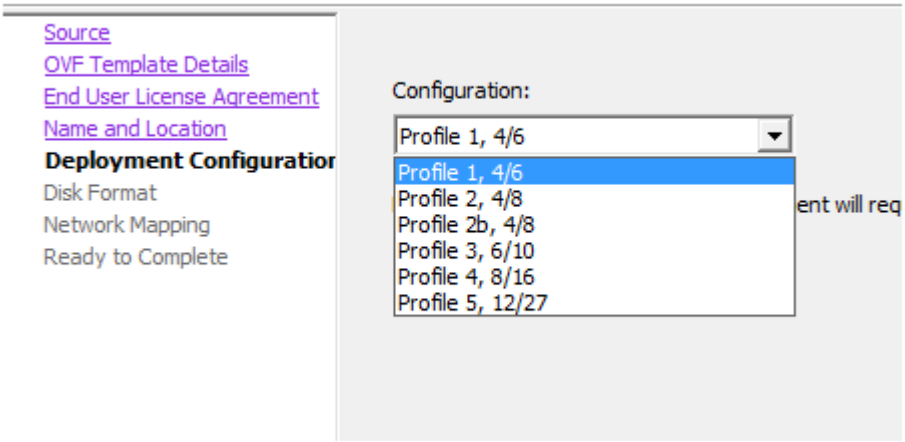
Procedure

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™ OVA. Click **Next**.
4. Verify that the details displayed match the version of the Avaya Breeze™ that you are expecting to deploy.
   - If the details do not match, you may have chosen the wrong OVA. Click **Back** and choose the correct OVA.
   - If the details match, click **Next**.



5. If you wish to accept the End User License Agreement click **Accept**, then click **Next**.
6. On the Name and Location page, enter a name for the Avaya Breeze™ Virtual Machine (VM). Select the inventory location for your VM , then click **Next**.

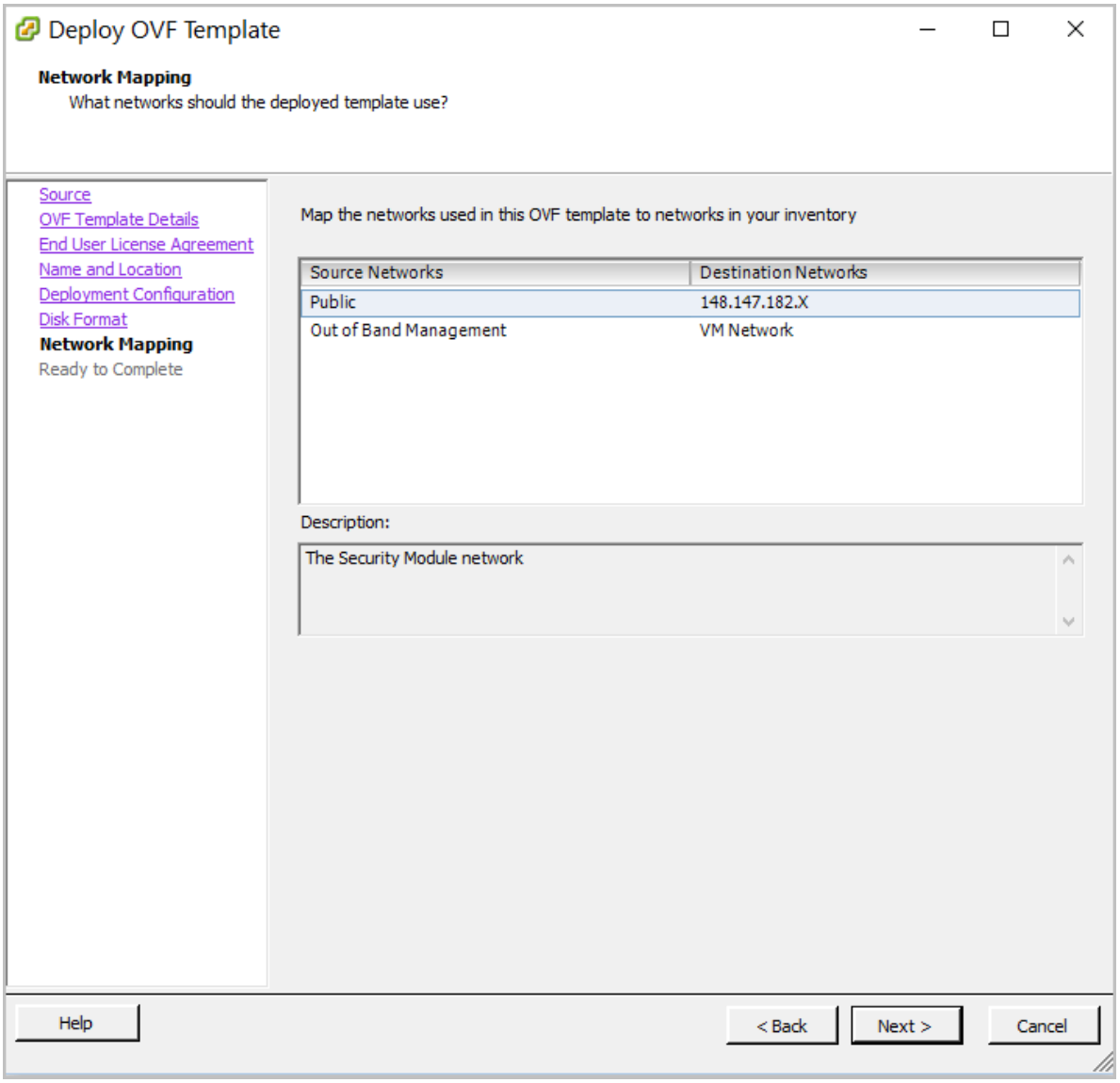
7. On the Deployment Configuration page, select the configuration profile that best fits the deployment, then click **Next**.



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™ interface, and click **Next**.

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

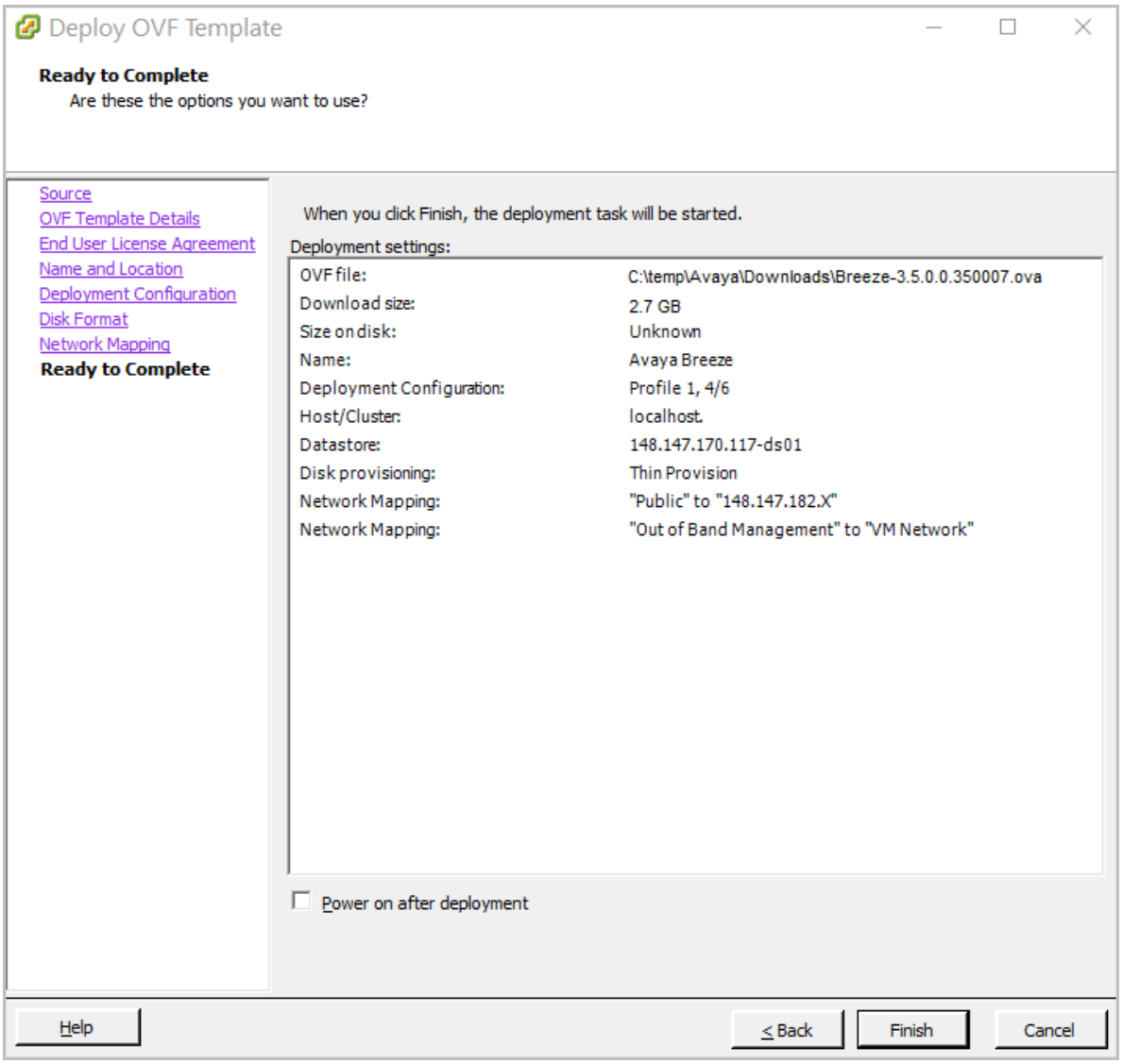
    - Public (eth1) - Asset/security module
    - Out of band management (eth0) - management NIC



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.



- 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™*.

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™ 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™ 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™, 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.

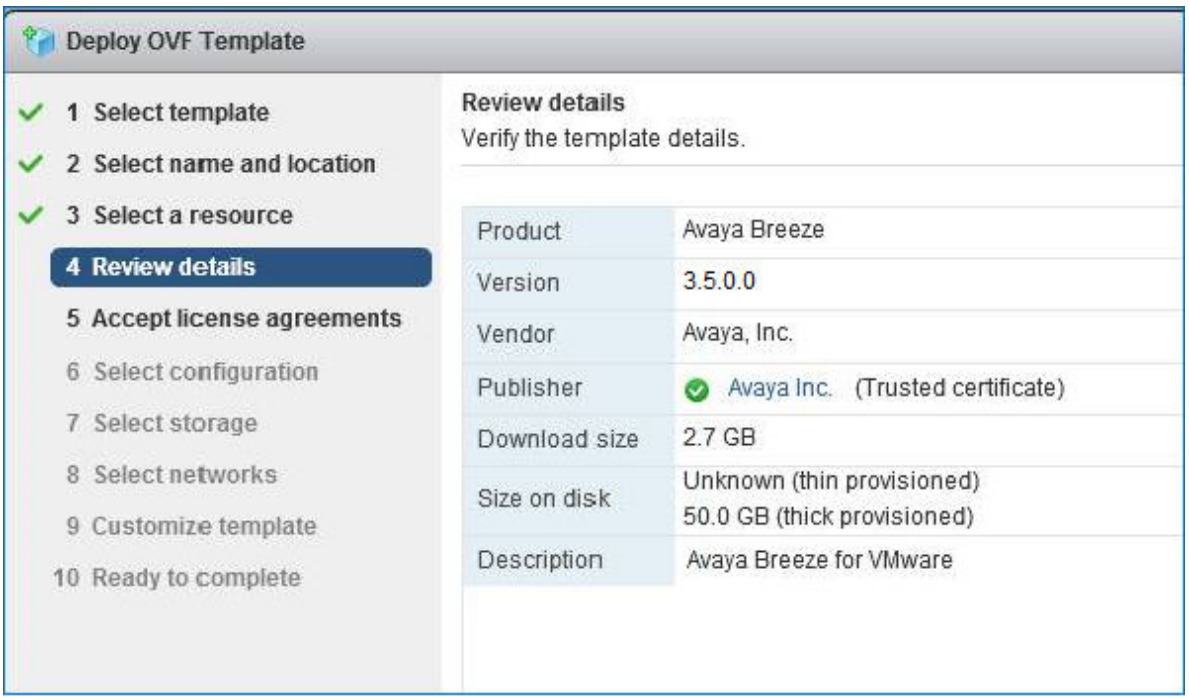
Procedure

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

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

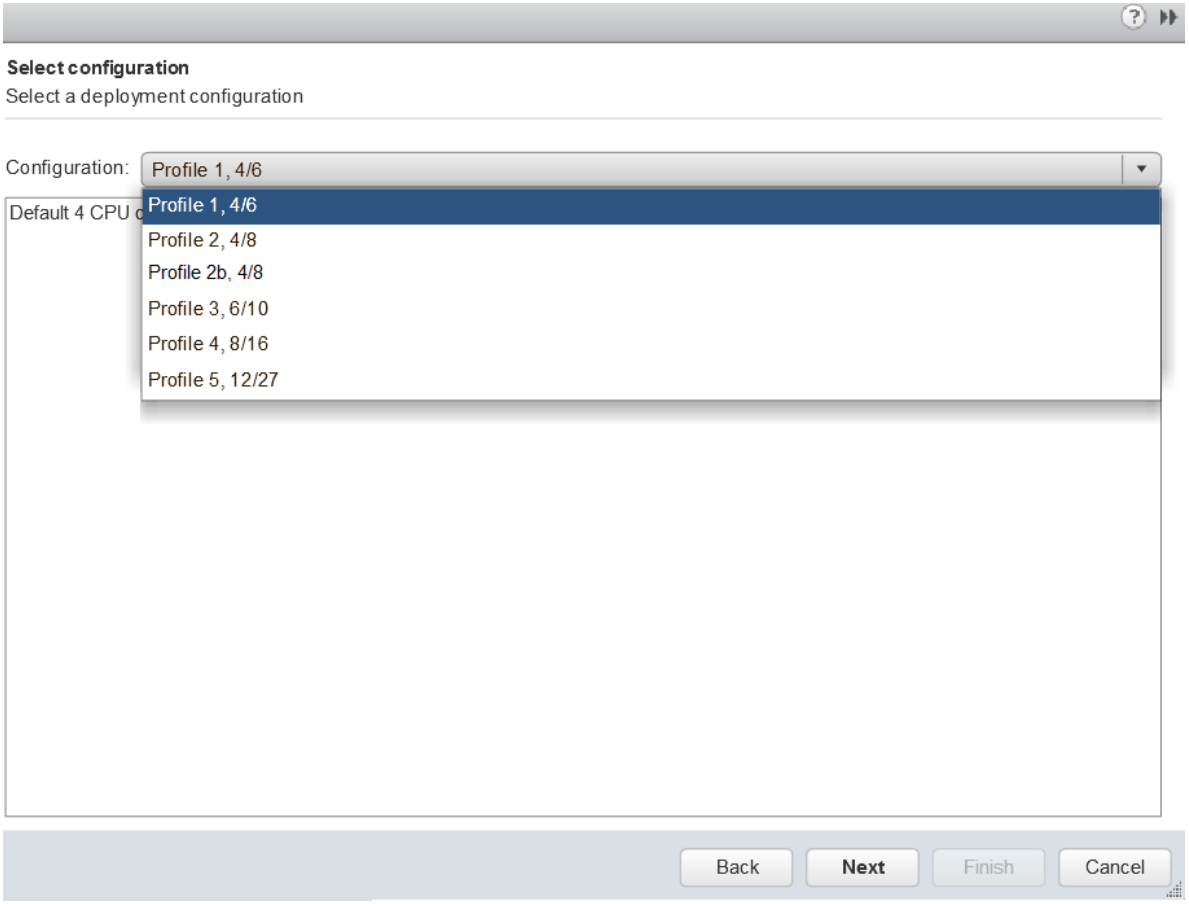
2. In the navigation pane, click **vCenter**.
3. Click **Inventory Trees** > **Hosts and Clusters**.
4. Expand **Hosts and Clusters** to locate and select the target deployment host.
5. Right-click the on the host and select **Deploy OVF Template**.
6. On the Select Source page, enter the **URL** or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



