Administering Avaya Breeze® platform

Release 3.9
Issue 4
October 2026

© 2013-2026 Avaya LLC.
All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

Copyright

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

Virtualization

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

Third Party Components

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE

PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.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 to comply with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

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

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

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Purpose 10
Change history 10

Chapter 2: The Avaya Breeze® platform 11
Avaya Breeze® platform overview 11

Chapter 3: Cluster administration 12
Creating a new cluster 12
Editing clusters 14
Deleting clusters 16
Rebooting a cluster 16
Assigning an Avaya Breeze® platform server to a cluster 16
Removing an Avaya Breeze® platform server from a cluster 18
Validations when removing a server from a cluster 19
Installing a snap-in on a cluster 20
Uninstalling a snap-in from a cluster 21
HTTP load balancing in an Avaya Breeze® platform cluster 21
Enabling HTTP load balancing in an Avaya Breeze® platform cluster 22
Enabling the cluster database 23
Adding a trusted certificate to all Avaya Breeze® platform servers in a cluster 24
Store types of the trusted certificates 24
Backing up a cluster database 25
Restoring the cluster database 26
Cancelling a pending job 26
Purging a backup 26
Migrating backup jobs to a different System Manager 27

Chapter 4: Services 28
Snap-in deployment checklists 28
Loading the snap-in 32
Snap-in attributes 33
Configuring snap-in attributes at the service profile level 33
Configuring snap-in attributes at the cluster level 34
Configuring snap-in attributes at the global level 34
Installing the snap-in 35
Service profiles 36
Creating a service profile 36
Configuring service invocation for service profiles 37
Searching service profiles 38

Application sequences and implicit sequencing 38
Creating an application and application sequence 38
Testing the snap-in 39
Testing a non-call-intercept snap-in 40
Creating a routing policy 40
Creating a dial pattern 40
Assigning a service profile to an implicit user pattern 41
Starting a snap-in 41
Stopping a snap-in 42
Uninstalling a snap-in 42
Deleting a snap-in 43
Deleting a service database 44

Chapter 5: Bundles 45
Loading a bundle 45
Installing the bundle 45
Uninstalling a bundle 46
Deleting the bundle 46

Chapter 6: User administration 48
Administering implicit sequencing for Avaya Breeze® platform 48
Service profile association options 49
Assigning a service profile to implicit users 50
Creating a new administered user 50
Assigning a service profile to an administered user 51

Chapter 7: Reliable eventing administration 52
Creating a Reliable Eventing group 52
Editing a Reliable Eventing group 53
Deleting a Reliable Eventing group 53
Viewing the status of Reliable Eventing destinations 53
Deleting a Reliable Eventing destination 53
Running a maintenance test for a broker 54

Chapter 8: Authorization service 55
Authorization resources 55
Viewing authorized clients 55
Configuring features for a resource server 55
Authorization clients 56
Avaya Breeze® platform authorization client 56
External authorization client 57
User authentication 58
User login experience 58
LDAP authentication 58
SAML authentication 61

Changing the authentication mechanism 63

Chapter 9: Administering HTTP security 64
Administering a whitelist for HTTP Security 64
Administering client certificate challenge for HTTPS 64
Administering HTTP CORS security 65

Chapter 10: JDBC resource providers and data source 66
JDBC provider 66
Adding a JDBC provider resource 66
Editing a JDBC provider resource 67
Deleting JDBC provider resources 67
Configuring the JDBC data source 67
Adding a JDBC data source 68
Editing a JDBC data source 68
Deleting a JDBC data source 69
Testing the connection using query validation 69
Sample configuration for database providers 69

Chapter 11: Service ports 71
Assigning service ports for Avaya-developed snap-ins 71

Chapter 12: Geo Redundancy 73
Managing Avaya Breeze® platform in a Geographic Redundancy solution 73
Avaya Breeze® platform administration in a geographic redundancy environment 73
Avaya Breeze® platform Status and Maintenance in a geographic redundancy environment 75
Fault management (alarming and logging) in a geographic redundancy environment 77
Geographic Redundancy Replication and data restoration 78
Performing system verification tests 79
Terminology 79

Chapter 13: Security 81
Generating a private key 81
Generating a certificate signing request (CSR) 82
Replacing a System Manager signed identity certificate with Cluster IP/FQDN 83

Chapter 14: User interface descriptions 85
Attribute configuration field descriptions 85
Authorization configuration field descriptions 87
New External Authorization Client field descriptions 88
Edit Grants for Authorization Client field descriptions 88

Create Grant for Authorization Client field descriptions 89
Resources Servers tab 89
View Authorized Clients of Resource Server field descriptions 90
Configure Features field descriptions 90
Service Instances tab field descriptions 90
Edit Keys for Authorization Service field descriptions 91
Authentication Mechanism tab field descriptions 91
Avaya Breeze® platform Instance Editor field descriptions 91
Avaya Breeze® Instance Status page field descriptions 93
Backup and Restore drop-down menu descriptions 94
Backup and Restore Status field descriptions 94
Backup Storage Configuration field descriptions 95
Broker Destination Status page field descriptions 96
Event catalog configuration field descriptions 97
Event Catalog Editor field descriptions 98
Bundles field descriptions 98
Bundle Details and Installation Status page 101
Services in Bundle or Dependencies table field descriptions 101
Installation status field descriptions 102
Cluster administration field descriptions 102
Cluster DB Backup field descriptions 109
Cluster Editor page field descriptions 110
Avaya Aura® Media Server priority settings 120
HTTP Security page field descriptions 121
Implicit User Profiles page field descriptions 123
Implicit User Profile Rule Editor page field descriptions 124
Install Trusted Certificate field descriptions 125
JDBC Providers page field descriptions 125
JDBC Provider Editor field descriptions 126
JDBC data source field descriptions 127
JDBC Data Source Editor field descriptions 128
Maintenance Tests page field descriptions 129
Media Server Monitoring page field descriptions 129
Reliable Eventing Groups page field descriptions 130
Reliable Eventing Group Editor page field descriptions 131
Server Administration page field descriptions 132
Services page field descriptions 136
Service Databases page field descriptions 138
Service Ports page field descriptions 139
Service Profile Configuration page field descriptions 140
Service Profile Editor field descriptions 141
Service Status field descriptions 142

SNMP MIB Download page field descriptions 143
System Resource Monitoring page field descriptions 143

Chapter 15: Deployment operations 146
Adding a trusted certificate to all Avaya Breeze® platform servers in a cluster 24
Administering an Avaya Breeze® platform instance 146
Administering Avaya Aura® Media Server URI 148

Chapter 16: Maintenance operations 149
Modifying the logging configuration 149
Downloading the Avaya Breeze® platform SNMP MIB 149
Running maintenance tests 150
Viewing the current usage of a cluster 150
Viewing the peak usage of a cluster 150
Resetting the peak usage of a cluster 151

Chapter 17: Certificate management 152
Certificates issued by System Manager 154
Identity certificate descriptions 155
Demo certificates 157
Determining whether you are using a demo identity certificate 157
Viewing identity certificates 157
Replacing an identify certificate with a System Manager CA certificate 157
Replacing an identify certificate with a third party CA certificate 159
Activating a new identity certificate 160
CSR generation 160
Generating a CSR and private key using OpenSSL 160
Bundling the identity certificate and private key into a PKCS #12 container 163
Identity certificate expiration alarms 164
Security Module SIP identity certificate attributes 165
Security Module HTTP identity certificate attributes 166
Management and SPIRIT identity certificate attributes 167
Replacing an identity certificate with a certificate issued by the System Manager CA 168
Replacing an identity certificate issued by a third party CA 169
Obtaining the new SIP identity certificate through a CSR 170
Obtaining the new SIP identity certificate through a PKCS#12 container 170
Trust management 170
Viewing trusted CA certificates 171
Adding trusted CA certificates 172
Removing trusted CA certificates 173
Exporting an Avaya Breeze® platform certificate 173

Exporting the System Manager root CA certificate 173
Peer certificate validation 173
Certificate validations for System Manager connection 173
Certificate validations for SIP TLS connections 174
CRL limitations 175
Certificate revocation management 175
Troubleshooting guidelines for common certificate issues 175

Chapter 18: Communication Manager administration 177
Administering Communication Manager 177

Appendix A: CEnetSetup 178
CLI commands 178

Appendix B: Apache Directory Studio Configuration 188
Configuring an LDAP provider and a SAML provider 188

Appendix C: Documentation for Collaboration Environment 226
Additional information 226

Chapter 1: Purpose

This document provides instructions for administering Avaya Breeze® platform and for installing and administering snap-ins running on Avaya Breeze® platform. Examples of Avaya snap-ins you can use include Context Store, Engagement Designer, and Work Assignment.

Snap-ins are also referred to as services. Some functionality is provided by a group of services. Customers, business partners, and Independent Software Vendors (ISVs) can use Avaya Breeze® platform as the deployment vehicle for their applications or services.

Important:

Before using this document, you must install and configure Avaya Breeze® platform. For more information, see *Deploying Avaya Breeze® platform*.

Change history

Issue	Date	Summary of changes
1	January 2024	Updated for Avaya Breeze® platform Release 3.9.
2	February 2024	Corrected the web links to other Avaya Breeze® platform documents.
3	November 2025	Updated the following sections for Release 3.9.0.3: • Assigning an Avaya Breeze® platform server to a cluster • Removing an Avaya Breeze® platform server from a cluster. • Cluster Editor page field descriptions. • Certificate Management. • Replacing an identify certificate with a System Manager CA certificate.
4	October 2026	Updated the following section for Release 3.9.0.4: • Importing the LDAP Server certificate into Avaya Breeze® platform cluster

Chapter 2: The Avaya Breeze® platform

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

Avaya Breeze® platform overview

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

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

Avaya Breeze® platform provides:

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

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

Chapter 3: Cluster administration

This section covers processes for Avaya Breeze® platform 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® platform servers to a cluster.
- Install snap-ins on a cluster.
- Subscribe to Reliable Eventing groups that are already created.

