Administering 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 ... 10
Purpose ... 10
Chapter 2: Overview ... 11
Avaya Breeze™ overview ... 11
Chapter 3: Cluster Administration ... 13
Cluster Administration ... 13
Creating a new cluster ... 13
Editing clusters ... 15
Deleting clusters ... 17
Rebooting a cluster ... 17
Assigning an Avaya Breeze™ server to a cluster ... 18
Removing an Avaya Breeze™ server from a cluster ... 19
Installing a snap-in on a cluster ... 21
Uninstalling a snap-in from a cluster ... 22
HTTP load balancing in an Avaya Breeze™ cluster ... 23
Enabling HTTP load balancing in an Avaya Breeze™ cluster ... 24
Enabling Cluster Database on a cluster ... 25
Adding a Trust Certificate to all Avaya Breeze™ servers in a cluster ... 25
Backing up a cluster ... 26
Restoring a cluster ... 27
Cancelling a pending job ... 28
Purging a backup ... 28
Chapter 4: Service Management ... 29
Services ... 29
Snap-in deployment checklists ... 29
Loading the snap-in ... 32
Configure service attributes ... 33
Installing the snap-in ... 35
Service Profiles ... 37
Application Sequences and implicit sequencing ... 40
Testing a call-intercept snap-in ... 41
Testing a non-call-intercept snap-in ... 41
Creating a routing policy ... 41
Creating a dial pattern ... 42
Assigning a service profile to an implicit user pattern ... 43
Starting a snap-in ... 43
Stopping a snap-in ... 44
Uninstalling a snap-in ... 44
Deleting a snap-in ... 45

Bundles ... 45
Loading a bundle ... 46
Installing the bundle ... 46
Uninstalling a bundle ... 47
Deleting the Bundle ... 47
Service Databases ... 48
Deleting a service database ... 48
Chapter 5: User Administration ... 49
Administering implicit sequencing for Avaya Breeze™ ... 49
Assign a Service Profile to a user or Implicit User Pattern ... 51
Assigning a Service Profile to implicit users ... 51
Creating a new administered user ... 52
Assigning a service profile to an administered user ... 53
Chapter 6: Reliable Eventing administration ... 54
Creating a Reliable Eventing group ... 54
Editing a Reliable Eventing group ... 55
Deleting a Reliable Eventing group ... 56
Viewing the status of Reliable Eventing destinations ... 56
Deleting a Reliable Eventing destination ... 56
Running a maintenance test for a broker ... 57
Chapter 7: Authorization Service ... 58
Authorization Resources ... 58
Viewing Authorized clients authorized by a Resource server ... 58
Configuring features for a Resource server ... 59
Authorization Clients ... 59
Avaya Breeze™ Authorization Client ... 59
External Authorization Client ... 60
End User Authentication ... 61
User login experience ... 61
LDAP Authentication ... 62
SAML authentication ... 64
Changing the authentication mechanism ... 66
Chapter 8: HTTP Security Administration ... 68
Administering HTTP Security ... 68
Administering a whitelist for HTTP Security ... 68
Administering client certificate challenge for HTTPS ... 68
Administering HTTP CORS security ... 69
Chapter 9: JDBC Resource Administration ... 70
JDBC Resource administration ... 70
JDBC resource providers and data source ... 70
Administering JDBC providers ... 70
Administering JDBC data source ... 72
Sample configuration for database providers ... 74

Chapter 10: Service Ports ... 76
Assigning service ports for Avaya-developed snap-ins ... 76
Chapter 11: Geo Redundancy ... 78
Avaya Breeze™ with System Manager Geographic Redundancy ... 78
Terminology ... 78
Managing Avaya Breeze™ in a Geographic Redundancy solution ... 79
Performing system verification tests ... 84
Chapter 12: Security ... 85
Generating a private key ... 85
Generating a certificate signing request (CSR) ... 86
Replacing a System Manager signed identity certificate with Cluster IP/FQDN ... 87
Chapter 13: User Interface description ... 89
Attribute Configuration field descriptions ... 89
Authorization Configuration field descriptions ... 91
New External Authorization Client field descriptions ... 91
Edit Grants for Authorization Client field descriptions ... 92
Create Grant for Authorization Client field descriptions ... 92
Resources servers tab ... 92
View Authorized Clients of Resource Server field descriptions ... 93
Configure features field descriptions ... 93
Service instances tab ... 93
Edit Keys for Authorization Service field descriptions ... 93
Authentication Instance tab ... 94
Avaya Breeze™ Instance Editor field descriptions ... 94
Avaya Breeze™ Instance Status field descriptions ... 95
Backup and Restore field descriptions ... 96
Backup and Restore Status field descriptions ... 96
Backup Storage Configuration field descriptions ... 97
Bundles field descriptions ... 97
Bundle Details and Installation Status ... 100
Services in Bundle and Dependencies Table field descriptions ... 100
Installation Status field descriptions ... 101
Cluster administration field descriptions ... 101
Cluster DB Backup field descriptions ... 107
Cluster Editor field descriptions ... 108
Destination Status field descriptions ... 116
Event catalog configuration field descriptions ... 116
Event Catalog Editor field descriptions ... 117
HTTP Security field descriptions ... 118
Implicit User Profiles field descriptions ... 119
Implicit User Profile Rule Editor field descriptions ... 120
Install Trusted Certificate field descriptions ... 121
JDBC provider field descriptions ... 121

JDBC Provider Editor field descriptions.... 121
JDBC data source field descriptions.... 122
JDBC Data Source Editor field descriptions.... 123
Maintenance Tests field descriptions.... 123
Media Server Monitoring field descriptions.... 124
Reliable Eventing Groups field descriptions.... 125
Reliable Eventing Group Editor field descriptions.... 126
Server Administration field descriptions.... 126
Services field descriptions.... 129
Service Databases field descriptions.... 132
Service Ports field descriptions.... 132
Service Profile Configuration field descriptions.... 134
Service Profile Editor field descriptions.... 134
Service Status field descriptions.... 135
SNMP MIB Download field descriptions.... 136
System Resource Monitoring field descriptions.... 136
Chapter 14: Deployment Procedures.... 138
Deployment procedures overview.... 138
Adding a Trust Certificate to all Avaya Breeze™ servers in a cluster.... 138
Administering an Avaya Breeze™ instance.... 139
Administering Avaya Aura® Media Server URI.... 140
Chapter 15: Maintenance Procedures.... 141
Maintenance procedures overview.... 141
Modifying the logging configuration.... 141
Downloading and using the Breeze SNMP MIB.... 142
Running maintenance tests.... 142
Viewing the current usage of a cluster.... 143
Viewing the peak usage of a cluster.... 143
Resetting the peak usage of a cluster.... 143
Chapter 16: Certificate management.... 145
Overview.... 145
Identity Certificates.... 147
Certificates issued by System Manager.... 149
Demo certificates.... 150
Determining whether you are using a demo identity certificate.... 150
Viewing Identity Certificates.... 150
Replacing an Identify Certificate with an System Manager CA issued certificate.... 151
Replacing an Identify Certificate by a third party CA issued certificate.... 152
Activating a new Identity Certificate.... 153
Certificate Signing Request (CSR) generation.... 153
CSR and Private Key generation via OpenSSL.... 154
Bundle the Identity Certificate and Private Key into a PKCS #12 container.... 156
Identity Certificates lifecycle.... 157

Security Module SIP identity certificate attributes..... 157
Security Module HTTP identity certificate attributes..... 158
Management and SPIRIT identity certificates attributes..... 159
Replacing an Identity Certificate issued by System Manager CA..... 160
Replacing an Identity Certificate issued by a third party CA..... 161
Obtaining new SIP Identity Certificate through Certificate Signing Request (CSR)..... 161
Obtaining SIP Identity Certificate through PKCS#12 container..... 162
Trust management..... 162
Viewing trusted CA certificates..... 163
Adding trusted CA certificates..... 164
Removing trusted CA certificates..... 165
Exporting Avaya Breeze™ certificate..... 165
Exporting System Manager root CA certificate..... 165
Peer Certificate Validation..... 166
Certificate validations for System Manager connection..... 166
Certificate validations for SIP TLS connections..... 166
Certificate Revocation Management..... 168
Troubleshooting Certificates issues..... 168
Chapter 17: Resources..... 169
Documentation..... 169
Finding documents on the Avaya Support website..... 171
Training..... 172
Avaya Breeze™ videos..... 172
Viewing Avaya Mentor videos..... 172
Support..... 173
Using the Avaya InSite Knowledge Base..... 173
Appendix A: CLI commands..... 175
CEnetSetup or AvayaNetSetup..... 175
custAccounts..... 178
check_breeze_status.sh..... 178
Appendix B: Configuring an LDAP provider and SAML provider..... 183
Configuring LDAP provider..... 183
Apache Directory Studio Configuration..... 183
Active Directory Configuration..... 195
Open LDAP configuration..... 214
Configuration of ADFS as an SAML provider..... 217
Configuration of Service Provider on Active Directory Federation Services..... 218
Configuration of the IdP of Active Directory Federation Services on System Manager..... 220
Enabling SAML profile..... 221
Testing the setup..... 221

Chapter 1: Introduction

Purpose

This document describes the procedures for administering Avaya Breeze™ and for installing and administering snap-ins running on Avaya Breeze™.

The Avaya Breeze™ provides a virtualized and secure application platform where Java programmers can develop and dynamically deploy advanced engagement capabilities that extend the power of Avaya Aura®. Avaya Breeze™ is also the platform where you can run Avaya snap-ins like Context Store, Engagement Designer, and Work Assignment.

Snap-in or service is the term used to describe a dynamically deployable component that delivers all or part of this functionality. Some functionality is provided by a group of services. Customers, business partners, and Independent Software Vendors (ISVs) can use the platform as the deployment vehicle for their applications (services).

Important:

This document assumes that you have installed and configured Avaya Breeze™. For administration tasks required to set up Avaya Breeze™, see *Deploying Avaya Breeze™*.

Chapter 2: Overview

Avaya Breeze™ overview

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

Avaya Breeze™ platform is for Avaya products, such as Avaya Oceana™ Solution, Presence Services, Engagement Designer, and Context Store. It enables the user to do the following:

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

Avaya Breeze™ provides:

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

Multiple SMS snap-ins are available in the Avaya Snapp Store at http://snappstore.avaya.com/.

- Zang call connector to interact with Zang.
- Zang SMS connector for snap-ins to interact with Zang to send and receive messages.
- Tools that log and monitor operations and provide troubleshooting support.
- High availability. For information about high availability, see “High Availability”.

Chapter 3: Cluster Administration

Cluster Administration

Creating a new cluster

Before you begin

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

About this task

Use the Cluster Editor page to:

- Select a cluster profile.
- Configure the cluster attributes.
- Add Avaya Breeze™ servers to a cluster.
- Install snap-ins on a cluster.
- Subscribe to Reliable Eventing groups that are already created.

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

Procedure

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

   Note:

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

   For example, select the general purpose cluster profile or a product specific cluster profile. Use the **Context Store** profile for the Context Store snap-in, **Work Assignment** profile for the Work Assignment snap-ins, **Customer Engagement** profile for Avaya Oceana™ Solution, **Core Platform** profile for Presence Services, **General Purpose Large** profile for the Engagement Call Control snap-in and the **General Purpose** profile for other snap-ins.

   Refer to the snap-in reference documentation for the cluster profile appropriate for the use case being deployed.

4. Enter the cluster attributes for your cluster. You can edit the default cluster attributes the system displays.

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

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

   Note:

   Do not assign a **Cluster IP** for a single-node cluster.

5. If you will be installing snap-ins that use the cluster database, check **Enable Cluster Database**.

   Note:

   If you attempt to install a snap-in using the cluster database on a cluster that has the **Enable Cluster Database** feature disabled, the installation will be blocked.

6. In the **Minimum TLS Version for SIP Call Traffic** field, specify the TLS version which will be used for SIP calls intercepting Avaya Breeze™.
7. In the **Minimum TLS Version for Non-SIP Call Traffic** field, specify the TLS version which will be applied for HTTP requests to Avaya Breeze™.
8. (Optional) Click the **Servers** tab to assign Avaya Breeze™ servers to the cluster.

   Important:

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

   For more information on upgrading clusters, see *Upgrading Avaya Breeze™*.

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

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

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

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

   Avaya recommends using TLS v1.2.

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

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

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

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

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

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

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

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

    Note:

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

Editing clusters

About this task

Use the Edit Cluster page to:

- Configure cluster attributes.
- Assign or remove one or more Avaya Breeze™ servers to the cluster.
- Assign or remove snap-ins to the cluster.
- Edit Reliable Eventing groups associated with the cluster.

Note:

This procedure is service impacting.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Cluster Administration**.
3. Select the targeted cluster, and click **Cluster State**.
   a. Click **Deny New Service**.
   b. Click **Continue** when prompted.

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

4. Select the cluster, and click **Edit**.

   Note:

   You cannot modify the cluster attributes that are greyed out.

5. On the Edit Cluster page, edit the cluster attributes.
6. Click the **Servers** tab, and do one of the following:
   - To add Avaya Breeze™ servers, select the Avaya Breeze™ servers you want to add to the cluster.
   - To remove Avaya Breeze™ servers and to move the servers to the unassigned pool, clear the Avaya Breeze™ servers from the selected list.

   Note:

   The action of adding one or more nodes to a cluster or removing one or more nodes from the cluster will restart both the node being added or removed from the cluster and the remaining nodes in the cluster. Therefore, a service outage for this cluster should be expected.

7. **(Optional)** Click the **Services** tab, and select the snap-ins that you want to assign to the cluster.
8. **(Optional)** To remove an existing snap-in from the cluster, click **Uninstall** to uninstall the snap-in or **Force Uninstall** to force uninstall the snap-in.

   The snap-in moves to the available services pool. However, force uninstall brings down active sessions that access the snap-in.

9. **(Optional)** Click the **Reliable Eventing Groups** tab to add Reliable Eventing Groups to the cluster.
   a. In the **Available Reliable Eventing Groups** table, click the plus sign (**+**) adjacent to a group.
   b. In the **Subscribed Reliable Eventing Groups** table, click the cross sign (**X**) to remove a group.
10. Click **Commit** to save the changes.

    The system displays the appropriate error message

11. Confirm the warnings presented.
12. Wait until all services have been installed successfully.
13. Select the targeted cluster, click **Cluster State**, and do the following:
    a. Click **Accept New Service**.
    b. Click **Continue** when prompted.

Deleting clusters

Before you begin

Place the cluster in Deny New Service state before you delete the cluster.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Cluster Administration**.
3. On the Cluster Administration page, select the cluster or clusters that you want to delete.
4. Click **Delete**.
5. Click **Continue** when prompted.

   When you delete a cluster, the Avaya Breeze™ instances assigned to the cluster are automatically removed from the cluster. The services assigned to the cluster are automatically uninstalled from the servers of the cluster.

Rebooting a cluster

About this task

Avaya Breeze™ restarts all nodes in server clusters simultaneously when you restart clusters. You can view the progress of the cluster restart operation in the Last reboot status column on the Server Administration page of the System Manager web console.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Cluster Administration**.
3. Select the cluster, and click **Cluster State** > **Deny New Service**.
4. When the system prompts, click **Continue**.
5. Select the cluster, and click **Reboot**.
6. Click **Continue** when the system prompts.

   The system reboots the cluster.

   After performing reboot operation on cluster, Database Auto Switchover gets disabled. After placing the cluster into **Accept New Service** state, the Database Auto Switchover gets enabled again.

   You can view the reboot status in the **Last Reboot Status** column of Cluster Administration.

Assigning an Avaya Breeze™ server to a cluster

About this task

Use this procedure to assign an Avaya Breeze™ server to a cluster. Note that assigning a server to a cluster is service affecting.

You can add upto five servers to a cluster.

Core Platform cluster profile alone supports up to 10 servers in a cluster.

Even when one of the assigned servers is not reachable by System Manager, you cannot edit any tab on the Cluster Administration page.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Cluster Administration**.
3. Select the targeted cluster, and click **Cluster State**.
   a. Click **Deny New Service**.
   b. Click **Continue** when prompted.

   You can add a server to the cluster only if all reachable nodes in the cluster are in the **Deny New Service** mode.
4. Select the cluster, and click **Edit**.
5. Click the **Servers** tab.
6. In the **Unassigned Servers** table, click the plus sign (**+**) next to the **Name** column to add the Avaya Breeze™ server to your cluster.

   Note:

   The action of adding one or more servers to a cluster will restart both the servers being added to the cluster and the remaining nodes in the cluster. Therefore, a service outage for this cluster should be expected.
7. Click **Commit**.

   Note:

   If you add a server to a single sever cluster, it affects service as WebSphere restarts to update the data grid properties. However, if you add a server to a cluster that has two or more servers, it does not affect service.
8. Confirm the warnings presented.
9. Wait until all services have been installed successfully.
10. Select the targeted cluster and click **Cluster State**.
    a. Click **Accept New Service**.

b. Click **Continue** when prompted.

Removing an Avaya Breeze™ server from a cluster

About this task

Use this procedure to remove an Avaya Breeze™ server from a cluster. Note that this procedure is service impacting.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Cluster Administration**.
3. Select the targeted cluster and click **Cluster State**.
   a. Click **Deny New Service**.
   b. Click **Continue** when prompted.

   You can remove a server from the cluster only if all reachable nodes in the cluster are in the **Deny New Service** mode.
4. Select the cluster, and click **Edit**.
5. On the Cluster Editor page, click the **Servers** tab.
6. In the **Assigned Servers** table, click the cross sign (**x**) next to the **Name** column .

   Note:

   The action of removing one or more servers from the cluster will restart both the servers being removed from the cluster and the remaining servers in the cluster. Therefore, a service outage for this cluster should be expected.
7. Click **Commit** to delete the server from the cluster you selected.

   Note:

   When you remove either the primary or the secondary Lookup server from a cluster, all the other servers in the cluster restart due to the configuration change. The system displays the Lookup server icon against the Lookup server on the **Server Administration** and **Cluster Administration** pages.
8. Confirm the warnings presented.
9. Wait until all services have been installed successfully.
10. Select the targeted cluster, and click **Cluster State**.
    a. Click **Accept New Service**.
    b. Click **Continue** when prompted.

Related links

Validations when removing a server from a cluster on page 20

Validations when removing a server from a cluster

You cannot delete an Avaya Breeze™ server from a cluster if:

- The minimum number of servers are not available in the Accept New Service state.
- The Avaya Breeze™ server is not in the Deny New Service state.
- The server is functioning as a load balancing server or as a lookup server, and you do not have another available server to take over.
- The cluster is associated with a reliable eventing group.

Additional validations when Cluster Database is enabled

The following are the validations when you want to remove a server from a cluster without auto switch over:

- You must manually switch over the active server to a standby server, or make an idle server a Standby, or both before removing servers.
- In a cluster with a single server you can remove the server provided the server is in the Deny New Service state.
- In a cluster with two servers, you can remove the standby or both the servers without any validation. If you want to remove the active server, you must manually switch over the active with the standby before you remove the current active server.
- In a cluster with three or more servers, you can remove a server if the server is in the Idle mode. If the server is an active server or a standby server, the action is blocked.

  If you want to remove the standby server, perform a manual switch over with the Idle server before you remove the server. If you want to remove the active server, perform a manual switch over with the standby before you remove the server.

Related links

Removing an Avaya Breeze server from a cluster on page 19
Performing manual switch over from active server to standby server on page 20
Converting an idle server to the standby server on page 21
Performing manual switch over from active server to standby server on page 20
Converting an idle server to the standby server on page 21

Performing manual switch over from active server to standby server

Before you begin

1. Ensure that the cluster contains two or more servers.
2. Perform this procedure only when the standby server is ready.

Procedure

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

2. Click **Cluster Administration**.
3. Click **show**.
4. On the **Cluster Database** column, click one of the following:
   - **Active**: To convert an active server to standby server.
   - **Standby**: To convert a standby server to an active server.
5. Click **Continue**.

Related links

Validations when removing a server from a cluster on page 20
Performing manual switch over from active server to standby server on page 20
Converting an idle server to the standby server on page 21

Converting an idle server to the standby server

About this task

Perform this procedure only when the cluster contains three or more servers.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. Click **Cluster Administration**.
3. Click **show**.
4. On the **Cluster Database** column, click **Idle**.

   This setting will convert the idle server to a standby server and will convert the existing standby server to an idle server.
5. Click **Continue**.

Related links

Validations when removing a server from a cluster on page 20

Installing a snap-in on a cluster

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Cluster Administration**.
3. On the Cluster Administration page, select a cluster and click **Edit**.
4. Click the **Services** tab.
5. From the **Available Services** table, click the **+** sign next to the **Name** column to add the snap-in to the cluster.

6. In the **Select TLS Version for Selected Snap-in** field, select the TLS version of the snap-in.
   - **Default**
   - **TLSv1.0**
   - **TLSv1.2**

   If you select **Default**, Avaya Breeze™ uses the value of the **Minimum TLS Version** field set in System Manager global configuration.
7. Click **Commit** to install the snap-in to the cluster.

   For every cluster type there is a set of required snap-ins that must be loaded so that they can be automatically installed on the cluster. If one or more of the required snap-ins is not loaded, the system displays a warning message. You cannot create or edit the cluster successfully.

   In a closed cluster, you cannot install snap-ins that are not part of the optional or mandatory snap-in list.

   If the snap-in being installed requires cluster database, a warning message is displayed that you must enable **Cluster Database** before the snap-in is installed. For more information, see “Enabling Cluster Database”.

Uninstalling a snap-in from a cluster

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Cluster Administration**.
3. On the Cluster Administration page, select the cluster from which you want to uninstall the snap-in.
4. Click **Edit**.
5. On the Cluster Editor page, click the **Services** tab.
6. From the **Assigned Services** tab, do one of the following:
   - Click **Uninstall** for the snap-ins that you want to uninstall.
   - Click **Force Uninstall** for the snap-ins that you want to force uninstall. When you click **Force Uninstall**, the snap-ins are immediately uninstalled and the system does not wait for the snap-in activities to complete.
   - Select **Do you want to delete the database?** check box to delete the snap-in database.
7. Click **Commit** to uninstall the snap-in from the cluster.

   You cannot uninstall a required snap-in from a cluster unless another version of the snap-in is installed in the cluster.

You can choose to uninstall a snap-in from specific clusters while retaining the snap-in in other clusters.

HTTP load balancing in an Avaya Breeze™ cluster

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

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

Name	Description
HTTP Load Balancer backend server max failure response timeout period (seconds)	The maximum timeout period of the failure response of the HTTP Load Balancer backend server. The default value is 15.
Max number of failure responses from HTTP Load Balancer backend server	The maximum number of failure responses from the HTTP Load Balancer backend server. The default value is 2.
Network connection timeout to HTTP Load Balancer backend server (seconds)	The network connection timeout period from the HTTP Load Balancer backend server. The default value is 10.

Load balancing validations

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

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

Session affinity

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

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

Use the Trusted addresses for converting to use X-Real-IP for session affinity cluster attribute to enter trusted addresses that are known to send correct replacement addresses so thatAvaya Breeze™ load balancer can use the real client IP when an HTTP request traverses through reverse

proxies like Avaya Session Border Controller for Enterprise. The header which is used to identify the real client IP address is X-Real-IP

Enabling HTTP load balancing in an Avaya Breeze™ cluster

About this task

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

Before you begin

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

Procedure

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

   If the **Is Load Balancer enabled** check box is selected and the load balancer node in the cluster is in the Accepting state, the **Cluster State** field displays **Accepting**. If the **Is Load Balancer enabled** check box is cleared and at least one of the node in the cluster is in the Accepting state, the **Cluster State** field displays **Accepting**. discuss
5. In the Basic section **Cluster IP** field, type the IP address of the cluster.

   The **Cluster IP** address used for load balancing must be unique. It must not match the Security Module IP address or the management IP address. The Security Module IP address must be on the same subnet as the Avaya Breeze™ **Cluster IP** address.
6. Click **Commit**.

   Two Avaya Breeze™ servers are automatically designated as active and standby to perform the load balancing functionality.

7. On the Cluster Administration page, in the **Cluster State** field, select **Accept New Service**.

Enabling Cluster Database on a cluster

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 edit, and click **Cluster State** > **Deny New Service**.
4. Click **Continue**.
5. Click **Edit**.
6. In the General tab, select the **Enable Cluster Database** check box.
7. Leave the **Enable Database Auto Switchover** field at the default setting, unless you want to manually control when a failover must occur.

   Cluster Database is disabled by default

   `Cluster Database requires at least 8 GB of memory. Check the Snap-in documentation for disk allocation recommendations when using Cluster Database to avoid possible service disruptions.`
8. Click **Commit**.
9. Select the cluster, and click **Cluster State** > **Accept New Service**.
10. Click **Continue**.

Adding a Trust Certificate to all Avaya Breeze™ servers in a cluster

Before you begin

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

Procedure

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

   Note:

   The Trust Certificate that you are about to add will apply to all the Avaya Breeze™ servers assigned to the cluster.

4. From the **Select Store Type to install trusted certificate** menu, select the appropriate store type.
5. Click **Browse** to the location of your Trust Certificate, and select the certificate.
6. Click **Retrieve Certificate**, and review the details of the Trusted Certificate.
7. Click **Commit** .

Related links

Store types of the trusted certificates on page 26

Store types of the trusted certificates

Store Type/Interface/ Service	Common Name	Connected peer party	Usage/Function
Security Module SIP	securitymodule_sip	Session Manager	SIP link
Management	smmgmt	System Manager	Data replication and other management information. The Avaya Breeze™ management link that communicates with System Manager.
SPIRIT	spiritalias	SAL server on System Manager	SAL
Security Module HTTPS	securitymodule_http	HTTPS interface to external HTTPS clients or servers	HTTPS
WebSphere	websphere	SECMOD, WebSphere	—
CLUSTER_DB	cdb	Snap-ins that connect to cluster database	Secured connection to the cluster database.
AUTHORIZATION_SERVICE	default	Not applicable	Validation of access tokens.

Backing up a cluster

About this task

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

You can backup on one cluster and restore on another.

Note:

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

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Cluster Administration**.
2. Click **Backup and Restore** > **Configure**.
3. Enter the backup server details.
4. Click **Test Connection** to verify the connection of the backup server.
5. Click **Commit**.
6. Select the cluster that you want to backup, and click **Backup and Restore** > **Backup**.

   The system displays the Cluster DB Backup page.
7. In the **Backup** section, select the services to back up.
8. In the **Job schedule** section, enter the following details:
   - In the **Backup password** field, enter a password.
   - In the **Schedule Job** field, select **Run immediately** or **Schedule later**.

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

Restoring a cluster

About this task

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

Note:

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

Before you begin

Cluster database must be enabled.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Cluster Administration**.
2. Click **Backup and Restore** > **Restore**.

   The system lists the backup and restore jobs.

3. Select a completed backup, and click **Restore**.
4. Select the cluster on which you want to restore the backup, and click **Continue**.

Cancelling a pending job

Procedure

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

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

Purging a backup

Before you begin

The backup to be purged must be complete.

Procedure

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

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

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

Chapter 4: Service Management

Services

Snap-in deployment checklists

The following are the types of Avaya Breeze™ snap-ins:

- Call-intercept snap-ins
- Callable snap-ins
- Other types of snap-ins:
  - Outbound calling snap-ins
  - HTTP-invoked snap-ins
  - Collaboration Bus-invoked snap-ins

Callable snap-ins are called directly by users rather than being called on behalf of the user who makes or receives a call.

Licensed snap-ins that are purchased separately from Avaya Breeze™ might require additional steps to deploy. For more information, see the snap-in documentation.

Note:

The terms snap-in and services used in this document mean the same. The term service is used to mean a snap-in, workflow or task in the “Bundles” section.

Call-intercept snap-in deployment checklist

No.	Task	Notes	Link/Reference	✔
1	Install the snap-in license.	This step applies only to Avaya-developed snap-ins that you purchase separately. Skip this step when installing a preloaded snap-in. Preloaded snap-ins are provided with Avaya Breeze™	See *Quick Start to deploying the HelloWorld Snap-in*.	

Table continues…

No.	Task	Notes	Link/Reference	✔
		Element Manager in System Manager.		
2	Load the snap-in.	Skip this step when installing a preloaded snap-in. Preloaded snap-ins are provided with Avaya Breeze™ Element Manager in System Manager.	Loading the snap-in on page 32	
3	Configure snap-in attributes.	—	Configuring snap-in attributes at the service profile level on page 33	
4	Install the snap-in.	—	Installing the snap-in on page 35	
5	Create a service profile.	—	Creating a Service Profile on page 37	
6	Assign service profile to users.	Skip this step if the service profile that contains your snap-in is already assigned to the users who want to receive the snap-in.	Assigning a service profile to an administered user on page 53	
7	Create an application and the application sequence.	Skip this step if you have an application sequence administered for Avaya Breeze™.	Application Sequences and implicit sequencing on page 40	
8	Administer implicit sequencing for a user or group of users.	Skip this step if you have administered implicit sequencing for Avaya Breeze™.	Administering implicit sequencing for Avaya Breeze on page 49	
9	Test the snap-in.	—	Testing a call-intercept snap-in on page 41	

Callable snap-in deployment checklist

No.	Task	Notes	Link	✔
1	Install the snap-in license.	This step applies only to Avaya-developed snap-ins that you purchase separately. Skip this step when installing a preloaded snap-in. Preloaded	See *Quick Start to deploying the HelloWorld Snap-in*.	

Table continues…

No.	Task	Notes	Link	✔
		snap-ins are provided with Avaya Breeze™ Element Manager in System Manager.		
2	Load the snap-in.	Skip this step when installing a preloaded snap-in. Preloaded snap-ins are provided with Avaya Breeze™ Element Manager in System Manager.	Loading the snap-in on page 32	
3	Install the snap-in.	—	Installing the snap-in on page 35	
4	Configure the snap-in attributes.	—	Configuring snap-in attributes at the service profile level on page 33	
5	Determine the dial string of the callable snap-in.	—	—	
6	Determine the pattern that includes the dial string and optionally includes other callable snap-in dial strings.	—	—	
7	Create the dial pattern that matches with the pattern specified in Step 6.	—	Creating a dial pattern on page 42	
8	Create a routing policy with the Avaya Breeze™ SIP Entity as the destination.	—	Creating a routing policy on page 41	
9	Create a service profile or add the snap-in to an existing service profile.	—	Service Profiles on page 37	
10	Create and assign the service profile to an implicit user pattern in Avaya Breeze™ that exactly matches the dial string determined in Step 5.	The implicit user pattern: • Must not match with any other callable snap-in or end user dial strings. • Must not be included in a Session Manager implicit user pattern.	Assigning a Service Profile to implicit users on page 51 Assigning a service profile to an implicit user pattern on page 43	

Other types of snap-ins deployment checklist

No.	Task	Notes	Link	✔
1	Install the snap-in license.	This step applies only to Avaya-developed snap-ins that you purchase separately. Skip this step when installing a preloaded snap-in. Preloaded snap-ins are provided with Avaya Breeze™ Element Manager in System Manager.	See *Quick Start to deploying the HelloWorld Snap-in*.	
2	Load the snap-in.	Skip this step when installing a preloaded snap-in. Preloaded snap-ins are provided with Avaya Breeze™ Element Manager in System Manager.	Loading the snap-in on page 32	
3	Install the snap-in.	—	Installing the snap-in on page 35	
4	Configure the snap-in attributes.	—	Configuring snap-in attributes at the service profile level on page 33	
5	Create a service profile or add the snap-in to an existing service profile.	Skip this step for snap-ins that do not require a service profile.	Service Profiles on page 37	

Loading the snap-in

About this task

This task describes how to load a snap-in to System Manager from your development environment or alternate location. You can skip this step when installing a pre-loaded snap-in. Pre-loaded snap-ins are provided with the Avaya Breeze™ Element Manager in System Manager. However, you can skip this step only if the pre-loaded snap-ins are not removed from System Manager by the administrator. If the pre-loaded snap-ins are removed, the administrator needs to reload the snap-in.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Service Management** > **Services**.
2. Click **LOAD**.

   You can load multiple snap-ins at a time.
3. On the Load Service page, depending on the browser used, click **Browse** or **Choose File**, and browse to your snap-in file location.

Note:

You can select up to 50 files or a maximum of 3 GB files whichever limit is reached first.

4. Browse and select the snap-in (`.svar`) file required, and then click **Open**.

   A snap-in file ends with `.svar`. For a snap-in that Avaya provides, the `.svar` file must be downloaded from PLDS.

5. On the Load Service page, click **LOAD**.
6. On the Accept End User License Agreement page, click **Accept** to accept the agreement.

   When the snap-in is loaded, the **Service Management** > **Services** page displays the **State** of the snap-in as **Loaded**.

   The system displays all the `.svar` files that you loaded in the All Services table on the **Service Management** > **Services** page.

Related links

Services field descriptions on page 129

Configure service attributes

There are four levels of service attributes: Service Profile, Service Cluster, Service Global, and Default. This order specifies the attribute level from the most specific level to the most generic. When an Avaya Breeze™ server is determining the attribute value to a snap-in, the server checks the value specified against the user's service profile. If no value has been specified, the server checks if an attribute value has been specified at the cluster level. Again if a value has not been specified, the server checks for the attribute value at the global level. If no value is found, the server uses the default attribute value.

Note:

The system displays different sets of attributes for services depending on the attribute scope set at the global, cluster, or user level. For more information, see *Avaya Breeze™ Snap-in Development Guide*.

Related links

Configuring snap-in attributes at the service profile level on page 33
Configuring snap-in attributes at the cluster level on page 34

Configuring snap-in attributes at the service profile level

Customize snap-ins for a specific group of users by assigning attributes to the snap-in in the Service Profile. You can assign attributes either as part of adding a snap-in to a Service Profile or at a later time.

Before you begin

Create or add a service profile and assign the required snap-in to the profile. For more information, see the topic *Creating a Service Profile*.

About this task

Use this task to configure values for attributes that will replace the default values assigned in the snap-in. Perform this task to configure attributes for a snap-in that is included in a Service Profile.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Configuration** > **Attributes**.
2. Click the **Service Profile** tab.
3. From the **Profile** field, select the Service Profile that contains the snap-in and the attributes that you want to configure.
4. From the **Service** field, select the snap-in in the Service Profile that contains the attributes you want to configure.

   The system displays all attributes that are configured at the service profile level for this snap-in.
5. For the attribute that you want to change:
   a. Click **Override Default**.
   b. Enter the new value or string in the **Effective Value** field.
6. Click **Commit** to save your changes.

Related links

Configure service attributes on page 33
Configuring snap-in attributes at the global level on page 35
Attribute Configuration field descriptions on page 89

Configuring snap-in attributes at the cluster level

Perform this procedure only after installing the snap-in.

About this task

Use this task to configure values for attributes that will replace the default values assigned in the snap-in. Perform this task to configure attributes for a snap-in when that snap-in is not included in a Service Profile, or when you want to assign the snap-in attributes at the cluster level.

For example, perform this task to configure attributes for email, conferencing (Scopia) and Zang SMS connector service.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Configuration** > **Attributes**.
2. Click the **Service Clusters** tab.
3. From the **Cluster** field, select the cluster to which you want to configure the snap-in attributes.

4. From the **Service** field, select the service to which you want to configure the snap-in attributes.

   The system displays all attributes that are configured at the cluster level for this snap-in.

5. For the attribute that you want to change:
   a. Click **Override Default**.
   b. Enter a new value or string in the **Effective Value** field.
6. Click **Commit** to save the changes.

Related links

Configure service attributes on page 33
Attribute Configuration field descriptions on page 89

Configuring snap-in attributes at the global level

About this task

Use this task to configure values for attributes that will replace the default values assigned in the snap-in. Perform this task to configure attributes for a snap-in when that snap-in is not included in a Service Profile, or when you want to assign the snap-in attributes at the global level.

For example, perform this task to configure attributes for email, conferencing (Scopia) and Zang SMS connector service.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Configuration** > **Attributes**.
2. Click the **Service Globals** tab.
3. From the **Service** drop-down menu, select the service that contains the service attributes you want to configure.

   The system displays all attributes that are configured at the global level for this snap-in.

4. For the attribute you want to change:
   a. Click **Override Default**.
   b. Enter the new value or string in the **Effective Value** field.
5. Click **Commit** to save your changes.

Related links

Attribute Configuration field descriptions on page 89

Installing the snap-in

About this task

Use this task to install the snap-in to a specific cluster(s).

Note:

For `.svar` files larger than 50 MB, schedule snap-in installation during a maintenance window.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Service Management** > **Services**.
2. Select the snap-in that you want to install.
3. Click **Install**.
4. Select the cluster(s) where you want the snap-in to reside, and click **Commit**.
5. 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 the 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 the servers.

   Note:

   Most of the snap-ins automatically start but a snap-in developer has provision to control starting/stopping snap-in.
6. To track the progress of a snap-in installation, on the Server Administration page, click the **Service Install Status** for an Avaya Breeze™ server.

   The Service Status page displays the installation status of all the snap-ins installed on that server.
7. **(Optional)** To designate a snap-in as the preferred version, do the following:
   a. Verify that the snap-in is in the installed state for the targeted cluster(s) by opening the System Manager web console, and clicking **Elements** > **Avaya Breeze** > **Service Management** > **Services**.
   b. From the **All Services** list, select the version of the snap-in you want to mark as Preferred.
   c. Click **Set Preferred Version**.
   d. Select the cluster(s) for which you want this to be the preferred version, and click **Commit**.

Related links

Services field descriptions on page 129
Avaya Breeze Instance Status field descriptions on page 95

Service Profiles

A Service Profile is an administered group of snap-ins, which will be invoked. Some snap-ins are associated with users while others are associated to a callable service.

You can have a Callable service and several Call Intercept services on the same cluster. All services can be placed in the same Service Profile, and the last service in the profile is treated as the Callable service. If a service profile has both Call Intercept services and a Callable service, you must configure a Route Pattern for the associated number, instead of configuring Session Manager Application Sequence.

You can associate a service profile on an individual user basis or scope the profile to a group of users through the Implicit User Profile association, where profile assignment is based on a range of extensions or numeric patterns.

- Use the Service Profile to link one or many Avaya Breeze™ snap-ins to a user or a group of users.

  Tailor the attributes of any snap-in in the Service Profile to the requirements of a specific group of users. For example, you could create one Service Profile for the entire sales department so they could enjoy the same Avaya Breeze™ snap-ins and attributes of those snap-ins. And then, create a different Service Profile for the finance department, with some of the same snap-ins, but with different attributes for the snap-ins.

  You can thus create a single Service Profile and assign the service profile to multiple users who require the same snap-ins, eliminating the need to administer these snap-ins individually for each user.

Use the Service Profile to link one or many Avaya Breeze™ snap-ins to a user or a group of users. You must include a snap-in in a Service Profile to associate it with users; users are associated with a Service Profile and not individual snap-ins.

Related links

Creating a Service Profile on page 37
Configuring service invocation for service profiles on page 38
Searching service profiles on page 39

Creating a Service Profile

About this task

Use this procedure to create a new Service Profile and add your snap-in to it. You can skip this procedure if you want to add the snap-in to an existing Service Profile or if your snap-in is not a call-intercept or callable service.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Configuration** > **Service Profiles**.
2. Click **New**.

3. Type a name for the Service Profile.
4. Select the **All Services** tab.
5. Select the snap-in and version to add to the profile.
   - To add the snap-in to the Service profile without selecting a version, in the **Available Service to Add to this Service Profile** list, click the **+** next to the snap-in. This selects the latest version of the snap-in.
   - To add the snap-in to the Service profile and select a specific version, do the following:
     a. In the list of **Available Service to Add to this Service Profile**, click **Advanced** next to the snap-in name.
     b. From the **Service Version** field, select the version of the snap-in to use in the Service Profile. Select from the following choices:
        - If you designated your snap-in as the Preferred Version at installation, select **Preferred** to use that version of the snap-in. If you later designate a different version of the snap-in as the Preferred Version, the Service Profile automatically uses the new Preferred Version.
        - Select **Latest** to always use the version of the snap-in with the latest version number.
        - Select a specific version number.
     c. Click **Add**.
6. To add another service to the same Service Profile repeat step 6.

   Note:

   If you have multiple services see *Administering Avaya Breeze™* for information on service invocation details.
7. Click **Commit** to save the Service Profile.

Related links

Service Profiles on page 37
Service Profile Configuration field descriptions on page 134

Configuring service invocation for service profiles

About this task

Use the **Service Invocation Details** tab to configure the calling and called service invocation order when you have more than one call-intercept service defined in the profile. You can have up to five call-intercept snap-ins assigned to a single service profile. To set the order of the call-intercept services, perform the following procedure.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **Service Profiles**.

3. Do one of the following:
   - Click **New**.
   - Click **Edit**.
4. On the Service Profile Editor page, complete the details of the service profile.
5. Click the **Service Invocation Details** tab. Based on the service you have added to your service profile, the appropriate call intercept services are listed in the **Calling Service Invocation Order** table and the **Called Service Invocation Order** table.
6. In the **Order: First to Last** column, click the arrows to move the services up or down in the invocation order of the call intercept services The order shown here defines the order that the snap-ins will be invoked by Avaya Breeze™ for calling or called user.
7. Click **Commit** to save the changes.

Related links

Service Profiles on page 37

Searching service profiles

About this task

Use the search bar on the Service Profile Configuration page to search service profiles. The search will bring all the results that contain the search string. You can search service profiles by using the search bar on various pages in System Manager.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **Service Profiles**.
3. On the Service Profile Configuration page, type your search string in the search bar.

   The system displays all the service profiles that contains your search string.
4. Hover your mouse over a service profile.

   The system displays a pop-up window with **Edit**, **Users**, and **Bulk Edit** options.
5. Click **Users** to view the list of users who have this Service Profile assigned to them.
6. Click **Edit** to edit the details of the service profile.
7. Click **Bulk Edit** to edit the Service Profile of the associated users for this Service Profile.

   The system displays the User Bulk Edit page, where you can edit the Service Profile of the associated users.

Related links

Service Profiles on page 37

Application Sequences and implicit sequencing

An Application Sequence is required in combination with implicit sequencing for call-intercept snap-ins to route calls for a specific user or group of users to Avaya Breeze™. In this way, calls to or from the user will invoke Avaya Breeze™ snap-ins based on their service profile.

An Application Sequence is required only for call-intercept snap-ins, that is, snap-ins that are invoked when a user receives or makes a call.