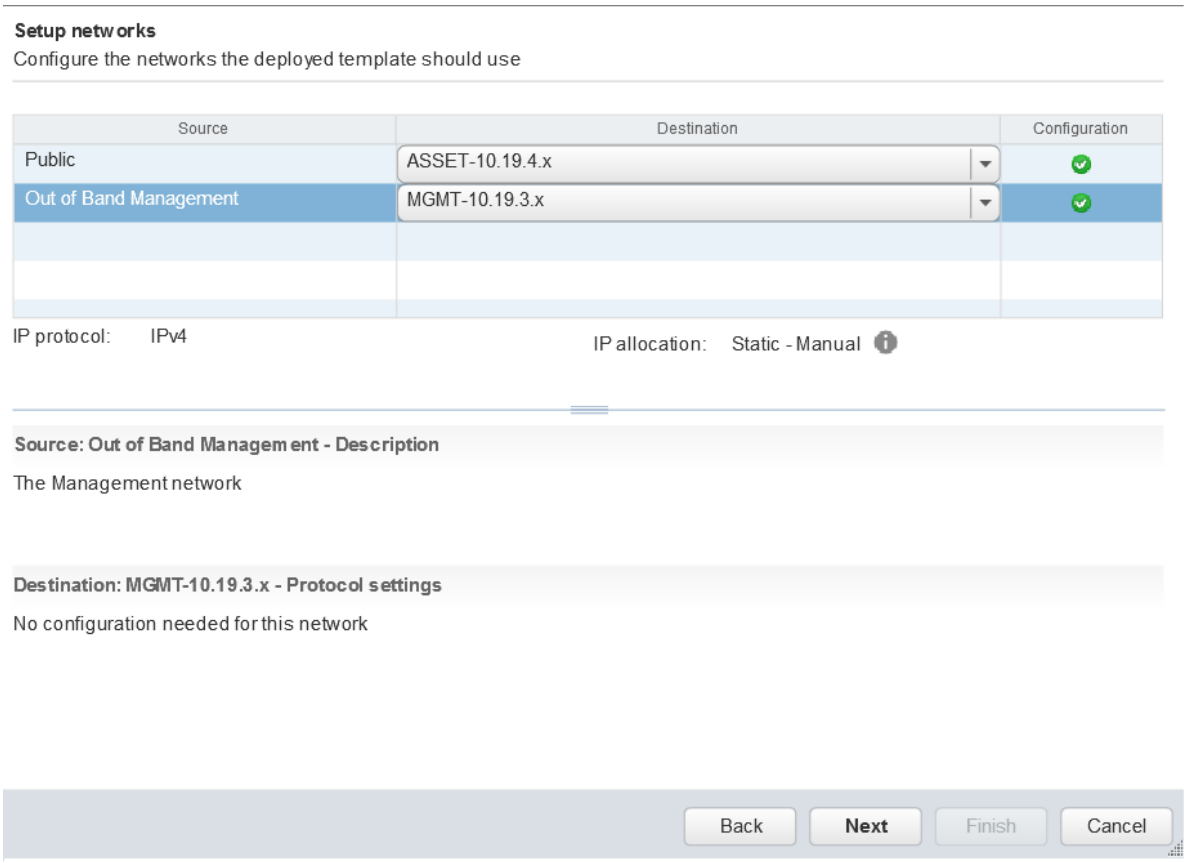
8. To accept the End User License Agreement, click **Accept**.
9. Click **Next**.
10. Enter a name for the Avaya Breeze™ VM and select the required datacenter folder for the VM.
11. Click **Next**.
12. On the Select a resource page, select the location to run the deployed template and click **Next**.

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



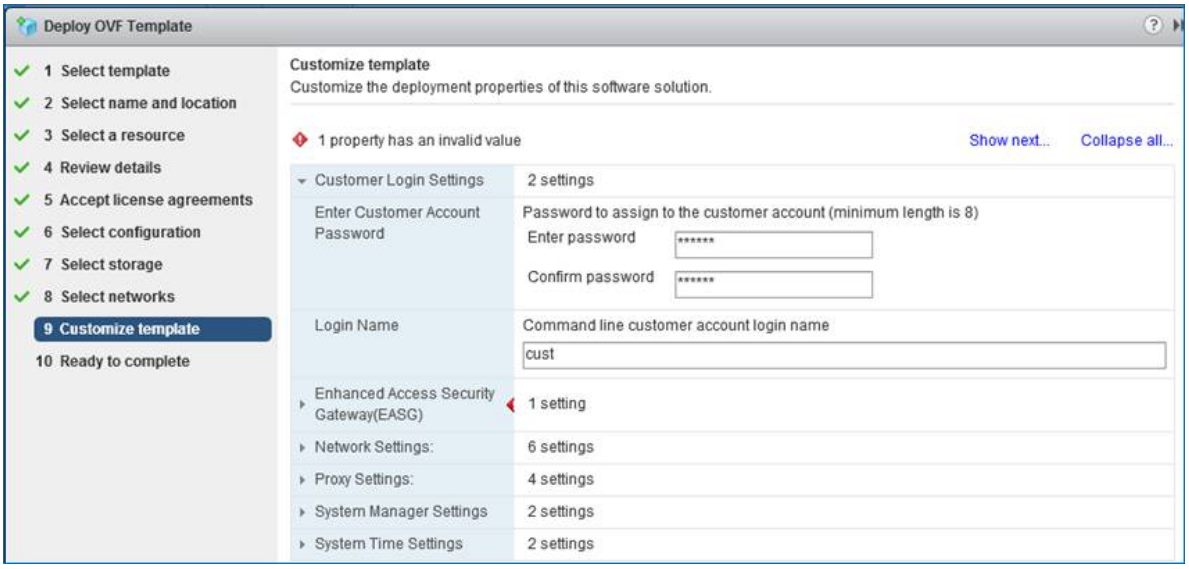
14. Select the virtual disk format you want and click **Next**.
15. Select the destination network for each Avaya Breeze™ interface and click **Next**.

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

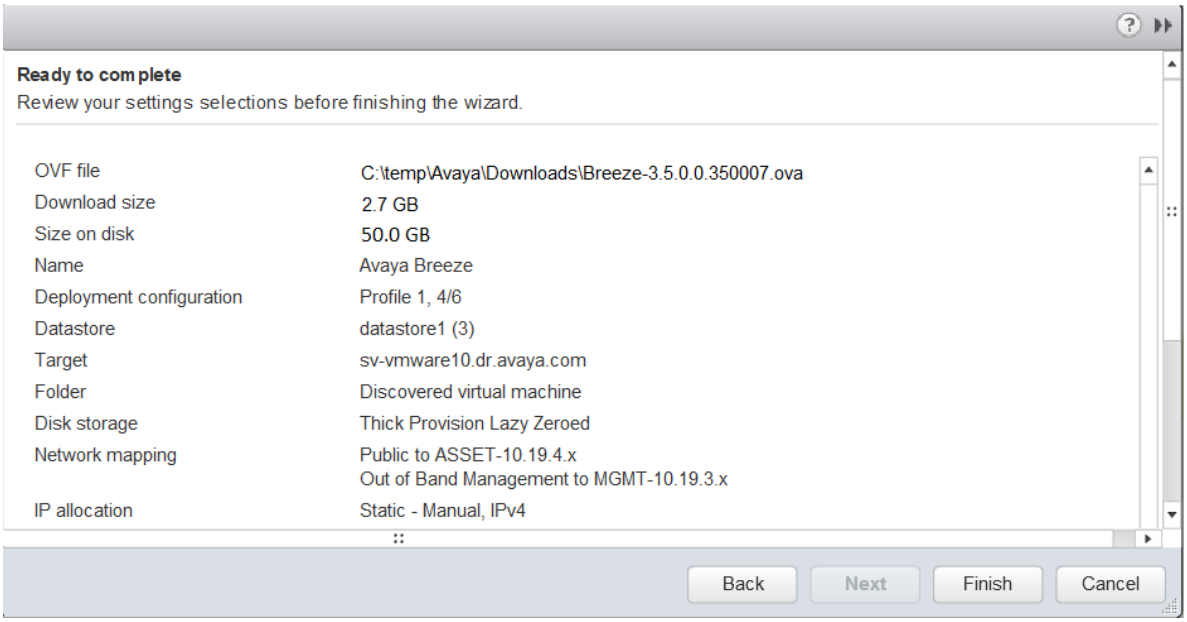


See the *Customer Configuration Information* you collected for the network configuration values.

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



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



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

Tip:

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

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

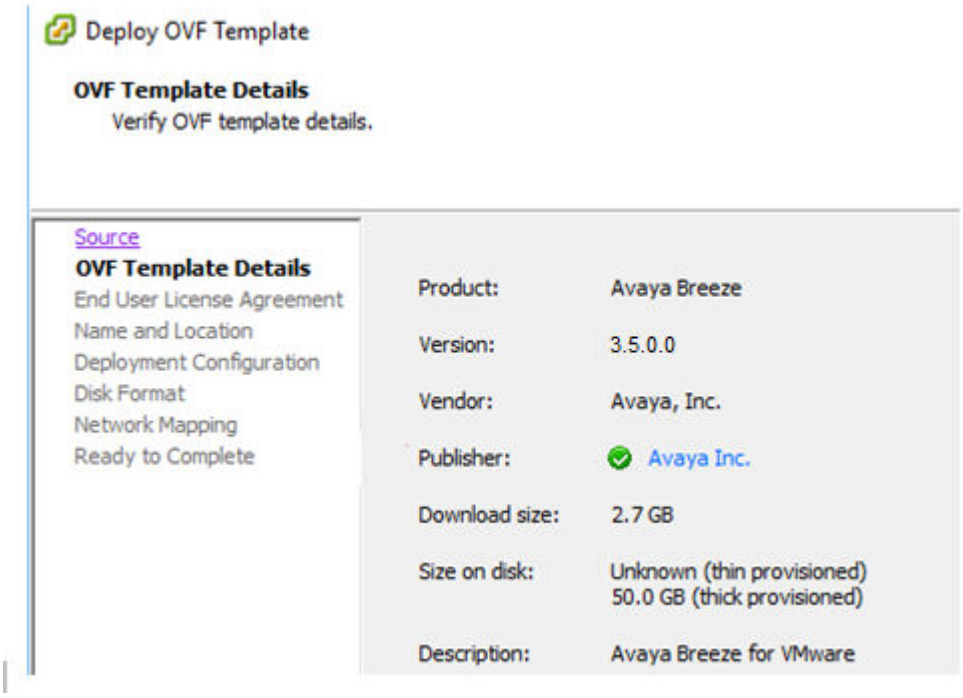
Use the *Customer Configuration Information* to get the required network settings for deployment. You can obtain the settings from an existing system if you are redeploying the OVA.

Verify that the Enrollment Password is administered and not expired.

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

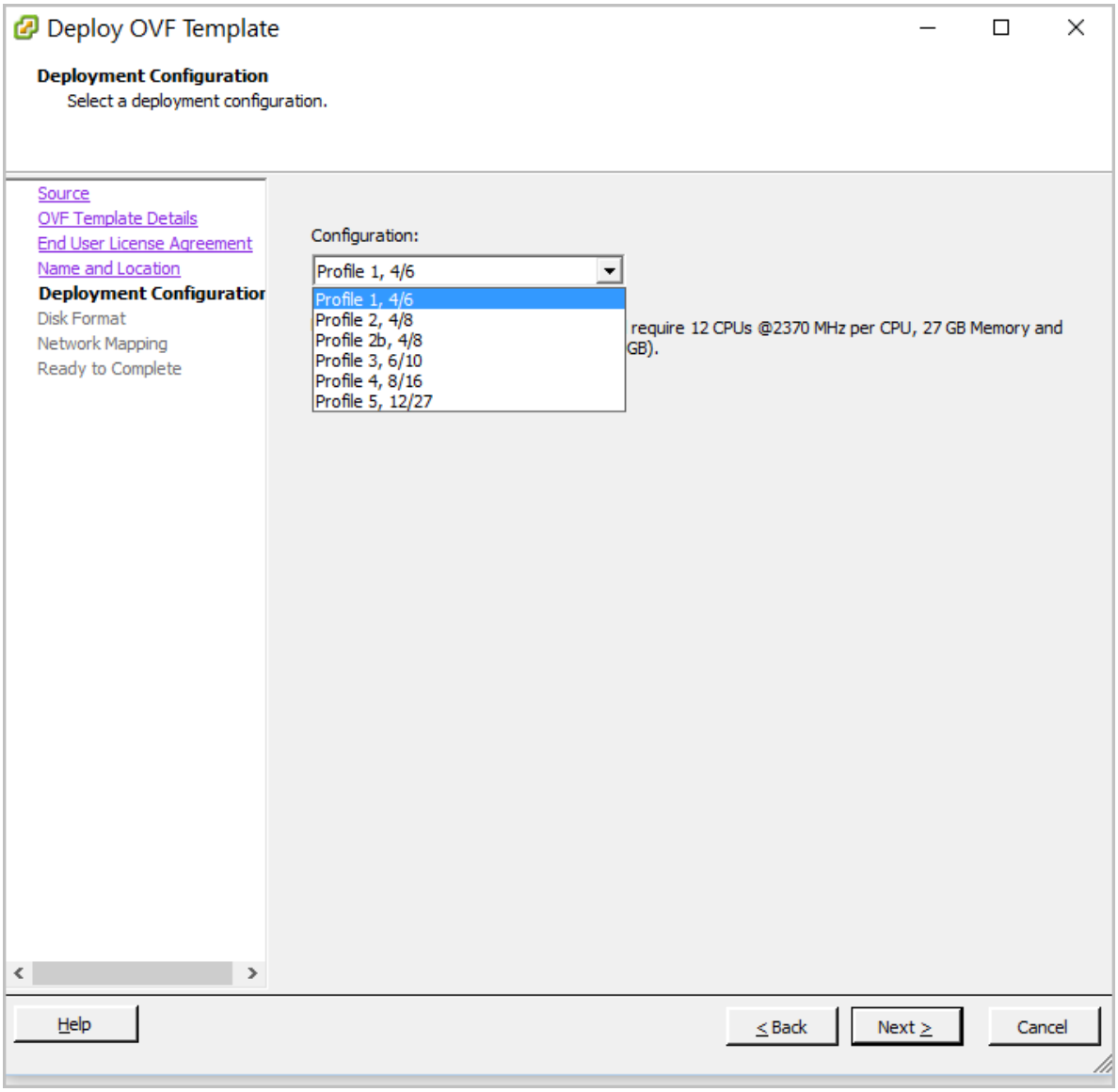
Procedure

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™ OVA.
4. Click **Next**.
5. Verify that the details displayed match the version of the Avaya Breeze™ that you are expecting to deploy.
   - If the details do not match, you may have chosen the wrong OVA. Click **Back** and find the correct OVA.
   - If the details do match, click **Next**.