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

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

Procedure

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

   > **Note:**
   >
   > You must select a cluster profile to view the appropriate cluster attributes.

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

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

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

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

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

   Note:

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

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

   Note:

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

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

   Important:

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

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

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

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

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

      - **Default**

        If you select **Default**, the Avaya Breeze® platform uses the **Minimum TLS Version** field value set in the System Manager global configuration.
      - **TLS v1.0**

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

  Avaya recommends using TLS v1.3.

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

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

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

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

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

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

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

    Note:

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

Editing clusters

About this task

Use the Edit Cluster page to:

- Configure cluster attributes.
- Assign or remove one or more Avaya Breeze® platform servers to the cluster.
- Assign or remove snap-ins to the cluster.
- Edit reliable eventing groups associated with the cluster.

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

Note:

This procedure is service impacting.

Procedure

1. In System Manager, click **Elements › Avaya Breeze®**.
2. In the navigation pane, click **Cluster Administration**.
3. Select the targeted cluster.
4. Click **Cluster State › Deny New Service**.
5. Click **Continue** when prompted.
6. Select the cluster and click **Edit**.

   You cannot modify the cluster attributes that are greyed out.
7. On the Edit Cluster page, edit the cluster attributes.
8. Click the **Servers** tab and do one of the following:

   - To add Avaya Breeze® platform servers, select the Avaya Breeze® platform servers you want to add to the cluster.
   - To remove Avaya Breeze® platform servers and move them to the unassigned pool, clear the Avaya Breeze® platform servers from the selected list.

   Note:

   The action of adding or removing one or more cluster nodes restarts both the node being added or removed and the remaining nodes in the cluster. Be prepared for a service outage.
9. **(Optional)** Click the **Services** tab and select the snap-ins that you want to assign to the cluster.
10. **(Optional)** To remove an existing snap-in from the cluster, click **Uninstall** or **Force Uninstall**.

    The snap-in moves to the available services pool.

    The **Force Uninstall** option brings down active sessions that access the snap-in.
11. **(Optional)** To add reliable eventing groups to the cluster, do the following:

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

       You can remove a group by clicking **X** in the Subscribed Reliable Eventing Groups table.
12. Click **Commit** to save your changes.
13. Accept the warnings presented.
14. Wait until all services have been installed successfully.
15. Select the targeted cluster and then click **Cluster State › Accept New Service**.
16. Click **Continue** when prompted.

Deleting clusters

Before you begin

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

Procedure

1. In 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® platform 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

If using a multi-node node cluster, reboot the cluster after completing all the preceding process This ensure the data grid comes up properly.

Avaya Breeze® platform 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. In 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.
   - Reboot a cluster disabled **Database Auto Switchover** until you place the cluster back into **Accept New Service**.
   - You can view the reboot status in the **Last Reboot Status** column of **Cluster Administration**.

Assigning an Avaya Breeze® platform server to a cluster

About this task

Use this procedure to assign an Avaya Breeze® platform server to a cluster. Perform this procedure during a maintenance window.

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.
- If you add a server to a single or two node clusters, it affects service as WebSphere restarts to update the data grid properties. However, if you add a server to a cluster that has three or more servers, it does not affect service.

You can add up to five servers to most clusters. With the Core Platform cluster profile, you can add up to ten servers.

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

Note:

When adding an Avaya Breeze® platform server to a single to 2-node cluster configuration, a cluster reboot is required.

Before you begin

Data replication and synchronization must be complete. Ensure that the nodes in the cluster are in the Synchronized state before you add an Avaya Breeze® platform server to a cluster.

Procedure

1. In 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 state.
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® platform server to your cluster.
7. Click **Commit**.
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® platform server from a cluster

About this task

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

Note:

When removing an Avaya Breeze® platform server from a 3-node cluster configuration, a cluster reboot is required.

Procedure

1. In 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.

Validations when removing a server from a cluster

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

- The minimum number of servers are not available in the Accept New Service state.
- The Avaya Breeze® platform 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

Performing manual switch over from active server to standby server on page 19

Converting an idle server to the standby server on page 20

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. In 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

Performing manual switch over from active server to standby server on page 19

Converting an idle server to the standby server on page 20

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. In 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**.

Installing a snap-in on a cluster

Procedure

1. In 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**

      If you select **Default**, the Avaya Breeze® platform uses the **Minimum TLS Version** field value set in the System Manager global configuration.
    - **TLS v1.0**
    - **TLS v1.2**
    - **TLS v1.3**

      Avaya recommends using TLS v1.3.

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. In 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® platform cluster

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

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

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

Load balancing validations

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

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

Session affinity

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

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

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

Enabling HTTP load balancing in an Avaya Breeze® platform cluster

About this task

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

Procedure

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

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

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

Enabling the cluster database

About this task

By default, the cluster database is disabled. Use this procedure to enable the cluster database. Some snap-ins require you to enable the cluster database.

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Cluster Administration**.
2. Select the cluster that you want to edit and then click **Cluster State › Deny New Service**.
3. Click **Continue**.
4. Click **Edit**.
5. In the General tab, select the **Enable Cluster Database** check box.

   When you enable the cluster database, the following message is displayed: `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.`
6. Leave the **Enable Database Auto Switchover** field at the default setting, unless you want to manually control when a failover must occur.

7. Click **Commit**.
8. Select the cluster and then click **Cluster State › Accept New Service**.
9. Click **Continue**.

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

Before you begin

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

Procedure

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

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® platform management link that communicates with System Manager.
SPIRIT	spiritalias	SAL server on System Manager	SAL

Table continues

Store Type/Interface/ Service	Common Name	Connected peer party	Usage/Function
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 database

About this task

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

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

Before you begin

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

Procedure

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

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

- In the **Schedule Job** field, to run an immediate backup select **Run immediately**. Otherwise, select **Schedule later** and enter the required details in the **Task Time**, **Recurrence**, and **Range** fields.

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

Restoring the cluster database

About this task

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

Before you begin

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

Procedure

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

Related links

Enabling the cluster database on page 23

Cancelling a pending job

Procedure

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

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

Purging a backup

Before you begin

The backup to be purged must be complete.

Procedure

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

2. Click **Backup and Restore › Purge**.

   The system displays the Backup and Restore Status page.

3. Select the backup and click **Purge**.

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

4. Click **Confirm**.

Migrating backup jobs to a different System Manager

About this task

You can export backup details from one System Manager instance and import them into another instance. For example, migrating backup jobs can be useful if you need to migrate users to a different environment.

Before you begin

- Ensure that all backup jobs have completed before you migrate them. Only completed jobs are exported in the backup description file.
- If you are using the same backup server on the original and new System Manager instances, ensure that it is configured on both instances.
- If you are using a different backup server on the new System Manager, manually copy the backup data from its location on the original backup server.

Procedure

1. On the original System Manager instance, click **Elements › Avaya Breeze® › Cluster Administration**.
2. Click **Backup and Restore › Job Status**.
3. Select the backup jobs that you are moving to the new System Manager.
4. Click **Export** and download the backup description file.

   The downloaded backup description file contains metadata about the completed backup jobs. The database backup files residing on the backup server are not affected by this export.

   Tip:

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

5. On the original System Manager instance, click **Elements › Avaya Breeze® › Cluster Administration**.
6. Click **Backup and Restore › Job Status**.
7. Click **Import** and select the backup description file to be imported.

   Any backup jobs that are already configured on System Manager are skipped during the import.

Chapter 4: Services

Snap-in deployment checklists

The following are the types of Avaya Breeze® platform 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® platform 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® platform Element Manager in System Manager.	See *Quick Start to deploying the HelloWorld Snap-in*.	

Table continues

No.	Task	Notes	Link/Reference	✔
2.	Load the snap-in.	Skip this step when installing a preloaded snap-in. Preloaded snap-ins are provided with Avaya Breeze® platform 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 36	
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 51	
7.	Create an application and the application sequence.	Skip this step if you have an application sequence administered for Avaya Breeze® platform.	Application sequences and implicit sequencing on page 38	
8.	Administer implicit sequencing for a user or group of users.	Skip this step if you have administered implicit sequencing for Avaya Breeze® platform.	Administering implicit sequencing for Avaya Breeze platform on page 48	
9.	Test the snap-in.	—	Testing the snap-in on page 39	

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 snap-ins are provided with Avaya Breeze® platform 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® platform 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 40	
8.	Create a routing policy with the Avaya Breeze® platform SIP Entity as the destination.	—	Creating a routing policy on page 40	

Table continues

No.	Task	Notes	Link	✔
9.	Create a service profile or add the snap-in to an existing service profile.	—	Service profiles on page 36	
10.	Create and assign the service profile to an implicit user pattern in Avaya Breeze® platform 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 50 Assigning a service profile to an implicit user pattern on page 41	

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® platform 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® platform Element Manager in System Manager.	Loading the snap-in on page 32	
3.	Install the snap-in.	—	Installing the snap-in on page 35	

Table continues

No.	Task	Notes	Link	✔
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 36	

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® platform 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. In 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 page field descriptions on page 136

Snap-in 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® platform 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® platform Snap-in Development Guide*.

Configuring snap-in attributes at the service profile level

About this task

You can configure values for attributes that will replace the default values assigned in the snap-in. Use this procedure to configure attributes for a snap-in that is included in a service profile.

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 a service profile and assign the required snap-in to the profile.

Procedure

1. In 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

Attribute configuration field descriptions on page 85

Configuring snap-in attributes at the cluster level

About this task

You can configure values for attributes that will replace the default values assigned in the snap-in. Use this procedure to configure attributes for a snap-in when that snap-in is not included in a service profile, or when you want to assign snap-in attributes at the cluster level.

Before you begin

Perform this procedure only after installing the snap-in.

Procedure

1. In 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 your changes.

Configuring snap-in attributes at the global level

About this task

You can configure values for attributes that will replace the default values assigned in the snap-in. Use this procedure to configure attributes for a snap-in when that snap-in is not included in a service profile, or when you want to assign snap-in attributes at the global level.