To set up the Application Sequence with implicit sequencing you must:

1. Add the target Avaya Breeze™ as an Application.
2. Add the Avaya Breeze™ Application to an Application Sequence.
3. Assign the Application Sequence to the implicit user (number or pattern) you want connected to Avaya Breeze™ snap-ins (administering implicit sequencing).

Creating an Application and Application Sequence

This procedure:

- Administers a target Avaya Breeze™ instance as an Application.
- Administers the Application as part of an Application Sequence. This only needs to be done once for each Avaya Breeze™ instance.

Procedure

1. Administer the target Avaya Breeze™ instance as an Application:
   a. On the System Manager, click **Elements** > **Session Manager** > **Application Configuration** > **Applications**.
   b. Click **New**.
   c. In the **Name** field, type a descriptive name for the Avaya Breeze™ instance.
   d. For the **SIP Entity**, select the Avaya Breeze™ where the service resides.

      For information about creating the SIP Entity, see *Deploying Avaya Breeze™*.
   e. To save your changes, click **Commit**.
2. Administer the Application as part of an Application Sequence:
   a. On the System Manager, click **Elements** > **Session Manager** > **Application Configuration** > **Application Sequences**.
   b. Click **New**.
   c. In the **Name** field, type a descriptive name for the Application Sequence.
   d. In the list of **Available Applications** click the **+** sign next to the Avaya Breeze™ Application that you created.
   e. If you don't want calls to fail when Avaya Breeze™ is not available, deselect the **Mandatory** check box if it is selected.

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

f. To save your Application Sequence, click **Commit**.

Testing a call-intercept snap-in

Before you begin

Verify that the SIP endpoints are registered to Session Manager before you attempt to make a call. For more information, see *Administering Avaya Aura® Session Manager*.

About this task

Testing a call-intercept snap-in can be as easy as calling from or to a user assigned to the Service Profile, and making sure you get the desired results.

Procedure

1. Make a call to or from the user you assigned to the Service Profile that contains the snap-in.
   - For a calling party snap-in, make the call from the user.
   - For a called party snap-in, make the call to the user.
2. Verify that the test call uses the new snap-in attributes you administered for the Service Profile.

Testing a non-call-intercept snap-in

Procedure

1. Test your snap-in by invoking it by whatever means is appropriate to the snap-in.

   For example, invoke your snap-in from an HTTP(S) URL.
2. Verify that the snap-in provides the expected functionality and that it is using the administered snap-in attributes.

   For troubleshooting help, see *Maintaining and Troubleshooting Avaya Breeze™* and *Avaya Breeze™ FAQ and Troubleshooting for Snap-in Developers*.

Creating a routing policy

About this task

Use this procedure to create a routing policy to an Avaya Breeze™ server or cluster. A routing policy to Avaya Breeze™ is necessary only when administering a callable service and is not appropriate for call-intercept services.

Procedure

1. On System Manager, click **Elements** > **Routing** > **Routing Policies**.
2. Click **New**.
3. In the **General** section, enter a routing policy name and notes in the relevant fields.
4. In the **Retries** field, enter the number of retries for the destination SIP entity.

   The default value in **Retries** field is `0`. The valid values are from 0 to 5.
5. Select the **Disabled** check box to disable the routing policy.
6. In the **SIP Entities as Destination** section, select **Avaya Breeze™**.
7. Select the Time of Day patterns that you want to associate with this routing pattern and click **Select**.
8. Enter the relative Rankings that you want to associate with each Time Range.

   Lower ranking values indicate higher priority.
9. In the **Dial Patterns and Regular Expressions** sections, click **Add** to associate existing Dial Patterns and Regular Expressions with the Routing Policy.
10. Click **Commit**.

Creating a dial pattern

About this task

Use this procedure to create a dial plan to an Avaya Breeze™ server or cluster. A dial plan to Avaya Breeze™ is necessary only when administering a callable service and is not appropriate for call-intercept services.

Procedure

1. On System Manager, click **Elements** > **Routing** > **Dial Patterns**.
2. Click **New**.
3. Enter the dial pattern.

   The system auto-populates the **Min** and **Max** fields.
4. In the **Originating Locations and Routing Policies** section, click **Add**.
5. In the **Originating Locations** section, select the required locations.
6. In the **Routing Policies** section, select the routing policy that we created earlier.
7. Click **Select**.
8. Click **Commit**.

Assigning a service profile to an implicit user pattern

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. Click **Configuration** > **Implicit User Profiles**.
3. Click **New**.
4. In the **Service Profile** field, select a service profile.
5. In the **Pattern** field, specify the pattern defined earlier.
6. Click **Commit**.

Starting a snap-in

About this task

The start snap-in functionality is required when you:

- Upgrade some snap-ins, specifically the Presence snap-in.
- Change some port assignments for snap-ins.
- Change the capacity of clusters.
- Change some configuration parameters of a snap-in. You must restart the snap-in for the configuration change to take effect.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Service Management** > **Services**.
3. On the Service Management page, select the snap-in that you want to start.
4. Click **Start**.

   Note:

   If the snap-in is already installed on all the servers, the **Start** button is disabled.
5. In the Confirm Start Service dialog box, select the cluster or clusters in which you want to start the snap-in.
6. Click **Start**.

   On the Service Management page, the **Service Install Status** changes to **Starting** and then **Installed**.

   Note:

   Restarting the Avaya Breeze™ server does not affect the snap-in install status.

Stopping a snap-in

About this task

The stop snap-in functionality is required when you:

- Upgrade some snap-ins, specifically the Presence snap-in.
- Change some port assignments for snap-ins.
- Change the capacity of clusters.
- Change some configuration parameters of a snap-in. You must restart the snap-in for the configuration change to take effect.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Service Management** > **Services**.
3. On the Service Management page, select the snap-in that you want to stop.
4. Click **Stop**.

   Note:

   If the snap-in is not in the **Installed** state, the Stop button is disabled.
5. In the Stop Service dialog box, select the cluster or clusters where you want to stop the snap-in.
6. Click **Stop**.

   The **Service Install Status** of the snap-in changes to **Stopping** and then **Stopped**.

Uninstalling a snap-in

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Service Management** > **Services**.
3. On the Service Management page, select the snap-in that you want to remove.
4. Click **Uninstall**.
5. From the Confirm Uninstall Service pop-up dialog box, select the cluster or clusters from which you want to remove the snap-in.

   Note:

   You cannot uninstall a required snap-in from a cluster unless another version of the required snap-in is already installed in the cluster.

The state of a snap-in as shown on the Service Management page is the aggregated status of the snap-in installation across clusters. If you uninstall a snap-in from a cluster, and if the snap-in is in the installed state in another cluster, the status continues to display as Installed.

6. If you want to forcefully remove the snap-in, select the **Force Uninstall** check box in the same pop-up dialog box.

   For a snap-in, the system displays the Call activity as part of the Activity counter on the Cluster Administration page. If you force uninstall the snap-in, the snap-in will be uninstalled immediately without waiting for the Activity counter to reach zero.

7. Select **Do you want to delete the database?** check box to delete the snap-in database.

   In a normal scenario the activity drains in about two hours and the Activity Link value comes to zero. This is when the snap-in is uninstalled.

Deleting a snap-in

About this task

You must uninstall a snap-in from all the clusters before you delete the snap-in. When you delete the snap-in, the snap-in is removed from the System Manager database.

Note:

If a user is uninstalling a service that was installed on different clusters while some other services are getting installed or uninstalled on these clusters, the user must wait for these operations to complete before deleting the uninstalled service.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Service Management** > **Services**.
3. On the Service Management page, select the service that you want to delete.
4. Click **Delete**.

   Important:

   Verify that the service is in the **Loaded** state before you click **Delete**.

5. In the Delete Service Confirmation dialog box, select the **Please Confirm** check box.
6. Click **Delete**.

Bundles

A bundle is a package of multiple snap-in SVARs and is itself an SVAR file.

External dependency is a service which is not packaged along with the bundle. Internal Dependency is a service which is packaged along with a bundle.

Note:

Workflows and Tasks that are loaded as part of a bundle are not be displayed on the Services page, Cluster Administration page, and the Service Profile page. However, snap-ins of type Java loaded through bundles are displayed on the Services page.

Loading a bundle

Before you begin

The external dependencies which are not packaged with the bundle itself need to be loaded before loading the bundle.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Service Management** > **Bundles**.
3. Click **Load**.

   The total size of all selected files cannot exceed the browser-specific upload limits.
4. On the Load bundle dialog box, click **Choose File**.
5. Select the file and click **Open**.
6. Click **Commit**.
7. When the bundle is loaded, the Service Management page displays the State of the bundle as **Loaded**.

Installing the bundle

About this task

The bundle installs starts only if the external dependencies are in loaded state explicitly from Services page or packaged along with the bundle.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Service Management** > **Bundles**.
3. Select the bundle that you want to install and click **Install**.
4. Select the cluster(s) where you want the bundle to reside, and click **Commit**.
5. To see the status of the bundle installation, click the Refresh Table icon located in the upper-left corner of the **All Bundles** list.

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

6. Click on the bundle to get the bundle installation status which precisely shows services and dependency installation status on the Avaya Breeze™ nodes.

Uninstalling a bundle

About this task

The external dependency will not get uninstalled while uninstalling a bundle from a cluster.

The internal dependency will only get uninstalled while uninstalling a bundle if no other bundle is dependent on it.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Service Management** > **Bundles**.
3. Select the bundle that you want to remove and click **Uninstall**.
4. Select the cluster or clusters from which you want to remove the bundle.
5. Click **Commit**.

Deleting the Bundle

Before you begin

The bundle must be in loaded state to delete the bundle.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Service Management** > **Bundles**.
3. Select the bundle that you want to delete.
4. Click **Delete**.
5. Select the **Please Confirm**.
6. Click **Delete**.

Service Databases

Deleting a service database

About this task

A service database must be deleted after all versions of that service have been uninstalled from the cluster. This procedure is not necessary if you select the **Do you want to delete the database?** check box when uninstalling the snap-in.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Service Management** > **Service Databases**.
3. In the **Cluster** field, select the cluster.
4. Select the service database that you want to delete.
5. Click **Delete**.

   Databases that are in use cannot be deleted.

Chapter 5: User Administration

Administering implicit sequencing for Avaya Breeze™

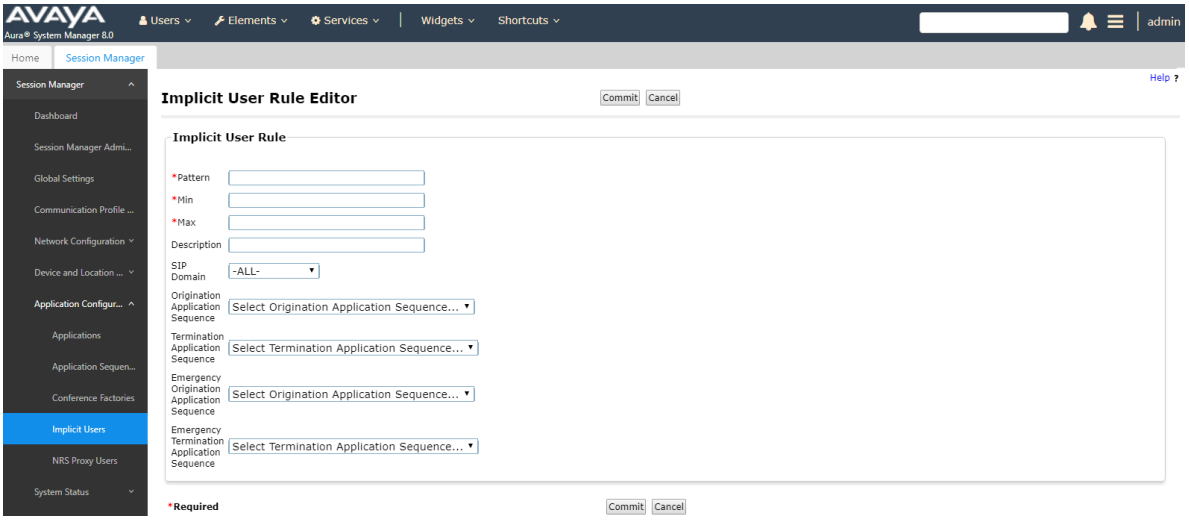
Administer implicit sequencing for a user or group of users for Avaya Breeze™ so that an application sequence can be assigned to those users for call-intercept snap-ins. Avaya Breeze™ uses implicit sequencing for both SIP and non-SIP endpoints. Therefore, you must administer implicit sequencing for all SIP and non-SIP endpoints that receive call-intercept snap-ins.

Before you begin

Create the Application and Application Sequence for the Avaya Breeze™ server before starting this task.

Procedure

1. On System Manager, click **Elements** > **Session Manager** > **Global Settings**.
2. Select the **Enable Implicit Users Applications for SIP users** field.
3. Click **Commit**.
4. Click **Session Manager** > **Application Configuration** > **Implicit Users**.
5. Click **New**.



6. In the **Pattern** field, specify the pattern as defined for Session Manager and Communication Manager digit routing.

For non-SIP users, the dial pattern should be the same pattern format as used in the Routing Policy Dial pattern. For SIP users, as a best practice use E.164 patterns to scope the SIP users either singularly or as a range. If that is not desired, use the **Communication Address** defined on the **User** > **User Management** > **Manage Users Communication Profile** tab.

The pattern range used can include both SIP and non-SIP users.

For example, in the **Pattern** field, do one of the following:

- Enter the user's full E.164 number (or minimally enter the **Communication Address** defined on the **User** > **User Management** > **Manage Users Communication Profile** tab for that user) for a single user.
- Enter "x" patterns as wildcards to match multiple users.

For example, for a single user using E.164 format, enter +13035551212, alternatively enter +1303555xxxx to match all users with the +1303555 prefix that is 12 digits in total length (including the +).

7. The **Min** value is auto-populated based on the pattern.

   You can define this value as required.

8. The **Max** value is auto-populated based on the pattern.

   You can define this value as required.

9. The **SIP Domain** default of `-ALL-`.

   Note:

   If you use multi-domain routing, see *Administering Avaya Aura® Session Manager* for information about what to enter in this field.

10. Select the Application Sequence for the **Origination Application Sequence** from the drop-down menu.

    The **Origination Application Sequence** tells Session Manager to send the call to the Avaya Breeze™ when the targeted user is placing or making a call. Use the Origination Application Sequence for Calling Party snap-ins.

11. Select the Application Sequence for the **Termination Application Sequence** from the drop-down menu.

    The **Termination Application Sequence** tells Session Manager to send the call to the Avaya Breeze™ when the targeted user is receiving a call. Use the Termination Application Sequence for Called Party snap-ins.

12. To save your changes, click **Commit**.

Assign a Service Profile to a user or Implicit User Pattern

Users are associated with a Service Profile and not with individual snap-ins. Assign a Service Profile to a user in the following ways:

- Implicit users – Create an Implicit User Profile Rule that encompasses all users you want to use the Service Profile. Assign the Service Profile to that group. Users do not need to be administered on System Manager.
- Administered users – Assign the Service Profile to an individual user who is administered on System Manager. To use this method, any SIP or H.323 user the Service Profile is assigned to must be administered as an explicit user. In general SIP users are already administered in System Manager as explicit users, but H.323 users may not be. Therefore, you may need to create a new user profile for a user you want to assign the Service Profile.

If a Service Profile is assigned to a user through both explicit and implicit administration, the explicitly assigned Service Profile takes precedence.

Related links

Assigning a Service Profile to implicit users on page 51
Creating a new administered user on page 52
Assigning a service profile to an administered user on page 53

Assigning a Service Profile to implicit users

Before you begin

You must create the Service Profile before it can be assigned.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the left navigation pane, click **Configuration** > **Implicit User Profiles.**
3. Click **New** to create a new rule, or select a pattern and click **Edit** to change an existing rule.
4. In the **Service Profile** field select the Service Profile for these users.
5. In the **Pattern** field specify the pattern as defined for the called or calling party number.
6. **(Optional)** Revise the **Min** and **Max** values for the number of digits from the pattern to match.

   These fields auto-populate based on the pattern.
7. Type a description of the rule, typically a description of the group of users the rule defines.
8. Click **Commit** to save your changes.

Related links

Implicit User Profile Rule Editor field descriptions on page 120

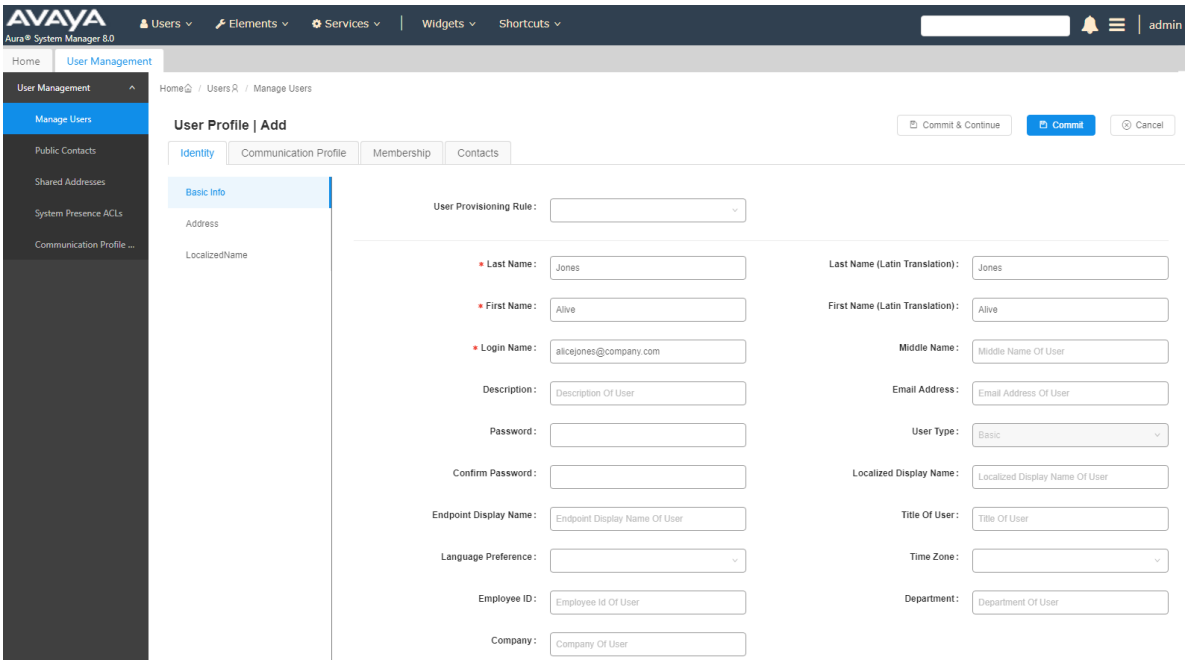
Creating a new administered user

About this task

Use this procedure to create a new explicit user in System Manager. You do not need to perform this procedure if you are using an implicit user profile rule to assign a Service Profile to users. It also is not required for users already administered as explicit users.

Procedure

1. On System Manager, click **Users** > **User Management** > **Manage Users**.
2. Click **New**.
3. Click the **Identity** tab.



4. Enter the user's Last, First, and Login names.

   The login name is in the form of `handle@domain`.
5. Click the **Communication Profile** tab.
6. Click **Communication Profile Password**.
7. Enter the **Communication Profile Password** and confirm the password.
8. Create a new Communication Address.
   a. In the **Communication Address** table, click **New**.
   b. In the **Type** field, select `Avaya E.164` or `Avaya SIP`.

c. In the first part of the **Fully Qualified Address** field, enter a number that matches the **Pattern** in the Implicit User Rule page. E.164 numbers can have a maximum of fifteen digits and are usually written with a + prefix, for example, +15553091337.

   This is the pattern that you created when administering implicit sequencing. Your user must fall in the implicit sequencing pattern range so that Avaya Breeze™ is invoked when a call is received or sent.

d. In the second field, select the domain for this user from the drop-down menu.

e. Click **OK**.

Assigning a service profile to an administered user

Before you begin

Create a service profile.

Procedure

1. On System Manager, click **Users** > **User Management** > **Manage Users**.
2. Select the check box by the appropriate user name or number.
3. Click **Edit**.
4. On the **Communication Profile** tab, in **Profiles**, click **Avaya Breeze™ Profile**.
5. In the **Service Profile** field, select the service profile with the required snap-in.
6. Click **Commit**.

Chapter 6: Reliable Eventing administration

Reliable Eventing Framework provides a new mechanism for delivering messages. The current Eventing Framework uses Collaboration Bus as a point-to-point delivery mode for intra-node asynchronous events with high performance. The Reliable Eventing Framework adopts Apache ActiveMQ that provides a richer set of capabilities like reliability, asynchronous events, inter-node, and inter-cluster which are not available in Eventing Framework.

Reliable Eventing Framework provides the following features beyond what Eventing Framework provides:

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

Related links

Creating a Reliable Eventing group on page 54
Editing a Reliable Eventing group on page 55
Deleting a Reliable Eventing group on page 56
Viewing the status of Reliable Eventing destinations on page 56
Deleting a Reliable Eventing destination on page 56
Running a maintenance test for a broker on page 57

Creating a Reliable Eventing group

Procedure

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

- **Type**: Select **HA** or **Standalone**.
  - If you select **HA**, you must select at least three Avaya Breeze™ nodes or brokers.
  - If you select **Standalone**, you must select at least one Avaya Breeze™ node or broker.

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

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

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

Related links

Reliable Eventing administration on page 54

Editing a Reliable Eventing group

Procedure

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

Related links

Reliable Eventing administration on page 54

Deleting a Reliable Eventing group

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Reliable Eventing Administration** > **Dashboard**.
2. Select the **Reliable Eventing group** and click **Delete**.
3. In the Confirm Delete window, click **Continue**.

Related links

Reliable Eventing administration on page 54

Viewing the status of Reliable Eventing destinations

Procedure

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

   The system displays the destination status.

Related links

Reliable Eventing administration on page 54

Deleting a Reliable Eventing destination

Procedure

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

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

   The system will purge the messages and delete the destination.

Related links

Reliable Eventing administration on page 54

Running a maintenance test for a broker

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **System Tools and Monitoring** > **Maintenance Tests**.
2. From the **Select Avaya Breeze to test** drop-down list, select the Avaya Breeze node to test.
3. Select the **Test Reliable Eventing Framework** check box.
4. Click **Execute Selected Tests**.

   The system displays the status as:

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

Related links

Reliable Eventing administration on page 54

Chapter 7: Authorization Service

Authorization Service provides the following security functions to other Avaya Breeze™ snap-ins:

- Authentication of end users through LDAP or SAML
- Authentication of client applications using PKI
- Fine-grained authorization of snap-in features through client application

Client applications may or may not be snap-ins. Using Authorization Service, a client application may authenticate the client credentials and optionally with a user credentials. The client is then provided with a token that can be used to securely access multiple Avaya Breeze™ snap-ins without being challenged.

For example, Avaya Context Store Snap-in leverages Authorization Service by acting as a Resource server. Client applications using Avaya Context Store Snap-in first authenticate with Authorization Service and then provide the token to Avaya Context Store Snap-in with a request for validation.

Note:

The existing whitelist or certificate-based HTTP(S) security mechanisms are supported with Avaya Context Store Snap-in.

Authorization Resources

Authorization Resources are snap-ins that have protected resources. These snap-ins are capable of accepting and responding to protected resource requests using access tokens.

To enable a snap-in as Authorization Resource, see *Avaya Breeze™ Snap-in Development Guide*.

Viewing Authorized clients authorized by a Resource server

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **Authorization**.
3. In the Resource Servers tab, select the Resource server, and click **View Authorized Client**.

   The system displays the Authorized clients authorized by the Resource server.

Configuring features for a Resource server

About this task

Configure the values of a specific feature.

The features for a Resource snap-in are specified in the `properties.xml` file. For more details, see *Avaya Breeze™ Snap-in Development Guide*.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **Authorization**.
3. In the Resource Servers tab, select the Resource server, and click **Configure Features**.
4. In the **Select Feature** field, select the feature that you want to configure.
5. In the **Values** table, add or delete values to the feature.
6. Click **Commit**.

Authorization Clients

Authorization Client is an application that sends protected resource requests on behalf of the resource owner and with its authorization.

Avaya Breeze™ Authorization Client

These are snap-ins interacting with Authorization Service for getting access tokens.

To enable a snap-in as Authorization Client, see *Avaya Breeze™ Snap-in Development Guide*.

Assigning and editing Grants for Authorization Client

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **Authorization**.
3. In the **Clients** tab, select the **Authorization Client** and click **Edit Grants**.
4. To edit values of an existing grant, select the grant and click **Edit Values**.
   a. Edit the features and values.
   b. Click **Commit**.
5. To create a new grant, click **New**.

6. In the **Resource Name** field, select the **Resource Server** that authorizes the Authorization Client.
7. In the **Resource Cluster** field, select the cluster.
8. In the **Feature** field, select a feature to which you want to assign values.
9. In the **Values** field, assign values to the selected feature.
10. Click **Commit**.

Viewing or regenerating keys for an Authorization Client Snap-in

About this task

Authorization Client snap-ins use public and private key pairs to authenticate with Authorization Service. The following procedure explains how existing keys can be revoked and new ones be regenerated in case of a security leak.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **Authorization**.
3. In the **Clients** tab, select the **Authorization Client Snap-in** and click **Edit Key**.
4. Click **Regenerate Keys**.

External Authorization Client

These are non-snap-in client applications that interact with Authorization Service to get tokens.

Adding an external Authorization Client

About this task

Use this procedure to add an external authorization client. External authorization clients are applications that are not snap-ins. You must provide the client certificate during the process. The certificate is used to authenticate the client when granting an access token.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **Authorization**.
3. In the **Clients** tab, click **New**.
4. Type the name of the client, and upload the client certificate.

   The redirection URI is an optional parameter. When using the code grant flow to login users, Authorization Service uses this URI to redirect the browser to the client.

Deleting an external Authorization Client

About this task

Use this procedure to delete an external Authorization Client. This option is disabled for Authorization Client Snap-ins. To delete Authorization Client Snap-ins, uninstall and delete the snap-in. For more information, see *Service Management*.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **Authorization**.
3. In the **Clients** tab, select the **Authorization Client** and click **Delete**.

End User Authentication

The Avaya Breeze™ Authorization Service supports SAML and LDAP end user authentication for the two OAuth 2.0 grant types used for handling user authentication. The below table provides an overview:

OAuth 2.0 Grant Type (Authorization)	Authentication Mechanism supported
Authorization Code	SAML, LDAP
Resource Owner Password Credentials	LDAP

Refer to *Avaya Breeze™ Snap-in Development Guide* on information about integrating an Authorization Client with the Authorization Service to support one of the two grant types mentioned earlier.

User login experience

With Authorization Code Grant flow and SAML Authentication deployments, the end-user trying to access an Authorization Client snap-in is redirected to an Identity Provider and presented with the Identity Provider owned login screen. On successful authentication, the user is redirected back to the Authorization Client with a logged-in session.

With Authorization Code Grant flow and LDAP Authentication deployments, the end-user trying to access an Authorization Client snap-in is redirected to the Avaya Breeze™ Authorization Service, which presents the user with a login screen. On successful authentication, the user is redirected back to the Authorization Client with a logged-in session.

With Resource Owner Password Credentials flow and LDAP Authentication deployments, the end-user trying to access an Authorization Client snap-in is presented with a login screen owned by the Authorization Client. On successful authentication, the user is logged in to the client.

The following sections detail on configuring the two authentication mechanisms supported.

LDAP Authentication

LDAP Authentication deployments use the System Manager Directory Synchronization to configure a datasource. The Avaya Breeze™ Authorization Service supports LDAP authentication for two types of OAuth 2.0 Authorization flows:

- Authorization Code Grant
- Resource Owner Password Credentials

Enabling LDAP Authentication for Authorization Code Grant Flow

Enabling LDAP Authentication Mechanism for Authorization

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Configuration** > **Authorization** > **Authentication Mechanism**.
2. Click **Change Authentication Mechanism**.
3. In the **Authentication Mechanism** field, select **LDAP**.
4. Click **Save**.

Testing the setup

Procedure

Perform one of the following:

- Deploy an Authorization Client snap-in which has been integrated to use the Avaya Breeze™ Authorization Code Grant flow.
- Use the Authorization Sample snap-ins provided in the Avaya Breeze™ SDK.

LDAP authentication will provide the end-user with an AD FS login screen when trying to access the Client snap-in. On successful authentication, the user is redirected back to the Client with a logged-in session.

Enabling LDAP Authentication for Resource Owner Password Credentials Flow

Procedure

Perform one of the following:

- Deploy an Authorization Client snap-in which has been integrated to use the Resource Owner Password Credentials flow
- Use the Authorization Sample snap-ins provided in the Avaya Breeze™ SDK.

The Client will provide the user with a login screen when trying to access it. On successful authentication, the user is logged in.

LDAP server certificate

The LDAP server certificate should be added as a trusted certificate to the Avaya Breeze™ cluster where Authorization Service has been installed. Authorization Service uses secure HTTP connections while authenticating users with the LDAP server.

Importing the LDAP Server certificate into System Manager

Procedure

1. On System Manager, click **Services** > **Inventory** > **Manage Elements**.
2. Select the System Manager instance and click **More Actions** > **Configured Trusted Certificates**.
3. Click **Add**.
4. Select the **Import using TLS** field.
5. In the **IP Address** field, enter the IP address of the LDAP server.
6. In the **Port** field, enter the port of the LDAP server.
7. Click **Retrieve Certificate** to import the certificate
8. Click **Commit**.
9. To export the imported LDAP certificate, on the Trusted Certificates page, click **Export**.

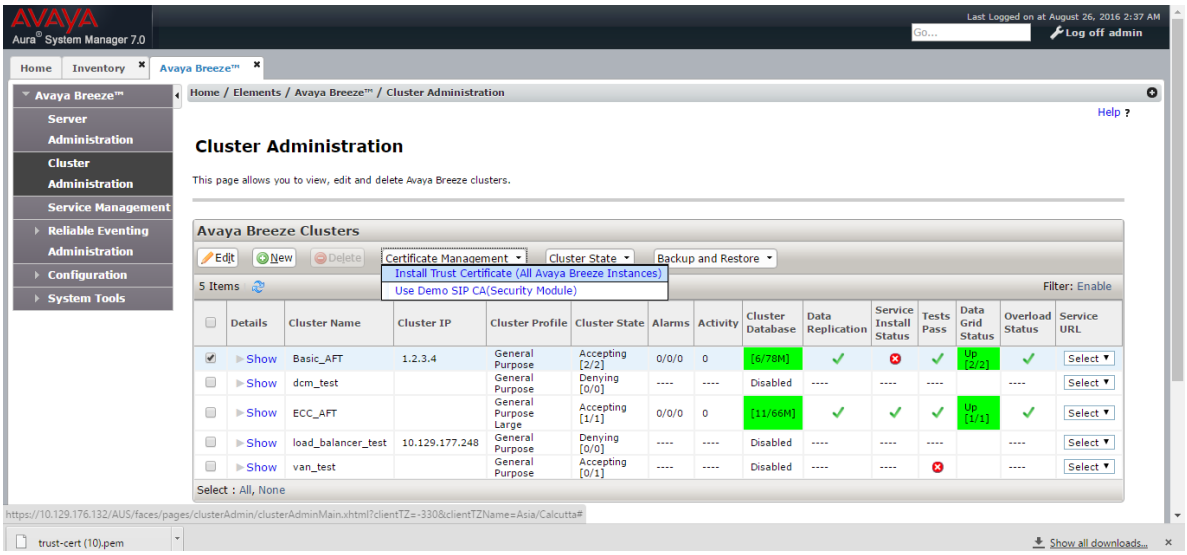
Importing the LDAP Server certificate into Avaya Breeze™ cluster

Procedure

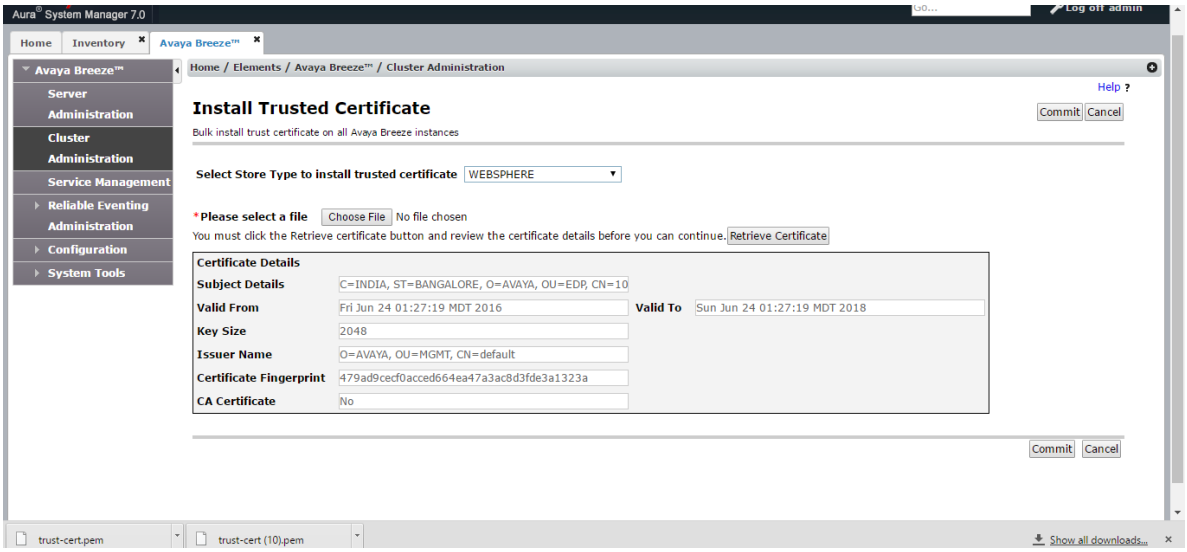
1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. Click **Cluster Administration**.
3. Select the cluster which has the Authorization Service snap-in instance and click **Certificate Management** > **Install Trusted Certificate (All Avaya Breeze Instances)**.

   The system displays the Install Trusted Certificate page.

4. Click **Add**.



5. In the **Store Type to install trusted certificate** field, select **WEBSPHERE**.
6. Provide the path of LDAP trusted certificate which was exported earlier.
7. Click **Retrieve Certificate**.



8. Click **Commit**.

SAML authentication

SAML deployments require agreements between system entities regarding identifiers, binding support and endpoints, certificates and keys, and so forth. A metadata specification is useful for describing this information in a standardized way.

The system entities involved here are the Avaya Breeze™ Authorization Service (acts as a Service Provider) and a far-end IdP. The metadata of both the entities are XML files which need to be exchanged between them:

- The Service Provider metadata is used for configuring the Service Provider at the IdP.
- The IdP Metadata is used for configuring the IdP at the Service Provider.

Getting the Service Provider metadata for Authorization Service

About this task

After you install Authorization Server in an Avaya Breeze™ cluster, it generates metadata on a per-node basis.

The downloaded Service Provider metadata file needs to be used while configuring Authorization Service as a Service Provider at a far-end IdP.

Procedure

Use the following path on each node to download the metadata:

```
https://<SecurityModuleIP>:9443/services/AuthorizationService/spmetadata
```

Configuring the IDP on SMGR

About this task

The Authorization Service acting as a Service Provider, obtains the IdP details from the SAML Authentication Mechanism configuration.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **Configuration** > **Authorization**.
2. Click **Authentication Mechanism** > **SAML**.
3. Enter the following details:
   a. **Configured Identity Provider**: Specify which IdP has been currently configured.
   b. **Should SAML requests be signed?**: Select the check box to enable. If enabled, SAML requests going to the IdP will be signed.
   c. **Attribute used as UserID**: Specify the SAML attribute name to be used as the user identifier. This setting is mapped to the subject of the token.
   d. **Authentication Context**: Specify the authentication methods in SAML authentication requests and authentication statements.
   e. **Authentication Context Comparison Type**: Specify the relative strength to be used when an IdP evaluates a requested authentication context.
   f. **Identity Provider Metadata File**: Specify the metadata file provided by the IdP.

   The different authentication contexts map to the following URIs:

Authentication Context	URI used internally
User Name and Password	urn:oasis:names:tc:SAML:2.0:ac:classes:Password
Password Protected Transport	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
Transport Layer Security (TLS) Client	urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient
X.509 Certificate	urn:oasis:names:tc:SAML:2.0:ac:classes:X509
Kerberos	urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos

Enabling SAML profile for Authorization

About this task

After configuring the IdP, SAML profile needs to be enabled so that the Authorization Service can read the configuration and start its Service Provider component.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. Click **Configuration** > **Attributes** > **Service Clusters**.
3. Select the Cluster where Authorization Service has been installed and select Service as Authorization Service.
4. In the **SAML Profile** field, select **Deploy**.
5. Click **Commit**.

Changing the authentication mechanism

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **Authorization**.
3. On the Authorization Configuration page, click the **Authentication Mechanism** tab.
4. Click **Change Authentication Mechanism**.
5. On the Change Authentication Mechanism page, in the **select Authentication Mechanism** field, select **LDAP** or **SAML**.
6. If you select **SAML**, enter the following details:
   - **Should SAML Request be Signed?**
   - **Attribute Used as UserID**
   - **Authentication Context**

- **Authentication Context Comparison Type**
- Click **Choose File** to select the Identity Provider Metadata file.

7. Click **Save**.

Chapter 8: HTTP Security Administration

Administering HTTP Security

Administering a whitelist for HTTP Security

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **HTTP Security**.
3. Select the cluster.

   Note:

   For Avaya Breeze™ Release 3.0 or earlier, select the **Legacy** option in the **Cluster** field. This option displays the preconfigured Whitelists.
4. Click the Whitelist tab.
5. Select the **Whitelist Enabled** check box.

   If you do not select the **Whitelist Enabled** check box, Avaya Breeze™ accepts HTTP or HTTPS requests from any system.
6. To add a new IP address to the Whitelist table:
   a. Click **New**.
   b. In the new row, type values in the **IP address** and the **Subnet Bits** fields.
7. Click **Commit**.

Related links

HTTP Security field descriptions on page 118

Administering client certificate challenge for HTTPS

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **HTTP Security**.

3. Select the cluster.
4. Click the Whitelist tab.
5. Select the **Client Certificate Challenge Enabled** check box.

   The client certificate must be signed by a trusted certificate authority.
6. Click **Commit**.

Related links

HTTP Security field descriptions on page 118

Administering HTTP CORS security

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **HTTP Security**.
3. Select the cluster.

   Note:

   For Avaya Breeze™ Release 3.0 or earlier, select the **Legacy** option in the **Cluster** field. This option displays the preconfigured HTTP CORS.
4. Click the HTTP CORS tab.
5. Perform one of the following:
   - Select the **Allow Cross-origin Resource Sharing for all** check box to allow any server to make requests.
   - Clear the **Allow Cross-origin Resource Sharing for all** check box to limit access to administered servers.
6. Limit the receipt of requests by adding authorized servers to the **Host Address** list:
   a. Verify that the **Allow Cross-origin Resource Sharing for all** check box is cleared.
   b. Click **New**.
   c. In the **Host address** field, type the complete origin address of the server that you want Avaya Breeze™ to have access permission to.

      For example, if the origin is `xyz.com`, add `xyz.com` as an origin in the CORS list. If the origin is `ip:port`, add `ip:port` as an origin in the CORS list.
7. Click **Commit**.

Related links

HTTP Security field descriptions on page 118

Chapter 9: JDBC Resource Administration

JDBC Resource administration

JDBC resource providers and data source

Create and manage JDBC providers to create data sources for pre-existing, external snap-in database. Use the JDBC providers to upload drivers to the Avaya Breeze™ clusters, which enables the use of multiple database variants like Oracle, MySQL.

As a user, download the JDBC driver jar file that is compatible with the database version. Download this file from the database vendor website.

Note:

JDBC providers or data sources created by using incorrect or incompatible jar files fail. Ensure that you use the correct jar file and the appropriate implementation class for the jar.

Use the JDBC jar file to create the JDBC provider resource. The JDBC provider creates the JDBC provider service, which is displayed on the Service Management page. Select and install the JDBC provider service on your cluster. After you install the provider, create the JDBC data source by using the provider. Ensure that you specify a unique JNDI name for the data source. You can access the data source using the JNDI name.

Important:

After you create or modify a JDBC provider or a data source, you must restart all the Avaya Breeze™ servers in the cluster. To restart a server, on the Server Administration page, select the servers that you want to restart and click **Shutdown System** > **Reboot**.

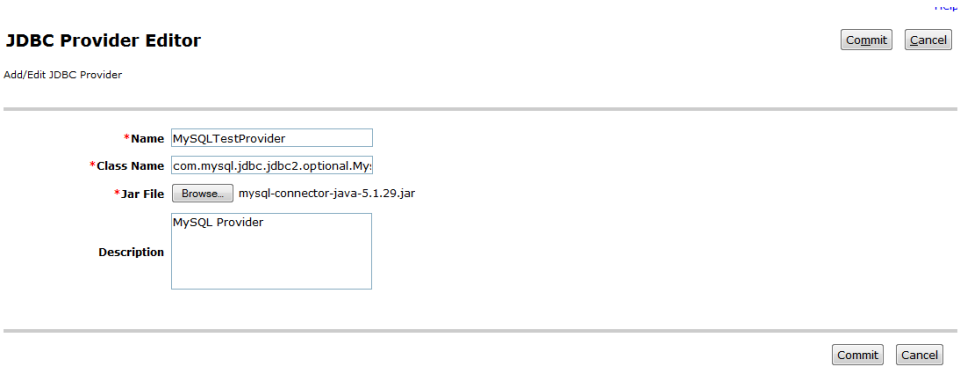
Administering JDBC providers

Adding a JDBC provider resource

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **JDBC Providers**.
3. Click **New**.

4. On the JDBC Provider Editor page, create a JDBC Provider using the JDBC driver jar.



5. Once the JDBC Provider is created, navigate to **Avaya Breeze™** > **Service Management**.
6. Select the Provider you created earlier and click **Install**.
7. Select the cluster on which you want to install and **Commit**.

Related links

JDBC Provider Editor field descriptions on page 121

Editing a JDBC provider resource

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **JDBC Providers**.
3. Select the JDBC source provider that you want to edit.
4. Click **Edit**.
5. On the JDBC Provider Editor page, edit the provider details.

   Note:

   You cannot edit all the fields in this page. For example, you cannot modify the jar path.