6. If you accept the End User License Agreement click **Accept**, and click **Next**.
7. Enter a name for the Avaya Breeze™ 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**.

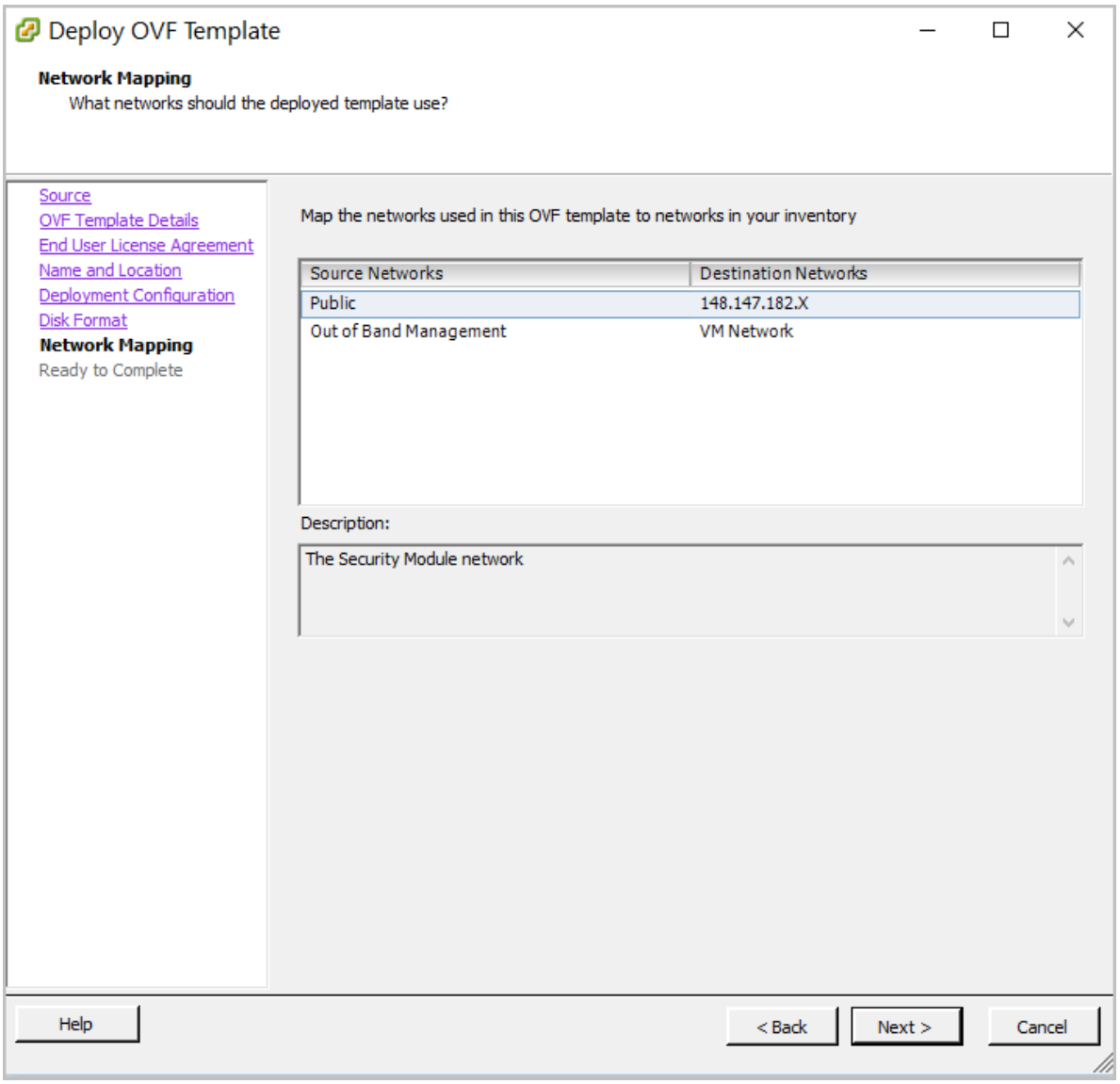
   While Avaya Breeze™ works with either thick or thin provisioned disk, Avaya recommends using a **Thick Provision Lazy Zeroed** disk.

10. On the Network Mapping page, select the destination network for each Avaya Breeze™ interface, then click **Next**.

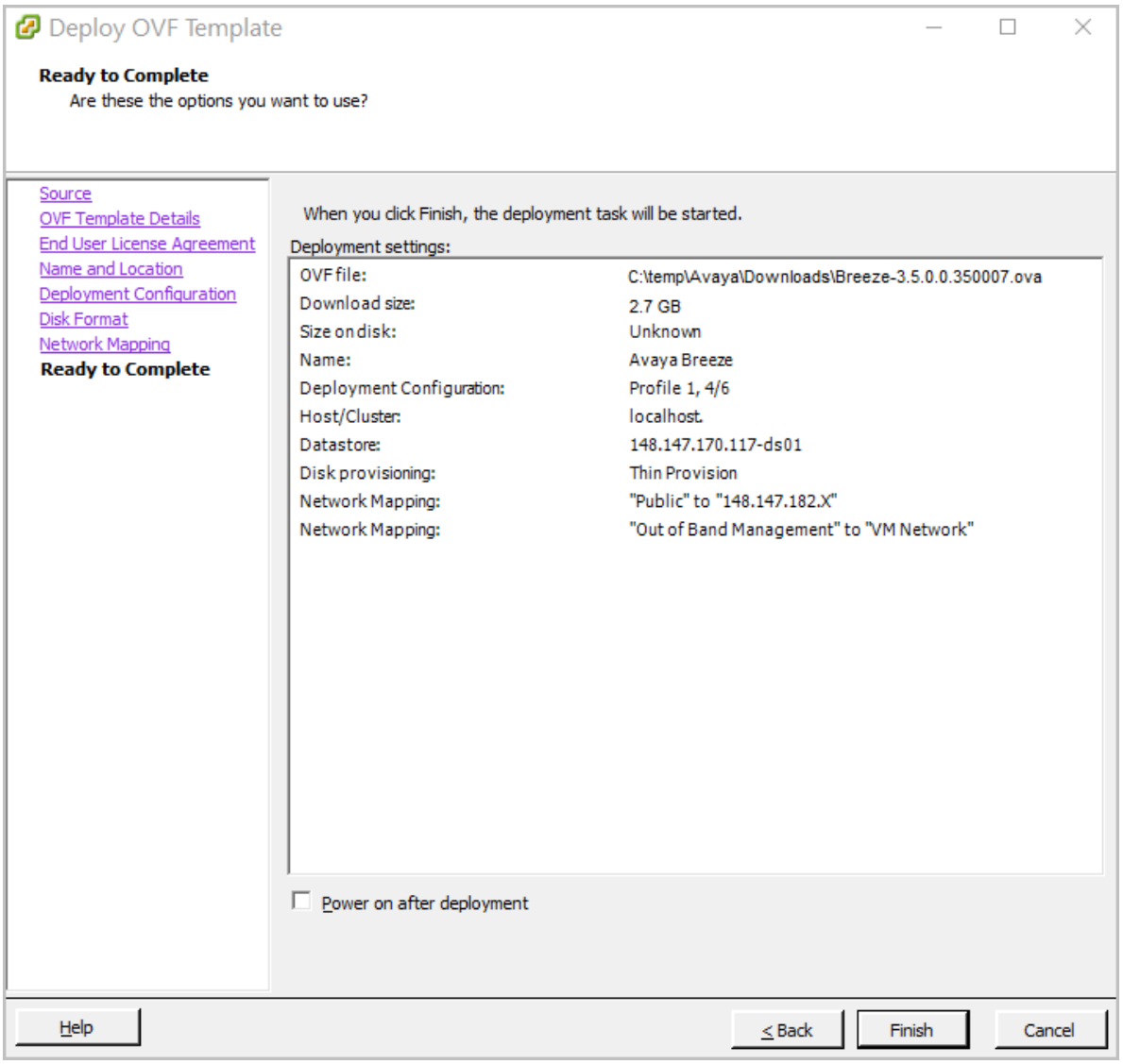
    We recommend that you use different physical networks for each of the Avaya Breeze™ interfaces.

    - Public (eth1) - Asset/security module

- Out of band management (eth0) - management NIC



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



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.

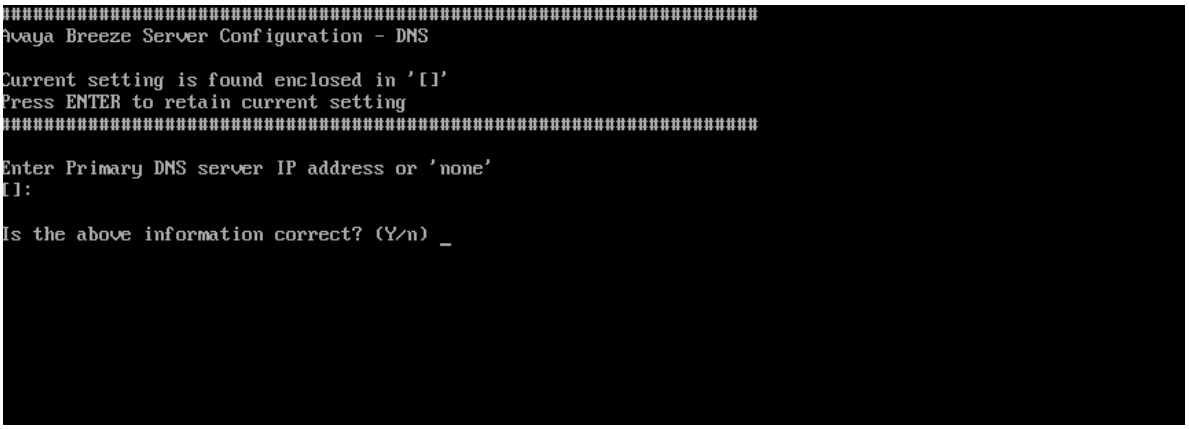
    The VM continues to boot.
16. Towards the end of the boot sequence you are prompted to configure the VM. Enter `y` to proceed.
17. When the system prompts, enter the management interface network parameters, date and time information, customer user information, and System Manager information.

    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™*.