Procedure

1. In 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 85

Installing the snap-in

About this task

Use this procedure to install the snap-in to specific clusters.

Note:

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

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Service Management › Services**.
2. Select the snap-in.
3. Click **Install**.
4. Select the clusters on which you want to install the snap-in, and click **Commit**.
5. To see the status of the snap-in installation, click **Refresh**.
   - **Installed** with a green check mark indicates that the snap-in has completed installation on all the Avaya Breeze® platform 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 snap-ins automatically start, but a snap-in developer can control starting and stopping the snap-in.

6. To track the progress of the installation, on the Server Administration page, click **Service Install Status** for the Avaya Breeze® platform 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 clusters 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 clusters for which you want this to be the preferred version, and click **Commit**.

Related links

Services page field descriptions on page 136

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 with 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 a 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® platform 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® platform 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® platform 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.

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. In System Manager, click **Elements › Avaya Breeze® › Configuration › Service Profiles**.

2. Click **New**.
3. Type a name for the service profile.
4. Click the **All Services** tab.
5. To select the latest version of the snap-in, in **Available Service to Add to this Service Profile**, click **+** next to the snap-in.

   If you want to select a specific version, skip this step and perform the next step instead.
6. **(Optional)** To specify a 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 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**.
7. To add another service to the same service profile, repeat step 5 or 6.
8. Click **Commit** to save the service profile.

Related links

Service Profile Configuration page field descriptions on page 140

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. In 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® platform for calling or called user.
7. Click **Commit** to save the changes.

Searching service profiles

About this task

Use this procedure to search for service profiles. You can then view users associated with the service profile or edit the service profile.

Procedure

1. In System Manager, click **Elements › Avaya Breeze®**.
2. In the navigation pane, click **Configuration › Service Profiles**.
3. On the Service Profile Configuration page, type a search string in the **Search** field.

   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. Do one of the following:
   - Click **Users** to view the list of users who have this service profile assigned to them.
   - Click **Edit** to edit the details of the service profile.
   - Click **Bulk Edit** to perform a bulk edit of service profiles for the associated users.

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® platform. In this way, calls to or from the user will invoke Avaya Breeze® platform snap-ins based on their service profile.

An application sequence is only required for call-intercept snap-ins, which are 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® platform as an application.
2. Add the Avaya Breeze® platform application to an application sequence.
3. Assign the application sequence to the implicit user (number or pattern) you want connected to Avaya Breeze® platform snap-ins (administering implicit sequencing).

Creating an application and application sequence

This procedure:

- Administers a target Avaya Breeze® platform instance as an application.

- Administers the application as part of an application sequence. This only needs to be done once for each Avaya Breeze® platform instance.

Procedure

1. Administer the target Avaya Breeze® platform instance as an application:
   a. On 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® platform instance.
   d. For the **SIP Entity**, select the Avaya Breeze® platform where the service resides.

      For information about creating the SIP entity, see *Deploying Avaya Breeze® platform*.
   e. To save your changes, click **Commit**.
2. Administer the application as part of an application sequence:
   a. On 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® platformapplication that you created.
   e. To prevent calls from failing when Avaya Breeze® platform 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 the snap-in

About this task

The HelloWorld snap-in can be invoked as a called or calling party snap-in. You can test the HelloWorld snap-in by making a call to or receiving a call from a user assigned to the service profile that contains the snap-in. The test was successful if the correct call display information appears, as defined in the snap-in attributes you configured.

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*.

Procedure

1. Test a call with the user assigned to the service profile that contains the snap-in.
   - To test the HelloWorld snap-in as a called party snap-in, make a call to the user assigned to the service profile.
   - To test the HelloWorld snap-in as a calling party snap-in, have the user assigned to the service profile make a call to another party.
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® platform* and *Avaya Breeze® platform 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® platform server or cluster. A routing policy to Avaya Breeze® platform is necessary only when administering a callable service and is not appropriate for call-intercept services.

Procedure

1. In 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® platform server or cluster. A dial plan to Avaya Breeze® platform is necessary only when administering a callable service and is not appropriate for call-intercept services.

Procedure

1. In 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. In 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. In 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® platform 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. In 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. In 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.

- 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 on the Service Management page is the aggregated status of its installation across clusters. If you uninstall a snap-in from a cluster and it is still installed in another cluster, the status remains 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. In 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**.

Deleting a service database

About this task

Delete the service database after all versions of that service have been uninstalled from the cluster. This procedure is not applicable if you selected the **Do you want to delete the database?** check box when uninstalling the snap-in.

You cannot delete databases that are in use.

Procedure

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

Chapter 5: Bundles

A bundle is a package of multiple snap-in SVARs and is itself an SVAR file. Snap-ins are often dependent on other snap-ins or services.

- With an internal dependency, the dependent snap-ins are packaged along with the bundle.
- With an external dependency, the snap-in that the bundled snap-in depends on is not packaged in the bundle. You must upload the snap-in to System Manager separately.

Workflows and tasks that are loaded as part of a bundle are not displayed on the Services, Cluster Administration, and Service Profile pages. You can create workflows and tasks using the Engagement Designer snap-in.

When snap-ins of the Java type are loaded through bundles, they are displayed on the Services page. For more information about Java type snap-ins, see the *Hello World Service* sample document, which you can access by navigating to `samples\helloservice\documents` in the Avaya Breeze SDK. The SDK and other documentation for Avaya Breeze® platform are available on the Avaya DevConnect website.

Loading a bundle

About this task

Use this procedure to load one or more bundles to System Manager. You can load multiple bundles at a time.

Before you begin

Ensure that any external dependency snap-ins are loaded. For more information, see Loading the snap-in on page 32.

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Service Management › Bundles**.
2. Click **Load**.

   The total size of all selected files cannot exceed the browser-specific upload limits.
3. On the Load bundle dialog box, click **Choose File**.
4. Select the file and click **Open**.
5. Click **Commit**.

   When the loading is complete, the Service Management page displays the status of the bundle as "Loaded".

Installing the bundle

About this task

After loading a bundle, you can install it onto one more Avaya Breeze® platform clusters. You can only install one bundle at a time.

Before you begin

- Load the bundle.
- Ensure that any external dependency snap-ins are loaded on the Services page. If dependencies are not loaded, the bundle installation will not start.

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Service Management › Bundles**.
2. Select the bundle that you want to install and click **Install**.
3. Select the cluster(s) where you want the bundle to reside, and click **Commit**.
4. Click  to refresh the list of bundles so that you can see the bundle installation status.

   The **State** column displays the installation status.

   -  Installed: Indicates that the bundle installation is complete.
   -  Installing: Indicates that the installation is not yet complete on all servers.
5. **(Optional)** Click the name of the bundle for more information, including service and dependency installation status on the Avaya Breeze® platform nodes.

Uninstalling a bundle

About this task

Use this procedure to uninstall a bundle from one or more Avaya Breeze® platform clusters. You can only uninstall one bundle at a time.

Uninstalling a bundle from a cluster does not uninstall external dependencies. An internal dependency is only uninstalled if no other bundles require it.

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Service Management › Bundles**.
2. Select the bundle that you want to uninstall and click **Uninstall**.
3. Select the cluster or clusters from which you want to remove the bundle.
4. Click **Commit**.

Deleting the bundle

About this task

You can delete multiple bundles at a time.

Before you begin

Before you can delete a bundle, it must be in the "Loaded" state. If the bundle you want to delete is installed, you must uninstall it.

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Service Management › Bundles**.

2. Select the bundle(s) that you want to delete.
3. Click **Delete**.
4. When prompted to confirm, click **Delete** again.

Chapter 6: User administration

Administering implicit sequencing for Avaya Breeze® platform

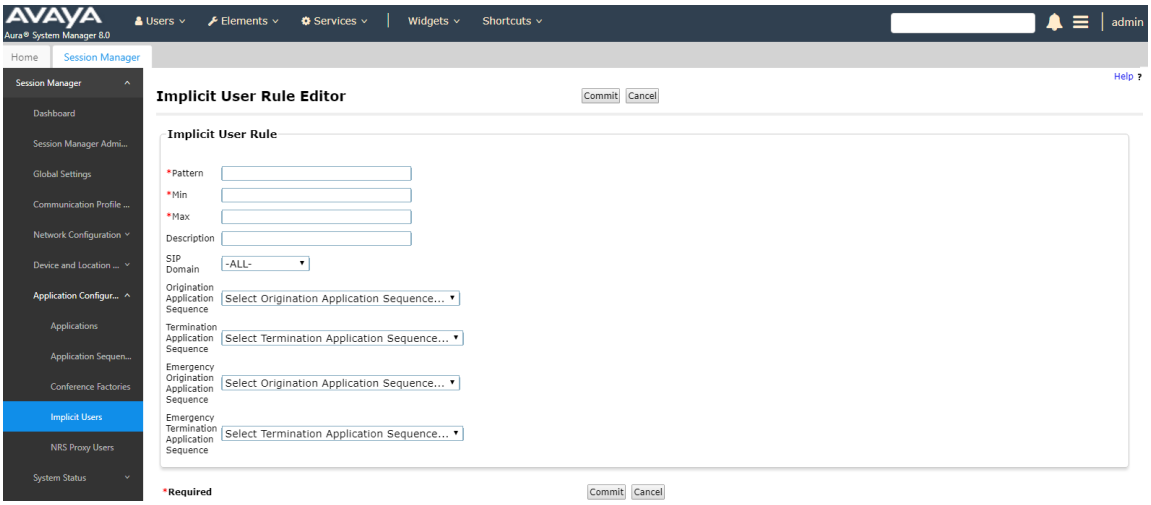
Administer implicit sequencing for a user or group of users for Avaya Breeze® platform so that an application sequence can be assigned to those users for call-intercept snap-ins. Avaya Breeze® platform uses implicit sequencing for both SIP and non-SIP endpoints. Therefore, you must administer implicit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

Procedure

1. In 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. Update the **Min** value as required.

   This value is auto-populated based on the pattern.