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

Related links

JDBC Provider Editor field descriptions on page 121

Deleting JDBC provider resources

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **JDBC Providers**.

3. On the JDBC Provider page, select the providers that you want to delete.

   Note:

   You cannot delete a JDBC provider if the provider is installed on a cluster through a snap-in.

4. Click **Delete**.

Administering JDBC data source

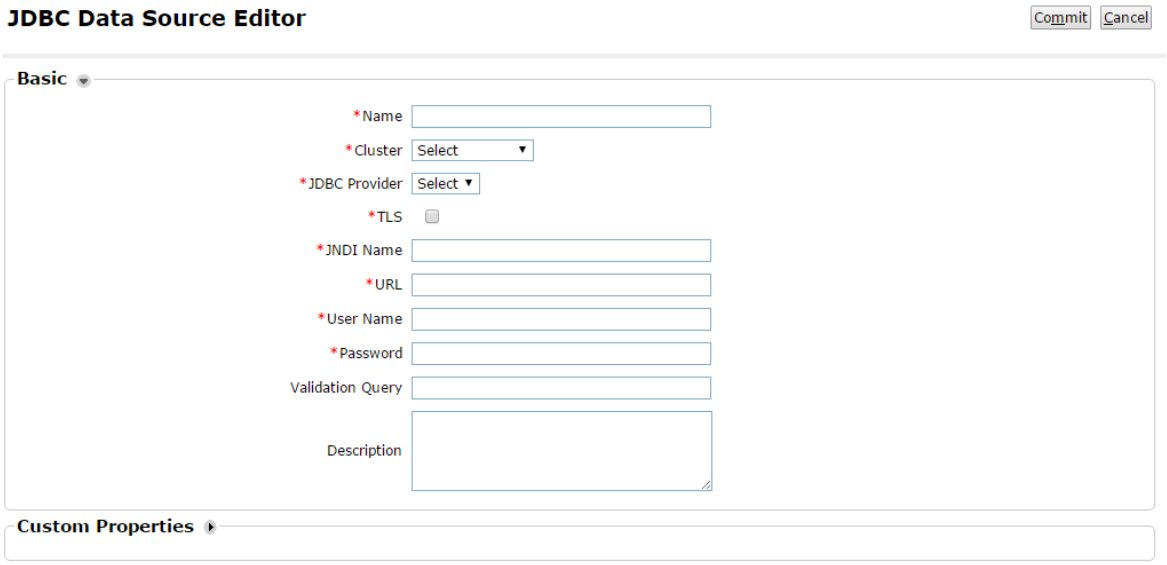
Adding a JDBC data source

Procedure

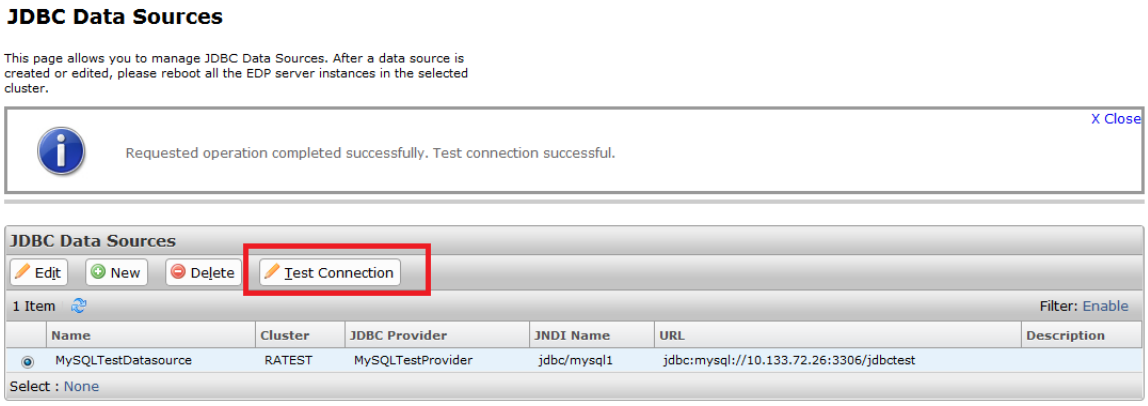
1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **JDBC Sources**.
3. Click **New**.
4. On the JDBC Data Source Editor page, enter the following details:
   a. In the **Cluster** field, select the cluster on which you installed the JDBC provider.

      The system populates the value of the **JDBC Provider** field.

   b. In the **JNDI Name** field, type a unique name.
   c. In the **URL** field, type the URL.
   d. In the **User Name** field, type a user name.
   e. In the **Password** field, type a password.



5. Click **Commit**.
6. To test the connection, select the data source, and click **Test Connection**.



Related links

JDBC Data Source Editor field descriptions on page 123

Editing a JDBC data source

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **JDBC Sources**.
3. Select the JDBC data source that you want to edit, and click **Edit**.
4. On the JDBC Data Source Editor page, make the required changes.
5. Click **Commit**.
6. After you modify the data source of a cluster, restart all the servers in the cluster.
   a. On the Server Administration page, select the servers that you need to restart.
   b. Click **Shutdown System** > **Reboot**.

Related links

JDBC Data Source Editor field descriptions on page 123

Deleting a JDBC data source

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **JDBC Sources**.
3. Select the JDBC data source that you want to delete.
4. Click **Delete**.

Testing the connection using query validation

About this task

Use this procedure to determine whether the data source you created is reachable.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **JDBC Sources**.
3. Select the JDBC data source whose connection you want to test.
4. Click **Test Connection**.

   The system runs the validation query and then displays a success or failure message.

Sample configuration for database providers

Field name	PostgreSQL	My SQL	MS SQL	Oracle
JDBC Provider				
Class name	org.postgresql.xa.PGXADataSource	com.mysql.jdbc.jdbc2.optional.MysqlXADataSource	com.microsoft.sqlserver.jdbc.SQLServerXADataSource	oracle.jdbc.xa.client.OracleXADataSource
Jar File	postgresql-9.2-1004-jdbc41.jar	mysql-connector-java-5.1.44.jar	sqljdbc42.jar	ojdbc7.jar
JDBC Data Source				
URL	jdbc:postgresql://(host):(port)/(database_name)	jdbc:mysql://(host):(port)/(database_name)	jdbc:sqlserver://(server_name):(port)	• jdbc:oracle:thin:@//(host):(port)/(service_name) • jdbc:oracle:thin:@(host):(port):SID
Validation Query	select 1	select 1	select 1	select 1
Custom Properties	• Name: databaseName; Value: <the database name> • Name: generateSimpleParameterMetadata; Value: true • Name: searchpath; Value: <the schema name>	Name: generateSimpleParameterMetadata; Value: true	• Name: generateSimpleParameterMetadata; Value: true • Name: instanceName; Value: <the SQL instance name> • Name: databaseName;	Name: generateSimpleParameterMetadata; Value: true

Table continues…

Field name	PostgreSQL	My SQL	MS SQL	Oracle
	• Name: serverName; Value: <the DB server IP address or FQDN> • Name: portNumber; Value: <the TCP port number of the DB server>		Value: <the database name>	

Note:

The jar file names and versions mentioned in the table are examples. When configuring JDBC provider for external database, refer to database documentation and select correct JDBC driver jar version.

Chapter 10: Service Ports

Assigning service ports for Avaya-developed snap-ins

About this task

Use the **Avaya Breeze™** > **Configuration** > **Service Ports** page to:

- Assign or reserve ports for Avaya-developed snap-ins.
- Administer ports enablement for Avaya-developed snap-ins.

The Service Ports page displays the default ports for a snap-in after you load the snap-in. You can override the default port value for the snap-in at the snap-in level and cluster level from this page.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the left navigation pane, click **Configuration** > **Service Ports**.
3. From the **Service** field, select the snap-in for which you want to configure the ports.

   The system displays the assigned snap-in ports for the snap-in that you selected.
4. (Optional) From the **Cluster** field, select the cluster.

   The system displays the selected snap-in ports for the snap-in and the cluster that you selected.
5. From the **Selected Service Ports** table, specify the ports that you want to assign to the snap-in.
6. (Optional) Select the **Override Default** check box to override the default port value.

   Note:

   If the specified Effective Port Value is already assigned to another snap-in or a reserved port, the system displays an error message. Specify another override port value.

   Similarly, port validation is done when you install the snap-in whose ports are specified.

   The field **Protocol** displays the protocol that will be used by the specified port for communication. This field cannot updated from Service ports page.
7. Click **Commit**.

The **All Service Used/System Reserved Ports** table displays the ports used by other snap-ins and the system reserved ports. Search for a specific port from this table before you assign the port to a snap-in.

Next steps

If the administrator wants to swap two ports, for example, 1100 and 1200, do the following:

1. Update port 1100 to 1108. Click **Commit**.

   1108 is just a placeholder. Ensure that port 1108 is unused.
2. Update port 1200 to 1100. Click **Commit**.
3. Update port 1108 to 1200. Click **Commit**.

Chapter 11: Geo Redundancy

Avaya Breeze™ with System Manager Geographic Redundancy

Terminology

The geographic redundancy section applies only if you use the System Manager geographic redundancy feature.

1. Element: An *element* is an instance of an Avaya Aura® network entity. System Manager manages elements such as a Session Manager server or a Avaya Breeze™ server in an Avaya Aura® network.

   Note:

   A Avaya Breeze™ server is *managed* by either the primary System Manager instance or the secondary System Manager instance in a geographically redundant solution. This means that you can use the System Manager interface to administer Avaya Breeze™ clusters, administer Avaya Breeze™ platforms, load snap-ins, uninstall snap-ins, and run on demand maintenance tests.

2. Primary server: The first or the master System Manager server in a Geographic Redundancy set up that serves all the requests. The primary System Manager server is always in the *active* mode unless you turn off the server. In fail back cases, the primary System Manager instance might not be in the active mode.
3. Secondary server: The System Manager server that functions as a backup to the primary System Manager server. The normal mode of operation of the secondary System Manager server is the *standby* mode.
4. Active server: The mode of operation of the System Manager server where the server provides the full System Manager functionality.
5. Standby server: The mode of operation of the System Manager server where the server serves only authentication and authorization requests. In the standby mode of operation, the system supports limited Geographic Redundancy configuration and the inventory service.
6. *Geographic Redundancy-aware* elements are those elements of the Avaya Aura® solution that support the **Geographic Redundancy** feature, such as Avaya Breeze™ Release 3.0.

7. *Geographic Redundancy-unaware* elements are those elements of the Avaya Aura® solution that do not support the **Geographic Redundancy** feature, such as Avaya Breeze™ instances earlier than Release 3.0.
8. Geographic Redundancy replication: Geographic The Geographic Redundancy feature provides the following replication mechanisms to ensure consistency of data between the primary and the secondary System Manager servers: database replication, file replication, and LDAP replication. For more information, see *Administering Avaya Aura System Manager*.

Managing Avaya Breeze™ in a Geographic Redundancy solution

Either the primary or the secondary System Manager server manages Avaya Breeze™ servers in different geographic redundancy scenarios. It is important to understand which System Manager server manages each Avaya Breeze™ server. For more information, see *Geographic Redundancy Scenarios* in *Administering Avaya Aura System Manager*.

1. Determining the System Manager that manages each Avaya Breeze™ server:

Avaya Breeze™ release 3.0:

To view the System Manager server that manages a particular Avaya Breeze™ server, see the **Managed By** column in the **Inventory** > **Manage Elements** webpage. The status can be *Primary*, *Secondary*, or *Unknown*. The *Unknown* value indicates that the System Manager instance cannot get the status from the Avaya Breeze™ server. Select a Avaya Breeze™ server and click **Get Current Status** to refresh the status for that Avaya Breeze™ server.

Avaya Breeze™ earlier than release 3.0:

Avaya Breeze™ servers earlier than release 3.0 are not Geographic Redundancy-aware. These Avaya Breeze™ servers can be managed only by the primary System Manager. For these Avaya Breeze™ servers, the **Inventory** > **Managed Elements** webpage displays **Not Supported** in the **Managed By** column.

Related links

Avaya Breeze administration in a geographic redundancy environment on page 79
Avaya Breeze Status and Maintenance on page 81
Fault management (alarming and logging) in a geographic redundant environment on page 82
Geographic Redundancy Replication and data restoration on page 83

Avaya Breeze™ administration in a geographic redundancy environment

This section provides information about the Avaya Breeze™ administration for different Geographic Redundancy scenarios. This section also covers the considerations when you make administration changes such as loading, installing, and uninstalling snap-ins, managing clusters, and loading Service Profiles. See the *Applicability* section for a full list of the administration webpages that are applicable.

Sunny day scenario

In this case, the primary System Manager manages all the Avaya Breeze™ instances. The primary System Manager replicates administration changes to all the Avaya Breeze™ instances. The secondary server is in the standby mode and you cannot make any administration changes using the secondary server.

Rainy day scenario

In this case, the secondary System Manager manages all the Avaya Breeze™ servers. The secondary System Manager replicates the administration changes to all the Avaya Breeze™ servers. The primary server is offline and you cannot make any administration changes using the primary server.

Split-network scenario

In this case the primary and the secondary servers run in the active mode. The primary and secondary servers do not communicate with each other due to a network outage. Before making administration changes, the administrator must confirm the group membership using the **Inventory** > **Managed Elements** webpage. The administrator must perform the administration changes on the primary System Manager for the Avaya Breeze™ instances that the primary server manages. Similarly, the administrator must perform the administration changes on the secondary System Manager for the Avaya Breeze™ instances that the secondary server manages. Each System Manager replicates the administration changes to the respective Avaya Breeze™ servers. Administration changes must also be compatible with non-Avaya Breeze™ elements in the split network. For example, a SIP user added on System Manager should have Avaya Breeze™ Profile, Session Manager Profile and CM Endpoint Profile that reference the Avaya Breeze™, Session Manager, and Communication Manager elements managed by the same System Manager. In other words, the elements are all on the same side of the network split.

Caution:

Before making administration changes, you must assess the extent of the enterprise network split. The network split results in partitioning of Avaya Breeze™ servers and other elements into two groups. The primary System Manager manages one group and the secondary System Manager manages the other group.

Note:

After a split-network scenario you can restore changes made only in one of the two System Manager servers.

Split-network warning messages

The Avaya Breeze™ Server Administration page displays a warning message when the System Manager server detects that the administrator is configuring for a split-network scenario. The primary System Manager can detect the possibility of a split-network configuration if:

- The primary System Manager does not manage all the Avaya Breeze™ instances.
- The secondary System Manager is not reachable on the network.
- The secondary System Manager is active.

The secondary System Manager can detect the possibility of a split-network configuration if:

- The secondary System Manager is active.
- The secondary server does not manage all the Avaya Breeze™ instances.

When the system displays a warning message, click the **Avaya Breeze™ Management Status** link to go to the **Inventory** > **Manage Elements** webpage. In this webpage, view the status of the System Manager that manages each Avaya Breeze™ server. Click **Minimize** to hide the warning message.

Applicability

The following table lists all the Avaya Breeze™ administration related functionalities for the respective webpages. When you make administration changes using any of these pages, System Manager replicates these changes only to those Avaya Breeze™ servers that the System Manager manages.

Web page	Functionality	Notes
Avaya Breeze™ > **Server Administration**.	Add, edit, delete the Avaya Breeze™ servers.	
Avaya Breeze™ > **Cluster Administration**>	Add, edit, view, and delete Avaya Breeze™ clusters.	
Avaya Breeze™ > **Service Administration**	Load, install, uninstall and delete services.	
Avaya Breeze™ > **Configuration**	Change the Service Profile configuration, attributes configuration, Avaya Aura® Media Server configuration, HTTP requests configuration.	
Inventory > **Manage Elements**	Add, edit, or delete the Avaya Breeze™ servers	
User Management > **Manage Users**	Change the Service Profile.	

Related links

Managing Avaya Breeze in a Geographic Redundancy solution on page 79

Avaya Breeze™ Status and Maintenance

This section provides information on using a System Manager to view the Avaya Breeze™ status and perform the maintenance operations on Avaya Breeze™. For example, you can view the status of a Avaya Breeze™ on the **Avaya Breeze™** > **Dashboard** webpage, or run the maintenance tests on a Avaya Breeze™ server from the **Avaya Breeze™** > **System Tools** > **Maintenance Tests** webpage.

Sunny day scenario

Using the primary System Manager, view the Avaya Breeze™ system status and perform the maintenance operations. You cannot use the secondary server to view the Avaya Breeze™ system status or to perform the maintenance operations.

Rainy day scenario

Use the secondary System Manager to view the Avaya Breeze™ system status and to perform the maintenance operations. You cannot use the primary server to view the Avaya Breeze™ system status or to perform the maintenance operations.

Split-network scenario

You must view the Avaya Breeze™ status and perform the maintenance operations from the System Manager server that manages the Avaya Breeze™ server.

Applicability

The following table lists all the system status functions of Avaya Breeze™ and maintenance operation functions for the respective webpages. The functions listed are only available for the Avaya Breeze™ servers that the System Manager manages.

Web page	Functionalities	Notes
Avaya Breeze™ > **Dashboard**	• View the Avaya Breeze™ system status. • Accept or deny new services.	
Session Manager > **System Tools**	• Run the maintenance tests for Avaya Breeze™ instances. • Download zipped copy of the Avaya Breeze™ related SNMP MIBs..	
Inventory > **Manage Elements**	View and edit the trusted certificate configuration and the identify certificate configuration of a Avaya Breeze™ instance by clicking the **More Actions** button.	

Related links

Managing Avaya Breeze in a Geographic Redundancy solution on page 79

Fault management (alarming and logging) in a geographic redundant environment

This section provides information on viewing the Avaya Breeze™ alarms and logs in the primary and secondary System Manager servers.

Sunny day scenario

Both the primary and the secondary System Manager servers collect alarms from all the Avaya Breeze™ instances. You can view all the Avaya Breeze™ related alarms from the **Events** > **Alarms** webpage on the primary System Manager.

Collect logs for a Avaya Breeze™ server from the **Events** > **Logs** > **Log Harvester** webpage on the primary System Manager.

View Avaya Breeze™ audit logs from the **Events** > **Logs** > **Log Viewer** webpage on the primary System Manager. These logs provide the details of the administration changes made on the primary System Manager.

The secondary System Manager is offline. During the Sunny day scenario you cannot view or collect any logs on the secondary System Manager.

Rainy day scenario

The secondary System Manager collects alarms from all the Avaya Breeze™ instances. After you configure the secondary System Manager into the active state, view the following alarms from the **Events** > **Alarms** webpage:

- Alarms collected when the secondary server was in the standby mode.
- New Avaya Breeze™ related alarms.

Collect logs from a Avaya Breeze™ server by navigating to the **Events** > **Logs** > **Log Harvester** webpage on the secondary System Manager.

View the Avaya Breeze™ audit logs from the secondary System Manager by navigating to the **Events** > **Logs** > **Log Viewer** webpage. These logs provide details of the administration changes made after the activation of the secondary System Manager.

The primary System Manager is offline. During the rainy day scenario you cannot view or collect alarms from the primary System Manager.

Split-network scenario

In the split-network scenario, both the primary and the secondary System Manager collect alarms from any Avaya Breeze™ that are reachable on the enterprise network. View these alarms from the **Events** > **Alarms** webpage. If a Avaya Breeze™ server cannot connect to a System Manager because of the network split, the Avaya Breeze™ forwards all the logs to that System Manager when the network connectivity restores. Go to the **Inventory** > **Manage Elements** webpage to view the status of the network connectivity from the current System Manager to each Avaya Breeze™ instance.

View the logs collected from a Avaya Breeze™ server by navigating to the **Events** > **Logs** > **Log Viewer** webpage of either the primary or the secondary System Manager, whichever manages the Avaya Breeze™ server. You cannot collect logs from a Avaya Breeze™ that the current System Manager does not manage.

View the Avaya Breeze™ audit logs from both the primary and secondary System Manager by navigating to the **Events** > **Logs** > **Log Viewer** webpage. Each System Manager displays audit logs for the administration changes made on that System Manager after that server became active.

Related links

Managing Avaya Breeze in a Geographic Redundancy solution on page 79

Geographic Redundancy Replication and data restoration

Geographic Redundancy Replication

The Geographic Redundancy feature provides the following replication mechanisms to ensure consistency of data between the primary and the secondary System Manager servers:

- Database replication
- File replication
- LDAP (Directory) replication

The primary System Manager server continuously replicates the data with the secondary System Manager server. If the system does not replicate the data for a specific period of time that is

configured in **Services** > **Configurations** > **Settings** > **SMGR** > **HealthMonitor**, the primary and the secondary System Manager servers raise alarms.

For more information on replication, see *Administering Avaya Aura® System Manager*.

Data restoration

In a Geographic Redundancy set up you must restore data when the primary System Manager server or the site fails. Restore the data from an old primary server or from the secondary server. In addition you may perform data restoration while replacing the primary or the secondary server, or while recovering the primary server from disaster. For more information on data restoration, see *Administering Avaya Aura® System Manager*.

Note:

When the primary server comes up after the server returns to the sunny day scenario, the alarms raised by the secondary server persist. You must manually clear the alarms raised by the secondary server in the rainy day scenario.

Related links

Managing Avaya Breeze in a Geographic Redundancy solution on page 79

Performing system verification tests

About this task

Use this procedure to verify that a Geographic Redundancy-enabled system is operating correctly in the *sunny day scenario*.

Procedure

1. To check the Geographic Redundancy status of the system, Go to the Geographical Redundancy webpage of the primary System Manager server and verify the configuration settings.
2. To view the Geographic Redundancy status, go to the **Geographic Redundancy** > **GR Health** webpage of the primary System Manager.

   For more information, see *Geographic Redundancy Health Monitoring* in *Administering Avaya Aura® System Manager*.
3. On the **Avaya Breeze™** dashboard, verify the status of each Avaya Breeze™ server.
4. Optionally, run the System Manager maintenance tests and the Avaya Breeze™ maintenance tests on the primary System Manager server. To run the maintenance tests, go to the **Avaya Breeze™** > **System Tools** > **Maintenance Tests** webpage.

   For more information, see *Maintenance Tests* in *Maintaining and Troubleshooting Avaya Breeze™*.

Chapter 12: Security

Generating a private key

About this task

Use this procedure to generate a private key if you want to use HTTPS (HTTP over TLS) to secure your Apache HTTP or Nginx web server, and you want to use a Certificate Authority (CA) to issue the SSL certificate.

Procedure

Run the following command: `openssl req -newkey rsa:2048 -nodes -keyout` *`my-private-key-file.key`*.

This command creates a 2048-bit private key. The -newkey rsa:2048 option specifies that the key should be 2048-bit, generated using the RSA algorithm. The -nodes option specifies that the private key should not be encrypted with a pass phrase.

Example

```
# openssl req -newkey rsa:2048 -nodes -keyout myPrivateKey.key
Generating a 2048 bit RSA private key
........+++
.........................+++
writing new private key to 'myPrivateKey.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:IN
State or Province Name (full name) []:Maharashtra
Locality Name (eg, city) [Default City]:Pune
Organization Name (eg, company) [Default Company Ltd]:Avaya
Organizational Unit Name (eg, section) []:Avaya
Common Name (eg, your name or your server's hostname) []:mihir-
edp-3-2-113.platform.avaya.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:Avaya
-----BEGIN CERTIFICATE REQUEST-----
MIIC3TCCAcUCAQAwgYExCzAJBgNVBAYTAklOMRQwEgYDVQQIDAtNYWhhcmFzaHRy
YTENMAsGA1UEBwwEUHVuZTEOMAwGA1UECgwFQXZheWExDjAMBgNVBAsMBUF2YXlh
MS0wKwYDVQQDDCRtaWhpci1lZHAtMy0yLTExMy5wbGF0Zm9ybS5hdmF5YS5jb20w
```

```
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDYhtdcZybDwYG5lzMy8U2D
V+iAZWIQ8JWldhb45I8raEXxPOFg6CHaXNX9b6VShJuHVswRqSpgDB7RSWzQoF4B
oBnKHPY9JIo3v+iMyfKwEuyXQEYMsN3e3TYleMQzRiCGpsM7BvkVrTLrXb9MdEeK
s8NFUwSbWj4Y4X/zJcy9Ebm60btWQAYvzM9X5KHNKU2i33hgxm0IbKe67hQFs+5c
Yaa8kv4Iu2ZkDHpIQiWNpRjzPrOdYmO+iYIqXKKGeQZgJIuE8vTtW4WE9DMulQm6
ct1YQzNCLirgSSgugBWepZTgkgg7BfmiwI7d0jhfxCfzX2BdRjPAxmaj58Z4nhVL
AgMBAAGgFjAUBgkqhkiG9w0BCQIxBwwFQXZheWEwDQYJKoZIhvcNAQEFBQADggEB
AK50mhlS0UJJo1vGb0pnAwVGx4f49+2ERFSPlRzd91fOMrN+Dc94cUuhPUzgU6/E
WUCJFc4tqbk07BEwqITMUDETd7Ki3K+zJoz4ncxVrs1F+AZDQcfG3gHC+EZmaKMb
4XeYI+9qnzmNXiFSM2yprHuEXm7TdAj+OwD2b2mHklSSiHMgxb8aTqCkzCHEfx4u
vYHPiKmoaAH/EEYAmbmYXKND7kOPFsS1TYx8uvVg6RxPFbD5JE+amddX/e8OMJI4
SOXzmgVusQ3G3Rz541tyfqGuRfxNuTMFLznDwWH+T5XgHePLksK+B+RhBQfJR/Eh
MPfuTLHLLtYglXPW4VkNcls=
-----END CERTIFICATE REQUEST-----


# ls -l
total 4
-rw-r--r-- 1 root root 1700 Jul 27 17:37 myPrivateKey.key
```

Generating a certificate signing request (CSR)

About this task

Use this method after you have created a private key using command in the "Generating a private key" section or if you already have a private key that you would like to use to request a certificate from a CA. This section deals with generating a CSR that can be sent to a CA to request the issuance of a CA-signed SSL certificate. If your CA supports SHA-2, add the -sha256 option to sign the CSR with SHA-2.

Procedure

1. Run the following command: `openssl req -key` *`my-private-key-file.key`* `-new -out` *`csr-file.csr`*.

   This command creates a new CSR based on an existing private key.

   The -key option specifies an existing private key that will be used to generate a new CSR. The -new option indicates that a CSR is being generated.

2. Enter the information in the CSR information prompt to complete the process.

Example

```
# openssl req -key myPrivateKey.key -new -out myCsr.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:IN
State or Province Name (full name) []:Maharashtra
Locality Name (eg, city) [Default City]:Pune
Organization Name (eg, company) [Default Company Ltd]:Avaya
Organizational Unit Name (eg, section) []:Avaya
Common Name (eg, your name or your server's hostname) []:mihir-
```

```
edp-3-2-113.platform.avaya.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:Avaya


# ls -l
total 8
-rw-r--r-- 1 root root 1070 Jul 27 17:45 myCsr.csr
-rw-r--r-- 1 root root 1700 Jul 27 17:37 myPrivateKey.key
```

Replacing a System Manager signed identity certificate with Cluster IP/FQDN

About this task

Use this procedure to replace the default System Manager signed Identity certificate with a new one having Cluster IP or Cluster FQDN added as Subject Alternative Name (SAN).

Procedure

1. On System Manager, click **Services** > **Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an element and click **More Actions** > **Configure Identity Certificates**.
4. On the Identity Certificates page, select the certificate that you want to replace.
5. Click **Replace**.
6. On the Replace Identity Certificate page, click **Replace this Certificate with Internal CA Signed Certificate**, and perform the following steps:
   a. Select the check box and type the common name (CN) that is defined in the existing certificate.
   b. Select the key algorithm and key size from the respective fields.

      Note:

      System Manager uses the SHA2 algorithm for generating certificates.

   c. In **Subject Alternative Name** field, select the check box, and perform the following:
      - In the **DNS Name** field, select the check box and enter the values. Enter the FQDN for both security IP and Cluster IP separated by a comma.
      - In the **IP Address** field, select the check box and enter the values. Enter both security IP and Cluster IP separated by a comma.

Note:

In both these fields, you can enter more values separated by a comma.

d. To replace the identity certificate with the internal CA signed certificate, click **Commit**.

e. Restart the service for which you replaced the certificate.

Chapter 13: User Interface description

Attribute Configuration field descriptions

Use this page to configure global attributes for a service, to configure attributes for a service within a service profile, or to configure attributes for a cluster.

Service Profiles tab

Use the fields on this tab to define values for attributes for a specific, selected Service Profile. The values that you specify in this tab overrides the default values specified in the cluster and global attributes.

Name	Description
Profile	The name of the service profile that will use the attributes configured on this page.
Service	A drop-down list of the services that are currently assigned to the selected profile.
Name	The names of the attributes that can be configured for this service.
Override Default	A check indicates you want to override the default value of the attribute. If the box is not checked, the default value is used.
Effective Value	If you override the existing value in this tab, the **Effective Value** displays the value you entered. Else the value displays the first of these to be set: the override value on the **Service Clusters** tab, the override value on the **Service Globals** tab or the default if there are no overrides.
Description	A description of the attribute.

Note:

If you override an attribute for a service at the cluster level for two different clusters, and the override is not at the service profile level, the system does not display the effective value. Instead the system displays the message *Effective value for the attribute cannot be displayed as it has been overridden for multiple clusters*.

Service Clusters tab

Use this tab to define the service attributes of the services installed on specific clusters. The values you specify in this tab will override the default values specified in the global service attributes.

Name	Description
Cluster	The name of the cluster that will use the attributes configured on this page.
Service	A drop-down list of the services that are currently assigned to the selected cluster.
Name	The names of the attributes that can be configured for this cluster.
Override Default	A check indicates you want to override the default value of the attribute. If the box is not checked, the default value is used.
Effective Value	If you override the existing value in this tab, the **Effective Value** displays the value you entered. Else the field either displays the override value on the **Service Globals** tab, or the default if there are no overrides.
Description	A description of the attribute.

Service Globals tab

Use this tab to define the service attributes of all the service profiles that use this service. When you install a service for the first time, the factory default value is used for each attribute of the service profile. Override the factory default value by using the **Service Globals** tab. You can override the service attribute values either at the service profile level or at the cluster level by configuring the attributes in the respective tabs.

Name	Description
Service	A drop-down list of the services you can select for which you can configure attributes.
Name	The names of the attributes that can be configured for this service.
Override Default	Select the check box to override the default value of the attribute. If the box is not checked, the default value is used.
Effective Value	If you override the existing value in this tab, this field displays the value you entered. Otherwise the system displays the default value.
Description	The description of the attribute.

Buttons

Button	Description
Cancel	If you navigated to this page from the Service Profile Editor page, clicking cancel returns you to that page. Otherwise, it resets the page forms and selections.
Commit	Saves changes made to both tabs of the Attribute Configuration page.

Related links

Configuring snap-in attributes at the global level on page 35
Configuring snap-in attributes at the service profile level on page 33

Authorization Configuration field descriptions

This page allows you to administer authorization clients, resources and authorization service instances.

Clients tab
Fields:

Name	Description
Name	Name of the Authorization Client.
ID	The Authorization Client ID.
Cluster Name	Name of the cluster on which the Authorization Client is installed.
Type	The type of Authorization Client: Authorization Client Snap-in or external application.

Buttons:

Name	Description
Edit Grants	Assigns authorization grants to the Authorization Clients.
Edit Key	Assigns an unique key to the external Authorization Client.
New	Creates an external Authorization Client. This option is unavailable for Authorization Client Snap-ins. Authorization Client Snap-ins are available as pre-loaded snap-ins.
Delete	Deletes an external Authorization Client. This option is disabled for Authorization Client Snap-ins.

New External Authorization Client field descriptions

This page allows you to create a new External Authorization Client.

Name	Description
Name	Name of the external Authorization Client.
Certificate	Adds external Authorization Client certificate.

Edit Grants for Authorization Client field descriptions

This page allows you to administer grants for an Authorization Client.

Fields:

Name	Description
Resource Name	Name of the Resource Server that authorizes the Authorization Client.
Resource Cluster	Name of the cluster on which the Resource Server is installed.
Feature	Features assigned to the Authorization Client.
Values	Values configured to the features.

Buttons:

Name	Description
New	Creates an Authorization Grant.
Edit values	Edits values of the Authorization Grant.
Delete	Deletes an Authorization Grant.

Create Grant for Authorization Client field descriptions

This page allows you to create or edit an Authorization Grant.

Name	Description
Resource Name	Name of the Resource Server that authorizes the Authorization Client.
Resource Cluster	Name of the cluster on which the Resource Server is installed.
Feature	Grants or features assigned to the Authorization Client.
Values	Values configured to the features.

Resources servers tab

Fields:

Name	Description
Resource Name	Name of the Resource Server that authorizes the Authorization Client.
Resource Cluster	Name of the cluster on which the Resource Server is installed.

Buttons:

Name	Description
View Authorized Client	Displays the Authorization Clients authorized by the Resource server.
Configure Features	Allows you to configure feature for the selected resource.

View Authorized Clients of Resource Server field descriptions

Name	Description
Resource Name	Name of the Resource Server that authorizes the Authorization Client.
Resource Cluster	Name of the cluster on which the Resource Server is installed.
Type	
Feature	Grants or features assigned to the Authorization Client.
Values	Values configured to the features.

Configure features field descriptions

This page allows you to configure feature values of the selected resource.

Name	Description
Select Feature	Features assigned to the Resource Server.

Service instances tab

Fields:

Name	Description
Name	Name of the Authorization Service.
Cluster Name	Name of the cluster on which the Authorization Service is installed.

Button:

Name	Description
Edit Key	Displays or regenerates key for the Authorization Service.

Edit Keys for Authorization Service field descriptions

This page allows you to view or regenerate key for the Authorization Service.

Name	Description
Regenerate Keys	Displays or regenerates key for the Authorization Service.

Authentication Instance tab

Name	Description
Authentication Mechanism Type	The authentication mechanism: LDAP or SAML.

Button	Description
Change Authentication Mechanism	Changes the authentication mechanism to LDAP or SAML.

Avaya Breeze™ Instance Editor field descriptions

Use this page to create a new Avaya Breeze™ instance, or to edit the properties of an existing instance.

Name	Description
SIP Entity	The name of the Avaya Breeze™ SIP entity. For a new instance, select the SIP entity from the pull-down menu. For information about how to create the SIP Entity, see *Deploying the Avaya Breeze™*. **Note:** You can edit the IP address of the SIP entity only from the **Routing** > **SIP Entity Administration** page.
Description	Your description of the Avaya Breeze™ SIP entity.
UCID Network Node ID	The unique, numeric node ID that is assigned to each Avaya Breeze™ server provisioned. As part of the Avaya Aura architecture, Avaya Breeze™ will add a Universal Call ID (UCID) on calls. The nodes that generate the UCIDs must have a unique node ID assigned to them.
Management Network Interface: **FQDN or IP Address**	The IP Address of the Avaya Breeze™ Management Network Interface. This is the same IP address entered during OVA deployment. For more information, see *Deploying the Avaya Breeze™*.
Security Module:	The IP address of the Avaya Breeze™ Security Module.

Table continues…

Name	Description
SIP Entity IP Address	
Network Mask	The Network Mask of the Avaya Breeze™ Security Module.
Default Gateway	The Default Gateway of the Avaya Breeze™ Security Module.
Call Control PHB	The Call Control PHB value for the Avaya Breeze™ instance. Valid entry can range between 0 to 63. The default value is 34. Call Control PHM provides scalable service discrimination in the Internet without per-flow state and signaling at every hop.
VLAN ID	The VLAN ID of the Avaya Breeze™ Security Module.

Avaya Breeze™ Instance Status field descriptions

Use this page to check the status of the service for each Avaya Breeze™ instance and to see which Service Profiles include this service.

Service Status tab

Name	Description
Name	The name of the Avaya Breeze™ instances that are associated with the service.
Service Install Status	The status of the service on the listed Avaya Breeze™ instance.
Details	A description of any problems the service is having with running on the Avaya Breeze™ instance.
Last Audit	The time and date of the last successful service install audit.

Service Profiles Summary tab

Name	Description
Service Profiles	The names of the Service Profiles that include this service.

Related links

Installing the snap-in on page 35

Backup and Restore field descriptions

Use this option to backup and restore a cluster.

Name	Description
Backup	Starts the backup process on the selected cluster.
Restore	Starts the restore process.
Configure	Configures the backup server location.
Job Status	Displays the status of the backup or restore operations.
Cancel	Cancels the pending and in-progress jobs.
Purge	Purges the completed backups.

Backup and Restore Status field descriptions

Name	Description
Backup Host	Host name or IP address of the backup server.
Directory	The directory location where backup files are stored on the backup server.
Retained Copies	The number of backup file copies retained on the backup location.
Cluster	The name of cluster that the backup was taken on or being restored to.
Operation	The current operation: backup or restore.
Time Requested	The time the operation was requested.
Time Initiated	The time the operation was initiated.
Time Completed	The time the operation was completed.
Service	The name of the service.
Database	The name of the database.
Schema Version	The version of database schema.
Size	The size of backup.
Status	The status of operation.
Disposition	The status disposition.
File Name	The file name of backup directory.
Server Path	The path on the server where backup is stored.
Backup Cluster	For restore operations, the name of cluster that the backup was taken on.

Backup Storage Configuration field descriptions

Use this page to configure the backup storage location.

Name	Description
FQDN or IP Address	The FQDN or IP address of the SSH server.
Login	The login ID that has SSH privileges and can gain access to the server.
Password	The password associated with the login ID.
SSH Port	The SSH port of the backup server.
Directory	The directory location where the backup files are stored on the backup server.
Retained backup copies per cluster per snap-in DB	The maximum number of backup file copies to retain on the backup location. If no value is specified, then all backup files are retained.

Button descriptions

Name	Description
Commit	Makes the configuration changes to the database.
Test Connection	Tests the SSH connection, directory access for the login and write/delete permissions.
Cancel	Does not make the configuration changes to the database.

Bundles field descriptions

Name	Description
Name	The names of all bundles that have been loaded to the System Manager database.
Version	The version number of the bundle.
Type	The deployment type: • For bundles, the system displays **Bundle**. • For services, workflows, and tasks, the system displays the deployment type, such as **Java**, **Workflow**, or **Task**.
State	Indicates the installation status of the bundle in the format: `x of y`, where *y* denotes the total number of clusters and *x* denotes the number of clusters on which the bundle is installed.

Table continues…

Name	Description
	When you click the State link, the system displays the Bundle Installation Status window which shows the status of the bundle installation on each cluster: • **Unknown**: The bundle installation status could not be obtained from the cluster. One or more servers in the cluster are not reachable or the cluster is empty. • **Partial**: Some of the services of the bundle or their dependencies are already installed on the cluster. Installing the bundle on the cluster will only install the services which are not currently installed. • **Failed**: Installation of one or more services of the bundle or their dependencies has previously failed on the cluster. Installing the bundle on the cluster will only install the failed ones. • **Not Installed**: The bundle is not installed on the cluster. • **Installed**: The bundle is completely installed on the cluster. The system displays one of the following icons: • Green check mark: Indicates that the bundle is installed. • Yellow exclamation icon: Indicates that the bundle is either queued for installation or for downloading to Avaya Breeze™. If downloading to Avaya Breeze™ fails, the column displays a red cross with the Transfer has failed message. • Red cross icon: Indicates that the bundle has failed to initialize, run, or deploy.
License Mode	The license mode of the services in the bundle. This field is only applicable to the services in the bundle. The possible license modes are: • **Not Applicable**: The value displayed in field for services which do not enforce or use licensing. • ✔ **License Normal Mode**: The bundle has a valid license file for normal operation of the bundle. License errors are not present.

Table continues…

Name	Description
	• **License Error Mode**: License error is seen in this mode. There is a thirty day grace period when the license in not loaded on System Manager. • **Snapins in this bundle will get uninstalled after 30 day grace period**: You must install a valid license file for the bundle to get it back to the normal mode. This column displays the grace period when the bundle is in the error mode. After the grace period expires, the bundle enters the restricted mode. • **License Restricted Mode**: The bundle has exceeded the license grace period. If you do not install a valid license file, the bundle is uninstalled from the Avaya Breeze™ clusters. The element manager raises a critical alarm. If you install the license file the bundle returns to the License Normal mode. You must manually re-install the bundle to any cluster from which the bundle was uninstalled.
Avaya Signed	Indicates whether the services in the bundle are Avaya signed. This field is only applicable to the services in the bundle. The column displays a green tick mark if the service is signed by Avaya. Else, the column displays **Not Signed**.

Name	Description
Load	Launches the Load Bundle window so you can browse to the location of a bundle and load it.
Install	Queues up the selected bundle to be installed on all the selected clusters. Depending on the number of Avaya Breeze™ nodes in these selected clusters, it may take a few minutes to install on all instances.
Uninstall	Uninstalls the selected bundle from the selected clusters. User is prompted to select between force uninstall or otherwise. A force uninstall terminates all active connections immediately. Not checking this will cause the bundle to wait for all active connections to drop before uninstalling the bundle.
Delete	Deletes the selected bundle. An **Installed** bundle can not be deleted. It must first be uninstalled. **Caution:** Deleting the last version of a bundle completely deletes all attribute settings and

Table continues…

Name	Description
	profile configuration of that bundle from the system.

Bundle Details and Installation Status

The system displays this page when you click the link in the bundle name on the Bundles page. This page displays the services in the bundle, dependencies of the services, and the installation status of the services and dependencies.

Services in Bundle and Dependencies Table field descriptions

The system displays the details in the Dependencies table when you click the link in the service name in the Services in Bundle table.

Name	Description
Name	The names of all services or dependencies that have been loaded to the System Manager database.
Version	The version number of the service or dependency.
Type	The service or dependency deployment type.
State	Indicates the service or dependency installation state. The system displays the details in the Installation Status table when you click the link in the service or dependency **State** column in the Services in Bundle or Dependencies table.
License Mode	The license mode that the service or dependency is currently in. The possible license modes are: • **Not Applicable**: The value displayed in field for services or dependencies that do not enforce or use licensing. • **License Normal Mode**: The service or dependency has a valid license file for normal operation. License errors are not present. • **License Error Mode**: License error is seen in this mode. There is a thirty day grace period when the license in not loaded on System Manager.

Table continues…

Name	Description
	• **License Restricted Mode**: The service or dependency has exceeded the license grace period. If you do not install a valid license file, the service or dependency is uninstalled from the Avaya Breeze™ clusters. The element manager raises a critical alarm. If you install the license file, the service or dependency returns to the License Normal mode. You must manually re-install the service or dependency.
Avaya Signed	Indicates whether the service or dependency is Avaya signed. The column displays a green tick mark if the service or dependency is signed by Avaya. Else, the column displays **Not Signed**.