    Refer to the following screenshots.



```
##########################################################################
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™ 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™ Open Virtual Appliance (OVA).

Verify that the Enrollment Password is administered and not expired.

Procedure

1. Copy the previously downloaded Avaya Breeze™ 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. For **Product Family**, **Device Type**, and **Software Type**, select **others**.
5. Click **Sync** and wait for the operation to complete.
6. 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.
7. Navigate to **Home** > **Services** > **Solution Deployment Manager** > **Software Library Management**.
8. Check SMGR_DEFAULT_LOCAL, click **Manage Files**, and confirm that the OVA file appears in the list of files under Software Library Files.
9. 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 **VM Management**.
   c. Select **New** under **Locations**.
   d. Populate the location properties and click **Save**.
10. 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 **VM Management Tree**, select the location to add the host to.
    b. Click the **Hosts** tab.
    c. Click **Add** on the Hosts tab.
    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.
11. Navigate to **Home** > **Services** > **Solution Deployment Manager** > **VM Management**.
12. Select **VM Management** under the **VM Management Tree**, click on the **Virtual Machines** tab, and click **New**.
13. In the Select Location and Host section, perform the following steps:
    a. In **Select Location**, select a location.
    b. In **Select Host**, select a host.
    c. In **Host FQDN**, type the virtual machine name.

14. Click **Next**.
15. In the Deploy OVA section, perform the following steps:
    a. In **Select Software Library**, 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.
    b. In **Select OVAs**, select the OVA file that you want to deploy.
    c. In **Flexi Footprint**, select a footprint.
16. Click the **Network Parameters** tab and select appropriate networks.
    - Select the network that provides the subnet that Avaya Breeze™ needs for SIP traffic (security module).
    - Select the network that provides the subnet that Avaya Breeze™ needs for the management interface (Avaya Breeze™ instance).
17. Click the **Configuration Parameters** tab and populate the Configuration Parameters fields.
18. Click **Deploy** to begin the OVA deployment.
19. Click **Accept the license terms**.
20. Click the Virtual Machines tab.
21. 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.

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.

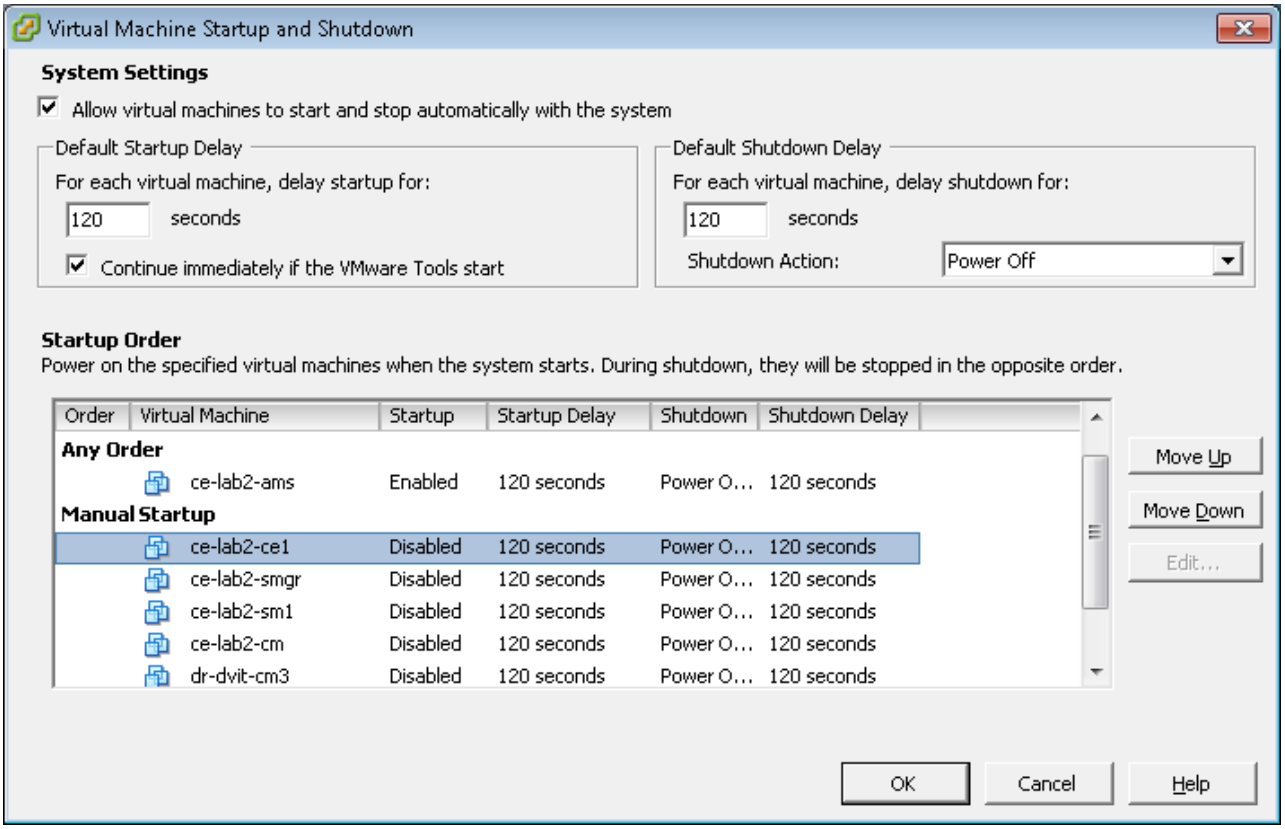
Procedure

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.



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™ VM to be included for Automatic Startup.

Creating multiple privileged user accounts

Procedure

1. Log in to Avaya Breeze™ 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.

Adding Avaya Breeze™ servers to the cluster after upgrading

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. Click **Cluster Administration**.
3. Select the targeted cluster and click **Edit**.
   a. Navigate to the Servers tab.
   b. Add all Avaya Breeze™ server to the cluster by selecting the **+** sign next to each Release 3.5 unassigned server.
   c. Re-enable HTTP Load Balancing, if applicable.
   d. Click **Commit**.
4. Wait until all services have been installed successfully.

Running maintenance tests

Procedure

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

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

Verifying replication status

About this task

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

Procedure

1. On System Manager, click **Services** > **Replication**.
2. Locate the Avaya Breeze™ in the **Replica Group** list.
3. In the **Synchronization Status** column, verify that the Avaya Breeze™ 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™*.

Verifying server status

About this task

Verify that the Avaya Breeze™ servers have upgraded to Release 3.5 and are functioning correctly.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Server Administration**.
2. In the row for each Avaya Breeze™ server in the cluster you are upgrading, 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 Release 3.5.

Editing cluster attributes

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Cluster Administration**.
2. On the **Cluster Administration** page, select the upgraded cluster and click **Edit**.

3. On the **Cluster Editor** page, click the **General** tab.
4. Optionally change the cluster name and IP address.
   a. Type a new **Cluster Name**.
   b. For load balancing, type a unique IP address for the cluster in the **Cluster IP** field.

      The Cluster IP address is required if load balancing is used. It must be a unique IP address on the same subnet as the Avaya Breeze™ servers in the cluster.
5. Configure the cluster attributes.

   Note:

   By default HTTP traffic is blocked. To allow HTTP traffic in additional to HTTPS, you must uncheck the **Only allow secure web communications** box when configuring cluster attributes.
6. Click **Commit**.

Cluster Editor field descriptions

You can edit the cluster attributes only when all reachable nodes in the cluster are in the **Deny New Service** mode.

General tab

Name	Description
Cluster Profile	The types of clusters. The options are: • **Context Store**: Product-specific cluster profile for the Context Store snap-in. Minimum two Avaya Breeze™ servers are required for this profile. • **Core Platform**: Closed cluster that supports up to 10 Avaya Breeze™ servers. Snap-ins that might be installed on this cluster profile include Presence Services and Call Park and Page. • **Engagement Assistant Speech**: Product-specific cluster profile for the Engagement Assistant snap-in. • **General Purpose**: General purpose cluster profile. Minimum one Avaya Breeze™ server is required for this profile. • **General Purpose Large**: An open cluster that supports up to five Avaya Breeze™ servers. This cluster profile mainly supports the Engagement Call Control solution. • **Work Assignment**: Product-specific cluster for the Work Assignment snap-in.

Table continues…

Name	Description
	• **Customer Engagement**: A cluster profile that mainly supports Avaya Oceana™ Solution.
Cluster Name	The unique name that you assign to the cluster. The cluster name is case sensitive. You can create clusters with the same name but different casing.
Cluster IPv4	The unique IP address assigned to the cluster. The IP address is used for HTTP load balancing. This field is mandatory if you select the load balancer check box. The **Cluster IP** field is optional if you do not enable load balancing. **Note:** Do not assign a **Cluster IP** for a single-node cluster.
Cluster Group	The cluster group number that you assign to the cluster. You can enter a value from 1 to 10. This optional field is used only to configure attributes for multiple snap-ins.
Cluster Fully Qualified Domain Name	The unique FQDN that you assign to the cluster.
Enable Cluster Database	The check box to enable Cluster Database. **Note:** You cannot clear the check box if snap-ins are installed on the cluster that require Cluster Database.
Enable Database Auto Switchover	The check box to enable auto switch over of clusters with two or more servers in a high availability database scenario. Select this check box if you want the standby server to automatically take over as the active server whenever the active server is down. **Note:** If you do not select this check box, you must manually enable the standby server to take over whenever the active server is nonfunctional.
Description	The cluster description.

Cluster Attributes

Name	Description
Authorization Service Address	The FQDN or IP address of the cluster on which the Authorization Service is running.
Use secure connection for centralized logging	The check box to enable Avaya Oceana™ Solution centralized logging. This field is available only for the **Customer Engagement** profile.
Centralized logging destination	The destination for centralized logging: **Breeze Cluster** or **External Server**. This field is available only for the **Customer Engagement** profile.
Breeze cluster as destination for centralized logging	The Avaya Breeze™ cluster on which you installed the centralized logging snap-in. This field is available only for the **Customer Engagement** profile. Configure the field only if you configure **Breeze Cluster** as the value of **Centralized logging destination**.
External destination for centralized logging	The IP address or FQDN of the destination server on which you configured centralized logging. This field is available only for the **Customer Engagement** profile. Configure the field only if you configure **External Server** as the value of **Centralized logging destination**.
Cluster Activity Status	The status of the cluster: • **Active** • **Standby**
Default SMS Connector Service	The default SMS Connector when multiple SMS Connectors are installed in a cluster.
The URL of the announcement to play during failover	The URL of the announcement that is to be played during a failover.
Additional Java options used by GSC	The additional Java options used by GSC.
Grid Heap Size	The size of grid heap.
Grid Heap Size for LU	The size of grid heap for LU.
Grid LRMI Selector Threads	The Grid LRMI Selector Threads.
Grid Password	The internal grid password.
Use secure grid?	The check box to secure all the grid communication.
Grid Thread Stack Size	The size of grid tread stack.
Http or Https limit on connections per client	The maximum number of HTTP or HTTPS connections at a given time per client. For General Purpose Large clusters, this value must be larger than 3.

Table continues…

Name	Description
Http or Https traffic rate limit in bytes/sec per client	The rate limit on the HTTP or HTTPS traffic served per connection. For General Purpose Large clusters, this value must be larger than 300,000 bytes per second.
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.
Only allow secure web communications	The check box to enable only HTTPS requests. By default, this check box is selected.
Is load balancer enabled	The check box to enable load balancing for the cluster. Use load balancing if you want to scale the HTTP services without targeting a particular Avaya Breeze™ server.
Is session affinity enabled	The check box to enable session affinity for the cluster. With session affinity, a particular client is always served by the same backend server.
Trusted addresses for converting to use X-Real-IP for session affinity	Trusted addresses that are known to send correct replacement addresses so that Avaya Breeze™ load balancer can use the real client IP when an HTTP request traverses through reverse proxies such as Avaya Session Border Controller for Enterprise. The header which is used to identify the real client IP address is X-Real-IP.
Default call provider for Make Call	The call provider used for a call that is initiated (Make Call) from an Avaya Breeze™ snap-in. The default value is **SIP**, which corresponds to using SIP to connect to Avaya Aura® for call processing. If ZangCallConnector is loaded, ZangCallConnector can be installed and used for making or initiating calls.
Default Identity for special make call cases	The default identity that is used for calls generating from Avaya Breeze™. If a user does not specify an identity, then the value in this field is used.
The maximum number of Avaya Breeze Servers allowed in Cluster	The maximum number of Avaya Breeze™ servers that you can add to a cluster.
Media server monitoring period (seconds)	The period of polling. Each Avaya Aura® Media Server is periodically polled from each Avaya

Table continues…

Name	Description
	Breeze™ that communicates with the Avaya Aura® Media Server to determine active status and normal function. When certain interactions with an Avaya Aura® Media Server are not functioning normally, the polling period is approximately 1/3 of this value.
Media server shuffle out timer (seconds)	The duration that Avaya Breeze™ waits after all media operations are complete before shuffling Avaya Aura® Media Server out of the media path. This cluster attribute is displayed in all cluster profiles that support SIP call processing. The default value is 3 seconds.
Select AAMS by caller location - Priority 1	The check box to configure the cluster to select Avaya Aura® Media Server based on the caller location as the first priority.
Select AAMS by Breeze server location - Priority 2	The check box to configure the cluster to select Avaya Aura® Media Server based on the Avaya Breeze™ location if the Priority 1 criterion is not met or the **Select AAMS by caller location - Priority 1** check box is disabled.
Select any AAMS - Priority 3	The check box to configure the cluster to select any Avaya Aura® Media Server if the Priority 1 or Priority 2 criteria are not met or the following check boxes are disabled: **Select AAMS by caller location - Priority 1** and **Select AAMS by Breeze server location - Priority 2** check boxes are disabled.
Media IP version to retry in case of ANAT failure	IPv6 is enabled only for systems hardened for enhanced security in a Department of Defense site. If the system has not been hardened, fields related to IPv6 are grey and must be ignored.
Retry IPv4 media in case of IPv6 failure	IPv6 is enabled only for systems hardened for enhanced security in a Department of Defense site. If the system has not been hardened, fields related to IPv6 are grey and must be ignored.
Retry IPv6 media in case of IPv4 failure	IPv6 is enabled only for systems hardened for enhanced security in a Department of Defense site. If the system has not been hardened, fields related to IPv6 are grey and should be ignored.
H.264 Video profile_idc	The H.264 video profile: • **CB(Constrained Baseline profile-42)** • **H(High profile-64)**
Avaya Aura® Media Server - User Id for RESTful TLS authentication	The user ID configured on the Avaya Aura® Media Server for basic authentication for REST signaling.

Table continues…

Name	Description
Avaya Aura® Media Server - Password for RESTful TLS authentication	The password configured on the Avaya Aura® Media Server for basic authentication for REST signaling.
Minimum TLS Version for SIP Call Traffic	The TLS version which will be used for SIP calls intercepting Avaya Breeze™. By default, Avaya Breeze™ uses the value of the **Minimum TLS version** field set in System Manager configuration. If the value of the **Minimum TLS Version** field is TLSv1.1, Avaya Breeze™ uses TLSv1.2. If the value of the **Minimum TLS Version** field is SSLv3, Avaya Breeze™ uses TLSv1.0.
Minimum TLS Version for Non-SIP Traffic	The TLS version which will be used for incoming HTTP requests to Avaya Breeze™. By default, Avaya Breeze™ uses the value of the **Minimum TLS version** field set in System Manager configuration. If the value of the **Minimum TLS Version** field is TLSv1.1, Avaya Breeze™ uses TLSv1.2. If the value of the **Minimum TLS Version** field is SSLv3, Avaya Breeze™ uses TLSv1.0.
List of optional snap-ins including version	The list of optional snap-ins for a specific cluster profile type. The version of each optional snap-in is also included. This attribute applies to the **Core Platform** and **Work Assignment** cluster profiles only.
List of required snap-ins including version	The list of required snap-ins for a specific cluster profile type. The minimum required version of each snap-in is also included.
Default SIP Domain	The default SIP domain for the cluster. If an Avaya Breeze™ snap-in does not include a domain in the addresses that the snap-in sends to the Call Manipulation API, this domain is appended to the address.
Use secure signaling for platform initiated SIP calls	The check box to use secure signaling to initiate WebRTC Snap-in calls, calls from snap-ins to individuals for playing announcements, and for snap-ins that initiate two-party calls. This attribute is not applicable for call intercept scenarios.
Preferred Minimum Session Refresh Interval (secs)	The minimum periodic refresh interval for the SIP session.
Use early pre-answer media?	The cluster attribute that defines the pre-answer media mode. Select the check box to use *the Early* pre-answer mode. Choose this setting to send a

Table continues…

Name	Description
	183 session progress response in the early media phase. If you do not select this check box, *the Connected* pre-answer mode is chosen. This is the default setting. *Connected* setting sends a 200 OK SIP response in the early media phase. This field is applicable for the General Purpose and General Purpose Large clusters only.
Use short replication interval?	The check box to use a short replication interval.
Work Flow Engine name	The name of the Engagement Designer snap-in Workflow Engine. This field is applicable only for the **General Purpose** cluster.
Limit on the memory (GB) to allocate for base processes	The field to set a limit on the memory allocated for base processes. **Note:** Do not change the value of this field unless recommended by snap-ins.
Percent of memory to allocate base processes	The percentage of memory to allocate for base processes. **Note:** Do not change the value of this field unless recommended by snap-ins.
Percent of memory to allocate for WAS	The percentage of memory to allocate for WAS. **Note:** Do not change the value of this field unless recommended by snap-ins.
Limit on the memory (GB) to allocate for WAS	The field to set a limit on the memory allocated for WAS. **Note:** Do not change the value of this field unless recommended by snap-ins.

Servers tab

This tab has the following columns in two tables: **Assigned Servers** and **Unassigned Servers**. When you add a server to a cluster, the system displays the server under the **Assigned Servers** table for that cluster.

Name	Description
Name	The name of the Avaya Breeze™ server.

Table continues…

Name	Description
Version	The version of the Avaya Breeze™ server.
Description	The description of the Avaya Breeze™ server.

Services tab

Name	Description
Name	The name of the snap-in that might already be installed in a cluster, or available in the database.
Version	The snap-in version.
Action Pending	The actions that are pending for the snap-in. If no actions are pending, the system displays **None**.
Uninstall icon	The uninstall icon. If you select a snap-in and click **Uninstall**, then the snap-in is removed from the cluster after all the activity ceases.
Force Uninstall icon	The force uninstall icon. If you select a snap-in and click **Force Uninstall**, the snap-in is forcefully removed from the cluster without waiting to complete any pending actions.
TLS Version	The TLS version of the snap-in.

Button	Description
Select TLS Version for Selected Snap-in	The TLS version of the snap-in. The acceptable values are: • **Default** • **TLS v1.0** • **TLS v1.2** If you select **Default**, Avaya Breeze™ uses the value of the **Minimum TLS Version** field set in System Manager global configuration. You can change the TLS version of multiple snap-ins at a time.

Reliable Eventing Groups tab

Name	Description
Group	The name of the Reliable Eventing group available in the database.

Button	Description
Commit	Adds the cluster or saves the changes to the cluster attributes.
Cancel	Cancels your action and displays the previous page.

Installing new snap-ins

About this task

Complete this procedure to install new snap-ins on the upgraded cluster and to optionally install new versions of updated snap-ins. Be sure to install the newest versions of connector snap-ins and the snap-ins that are mandatory for your cluster profile. Mandatory services for a cluster profile are listed on the Cluster Editor page. For a list of connector snap-ins, see *Avaya Breeze™ Overview and Specification*.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Service Management**.
2. Load the snap-in.
   a. Click **Load**.
   b. In the Load Service window, click **Choose file**, browse to select your snap-in and click **Open**.
   c. Click **Load** in the Load Service window.
   d. For licensed snap-ins, if you agree to the Avaya End User License Agreement (EULA), click **Accept**.

      Your snap-in displays on the Service Management page with a **State** of **Loaded**.
3. Install the snap-in.
   a. Select the snap-in you want to install.
   b. Click **Install**.
   c. Select the clusters where you want the snap-in to reside, and click **Commit**.
   d. To see the status of the snap-in installation, click the Refresh Table icon located in the upper-left corner of the **All Services** list.

      Installed with a green check mark indicates that the snap-in has completed installation on all Avaya Breeze™ servers in the cluster. **Installing** with a yellow exclamation mark enclosed in a triangle indicates that the snap-in has not completed installation on all servers.

Setting preferred snap-in version

About this task

It is possible to set a preferred version of a snap-in. This designation can then be used in a service profile to indicate the version of the snap-in to provide to a group of users. You must first designate the version of the snap-in that you want to be the preferred version. Then, change the version designation for the snap-in in the service profile. For more information about service profiles and version designations, see *Administering Avaya Breeze™*.