8. Update the **Max** value as required.

   This value is auto-populated based on the pattern.

9. Update **SIP Domain** as required.

   The default value is **-ALL-**.

   Note:

   - If you use multi-domain routing, see *Administering Avaya Aura® Session Manager* for information about what to enter in this field.
   - If you use a snap-in that uses the Remove Service From Call feature, you must select a specific domain. Otherwsie, Avaya Breeze® platform sequences again after the snap-in has requested to be removed from a call.

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

    The Origination Application Sequence tells Session Manager to send the call to the Avaya Breeze® platform when the targeted user is making a call.

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

    The Termination Application Sequence tells Session Manager to send the call to the Avaya Breeze® platform when the targeted user is receiving a call.

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

Related links

Creating an application and application sequence on page 38

Service profile association options

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.

Assigning a service profile to implicit users

Before you begin

You must create the service profile before it can be assigned.

Procedure

1. In 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 for the rule.

   You can provide a description of the group of users the rule defines.
8. Click **Commit** to save your changes.

Related links

Implicit User Profile Rule Editor page field descriptions on page 124

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. This procedure is also not required for users already administered as explicit users.

Procedure

1. In 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.

      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® platform is invoked when a call is received or sent.

      E.164 numbers can have a maximum of fifteen digits and are usually written with a + prefix. For example, +15553091337.

   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. In 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 7: Reliable eventing administration

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

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

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

Creating a Reliable Eventing group

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Reliable Eventing Administration › Dashboard**.
2. Click **New**.
3. Enter the following details:
    - **Cluster**: Select the cluster on which you want to create the Reliable Eventing group.
    - **Group Name**: Assign a name to the Reliable Eventing group.
    - **Description**: Enter a brief description.
    - **Type**: Select **HA** or **Standalone**.
        - If you select **HA**, you must select at least three Avaya Breeze® platform nodes or brokers.
        - If you select **Standalone**, you must select at least one Avaya Breeze® platform node or broker.
4. In the Unassigned Brokers table, click **+** to assign the Avaya Breeze® platform nodes or brokers to the Reliable Eventing group.
5. Click the Associated clusters tab:
    a. In the **Unassigned associated clusters** table, click **+** to add an associated cluster.
    b. In the **Assigned associated clusters** table, click **X** to remove an associated cluster.
6. Click **Commit**.

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

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

Editing a Reliable Eventing group

Procedure

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

Deleting a Reliable Eventing group

Procedure

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

Viewing the status of Reliable Eventing destinations

Procedure

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

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

Deleting a Reliable Eventing destination

Procedure

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

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

   The system purges the messages and deletes the destination.

Running a maintenance test for a broker

Procedure

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

   Avaya Breeze® platform displays one of the following statuses:

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

Chapter 8: Authorization service

The authorization service provides the following security functions to other Avaya Breeze® platform 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 might or might not be snap-ins. The authorization service enables a client application to authenticate client credentials. The client application can also authenticate with user credentials. The client is then provided with a token that can be used to securely access multiple Avaya Breeze® platform snap-ins without being challenged.

For example, Avaya Context Store Snap-in leverages the authorization service by acting as a resource server. Client applications using Avaya Context Store Snap-in first authenticate with the authorization service and then provide the token to Avaya Context Store Snap-in with a request for validation. 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 can accept and respond to protected resource requests using access tokens.

To enable a snap-in as an authorization resource, see *Avaya Breeze® platform Snap-in Development Guide*.

Viewing authorized clients

About this task

Use this procedure to view clients authorized by the resource server.

Procedure

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

   The system displays the authorized clients.

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® platform Snap-in Development Guide*.

Procedure

1. In System Manager, click **Elements › Avaya Breeze®**.
2. In the navigation pane, click **Configuration › Authorization**.
3. On 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.
6. Click **Commit**.

Authorization clients

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

Avaya Breeze® platform authorization client

Avaya Breeze® platform authorization client snap-ins interact with the authorization service to obtain access tokens.

To enable a snap-in as an authorization client, see *Avaya Breeze® platform Snap-in Development Guide*. Additional information is also available in *Sample Authorization Snap-ins*, which you can access by navigating to `samples/Authorization/documents` in the Avaya Breeze SDK. The SDK and other documentation for Avaya Breeze® platform are available on the Avaya DevConnect website.

Assigning and editing grants for an authorization client

Procedure

1. In System Manager, click **Elements › Avaya Breeze®**.
2. In the navigation pane, click **Configuration › Authorization**.
3. On 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 authorized 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 the authorization service. This procedure explains how to revoke existing keys and regenerate new ones in case of a security leak.

Procedure

1. In System Manager, click **Elements › Avaya Breeze®**.
2. In the navigation pane, click **Configuration › Authorization**.
3. On the Clients tab, select the authorization client snap-in and click **Edit Key**.
4. Click **Regenerate Keys**.

External authorization client

External authorization clients are non-snap-in client applications that interact with the 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. In 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 the "Service Management" information in this online help document.

Procedure

1. In System Manager, click **Elements › Avaya Breeze®**.
2. In the navigation pane, click **Configuration › Authorization**.
3. On the Clients tab, select the authorization client and click **Delete**.

User authentication

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

OAuth 2.0 Grant Type (Authorization)	Authentication Mechanism supported
Authorization code	SAML, LDAP
Resource owner password credentials	LDAP

See *Avaya Breeze® platform Snap-in Development Guide* for information about integrating an authorization client with the authorization service to support one of the two grant types mentioned above.

User login experience

With the authorization code grant flow and SAML authentication options, the end user trying to access an authorization client snap-in is redirected to an identity provider and presented with a Login screen. On successful authentication, the user is redirected back to the authorization client with a logged-in session.

With the authorization code grant flow and LDAP authentication options, the end user trying to access an authorization client snap-in is redirected to the Avaya Breeze® platform 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 the resource owner password credentials flow and LDAP authentication options, 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.

LDAP authentication

LDAP authentication uses the System Manager Directory Synchronization to configure a datasource. The Avaya Breeze® platform 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. In System Manager, click **Elements › Avaya Breeze® › Configuration › Authorization › Authentication Mechanism**.
2. Click **Change Authentication Mechanism**.

Comments on this document?

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 integrated to use the Avaya Breeze® platform Authorization Code Grant flow.
- Use the Authorization Sample snap-ins provided in the Avaya Breeze® platform 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® platform 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® platform 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. In 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® platform cluster

Before you begin

For Avaya Breeze 3.9.0.4 or later, verify the LDAP/LDAPS server certificate used by the Authorization Service. The certificate must use the RSA 2048 / SHA256WITHRSA signature algorithm.

- If the existing LDAP certificate already uses RSA 2048 / SHA256WITHRSA, no certificate renewal is required.
- If the existing LDAP certificate uses RSA 2048 / SHA1WITHRSA, the customer must do the following:
  - Follow their respective CA certificate-generation procedure to obtain a new RSA 2048 / SHA256WITHRSA certificate.
  - Import the required new LDAP/CA certificate into the Authorization Service trusted store on the Breeze node(s) And System Manager Element.
  - Verify the LDAPS connection before proceeding with the Breeze 3.9.0.4 upgrade.

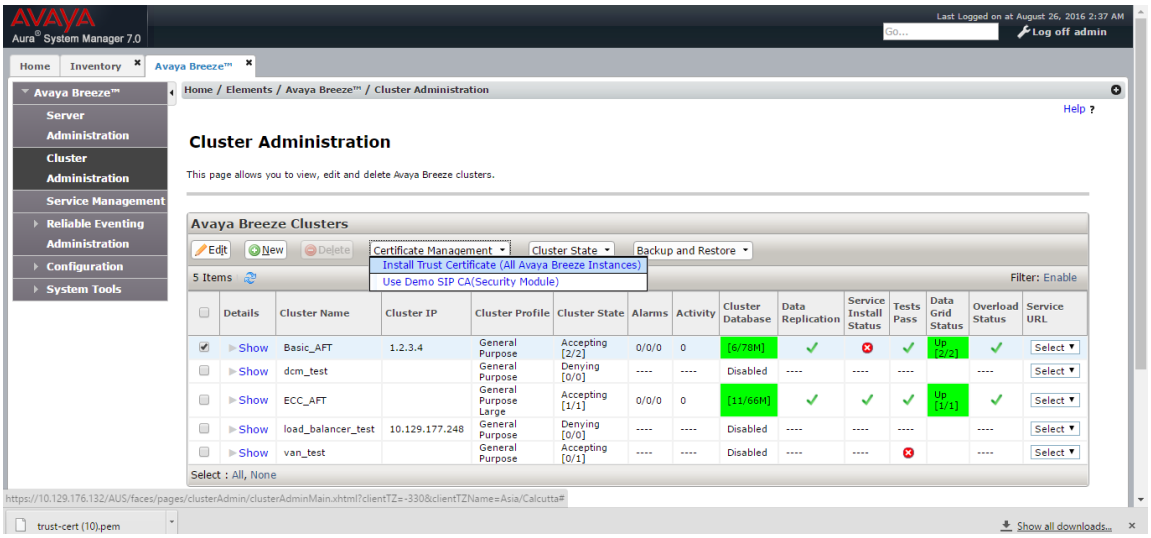
Note:

LDAP certification SHA-1 algorithm no longer supports on Breeze 3.9.0.4.