Installation Status field descriptions

The system displays the details in the Installation Status table when you click the link in the **State** column in the Services in Bundle or Dependencies table.

Name	Description
Name	Name of the Avaya Breeze™ instance.
Cluster name	Name of the cluster on which the service is installed.
Service Install Status	Installation status of the service on the Avaya Breeze™ instance in the cluster.
Details	Description of any problems the service is having with running.
Last Audit	The time and date of the last successful service install audit.

Cluster administration field descriptions

Name	Description
Details	The details of the cluster. You can view the Avaya Breeze™ instances and services assigned to the cluster.
Cluster Name	The unique name of the cluster.
Cluster Group	The group number that you assign to the cluster. You can enter a value from 1 to 10.

Table continues…

Name	Description
	This optional field is used only to configure attributes for multiple snap-ins.
Cluster IP	The IP address of the cluster. The **Cluster IP** value is applicable only for HTTP/HTTPS. **Note:** Do not assign a **Cluster IP** for a single-node cluster.
Cluster FQDN	The unique FQDN that you assign to the cluster.
Cluster Profile	The type of cluster. The options are: • **Context Store** • **Core Platform** • **Engagement Assistant Speech** • **General Purpose** • **General Purpose Large** • **Work Assignment** • **Customer Engagement**
Cluster State	The state of the cluster. The options are: • **Accepting**: The cluster can serve service requests. • **Denying**: The cluster cannot serve services or calls. **Note:** The **Cluster State** field displays **Accepting** if any of the reachable nodes in the cluster is in the **Accepting** state. If all the reachable nodes in the cluster are in **Deny New Service** mode, the **Cluster State** field displays **Denying**.
Alarms	The number of alarms for the cluster. This value is displayed in the following format: *<critical + major alarm count>/<minor alarm count>/<warning alarm count>*.
Activity	The sum of active calls, HTTP sessions, and other custom-defined sessions of all snap-ins installed on the Avaya Breeze™ servers in the cluster.

Table continues…

Name	Description
Cluster Database	The High Availability status between the active Avaya Breeze™ server and the standby Avaya Breeze™ server in a cluster. This field displays: • A green background when the connection between the active and the standby servers is up. • A yellow background when the standby server is getting ready to take over if the need arises. • A red background when the connection between the active and the standby server is nonfunctional. • No background color and **Disabled** when the cluster database is disabled. The **Cluster Database** displays: • The number of active components and the disk consumption in the following format: *<number of active connections>/<disk consumption>*. • **A series of dashes (- - - -)** if the server does not report the disk consumption. • **Disabled** if the cluster database is disabled.
Data Replication	The aggregated data replication status between all Avaya Breeze™ servers in a cluster and System Manager. The field displays: • A green check mark (graphic) when the replication is successful. • A red cross (graphic) icon when one or more node replication has failed.
Service Install Status	The aggregated service installation status of all the Avaya Breeze™ servers in a cluster. The field displays: • A green check mark when all snap-ins are installed. • A yellow exclamation mark when the snap-in is either queued for installation or for downloading to Avaya Breeze™. • A red cross icon when one or more snap-ins have failed to initialize, run, or deploy.
Tests Pass	The aggregated maintenance test result for all Avaya Breeze™ servers in the cluster. A green check mark indicates that all Avaya Breeze™ servers in the cluster have passed the maintenance tests.

Table continues…

Name	Description
Data Grid Status	The aggregate status of the data grid in the cluster. The field displays: • A green check mark when the data grid status is up. • A yellow exclamation mark when the status of one or more servers in the cluster is down. • A red cross icon when the data grid status is down.
Overload Status	The overload status of the Avaya Breeze™ cluster. The field displays: • A green check mark when none of the servers in the cluster are in the overloaded state. • A red cross icon when one or more servers are in the overloaded state.
Service URL	The list of cut-through URLs for the services installed on the Avaya Breeze™ cluster. If you have administered the cluster IP, it is used as the host for the URL. If not, one of the Avaya Breeze™ server IP address is used as the host for the URL.

Server details

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

Name	Description
Server Name	The name of the Avaya Breeze™ server.
Security Module	The status of the security module for the server.
Server Version	The version of the Avaya Breeze™ server.
Server State	The state of the server: • Accepting • Denying
Alarms	The number of alarms for the server. This value is displayed in the following format: *<critical + major alarm count>/<minor alarm count>/<warning alarm count>*.
Activity	The sum of active Call, HTTP session, and other custom-defined sessions of all the snap-ins installed on the Avaya Breeze™ server.

Table continues…

Name	Description
Cluster Database	The state of the server in a High Availability database setup. This field displays: • A Green background when the active server, standby server, and the idle server are ready. • A yellow background when the standby server is preparing. • A red background when the active server and the standby server fail. • No background and **---** when cluster database is disabled.
Cluster Database Connection	The status of the connection between the active server and the standby server in a high availability database scenario. This field displays: • A green check mark when the connection between the active and the standby servers is up. • A yellow exclamation mark when the standby server is getting ready to take over if the active server goes down. • A red cross when that the connection between the active and standby servers is down. • No background color and **---** when the cluster database is disabled.
Data Replication	The status of data replication between the Avaya Breeze™ server and System Manager. This field displays: • A green check mark when the replication is successful. • A red cross when the replication failed.
Service Install Status	The service install status for the Avaya Breeze™ server. This field displays: • A green check mark when all the snap-ins are installed. • A yellow exclamation mark when the snap-in downloading to Avaya Breeze™ is in progress. • A red cross icon when one or more snap-ins failed to initialize, run, or deploy.
Tests Pass	The maintenance test result for the Avaya Breeze™ server.

Table continues…

Name	Description
Data Grid Status	The data grid status of the Avaya Breeze™ server: • **Up** • **Down**
Overload Status	The overload status of the Avaya Breeze™ server. This field displays: • A green check mark when the server is not overloaded. • A red cross icon when the server is in an overloaded state.
Last Reboot Status	The status of the last cluster reboot operation.

Button	Description
New	Adds a new Avaya Breeze™ cluster.
Edit	Displays or modifies the Avaya Breeze™ cluster attributes or modifies the cluster profile.
Delete	Deletes the Avaya Breeze™ cluster. You cannot delete legacy clusters.
Certificate Management > **Install Trust Certificate (All Avaya Breeze™ Instances)**	Opens the Install Trusted Certificate page, where you can download a trusted certificate to install Avaya Breeze™ servers in a cluster.
Cluster State > **Accept New Service**	Allows incoming calls and requests for the cluster that you select.
Cluster State > **Deny New Service**	Blocks incoming calls and requests for the cluster that you select.
Backup and Restore > **Backup**	Starts the backup process on the selected cluster.
Backup and Restore > **Restore**	Starts the restore process.
Backup and Restore > **Configure**	Configures the backup server location.
Backup and Restore > **Job Status**	Displays the status of the backup or restore operations.
Backup and Restore > **Cancel**	Cancels the pending and in-progress jobs.
Backup and Restore > **Purge**	Purges the completed backups.
Reboot	Reboots all Avaya Breeze™ nodes in the server cluster simultaneously.
Filter: Enable	Enables filtering of clusters on the basis of the cluster name, IP address, profile, state, alarms, and activity.
Refresh icon	Refreshes the values in the **Cluster Administration** table.

Icon	Description
	Indicates that the server is one of the lookup servers.
	Indicates that the server is the active load balancer.
	Indicates that the server is the active load balancer, but it is unable to connect to the standby server.
	Indicates that this server is the standby load balancer.
	Indicates that the load balancing server is: • Transitioning over to the standby server. • Experiencing a connection failure. • In an error state.
A	Indicates an active cluster database.
S	Indicates a standby cluster database.

Cluster DB Backup field descriptions

Backup section

Name	Description
Service	The service assigned to the cluster.
Database	The name of the cluster database.
Schema Version	The version of the database schema.

Job schedule section

Name	Description
Backup Password	The password for scheduled backup jobs.
Schedule Job	Configures a schedule for backup jobs. You can choose between: • **Run immediately** • **Schedule later**: If you select this option, you must choose the time for the schedule. Optionally, you can also choose a recurring schedule.
Task Time	The time when scheduled backup job starts.

Table continues…

Name	Description
Recurrence	Creates a recurring backup schedule. You can choose between: • **Execute task one time only** • **Tasks are repeated**: If you select this option, you must choose the duration when the recurring backup repeats.
Range	Creates a range for the recurring backup schedule. You can choose between: • **End after**: If you select this option, you must choose the number of times that the backup schedule repeats. • **End By date**

Scheduled Backup Job Status section

Name	Description
Cluster	The name of the cluster.
Service	The service assigned to the cluster.
Database	The name of the cluster database.
Start Time	The time when scheduled backup job starts.
Recurrence	The recurring schedule of the backup job.
Status	The status of the backup job.
Job Name	The name of the backup job.

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

Table continues…

Name	Description
	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. • **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

Table continues…

Name	Description
	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.

Table continues…

Name	Description
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.
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.

Table continues…

Name	Description
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 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.

Table continues…

Name	Description
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.
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

Table continues…

Name	Description
	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 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.

Table continues…

Name	Description
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.
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.

Button	Description
	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.

Destination Status field descriptions

Name	Description
Destination Name	Name of the destination.
Type	Type of the destination: Queue or Topic.
Enqueue Message Count	The number of messages added to the destination.
Dequeue Message Count	The number of messages removed from the destination.
Consumers count	Number of consumers associated of the destination.

Buttons:

Name	Description
Group	Enables selecting a Reliable Eventing group for which the destination status is to be displayed.
Delete	Deletes a destination.

Event catalog configuration field descriptions

Name	Description
Family	The family to which the event belongs.
Family Display Name	The name of the Event Catalog family as it is displayed in the Avaya Engagement Designer.

Table continues…

Name	Description
Type	The type of the event.
Type Display Name	The name of the Event Catalog type as it is displayed in the Avaya Engagement Designer.
Version	The version of the event.
Schema Name	The name of the event schema. You can use the same schema for multiple event types.
Schema Type	The schema type. JSON is supported for this release.

Button	Description
View	Displays the details of the event.
Edit	Displays the edit custom event page for you to edit the details of the event.
New	Creates a new event.
Delete	Deletes a custom event.

Event Catalog Editor field descriptions

Name	Description
Family	The family to which the event belongs. The default families include Call Events, System Events, and Eventing Framework Events.
Family Display Name	The name of the Event Catalog family as it is displayed in the Avaya Engagement Designer.
Type	The type of the event. The type name must be unique within a family.
Type Display Name	The name of the Event Catalog type as it is displayed in the Avaya Engagement Designer.
Version	The version of the schema.
Schema Name	The name of the schema.
Schema Type	The schema type. JSON is supported for this release.
Schema	The schema for the default or the custom event.

Button	Description
Commit	Adds an event or edits the changes to a custom event.

HTTP Security field descriptions

Use this page to configure access permissions for HTTP requests to Avaya Breeze™.

Name	Description
Cluster	If you select a cluster from the **Cluster** drop-down list on HTTP Security page, the system lists all the configured hosts for the Whitelist tab and the HTTP CORS tab if any. If you configure any new hosts for selected cluster, the new hosts will be applicable only for the Avaya Breeze™ for that cluster. **Note:** The **Legacy** option shown in the **Cluster** drop-down list can be used to administer the existing configured Whitelist and HTTP CORS for Avaya Breeze™ Release 3.1 or earlier. For Legacy clusters on Avaya Breeze™ Release 3.1 or earlier, the configured trusted hosts for other clusters (white-list) will also be applicable as trusted hosts.

Whitelist tab

Name	Description
Whitelist Enabled	If you select this check box, Avaya Breeze™ for the selected cluster accepts HTTP or HTTPS requests only from the IP Addresses listed in the table. If you do not select this check box, Avaya Breeze™ for the selected cluster accepts any HTTP or HTTPS request that passes the optional client certificate challenge.
Client Certificate Challenge Enabled	If you select this check box, Avaya Breeze™ for the selected cluster accepts an HTTPS request only when a valid client certificate is presented. The client certificate must be signed by a trusted certificate authority.
Host Address	An IP address from which Avaya Breeze™ for the selected cluster will accept HTTP requests when Whitelist Enabled is checked.
Subnet Bits	The subnet bits used when a range of clients need to access Avaya Breeze™ for the selected cluster through HTTP. Subnet bits vary based on the value in the **IP Address** field.

HTTP CORS tab

Name	Description
Allow Cross-origin Resource Sharing for all	Select this check box to enable cross-origin resource sharing, where any JavaScript from any application server can send HTTP or HTTPS requests to Avaya Breeze™ for the selected cluster. You must use this setting only in the lab environment.
Host Address	The authorized IP addresses or domain names that generate HTTP requests to Avaya Breeze™ for the selected cluster using JavaScript.

Button	Description
New	Adds an IP address or a domain name.
Delete	Marks the selected IP addresses or domain names for deletion.

Related links

Administering a whitelist for HTTP Security on page 68

Implicit User Profiles field descriptions

Use Implicit User Profiles to assign groups of users to a service profile whether or not they are explicitly administered on System Manager . This allows you to invoke call intercept snap-ins for non-SIP users without adding them as users on System Manager.

Name	Description
Service Profile	The name of the Service Profile used to invoke call intercept snap-ins for this group of implicit users.
Pattern	The pattern as defined for Session Manager and Communication Manager digit routing. The range includes users to add to the Service Profile.
Min	The minimum number of digits to be matched from the pattern. Value is auto-populated based on the pattern.
Max	The maximum number of digits to be matched from the pattern. Value is auto-populated based on the pattern.
Desc	A description of the rule, typically a description of the group of users the rule defines.

Button	Description
Edit	Modifies the selected Implicit User Profile Rule.
New	Creates a new Implicit User Profile Rule.
Delete	Deletes the selected Implicit User Profile Rule.

Implicit User Profile Rule Editor field descriptions

Use the Implicit User Profile Rule Editor page to define the dialing pattern parameters of the implicit users who are to be assigned to a Service Profile.

Name	Description
Service Profile	The name of the Service Profile used to invoke call intercept snap-ins for this group of implicit users.
Pattern	The pattern defined as Implicit Users in Session Manager. The Service Profile is linked with this pattern for call-intercept snap-in invocation. For non-SIP users, the dial pattern should be the same pattern format as used in the Routing Policy Dial pattern. For SIP users, as a best practice use E.164 patterns to scope the SIP users either singularly or as a range. If that is not desired, use the Communication Address defined on **User** > **User Management** > **Manage Users** User Profile **Communication Profile** tab. Enter “x” patterns at the end of the string as wildcards to match multiple users. The pattern range can include both SIP and non-SIP users.
Min	The minimum number of digits to be matched from the pattern. Value is auto-populated based on the pattern.
Max	The maximum number of digits to be matched from the pattern. Value is auto-populated based on the pattern.
Desc	A description of the rule, typically a description of the group of users the rule defines.

Button	Description
Commit	Saves new profile or changes to the existing profile.

Related links

Assigning a Service Profile to implicit users on page 51

Install Trusted Certificate field descriptions

Use this page to retrieve a trust certificate that will be used for all the Avaya Breeze™ clusters listed on the Cluster Administration page.

Name	Description
Select Store Type to install trusted certificate	Lists the different locations where the trusted certificate can be applied.
Please select a file	The trust certificate you have selected.

Button	Description
Browse	Click to browse to the location where the trusted certificate is stored.
Retrieve Certificate	Click to retrieve the certificate and view the certificate details on this page.

JDBC provider field descriptions

Name	Description
Name	The name of the resource provider.
Class	The name of the class file.
Jar	The JDBC jar file or library that you have uploaded.
Desc	The description of the resource provider as specified in the configuration page.

Button	Description
Edit	Edits the JDBC provider details.
New	Adds a new JDBC provider resource.
Delete	Deletes the JDBC provider that you select.
Filter: Enable	Filters the JDBC providers according to name, class, jar, or description.

JDBC Provider Editor field descriptions

Name	Description
Provider	The name of the JDBC provider

Table continues…

Name	Description
Class Name	The name of the class file in the jar.
Select Jar File	The jar file that contains the JDBC drivers. Select **Browse...** to upload the jar file from your local computer. **Note:** Verify the jar file before uploading it. Verify the file using the command `jar tf <filename of the jar file>` or by opening the jar file using WinZip.
Description	The description for the JDBC provider.

Button	Description
Commit	Adds the JDBC provider or saves the changes to the JDBC configuration.
Cancel	Cancels the add or edit action.

JDBC data source field descriptions

Name	Description
Name	The name of the data source.
Cluster	The cluster with which the data source is associated.
JDBC Provider	The JDBC resource provider used for the data source.
JNDI Name	The JNDI name for the data source.
URL	The database URL for which the data source is created.
Description	The description for the data source.

Button	Description
Edit	Edits the JDBC data source details.
New	Adds a new JDBC data source.
Delete	Deletes the JDBC data source that you select.
Filter: Enable	Filters the data source according to name, cluster, provider resource, JNDI, URL and description.
Test Connection	Displays the success or failure response after you execute a validation query.

JDBC Data Source Editor field descriptions

Name	Description
Name	The name of the JDBC data source.
TLSEnabled	The check box that indicates whether the JDBC data source uses TLS-secured communication.
Cluster	The cluster on which the snap-in using the JDBC data source is installed.
JDBC Provider	The JDBC resource provider used for the data source. Select the JDBC provider from the list of the uploaded JDBC providers.
JNDI Name	The JNDI name for the data source.
URL	The database URL for which the data source is created.
User Name	The database server user name.
Password	The database server password.
Validation Query	The validation query for the data source. This is the query that is tested when you click **Test Connection** for a data source.
Description	The description for the data source.

Custom Properties

Add custom attributes for your data source by using this section. Click the **+** symbol to add an attribute. Click the **-** symbol to delete an attribute.

Name	Description
Name	The name of the custom attribute that you want to add for the data source.
Value	The value for the custom attribute.

Button	Description
Commit	Adds or edits the JDBC data source.
Cancel	Cancels the add or edit action.

Maintenance Tests field descriptions

Use this page to run maintenance tests. For a description of the tests, see *Maintaining and Troubleshooting Avaya Breeze™*.

Name	Description
Select Avaya Breeze™ to test	The name of the Avaya Breeze™ instance that you are testing. Select the instance from the drop-down menu.
Test Description	The name of the maintenance test.
Test Result	Indicates whether the test was successful or failed.
Test Result Time Stamp	When the test completed.

Button	Description
Execute All Tests	Click to run all maintenance tests in the list.
Execute Selected Tests	Click to run only the maintenance tests you have selected from the list.

Media Server Monitoring field descriptions

This page displays the connection status only when Avaya Breeze™ nodes and Avaya Aura® Media Server nodes are in same administered location.

Name	Description
Media Server	The name of the Avaya Aura® Media Server instance.
Overload Status	The status of Avaya Aura® Media Server. This field displays: • A green check mark when Avaya Aura® Media Server is not overloaded. • A red cross icon when Avaya Aura® Media Server is overloaded.
License Mode	The license mode of the Avaya Aura® Media Server instance: • **licensed** • **unlicensed**
Lock Mode	The operation state of Avaya Aura® Media Server: • **locked** • **unlocked**
Authentication	The field indicates whether Avaya Breeze™ is able to authenticate with Avaya Aura® Media Server.
Avaya Breeze Server	The name of the Avaya Breeze™ server.

Table continues…

Name	Description
	The system will not display the value for: • The Avaya Breeze™ servers prior to Release 3.3. • The Avaya Breeze™ servers that are not reachable.
Connection Status	The connection status of Avaya Breeze™ with Avaya Aura® Media Server. This field displays: • A green check mark when Avaya Breeze™ is able to connect with Avaya Aura® Media Server. • A red cross icon when Avaya Breeze™ is unable to connect with Avaya Aura® Media Server. This field displays **Connection Disabled** when the **Select AAMS by Breeze server Location - Priority 2** cluster attribute is selected and the location of Avaya Breeze™ server is different than the location of Avaya Aura® Media Server.

Reliable Eventing Groups field descriptions

Name	Description
Name	Name of the Reliable Eventing group.
Type	Type of Reliable Eventing group: HA or standalone.
Broker 1	Name of the broker assigned to the Reliable Eventing group.
Broker 2	Name of the broker assigned to the Reliable Eventing group.
Status	Status of the Reliable Eventing group.

Buttons:

Name	Description
Edit	Edits a Reliable Eventing group.
New	Creates a Reliable Eventing group.
Delete	Deletes a Reliable Eventing group.

Reliable Eventing Group Editor field descriptions

General tab

Name	Description
Reliable Eventing Group Detail section	
Cluster	The name of the cluster assigned to the Reliable Eventing group.
Group Name	The name of the Reliable Eventing group.
Description	A brief description of the Reliable Eventing group.
Type	The type of the Reliable Eventing group. You can choose between: • **HA**: If you select this option, you must assign minimum three Avaya Breeze™ brokers. • **Standalone**: If you select this option, you must assign minimum one Avaya Breeze™ broker.
Assigned Brokers section	
Name	The name of Avaya Breeze™ server.
Version	The version of the Avaya Breeze™ server.
Description	The description of the Avaya Breeze™ server.
Unassigned Brokers section	
Name	The name of Avaya Breeze™ server.
Version	The version of the Avaya Breeze™ server.
Description	The description of the Avaya Breeze™ server.

Associated clusters tab

Name	Description
Assigned associated clusters section	
Cluster Name	The name of the cluster assigned to the Reliable Eventing group.
Unassigned associated clusters section	
Cluster Name	The name of the cluster not assigned to the Reliable Eventing group.

Server Administration field descriptions

Use this page to:

- Add or edit an Avaya Breeze™ server.

- Shutdown or restart an Avaya Breeze™ server.
- Assign trust and identity certificates to the Avaya Breeze™ servers.
- Access information about the service status and maintenance tests for each Avaya Breeze™ server.

Name	Description
Name	The name of the Avaya Breeze™ server. Click the name to navigate to the Avaya Breeze™ Instance Editor page.
Cluster Name	The name of the cluster to which this Avaya Breeze™ server belongs.
Service Install Status	The status of the installed services. • A green check mark icon indicates all services have been installed. • An orange triangle icon indicates the service is in the process of installing or uninstalling. • A red X icon indicates a service has not downloaded properly or is not installed. Click on an icon to navigate to the **Service Status** page.
Tests pass	Maintenance test result. A green check mark indicates the test or tests passed. A red X indicates a test failed. Click the check mark or X to navigate to the **Maintenance Tests** page.
Alarms	The number of alarms raised for the Avaya Breeze™ server. This value is in the format <critical + major alarm count>/<minor alarm count>/<warning alarm count>.
System State	The current state of the Avaya Breeze™ server. The system states are: • Accepting • Denying
Security Module	The state of the Security Module. The states are Up, Down, and - - - (unknown).
Activity	The sum of active Call, HTTP, and other custom defined sessions of all the snap-ins installed on the Avaya Breeze™ server.
License mode	The license mode of the Avaya Breeze™ server. It is mandatory that all the Avaya Breeze™ servers be in compliance with the license file, including the major release and the total number of Avaya Breeze™ servers.

Table continues…

Name	Description
	The possible license modes are: • **License Normal Mode**: A valid license file is installed. License errors are not found. The complete functionality is present for the Avaya Breeze™ instance. • **License Error Mode**: License error is seen in this mode. The Avaya Breeze™ instance is in a 30 day grace period during this mode. Complete functionality is available during the grace period. The system displays the warning icon along with the date and time of the grace period expiration in the **License Mode** column. • **License Restricted Mode**: The Avaya Breeze™ instance goes in to the restricted mode after the 30 day grace period expires. The Avaya Breeze™ server goes in to the Deny New Service mode. The server automatically returns to service when the server returns to the License Normal mode. For more information on determining and troubleshooting the license errors, see *Maintaining and Troubleshooting Avaya Breeze™*.
Overload Status	The overload status of the Avaya Breeze™ server. • A green check mark indicates that the server is not in an overloaded state. • A red cross icon indicates that the server is in an overloaded state.
Version	The version of the Avaya Breeze™ software that is installed on the Avaya Breeze™ server.
Last Reboot Status	The status of the last cluster reboot operation.

Button	Description
Edit	Edits the selected Avaya Breeze™ server. It launches the Avaya Breeze™ Instance Editor page.
New	Adds a new Avaya Breeze™ server. It launches the Avaya Breeze™ Instance Editor page.
Delete	Deletes the selected Avaya Breeze™ server.
System State > **Accept New Service**	Allows incoming calls or requests for the Avaya Breeze™ server you select.
System State > **Deny New Service**	Blocks incoming calls or requests for the Avaya Breeze™ server you select.

Table continues…

Button	Description
Shutdown System > **Shutdown**	Shuts down the Avaya Breeze™ server you select.
Shutdown System > **Reboot**	Reboots the Avaya Breeze™ server you select.

Icon	Description
	Indicates that the Avaya Breeze™ server is one of the lookup servers.
	Indicates that the Avaya Breeze™ server is the active load balancer.
	Indicates that the Avaya Breeze™ server is the active load balancer, but it is unable to connect to the standby server.
	Indicates that this Avaya Breeze™ server is the standby load balancer.
	Indicates that this load balancing server is: • transitioning over to the standby server • experiencing a connection failure • in an error state
A	Indicates that the Avaya Breeze™ server is the Active server in a cluster database.
S	Indicates that the Avaya Breeze™ server is the Standby server in a cluster database.

Services field descriptions

Use this page to load, install, uninstall, start, stop and delete a snap-in.

Name	Description
Name	The names of all snap-ins that have been loaded to the System Manager database.
Version	The version number of the snap-in. You can not install versions of the same snap-in if the version number is identical.
Preferred Version	The preferred version of a snap-in. In a cluster, if you choose a preferred version of a snap-in, that particular version is used by default. Even if you install a newer version of the snap-in, the preferred version is continued.

Table continues…

Name	Description
State	Indicates if the service is LOADED or INSTALLED. Loaded snap-ins have been loaded to the System Manager database. Installed indicates that a request has been sent to install the snap-in to the Avaya Breeze™ instances. This state is an aggregated state across various clusters. To check the actual status of the service installation, see the **Service Install Status** column on the Avaya Breeze™ Instance Status page.
Deployment Type	The snap-in deployment type. Possible values include Java, Workflow. JDBC Provider is the custom defined type. The deployment type value is stored in the database. You can filter and sort snap-ins based on the deployment type.
License Mode	The license mode that the snap-in is currently in. The possible license modes are: • **License Normal Mode**: The snap-in has a valid license file for normal operation of the snap-in. License errors are not present. • **License Error Mode**: License error is seen in this mode. The snap-in is in the thirty day grace period. There are no restrictions on the functionalities. You must install a valid license file for the snap-in to get it back to the normal mode. This column displays the grace period when the snap-in is in the error mode. After the grace period expires, the snap-in enters the restricted mode. • **License Restricted Mode**: The snap-in has exceeded the license grace period. If you do not install a valid license file, the snap-in is uninstalled from the Avaya Breeze™ clusters. The element manager raises a critical alarm. If you install the license file the snap-in returns to the License Normal mode. You must manually re-install the snap-in to any cluster from which the snap-in was uninstalled. • **Not Applicable**: Many services do not require a license file. The value for these services is **Not Applicable**.
Avaya Signed	Indicates whether the snap-in is Avaya signed. The column displays a green tick mark if the snap-in is

Table continues…

Name	Description
	signed by Avaya. Else, the column displays **Not Signed**. The supplier id for Avaya provided snap-ins is 10000000. The Supplier id uniquely identifies the supplier of a particular snap-in offered through the Avaya Snapp-store. All the snap-ins from a given supplier will have the same Supplier Id. This is mandatory for the snap-ins offered through the Avaya Snapp-store and is optional for other snap-ins.
Log Size(MB)	The total space for the logs of the snap-in declared in the `properties.xml` file. If the total space is not declared, the system displays the default value of **100MB**.

Button	Description
Load	Launches the Load Service window so you can browse to the location of a service and load it. Acceptable services have a file extension of .svar.
Install	Queues up the selected service be installed on all the administered Avaya Breeze™ instances. Depending on the number of instances, it may take a few minutes to install on all instances
Uninstall	Uninstalls the selected service from all the Avaya Breeze™ instances. A dialog will display to ask if you want to force uninstall or not. A force uninstall terminates all active connections immediately. Not checking this will cause the service to wait for all active connections to drop before uninstalling the service.
Delete	Deletes the selected service. An **Installed** service can not be deleted. It must first be uninstalled. **Caution:** Deleting the last version of a service completely deletes all attribute settings and profile configuration of that service from the system.
Set Preferred Version	Sets the preferred version of a service. The preferred version of any service is cluster specific. You can set the same version of a service as the preferred version across several clusters. You can set the preferred version for multiple snap-ins in a single transaction.

Table continues…

Button	Description
Start	Starts or restarts the snap-in. Start snap-in is used after installing a higher version of a snap-in, or after making some configuration changes to the snap-in.
Stop	Stops the snap-in. Stop snap-in is used while installing a higher version of a snap-in.

Related links

Loading the snap-in on page 32
Installing the snap-in on page 35

Service Databases field descriptions

Use this page to view all the service databases with their version, size and status. You can also delete the databases which are not in use.

Name	Description
Service	The name of the snap-in
Database	The name of the service database.
Schema Version	The database schema version.
Size	The size of the database.
In Use	Specifies whether the snap-in is actively using the database.

Button	Description
Cluster	Selects a cluster for which you want to view the service databases. The system displays only those clusters for which you have enabled the **Enable Cluster Database** field.
Delete	Deletes the selected database.

Service Ports field descriptions

Note:

If you modify the port configuration for an Avaya-developed snap-in, you must start and stop the snap-in for the change to take effect.

Name	Description
Service	The list of Avaya-developed snap-ins that have default ports specified. Select the snap-in whose ports you want to configure.
Cluster	The list of clusters that are available.

Selected Service Ports

Name	Description
Port Name	The name of the assigned ports for the snap-in.
Override Default	Select this check box to override the default port value that is assigned to the snap-in.
Effective Port Value	The effective port value. When you specify an override value, that value becomes the effective port value.
Description	The description for the assigned ports.

All Service Used/System Reserved Ports

The table lists all the assigned ports for all the Avaya-developed snap-ins, both at the snap-in level and cluster level.

Name	Description
Port Name	The name of the port that is assigned to the snap-in.
Port Number	The port number of the port that is assigned to the snap-in.
Default Port Number	The default port number that is assigned to the snap-in.
Port Type	The port type. This port type can be **snapin** or **reserved**.
Service	The snap-in for which you have configured the ports.
Cluster	The cluster in which the snap-in with the assigned port is installed. If the port is assigned at the snap-in level, this field is blank.
Description	The description for the reserved or assigned port.

Button	Description
Commit	Assigns the port you have chosen to the snap-in.
Cancel	Cancels the port configuration action.

Service Profile Configuration field descriptions

Use this page to create, edit or delete a Service Profile.

Name	Description
Name	The administered name of the Service Profile.
Description	A description of the Service Profile.

Button	Description
Edit	Click to edit the selected Service Profile. Launches the Service Profile Editor page.
New	Click to create a new Service Profile. Launches the Service Profile Editor page.
Delete	Click to delete the selected Service Profile. You cannot delete a Service Profile if it still has a user assigned to it.

Related links

Creating a Service Profile on page 37

Service Profile Editor field descriptions

Use this page to create or edit a Service Profile, to add or remove services in a Service Profile and to define the invocation order of services in the profile.

Identity

Name	Description
Name	The name of the service profile.
Description	The description of the service profile.

All Services tab

Name	Description
Remove from Service Profile	Click the X in this column to remove a service from the service profile.
Name	The name of each service in the service profile.
Version	The version of each service in the service profile.
Description	The description of the service.

Service Invocation Details

Includes fields for: Calling Service Invocation Order; Called Service Invocation Order; and Service Not in an Invocation Order.

Name	Description
Order: First to Last	Provides arrows used to move services up and down in the invocation order. You can include up to five Call Intercept (calling or called party) services in a service profile.
Name	The name of each service in the service profile.
Version	The version of each service in the service profile.
Description	The description of the service.

Available Service to Add to this Service Profile

Name	Description
Add to Service Profile	Click **+** to add the latest version of a service to the service profile. Click **Advanced** to select the version of a service to add to the service profile. You can also set the preferred version of a service to a service profile from the **Add Service- Advanced** pop-up dialog box.
Name	The names of services that can be added to the service profile.
Description	The descriptions of services that can be added to the service profile.

Service Status field descriptions

Use this page to check the status of the snap-ins associated with the Avaya Breeze™ server you selected on the Server Administration page.

Name	Description
Name	The name of each snap-in that is associated with the selected Avaya Breeze™ sever.
Service Version	The snap-in version.
Service Install Status	The status of each snap-in. • A green check mark icon indicates that the snap-in is installed. • A yellow triangle icon indicates that the snap-in has been queued to be installed or uninstalled. • A red X icon indicates that the snap-in has failed to install or uninstall.

Table continues…

Name	Description
Activity	The sum of active Call, HTTP, and other custom defined sessions of a specific snap-in installed on a specific Avaya Breeze™ server.

Button	Description
Reinstall Service	Reinstalls the snap-in you selected.

SNMP MIB Download field descriptions

Use this page to download the SNMP MIB to a selected location.

Name	Description
File Name	The name of the SNMP MIB file.
Description	A description of the file and its contents.

Button	Description
Download	Launches a File Download window from which you can select a location to save the SNMP MIB file.

System Resource Monitoring field descriptions

Use this page to view the current resource usage and peak usage for Avaya Breeze™ servers in the selected cluster.

Name	Description
Cluster	The cluster for which you want to view usage details.
Time Period	The time period for which you want to view the usage details.
Server Name	The name of the Avaya Breeze™ server.
CPU % Used	The percentage of the CPU processing power that the Avaya Breeze™ server uses.
WebSphere Memory (MB)	The WebSphere memory use information. The column displays the following information: • **Used**: The memory that the server uses. • **Total**: The total memory available to the server.

Table continues…

Name	Description
	• **% Used**: The percentage of the total memory that the server uses.
Cluster Database Connections	The status of the connection between the active server and the standby server in a high availability database scenario. • A green check mark indicates that the connection between the active and the standby servers is up. • A yellow exclamation mark indicates that the standby server is getting ready to take over if the active server goes down. • A red cross indicates that the connection between the active and standby servers is down. • No background color with the value **---** indicates that the cluster database is disabled.
SIP	The details of the SIP sessions active on the server. The column displays the following information: • **Sessions**: The number of SIP sessions. • **Request Rate**
HTTP	The details of the HTTP connections active on the server. The column displays the following information: • **Connections**: The number of HTTP connections. • **Request Rate**
Disk (MB)	The disk space allocated to the server.

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

Chapter 14: Deployment Procedures

Deployment procedures overview

This section includes deployment procedures that must be performed exclusively using the System Manager web console. For a description of all the deployment procedures, see *Deploying Avaya Breeze™*.

Adding a Trust Certificate to all Avaya Breeze™ servers in a cluster

Before you begin

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

Procedure

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

   Note:

   The Trust Certificate that you are about to add will apply to all the Avaya Breeze™ servers assigned to the cluster.
4. From the **Select Store Type to install trusted certificate** menu, select the appropriate store type.
5. Click **Browse** to the location of your Trust Certificate, and select the certificate.
6. Click **Retrieve Certificate**, and review the details of the Trusted Certificate.
7. Click **Commit** .

Related links

Store types of the trusted certificates on page 26

Administering an Avaya Breeze™ instance

Before you begin

To complete this task you will need:

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

  This is the same IP address you used when deploying the Virtual Machine (VM).

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

  System Manager supports HTTP Cookie based Single Sign On (SSO). To facilitate SSO between System Manager and Avaya Breeze™, the domain name component of Avaya Breeze™ FQDN must match all or at least a part of the domain name of System Manager FQDN.
- The IP address including the network mask, and default gateway for the Avaya Breeze™ **Security Module**.
- The SIP entity name associated to the Avaya Breeze™ **Security Module**.

Note:

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

Procedure

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

   UCID Network Node ID is a unique, numeric node ID that is assigned to each Avaya Breeze™ server provisioned.
5. In the Management Network Interface **FQDN or IP Address** field, type the IP address or FQDN of the Avaya Breeze™ **Management Network Interface**.
6. In the Security Module **IPv4 Network Mask** field, type the network mask used for the SIP (Security Module) network.
7. In the Security Module **IPv4 Default Gateway** field, type the default gateway used for the SIP (Security Module) network.
8. Click **Commit** to save your changes.

   Note:

   The Commit fails if the Avaya Breeze™ license file on WebLM does not have the sufficient capacity to allow addition of another Avaya Breeze™ server.

9. To put the Avaya Breeze™ instance in service complete the following steps:

   Note:

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

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

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

      For more information, see “Accepting new service”.

Administering Avaya Aura® Media Server URI

About this task

Starting with Breeze 3.3 the configuration on this page is generally not needed. Only select snap-ins require this page to be configured. Check the documentation and/or release notes for your snap-in to confirm if this configuration is needed.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **Avaya Aura® Media Server**.

   The system displays the Avaya Aura® Media Server Configuration page.
3. In the **Avaya Aura® Media Server URI** field, enter the URI.

Chapter 15: Maintenance Procedures

Maintenance procedures overview

This section includes maintenance procedures that can be performed exclusively from the Avaya Breeze™ element of System Manager. For a description of all maintenance procedures, see *Maintaining and Troubleshooting Avaya Breeze™*.

Modifying the logging configuration

About this task

Use the Logging Configuration page to change the logging level of an installed server on Avaya Breeze™ servers or a cluster. You can also clear the logs for an installed service.

The log level for a snap-in does not persist when you:

- Upgrade the Avaya Breeze™ servers on which you installed the snap-in.
- Reinstall the snap-in.

Procedure

1. On the System Manager web interface, click **Elements** > **Avaya Breeze™** > **Configuration** > **Logging**.
2. On the Logging Configuration page, do the following:
3. In the **Cluster** field, select the cluster to which you want to apply the log level.
4. In the **Server** field, select the server to which you want to apply the log level.
5. In the **Service** field, select the snap-in whose logging level you want to change.
6. In the **Log Level** field, select the logging level of the snap-in that you selected.

   The system displays the clusters and instances where the snap-in is loaded.
7. Click **Set Log Level**.
8. To clear the logs of the selected snap-in, click **Clear Logs**.

Downloading and using the Breeze SNMP MIB

About this task

This page displays the name of the compressed file, a description of the compressed file, and a Download button, how to obtain Breeze related MIB files on customer using a third–party NMS system. Download a compressed copy of the MIBs related to Avaya Breeze™.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™** > **System Tools and Monitoring** > **SNMP MIB**.
2. On the SNMP MIB Download page, click **Download** .

   Avaya Breeze™ generates a `ce-mibs-version.zip` or a `ce-services-mib.zip` file.
3. Open the file using WinZip or a different utility.
4. Save the file.
5. Expand the downloaded compressed files.
6. Import all the MIB files with .my extension contained in the downloaded compressed files into NMS system.
7. Download the following MIB file from http://support.avaya.com and import them into NMS system:
   - Avaya_Aura_ServicabilityAgent_Mib.my

   Note:

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

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**.

Viewing the current usage of a cluster

Procedure

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

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

Viewing the peak usage of a cluster

Procedure

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

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

Resetting the peak usage of a cluster

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. Click **System Tools And Monitoring** > **System Resource Monitor**.
3. In the **Cluster** field, select the cluster for which you want to reset the peak usage.

4. In the **Time Period** field, select **Today**.
5. Click **Reset Peak Usage**.

Chapter 16: Certificate management

Overview

Avaya Breeze™ certificate deployment is managed by Avaya Aura® System Managerthrough the Trust Management service. The Trust Management Service provides certificates to ensure secure communication between elements. Trust Management provides Identity and Trusted (Certificate Authority (CA)) certificates to establish mutually authenticated TLS sessions.

Using the Trust Management service, you can perform the following operations for an application instance:

- View installed Trusted and Identity Certificates on the Avaya Breeze™server.
- Add or remove Trusted Certificates on the Avaya Breeze™server.
- Replace or renew Identity Certificates on the Avaya Breeze™server signed by Avaya Aura® System ManagerCA.
- Replace Identity Certificates on the Avaya Breeze™server signed by a third party CA.

Note:

If an external CA is used that does not provide Certificate Revocation List (CRL) information, you must disable CRL on the System Manager instance to which Avaya Breeze™ is registered for Oceana 3.4. On the **Security** > **Configuration** > **Security Configuration** page, set the **Certification Recovation Validation** field to **NONE**.

If a outgoing HTTP proxy is setup, CRL download might not work. In this case, you must download CRL list and then update on System manager at **Home** > **Services** > **Security** > **Configuration** > **CRL Download**.

Before attempting to make Certificate changes in Avaya Breeze™, it is recommended to get a solution level view to instand which network elements will be affected. This will require planning and network audits before deploying new certificates. Typically certificate change takes following stages like:

- Assessment: Identify and scope the migration work for your network (Security level required, TLS inventory, software inventory)
- Planning: Plan and schedule the migration
- Migration: The actual migration which includes possible software upgrades, Trust deployment, Identity Certificate deployment and cleanup.
- Post-migration: Ongoing audits to avoid certificate expirations.

Avaya Breeze™uses eight Identity Certificates for TLS connections:

- WebSphere
- SPIRIT
- Management
- SIP
- HTTPS
- Cluster Database (CDB)
- Authorization
- Postgres

The SIP, HTTPS, CDB and Postgres are the most important because these certificates communicate with outside entities such as the Avaya Aura Session Manager.