Non-call-intercept snap-ins automatically use the preferred version. If a preferred version is not specified for a non-call-intercept snap-in, by default the latest version of the snap-in is used. Non-call-intercept snap-ins are not included in a service profile.

Procedure

1. Designate the preferred version.
   a. On System Manager,click **Elements** > **Avaya Breeze™** > **Service Management**.
   b. From the **All Services** list, select the version of the snap-in that you want to be the preferred version.
   c. Click **Set Preferred Version**.
   d. Select the clusters for which you want this to be the preferred version and click **Commit**.

      Note:

      You can set the preferred version for multiple snap-ins in a single transaction.
2. Edit the service profile.
   a. On System Manager,click **Elements** > **Avaya Breeze™** > **Configuration** > **Service Profiles**.
   b. Select the service profile and click **Edit**.
   c. Remove the snap-in from the service profile by clicking the **X** next to the snap-in name.
   d. In the list of **Available Service to Add to this Service Profile** click **Advanced** next to the snap-in name.
   e. For **Service Version** select **Preferred** and click **Add**.
   f. Click **Commit** to save the service profile.

Accepting new service

About this task

You must return the servers to service as a cluster from the Cluster Administration page after you have upgraded all the servers. Do not return them to service individually from the Server Administration page.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Cluster Administration**.
2. Click the checkbox in front of the upgraded cluster.
3. From the **Cluster State** drop-down menu, select **Accept New Service**.
4. Verify that the **Cluster State** column for the cluster changed to **Accepting**.

Verifying the Avaya Breeze™ Entity Link connection

About this task

Complete this task to verify that Session Manager can connect with Avaya Breeze™ using the SIP Entity Link. To do this you must verify the status of SIP link monitoring on the Session Manager instance.

Procedure

1. On System Manager, click **Elements** > **Session Manager** > **System Status** > **SIP Entity Monitoring**.
2. Click the name of the Session Manager Instance that you linked to Avaya Breeze™.

   The system displays a list with the status of all the Entity Links for the selected Session Manager.
3. Locate the Avaya Breeze™ 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 *Maintaining and Troubleshooting Avaya Breeze™*.

Upgrading with Method 2

Method 2 overview

Use Method 2 to simultaneously upgrade all nodes within a cluster within five minutes of each other. The upgrade is service impacting. Complete the upgrade during a maintenance window.

You can upgrade using one of the following methods:

- Using the ISO file
- Using System Manager Solution Deployment Manager

Follow the checklists for the required upgrade method.

Checklist for Method 2 upgrades

An ISO upgrade might fail due to networking issues and other problems outside the control of Avaya Breeze™. When this happens and the ISO was complete and not truncated by SFTP to the VM, it may be possible to successfully redo the upgrade.

Snap-ins may have prerequisite activity and post-upgrade activity that needs consideration before proceeding with the Platform upgrade. For information, refer to the snap-in documentation.

#	Action	Link/Notes	✔
1	Before upgrading Avaya Breeze™, upgrade the following in this order to the required release: 1. System Manager 2. Session Manager	—	

Table continues…

#	Action	Link/Notes	✔
2	Upgrade Avaya Aura® Media Server.	Refer to *Deploying and Updating Avaya Aura® Media Server Appliance*. Upgrade Avaya Aura® Media Server within the same maintenance window as when you upgrade Avaya Breeze™.	
3	If you have cluster database enabled, take a backup.	Refer to *Administering Avaya Breeze™*.	
4	For upgrading using ISO file method, download the ISO file and patch file (if required) from PLDS. Confirm the files are complete by running the checksum comparisons and then compare to the value on the PLDS page. If the file is correct, copy the ISO file and the patch file to each Avaya Breeze™ server you will be upgrading. For upgrading using Solution Deployment Manager method: • Download the OVA file and patch file (if required) from PLDS. Confirm the files are complete by running the checksum comparisons and then compare to the value on the PLDS page. • Download the versions*.xml file.	Downloading software from PLDS on page 59. Downloading the version_edp.xml file on page 64.	
5	Verify that the **Enrollment Password** is not expired.	Verifying Enrollment Password status on page 61.	
6	Change the state of the cluster you are upgrading to **Deny New Service**.	Denying new service on page 61.	
7	Verify that the server **Activity** field is zero.	Verify activity on page 61.	
8	Clear the **Enable Database Auto Switchover** field on the **Elements** > **Avaya Breeze™** > **Cluster Administration** general page.	This step is only required for multi-node clusters with Cluster database.	
9	Take a snapshot of the current VM to enable reverting if necessary.	This task is not required if using the Solution Deployment Manager method.	
10	Upgrade the Avaya Breeze™ software.	For upgrading using ISO file method: Upgrading the Avaya Breeze server on page 62.	

Table continues…

#	Action	Link/Notes	✔
		For upgrading using Solution Deployment Manager method: Upgrades using Solution Deployment Manager on page 62. The server reboots automatically when the upgrade script completes. Upgrade all within the cluster simultaneously.	
11	Install the patch file (if required) .	Patching Avaya Breeze on page 95.	
12	Upgrade the mandatory snap-ins and connector snap-ins. For more information, refer to the snap-in documentation.	—	
13	Select the **Enable Database Auto Switchover** field on the **Elements** > **Avaya Breeze™** > **Cluster Administration** general page.	—	This step is only required for multi-node clusters with Cluster database.
14	Verify data replication between System Manager and Avaya Breeze™.	Verifying replication status on page 69.	
15	Run Avaya Breeze™ maintenance tests for the server.	Running maintenance tests on page 70. Resolve errors before proceeding. For information, see *Maintaining and Troubleshooting Avaya Breeze™*.	
16	On the **Server Administration** page verify the following for the upgraded server: • The **Service Install Status** is a green checkmark. • The **Security Module** is Up. • The **License mode** is a green checkmark. • The **Version** displays Release Release 3.5. If using Reliable Eventing Framework, verify that the state of the node changes from Electing to Slave.	Verifying server status on page 70.	Complete this procedure only if you have disabled secure grid for the cluster that contains the servers you are upgrading. This procedure

Table continues…

#	Action	Link/Notes	✔
			is service impacting.
17	Change the state to **Accept New Service** for the upgraded Avaya Breeze™ cluster.	Accepting new service on page 70.	
18	Verify the Avaya Breeze™ SIP Entity Link with Session Manager.	Verifying the Avaya Breeze Entity Link connection on page 71.	
19	Repeat steps 7 through 17 for each server you are upgrading.	—	
20	Install new snap-ins.	Installing new snap-ins on page 71.	
21	Set the preferred version for each snap-in.	Setting preferred snap-in version on page 72.	
22	Test Avaya Breeze™ snap-ins to verify that they are functioning correctly. Delete any snapshots that you no longer need.	—	
23	Run a test alarm.	—	

Customer configuration information for ISO upgrades

You require the following information to upgrade Avaya Breeze™ with an ISO file. Have this information before you begin the upgrade.

Customer Login Settings

Field	Information to enter	Notes
Login Name	`Enter Login ID to use for the customer account.`	Login ID and password for customer account you will use during deployment
Enter Password	`Enter the customer account password.`	

Downloading software from PLDS

About this task

Note:

You can download product software from http://support.avaya.com also.

Procedure

1. In your web browser, type http://plds.avaya.com to go to the Avaya PLDS website.
2. On the PLDS website, enter your Login ID and password.
3. On the Home page, select **Assets**.
4. Select **View Downloads**.

5. Click the search icon ( ) for Company Name.
6. In the Search Companies dialog box, do the following:
   a. In the **%Name** field, type `Avaya` or the Partner company name.
   b. Click **Search Companies**.
   c. Locate the correct entry and click the **Select** link.
7. Search for the available downloads by using one of the following:
   - In **Download Pub ID**, type the download pub ID.
   - In the **Application** field, click the application name.
8. Click **Search Downloads**.
9. Scroll down to the entry for the download file, and click the **Download** link.
10. Select a location where you want to save the file, and click **Save**.
11. On the PLDS page, get the md5sum and sha1sum.
    a. In the directory where the ISO was downloaded, run the command: `md5sum aus-installer-correct version.iso`.
    b. Confirm that the checksum generated by this command matches the value on the PLDS page.
    c. If the values do not match, there was a network failure during transmission, and it is recommended to retry.
    d. If it fails again, contact Avaya Support.
12. **(Optional)** If you receive an error message, click the message, install Active X, and continue with the download.
13. **(Optional)** When the system displays the security warning, click **Install**.

    When the installation is complete, PLDS displays the downloads again with a check mark next to the downloads that have completed successfully.

Disabling the secure grid

About this task

Complete this procedure only if you have enabled the secure grid for a cluster. This procedure is service impacting.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Cluster Administration**.
2. Select the cluster that contains the servers you want to upgrade.
3. From the **Cluster State** drop-down menu, select **Deny New Service**.
4. Verify that the system displays **Denying** in the **Cluster State** column.

5. Select the cluster that contains the servers you want to upgrade and click **Edit**.
6. Under Cluster Attributes uncheck **Use secure grid?**
7. Click **Commit**.
8. Select the cluster that contains the servers you want to upgrade.
9. From the **Cluster State** drop-down menu, select **Accept New Service**.

Verifying Enrollment Password status

Avaya Breeze™ requires an Enrollment Password during the initial installation and deployment process. Enrolling a password establishes trust between System Manager and Avaya Breeze™. 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.

Denying new service

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Server Administration**.
2. Select the server that you want to upgrade.
3. From the **System State** drop-down menu, select **Deny New Service**.
4. Verify that the system displays **Denying** in the **System State** column.

Verify activity

About this task

Verify that currently there is no activity on the Avaya Breeze™ server you are upgrading.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Server Administration**.

2. In the row for the server you are upgrading, look in the **Activity** column.
3. Verify that the Activity is 0.

   Even after new service is stopped, it can take a couple of hours for activity to reach zero. If activity has not stopped in a reasonable time, you can choose to proceed with the upgrade. Active calls will continue, but Avaya Breeze™ snap-in call control for those calls will be lost.

Upgrading the Avaya Breeze™ server

Before you begin

1. Verify that you have copied the ISO upgrade file to the server that you are upgrading.
2. Take a snapshot of the current VM to enable reverting if necessary.

Procedure

1. Log on to the Avaya Breeze™ server.
2. Enter the command **`upgradeCE`** <*iso filename*>.
3. Step through prompts until the upgrade is installed.

Upgrades using Solution Deployment Manager

You can use System Manager Solution Deployment Manager, the centralized upgrade solution, to upgrade Avaya Breeze™. With Solution Deployment Manager, you can upgrade Avaya Breeze™ 3.3 to Release 3.5.

For this Solution Deployment Manager upgrade procedure, Solution Deployment Manager accesses the OVA file in the System Manager software library.

Refer to the following documents for more information:

- *Upgrading and Migrating Avaya Aura® applications from System Manager*
- *Administering Avaya Aura® System Manager*
- *Avaya Aura® System Manager Solution Deployment Manager Job-Aid*

Prerequisites

- Avaya Breeze™ must be running Release 3.3 or later.
- The VMware host or Appliance Virtualization Platform, and the Avaya Breeze™ virtual machine are administered in Solution Deployment Manager VM Management. For more information, see *Administering Avaya Aura® System Manager*.

Checklist for upgrading Avaya Breeze™ using Solution Deployment Manager

After completing this checklist, return to row 13 of the “Checklist for upgrading from Release 3.3.x to Release 3.5” to complete the remaining steps.

#	Task	References	✔
1	Complete the steps in this checklist after you have completed the step 1 through 11 in the “Checklist for upgrading from Release 3.3.x to Release 3.5”.		
2	Upload the versions_edp.xml to Solution Deployment Manager. For more information, see *Avaya Aura® System Manager Solution Deployment Manager Job-Aid*.		
3	Install the OVA file into the System Manager software library.	Installing the OVA file into the software library on page 63.	
4	Re-establish trust connection.	Re-establishing trust connection on page 64	
5	Refresh hosts.	Refreshing host on page 64	
6	Refresh the elements.	Refreshing elements on page 65	
7	Analyze the inventory.	Analyzing software on page 65	
8	Perform the preupgrade check.	Performing the preupgrade check on page 66	
9	Perform the upgrade.	Upgrading Avaya Breeze using Solution Deployment Manager on page 67	
10	Commit the upgrade of Avaya Breeze™.	Committing the upgrade of Avaya Breeze on page 69	
11	Copy the patch file to the Avaya Breeze™ server.		
12	Return to row 13 of the “Checklist for Method 2 upgrades” to complete the remaining steps.		

Installing the OVA file into the software library

Procedure

1. Copy the previously downloaded Avaya Breeze™ OVA file to the System Manager `/swlibrary/staging/sync/` directory. (If necessary, add the `staging/sync` folders to the directory structure.)
2. Navigate to **Home** > **Services** > **Solution Deployment Manager** > **Software Library Management** and click **Manage Files**.
3. In the list of Sync Files from directory, enter the SHA256 checksum and select a software library. For **Product Family**, **Device Type**, and **Software Type**, select **others**.
4. Click **Sync** and wait for the operation to complete.
5. 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.

6. Navigate to **Home** > **Services** > **Solution Deployment Manager** > **Software Library Management**.
7. Check SMGR_DEFAULT_LOCAL, click **Manage Files**, and confirm that the OVA file appears in the list of files under Software Library Files.

Downloading the version_edp.xml file

Procedure

1. Log in to https://plds.avaya.com.
2. Search for the `smgr-versionsxmls.zip` using PLDS ID **SMGRSUM0001**:
   a. Go to Assets tab.
   b. Click **View Downloads**.
   c. Select **Search by Download**.
   d. In the **Download pub ID** field, enter `SMGRSUM0001`.
   e. Click **Search Downloads**.
3. Download the zip file.
4. Extract the zip file.

Re-establishing trust connection

About this task

Use this procedure to upgrade an application that was not deployed from Solution Deployment Manager.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **VM Management**.
3. On the VM Management page, select the virtual machine.
4. To establish trust, click **More actions** > **Re-establish connection**.
5. In the Select Version pane, select `others`.
6. Type the credentials and click **Reestablish Connection**.

   The Current Action Status column displays the status of the virtual machine reestablishment.

Refreshing host

Procedure

1. On System Manager, click **Services** > **Solution Deployment Manager** > **VM Management**.
2. On **VM Management Tree**, click the required location.

3. Click the **Hosts** tab.

   The system displays the list of hosts for the selected location.

4. Select the required host.
5. Click **Refresh**.

   The **Current Action Status** column displays the status of the host.

Refreshing elements

Before you begin

- Configure the SNMP parameters on the device before you configure the same device in System Manager from Manage Elements.

  Note:

  Use the same SNMP credentials for the device in System Manager.

- On the User Settings page, configure the user settings.
- To upgrade a Communication Manager device, you must configure a profile 18 user on Communication Manager. You cannot use init and craft user profiles while configuring a profile 18 user.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, do the following:
   a. Select one or more devices.
   b. Click **Pre-upgrade Actions** > **Refresh Element(s)**.
4. On the Job Schedule page, click one of the following:
   - **Run Immediately**: To perform the job.
   - **Schedule later**: To perform the job at a scheduled time.
5. If you select **Schedule later**, select the date, time, and timezone.
6. Click **Schedule**.

   The **Last Action Status** column displays and the **Current Version** column displays the current version of the element.

Analyzing software

About this task

Analyze works on the version of OVA, service pack, and feature pack files uploaded to the software library. To get the correct entitle update or upgrade version, the version field must contain valid value. You can get the version values from versions files that are available on PLDS.

Custom patching does not require the analyze operation.

Before you begin

- On the Roles page, set the Software Management Infrastructure permission.
- Perform the Refresh elements operation.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, do the following:
   a. Select a device that you want to analyze.
   b. Click **Pre-upgrade Actions** > **Analyze**.
4. On the Job Schedule page, click one of the following:
   - **Run Immediately**: To perform the job.
   - **Schedule later**: To perform the job at a scheduled time.
5. If you select **Schedule later**, select the date, time, and timezone.
6. Click **Schedule**.

   The **Last Action Status** column displays a ✓, the **Current Version** column displays the current version of the element, and the **Entitled Upgrade Version** column displays the next version of the element for which the element is entitled to be upgraded.

Performing the preupgrade check

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, do the following:
   a. Select an application to upgrade.
   b. Click **Pre-upgrade Actions** > **Pre-upgrade Check**.
4. On the Pre-upgrade Configuration page, fill in the required information.

   Note:

   To migrate to an ESXi host from the old server, in **Target Host**, select the ESXi host.
5. On the Job Schedule page, click one of the following:
   - **Run Immediately**: To perform the job.
   - **Schedule later**: To perform the job at a scheduled time.
6. Click **Schedule**.

   On the Upgrade Management page, the status of the **Last Action Status** and **Pre-upgrade Check Status** columns display a ✓.

Upgrading Avaya Breeze™ using Solution Deployment Manager

About this task

Use this procedure to upgrade Avaya Breeze™ using System Manager Solution Deployment Manager. To upgrade using Solution Deployment Manager client. install the client and perform the following steps. For more information, see “Installing the Solution Deployment Manager client”.

Procedure

1. Perform one of the following:
   - On the System Manager web console, click **Services** > **Solution Deployment Manager**.
   - To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client**, or click the Solution Deployment Manager client icon ( ) on your desktop.
2. In the left navigation pane, click **Upgrade Management**.
3. Click the Avaya Breeze™ application to upgrade.
4. Click **Upgrade Actions** > **Upgrade/Update**.
5. On the Upgrade Configuration page, to view the devices associated with the application that you want to upgrade, perform the following:
   a. Click **Details** and review the dependent devices.
   b. Click **Done**.
6. To continue with upgrade when the recommended checks fail during the preupgrade check, select the **Override preupgrade check** check box.
7. To provide the upgrade configuration details, click **Edit**.
8. To upgrade:
   a. Select the appropriate ESXI host.
   b. In the **Upgrade Source** field, select **SMGR_DEFAULT_LOCAL**.
   c. In the **Upgrade To** field, select the OVA file.
   d. In **Existing Administrative User**, type the customer login name.
   e. In **Existing Administrative Password**, type the customer login password.
   f. Click **Pre-populate Data**.