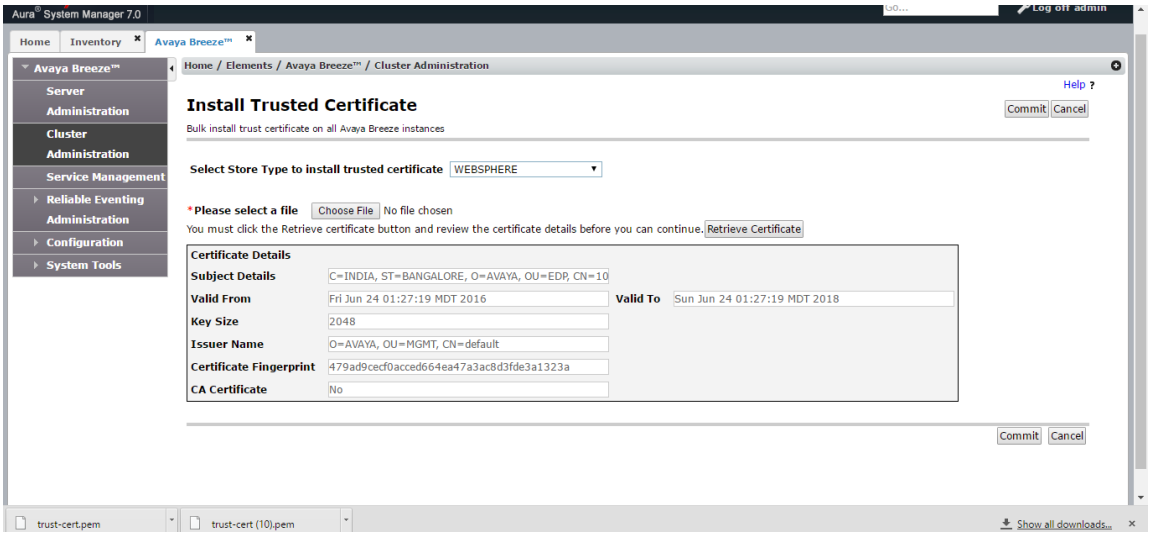
Procedure

1. In 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 authentication requires agreements between system entities regarding identifiers, binding support and endpoints, certificates and keys, and so on. A metadata specification is useful for describing this information in a standardized way.

The system entities involved here are the Avaya Breeze® platform authorization service (acts as a service provider) and a far-end identity provider (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 the authorization server in an Avaya Breeze® platform cluster, it generates metadata on a per-node basis.

The downloaded service provider metadata file needs to be used while configuring the 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 identity provider in System Manager

About this task

The authorization service acts as a service provider and obtains the IdP details from the SAML authentication mechanism configuration.

Procedure

1. In 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 the SAML profile for authorization

About this task

After configuring the IdP, the SAML profile needs to be enabled so that the authorization service can read the configuration and start its service provider component.

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Configuration › Attributes**.
2. Click the **Service Clusters** tab.
3. From **Cluster**, select the cluster where the authorization service is installed.
4. From **Service**, select the **Authorization Service** option.
5. In **SAML Profile**, click **Deploy**.
6. Click **Commit**.

Changing the authentication mechanism

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Configuration › Authorization**.
2. On the Authorization Configuration page, click the **Authentication Mechanism** tab.
3. Click **Change Authentication Mechanism**.
4. On the Change Authentication Mechanism page, in the **select Authentication Mechanism** field, select **LDAP** or **SAML**.
5. If you selected **SAML**, do the following:
   a. Select **Should SAML Request be Signed?** if appropriate.
   b. Complete the **Attribute Used as UserID** field.
   c. Select an option from the **Authentication Context** drop-down menu.
   d. Select an option from the **Authentication Context Comparison Type** drop-down menu.
   e. Click **Choose File** to select the identity provider metadata file.
6. Click **Save**.

Chapter 9: Administering HTTP security

Administering a whitelist for HTTP Security

Procedure

1. In 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 **Whitelist Enabled** check box.

   If you do not select the **Whitelist Enabled** check box, Avaya Breeze® platform 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 page field descriptions on page 121

Administering client certificate challenge for HTTPS

Procedure

1. In 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 page field descriptions on page 121

Administering HTTP CORS security

Procedure

1. In System Manager, click **Elements › Avaya Breeze®**.
2. In the navigation pane, click **Configuration › HTTP Security**.
3. Select the cluster.
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® platform 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 page field descriptions on page 121

Chapter 10: 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® platform 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® platform 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**.

JDBC provider

Adding a JDBC provider resource

Procedure

1. In 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 by using the JDBC driver jar.
5. 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 the provider and **Commit**.

Related links

JDBC Provider Editor field descriptions on page 126

Editing a JDBC provider resource

Procedure

1. In 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 126

Deleting JDBC provider resources

Procedure

1. In 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**.

Configuring the JDBC data source

Adding a JDBC data source

Procedure

1. In 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, do the following:
   a. In the **Cluster** field, click the cluster on which you installed the JDBC provider.

      Avaya Breeze® platform populates the value of the **JDBC Provider** field.
   b. Select the **TLS** check box if the database server is accepting TLS connections. The JDBC driver provided by database vendor determines which TLS version is used. Clear this check box if the server does not support TLS.
   c. In the **JNDI Name** field, type a unique name.
   d. In the **URL** field, type the URL.
   e. In the **User Name** field, type a user name.
   f. 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 128

Editing a JDBC data source

Procedure

1. In 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 128

Deleting a JDBC data source

Procedure

1. In 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. In 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

Table continues

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

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 11: 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. In 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.

   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 the 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.
8. To swap two ports, such as 1100 and 1200, do the following:

   a. Update port 1100 to 1108 and then click **Commit**.

      1108 is just a placeholder. Ensure that port 1108 is unused.

b. Update port 1200 to 1100 and then click **Commit**.
c. Update port 1108 to 1200 and then click **Commit**.

Chapter 12: Geo Redundancy

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

Managing Avaya Breeze® platform in a Geographic Redundancy solution

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

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

Avaya Breeze® platform Release 3.0 and later:

To view the System Manager server that manages a particular Avaya Breeze® platform 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® platform server. Select a Avaya Breeze® platform server and click **Get Current Status** to refresh the status for that Avaya Breeze® platform server.

Avaya Breeze® platform earlier than release 3.0:

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

Avaya Breeze® platform administration in a geographic redundancy environment

This section provides information about the Avaya Breeze® platform 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® platform instances. The primary System Manager replicates administration changes to all the Avaya Breeze® platform 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® platform servers. The secondary System Manager replicates the administration changes to all the Avaya Breeze® platform 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® platform instances that the primary server manages. Similarly, the administrator must perform the administration changes on the secondary System Manager for the Avaya Breeze® platform instances that the secondary server manages. Each System Manager replicates the administration changes to the respective Avaya Breeze® platform servers. Administration changes must also be compatible with non-Avaya Breeze® platform elements in the split network. For example, a SIP user added on System Manager should have Avaya Breeze® platform Profile, Session Manager Profile and CM Endpoint Profile that reference the Avaya Breeze® platform, 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® platform 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® platform 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® platform 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® platform 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® platform server. Click **Minimize** to hide the warning message.

Applicability

The following table lists all the Avaya Breeze® platform 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® platform servers that the System Manager manages.

Web page	Functionality	Notes
Avaya Breeze® › Server Administration.	Add, edit, delete the Avaya Breeze® platform servers.	
Avaya Breeze® › Cluster Administration>	Add, edit, view, and delete Avaya Breeze® platform 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® platform servers	
User Management › Manage Users	Change the Service Profile.	

Avaya Breeze® platform Status and Maintenance in a geographic redundancy environment

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

Sunny day scenario

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

Rainy day scenario

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

Split-network scenario

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

Applicability

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

Web page	Functionalities	Notes
Avaya Breeze® › Server Administration	• View the Avaya Breeze® platform system status. • Accept or deny new services.	
Avaya Breeze® › Cluster Administration	• View the Avaya Breeze® platform cluster status. • Accept or deny new services.	
Avaya Breeze® › System Tools and Monitoring	• Run the maintenance tests for Avaya Breeze® platform instances. • Download zipped copy of the Avaya Breeze® platform related SNMP MIBs..	

Table continues

Web page	Functionalities	Notes
Inventory › Manage Elements	View and edit the trusted certificate configuration and the identify certificate configuration of a Avaya Breeze® platform instance by clicking the **More Actions** button.	

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

This section provides information on viewing the Avaya Breeze® platform 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® platform instances. You can view all the Avaya Breeze® platform related alarms from the **Events › Alarms** webpage on the primary System Manager.

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

View Avaya Breeze® platform 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® platform 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® platform related alarms.

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

View the Avaya Breeze® platform 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® platform that are reachable on the enterprise network. View these alarms from the **Events › Alarms** webpage. If a Avaya Breeze® platform server cannot connect to a System Manager because of the network split, the Avaya Breeze® platform 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® platform instance.

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

View the Avaya Breeze® platform 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.

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.

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® platform server.
4. Optionally, run the System Manager maintenance tests and the Avaya Breeze® platform maintenance tests on the primary System Manager server. To run the maintenance tests, go to the **Avaya Breeze® › System Tools and Monitoring › Maintenance Tests** webpage.

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

Terminology

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® platform server in an Avaya Aura® network.

Note:

A Avaya Breeze® platform 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® platform clusters, administer Avaya Breeze® platform platforms, load snap-ins, uninstall snap-ins, and run on demand maintenance tests.

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.

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.

Active server

The mode of operation of the System Manager server where the server provides the full System Manager functionality.

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.

Geographic Redundancy-aware elements

Those elements of the Avaya Aura® solution that support the **Geographic Redundancy** feature, such as Avaya Breeze® platform Release 3.0.

Geographic Redundancy-unaware elements

Those elements of the Avaya Aura® solution that do not support the **Geographic Redundancy** feature, such as Avaya Breeze® platform instances earlier than Release 3.0.

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, and LDAP replication. For more information, see *Administering Avaya Aura System Manager*.

Chapter 13: 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. In 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 14: User interface descriptions

Attribute configuration field descriptions

On System Manager, navigate to **Elements › Avaya Breeze® › Configuration › Attributes** to configure:

- Attributes for a service within a service profile
- Attributes for a cluster
- Global attributes for a service

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 override 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 attributes for 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, **Effective Value** displays the value you entered. Otherwise, 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. Use this tab to override the factory default value. 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 your attribute configuration changes.