Caution:

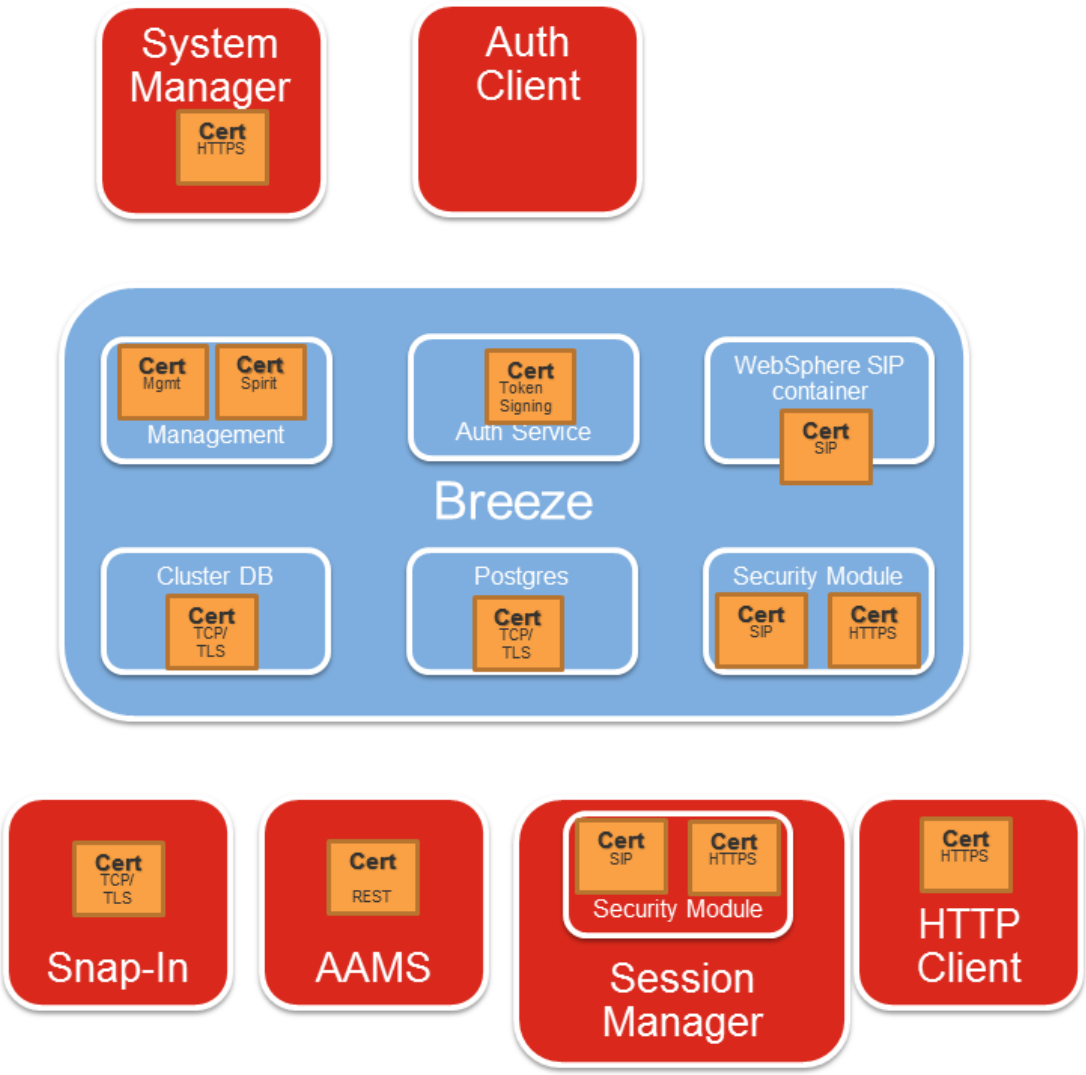
Any changes to these interfaces can cause major service interruptions.

The near-end and far-end entities may use certificates to authenticate each other, and each side presents its Identity Certificate during the TLS negotiation. If one side does not trust the signer of the Identity Certificate of the other side, the connection fails. For an entity to trust another certificate, the entity must possess the root CA certificate from the CA that issued the Identity Certificate. For example, VeriSign, Symantec, and System Manager. The root CA certificate must be stored in the entity's trusted list, also known as a Trust Store.

Warning:

To change the any Identity Certificate of an Avaya Breeze™ node, each far-end entity must first contain the new root CA certificate in its trusted list. You must add the new root CA certificate to the trusted list of the far end before changing the identity certificates.

The following diagram depicts the Identity Certificates on Avaya Breeze™, and its TLS connections to other elements in the network. Only a small subset of elements is represented.



Identity Certificates

Multiple Identity Certificates exist on Avaya Breeze™.

Service Name	To/from	Protocol	Port	Support 2048 key length and SHA2 signature	Notes
Security Module HTTPS	Secure HTTP interfaces for connections into snap-ins.	HTTPS	Port 443 on Avaya Breeze™.	Yes	Incoming secure REST and HTTP traffic use this certificate. Outg oing connections use the WebSphere certificate.
Security Module SIP	SIP TLS connections between Avaya Breeze™ and external servers. For example, Session Manager.	SIP	Default port 5061 on Avaya Breeze™. Other ports also supported.	Yes	Any product that needs a SIP TLS link to Avaya Breeze™.
WebSphere	IP TLS connection between the Security Module and the WebSphere (WAS) container and outgoing communication s from snap-ins.	SIP	Internal port 15061	Yes	This certificate is only used for internal connections between WAS and SECMOD and for snap-ins that send requests to external clients.
SPIRIT	SAL server on System Manager	HTTPS	Avaya Breeze™ephem eral port 22 connections to SMGR port 443 (HTTPS)	Yes	
Management (JBOSS)	Connections between System Manager and Avaya Breeze™for management.	JMX, RMI, HTTPS	JMX for DRS. Avaya Breeze™port 2009 RMI Avaya Breeze™port 11099, JMX	Yes	Use for both Internal communication and for external access from some snap-ins.

Table continues…

Service Name	To/from	Protocol	Port	Support 2048 key length and SHA2 signature	Notes
	For example, RMI/JMX and DRS replication.		Avaya Breeze™ port 11100 HTTPS port 443 on SMGR		
CDB	Connections to Avaya Breeze™ local cluster DB	TCP/TLS	Port 5433 on Avaya Breeze™	Yes	
Authorization	Connections to utilize the alternative OAuth-based platform security Framework for all incoming requests that have an OAuth token			Yes	
Postgres	Connections to Avaya Breeze™ local Postgres DB	TCP/TLS	Port 5432 on Avaya Breeze™	Yes	

Certificates issued by System Manager

System Manager can act as a Certificate Authority (CA) similar to VeriSign, Symantec or any other third-party CA. Many adopters, such as Communication Manager, Avaya Breeze™, and Presence use certificates issued by System Manager.

For fresh installations, all Identity Certificates, including SIP and HTTPS, are issued by the System Manager CA. These preinstalled certificates do not contain the complete set of attributes that some peer devices need to validate the certificate. To use these certificates, you must set the Common Name and Subject Alternate Name fields of the SIP and HTTP certificates. For more information, see “Replacing an Identify Certificate by System Manager CA issued certificate” section.

Demo certificates

Avaya Breeze™was shipped with demo certificates issued by the Avaya SIP CA to simplify TLS connection setup. Demo certificates are non-unique identity certificates issued by the Avaya SIP Product Certificate Authority. Demo certificates are very insecure and do not meet current NIST standards (SHA256 and 2048 bit keys).

Avaya Breeze™no longer uses or supports default demo certificates for new installations. Fresh installations of Avaya Breeze TM result in SIP and HTTP certificates signed by System Manager CA. In most cases, existing TLS connections will break until the System Manager root CA certificate is installed on the far end Trust Store. If you are currently using a demo certificate, Avaya strongly recommends that you immediately replace it.

Determining whether you are using a demo identity certificate

Procedure

1. On System Manager, click **Services** > **Inventory** > **Manage Elements**.
2. Select the Avaya Breeze™instance.
3. Click **More Actions** > **Configure Identity Certificates**.
4. Select the **securitymodule** checkbox.
5. Select the **Issuer Name** checkbox.

   If the **Issuer Name** field contains **CN=SIP Product Certificate Authority**, **OU=SIP Product Certificate Authority**, **O=Avaya Inc., C=US**, you have a demo identity certificate.

Viewing Identity Certificates

Procedure

1. On System Manager, click **Services** > **Inventory** > **Manage Elements**.
2. Select Avaya Breeze™instance.
3. Click **More Actions** > **Configure Identity Certificates**.
4. Click **View**.

Example

Replacing an Identify Certificate with an System Manager CA issued certificate

About this task

Use this procedure to replace an Identity Certificate of an Avaya Breeze™the one signed by the System Manager CA.

Important:

Peer servers, such as Session Manager need to trust the System Manager Root CA certificate before you replace a SIP or HTTP certificates. Failure to do so results in the loss of communication with the devices.

Procedure

1. On System Manager, click **Services** > **Inventory** > **Manage Elements**.
2. Select the appropriate Avaya Breeze™from the list and click **More Actions**.
3. Select **Configure Identity Certificates**.
4. On the Identity Certificates page, select the specific service.
5. Click **Replace**.
6. On the Replace Identity Certificate page, select **Replace this Certificate with Internal CA Signed Certificate**.
7. Select the **Common Name (CN)**check box.
8. Enter the host name or IP address.
9. For the Security Module SIP or Security Module HTTP identity certificates, enter the hostname or IP address of the Security Module.

   The address is the same as the SIP Entity address. It is recommended that host names must be used wherever possible rather than IP addresses.
10. Select **RSA** for the **Key Algorithm**.
11. Select **2048** or **4096** as the **Key Size**.
12. For the Security Module SIP identity certificate, select the **DNS Name** check box and enter the SIP domain. You can enter multiple SIP domains using commas (no spaces), such as avaya.com,company.com,xyz.com.
13. For the Security Module SIP or Security Module HTTP identity certificates, select the **IP Address** check box and enter the Security Module IP address (the SIP Entity address).

    Use only a single IP in this field. For the WebSphere or Management identity certificates, it is not necessary to enter an **IP address**. Leave the IP Address unchecked.

14. For the Security Module SIP identity certificate, select the **URI** check box and enter the SIP domain preceded by **sip**: schema. You can enter multiple URIs using commas (no spaces), such as sip:avaya.com,sip:company.com,sip:xyz.com.

    The use of the Subject Alternative Name extension entries of **URI** type and sip scheme is suggested by RFC5922 over the **DNS** type entries. Avaya SIP Endpoints currently only support the **DNS** type entries. It is recommended to have both **DNS** and **URI** entries to cover third party SIP devices which may require them.

15. Click **Commit**.

Replacing an Identify Certificate by a third party CA issued certificate

About this task

Use this procedure to replace an Identity Certificate of an Avaya Breeze™by one signed by a third party CA. A third party CA can be a commercial vendor such as VeriSign and Symantec, or an enterprise-run CA that is maintained by the customer's IT department. When the Security Module SIP certificate changes to the third party certificate, each SIP Entity must trust the third party CA.

Important:

Peer servers, such as Session Manager, need to trust the third party root CA certificate before you replace a SIP or HTTP certificates. Failure to do so results in the loss of communication with the devices.

Before you begin

Make sure you have the following:

- An identity certificate with the correct attributes that is signed by the third party certificate authority (CA). This certificate must be in the PKCS#12 format. The identity certificate attributes are described in the sections below. For instance, for the SIP certificate follow Security Module SIP identity certificate attributes.
- The entire certificate chain which signed the identity certificate. This includes the third-party Root CA certificate as well as any intermediate CA certificates.

Procedure

1. On System Manager, click **Services** > **Inventory** > **Manage Elements**.
2. Select the appropriate Avaya Breeze™from the list and click **More Actions**.
3. Select **Configure Identity Certificates**from the drop-down menu.
4. On the Identity Certificates page, select the specific service (e.g. **Security Module SIP**, **Security Module HTTPS**or other)
5. Click **Replace**.
6. On the Replace Identity Certificate page, select **Import third party PKCS#12 file**.

7. When prompted for **Please select a file**, browse for the third party signed certificate.
8. Enter the password in the **Password**field.
9. Click **Retrieve Certificate**.

   The certificate details section displays the details of the certificate.
10. 10. Click **Commit**.

Activating a new Identity Certificate

About this task

To activate a new Identity Certificate, an Avaya Breeze™reboot is required which is service impacting.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze™**.
2. Select an Avaya Breeze™instance.
3. Select **Shutdown System** > **Reboot**.
4. Click **Confirm**.

Certificate Signing Request (CSR) generation

Avaya Breeze™does not provide a GUI based interface to generate a CSR to replace its Identity Certificates. An alternate tool (e.g. OpenSSL) needs to be used to generate the CSR.

The high level steps to replace Avaya Breeze™Identity Certificates via a CSR are:

- Generate a CSR and its corresponding private key using OpenSSL or other adequate tool (e.g. Microsoft Server). Make sure the CSR contains the correct certificate attributes. Follow CSR and Private Key generation via OpenSSL when using OpenSSL.
- Send the CSR to the PKI administrator to get it signed by the third party CA. The result is a (signed) identity certificate.
- Bundle the identity certificates and private key into PKCS#12 container using OpenSSL or other adequate tool. Follow Bundle the Identity Certificate and Private Key into a PKCS #12 container. when using OpenSSL.
- Import the PKCS#12 certificate and private key into Avaya Breeze TM following Replacing an Identify Certificate by a third party CA issued certificate

CSR and Private Key generation via OpenSSL

About this task

This section describes the procedure to generate a private key and a CSR via OpenSSL. This is an example to replace the Security Module SIP identity certificate. A similar procedure needs to be follow to replace other Identity Certificates.

Procedure

1. Log in to Avaya Breeze™using SSH connection as **cust**.
2. 2) Copy the default OpenSSL configuration file to be modified:

   ```
   $ cp /etc/pki/tls/openssl.cnf /home/cust/openssl_csr.cnf
   ```

3. Modify the configuration file to meet the certificates attributes needed for each Identity Certificate. As an example of the configuration is shown as follows with the highlighted items in bold text showing the edits to the default configuration file. This example is for a Security Module SIP identity certificate which meets the Security Module SIP identity certificate attributes.

   ```
   $ vi /home/cust/openssl_csr.cnf
   …
   [ req ]
   default_bits            = 2048
   default_md              = sha256
   default_keyfile         = privkey.pem
   distinguished_name      = req_distinguished_name
   attributes              = req_attributes
   x509_extensions = v3_ca # The extentions to add to the self signed cert
   …
   # WARNING: ancient versions of Netscape crash on BMPStrings or UTF8Strings.
   string_mask = utf8only

   req_extensions = v3_req # The extensions to add to a certificate request

   …
   [ v3_req ]

   # Extensions to add to a certificate request

   basicConstraints = CA:FALSE
   keyUsage = nonRepudiation, digitalSignature, keyEncipherment, keyAgreement
   extendedKeyUsage=serverAuth, clientAuth
   subjectAltName= @alt_names

   [alt_names]
   DNS.1 = example.com              # The Avaya Breeze TM SIP domain
   DNS.2 = sip.example.com          # Another Avaya Breeze TM SIP domain
   IP = 192.168.1.100               # The Avaya Breeze TM SIP interface (eth1) IP
   address
   URI.1 = sip:example.com          # The Avaya Breeze TM SIP domain preceded by the
   sip schema
   URI.2 = sip:sip.example.com      # Another Avaya Breeze TM SIP domain preceded by
   the sip schema
   …
   ```

Note:

Some public CA's do not allow signing a CSR with a Subject Alternative Name extension entry of type URI and sip scheme (e.g. URI=sip:sip.example.com). In those cases use only the DNS type entry with the corresponded SIP Domain. In the above example, remove the lines that start with URI.1 and URI.2

4. Generate the CSR and Private Key. The generated CSR file is asm1.csr and the private key asm1.key. The private key is protected with a pass phrase that is prompted at the beginning. Remember this pass phrase as it will be used to create the PKCS#12 container. The private key file should stay on the server all the time and not distributed. If the private key gets compromised, an attacker could potentially decrypt TLS traffic or impersonate the Avaya Breeze™.

```
$ openssl req -out asm1.csr -new -newkey rsa:2048 -keyout asm1.key -config /home/
cust/openssl_csr.cnf
Generating a 2048 bit RSA private key
....+++
...............................................+++
writing new private key to 'asm1.key'
Enter PEM pass phrase:     <<< Private key pass phrase
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:CO
Locality Name (eg, city) [Default City]:Thornton
Organization Name (eg, company) [Default Company Ltd]:My example company
Organizational Unit Name (eg, section) []:IT
Common Name (eg, your name or your server's hostname) []:asm1.example.com   <<<
Avaya Breeze TM hostname
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

5. Verify the CSR contains the correct attributes. Run the following openssl command:

```
$ openssl req -in asm1.csr -text
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=US, ST=CO, L=Thornton, O=My example company, OU=IT,
CN=asm1.example.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:f2:d7:35:5a:f9:f7:9f:5f:1e:9e:f5:e0:4f:…
                Exponent: 65537 (0x10001)
        Attributes:
        Requested Extensions:
            X509v3 Basic Constraints:
                CA:FALSE
```

```
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment, Key
Agreement
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Subject Alternative Name:
                DNS:example.com, DNS:sip.example.com, IP Address:192.168.1.100,
URI:sip:example.com, URI:sip:sip.example.com
    Signature Algorithm: sha256WithRSAEncryption
         1f:64:2a:92:89:ce:bd:ff:80:7a:c8:50:7b:f2:bd:80:57:ce:…
-----BEGIN CERTIFICATE REQUEST-----
MIIDWDCCAkACAQAwcjELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAkNPMREwDwYD…
-----END CERTIFICATE REQUEST-----
```

6. Send the CSR file asm1.csr to the PKI administrator to get it signed by the third party CA. The result is a (signed) identity certificate.

Bundle the Identity Certificate and Private Key into a PKCS #12 container

About this task

This section describes the procedure to bundle the (signed) identity certificate and its corresponding private key into a PKCS#12 container using OpenSSL. PKCS#12 is the format required by System Manager to install the identity certificate into Avaya Breeze™.

Before you begin

- You should have obtained an identity certificate from the PKI administrator.
- The identity certificate should be in PEM format. If it is in a different form, OpenSSL could also be used to change it to PEM.

Procedure

1. This procedure is a continuation from CSR and Private Key generation via OpenSSL. It assumes the identity certificate file is asm1_signed.pem and the private key is asm1.key
2. Copy the asm1_signed.pem from your PC to the Avaya Breeze™and place it in `/home/cust/`.
3. Log into Avaya Breeze™using SSH connection as **cust**.
4. Run the following openssl command to generate the PKCS#12 file. It would prompt for:
   a. The private key pass phrase from Step 4) of CSR and Private Key generation via OpenSSL
   b. A new password to protect the PKCS#12 file. This password will be required when installing the identity certificate thru System Manager.

   Example:

```
$ openssl pkcs12 -export -out asm1.p12 -inkey asm1.key -in asm1_signed.pem
Enter pass phrase for asm1.key:
Enter Export Password:
Verifying - Enter Export Password:
```

5. The generated PKCS#12 container file is asm1.p12. Download this file and follow Replacing an Identify Certificate by a third party CA issued certificate to install it on Avaya Breeze™.
6. It is also recommended to delete the private key asm1.key from the Avaya Breeze™server to avoid it get compromised.

```
$ rm /home/cust/asm1.key
```

Identity Certificates lifecycle

All certificates have a limited valid lifetime. For Identity Certificates that are signed by the System Manager root CA, the lifetime is two years after they were first installed. Session Manger will auto renew those Identity Certificates 60 days prior to expiration. For Identity Certificates signed by a third party CA, the PKI administrator is responsible to replace/renew them prior to expiration.

Avaya Breeze™notifies for certificate expiration by generating alarms. These alarms are sent when either the auto renew process fails, or a third party Identity Certificate is about to expire:

- Critical alarm (OP_MMTC20050) if the certificate expires in less than 15 days
- Major alarm (OP_MMTC20049) if the certificate expires between 15 and 29 days
- Warning alarm (OP_MMTC20048) if the certificate expires between 30 and 60 days

For more details about the alarms and the expiration process check the *Maintaining and Troubleshooting Avaya Breeze™* document.

Security Module SIP identity certificate attributes

Generate the Security Module SIP identity certificate with the following X509v3 extensions and attributes.

Attribute	Value	Required
Subject	CN={breeze-fqdn}	required
Validity	validity period	required
Authority Key Identifier	hash	required[1]
Subject Key Identifier	hash	recommended
Key Usage	digitalSignature	required
	nonrepudiation	required
	keyEncipherment	required

Table continues…

[1] Authority key identifiers are required elements in end entity certificates to properly establish the trust chain.

Attribute	Value	Required
Extended Key Usage	id-kp-serverAuth = 1.3.6.1.5.5.7.3.3.1	required
	id-kp-clientAuth = 1.3.6.1.5.5.7.3.3.2	required[2]
	id-kp-sipDomain = 1.3.6.1.5.5.7.3.20	contraindicated[3]
Subject Alternative Name	IP:{breeze-security-module-ip}	optional
	URI:sip:{sip-domain}	optional[4]
	DNS:{sip-domain}	optional[5]
	DNS:{breeze-fqdn}	required
Authority Information Access	OCSP - URI:http://{ocsp-server}{:ocsp-port}{/ocsp-path}	optional
CRL Distribution Points	URI:http://{crl-server}{:crl-port}{/crl-path}	optional
	URI:ldap://{crl-server}{:crl-port}{/crl-dn} [6]	optional

Security Module HTTP identity certificate attributes

Generate the Security Module HTTP identity certificate with the following X509v3 extensions and attributes.

Attribute	Value	Required
Subject	CN={breeze-fqdn}	Required
Validity	validity period	Required
Authority Key Identifier	hash	Required
Subject Key Identifier	hash	Recommended

Table continues…

[2] Required as this Identity Certificate is used when the server is acting as a client (TLS mutual authentication)

[3] Validation of the presence of the id-kp-sipDomain extended key usage as described in RFC 5924 is discouraged, as it limits use of the certificate to SIP only and forces certificate proliferation.

[4] The SIP domain may not be known at install time, so the URI:sip:{domain} Subject Alternative Name value suggested by RFC 5922 is not likely to be present. Once the SIP domain is known, replace this Identity Certificate with the correct domain. Some public CA's do not allow signing a CSR with a Subject Alternative Name extension entry of type URI and sip scheme (e.g. URI=sip:sip.example.com). In those cases use only the DNS type entry with the corresponded SIP Domain. Follow either Replacing an Identify Certificate by an System Manager CA issued certificate or Replacing an Identify Certificate by a third party CA issued certificate

[5] The 96xx endpoints require the SIP domain to be present in the **CN** or as a DNS:{domain} entry in the Subject Alternative Name field.

[6] URLs and DNs used to identify the location of CRLs in LDAP directories may be quite complex; entities configuring or consuming these must be able to handle characters as defined by the LDAP URI specification in RFC 4516.

Attribute	Value	Required
Key Usage	digitalSignature	Required
	nonrepudiation	Required
	keyEncipherment	Required [7]
Extended Key Usage	id-kp-serverAuth = 1.3.6.1.5.5.7.3.3.1	Required
	id-kp-clientAuth = 1.3.6.1.5.5.7.3.3.2	Optional [8]
Subject Alternative Name	IP:{breeze-security-module-ip}	Required [9]
	DNS:{breeze-fqdn}	Required
Authority Information Access	OCSP - URI:http://{ocsp-server}{:ocsp-port}{/ocsp-path}	Optional
CRL Distribution Points	URI:http://{crl-server}{:crl-port}{/crl-path} [10]	Optional
	URI:ldap://{crl-server}{:crl-port}{/crl-dn}	Optional

Management and SPIRIT identity certificates attributes

Attribute	Value	Required
Subject	CN={breeze-fqdn}	Required
Validity	validity period	Required
Authority Key Identifier	hash	Required [11]
Subject Key Identifier	hash	Recommended
Key Usage	digitalSignature	Required
	nonrepudiation	Required
	keyEncipherment	Required
	dataEncipherment	Required
	keyAgreement	Required
Extended Key Usage	id-kp-serverAuth = 1.3.6.1.5.5.7.3.3.1	Required

Table continues…

[7] Authority key identifiers are required elements in end entity certificates to properly establish the trust chain.
[8] Required if the same identity certificate is used when the server is acting as a client.
[9] For the 96xx endpoints, PPM is defined as an IP address so PPM certificates must contain the IP:{ip} Subject Alternative Name entry when these endpoints are part of the solution.
[10] URLs and DNs used to identify the location of CRLs in LDAP directories may be quite complex; entities configuring or consuming these must be able to handle characters as defined by the LDAP URI specification in RFC 4516.
[11] Authority key identifiers are required elements in end entity certificates to properly establish the trust chain.

Attribute	Value	Required
	id-kp-clientAuth = 1.3.6.1.5.5.7.3.3.2	Required
Authority Information Access	OCSP - URI:http://{ocsp-server}{:ocsp-port}{/ocsp-path}	Optional
CRL Distribution Points	URI:http://{crl-server}{:crl-port}{/crl-path}	Optional
	URI:ldap://{crl-server}{:crl-port}{/crl-dn} [12]	Optional

Replacing an Identity Certificate issued by System Manager CA

About this task

Use this procedure to replace the Avaya Breeze™ SIP Identity Certificate signed by System Manager CA.

Procedure

1. Obtain the System Manager root CA certificate. See “Exporting the System Manager root CA certificate”
2. Deploy the System Manager root CA certificate on peer devices that connect SIP TLS to Avaya Breeze™.
   a. Identify all the peer servers that connect to Avaya Breeze™ through SIP over TLS. For example, Session Manager.
   b. Deploy the System Manager root CA certificate following the peer server documentation on how to deploy the trusted CA certificate into their respective Trust Stores.
3. Replace the SIP Identity certificate. See “ Replacing an Identify Certificate by an System Manager CA issued certificate.”
4. Activate the new SIP Identity Certificate. See “Activating a new Identity Certificate.”
5. Verify the SIP TLS connections are now using the new identity certificate.
6. On System Manager, click **Elements** > **Session Manager** > **System Status** > **SIP Entity Monitoring**.
7. Verify the Avaya Breeze™ entities that are TLS connected that the link status is UP.

[12] URLs and DNs used to identify the location of CRLs in LDAP directories may be quite complex; entities configuring or consuming these must be able to handle characters as defined by the LDAP URI specification in RFC 4516.

Replacing an Identity Certificate issued by a third party CA

About this task

Use this procedure to replace an Identity Certificate issued by a third party CA. A third party CA can be a commercial vendor such as VeriSign and Symantec, or an enterprise-run CA that is maintained by the customer's IT department. A third party CA in this context means a CA other than the System Manager CA.

Procedure

1. Obtain the new SIP Identity Certificate. See, "Obtaining new SIP Identity Certificate through Certificate Signing Request (CSR)" or "Obtaining new SIP Identity Certificate through PKCS#12 container"
2. Deploy the trusted third party root CA certificate on Avaya Breeze™.
   a. Obtain from the third party CA PKI administrator the root CA certificate.
   b. Add the root CA certificate into the Avaya Breeze™ SECURITY_MODULE_SIP and WEBSPHERE trust stores. See "Adding trusted CA certificates."
3. Deploy the trusted third party root CA certificate on peer devices that connect SIP TLS to Avaya Breeze™.
   a. Identity all the peer devices that connect to Avaya Breeze™ through SIP over TLS. For example, Session Manager.
   b. Obtain from the third party CA PKI administrator the root CA certificate.
   c. Follow the peer device documentation on how to deploy the trusted CA certificate into their respective Trust Stores.
4. Replace the SIP Identity Certificate. See "Replacing an Identify Certificate by a third party CA issued certificate."
5. Activate the new SIP Identity Certificate. See "Activating a new Identity Certificate."
6. Verify the SIP TLS connections are now using the new identity certificate.
7. On System Manager, click **Elements** > **Session Manager** > **System Status** > **SIP Entity Monitoring**.
8. Verify that the Avaya Breeze™ entities that are TLS connected that the link status is UP.

Obtaining new SIP Identity Certificate through Certificate Signing Request (CSR)

About this task

Use this procedure to obtain SIP Identity Certificate through Certificate Signing Request (CSR).

Procedure

1. Generate a CSR on Avaya Breeze™. See “Generating Certificate Signing Request (CSR)”.
2. Send the CSR to the third party CA PKI administrator to get it signed.
3. Obtain from the PKI administrator the signed SIP Identity Certificate. Preferably the certificate would be in PEM format.
4. Bundle the SIP Identity Certificate and the private key into a PKCS#12 container.

Obtaining SIP Identity Certificate through PKCS#12 container

About this task

Use this procedure to obtain SIP Identity Certificate through PKCS#12 container.

Procedure

1. Obtain from the third party CA PKI administrator a SIP Identity Certificate.
2. Obtain the associated private key of a SIP Identity Certificate bundled in PKCS#12 container.
3. Verify that the SIP Identity Certificate have the attributes described in Security Module SIP identity certificate attributes on page 157.

Trust management

Multiple Trust Stores exist on Avaya Breeze™. Each Trust Store contains a set of CA certificates that are trusted by a given service. The following table describes them.

Store type	Purpose	Protocol	Note
SECURITY_MODULE_HTTP	Used for validating client identity certificates on secure HTTP connections from SIP Endpoints (Hardphones, Softphones, etc.). The endpoints use this HTTP connection for PPM protocol.	HTTPS	
SECURITY_MODULE_SIP	Used for validating identity certificates for SIP TLS connections between Avaya Breeze™ and external devices	SIP	

Table continues…

Store type	Purpose	Protocol	Note
	(e.g. Communication Manager, SBC, SIP Endpoints, etc.)		
WEBSPHERE	Used by the WebSphere SIP container for validating the identity certificate of the Security Module	SIP	This store should only contain the CA certificate that signed the Security Module SIP identity certificate. This store is not used to validate any identity certificate presented by an external TLS connection.
SPIRIT	Used by the Spirit Agent to validate the identity certificate	HTTPS	
MGMT_JBOSS	Used for validating the identity certificates of System Manager for management (RMI/JMX, DRS replication, etc.)	JMX, RMI, HTTPS	
CLUSTER_DB	Used for validating the Cluster DB certificates	DB	
POSTGRES	Used for validating the POSTGRES DB certificates	DB	
AUTHORIZATION_SERVICE	Used for validating the Authorization service certificates	AS	

Viewing trusted CA certificates

About this task

Use this procedure to view trusted CA certificates.

Before you begin

You must have permission to view the certificates of an application instance.

Procedure

1. On System Manager, click **Services** > **Inventory** > **Manage Elements**.
2. Select an Avaya Breeze™ instance.
3. Click **More Actions** > **Configure Trusted Certificates**.
4. On the Trusted Certificates page, select the certificate, and the store type it resides and click **View**.

Adding trusted CA certificates

About this task

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

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

Procedure

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

      `-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE----.`

   e. Paste the contents of the file in the box provided at the bottom of the page.
   f. Click **Commit**.
7. To import certificates from existing certificates:
   a. Click **Import from existing**.
   b. Select the certificate from the Global Trusted Certificate section.
   c. Click **Commit**.

8. To import certificates using TLS:
   a. Click **Import using TLS**.
   b. Enter the IP Address of the location in the **IP Address** field.
   c. Enter the port of the location in the **Port** field.
   d. Click **Retrieve Certificate**.
9. Click **Commit**.
10. Restart the JBoss service on System Manager.

Removing trusted CA certificates

Procedure

1. On System Manager, click **Services** > **Inventory** > **Manage Elements**.
2. Select an Avaya Breeze™ instance.
3. Click **More Actions** > **Configure Trusted Certificates**.
4. Select the certificates you want to remove, and click **Remove**.

Exporting Avaya Breeze™ certificate

Procedure

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

Exporting System Manager root CA certificate

About this task

When Avaya Breeze™ uses System Manager CA signed Identity Certificates, it is necessary to obtain the System Manager root CA certificate to be added to the Trust Store of peer devices that connect to Avaya Breeze™ (e.g. Communication Manager, SIP Endpoint, other SIP devices, etc.). This section describes how to obtain the System Managerroot CA certificate.

Procedure

1. On System Manager, click **Services** > **Security** > **Certificates** > **Authority**.
2. In **CA Functions**, click **CA Structure & CRLs**.

3. On the main page, click **Download PEM file**.
4. Save the file.

Note:

To avoid HTTP download issues, save the file with the .txt extension.

Peer Certificate Validation

All the Avaya Breeze™ TLS services support validation of peer Identity Certificates that have a SHA2 signature and have a public key length of 2048 bits. Avaya Breeze™ verifies that the peer identity certificate could be traced all the way to a trusted root CA certificate. The root CA certificate must reside on the service Trust Store.

Certificate validations for System Manager connection

For the TLS connection between Avaya Breeze™ and System Manager, the identity certificate is validated using standard path validation which complies with the RFC5280 section “Certificate Path Validation”. In addition, hostname validation is performed. The System Manager identity certificate should have a Subject Alternate Name extension with two DNS name entries:

1. The actual System Manager hostname (e.g. systemmanager-1.example.com)
2. The second DNS entry should contain "active.smgr.com" value. This last one is used as Data Replication (DRS) uses that hostname for certificate validation.

Certificate validations for SIP TLS connections

For trusted (e.g. SIP Entities) SIP TLS connections, Avaya Breeze™ applies the following validations:

1. Mutual TLS authentication: During the TLS handshake, the SIP entity and Avaya Breeze™ validate the certificate of each other and perform mutual TLS authentication.
2. Additional validation of the SIP entity identity certificate: If the mutual TLS authentication is successful, further validation is performed using the credential name or the far end IP address of the SIP entity identity certificate. Use the Credential name field of the SIP Entity page to assign it.
   a. If the credential name string is empty, the connection is accepted.
   b. If the credential name string is not empty, the credential name and the IP address of the SIP entity is searched in the identity certificate provided by the SIP entity.
   - CN value from the Subject

- subjectAltName.dNSName
- subjectAltName.uniformResourceIdentifier

For IP address comparison, the IP address string is converted to SIP:W.X.Y.Z before comparison. W.X.Y.Z is the remote socket IPV4 address. Also case insensitive search is performed in this case.

For untrusted (e.g. SIP Endpoints) SIP TLS connections, Avaya Breeze™ behavior depends on the version and its configuration:

- For Avaya Breeze™ 3.0.0 and earlier, the Enable TLS Endpoint Certificate Validation setting on the Avaya Breeze™ Administration page controls the validation:
- If Enable TLS Endpoint Certificate Validation is checked, Avaya Breeze™ requests a client certificate (via TLS Certificate Request message):
- If the client provides an identity certificate, its certificate chain must be traced to a trusted CA certificate in order for the connection to get established.
- If the client does not provide a certificate, the connection is allowed.
- If Enable TLS Endpoint Certificate Validation is unchecked, no TLS client authentication is performed.
- For Avaya Breeze™ 3.0.1 and later, the TLS Endpoint Certificate Validation setting on the Avaya Breeze™ Administration page controls the validation performed on the client certificate. Avaya Breeze™ always requests a client certificate (via TLS Certificate Request message), and its validation depend on the configuration value:
- If TLS Endpoint Certificate Validation is set to Required:
  - If the client provides a certificate, its certificate chain must be traced to a trusted CA certificate in order to connect.
  - If the client does not provide a certificate, the connection is refused.
- If TLS Endpoint Certificate Validation is set to Optional:
  - If the client provides a certificate, its certificate chain must be traced to a trusted CA certificate in order to connect.
  - If the client does not provide a certificate, the connection is allowed
- If TLS Endpoint Certificate Validation is set to None
  - If the client provides a certificate, its certificate will be saved for reporting but not validated. The connection is allowed
  - If the client does not provide a certificate, the connection is allowed

Certificate Revocation Management

Avaya Breeze™ verifies that certificates are valid and not contained in a Certificate Revocation List (CRL). If a certificate is on a CRL, Avaya Breeze™ will not allow a secure connection to be created using that certificate, and the certificate must be updated.

Troubleshooting Certificates issues

Certificate expired

The lifespan of Identity Certificates are usually shorter than the CA certificates. When a certificate is attempted to be used after the “Valid to” value, the TLS connection fails with certificate_expired (45) description in the TLS Alert message. This could be seen with a Wireshark capture on the specific port. Some services will fail to start if the Identity Certificate they use expired. This could be seen on their corresponding log files.

Identity Certificate not trusted (Unknown CA).

When a TLS service connects to a peer device, and the peer device presents its Identity Certificate, the issuer of that certificate needs to be trusted in order for the connection to be established. If that is not the case, the TLS handshake fails with unknown_ca (48) description in the TLS Alert message.

Unsupported Certificate

When an Identity Certificate does not contain all the correct attributes, the TLS handshake could fail with unsupported_certificate(43) description in the TLS Alert message. The certificate attributes that are usually mis-configured are those in extensions Key Usage and/or Extended Key Usage.

Certificate not yet valid

A newly generated Identity Certificate with current “Valid From” date/time may not be valid for the peer device validating it. Check that the clock on both devices are in sync.

Certificate Revoked

The certificate has been placed on a CRL and must be replaced.

Chapter 17: 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 173

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 173

Appendix A: CLI commands

CEnetSetup or AvayaNetSetup

Use this command to change the OVA properties specified during deployment.

If you change the IP address or FQDN using this command, you must follow the steps in the “Configuring Avaya Breeze” after changing the IP address or FQDN using AvayaNetSetup or CEnetSetup section in *Deploying Avaya Breeze™*.

Syntax

`CEnetSetup` or `AvayaNetSetup`

Sample output

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

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

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

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

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

Enter Primary DNS server IP address or 'none'
[]:

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

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

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

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

```
Avaya Timezone Selection

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

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

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

Select Timezone
[America/Denver]: America/Denver

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

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


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

```
Verify the settings below:

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

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

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


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

custAccounts

Use this command to add a customer account, delete a customer account, or clear failed login attempts for a user.

Syntax

```
custAccounts [-a | —d | —c | —h]
```

Options:

- -a: Adds a new customer account.
- -d: Deletes a customer account.
- -c: Clears failed login attempts for a user.
- -h: Displays help for the command.

Sample output 1

```
# custAccounts -a
```

```
Enter Login ID to use for customer account: user1

Set password for user1
Changing password for user user1.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Sample output 2

```
# custAccounts -c
```

```
Login ID for customer account to clear failed login attempts on: user1
Login           Failures Latest failure     From
user1               2    09/19/16 07:14:20  135.123.150.165
```

Sample output 3

```
# custAccounts -d
```

```
Login ID for Customer account to be deleted: user1
```

check_breeze_status.sh

Use this command to check the status of the Avaya Breeze™ system. This command displays the following:

- System Manager IP/FQDN provisioning
- Certificate status
- Application status
- Deployed snap-ins status

- Platform status

The system displays the status automatically on login. Use this command to view the status on demand.

Syntax

```
check_breeze_status.sh [-s] [-l]
```

Options:

- -s: Displays the concise view. The output includes the following information:
  - Certificates status.
  - Output of the **statapp** command.
  - A check of partitions.
  - A List of loaded snap-ins if the number of snap-ins are nine or less. Else, the number of configured snap-ins.
  - Platform status.
  - Summary.
- -l: Displays the view presented at login time. This is automatically displayed on SSH login. The output includes the following information:
  - Certificate status.
  - Output of the **statapp** command.
  - A check of partitions.
  - A List of loaded snap-ins if the number of snap-ins are nine or less. Else, the number of configured snap-ins.
  - A List of platform services that are running.
- No options: Displays the verbose view. The output includes the following information:
  - List of current certificates
  - Output of the **statapp -l** command
  - A check of partitions
  - Details of snap-ins
  - A List of platform services that are running

Sample summary status log:

```
# check_breeze_status.sh -s
```

```
Avaya Breeze Login Time and On Demand Status Report for Avaya Breeze Management IP
10.138.46.22

  SMGR info for Avaya Breeze instance
    * Primary System Manager:   10.138.46.26 (bv-edp-smgr-r046026.ca.avaya.com)
    * SMGR 2 is not currently provisioned.   Geo-redundancy is not available.

  Trust Management Status
    Trust store certificates are present.
    Key store certificates are present.
```

```
  State of the applications on this virtual machine:
    Watchdog          9/  9 UP
    logevent         15/ 15 UP
    postgres-db      33/ 33 UP
    mgmt            301/301 UP
    WebSphere       235/235 UP
    sal-agent        51/ 51 UP
    dcm               1/  1 UP
    secmod            4/  4 UP

    Depending on the config, the "statapp -l" can give a more detailed view.

  Capacity check for partitions
    No disk partitions using over 70% of capacity.

  Current services detected on this system:
    Provisioned services and version number:

    The platformApp is deployed.

Health Status Summary: Good.
```

Sample status log displayed at login

```
# check_breeze_status.sh -l
```

```
Avaya Breeze Login Time and On Demand Status Report for Avaya Breeze Management IP
10.138.46.22

  SMGR info for Avaya Breeze instance
    * Primary System Manager:   10.138.46.26 (bv-edp-smgr-r046026.ca.avaya.com)
    * SMGR 2 is not currently provisioned.   Geo-redundancy is not available.

  Trust Management Status
    Trust store certs:
      -  asset_http_truststore.pem
      -  asset_truststore.pem
      -  cdb_truststore.pem
      -  postgres_truststore.pem
    Key store certs:
      -  asset_http_keystore.pem
      -  asset_keystore.pem
      -  cdb_keystore.pem
      -  postgres_keystore.pem

  State of the applications on this virtual machine:
    Using the statapp -l command.   Note that certain apps may show "DOWN" legitimately;
    they come up only when specific services are installed, or enabled by configuration.

    Service           x/  x State
    --------------  ------- -----
    Watchdog          9/  9 UP
    logevent         15/ 15 UP
    postgres-db      33/ 33 UP
    mgmt            293/293 UP
    mgmt-monitor     19/ 19 UP
    WebSphere       235/235 UP
    was-monitor       1/  1 UP
    sal-agent        51/ 51 UP
    dcm               1/  1 UP
    activemqd         0/  1 DOWN
    zookeeper         0/  1 DOWN
    asset-SW         48/ 46 UP
    Cron              2/  2 UP
```

```
    SNMP              1/  1 UP
    DNS               7/  1 UP * 7
    MISC            236/  0 UP
    secmod            4/  4 UP

  Capacity check for partitions
    No disk partitions using over 70% of capacity.
 Current services detected on this system:
    (This operation may take a while...)

    Provisioned services:

    Platform services (not provisionable) that are present:
      filetransferSecured
      ibmasyncrsp
      pfa
      platformApp
      SipContainerModule

    The platformApp is deployed, based on the app list above.

Health Status Summary: Good.
```

Sample verbose status log

```
# check_breeze_status.sh
```

```
Avaya Breeze Login Time and On Demand Status Report for Avaya Breeze Management IP
10.138.46.22

  SMGR info for Avaya Breeze instance
    * Primary System Manager:   10.138.46.26 (bv-edp-smgr-r046026.ca.avaya.com)
    * SMGR 2 is not currently provisioned.   Geo-redundancy is not available.

  Trust Management Status
    Trust store certs:
      -  asset_http_truststore.pem
      -  asset_truststore.pem
      -  cdb_truststore.pem
      -  postgres_truststore.pem
    Key store certs:
      -  asset_http_keystore.pem
      -  asset_keystore.pem
      -  cdb_keystore.pem
      -  postgres_keystore.pem

  State of the applications on this virtual machine:
    Using the statapp -l command.   Note that certain apps may show "DOWN" legitimately;
    they come up only when specific services are installed, or enabled by configuration.

    Service           x/  x State
    --------------  ------- -----
    Watchdog          9/  9 UP
    logevent         15/ 15 UP
    postgres-db      39/ 39 UP
    mgmt            294/294 UP
    mgmt-monitor     19/ 19 UP
    WebSphere       367/367 UP
    was-monitor       1/  1 UP
    sal-agent        51/ 51 UP
    dcm               1/  1 UP
    activemqd         0/  1 DOWN
    zookeeper         0/  1 DOWN
    asset-SW         48/ 46 UP
    Cron              2/  2 UP
```

```
    SNMP              1/  1 UP
    DNS               7/  1 UP * 7
    MISC            242/  0 UP
    secmod            4/  4 UP

  Capacity check for partitions
    No disk partitions using over 70% of capacity.

  Current services detected on this system:
    (This operation may take a while...)

    Provisioned services:
      load: + deploy: + run: + car: + HelloWorld-3.3.1.0.07331008
      load: + deploy: + run: + car: + CallEventControl-3.4.0.0.81001
      load: + deploy: + run: + car: + CEDebugger-3.3.0.0.0
      load: + deploy: + run: + car: + EventingConnector-3.4.0.0.81001
      load: + deploy: + run: + car: = AuthorizationService-3.4.0.1.0
      load: + deploy: + run: + car: + CMATestService-3.3.0.0.27
      load: + deploy: + run: + car: = EmailConnector-3.3.1.0.07331008

    Platform services (not provisionable) that are present:
      filetransferSecured
      ibmasyncrsp
      pfa
      platformApp
      SipContainerModule

    The platformApp is deployed, based on the app list above.


Health Status Summary: Good.
```

Appendix B: Configuring an LDAP provider and SAML provider

Configuring LDAP provider

Apache Directory Studio Configuration

This section provides example configuration procedures for Apache Directory Studio. This section is purely for reference.