      The system populates the data for the following fields:
      - IP Address
      - Short Hostname
      - Network Domain
      - Netmask

- Default Gateway
- DNS server(s)
- Timezone
- NTP server(s)
- Login Name
- Enter Customer Account Password
- Primary System Manager IP
- Enrollment Password
- Accept the License Agreement

g. In the **Flexi Footprint** field, select the footprint based on the user requirement.

h. Do one of the following in the **EASG User Access** field:

- Type `1` to enable EASG.

  Avaya recommends to enable EASG.

- Type `2` to disable EASG.

i. In the **Public** field, select the network that will supports Avaya Breeze™ security module network.

j. In the **Out of Band Management** field, select the network that supports the AAvaya Breeze™ management network.

k. In the **Datastore** field, select the datastore that supports the Avaya Breeze™ server.

l. Click **Save**.

   The system displays the Upgrade Configuration page.

9. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays ✅.

   If the field displays ❌, review the information on the Edit Upgrade Configuration page.

10. On the Upgrade Configuration page, click **Upgrade**.
11. On the Job Schedule page, click one of the following:
    - **Run Immediately**: To perform the job.
    - **Schedule later**: To perform the job at a scheduled time.
12. Click **Schedule**.
13. Click **Upgrade**.
14. To view the upgrade status, perform the following:

    a. In the navigation pane, click **Upgrade Job Status**.

    b. In the **Job Type** field, click **Upgrade**.

c. Click the upgrade job that you want to view.

15. Verify that the upgrade of the application is successful.

Committing the upgrade of Avaya Breeze™

Procedure

1. On System Manager, click **Services** > **Solution Deployment Manager** > **Upgrade Management**.
2. Select the Avaya Breeze™ by selecting the check box to the left of the **Name** column.
3. In the Upgrade Actions menu, click **Commit/Rolback Upgrade**.

   The system displays the Job Schedule page.
4. Select **Commit** in the **Upgrade Actions** column.
5. Click **Run Immediately** to perform the job, or click **Schedule later** to perform the job at a scheduled time.
6. Click **Schedule**.

   The system returns to the Upgrade Management page.
7. Click **Enable Auto Refresh**.

   The system will update the **Last Action** and **Last Action Status** fields when the Commit job is complete.
8. Click the icon in the **Last Action Status** field.

   The system displays the Element Check Status popup.
9. Click **Done**.
10. To view the Commit job status, perform the following:
    a. In the navigation pane, click **Upgrade Jobs Status**.

       The system displays the Upgrade Jobs Status page.
    b. In the **Job Type** menu, click **Commit/Rollback Upgrade**.
    c. In the **Job Name** column, click the job that you want to view.

       The system displays the Element Job Status Details.
    d. Click **Done**.

Verifying replication status

About this task

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

Procedure

1. On System Manager, click **Services** > **Replication**.
2. Locate the Avaya Breeze™ in the **Replica Group** list.

3. In the **Synchronization Status** column, verify that the Avaya Breeze™ 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™*.

Running maintenance tests

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **System Tools And Monitoring** > **Maintenance Tests**.
3. In the **Select Avaya Breeze™ to test** field, select an Avaya Breeze™ server from the drop-down menu.
4. To run all the tests, click **Execute All Tests**.
5. To run specific tests:
   a. Select the test or tests that you want to run.
   b. Click **Execute Selected Tests**.

Verifying server status

About this task

Verify that the Avaya Breeze™ server has upgraded to Release 3.5 and is functioning correctly.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Server Administration**.
2. In the row for the Avaya Breeze™ server you are upgrading, 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.

Accepting new service

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Server Administration**.
2. Select the server and click **System State** > **Accept New Service**.
3. Verify that the **System State** column for the server changes to **Accepting**.

Verifying the Avaya Breeze™ Entity Link connection

About this task

Complete this task to verify that Session Manager can connect with Avaya Breeze™ using the SIP Entity Link. To do this you must verify the status of SIP link monitoring on the Session Manager instance.

Procedure

1. On System Manager, click **Elements** > **Session Manager** > **System Status** > **SIP Entity Monitoring**.
2. Click the name of the Session Manager Instance that you linked to Avaya Breeze™.

   The system displays a list with the status of all the Entity Links for the selected Session Manager.
3. Locate the Avaya Breeze™ 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 *Maintaining and Troubleshooting Avaya Breeze™*.

Installing new snap-ins

About this task

Complete this procedure to install new snap-ins on the upgraded cluster and to optionally install new versions of updated snap-ins. Be sure to install the newest versions of connector snap-ins and the snap-ins that are mandatory for your cluster profile. Mandatory services for a cluster profile are listed on the Cluster Editor page. For a list of connector snap-ins, see *Avaya Breeze™ Overview and Specification*.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Service Management**.
2. Load the snap-in.
   a. Click **Load**.
   b. In the Load Service window, click **Choose file**, browse to select your snap-in and click **Open**.
   c. Click **Load** in the Load Service window.
   d. For licensed snap-ins, if you agree to the Avaya End User License Agreement (EULA), click **Accept**.

      Your snap-in displays on the Service Management page with a **State** of **Loaded**.
3. Install the snap-in.
   a. Select the snap-in you want to install.
   b. Click **Install**.

c. Select the clusters where you want the snap-in to reside, and click **Commit**.

d. To see the status of the snap-in installation, click the Refresh Table icon located in the upper-left corner of the **All Services** list.

   Installed with a green check mark indicates that the snap-in has completed installation on all Avaya Breeze™ servers in the cluster. **Installing** with a yellow exclamation mark enclosed in a triangle indicates that the snap-in has not completed installation on all servers.

Setting preferred snap-in version

About this task

It is possible to set a preferred version of a snap-in. This designation can then be used in a service profile to indicate the version of the snap-in to provide to a group of users. You must first designate the version of the snap-in that you want to be the preferred version. Then, change the version designation for the snap-in in the service profile. For more information about service profiles and version designations, see *Administering Avaya Breeze™*.

Non-call-intercept snap-ins automatically use the preferred version. If a preferred version is not specified for a non-call-intercept snap-in, by default the latest version of the snap-in is used. Non-call-intercept snap-ins are not included in a service profile.

Procedure

1. Designate the preferred version.

   a. On System Manager,click **Elements** > **Avaya Breeze™** > **Service Management**.

   b. From the **All Services** list, select the version of the snap-in that you want to be the preferred version.

   c. Click **Set Preferred Version**.

   d. Select the clusters for which you want this to be the preferred version and click **Commit**.

   Note:

   You can set the preferred version for multiple snap-ins in a single transaction.

2. Edit the service profile.

   a. On System Manager,click **Elements** > **Avaya Breeze™** > **Configuration** > **Service Profiles**.

   b. Select the service profile and click **Edit**.

   c. Remove the snap-in from the service profile by clicking the **X** next to the snap-in name.

   d. In the list of **Available Service to Add to this Service Profile** click **Advanced** next to the snap-in name.

   e. For **Service Version** select **Preferred** and click **Add**.

   f. Click **Commit** to save the service profile.

Upgrading with Method 3

Method 3 overview

Use Method 3 for a rolling upgrade where each node is upgraded individually and the upgrade is not service impacting. This upgrade method is not available with Release 3.5 upgrades.

You can upgrade using one of the following methods:

- Using the ISO file
- Using System Manager Solution Deployment Manager

Follow the checklists for the required upgrade method.

Checklist for Method 3 upgrades

An ISO upgrade might fail due to networking issues and other problems outside the control of Avaya Breeze™. When this happens and the ISO was complete and not truncated by SFTP to the VM, it may be possible to successfully redo the upgrade.

Snap-ins may have prerequisite activity and post-upgrade activity that needs consideration before proceeding with the Platform upgrade. For information, refer to the snap-in documentation.

#	Action	Link/Notes	✔
1	Before upgrading Avaya Breeze™, upgrade the following in this order to the required release: 1. System Manager 2. Session Manager	—	
2	Upgrade Avaya Aura® Media Server.	Refer to *Deploying and Updating Avaya Aura® Media Server Appliance*. Upgrade Avaya Aura® Media Server within the same maintenance window as when you upgrade Avaya Breeze™.	
3	If you have cluster database enabled, take a backup.	Refer to *Administering Avaya Breeze™*.	
4	On the Cluster Administration page, identify the cluster you want to upgrade. For clusters with multiple servers, determine the sequence in which you want to upgrade the servers.	Viewing and changing server cluster database status on page 76. Server upgrade sequence on page 76. This step is for upgrading Avaya Breeze™ nodes with snap-ins that	

Table continues…

#	Action	Link/Notes	✔
		support non-service impacting upgrades. Check your snap-in documentation for specific upgrade considerations.	
5	For upgrading using ISO file method, download the ISO file and patch file (if required) from PLDS. Confirm the files are complete by running the checksum comparisons and then compare to the value on the PLDS page. If the file is correct, copy the ISO file and the patch file to each Avaya Breeze™ server you will be upgrading. For upgrading using Solution Deployment Manager method: • Download the OVA file and patch file (if required) from PLDS. Confirm the files are complete by running the checksum comparisons and then compare to the value on the PLDS page. • Download the versions*.xml file.	Downloading software from PLDS on page 77. Downloading the version_edp.xml file on page 81.	
6	Verify that the **Enrollment Password** is not expired.	Verifying Enrollment Password status on page 78.	
7	Change the state of the node you are upgrading to **Deny New Service**.	Denying new service on page 78.	
8	If cluster database is enabled and the next node is an active node, change the status of the active node to standby.	Viewing and changing server cluster database status on page 76.	
9	Verify that the server **Activity** field is zero.	Verify activity on page 79.	
10	Take a snapshot of the current VM to enable reverting if necessary.	This task is not required if using the Solution Deployment Manager method.	
11	Upgrade the Avaya Breeze™ software.	For upgrading using ISO file method: Upgrading the Avaya Breeze server on page 79. For upgrading using Solution Deployment Manager method: Upgrades using Solution Deployment Manager on page 79. The server reboots automatically when the upgrade script completes.	

Table continues…

#	Action	Link/Notes	✔
12	Install the patch file (if required) .	Patching Avaya Breeze on page 95.	
13	Upgrade the mandatory snap-ins and connector snap-ins. For more information, refer to the snap-in documentation.	—	
14	Verify data replication between System Manager and Avaya Breeze™.	Verifying replication status on page 88.	
15	Run Avaya Breeze™ maintenance tests for the server.	Running maintenance tests on page 89. Resolve errors before proceeding. For information, see *Maintaining and Troubleshooting Avaya Breeze™*.	
16	On the **Server Administration** page verify the following for the upgraded server: • The **Service Install Status** is a green checkmark. • The **Security Module** is Up. • The **License mode** is a green checkmark. • The **Version** displays Release Release 3.5. If using Reliable Eventing Framework, verify that the state of the node changes from Electing to Slave.	Verifying server status on page 89.	Complete this procedure only if you have disabled secure grid for the cluster that contains the servers you are upgrading. This procedure is service impacting.
17	Change the state to **Accept New Service** for the upgraded Avaya Breeze™ node.	Accepting new service on page 89.	
18	Verify the Avaya Breeze™ SIP Entity Link with Session Manager.	Verifying the Avaya Breeze Entity Link connection on page 90.	
19	Repeat steps 7 through 17 for each server you are upgrading.	—	
20	Install new snap-ins.	Installing new snap-ins on page 90.	
21	Set the preferred version for each snap-in.	Setting preferred snap-in version on page 91.	
22	Test Avaya Breeze™ snap-ins to verify that they are functioning correctly. Delete any snapshots that you no longer need.	—	
23	Run a test alarm.	—	

Customer configuration information for ISO upgrades

You require the following information to upgrade Avaya Breeze™ with an ISO file. Have this information before you begin the upgrade.

Customer Login Settings

Field	Information to enter	Notes
Login Name	`Enter Login ID to use for the customer account.`	Login ID and password for customer account you will use during deployment
Enter Password	`Enter the customer account password.`	

Server upgrade sequence

If you have multiple servers in a cluster and have snap-ins that use the cluster database, you must upgrade the servers in the correct sequence to avoid customer impact. The sequence depends on the active, standby, or idle status of the server. View the status on the System Manager Avaya Breeze™ Cluster Administration page.

Upgrade sequence

1. Upgrade all idle servers one at a time.
2. Upgrade the standby server.
3. Switch the active server to be the standby server. (The standby server becomes the new active server.)
4. Upgrade the new standby server.

If using Reliable Eventing Framework, you can upgrade the broker nodes in any sequence.

Viewing and changing server cluster database status

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Cluster Administration**.
2. Click **Show** in front of the cluster that contains the servers you are upgrading.
3. In the Cluster Database column, identify the Active, Standby, and Idle servers.
4. To change the server cluster database status, put the cluster in **Deny New State** and click the status in the Cluster Database column.
   - Active status changes to standby
   - Standby status changes to active
   - Idle status changes to standby

Downloading software from PLDS

About this task

Note:

You can download product software from http://support.avaya.com also.

Procedure

1. In your web browser, type http://plds.avaya.com to go to the Avaya PLDS website.
2. On the PLDS website, enter your Login ID and password.
3. On the Home page, select **Assets**.
4. Select **View Downloads**.
5. Click the search icon ( ) for Company Name.
6. In the Search Companies dialog box, do the following:
   a. In the **%Name** field, type `Avaya` or the Partner company name.
   b. Click **Search Companies**.
   c. Locate the correct entry and click the **Select** link.
7. Search for the available downloads by using one of the following:
   - In **Download Pub ID**, type the download pub ID.
   - In the **Application** field, click the application name.
8. Click **Search Downloads**.
9. Scroll down to the entry for the download file, and click the **Download** link.
10. Select a location where you want to save the file, and click **Save**.
11. On the PLDS page, get the md5sum and sha1sum.
    a. In the directory where the ISO was downloaded, run the command: `md5sum aus-installer-correct version.iso`.
    b. Confirm that the checksum generated by this command matches the value on the PLDS page.
    c. If the values do not match, there was a network failure during transmission, and it is recommended to retry.
    d. If it fails again, contact Avaya Support.
12. **(Optional)** If you receive an error message, click the message, install Active X, and continue with the download.
13. **(Optional)** When the system displays the security warning, click **Install**.

    When the installation is complete, PLDS displays the downloads again with a check mark next to the downloads that have completed successfully.

Disabling the secure grid

About this task

Complete this procedure only if you have enabled the secure grid for a cluster. This procedure is service impacting.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Cluster Administration**.
2. Select the cluster that contains the servers you want to upgrade.
3. From the **Cluster State** drop-down menu, select **Deny New Service**.
4. Verify that the system displays **Denying** in the **Cluster State** column.
5. Select the cluster that contains the servers you want to upgrade and click **Edit**.
6. Under Cluster Attributes uncheck **Use secure grid?**
7. Click **Commit**.
8. Select the cluster that contains the servers you want to upgrade.
9. From the **Cluster State** drop-down menu, select **Accept New Service**.

Verifying Enrollment Password status

Avaya Breeze™ requires an Enrollment Password during the initial installation and deployment process. Enrolling a password establishes trust between System Manager and Avaya Breeze™. 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.

Denying new service

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Server Administration**.

2. Select the server that you want to upgrade.
3. From the **System State** drop-down menu, select **Deny New Service**.
4. Verify that the system displays **Denying** in the **System State** column.

Verify activity

About this task

Verify that currently there is no activity on the Avaya Breeze™ server you are upgrading.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Server Administration**.
2. In the row for the server you are upgrading, look in the **Activity** column.
3. Verify that the Activity is 0.

   Even after new service is stopped, it can take a couple of hours for activity to reach zero. If activity has not stopped in a reasonable time, you can choose to proceed with the upgrade. Active calls will continue, but Avaya Breeze™ snap-in call control for those calls will be lost.

Upgrading the Avaya Breeze™ server

Before you begin

1. Verify that you have copied the ISO upgrade file to the server that you are upgrading.
2. Take a snapshot of the current VM to enable reverting if necessary.

Procedure

1. Log on to the Avaya Breeze™ server.
2. Enter the command **`upgradeCE`** <*iso filename*>.
3. Step through prompts until the upgrade is installed.

Upgrades using Solution Deployment Manager

You can use System Manager Solution Deployment Manager, the centralized upgrade solution, to upgrade Avaya Breeze™. With Solution Deployment Manager, you can upgrade Avaya Breeze™ 3.3 to Release 3.5.

For this Solution Deployment Manager upgrade procedure, Solution Deployment Manager accesses the OVA file in the System Manager software library.

Refer to the following documents for more information:

- *Upgrading and Migrating Avaya Aura® applications from System Manager*
- *Administering Avaya Aura® System Manager*
- *Avaya Aura® System Manager Solution Deployment Manager Job-Aid*

Prerequisites

- Avaya Breeze™ must be running Release 3.3 or later.

- The VMware host or Appliance Virtualization Platform, and the Avaya Breeze™ virtual machine are administered in Solution Deployment Manager VM Management. For more information, see *Administering Avaya Aura® System Manager*.

Checklist for upgrading Avaya Breeze™ using Solution Deployment Manager

After completing this checklist, return to row 13 of the "Checklist for upgrading from Release 3.3.x to Release 3.5" to complete the remaining steps.

#	Task	References	✔
1	Complete the steps in this checklist after you have completed the step 1 through 11 in the "Checklist for upgrading from Release 3.3.x to Release 3.5".		
2	Upload the versions_edp.xml to Solution Deployment Manager. For more information, see *Avaya Aura® System Manager Solution Deployment Manager Job-Aid*.		
3	Install the OVA file into the System Manager software library.	Installing the OVA file into the software library on page 80.	
4	Re-establish trust connection.	Re-establishing trust connection on page 81	
5	Refresh hosts.	Refreshing host on page 82	
6	Refresh the elements.	Refreshing elements on page 82	
7	Analyze the inventory.	Analyzing software on page 83	
8	Perform the preupgrade check.	Performing the preupgrade check on page 83	
9	Perform the upgrade.	Upgrading Avaya Breeze using Solution Deployment Manager on page 84	
10	Commit the upgrade of Avaya Breeze™.	Committing the upgrade of Avaya Breeze on page 88	
11	Copy the patch file to the Avaya Breeze™ server.		