Related links

Configuring snap-in attributes at the global level on page 34

Authorization configuration field descriptions

On System Manager, navigate to **Elements › Avaya Breeze® › Configuration › Authorization** to administer authorization clients, resources, and authorization service instances.

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.

Table continues

Name	Description
Delete	Deletes an external Authorization Client. This option is disabled for Authorization Client Snap-ins.

New External Authorization Client field descriptions

From the Clients tab on the Authorization Configuration page, click **New** to configure an external authorization client. The following are the mandatory fields:

Name	Description
Name	Name of the external authorization client.
Certificate	Upload an eexternal authorization client certificate.

Edit Grants for Authorization Client field descriptions

From the Clients tab on the Authorization Configuration page, click **Edit Grants** to administer grants for an authorization client.

Fields:

When you create or edit an authorization grant, complete the following 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 for the features.

Buttons

Name	Description
New	Creates an authorization grant.
Edit values	Edits values of the authorization grant.

Table continues

Name	Description
Delete	Deletes an authorization grant.

Create Grant for Authorization Client field descriptions

From the Edit Grants for Authorization Client page, you can 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

On the Authorization Configuration page, click the **Resource Servers** tab to view authorized clients and configure features for resource servers.

Fields:

Name	Description
Name	Name of the resource server that authorizes the authorization client.
Cluster Name	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 features 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	Client type. For example, External.
Feature	Grants or features assigned to the authorization client.
Values	Values configured to the features.

Configure Features field descriptions

On the Resource Servers tab, click **Configure Features**. This page allows you to select a feature value for the selected resource.

Name	Description
Select Feature	Features assigned to the resource server.

Service Instances tab field descriptions

The following options are available from the Service Instances tab on the Authorization Configuration page.

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 a key for the authorization service.

Edit Keys for Authorization Service field descriptions

Click **Edit Key** on the Service Instances tab to view information about the public key for the authorization service. The following information is displayed:

- Key fingerprint
- Generated by
- Date and time generated
- Public key

The following buttons are available on this page.

Name	Description
Regenerate Keys	Regenerates the key for the authorization service.
Done	Saves your changes and then returns to the Authorization Configuration page.

Authentication Mechanism tab field descriptions

This section describes the Authentication Mechanism tab on the Authorization Configuration page.

Field	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® platform Instance Editor field descriptions

On System Manager, navigate to **Elements › Avaya Breeze® › Server Administration** to manage server instances. When you click **New** or **Edit**, the Avaya Breeze Instance Editor page is displayed.

Name	Description
Identity:	

Table continues

Name	Description
SIP Entity	The name of the Avaya Breeze® platform SIP entity. For a new instance, select the SIP entity from the drop-down list. For information about how to create the SIP Entity, see *Deploying Avaya Breeze® platform*. **Note:** You can edit the IP address of the SIP entity only from the **Routing › SIP Entity Administration** page.
Description	The description of the Avaya Breeze® platform SIP entity.
UCID Network Node ID	The unique, numeric node ID that is assigned to each provisioned Avaya Breeze® platform server. As part of the Avaya Aura architecture, Avaya Breeze® platform adds Universal Call ID (UCID) to calls. Ensure that a unique node ID is assigned to the nodes that generate the UCIDs.
Management Network Interface:	
FQDN or IPv4 Address	The IPv4 Address of the Avaya Breeze® platform Management Network Interface. This is the same IP address that you enter during OVA deployment. For more information, see *Deploying Avaya Breeze® platform*. You must enter the IPv4 address even if administering an IPv6 address.
FQDN or IPv6 Address	The IPv6 address of the Avaya Breeze® platform Management Network Interface. You must also enter the IPv4 address.
Security Module:	
SIP Entity IPv4 Address	The IPv4 address of the Avaya Breeze® platform Security Module.
IPv4 Network Mask	The IPv4 network mask of the Avaya Breeze® platform Security Module.
IPv4 Default Gateway	The IPv4 default gateway of the Avaya Breeze® platform Security Module.
SIP Entity IPv6 Address	The IPv6 address of the Avaya Breeze® platform Security Module.
IPv6 Network prefix length	The IPv6 network prefix length.

Table continues

Name	Description
IPv6 Default Gateway	The IPv6 default gateway of the Avaya Breeze® platform Security Module.
Call Control PHB	The Call Control PHB value for the Avaya Breeze® platform instance. You can enter a value from 0 to 63. The default value is 34. This value provides scalable service discrimination in the Internet without per-flow state and signaling at every hop.

Avaya Breeze® Instance Status page field descriptions

On the Server Administration page, you can click the status indicator in the **Service Install Status** column and then click on a service to view the Avaya Breeze® Instance Status page. Use this page to check the status of the service for each Avaya Breeze® platform instance and to see which service profiles include this service.

Service Status tab

Name	Description
Name	The name of the Avaya Breeze® platform instances that are associated with the service.
Service Install Status	The status of the service on the listed Avaya Breeze® platform instance.
Details	A description of any problems the service is having with running on the Avaya Breeze® platform 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.

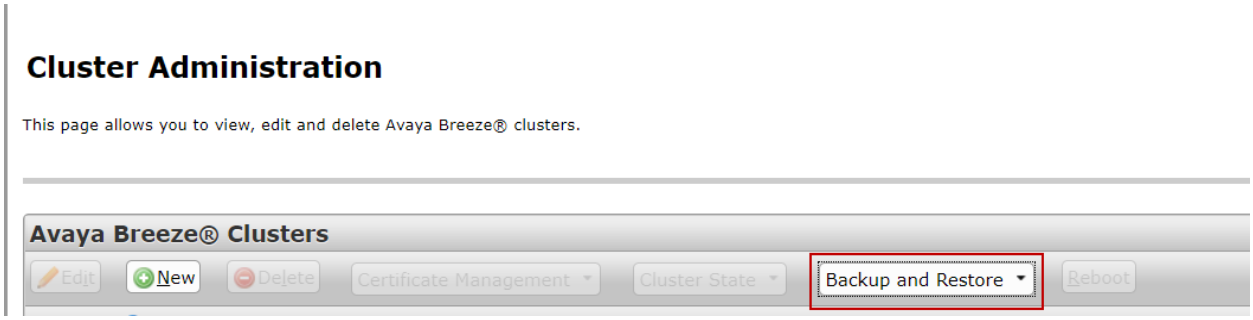
Related links

Installing the snap-in on page 35

Backup and Restore drop-down menu descriptions

This section describes the options available from the **Backup and Restore** drop-down menu on the **Cluster Administration** page, which you can access on System Manager under **Elements › Avaya Breeze®**.

The following image shows the location of this drop-down menu:



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

Select an option from the **Backup and Restore** menu on the **Cluster Administration** page. Almost every option on the drop-down menu, except **Configure**, displays the Backup and Restore Status page.

Table 1:

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.

Table continues

Name	Description
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

On the **Backup and Restore** drop-down menu, click **Configure** 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.

Table continues

Name	Description
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.

Broker Destination Status page field descriptions

Use the Broker Destination Status page to manage Reliable Eventing destinations. You can access this page on System Manager by navigating to **Elements › Avaya Breeze® › Reliable Eventing Administration › Destination Status**.

Name	Description
Destination Name	Name of the destination.
Type	Type of destination: Queue or Topic.
Enqueued Messages	The number of messages added to the destination.
Dequeued Messages	The number of messages removed from the destination.
Dispatched Messages	The number of messages that are dispatched.
Pending Messages	The number of messages in the queue that the user has not acknowledged.
InFlight Messages	The number of messages that are being processed.

Table continues

Name	Description
Expired Messages	The number of messages that have expired.
Consumers count	Number of consumers associated with 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.
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.

Table continues

Button	Description
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.

Bundles field descriptions

You can access the Bundles page on System Manager by navigating to **Elements › Avaya Breeze® › Service Management › Bundles**.

Bundle configuration options

Button name	Description
Load	Launches the Load Bundle window so you can browse to the location of a bundle and upload it.
Install	Queues up the selected bundle to be installed on all the selected clusters. Depending on the number of Avaya Breeze® platform nodes in the selected clusters, it might take a few minutes to install the bundle on all instances.
Uninstall	Uninstalls the selected bundle from the selected clusters. You can choose to perform a forced uninstallation, which terminates all active connections immediately. Otherwise, the system waits for all active connections to drop before uninstalling the bundle.
Delete	Deletes the selected bundle. You must uninstall a bundle before you can delete it. ⚠ **Caution:** Deleting the last version of a bundle completely deletes all attribute settings and profile configuration for that bundle from the system.

Bundle information fields

Field name	Description
Name	The names of all bundles that are loaded to the System Manager database.
Version	The version number of the bundle.
Type	The deployment type: • **Bundle**: For bundles. • **Java**, **Workflow**, or **Task**: For services, workflows, and tasks.
State	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. When you click the **State** link, Avaya Breeze® platform displays the status of the bundle installation on each cluster:

Table continues

Comments on this document?

Field name	Description
	• **Unknown**: The bundle installation status could not be obtained from the cluster. One or more servers in the cluster are unreachable, or the cluster is empty. • **Partial**: Some services of the bundle or their dependencies are already installed on the cluster. Installing the bundle on the cluster only installs the services that are not currently installed. • **Failed**: Installation of one or more services of the bundle or their dependencies previously failed on the cluster. Installing the bundle on the cluster only installs the failed ones. • **Not Installed**: The bundle is not installed on the cluster. • **Installed**: The bundle is completely installed on the cluster. Avaya Breeze® platform displays one of the following icons: • ✔: Indicates that the bundle is installed. • ⚠: Indicates that the bundle is queued for installation or for downloading to Avaya Breeze® platform. • ✖: Indicates that the bundle failed to initialize, run, or deploy. If the download fails, this icon is displayed with the `Transfer has failed` message.
License Mode	The license mode of the services in the bundle. This field is only applicable to the services in the bundle. The license mode options are: • **Not Applicable**: The value displayed in the field for services does not enforce or use licensing. • ✔ **License Normal Mode**: The bundle has a valid license file for normal operation of the bundle. License errors are absent. • ⚠ **License Error Mode**: A license error has a 30–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 return to License Normal mode. This column displays the grace period when the bundle is in Error mode. After the grace period expires, the bundle enters 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 Avaya Breeze® platform clusters. Element Manager raises a critical alarm. If you install the license file, the bundle returns to License Normal mode. You must manually re-install the bundle to any cluster from which the bundle was uninstalled.