Related links

Prerequisites on page 183
Installing Apache Directory Studio on page 183
Creating a new LDAP server on page 184
Downloading the CA that signed the certificate on page 185
Editing the configuration on page 186
Creating a new LDAP Client on page 189
Creating LDAP users on page 191

Prerequisites

Java 7.0 or newer. Oracle's JDK is recommended.

Related links

Apache Directory Studio Configuration on page 183

Installing Apache Directory Studio

Procedure

1. Go to http://directory.apache.org/studio/.
2. Download the Apache Directory Studio version 2.0.0-M10, compatible with your operating system and the user guide.
3. Extract the downloaded archive and place the extracted folder where you want Apache Directory Studio to be installed.

4. After installing the Apache Directory Studio in a directory, you can start Apache Directory Studio by running the ApacheDirectoryStudio executable included with the release.

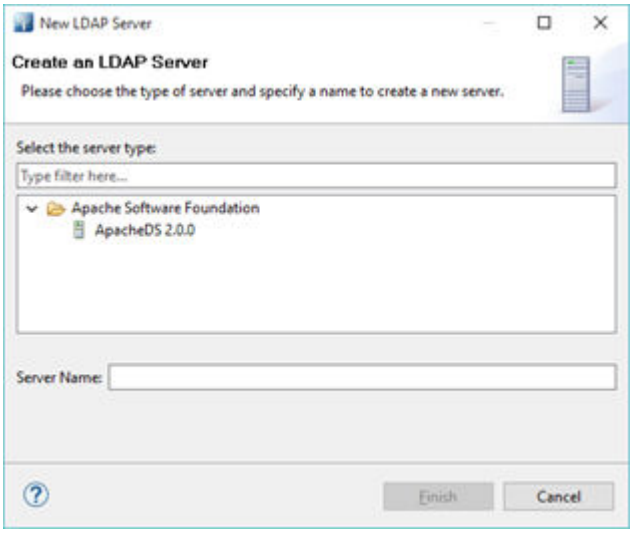
Related links

Apache Directory Studio Configuration on page 183

Creating a new LDAP server

Procedure

1. On Apache Directory Studio, in the Servers view toolbar, click **New Server**, or use the **Ctrl +E** shortcut.



2. Choose Apache DS 2.0.0 or whichever available given under Apache Software Foundation.
3. Click **Finish**.

Related links

Apache Directory Studio Configuration on page 183

Creating SSL Certificates for LDAP Server

Creating an end entity

Procedure

1. On System Manager, click **Services** > **Security** > **Certificates** > **Authority**.
2. In the **RA Functions** section, click **Add End Entity**.
3. In the **End Entity Profile** field, select `INBOUND_OUTBOUND_TLS`.
4. Type the user name and password of the entity.

   The password is mandatory and without the password you cannot generate the certificate generation request.

5. In the **Certificate Profile** field, type `ID_CLIENT_SERVER`.
6. In the **CA field**, type `tmdefaultca`.
7. In the **Token** field select **JKS file**.
8. Complete the fields that you want in your certificate.
9. Click **Add**.

Result

The system displays the following message:

```
End Entity <username> added successfully.
```

Next steps

This is the signed certificate you have to import into the LDAP server.

Related links

Apache Directory Studio Configuration on page 183

Creating the LDAP Server certificate

Procedure

1. On System Manager, click **Services** > **Security** > **Certificates** > **Authority**.
2. In the navigation page, click **Public Web**.
3. On Public Web page, click **keystore**
4. Enter the user name and password from earlier procedure and click **OK**.
5. Select the certificate key length.

   2048 is recommended.
6. Click **Enroll**.
7. Save the server certificate.

   This is the signed certificate you have to import into the LDAP server.

Related links

Apache Directory Studio Configuration on page 183

Downloading the CA that signed the certificate

Procedure

1. On System Manager, click **Services** > **Security** > **Certificates** > **Authority**.
2. In the navigation page, click **Public Web**.
3. Click **Fetch CA certificates**.
4. Click **Download PEM chain**.
5. Save the CA certificate.

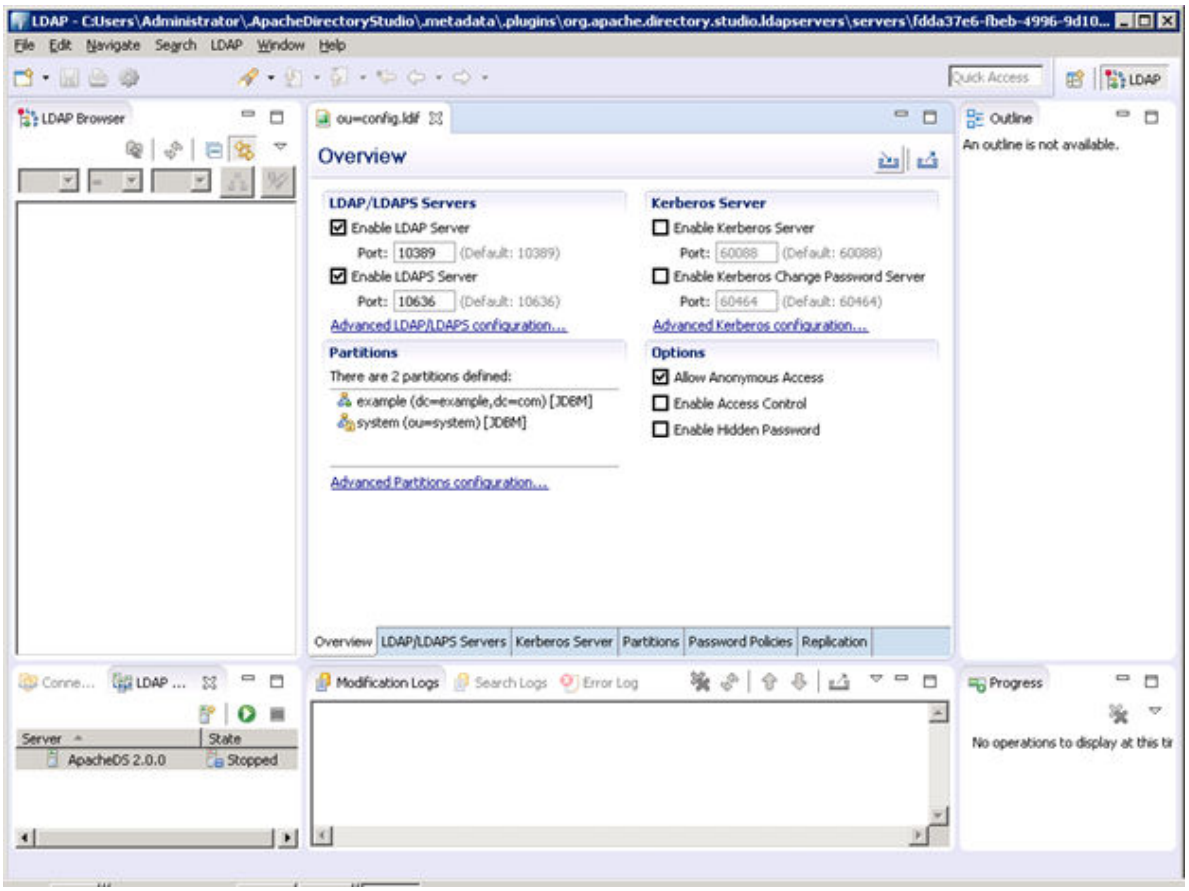
Related links

Apache Directory Studio Configuration on page 183

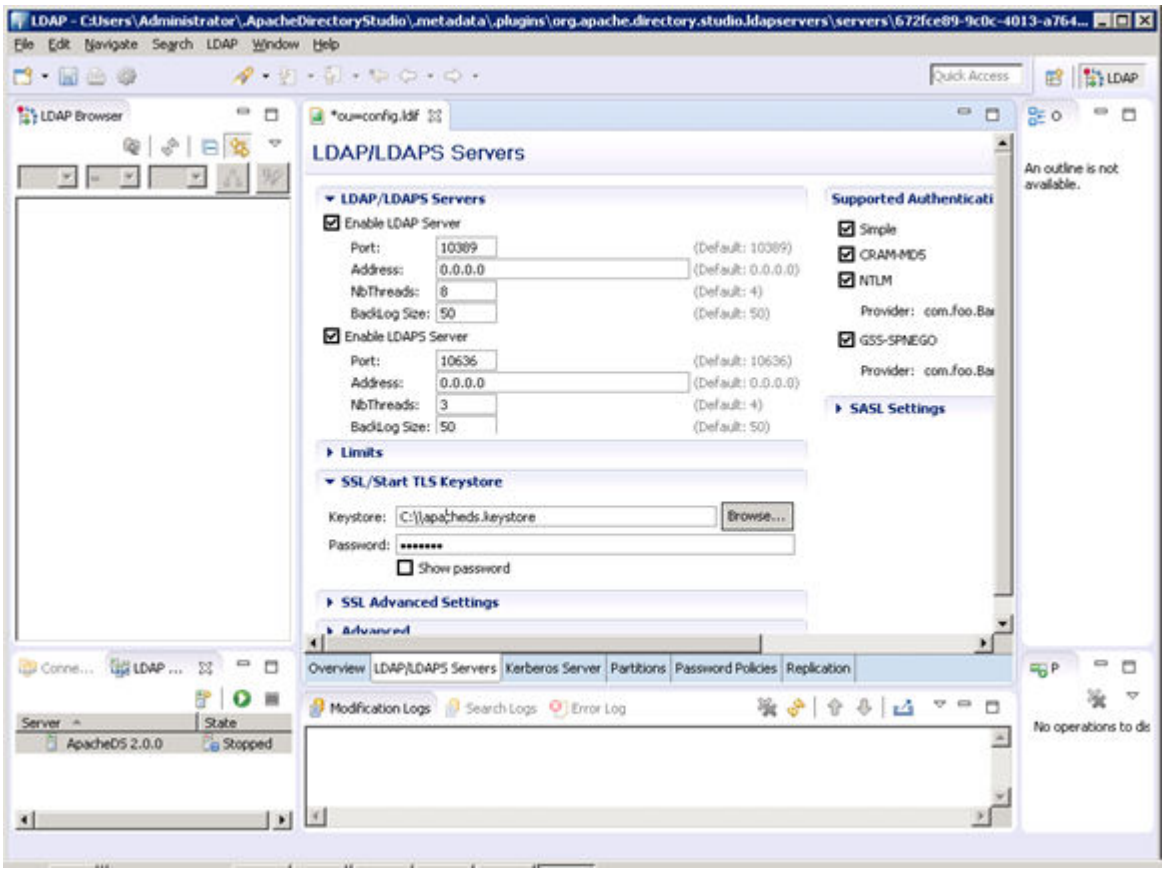
Editing the configuration

Procedure

1. On Apache Directory Studio, in the Servers view, double-click the server or press **F3**.

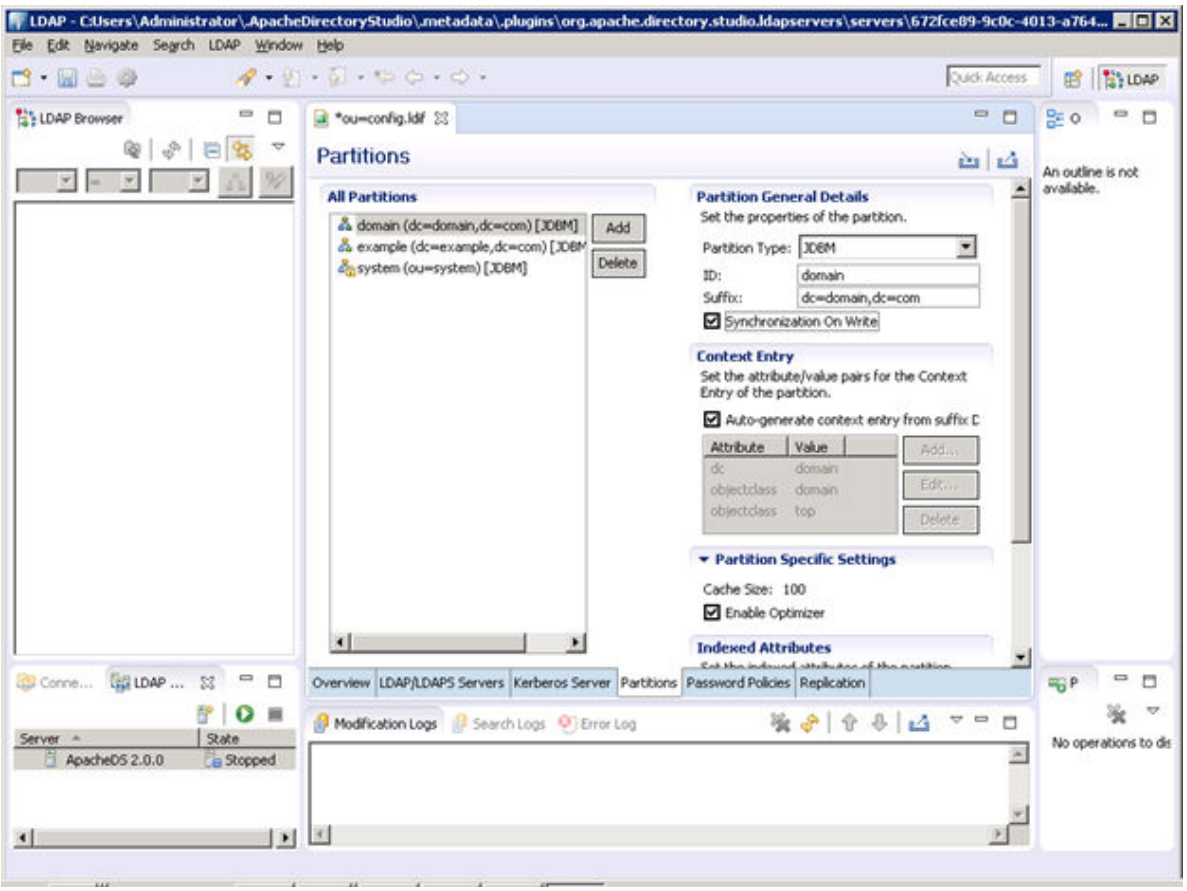


2. Select the **Advanced LDAP/LDAPS Configuration** option.



3. To configure **SSL/start TLS Keytsore**, provide the path of downloaded keystore and password.

4. Click the Partitions Configuration tab to add the partition:



5. Press **Ctrl+s** to save the configuration.

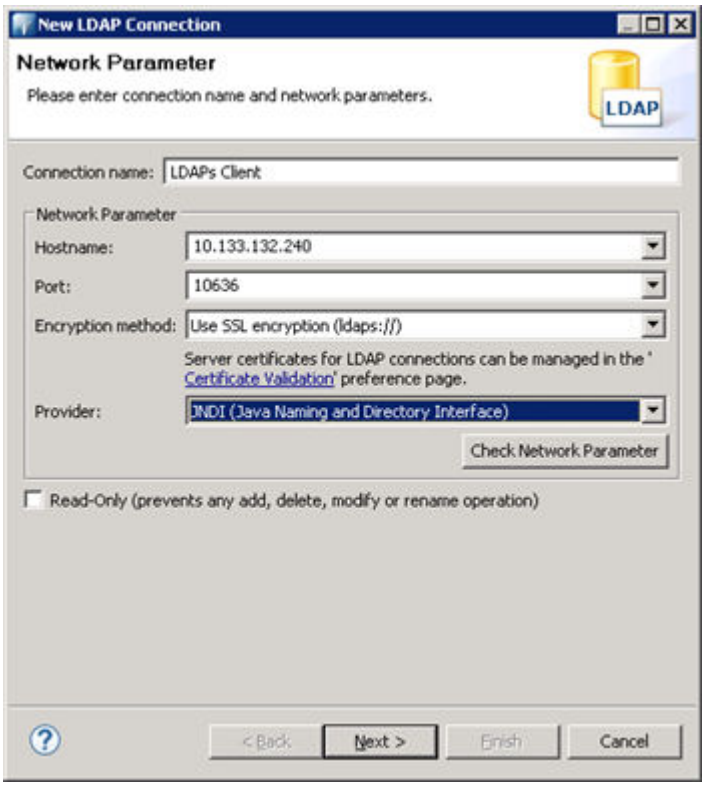
Related links

Apache Directory Studio Configuration on page 183

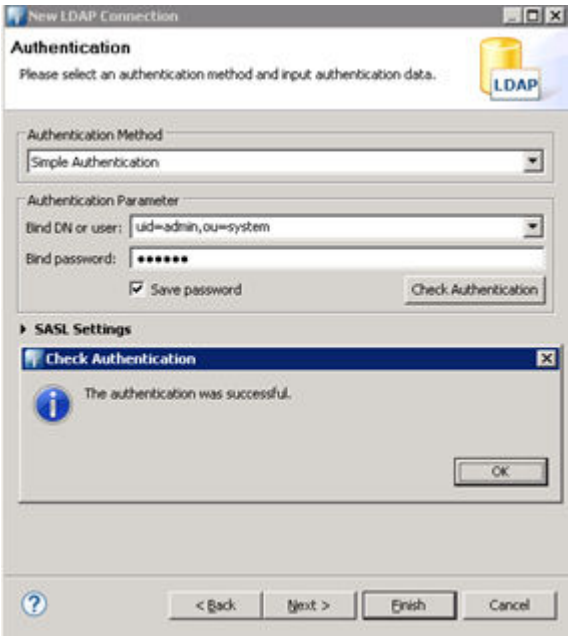
Creating a new LDAP Client

Procedure

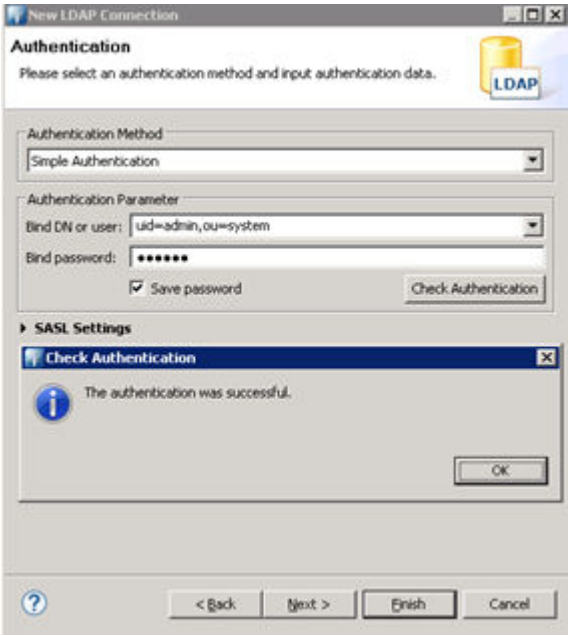
1. On Apache Directory Studio, in the LDAP menu, click **New Connection** and enter the required information.



2. Add the CA certificate and click **Next**.



3. Enter the following information, and click **Check Authentication**.



4. Click **Finish**.

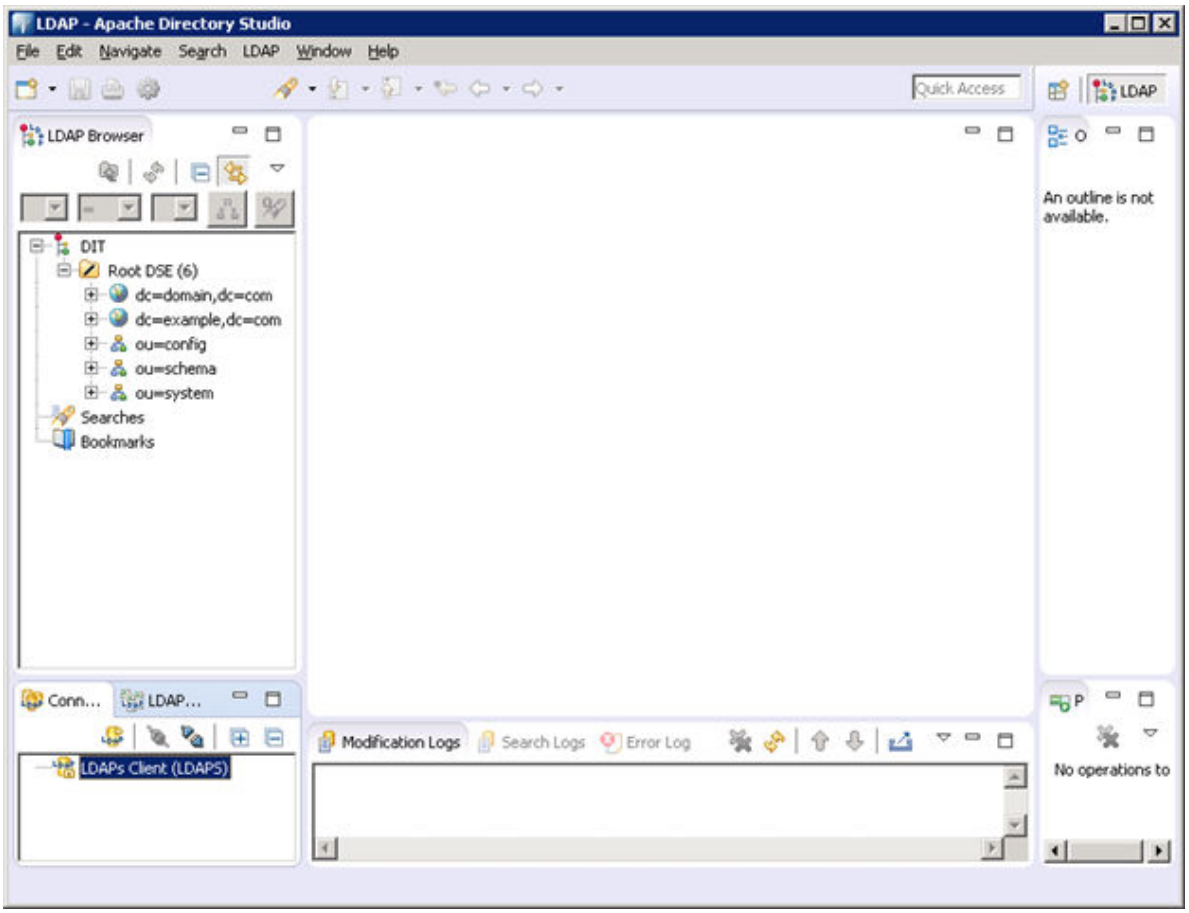
Related links

Apache Directory Studio Configuration on page 183

Creating LDAP users

Procedure

1. On Apache Directory Studio, go to the Connections view toolbar and double-click the LDAP connection.

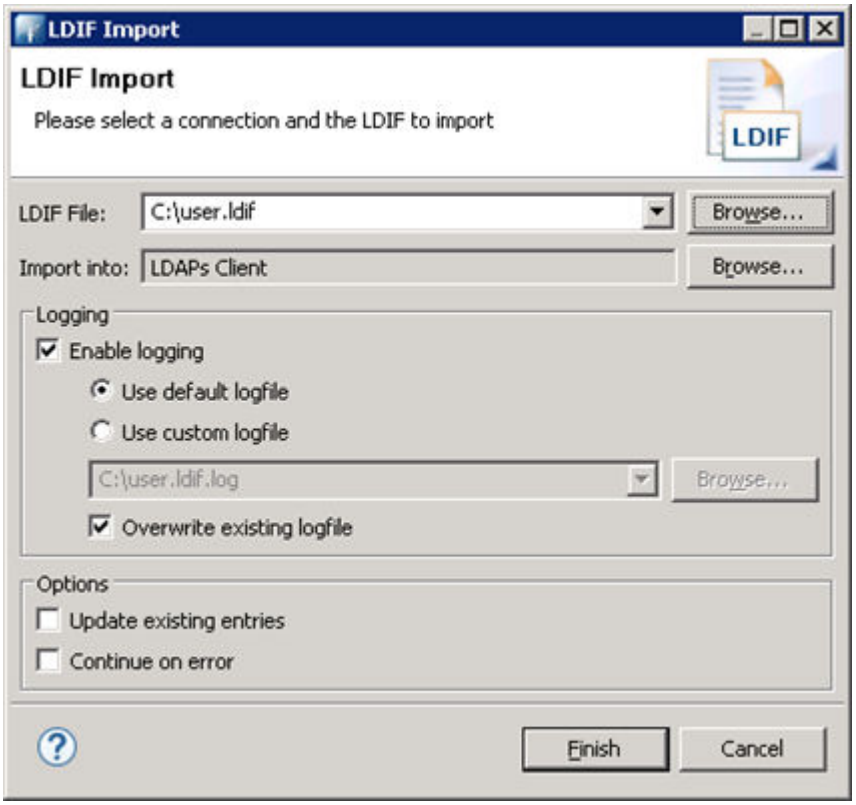


2. Create an LDIF file with the following details:

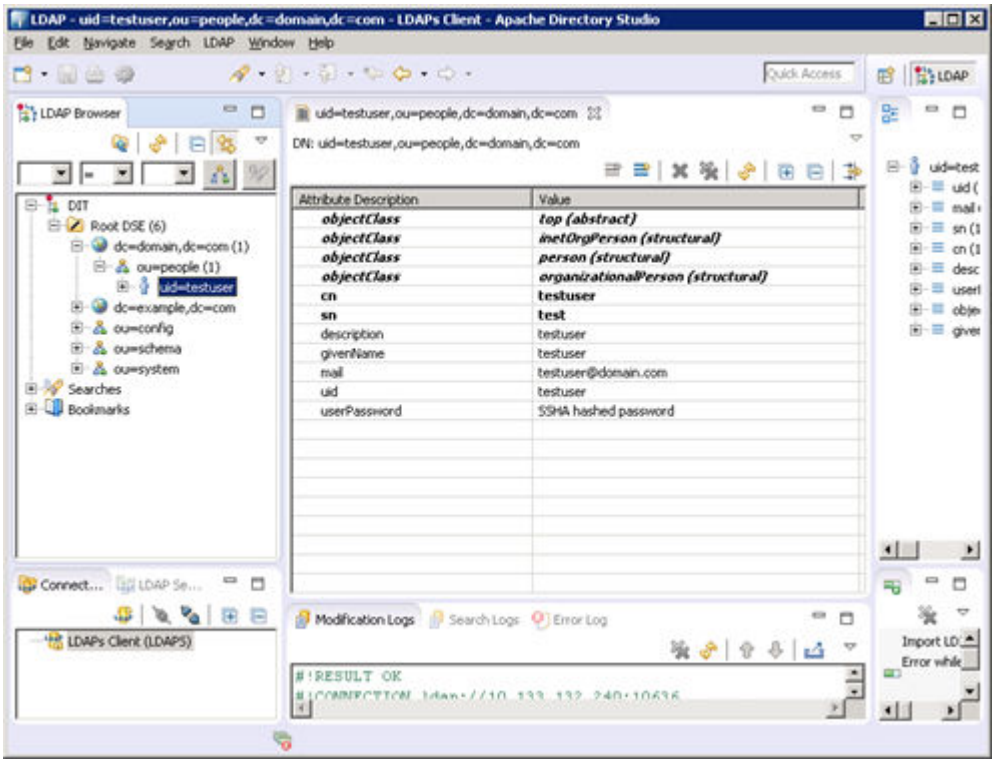
```
dn: ou=people,dc=domain,dc=com
objectClass: top
objectClass: organizationalUnit
ou: people


dn: uid=testuser,ou=people,dc=domain,dc=com
objectClass: top
objectClass: inetOrgPerson
objectClass: person
objectClass: organizationalPerson
cn: testuser
description: testuser
givenName: testuser
mail: testuser@domain.com
sn: test
uid: testuser
userPassword: 123456
```

3. Select `dc=domain, dc=com`.
4. Click **LDAP Browser** > **Root DSE**.
5. Right click on partition to import the above created `ldif` file from **Import** > **LDIF Import**.
6. Provide the LDIF file path and click **Finish**.



This will create the test under your partition/domain.



Related links

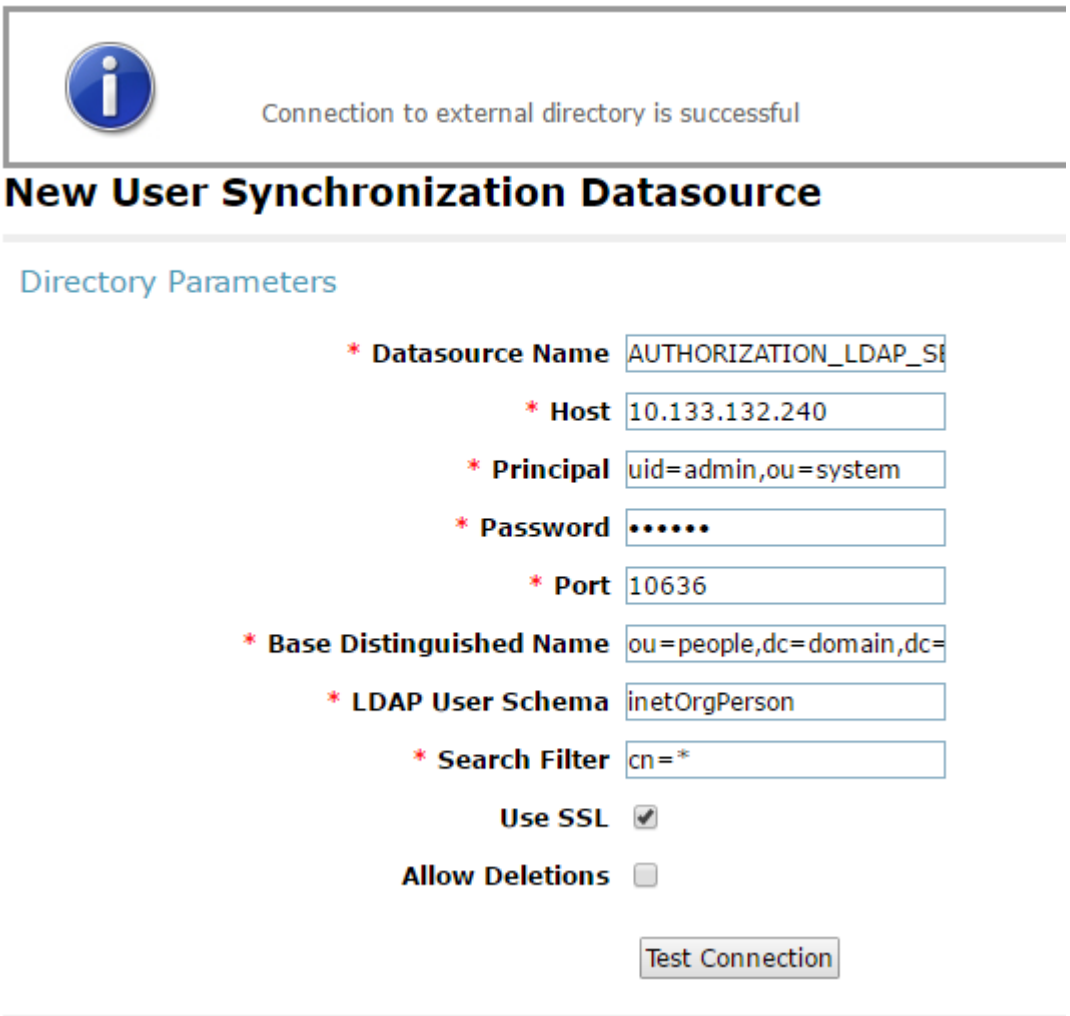
Apache Directory Studio Configuration on page 183

System Manager directory synchronization

Adding a data source in System Manager

Procedure

1. On the System Manager web console, navigate to **Users** > **Directory Synchronization**.
2. Add a new data source and enter the following LDAP server details, and click **Test Connection**.
   - **DS Name**
   - **Host**
   - **Principal**
   - **Port**
   - **Base DN**
   - **LDAP User Schema**
   - **Search Filter**
   - **Use SSL**: Select the check box.



Upon successful connection with the LDAP server, mapping attributes would be displayed.

3. Map the LDAP Server attributes with corresponding System Manager attributes and save.

```
description          -->  SourceUserKey
mail                 -->  loginName
sn                   -->  surname
givenName            -->  givenName
displayName          -->  displayName
```

Related links

Apache Directory Studio Configuration on page 183

Performing directory synchronization

Procedure

1. On System Manager, click **Users** > **Directory Synchronization**.
2. Click the Active Synchronization Jobs tab.
3. Click **Create New Job** to create a new job for the data source created earlier.

Synchronization should be successful and the system will display the number of records synced in Synchronization job history.

Related links

Apache Directory Studio Configuration on page 183

Active Directory Configuration

This section provides example configuration procedures for Active Directory. This section is purely for reference.

Related links

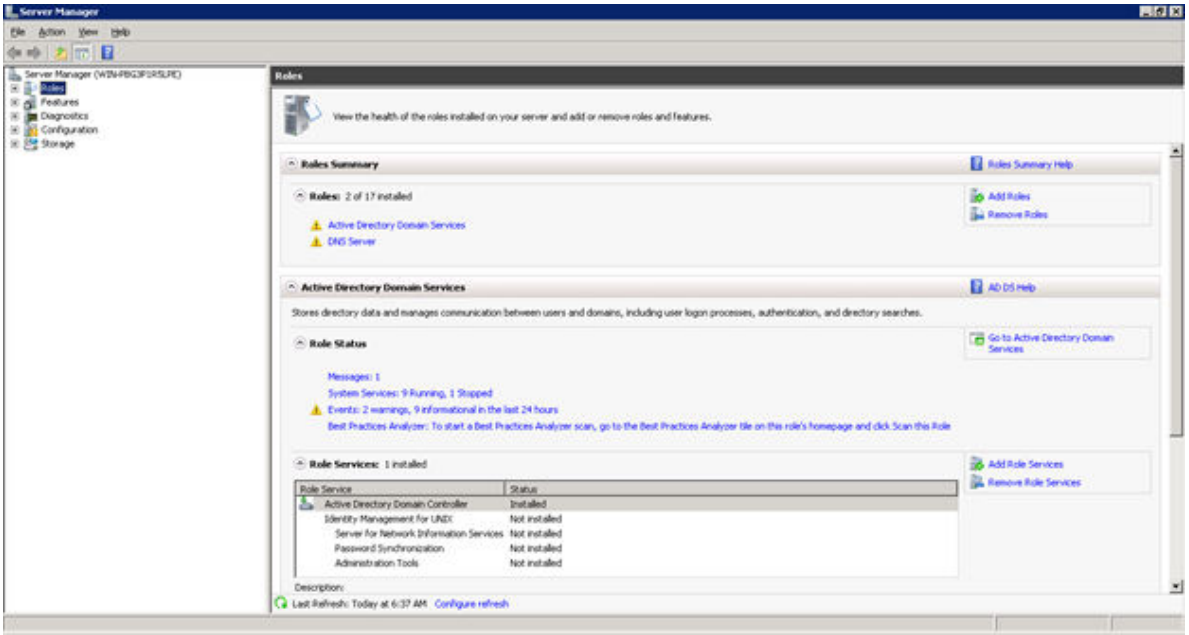
Performing directory synchronization on page 211
Inserting bulk users using batch file on page 214

Enabling SSL on Windows Server 2008

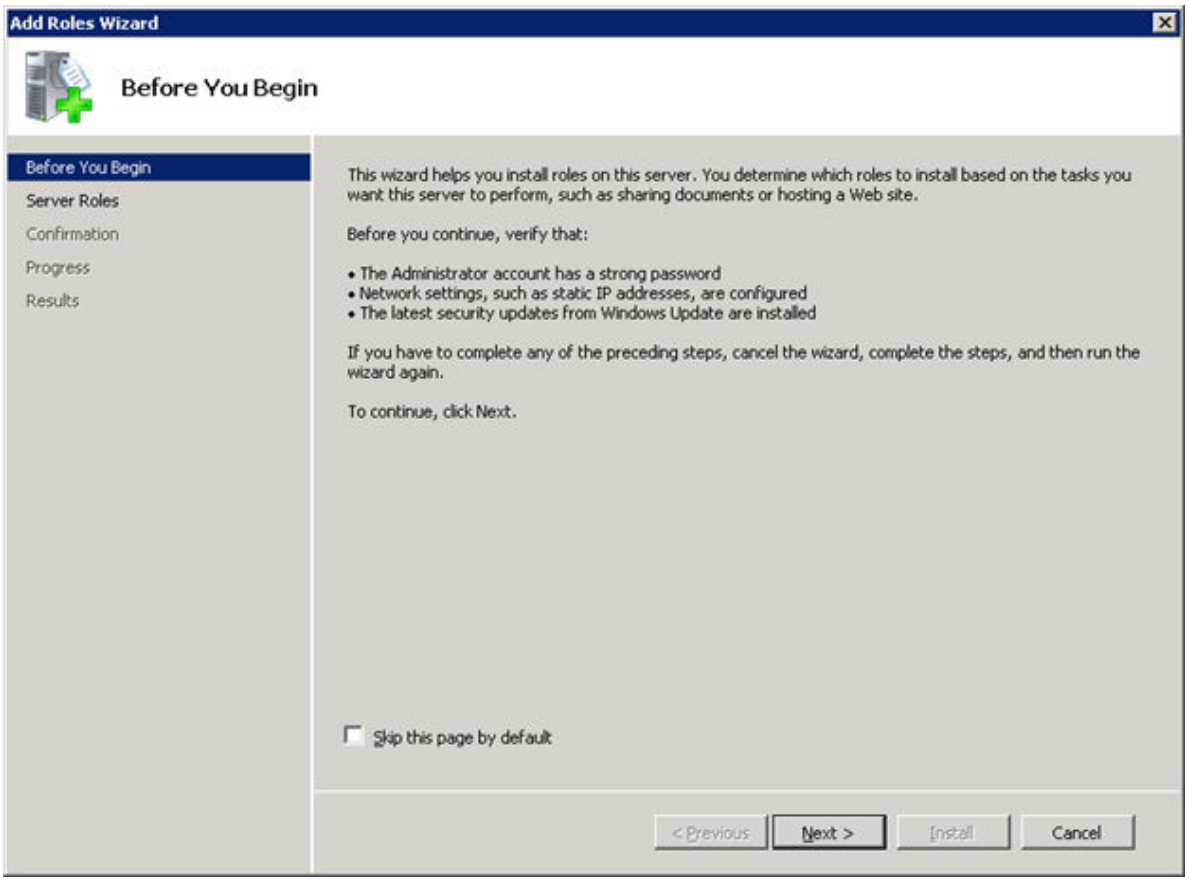
Installing and configuring Active Directory

Procedure

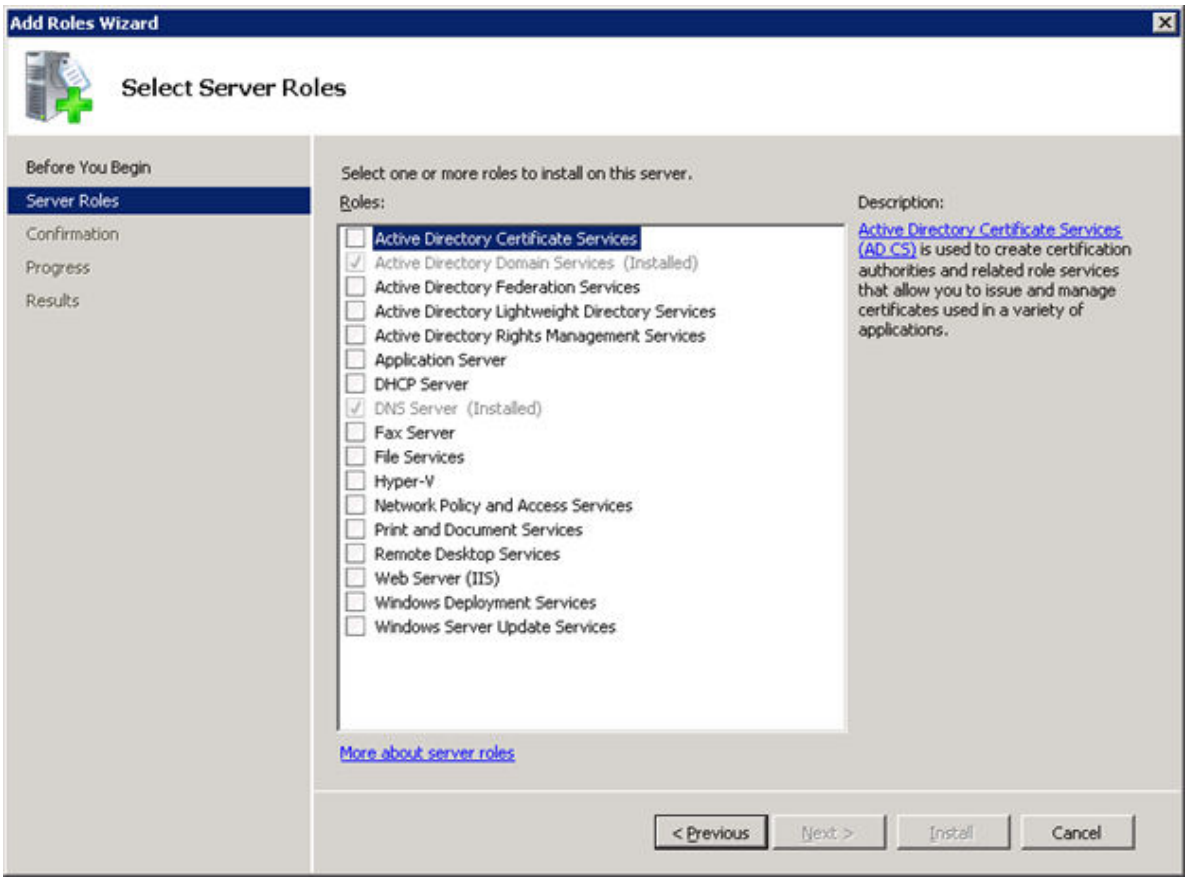
1. Log in to Windows server to enable SSL on Active Directory.
2. Go to **Server Manager Tool** by typing server manager in search program and files.