12	Return to row 13 of the "Checklist for upgrading from Release 3.3.x to Release 3.5" to complete the remaining steps.		

Installing the OVA file into the software library

Procedure

1. Copy the previously downloaded Avaya Breeze™ OVA file to the System Manager `/swlibrary/staging/sync/` directory. (If necessary, add the `staging/sync` folders to the directory structure.)

2. Navigate to **Home** > **Services** > **Solution Deployment Manager** > **Software Library Management** and click **Manage Files**.
3. In the list of Sync Files from directory, enter the SHA256 checksum and select a software library. For **Product Family**, **Device Type**, and **Software Type**, select **others**.
4. Click **Sync** and wait for the operation to complete.
5. 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.
6. Navigate to **Home** > **Services** > **Solution Deployment Manager** > **Software Library Management**.
7. Check SMGR_DEFAULT_LOCAL, click **Manage Files**, and confirm that the OVA file appears in the list of files under Software Library Files.

Downloading the version_edp.xml file

Procedure

1. Log in to https://plds.avaya.com.
2. Search for the `smgr-versionsxmls.zip` using PLDS ID **SMGRSUM0001**:
   a. Go to Assets tab.
   b. Click **View Downloads**.
   c. Select **Search by Download**.
   d. In the **Download pub ID** field, enter `SMGRSUM0001`.
   e. Click **Search Downloads**.
3. Download the zip file.
4. Extract the zip file.

Re-establishing trust connection

About this task

Use this procedure to upgrade an application that was not deployed from Solution Deployment Manager.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **VM Management**.
3. On the VM Management page, select the virtual machine.
4. To establish trust, click **More actions** > **Re-establish connection**.
5. In the Select Version pane, select `others`.
6. Type the credentials and click **Reestablish Connection**.

The Current Action Status column displays the status of the virtual machine reestablishment.

Refreshing host

Procedure

1. On the System Manager Web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. On **Application Management Tree**, click the required location.
3. Click the **Hosts** tab.

   The system displays the list of hosts for the selected location.
4. Select the required host.
5. Click **Refresh**.

   The **Current Action Status** column displays the status of the host.

Refreshing elements

Before you begin

- Configure the SNMP parameters on the device before you configure the same device in System Manager from Manage Elements.

  Note:

  Use the same SNMP credentials for the device in System Manager.
- On the User Settings page, configure the user settings.
- To upgrade a Communication Manager device, you must configure a profile 18 user on Communication Manager. You cannot use init and craft user profiles while configuring a profile 18 user.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, do the following:
   a. Select one or more devices.
   b. Click **Pre-upgrade Actions** > **Refresh Element(s)**.
4. On the Job Schedule page, click one of the following:
   - **Run Immediately**: To perform the job.
   - **Schedule later**: To perform the job at a scheduled time.
5. If you select **Schedule later**, select the date, time, and timezone.
6. Click **Schedule**.

   The **Last Action Status** column displays and the **Current Version** column displays the current version of the element.

Analyzing software

About this task

Analyze works on the version of OVA, service pack, and feature pack files uploaded to the software library. To get the correct entitle update or upgrade version, the version field must contain valid value. You can get the version values from versions files that are available on PLDS.

Custom patching does not require the analyze operation.

Before you begin

- On the Roles page, set the Software Management Infrastructure permission.
- Perform the Refresh elements operation.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, do the following:
   a. Select a device that you want to analyze.
   b. Click **Pre-upgrade Actions** > **Analyze**.
4. On the Job Schedule page, click one of the following:
   - **Run Immediately**: To perform the job.
   - **Schedule later**: To perform the job at a scheduled time.
5. If you select **Schedule later**, select the date, time, and timezone.
6. Click **Schedule**.

   The **Last Action Status** column displays a ✓, the **Current Version** column displays the current version of the element, and the **Entitled Upgrade Version** column displays the next version of the element for which the element is entitled to be upgraded.

Performing the preupgrade check

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, do the following:
   a. Select an application to upgrade.
   b. Click **Pre-upgrade Actions** > **Pre-upgrade Check**.
4. On the Pre-upgrade Configuration page, fill in the required information.

   Note:

   To migrate to an ESXi host from the old server, in **Target Host**, select the ESXi host.

5. On the Job Schedule page, click one of the following:
   - **Run Immediately**: To perform the job.
   - **Schedule later**: To perform the job at a scheduled time.
6. Click **Schedule**.

   On the Upgrade Management page, the status of the **Last Action Status** and **Pre-upgrade Check Status** columns display a ✓.

Upgrading Avaya Breeze™ using Solution Deployment Manager

About this task

Use this procedure to upgrade Avaya Breeze™ using System Manager Solution Deployment Manager. To upgrade using Solution Deployment Manager client. install the client and perform the following steps. For more information, see “Installing the Solution Deployment Manager client”.

Procedure

1. Perform one of the following:
   - On the System Manager web console, click **Services** > **Solution Deployment Manager**.
   - To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client**, or click the Solution Deployment Manager client icon (SDM) on your desktop.
2. In the left navigation pane, click **Upgrade Management**.
3. Click the Avaya Breeze™ application to upgrade.
4. Click **Upgrade Actions** > **Upgrade/Update**.
5. On the Upgrade Configuration page, to view the devices associated with the application that you want to upgrade, perform the following:
   a. Click **Details** and review the dependent devices.
   b. Click **Done**.
6. To continue with upgrade when the recommended checks fail during the preupgrade check, select the **Override preupgrade check** check box.
7. To provide the upgrade configuration details, click **Edit**.
8. To upgrade:
   a. Select the appropriate ESXI host.
   b. In the **Upgrade Source** field, select **SMGR_DEFAULT_LOCAL**.
   c. In the **Upgrade To** field, select the OVA file.
   d. In **Existing Administrative User**, type the customer login name.
   e. In **Existing Administrative Password**, type the customer login password.
   f. Click **Pre-populate Data**.

The system populates the data for the following fields:

- IP Address
- Short Hostname
- Network Domain
- Netmask
- Default Gateway
- DNS server(s)
- Timezone
- NTP server(s)
- Login Name
- Enter Customer Account Password
- Primary System Manager IP
- Enrollment Password
- Accept the License Agreement

g. In the **Flexi Footprint** field, select the footprint based on the user requirement.

h. Do one of the following in the **EASG User Access** field:

- Type `1` to enable EASG.

  Avaya recommends to enable EASG.

- Type `2` to disable EASG.

i. In the **Public** field, select the network that will supports Avaya Breeze™ security module network.

j. In the **Out of Band Management** field, select the network that supports the AAvaya Breeze™ management network.

k. In the **Datastore** field, select the datastore that supports the Avaya Breeze™ server.

l. Click **Save**.

The system displays the Upgrade Configuration page.

9. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays ✓.

   If the field displays ✗, review the information on the Edit Upgrade Configuration page.

10. On the Upgrade Configuration page, click **Upgrade**.

11. On the Job Schedule page, click one of the following:

- **Run Immediately**: To perform the job.
- **Schedule later**: To perform the job at a scheduled time.

12. Click **Schedule**.
13. Click **Upgrade**.
14. To view the upgrade status, perform the following:
    a. In the navigation pane, click **Upgrade Job Status**.
    b. In the **Job Type** field, click **Upgrade**.
    c. Click the upgrade job that you want to view.
15. Verify that the upgrade of the application is successful.

Installing the Solution Deployment Manager client

Procedure

1. Download the `Avaya_SDMClient_win64_8.0.0.0.0931322_6.zip` file from the Avaya Support website at http://support.avaya.com or from the Avaya PLDS website, at https://plds.avaya.com/.
2. On the Avaya Support website, click **Support by Products** > **Downloads**, and type the product name as **System Manager**, and Release as **8.0.x**.
3. Click the **Avaya Aura® System Manager Release 8.0.x SDM Client Downloads, 8.0.x** link. Save the zip file, and extract to a location on your computer by using the WinZip application.

   You can also copy the zip file to your software library directory, for example, `c:/tmp/Aura`.
4. Right click on the executable, and select **Run as administrator** to run the `Avaya_SDMClient_win64_8.0.0.0.0931322_6.exe` file.

   The system displays the Avaya Solution Deployment Manager screen.
5. On the Welcome page, click **Next**.
6. On the License Agreement page, read the License Agreement, and if you agree to its terms, click **I accept the terms of the license agreement** and click **Next**.
7. On the Install Location page, perform one of the following:
   - To install the Solution Deployment Manager client in the system-defined folder, leave the default settings, and click **Next**.
   - To specify a different location for installing the Solution Deployment Manager client, click **Choose**, and browse to an empty folder. Click **Next**.

     To restore the path of the default directory, click **Restore Default Folder**.

   The default installation directory of the Solution Deployment Manager client is `C:\Program Files\Avaya\AvayaSDMClient`.
8. Click **Next**.
9. On the Pre-Installation Summary page, review the information, and click **Next**.

10. On the User Input page, perform the following:
    a. To start the Solution Deployment Manager client at the start of the system, select the **Automatically start SDM service at startup** check box.
    b. To change the default directory, in Select Location of Software Library Directory, click **Choose** and select a directory.

       The default software library of the Solution Deployment Manager client is `C:\Program Files\Avaya\AvayaSDMClient\Default_Artifacts`.

       You can save the artifacts in the specified directory.
    c. In **Data Port No**, select the appropriate data port.

       The default data port is 1527. The data port range is from 1527 through 1627.
    d. In **Application Port No**, select the appropriate application port.

       The default application port is 443. If this port is already in use by any of your application on your system, then the system does not allow you to continue the installation. You must assign a different port number from the defined range. The application port range is from 443 through 543.

       Note:

       After installing the Solution Deployment Manager client in the defined range of ports, you cannot change the port after the installation.
    e. **(Optional)** Click **Reset All to Default**.
11. Click **Next**.
12. On the Summary and Validation page, verify the product information and the system requirements.

    The system performs the feasibility checks, such as disk space and memory. If the requirements are not met, the system displays an error message. To continue with the installation, make the disk space, memory, and the ports available.
13. Click **Install**.
14. To exit the installer, on the Install Complete page, click **Done**.

    The installer creates a shortcut on the desktop.
15. To start the client, click the Solution Deployment Manager client icon, .

Next steps

- Configure the laptop to get connected to the services port if you are using the services port to install.
- Connect the Solution Deployment Manager client to Appliance Virtualization Platform through the customer network or services port.

  For information about “Methods to connect the Solution Deployment Manager client to Appliance Virtualization Platform”, see *Using the Solution Deployment Manager client*.

Committing the upgrade of Avaya Breeze™

Procedure

1. On System Manager, click **Services** > **Solution Deployment Manager** > **Upgrade Management**.
2. Select the Avaya Breeze™ by selecting the check box to the left of the **Name** column.
3. In the Upgrade Actions menu, click **Commit/Rolback Upgrade**.

   The system displays the Job Schedule page.
4. Select **Commit** in the **Upgrade Actions** column.
5. Click **Run Immediately** to perform the job, or click **Schedule later** to perform the job at a scheduled time.
6. Click **Schedule**.

   The system returns to the Upgrade Management page.
7. Click **Enable Auto Refresh**.

   The system will update the **Last Action** and **Last Action Status** fields when the Commit job is complete.
8. Click the icon in the **Last Action Status** field.

   The system displays the Element Check Status popup.
9. Click **Done**.
10. To view the Commit job status, perform the following:
    a. In the navigation pane, click **Upgrade Jobs Status**.

       The system displays the Upgrade Jobs Status page.
    b. In the **Job Type** menu, click **Commit/Rollback Upgrade**.
    c. In the **Job Name** column, click the job that you want to view.

       The system displays the Element Job Status Details.
    d. Click **Done**.

Verifying replication status

About this task

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

Procedure

1. On System Manager, click **Services** > **Replication**.
2. Locate the Avaya Breeze™ in the **Replica Group** list.
3. In the **Synchronization Status** column, verify that the Avaya Breeze™ 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™*.

Running maintenance tests

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **System Tools And Monitoring** > **Maintenance Tests**.
3. In the **Select Avaya Breeze™ to test** field, select an Avaya Breeze™ server from the drop-down menu.
4. To run all the tests, click **Execute All Tests**.
5. To run specific tests:
   a. Select the test or tests that you want to run.
   b. Click **Execute Selected Tests**.

Verifying server status

About this task

Verify that the Avaya Breeze™ server has upgraded to Release 3.5 and is functioning correctly.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Server Administration**.
2. In the row for the Avaya Breeze™ server you are upgrading, 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.

Accepting new service

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Server Administration**.
2. Select the server and click **System State** > **Accept New Service**.
3. Verify that the **System State** column for the server changes to **Accepting**.

Verifying the Avaya Breeze™ Entity Link connection

About this task

Complete this task to verify that Session Manager can connect with Avaya Breeze™ using the SIP Entity Link. To do this you must verify the status of SIP link monitoring on the Session Manager instance.

Procedure

1. On System Manager, click **Elements** > **Session Manager** > **System Status** > **SIP Entity Monitoring**.
2. Click the name of the Session Manager Instance that you linked to Avaya Breeze™.

   The system displays a list with the status of all the Entity Links for the selected Session Manager.
3. Locate the Avaya Breeze™ 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 *Maintaining and Troubleshooting Avaya Breeze™*.

Installing new snap-ins

About this task

Complete this procedure to install new snap-ins on the upgraded cluster and to optionally install new versions of updated snap-ins. Be sure to install the newest versions of connector snap-ins and the snap-ins that are mandatory for your cluster profile. Mandatory services for a cluster profile are listed on the Cluster Editor page. For a list of connector snap-ins, see *Avaya Breeze™ Overview and Specification*.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Service Management**.
2. Load the snap-in.
   a. Click **Load**.
   b. In the Load Service window, click **Choose file**, browse to select your snap-in and click **Open**.
   c. Click **Load** in the Load Service window.
   d. For licensed snap-ins, if you agree to the Avaya End User License Agreement (EULA), click **Accept**.

      Your snap-in displays on the Service Management page with a **State** of **Loaded**.
3. Install the snap-in.
   a. Select the snap-in you want to install.
   b. Click **Install**.

c. Select the clusters where you want the snap-in to reside, and click **Commit**.

d. To see the status of the snap-in installation, click the Refresh Table icon located in the upper-left corner of the **All Services** list.

   Installed with a green check mark indicates that the snap-in has completed installation on all Avaya Breeze™ servers in the cluster. **Installing** with a yellow exclamation mark enclosed in a triangle indicates that the snap-in has not completed installation on all servers.

Setting preferred snap-in version

About this task

It is possible to set a preferred version of a snap-in. This designation can then be used in a service profile to indicate the version of the snap-in to provide to a group of users. You must first designate the version of the snap-in that you want to be the preferred version. Then, change the version designation for the snap-in in the service profile. For more information about service profiles and version designations, see *Administering Avaya Breeze™*.

Non-call-intercept snap-ins automatically use the preferred version. If a preferred version is not specified for a non-call-intercept snap-in, by default the latest version of the snap-in is used. Non-call-intercept snap-ins are not included in a service profile.

Procedure

1. Designate the preferred version.

   a. On System Manager,click **Elements** > **Avaya Breeze™** > **Service Management**.

   b. From the **All Services** list, select the version of the snap-in that you want to be the preferred version.

   c. Click **Set Preferred Version**.

   d. Select the clusters for which you want this to be the preferred version and click **Commit**.

   Note:

   You can set the preferred version for multiple snap-ins in a single transaction.

2. Edit the service profile.

   a. On System Manager,click **Elements** > **Avaya Breeze™** > **Configuration** > **Service Profiles**.

   b. Select the service profile and click **Edit**.

   c. Remove the snap-in from the service profile by clicking the **X** next to the snap-in name.

   d. In the list of **Available Service to Add to this Service Profile** click **Advanced** next to the snap-in name.

   e. For **Service Version** select **Preferred** and click **Add**.

   f. Click **Commit** to save the service profile.

Enhanced Access Security Gateway

Avaya Breeze™ 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™ 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™ 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™ 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™ 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™. 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™ 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 4: Patching

Determining patching sequence

About this task

If you do not have snap-ins that use the cluster database, patch the servers in any sequence one at a time. See Patching Avaya Breeze on page 95. If you have multiple servers in a cluster and have snap-ins that use the cluster database, you must patch the servers in the correct sequence to avoid customer impact. The sequence depends on the active, standby, or idle status of the server. Follow the sequence in this procedure to patch your servers.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Cluster Administration**.
3. Click **Show** in front of the cluster you are patching 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	✓

4. In the Cluster Database column, identify the Active, Standby and idle servers.
5. Patch all Idle servers one at a time.
6. Patch the server with the Standby cluster database.
7. Click **Active** in the **Cluster Database** column of the Active server to switch it to Standby.
8. Click **Continue** to complete the switch to Standby.
9. Patch the server that now is the Standby.

Patching Avaya Breeze™

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™ 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™ server. The patch should have the following Linux permissions: `rw-r--r--`.

Procedure

1. Log in to Avaya Breeze™ 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™ 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™ and execute the command **`patchCE -s`**.
   - Log in to Avaya Breeze™ 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™ 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.

Related links

Patch command options on page 96

Patch command options