Table continues

Field name	Description
Avaya Signed	The services in the bundle that are Avaya signed. This field is only applicable to the services in the bundle. The column displays ✔ if the service is signed by Avaya. Otherwise, the column displays **Not Signed**.

Bundle Details and Installation Status page

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

Services in Bundle or Dependencies table field descriptions

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

Table continues

Name	Description
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 is not loaded on System Manager. • **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® platform clusters. 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 if the service or dependency is signed by Avaya. Otherwise, the column displays **Not Signed**.

Installation status field descriptions

The following installation status details are displayed 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® platform 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® platform 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 installation audit.

Cluster administration field descriptions

You can access the Cluster Administration page on System Manager by navigating to **Elements › Avaya Breeze® › Cluster Administration**. The following sections describe the buttons and information fields on the Cluster Administration page.

Button and menu descriptions

Button	Description
New	Adds a new Avaya Breeze® platform cluster.
Edit	Displays or modifies the Avaya Breeze® platform cluster attributes or modifies the cluster profile.
Delete	Deletes the Avaya Breeze® platform 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® platform 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® platform 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.

Table continues

Button	Description
 icon	Refreshes the values in the Cluster Administration table.

Cluster information

The following columns are displayed on the Cluster Administration page.

Name	Description
Details	Click **Show** under this column to view details about the servers in 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. 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 IPv6	The IPv6 address of the cluster. The **Cluster IPv6** value is applicable only for HTTP/HTTPS. **Note:** Do not assign a **Cluster IPv6** 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**

Table continues

Name	Description
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® platform servers in the cluster.
Cluster Database	The High Availability status between the active Avaya Breeze® platform server and the standby Avaya Breeze® platform server in a cluster. 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® platform servers in a cluster and System Manager. The field displays: • ✓ when the replication is successful. • ✗ when replication for one or more nodes fails.

Table continues

Comments on this document?

Name	Description
Service Install Status	The aggregated service installation status of all the Avaya Breeze® platform servers in a cluster. The field displays: • ✓ when all snap-ins are installed. • ⚠ when the snap-in is either queued for installation or for downloading to Avaya Breeze® platform. • ✗ when one or more snap-ins have failed to initialize, run, or deploy.
Tests Pass	The aggregated maintenance test result for all Avaya Breeze® platform servers in the cluster. ✓ indicates that all Avaya Breeze® platform servers in the cluster have passed the maintenance tests.
Data Grid Status	The aggregate status of the data grid in the cluster. The field displays: • ✓ when the data grid status is up. • ⚠ when the status of one or more servers in the cluster is down. • ✗ when the data grid status is down.
Overload Status	The overload status of the Avaya Breeze® platform cluster. The field displays: • ✓ when no servers in the cluster are in the overloaded state. • ✗ 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® platform cluster. If you have administered the cluster IP, it is used as the host for the URL. If not, one of the Avaya Breeze® platform server IP addresses is used as the host for the URL.

Server details

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

Name	Description
Server Name	The name of the Avaya Breeze® platform server. Click **Show** for more information about the server status.
Security Module	The status of the security module for the server.
Server Version	The version of the Avaya Breeze® platform server.

Table continues

Name	Description
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 for all the snap-ins installed on the Avaya Breeze® platform server.
Cluster Database	The state of the server in a High Availability database setup. This 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 when the 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: • ✔ when the connection between the active and standby servers is up. • ⚠ when the standy server is getting ready to take over if the active server goes down. • ✖ when the connection between the active and standby servers is down. • No background when the cluster and database is disabled.
Data Replication	The status of data replication between the Avaya Breeze® platform server and System Manager. This field displays: • ✔ when the replication is successful. • ✖ when the replication fails.
Service Install Status	The service install status for the Avaya Breeze® platform server. This field displays: • ✔ when all the snap-ins are installed.

Table continues

Name	Description
	• when the snap-in downloading to Avaya Breeze® platform is in progress. • when one or more snap-ins failed to initialize, run, or deploy.
Tests Pass	The maintenance test result for the Avaya Breeze® platform server.
Data Grid Status	The data grid status of the Avaya Breeze® platform server: • **Up** • **Down**
Overload Status	The overload status of the Avaya Breeze® platform server. This field displays: • when the server is not overloaded. • when the server is in an overloaded state.
Last Reboot Status	The status of the last cluster reboot operation.

Other server indicators

The following indicators provide additional information about the servers in the cluster. Click **Show** under **Server Name** to see these indicators.

Indicator	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.

Table continues

Indicator	Description
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.
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:

Table continues

Name	Description
	• **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.

Related links

Backing up a cluster database on page 25

Cluster Editor page field descriptions

When you click **New** or **Edit** on the Cluster Administration screen, the Cluster Editor screen opens. 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:

Table continues

Name	Description
	• **Context Store**: Product-specific cluster profile for Context Store Snap-in. This profile requires at least two Avaya Breeze® platform servers. • **Core Platform**: Closed cluster that supports up to 10 Avaya Breeze® platform servers. Snap-ins that might be installed on this cluster profile include Presence Services and Call Park and Page. • **Engagement Assistant Speech**: Product-specific cluster profile for Engagement Assistant Snap-in. • **General Purpose**: General purpose cluster profile. This profile requires at least one Avaya Breeze® platform server. • **General Purpose Large**: Open cluster that supports up to five Avaya Breeze® platform servers. This cluster profile mainly supports the Engagement Call Control solution. • **Work Assignment**: Deprecated. Do not use this option. • **Customer Engagement**: A cluster profile for Avaya contact center snap-ins. Use when instructed by the appropriate Avaya product installation guides.
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 Group	The cluster group number that you assign to the cluster. You can enter a value from 1 to 10. This optional field is only used to configure attributes for multiple snap-ins.
Cluster IPv4	The unique IPv4 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. Leave this field blank for a single-node cluster.
Cluster IPv6	The unique IPv6 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. Leave this field blank for a single-node cluster.
Cluster Fully Qualified Domain Name	The unique FQDN that you assign to the cluster.

Table continues

Name	Description
Enable Cluster Database	The check box to enable a cluster database. **Note:** You cannot clear the check box if snap-ins are installed on the cluster that require a cluster database.
Enable Database Auto Switchover	The check box to enable automatic switchover of clusters with two or more servers in a high availability database scenario. If you do not select this check box, you must manually enable the standby server to take over whenever the active server is down.
Description	The cluster description.

Cluster Attributes

Name	Description
Pre-3.8.1 Cluster	Clear this attribute if the cluster has Avaya Breeze® platform R3.8.1 or later installed. Select this attribute only if the cluster has an earlier version of Avaya Breeze® platform installed.
Authorization Service Address	The FQDN or IP address of the cluster on which the Authorization Service is running.
Use secure connection for centralized logging	Check box to ensure that connections to the Centralized Logging destination are secure. This field is only available for the Customer Engagement profile.
Centralized logging destination	The destination for centralized logging: **Breeze Cluster** or **External Server**. This field is only available for the Customer Engagement profile.
Breeze cluster as destination for centralized logging	The Avaya Breeze® platform cluster on which you installed the centralized logging snap-in. This field is only available for the Customer Engagement profile. Configure this field if you set **Breeze Cluster** as the value for **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 only available for the Customer Engagement profile. Configure this field if you set **External Server** as the value for **Centralized logging destination**.

Table continues

Name	Description
Default SMS Connector Service	The default SMS connector when multiple SMS connectors are installed in a cluster. You can override the default by creating an implicit user pattern that matches the sending SMS number and assigning an SMS connector to that implicit user.
The URL of the announcement to play during failover	The URL of the announcement that is played during a failover.
Additional Java options used by GSC	The additional Java options used by GSC. This option is only available for the Customer Engagement profile.
Grid Heap Size	The size of the grid heap. This option is only available for the Customer Engagement profile.
Grid Heap Size for LU	The size of the grid heap for LU. This option is only available for the Customer Engagement profile.
Grid LRMI Selector Threads	The grid LRMI selector threads. This option is only available for the Customer Engagement profile.
Grid Password	The internal grid password.
Cluster requires a grid	The check box to specify whether the cluster requires a grid. This field is only available for the Core Platform profile. When you edit this attribute, Avaya Breeze® platform displays the following warning message: `Ensure that all Avaya Breeze® server restarts are complete before placing the cluster into Accept New Service state`.
Use secure grid	The check box to secure grid communication.

Table continues

Name	Description
	Note: Enabling or disabling **Use secure grid**: After enabling or disabling **Use secure grid**, wait 10 minutes after committing the change before rebooting the cluster. A reboot is not required for this change to take effect. However, if you plan to reboot the cluster for other reasons, do not reboot immediately. The 10-minute wait allows internal reconfiguration to complete and ensures cluster stability. Recovery in case of service inaccessibility: If service URLs become inaccessible "404 – Not Found", even though System Manager shows the cluster as healthy, it indicates that the cluster was rebooted before the secure grid internal reconfiguration completed. To recover: • Revert the **Use secure grid** setting in **Cluster Editor**. • A reboot is not required. • The cluster will recover automatically once the setting is reverted. For more information on using the **Use secure grid** communication option, see the solution documentation.
Grid Thread Stack Size	The size of the grid thread stack. This option is only available for the Customer Engagement profile.
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 greater than 3.
Http or Https traffic rate limit in bytes/sec per client	The rate limit on the HTTP or HTTPS traffic served for each connection. For General Purpose Large clusters, this value must be greater than 300,000 bytes for each 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 seconds.
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.