3. Click **Add Roles** in the **Roles Summary** section.

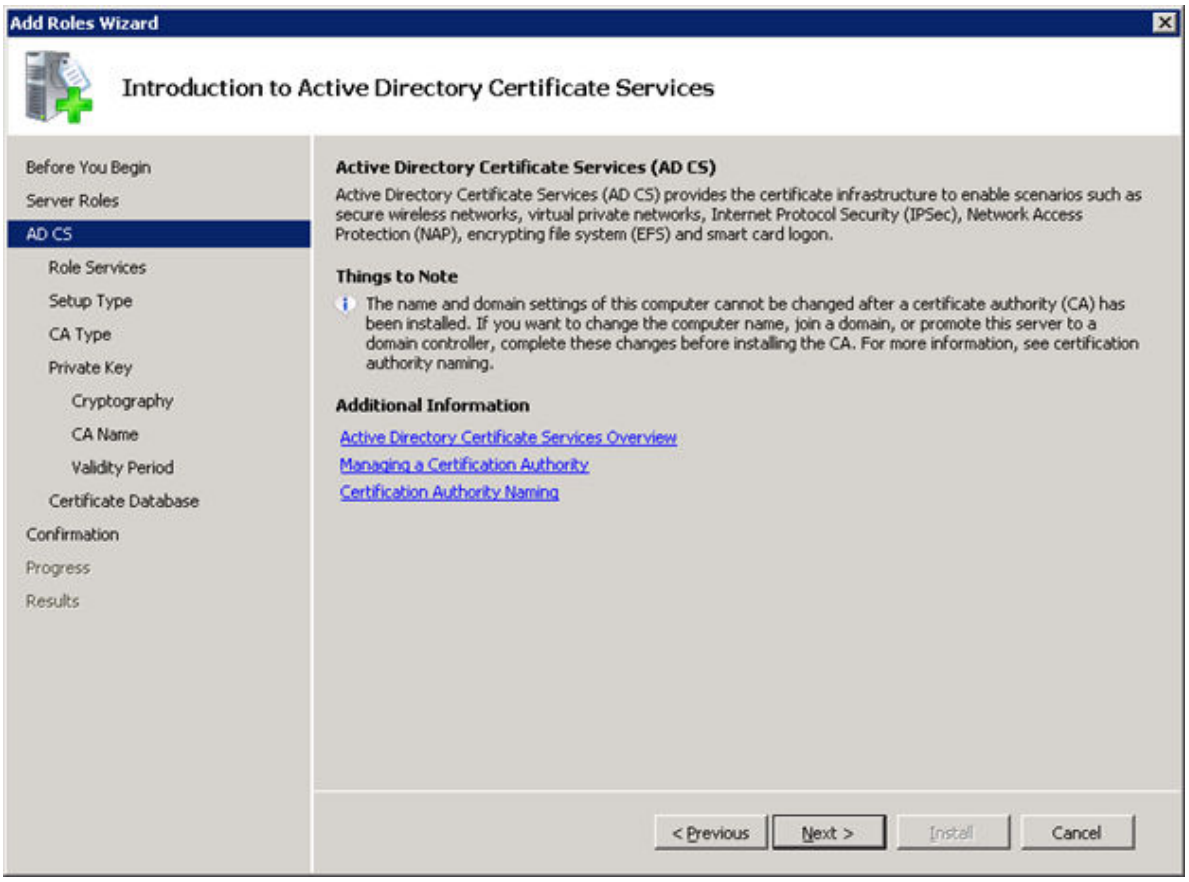


4. Click **Next** to proceed further to install **Active Directory Certificate Services**.



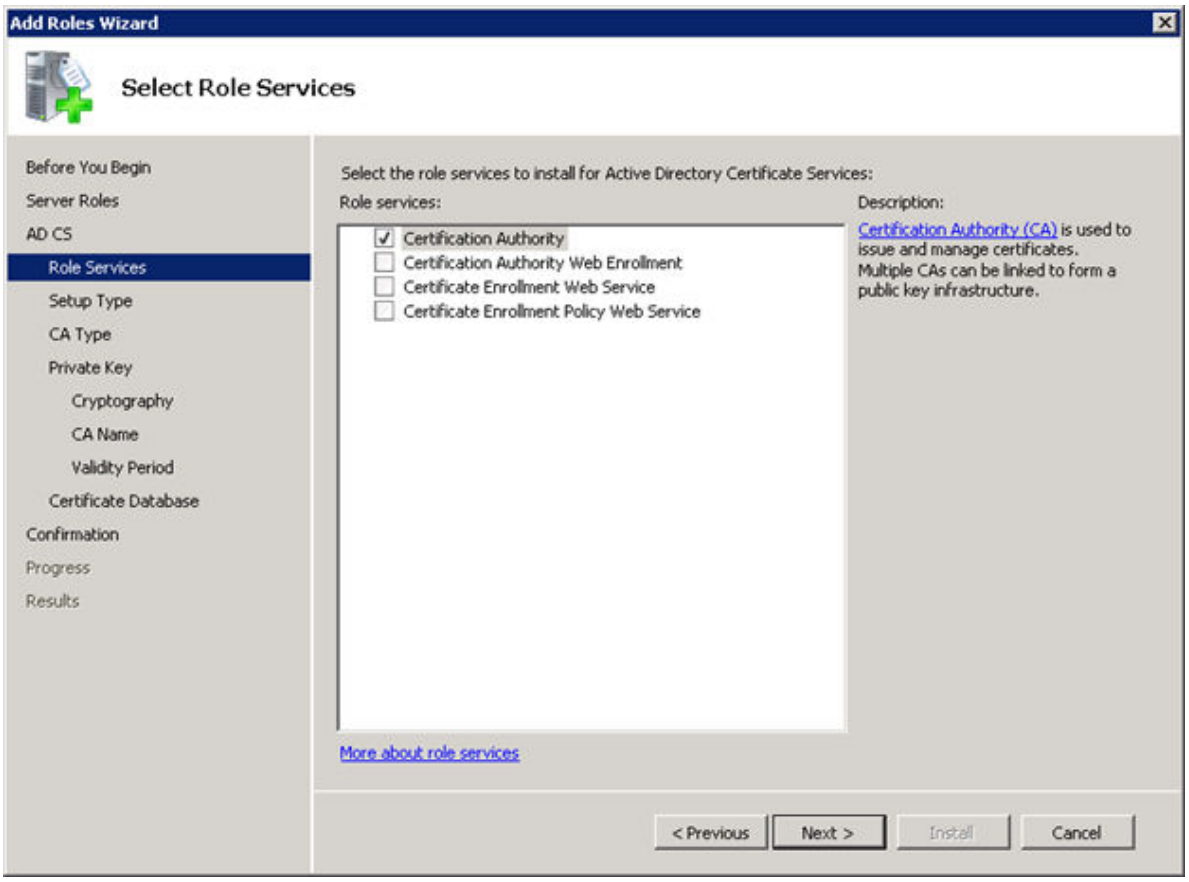
5. Click the **Active Directory Certificate Services** check box.

6. Click **Next**.



This window provides the introduction to Active Directory Certificate Services.

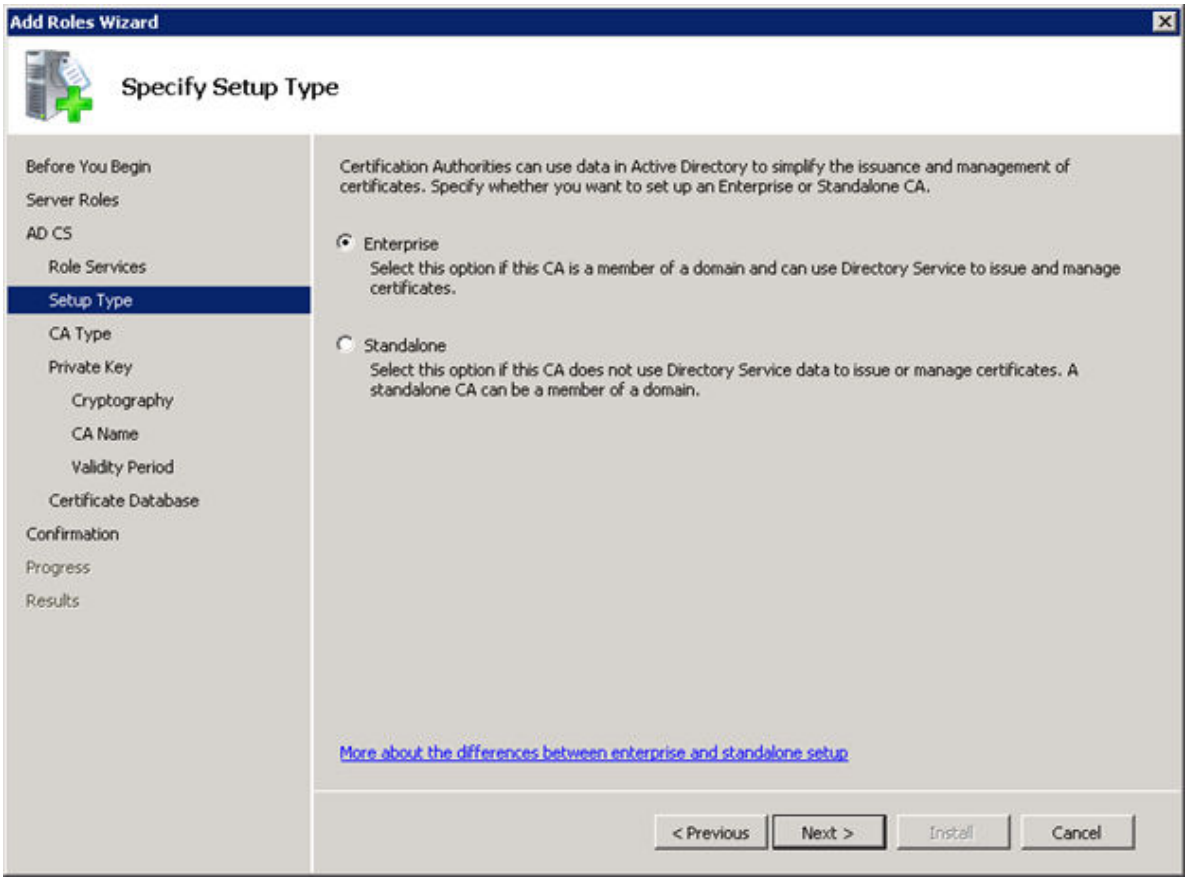
7. Click **Next**.



By default the first check box will be enabled.

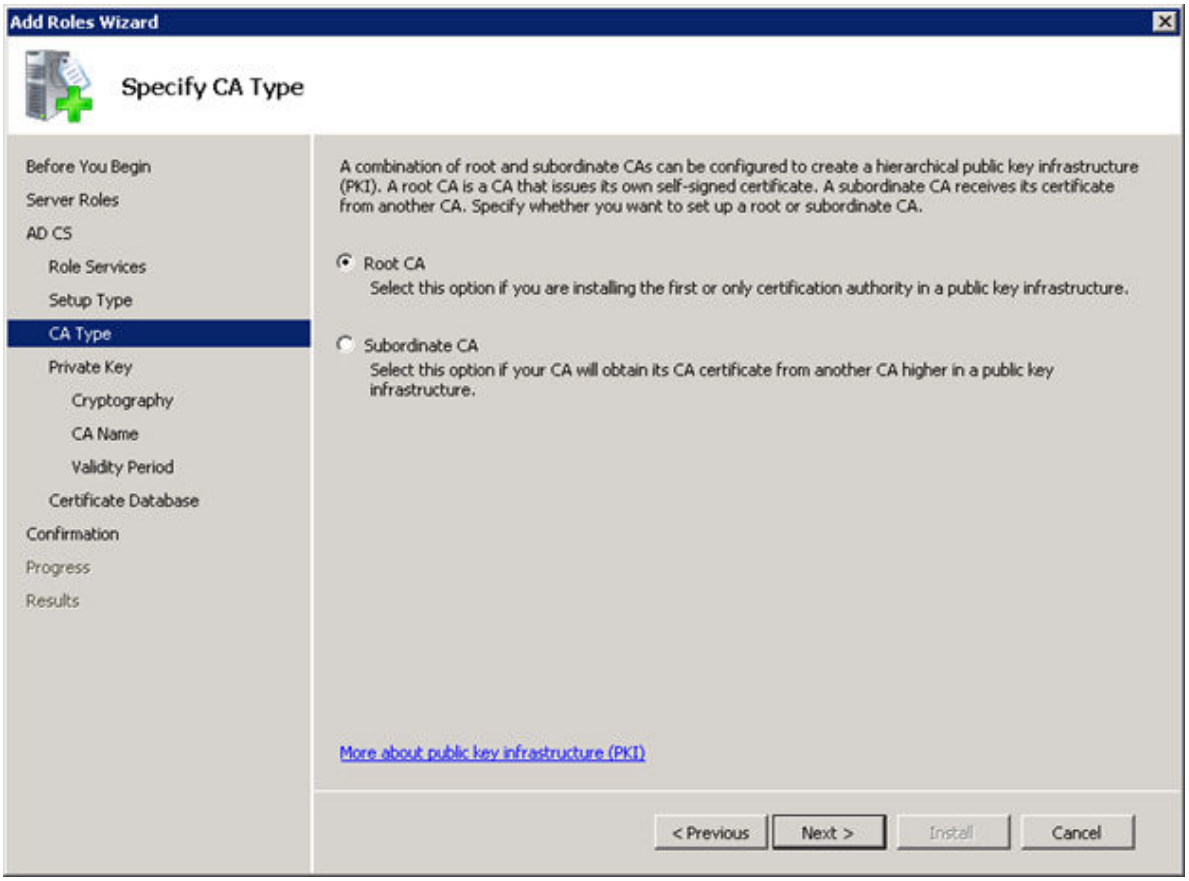
8. Click **Next**.

This window specifies set up type for the role installation.



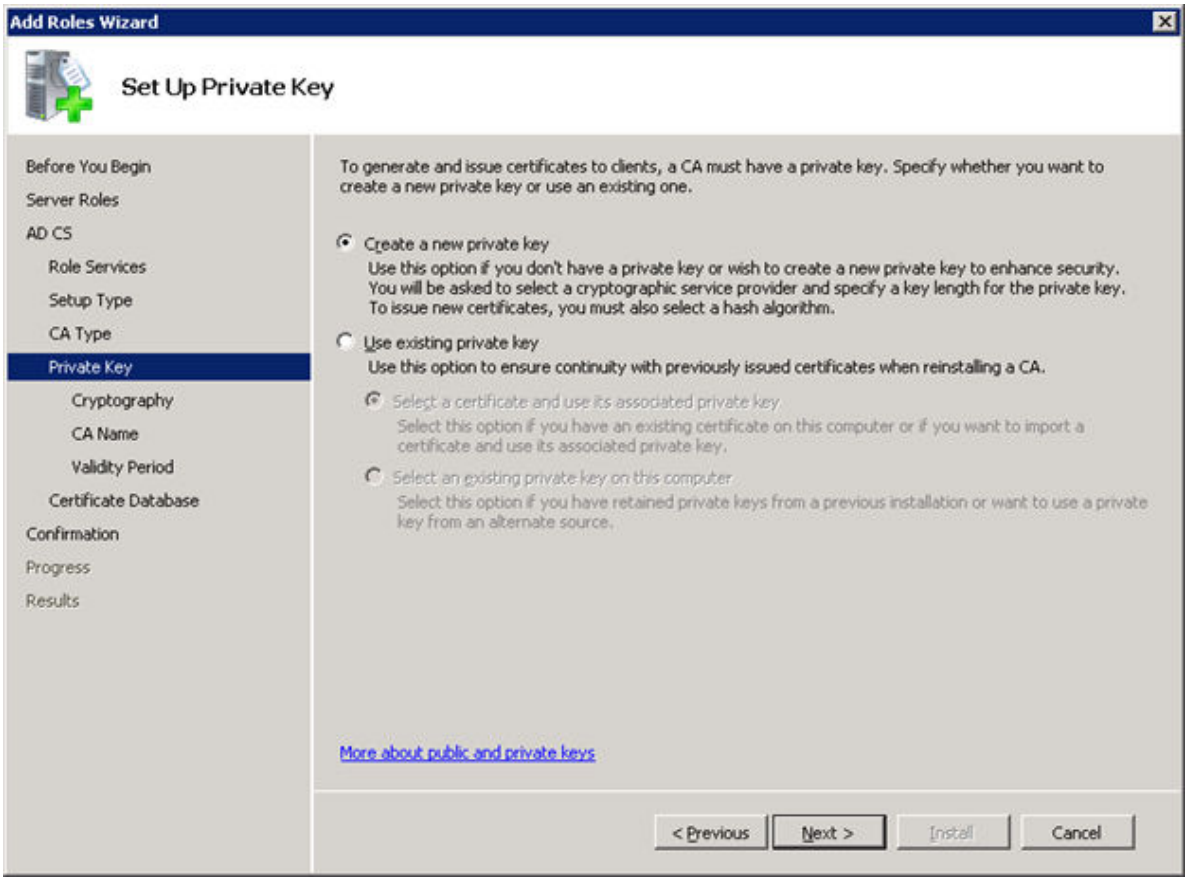
9. Click **Next**.

   The next window focuses on CA type to create hierarchical public key infrastructure.

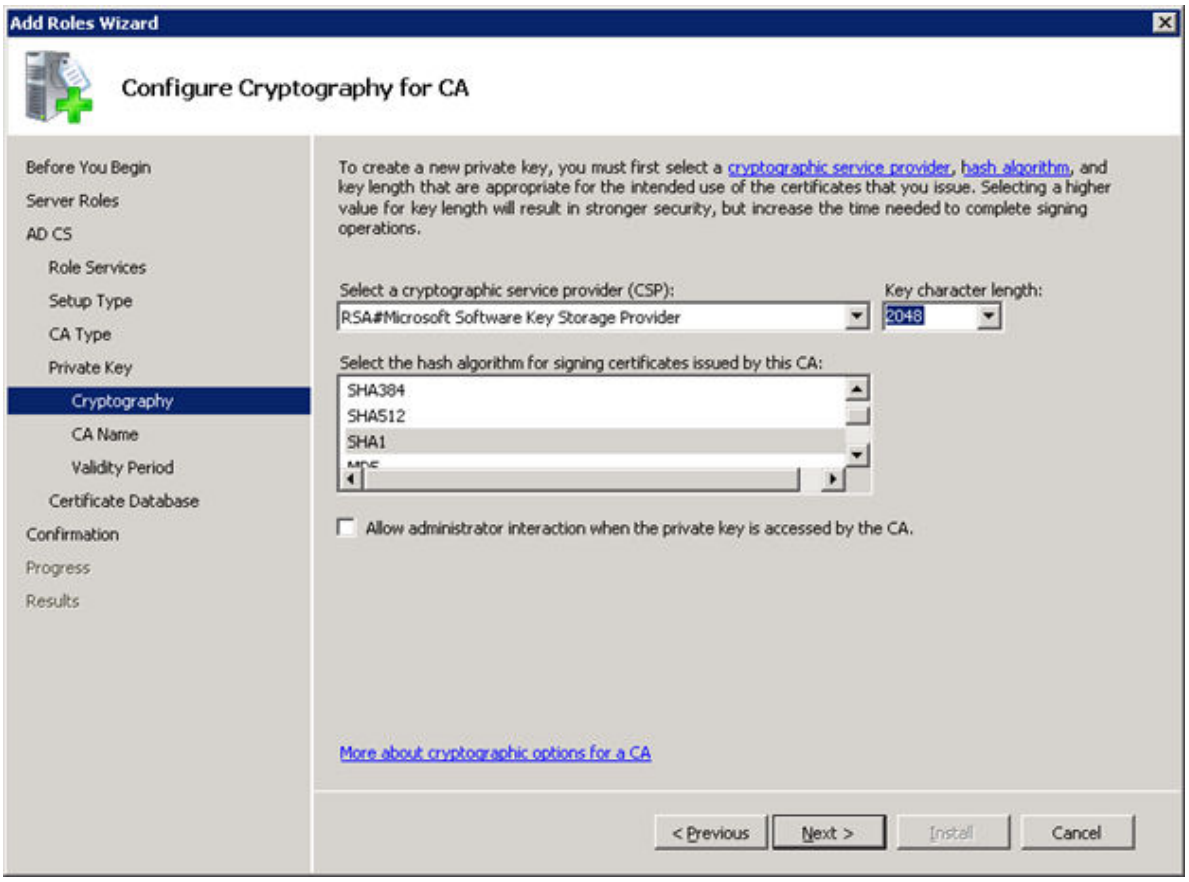


10. Click **Next**.

    This window focuses on Private Key generation and issues certificate to clients.

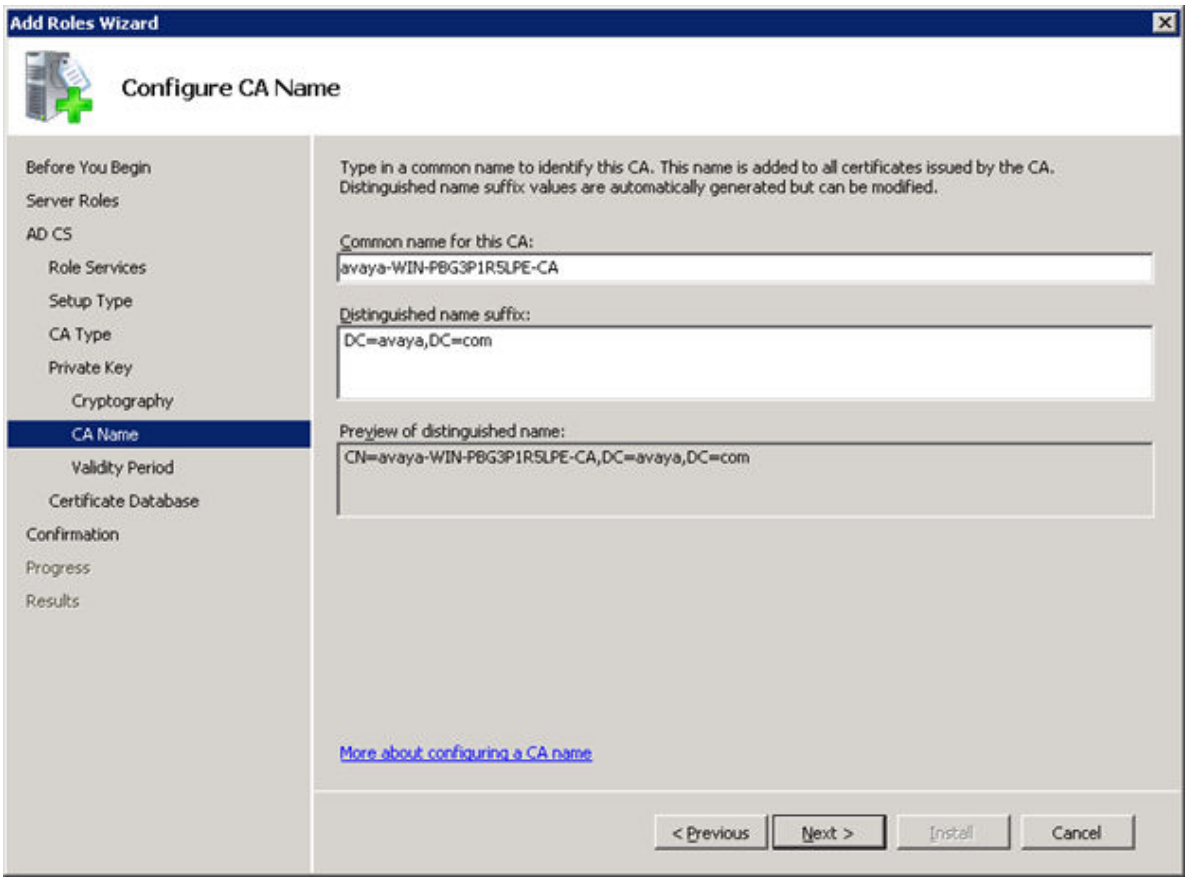

Add Roles Wizard
Set Up Private Key
Before You Begin
Server Roles
AD CS
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
To generate and issue certificates to clients, a CA must have a private key. Specify whether you want to create a new private key or use an existing one.
Create a new private key
Use this option if you don't have a private key or wish to create a new private key to enhance security. You will be asked to select a cryptographic service provider and specify a key length for the private key. To issue new certificates, you must also select a hash algorithm.
Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.
Select a certificate and use its associated private key
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.
Select an existing private key on this computer
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.
More about public and private keys
< Previous
Next >
Install
Cancel

11. Click **Next**.

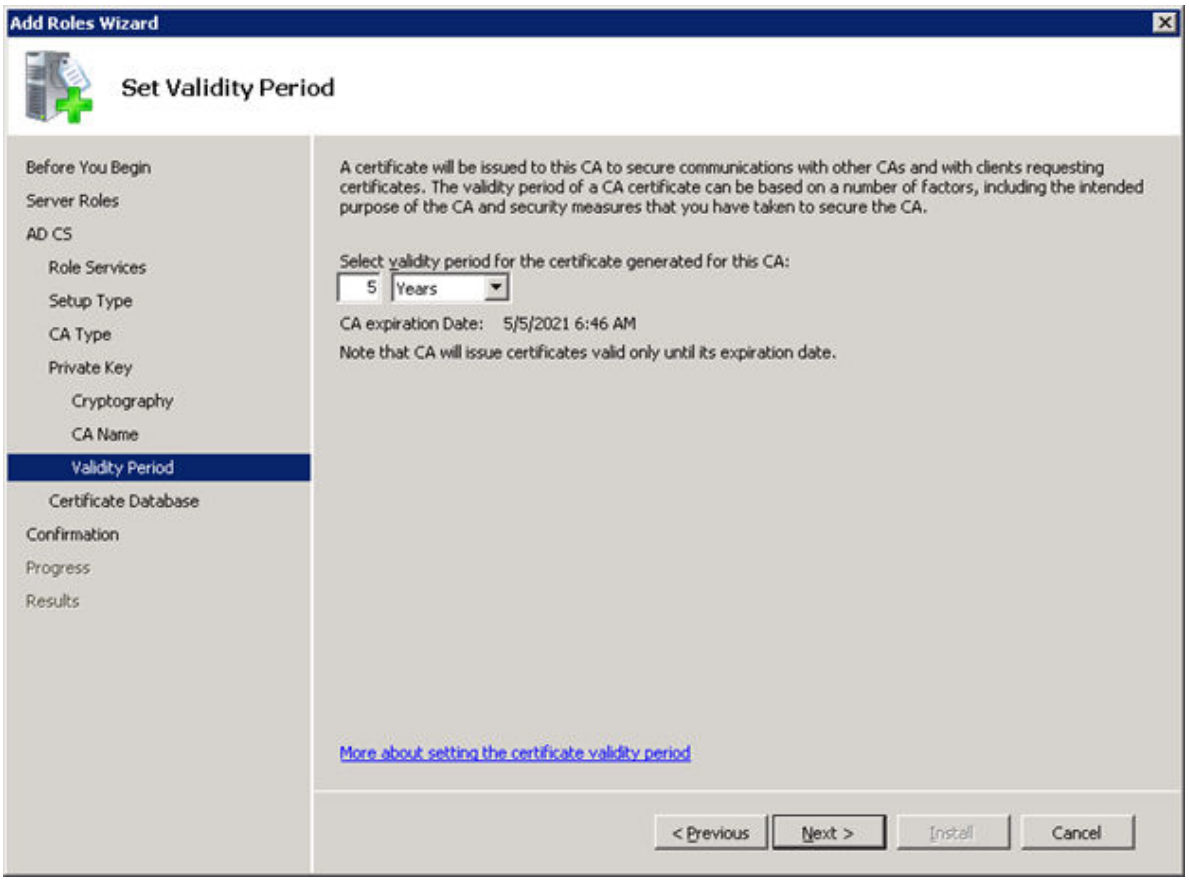


12. Click **Next**.

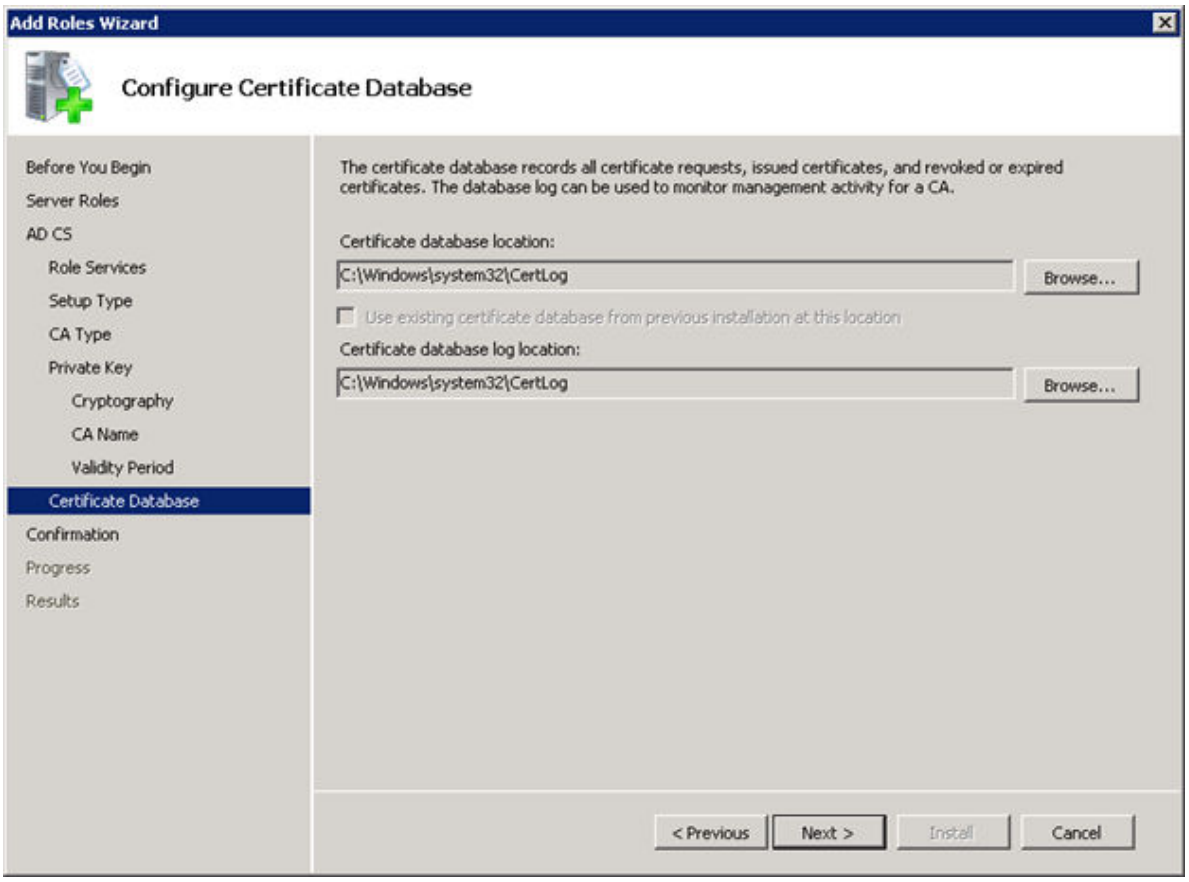
13. Configure the CA name and click **Next**.



14. Set the validity of the CA certificate, and click **Next**.

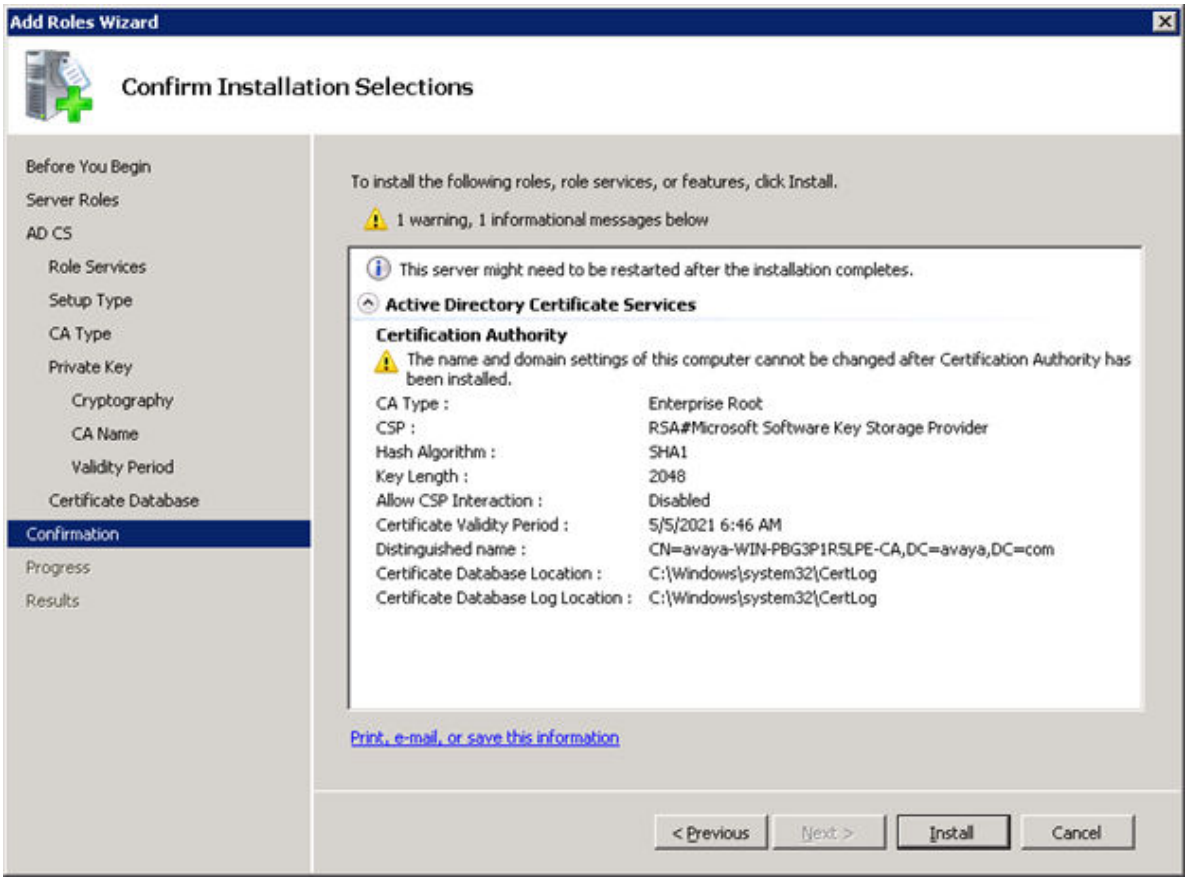


15. Configure the Certificate database.

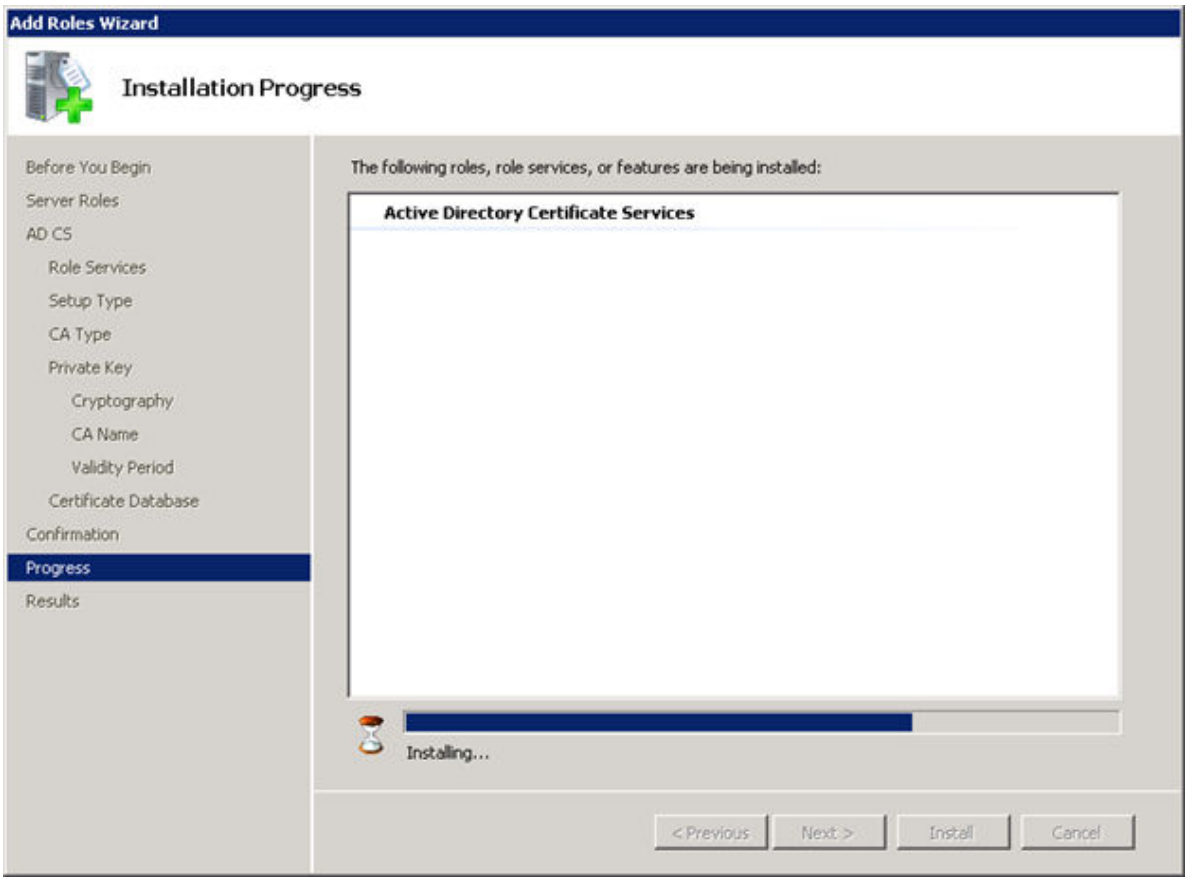


16. Click **Next**.

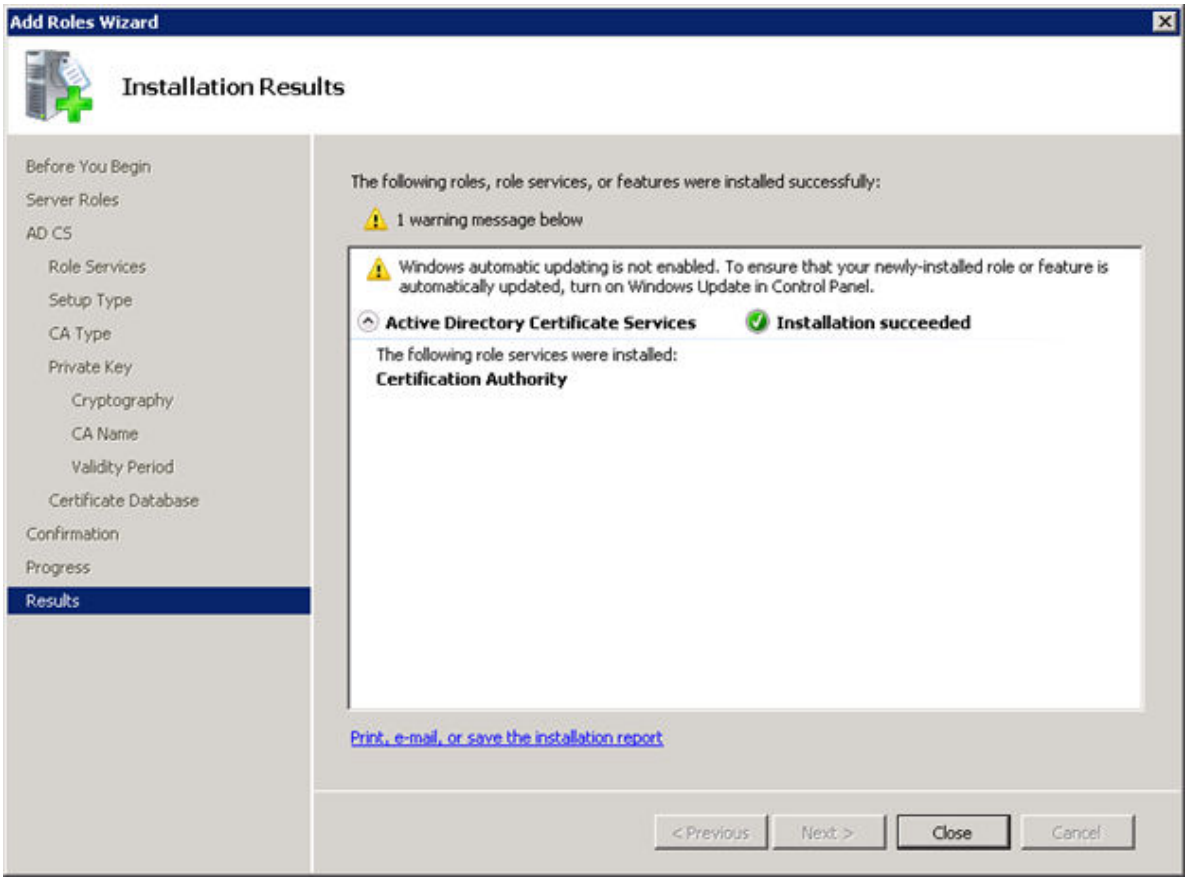
    This window displays the complete summary to begin the installation.