```
patchCE [i|s|v] [patch file]
```

- i<patch file>: install patch
<patch file>: install patch
- s [patch file]: show patch information for binary or installed patch
- v <patch file>: verify patch can be installed

Related links

Patching Avaya Breeze on page 95

Chapter 5: Resources

Documentation

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

Title	Use this document to:	Audience
Understanding		
Avaya Breeze™ Overview and Specification	Understand the Avaya Breeze™ platform, customer requirements, and design considerations.	Sales engineers Programmers System administrators Services and support personnel
Avaya Aura® System Manager Overview and Specification	Understand System Manager customer requirements and design considerations.	Sales engineers Programmers System administrators Services and support personnel
Implementing		
Deploying Avaya Breeze™	Deploy and configure Avaya Breeze™.	Services and support personnel System administrators
Deploying Zang-Enabled Avaya Breeze™	Deploy and configure Zang-enabled Avaya Breeze™.	Services and support personnel System administrators
Upgrading Avaya Breeze™	Upgrade Avaya Breeze™.	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™ SDK	Deploy and configure the Eclipse IDE, Apache Maven, and the Avaya Breeze™ SDK.	Programmers
Avaya Breeze™ Snap-in Development Guide	Understand the key concepts needed to develop the different types of Avaya Breeze™ snap-ins.	Programmers
Avaya Breeze™ FAQ and Troubleshooting for Snap-in Developers	Troubleshoot Avaya Breeze™.	Programmers
Avaya Breeze™ API Javadocs	Understand API classes and uses.	Programmers
Supporting		
Maintaining and Troubleshooting Avaya Breeze™	Troubleshoot Avaya Breeze™.	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™ snap-in service, specifically the HelloWorld call-intercept snap-in.	Programmers System administrators
Administering Avaya Breeze™	Administer Avaya Breeze™ 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. Navigate to http://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**.

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
20970W	Introducing Avaya Device Adapter

Avaya Breeze™ videos

Avaya Breeze™ 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™ SDK: Windows	Programmers
Getting Started with the Avaya Breeze™ 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
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

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

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™ API, SDK, sample applications, developer-oriented technical documentation, and training materials.

Related links

Using the Avaya InSite Knowledge Base on page 101

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation

- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product Specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Related links

Support on page 101

Appendix A: Removing obsolete Avaya Aura® Media Server configuration

Checklist for removing obsolete Avaya Aura® Media Server configuration in System Manager

No.	Task	Reference	✔
1	Remove the Avaya Aura® Media Server Routing Pattern.	Removing the Avaya Aura Media Server Routing Pattern on page 103	
2	Remove the SIP Entity Links for Avaya Aura® Media Server.	Removing the SIP Entity Links for Avaya Aura Media Server on page 104	
3	Remove the SIP Entities for each Avaya Aura® Media Server.	Removing the SIP Entity for each Avaya Aura Media Server on page 104	
4	Remove the Avaya Aura® Media Server Host Name Resolution.	Removing the Avaya Aura Media Server Host Name Resolution on page 104	

Removing the Avaya Aura® Media Server Routing Pattern

Procedure

1. On System Manager, click **Elements** > **Routing** > **Routing Policies**.
2. Select the Routing Pattern created for Avaya Aura® Media Server.
3. Click **Delete**.
4. In the navigation pane, click **Regular Expressions**.
5. Select the Regular Expression created for Avaya Aura® Media Server.
6. Click **Delete**.

Removing the SIP Entity Links for Avaya Aura® Media Server

Procedure

1. On System Manager, click **Elements** > **Routing** > **Entity Links**.
2. Select the Entity Link created for Avaya Aura® Media Server.
3. Click **Delete**.

Removing the SIP Entity for each Avaya Aura® Media Server

Procedure

1. On System Manager, click **Elements** > **Routing** > **SIP Entities**.
2. Select the SIP Entity created for each Avaya Aura® Media Server.
3. Click **Delete**.

Removing the Avaya Aura® Media Server Host Name Resolution

Procedure

1. On System Manager, click **Elements** > **Session Manager** > **Network Configuration** > **Local Host Name Resolution**.
2. Select the FQDN Host Name created for Avaya Aura® Media Server.
3. Click **Delete**.

Index

A

AAMS support 7
accepting new service 55, 70, 89
active cluster database server
    identifying 76
    upgrade sequence 76
adding Avaya Breeze server 44
adding nodes 44
analyze inventory
    SDM 65, 83
applications
    preupgrade check 66, 83
assigning
    media server 20
automatic restart
    virtual machine 42, 43
Avaya Aura Media Server selection algorithm 9

C

checklist
    SDM 62, 80
cluster
    accepting new service 55
    attributes 45
    denying service 21
    verify activity 22
cluster database servers
    identifying 94
cluster editor
    field descriptions 46
cluster IP 45
clusters
    field description 46
committing upgrade 69, 88
Communication Manager support 7
configuring
    VM automatic restart 42, 43
craft account 7
Creating multiple privileged user accounts 44
customer account 7
customer configuration information
    ISO requirements 59, 76
    locating 15

D

deny service 21, 61, 78
deploying using SDM 40
deploying using vSphere client 23
Deploying using web-based client 28
downloading software 59, 77

E

EASG 92
    certificate information 92
    disabling 92
    enabling 92
    site certificates 93
EASG site certificate 93
elements
    refresh 65, 82
Enhanced Access Security Gateway 92
Enrollment Password status 21, 61, 78
entity link
    verification 55, 71, 90
entity links 104

F

field descriptions, cluster editor 46

H

Host Name Resolution 104
HTTP traffic 45

I

idle cluster database server
    identifying 76
    upgrade sequence 76
InSite Knowledge Base 101
inventory
    refresh elements 65, 82
ISO upgrade 56, 73

L

latest software patches 8
licensing upgrades 8
load balancing 45

M

maintenance tests
    on-demand 44, 70, 89
memory reservation 11
    increasing 11
multiple user accounts
    configure 44
    create 44

N

new cluster
  field description 46

O

OVA deployment
  without vCenter 33
  with SDM 40
  with vCenter 23
  with VMware vSphere client connected to ESXi host ...33
  with VMware vSphere web client 28
OVA upgrade 11

P

password restriction 8
patch command options 96
patch information 8
patching the server 95
permissions 7
PLDS 8, 11, 56, 73
  downloading software 20, 59, 77
preferred version 54, 72, 91
preupgrade check
  applications 66, 83
Preupgrade Configuration 66, 83

R

refresh elements in inventory 65, 82
refreshing host 64, 82
release notes 101
release notes for latest software patches 8
removing Avaya Breeze server 22
removing nodes 22
removing obsolete Avaya Aura Media Server configuration
....103
replication status verification 45, 69, 88
REST 19
routing pattern 103

S

SDM OVA deployment 40
secure grid
  disabling 60, 78
server
  accepting new service 70, 89
  denying service 61, 78
  iso file upgrade command 62, 79
  verify activity 61, 79
servers
  shutdown 23
service impact 11
service packs 101
service profiles 54, 72, 91
Session Manager support 7
shut down servers 23
SIP entity 104
SMGR_DEFAULT_LOCAL 63, 80
snap-ins
  installing new 54, 71, 90
software patches 8
Solution Deployment Manager 62, 65, 79, 83
Solution Deployment Manager client 86
standby cluster database server
  identifying 76
  upgrade sequence 76
status
  Enrollment Password 21, 61, 78
  server 45, 70, 89
support 101
System Manager license upgrade 8
System Manager support 7

T

training 100
trust connection 64, 81

U

upgrade 10
  OVA 10
  SDM 67, 84
upgrade checklist 11, 56, 73
upgrade command 62, 79
upgrade requirements 7
upgrade sequence with ISO upgrades 76
upgrade status check 45, 70, 89

V

verification
  entity link 55, 71, 90
  replication status 45, 69, 88
  server upgrade status 45, 70, 89
verify activity 61, 79
version_edp 64, 81
videos 100
virtual machine
  automatic restart 42, 43
vSphere client connect to ESXi host OVA deployment 33
vSphere client OVA deployment 23
vSphere web client OVA deployment 28