Add Roles Wizard
Confirm Installation Selections
Before You Begin
Server Roles
AD CS
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
To install the following roles, role services, or features, click Install.
1 warning, 1 informational messages below
This server might need to be restarted after the installation completes.
Active Directory Certificate Services
Certification Authority
The name and domain settings of this computer cannot be changed after Certification Authority has been installed.
CA Type : Enterprise Root
CSP : RSA#Microsoft Software Key Storage Provider
Hash Algorithm : SHA1
Key Length : 2048
Allow CSP Interaction : Disabled
Certificate Validity Period : 5/5/2021 6:46 AM
Distinguished name : CN=avaya-WIN-PBG3P1R5LPE-CA,DC=avaya,DC=com
Certificate Database Location : C:\Windows\system32\CertLog
Certificate Database Log Location : C:\Windows\system32\CertLog
Print, e-mail, or save this information
< Previous
Next >
Install
Cancel

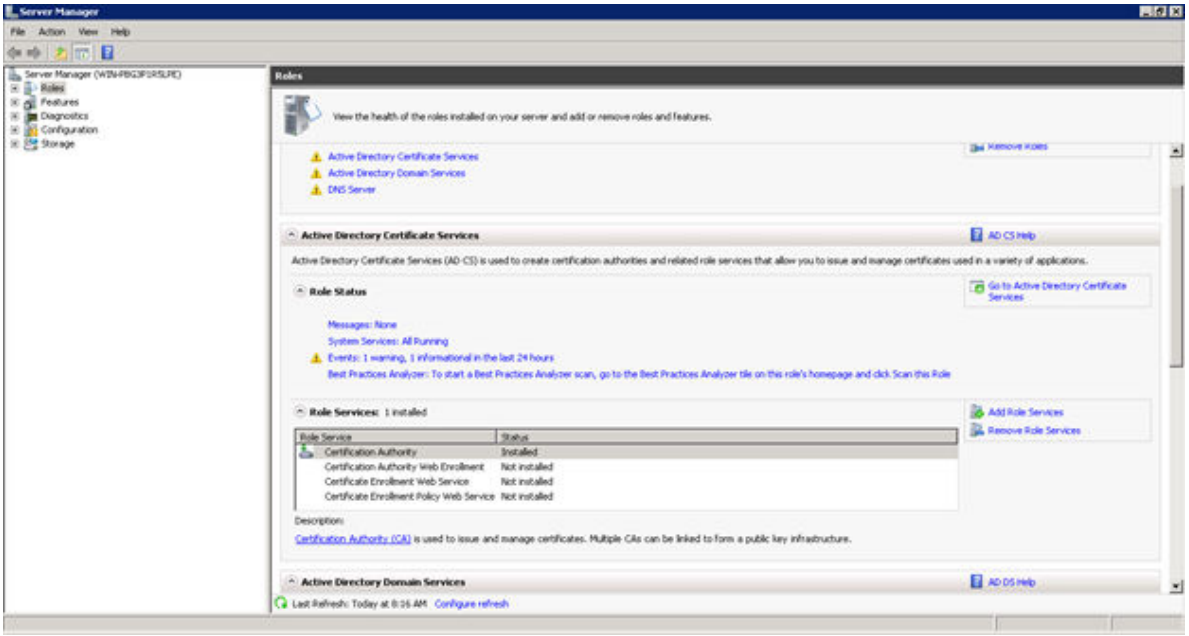
17. Click **Install**.



After the installation is completed, the following window is displayed.

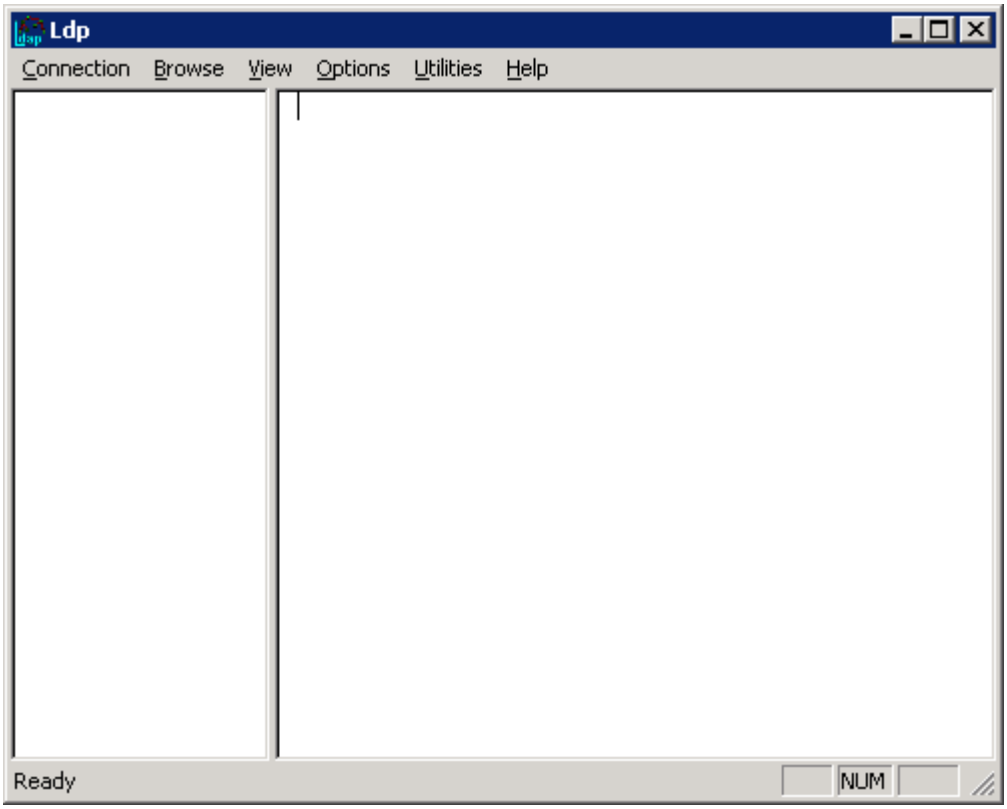


18. In the Server Manager window, you can see that the Certificate service has been installed successfully.

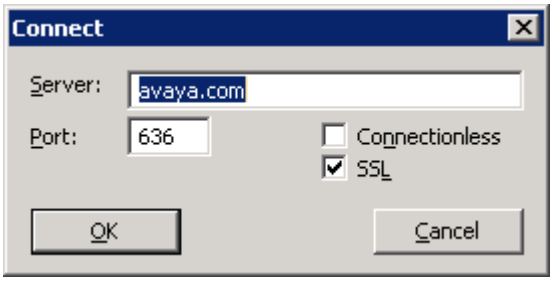


In the Role Services section, you can see the status of the service being shown as installed. After installation it is recommended to restart the Windows Server machine.

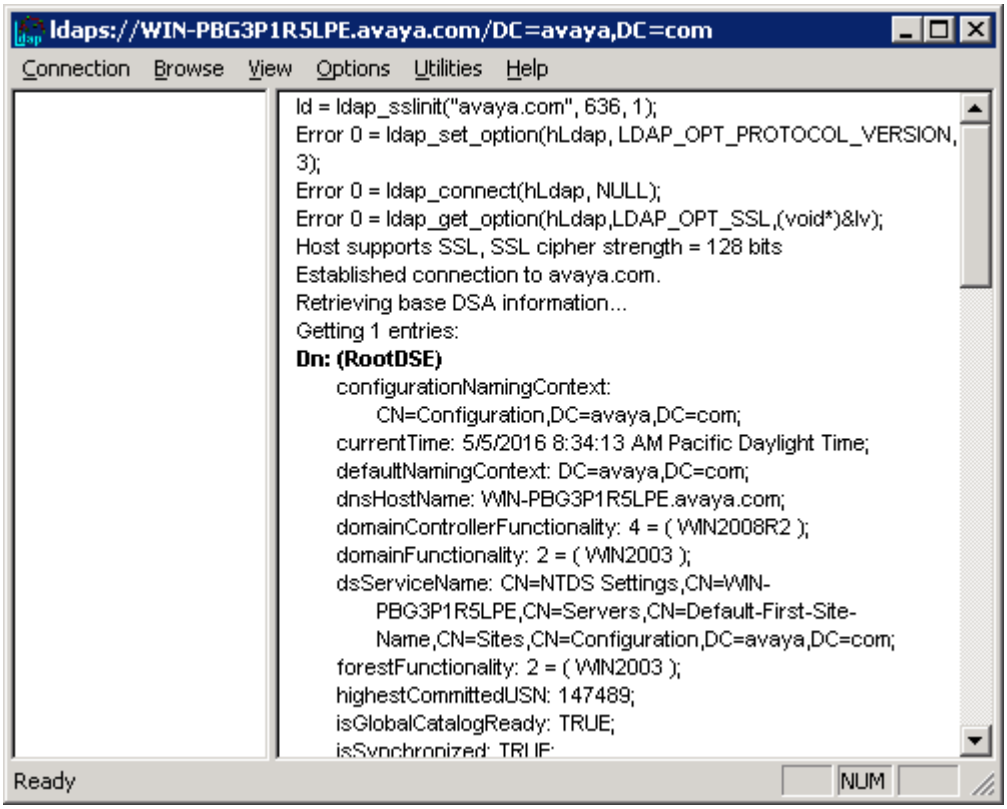
19. To check whether SSL is being enabled on Active directory, type `ldp.exe` in search programs and files.



20. Go to connection menu and select **Connect**.
21. In the **Server** field, specify domain name of server and in the **Port** field, enter the port number, and select the **SSL** check box to connect to Active Directory.



Active Directory now supports SSL.



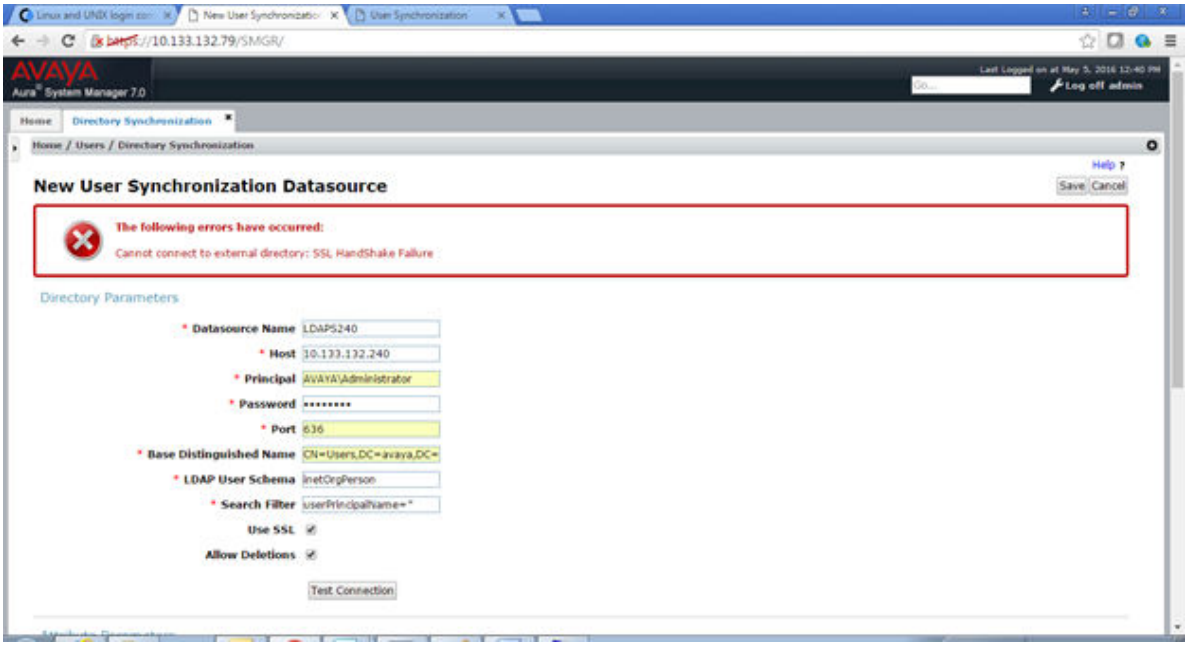
Related links

Active Directory Configuration on page 195

Performing directory synchronization

Procedure

1. On System Manager, click **Users** > **Directory Synchronization**.
2. Add a new data source and enter the following LDAP server details, and click **Test Connection**.
   - **DS Name**
   - **Host**
   - **Principal**
   - **Port**
   - **Base DN**
   - **LDAP User Schema**
   - **Search Filter**
   - **Use SSL**: Select the check box.
   - **Allow Deletions**: Select the check box.

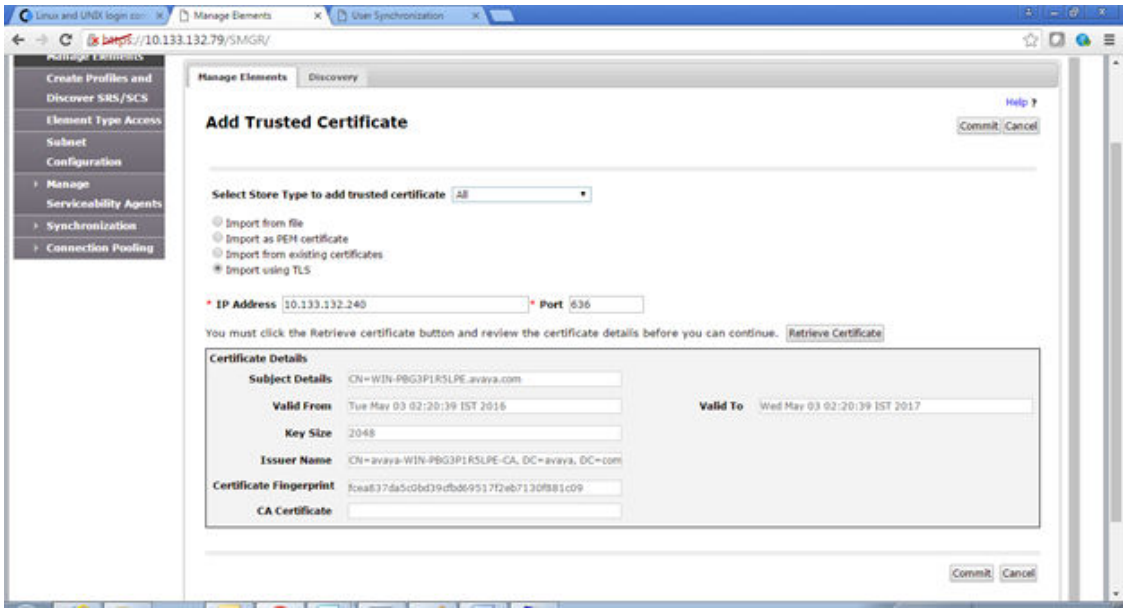


As shown in the figure, the system displays the following error: `Cannot connect to external directory: SSL Hand Shake Failure`.

The system displays this error because we have not imported the Active Directory Certificate in System Manager.

3. To resolve we need to import the Certificate:
   a. Navigate to **Services** > **Inventory** > **Manage Elements**.
   b. Select the System Manager instance and click **More Actions** > **Configured Trusted Certificates**.
   c. Click **Add**.

d. Select the **Import using TLS** field.



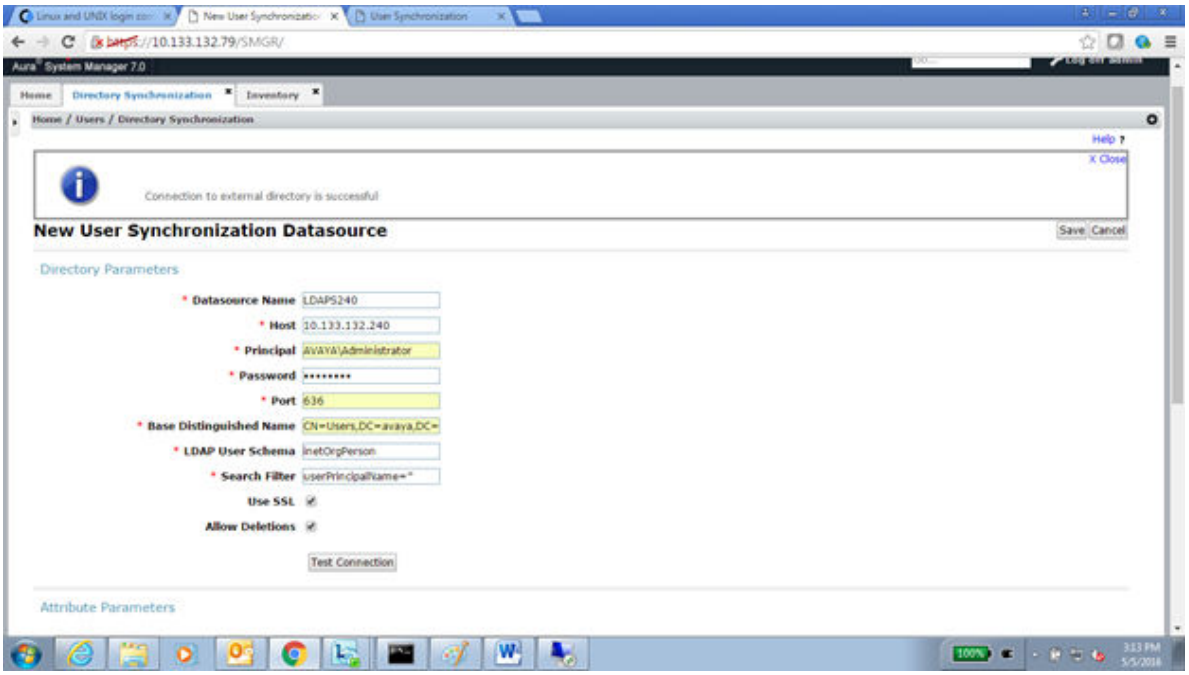
e. In the **IP Address** field, enter the IP address of the LDAP server.

f. In the **Port** field, enter the port of the LDAP server.

g. Click **Retrieve Certificate** to import the certificate

h. Click **Commit**.

4. Go to the **New User Synchronization** data source page and specify the details to test the connection.



Related links

Active Directory Configuration on page 195

Inserting bulk users using batch file

Procedure

1. Go to the Windows Server command prompt.
2. Navigate o to the folder where the batch file is located.
3. Type the name of batch file to insert users.

   For example, `bulkUsersInsert.bat`
4. Press `Enter`.

Related links

Active Directory Configuration on page 195

Open LDAP configuration

This section provides example configuration procedures for OpenLDAP. This section is purely for reference.

Related links

Installing and configuring Open LDAP on CentOS 6.3 on page 214
Performing System Manager directory synchronization on page 217

Installing and configuring Open LDAP on CentOS 6.3

Procedure

1. Log in as root user and install the following three packages:
   - openldap-servers: This package contains the main LDAP server.
   - openldap-clients: This package contains all required LDAP client utilities.
   - openldap: This packages contains the LDAP support libraries.

     To install, run the following command: `yum install -y openldap openldap-clients openldap-servers`.
2. Edit the `ldap.conf` file and enter the IP address or domain name of your server.

   ```
   vi /etc/openldap/ldap.conf
   URI ldap://10.133.132.210
   BASE dc=avaya,dc=com
   ```
3. Copy the parameter file to the LDAP database directory.

   ```
   cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
   ```

   LDAP needs the parameter file to start a new database.

4. Copy the sample `slapd` file from `/usr/share/openldap-servers` to `/etc/openldap`.

```
cp /usr/share/openldap-servers/slapd.conf.obsolete /etc/openldap/slapd.conf
```

5. Setup a new root password and run the password utility to run generate a secure password and copy the password as you need to enter the password in `slapd.conf`.

```
Slappasswd
New password:openldap
Re-enter new password:openldap
{SSHA}xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

6. Update the slapd.conf file to reflect your environment: database section where the domain and password are updated.

```
vi /etc/openldap/slapd.conf
:%s/dc=my-domain/dc=avaya/g           #This regex will replace all the instances
of my-domain with your domain name.
#Enter the below key with password value which is generated in previous steps
rootpw {SSHA}xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

The password is the output of the slappasswd utility.

7. Create a `root.ldif` file and enter the following details.

```
vi /root/root.ldif
#root
dn: dc=avaya,dc=com
dc: avaya
objectClass: dcObject
objectClass: organizationalUnit
ou: avaya.com
```

8. Remove everything in slapd.d directory and tell the slapd for root.ldif file

```
rm -rf /etc/openldap/slapd.d/*
slapadd -n 2 -l /root/root.ldif
```

9. Verify The Configuration files. Use slaptest command to verify the configuration file.

```
slaptest -u
config file testing succeeded
```

```
slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d
config file testing succeeded
```

10. Set the appropriate permissions.

```
chown -R ldap:ldap /var/lib/ldap
chown -R ldap:ldap /etc/openldap/slapd.d
```

11. Make sure the service is on on the runlevel 3.

```
chkconfig --level 235 slapd on
```

12. To start the ldap server, enter the following command from a terminal window.

```
service slapd start
```

13. Restart the service again after setting up.

```
rm -rf /etc/openldap/slapd.d/*
slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d
chown -R ldap:ldap /etc/openldap/slapd.d
service slapd restart
```

14. Test that you can connect to the LDAP server.

```
ldapsearch -h localhost -D "cn=Manager,dc=avaya,dc=com" -w
<openldap_root_password> -b "dc=avaya,dc=com" -s sub "objectclass=*"
```

<openldap_root_password> is the Open LDAP root password which was configured in Step 5.

15. Create sample LDIF file to create LDAP directory structure.

```
vi ldap_init.ldif
dn: dc=avaya,dc=com
dc: avaya
objectClass: dcObject
objectClass: organizationalUnit
ou: avaya.com

dn: ou=dev,dc=avaya,dc=com
objectClass: top
objectClass: OrganizationalUnit
ou: dev

dn: ou=people,ou=dev,dc=avaya,dc=com
objectClass: top
objectClass: OrganizationalUnit
ou: people
```

16. Load initial data into the directory. You can do this using an LDIF file and then run the `ldapadd` command.

```
ldapadd -x -D "cn=Manager,dc=avaya,dc=com" -W -f ldap_init.ldif
```

17. Test that you can connect to the LDAP server.

```
ldapsearch -h localhost -D "cn=Manager,dc=avaya,dc=com" -w
<openldap_root_password> -b "dc=avaya,dc=com" -s sub "objectclass=*"
```

<openldap_root_password> is the Open LDAP root password which was configured in Step 5.

18. Create an SSL certificate for LDAPs.

```
cd /etc/pki/tls/certs
rm slapd.pem
make slapd.pem
chmod 640 slapd.pem
chown :ldap slapd.pem
mkdir /etc/openldap/cacerts/
ln -s /etc/pki/tls/certs/slapd.pem /etc/openldap/cacerts/slapd.pem
```

19. Start the LDAP servers.

```
vi /etc/sysconfig/ldap
SLAPD_LDAPS=yes
```

20. Add or update the following lines to the global section of the `/etc/openldap/slapd.conf` file.

```
vi /etc/openldap/slapd.conf
TLSCACertificateFile /etc/pki/tls/certs/ca-bundle.crt
TLSCertificateFile /etc/pki/tls/certs/slapd.pem
TLSCertificateKeyFile /etc/pki/tls/certs/slapd.pem
```

21. Add the following lines to the configuration file for the LDAP server, `/etc/openldap/ldap.conf`.

```
vi /etc/openldap/ldap.conf
TLS_CACERTDIR /etc/openldap/cacerts
```

22. Restart the service again after setting up.

```
rm -rf /etc/openldap/slapd.d/*
slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d
chown -R ldap:ldap /etc/openldap/slapd.d
service slapd restart
```

Related links

Open LDAP configuration on page 214

Performing System Manager directory synchronization

Procedure

1. On System Manager, click **Services** > **Inventory** > **Manage Elements**.
2. Select the System Manager instance and click **More Actions** > **Configured Trusted Certificates**.
3. Click **Add**.
4. Select the **Import using TLS** field.
5. In the **IP Address** field, enter the IP address of the LDAP server.
6. In the **Port** field, enter the port of the LDAP server.
7. Click **Retrieve Certificate** to import the certificate
8. Click **Commit**.

Related links

Open LDAP configuration on page 214

Configuration of ADFS as an SAML provider

The topics in this section describe an example of how to enable SAML authentication with Active Directory Federation Services (ADFS).

Prerequisites

- Active Directory and Active Directory Federation Services must be configured.
- Avaya Breeze™ Authorization Service must be installed.
- The Service Provider metadata of the Avaya Breeze™ instances with Authorization Service must be available on the Active Directory setup.

Configuration of Service Provider on Active Directory Federation Services

Adding a new Relying Party

Procedure

1. On the Active Directory system, go to **Server Manager** > **Tools** > **Select Active Directory Federation Services Management**.
2. On the Active Directory Federation Services screen, click **Relying Party Trusts**.
3. Click **Add Relying Party Trust**.
4. On the **Add Relying Party Trust** Wizard, select **Claims Aware**, and click **Start**.
5. On the Select Data Source screen, select the **Import data about the relying party from a file** option.
6. Click **Browse**.
7. Locate and select the SP metadata file downloaded from the Avaya Breeze™node.
8. On the Specify Display Name screen, enter a name.

   For example, BreezeNode112.
9. On the Choose Access Control Policy screen, select **Permit everyone** and click **Next**.
10. On the Ready to Add Trust screen, click **Next**.
11. Click **Finish**.
12. On the Relying Party Trusts screen, right-click the newly added entry and click **Properties**.
13. On the Properties screen, select **Advanced**.
14. Change the secure hash algorithm to **SHA-1** and click **Apply**.

Adding the UPN Custom Rule

Procedure

1. On the Active Directory system, go to **Server Manager** > **Tools** > **Select Active Directory Federation Services Management**.
2. On the Active Directory Federation Services screen, click **Relying Party Trusts**.
3. Make a note of the **Identifier** of the newly added entry.
4. Right-click on the entry and select **Edit Claims Issuance Policy**.
5. Click **Add Rule**.
6. On the Select Rule Template page, in the **Claim Rule Template** field, select **Send Claims using a custom rule**.

7. On the Configure Claim Rule page, enter the Display Name as `UPNCustomRule` and add the following code in the **Custom Rule** section:

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"]
 => issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/
nameidentifier",
          Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer,
               Value = c.Value, ValueType = c.ValueType,
               Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/
claimproperties/format"]
                    = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
               Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/
claimproperties/namequalifier"]
                    = "http://idp01.bbb.local/adfs/services/trust",
               Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/
claimproperties/spnamequalifier"]
                    = "BREEZE_IDENTIFIER");
```

8. Modify the Custom Rule section and replace the `BREEZE_IDENTIFIER` text with the Identifier noted in Step 3.
9. Click **Finish**.

Adding an LDAP Attribute Rule

Procedure

1. On the Active Directory system, go to **Server Manager** > **Tools** > **Select Active Directory Federation Services Management**.
2. On the Active Directory Federation Services screen, click **Relying Party Trusts**.
3. On the Relying Party Trusts screen, right-click the newly added entry and select **Edit Claims Issuance Policy**.
4. Click **Add Rule**.
5. On the **Select Rule Template** screen, in the **Claim Rule Template** field, select **Send LDAP Attributes as Claims**.
6. On the Configure Claim Rule page, enter a name in **Claim Rule Name**.

   For example, you can enter the E-mail address.
7. Select the Active Directory configured as the **Attribute Store**.
8. In the Mapping of LDAP Attributes to outgoing claim types section, select the LDAP attribute to be mapped to Outgoing Claim Type.
9. Click **Finish**.

Result

This setting will enable Active Directory Federation Services to send the authenticated user email address as a SAML Attribute statement when responding to Authorization Service with a SAML assertion.

Disabling Revocation checks for Signing certificate and Encryption certificates

About this task

Active Directory Federation Services fails an authentication request if it is unable to perform Authorization Service (SP) certificate revocation checks. Use the following procedure to disable Revocation checks.

Procedure

1. Open Windows PowerShell on the Active Directory setup.
2. Run the following command with **Relying Party Trust Identifier**:

```
Get-AdfsRelyingPartyTrust -Identifier <Identifier> | Set-AdfsRelyingPartyTrust
-SigningCertificateRevocationCheck None -EncryptionCertificateRevocationCheck None
```

Configuration of the IdP of Active Directory Federation Services on System Manager

Downloading the Active Directory Federation Services metadata file

Procedure

You can download the file from the Active Directory URL:

```
<FQDN>/FederationMetadata/2007-06/FederationMetadata.xml
```

Removing sections from the Active Directory Federation Services metadata file

Procedure

1. Edit the downloaded metadata file and remove the following sections:
   - Ds:Signature
   - RoleDescription
   - SPSSODescriptor
2. Ensure that the metadata file has only the following two sections:
   - EntityDescriptor
   - IDPSSODescriptor

SAML attribute UserID

As the LDAP attribute claim being sent by Active Directory Federation Services in the current configuration is email address, Active Directory Federation Services sends the user email address as a SAML assertion attribute:

```
<AttributeStatement>
<Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">
<AttributeValue>testuser</AttributeValue>
```

```
</Attribute>
</AttributeStatement>
```

You must specify this attribute when configuring SAML authentication on System Manager.

Configuring SAML Authentication

Procedure

1. Determine the metadata file and the SAML attribute to be used as UserID .
2. On System Manager, click **Elements** > **Avaya Breeze™** > **Configuration** > **Authorization** > **Authentication Mechanism**.
3. Click **Change Authentication Mechanism**.
4. In the **Authentication Mechanism** field, select **SAML**.
5. In the **UserID** field, enter: `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress`.
6. In the **Authentication Context** field, select **Password Protected Transport**.
7. In the **Authentication Context Comparison Type** field, select **exact**.
8. Click **Next**.
9. Browse and select the Active Directory Federation Services metadata file.
10. Click **Save**.

Enabling SAML profile

Procedure

1. Go to **Avaya Breeze™** > **Configuration** > **Attributes** > **Service Clusters**.
2. Select the Cluster where Authorization Service has been installed and in the **Service** field, select **Authorization**.
3. In the **SAML Profile** field, select **Deploy**.
4. Click **Commit**.

Testing the setup

Procedure

Perform one of the following:

- Deploy an Authorization Client snap-in which has been integrated to use the Avaya Breeze™ Authorization Code Grant flow.
- Use the Authorization Sample snap-ins provided in the Avaya Breeze™ SDK.

LDAP authentication will provide the end-user with an AD FS login screen when trying to access the Client snap-in. On successful authentication, the user is redirected back to the Client with a logged-in session.

Index

A

activating a new identity certificate 153
Active Directory 195
Active Directory Configuration 195
add
    trusted CA certificates 164
Add Data Source in SMGR 193
Adding
    LDAP Attribute Rule 219
    new Relying Party 218
    UPN Custom Rule 218
adding a JDBC data source 72
adding a JDBC provider 70
adding a JDBC provider resource 70
adding an external Authorization Client
    Authorization client 60
Administration
    Geographic redundancy 79
alarming
    geographic redundancy 82
Allow Cross-origin Resource Sharing for all 69
Apache Directory Studio 183
application, creating 40
application sequences
    assigning a user 49
    creating 40
    description 40
    origination 49
    termination 49
assigning and editing grants for authorization 59
assigning a user
    to an application sequence 49
assigning instance
    clusters 18
assigning ports field descriptions 132
assigning service ports for snap-ins 76
assigning to users
    service profile 51, 53
Attribute Configuration page description 89
attributes
    clusters 89
    configure 35
    configuring 33, 89
    description 37
authentication
    SAML 64
Authentication Instance 94
authentication mechanism 66
Authorization Client 92
Authorization Clients 59
    Avaya Breeze Authorization Client 59
    External Authorization Client 60
Authorization Configuration field descriptions
    field descriptions 91
Authorization Resources 58
Authorization Service 58, 93
    getting Service Provider metadata 65
Authorized Clients 58
Avaya Breeze Authorization Client 59
Avaya Breeze certificate 165
Avaya Breeze instance administration 139
AvayaNetSetup 175

B

backup
    field descriptions 96
back up 26
Backup and Restore Status 96
Backup Storage Configuration
    field descriptions 97
batch file 214
bundle
    uninstalling 47
Bundle Details and Installation Status 100
bundles 45
Bundles
    field descriptions 97
Bundle the Identity Certificate and Private Key into a PKCS #12 container 156

C

CA 185
call-intercept snap-in
    deployment checklist 29
    testing 41
cancel 28
CEnetSetup 175
certificate management 145
Certificate Revocation Management 168
certificate signing request 86, 161
certificate signing request (CSR) generation 153
Certificates issued by System Manager 149
Certificate validations 166
Certificate validations for SIP TLS connections 166
change 71
check_breeze_status.sh 178
client certificate challenge
    HTTPS 68
client certificate for HTTP security 118
cluster
    reboot 17
Cluster DB Backup field descriptions 107
cluster editor

cluster editor *(continued)*
field descriptions 108
clusters
assigning server 18
create 13
delete 17
field description 108
load balancing 24
new 13
removing servers 20
view 13
view attributes 13
Clusters
assign snap-ins 21
configuring snap-in attributes 34
delete servers 19
installing snap-ins 21
snap-ins 21
uninstall snap-ins 22
clusters attributes
editing 15
configure cluster level service attributes 33
Configure features field descriptions
field descriptions 93
configure global level service attributes 33
configure service attributes 33
service profiles 33
configuring
SAML authentication example 217
snap-in attributes 33, 35
Configuring
IDP on SMGR 65
SAML Authentication 221
configuring attributes
global 35, 89
service profile 89
snap-ins 33
Configuring attributes at cluster level 34
configuring service invocation 38
configuring service ports 76
configuring snap-in attributes
clusters 34
Create Grant 92
creating
an application 40
an application sequence 40
new administered user 52
service profile 37
creating a new cluster 13
CSR 86
CSR and Private Key generation via OpenSSL 154
current usage 143
custAccounts 178

D

data source
data source *(continued)*
delete 73
edit 73
default SIP CA 126
delete
a service 129
a service profile 134
deleting a JDBC data source 73
Deleting an external Authorization Client
Authorization client 61
Deleting a Reliable Eventing destination
Eventing destination 56
Deleting a Reliable Eventing group
Eventing group 56
deleting clusters 17
deleting JDBC provider resources 71
deleting services 45
Deleting the Bundle 47, 48
Demo certificates 150
deployment checklist
call-intercept snap-in 29
non-call-intercept snap-in 29
deployment procedures 138
Destination Status field descriptions
field descriptions 116
Determining whether you are using a demo identity certificate
..... 150
dial pattern
Callable Services 42
directory synchronization 194, 211, 217
Disabling
revocation checks 220
downloading
SNMP MIB 142
Downloading
Active Directory Federation Services metadata file 220

E

Edit Grants 92
Editing a JDBC data source 73
Editing a Reliable Eventing group
Eventing group 55
editing cluster attributes 15
editing JDBC provider resource 71
Editing the configuration 186
Edit Keys 93
Enable Cluster Database 25
Enabling
SAML Profile 221
SAML profile for Authorization 66
end entity 184
End User Authentication 61
EULA 32
event catalog configuration
field description 116
event catalog configuration field descriptions 116

Event catalog editor
page description 117
Event catalog editor field descriptions 117
example
enabling SAML authentication 217
explicit user administration 52
External Authorization Client 60

F

Fault management
geographic redundancy 82
field descriptions 95
Attribute Configuration 89
Avaya Breeze Instance Editor 94
Bundles 100
Cluster administration 101
Cluster DB Backup 107
dependencies 100
HTTP Security 118
Implicit User Profile Rule Editor 120
Implicit User Profiles 119
Install Trusted Certificate 121
Maintenance Tests 123
Reliable Eventing Group Editor 126
Server Administration 126
Service Databases 132
Service Profile Configuration 134
Service Profile Editor 134
Services 129
Service Status 135
SNMP MIB Download 136
field descriptions, cluster editor 108

G

geographic redundancy 81
Geographic Redundancy 79
replication
restoration 83
System Verification Tests 84
terminology 78
Geographic Redundancy replication 83
Geographic Replication data restoration 83
getting
Service Provider metadata for Authorization Service ... 65
global attributes 35, 89

H

HTTP CORS security
administering 69
configuring 69
HTTP load balancing 23
HTTP Security page description 118
HTTPS security
HTTPS security *(continued)*
whitelist 68

I

identity certificate 87, 160
identity certificates 147
Identity Certificates lifecycle 157
idle server 21
implicit sequencing 49
description 40
implicit user pattern 43
Implicit User Profile Rule Editor page description 120
Implicit User Profiles page description 119
insert bulk users 214
InSite Knowledge Base 173
install
a service 129
trust certificates 25, 138
Installation Status
field descriptions 101
Installing the Bundle 46
install status
service 95, 126, 135
Install Trusted Certificate page description 121

J

JDBC data source 70
add 72
change 73
delete 73
edit 73
field descriptions 122
modify 73
query validation 74
remove 73
JDBC Data Source Editor
field descriptions 123
JDBC data source field descriptions 122
JDBC provider
add 70
create 70
new 70
JDBC provider editor
field descriptions 121
JDBC provider resource
edit 71
field descriptions 121
JDBC provider resources
delete 71
remove 71
JDBC resource providers 70

L

LDAP Authentication 62
LDAP Client 189
LDAP server 184
LDAP server certificate 63
LDAP Server certificate 63, 185
LDAP users 191
legacy 69
load a service 129
load balancing 24
    restrictions 23
    validations 23
Loading a bundle 46
loading snap-ins
    service 32
load snap-ins 32
logging
    geographic redundancy 82
logging configuration 141

M

maintenance procedures 141
maintenance test
    broker 57
maintenance tests 126
    on-demand 142
Maintenance Tests page description 123
Management and SPIRIT identity certificates attributes 159
managing JDBC providers 70
managing JDBC resources 70
mandatory applications 40
manual switch over 20
Media Server Monitoring, field descriptions 124
MIB download 136, 142
modify 71

N

new administered user
    creating 52
new cluster
    field description 108
New External Authorization Client field descriptions
    field description 91
non-call-intercept snap-in
    deployment checklist 29
    testing 41

O

Obtaining new SIP Identity Certificate 162
Open LDAP 214
Open LDAP configuration 214
origination application sequence 49
overview 11

P

peak usage 143
    reset 143
Peer Certificate Validation 166
PKCS#12 container 162
preferred version
    setting 35
private key 85
purge 28

R

reboot system 126
regenerating keys 60
release notes 173
Reliable Eventing 54
Reliable Eventing group
    creating 54
Reliable Eventing Group Editor field descriptions 126
Reliable Eventing Groups field descriptions
    field descriptions 125
Reliable Eventing status 56
Removing 19
removing servers from a cluster
    validations 20
Removing trusted CA certificates 165
Replacing an Identify Certificate by a third party CA issued certificate 152
Replacing an Identify Certificate with an System Manager CA issued certificate 151
replacing an Identity Certificate 161
replacing identity certificate 160
reserving ports field descriptions 132
Resource server
    features 59
Resource Server 93
Resources servers tab
    servers tab 92
restore 27
    field descriptions 96
routing policy
    callable services 41

S

SAML attribute 220
SAML authentication 64
    configuration example 217
sample configuration
    database providers 74
Searching service profiles 39
security
    HTTP 118

security *(continued)*
trust certificates ... 25, 138
trusted certificates ... 121, 126
Security Module HTTP identity certificate attributes ... 158
Security Module SIP identity certificate attributes ... 157
Server Administration page description ... 126
service
attributes ... 33
delete ... 45
snap-in ... 43
stop ... 44
service checksum ... 135
Service instances tab
instances tab ... 93
service invocation
configure ... 38
service packs ... 173
service ports
assign ... 76
change ... 76
configure ... 76
Presence ... 76
services ... 76
snap-ins ... 76
Service ports
field descriptions ... 132
service profile
adding services ... 134
adding snap-ins to new ... 37
assigning to users ... 51, 53
assigning users ... 51
attributes ... 89
Callable Services ... 43
creating ... 37, 134
deleting ... 134
description ... 37
implicit user pattern ... 43
modifying ... 134
selecting snap-in version ... 37
uses ... 37
Service Profile Configuration page description ... 134
Service Profile Editor page description ... 134
service profiles
service invocation ... 38
Service profiles
search ... 39
users assigned ... 39
Service Provider
getting metadata for Authorization Service ... 65
services
adding to service profile ... 134
configuring attributes for a service profile ... 33
delete ... 129
deleting from service profile ... 134
install ... 129
load ... 129
reinstall ... 135
services *(continued)*
uninstall ... 44
services in a service profile list ... 95
Service Status page description ... 135
setting up load balancing ... 24
shutdown system ... 126
SIP identity certificate ... 161
snap-in
installation ... 35
loading ... 32
start ... 43
stop ... 44
snap-in attributes
configuring ... 33, 35
snap-in install status ... 35
snap-in ports ... 132
snap-ins
uninstall from clusters ... 22
Snap-ins
clusters ... 21
SNMP MIB
downloading ... 142
SNMP MIB Download page description ... 136
standby server ... 21
starting a service ... 43
starting a snap-in ... 43
stopping a service ... 44
Stopping a snap-in ... 44
Store types ... 26
support ... 173
System Manager root CA certificate ... 165
System Resource Monitoring ... 136
system state ... 126

T

termination application sequence ... 49
testing call-intercept snap-in ... 41
testing non-call-intercept snap-in ... 41
testing the connection
data source ... 74
third party CA ... 161
training ... 172
Troubleshooting Certificates issues ... 168
trust certificates ... 25, 138
trusted CA certificates ... 163
trusted certificates ... 121, 126
trust management ... 162

U

uninstall
services ... 44
uninstalling a service ... 44
Uninstalling snap-ins ... 22
URI ... 140
User login experience ... 61

V

videos 172
View Authorized Clients 93
viewing cluster attributes 13
Viewing Identity Certificates 150

W

whitelist for HTTP security 118