Table continues

Name	Description
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 seconds.
Only allow secure web communications	The check box to enable only HTTPS requests. By default, this check box is selected.
Hung Thread Detection Threshold (seconds)	Available only with the Customer Engagement cluster profile. Causes a Java core to be generated when a thread has been running longer than the administered value. The default value should be sufficient in most cases. When an application causes a thread to be in use for a longer period of time, such as a complex database request, and the expected completion time is expected to be long, then changing this value will reduce or eliminate the Java Cores. Increasing this value will mask any hung threads that would have been detected at a lower interval. Modification of this value requires a cluster reboot for the change to take effect.
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® platform 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. With this, Avaya Breeze® platform 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 that is used to identify the real client IP address is X-Real-IP.
Default call provider for Make Call	The call provider used for Make Call, a call that is initiated (Make Call) from an Avaya Breeze® platform snap-in. The default value is **SIP**, which corresponds to using SIP to connect to Avaya Aura® for call processing. If ZangCallConnector is loaded, you can install and use ZangCallConnector for making or initiating calls.
Default Identity for special make call cases	The default identity that is used for calls generating from Avaya Breeze® platform. If a user does not specify an identity, then Breeze uses the value in this field.
The maximum number of Avaya Breeze Servers allowed in Cluster	The maximum number of Avaya Breeze® platform servers that you can add to a cluster.

Table continues

Name	Description
Media server monitoring period (seconds)	The period of polling. Each Avaya Aura® Media Server is periodically polled from each Avaya Breeze® platform 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® platform waits after all media operations are complete before shuffling Avaya Aura® Media Server out of the media path. All cluster profiles that support SIP call processing display this cluster attribute. The default value is 3 seconds.
Select AAMS by caller location - Priority 1	The check box to configure the cluster to select the 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 the Avaya Aura® Media Server based on the Avaya Breeze® platform location if the **Select AAMS by caller location - Priority 1** criteria is not met or its check box is disabled.
Select any AAMS - Priority 3	The check box to configure the cluster to select the Avaya Aura® Media Server if the **Select AAMS by caller location - Priority 1** and **Select AAMS by Breeze server location - Priority 2** criteria are not met or their check boxes are disabled.
Avaya Aura® Media Server - Media Preservation Time (minutes)	The amount of time that Avaya Aura® Media Server should wait before terminating an audio or video stream after a failure is detected in the call signaling path.
Media IP version to retry in case of ANAT failure	Select an option from the drop-down list.
Retry IPv4 media in case of IPv6 failure	Check box to try IPv4 media if IPv6 fails.
Retry IPv6 media in case of IPv4 failure	Check box to try IPv6 media if IPv4 fails.
H.264 Video profile_idc	The H.264 video profile: • **CB(Constrained Baseline profile-42)** • **H(High profile-64)**

Table continues

Comments on this document?

Name	Description
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 of REST signaling.
Minimum TLS Version for Non-SIP Traffic	The TLS version that is used for incoming HTTP requests to Avaya Breeze® platform. By default, Avaya Breeze® platform uses the value of the **Minimum TLS version** field set in the System Manager configuration. • If the value of the **Minimum TLS Version** field is TLSv1.1, Avaya Breeze® platform uses TLSv1.2. • If the value of the **Minimum TLS Version** field is SSLv3, Avaya Breeze® platform uses TLSv1.0.
Minimum TLS Version for SIP Call Traffic	The TLS version that is used for SIP calls intercepting Avaya Breeze® platform. By default, Avaya Breeze® platform uses the value of the **Minimum TLS version** field set in the System Manager configuration. • If the value of the **Minimum TLS Version** field is TLSv1.1, Avaya Breeze® platform uses TLSv1.2. • If the value of the **Minimum TLS Version** field is SSLv3, Avaya Breeze® platform uses TLSv1.0.
Platform Space Container Heap Size (MB)	The size of the platform space container heap in MB. This option is only available for the Customer Engagement profile.
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 minimum version	The list of required snap-ins for a specific cluster profile type. The minimum required version of each snap-in is also included.

Table continues

Name	Description
Reverse Proxy URL (protocol://FQDN) used to access the cluster	Use this field to specify the URL of a reverse proxy deployed in front of the Avaya Breeze® platform cluster. Login-related redirections from adopting services or snap-ins use the URL specified in this field instead of the default Avaya Breeze® platform cluster FQDN. Currently, a limitation exists. When this field is configured, if a user attempts to log in using the cluster FQDN, further redirections are forced to happen through the proxy URL instead of the cluster FQDN.
Default SIP Domain	The default SIP domain for the cluster. If an Avaya Breeze® platform snap-in does not include a domain in the addresses that the snap-in sends to the Call Manipulation API, the snap-in appends this domain to the address.
Use secure signaling for platform initiated SIP calls	The check box to use secure signaling to initiate WebRTC Connect 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, Avaya Breeze® platform selects the *Connected* pre-answer mode. 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.

Table continues

Name	Description
Percent of memory to allocate base processes	The percentage of memory to allocate for base processes. **Note:** Do not change the value of this field unless recommended by snap-ins.
Percent of memory to allocate for WAS	The percentage of memory to allocate for WAS. **Note:** Do not change the value of this field unless recommended by snap-ins.
Limit on the memory (GB) to allocate for WAS	The field to set a limit on the memory allocated for WAS. **Note:** Do not change the value of this field unless recommended by snap-ins.

Servers tab

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

Name	Description
Name	The name of the Avaya Breeze® platform server.
Version	The version of the Avaya Breeze® platform server.
Description	The description of the Avaya Breeze® platform 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.

Table continues

Name	Description
Action Pending	The actions that are pending for the snap-in. If no actions are pending, the system displays **None**.
Uninstall	If you select a snap-in and click **Uninstall**, then the snap-in is removed from the cluster after all activity ceases.
Force Uninstall	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	Selects the TLS version of the snap-in. The acceptable values are: • **Default** • **TLS v1.0** • **TLS v1.2** • **TLS v1.3** If you select **Default**, the Avaya Breeze® platform uses the the **Minimum TLS Version** field value set in the System Manager global configuration. You can change the TLS version of multiple snap-ins at a time.

Reliable Eventing Groups tab

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

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

Avaya Aura® Media Server priority settings

The following three priority check boxes determine how Avaya Breeze® platform selects which media server to use:

- **Select AAMS by caller location - Priority 1**
- **Select AAMS by Breeze server location - Priority 2**
- **Select any AAMS - Priority 3**

By default, all three check boxes are selected.

Avaya Breeze® platform uses the following selection algorithm:

1. If the **Select AAMS by caller location - Priority 1** check box is selected, Avaya Breeze® platform checks if the caller's location is defined and selects an Avaya Aura® Media Server in the same location.
2. If Avaya Breeze® platform has not yet found an Avaya Aura® Media Server and if the **Select AAMS by Breeze server location - Priority 2** check box is selected, the Avaya Breeze® platform server location is used, if available. Avaya Breeze® platform selects an Avaya Aura® Media Server in the same location.
3. If Avaya Breeze® platform has not yet found an Avaya Aura® Media Server and if the **Select any AAMS - Priority 3** check box is selected, Avaya Breeze® platform selects the least loaded Avaya Aura® Media Server in the system.

If there is no Avaya Aura® Media Server with remaining capacity, the media operation fails.

Location settings

Avaya Breeze® platform uses location settings, if provided, to select a media server for a given call. You can configure locations and devices on System Manager from **Elements › Routing › Locations**. While configuring a location, you can configure IP address patterns for devices.

When you configure SIP entities, such as Avaya Breeze® platform, from **Elements › Routing › SIP Entities**, you can choose to select a location for the SIP entity. The locations in the **Location** drop-down list are based on what you configured in **Elements › Routing › Locations**. The SIP entity location overrides any device settings you configured on the Location Details page.

Tip:

- Configure Avaya Aura® Media Server locations for each media server in **Elements › Media Server › Server Administration**. You can only see enrolled media servers on this page.
- If Avaya Breeze® platform and Avaya Aura® Media Server are co-located in the same data center, select the same location for them.

HTTP Security page field descriptions

Use this page to configure access permissions for HTTP requests to Avaya Breeze® platform. You can access this page on System Manager by navigating to **Elements › Avaya Breeze® › Configuration › HTTP Security**.

Name	Description
Cluster	If you select a cluster from the **Cluster** drop-down list, 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 the selected cluster, the new hosts will be applicable only for the Avaya Breeze® platform 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® platform Release 3.1 or earlier. For Legacy clusters on Avaya Breeze® platform 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® platform 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® platform 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® platform 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® platform 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® platform 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® platform for the selected cluster.

Table continues

Name	Description
	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® platform 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 64

Implicit User Profiles page field descriptions

You can access the Implicit User Profiles page on System Manager by navigating to **Elements › Avaya Breeze® › Configuration › Implicit User Profiles**. Use this page 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 page 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. This page is displayed when you click **New** or **Edit** on the Implicit User Profiles page.

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 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. Alternatively, you can use the communication address defined on the Communication Profile tab of the user profile, which you can access on System Manager by navigating to **User › User Management › Manage Users**. 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. The value is auto-populated based on the pattern.
Max	The maximum number of digits to be matched from the pattern. The 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 a new profile or changes to the existing profile.

Related links

Assigning a service profile to implicit users on page 50

Install Trusted Certificate field descriptions

Use this page to retrieve a trust certificate that will be used for all the Avaya Breeze® platform 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
Choose file	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.

Related links

Adding a trusted certificate to all Avaya Breeze platform servers in a cluster on page 24

JDBC Providers page field descriptions

Option name	Description
Name	The name of the resource provider.
Class Name	The name of the class file.
Jar File	The JDBC jar file or library that you have uploaded.

Table continues

Option name	Description
Description	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
Class Name	The name of the class file in the driver jar that implements the javax.sql.DataSource interface. The actual class name might differ per the uploaded driver jar. For example: For Postgres, you can enter `org.postgresql.xa.PGXADataSource` For MySQL, you can enter `com.mysql.jdbc.jdbc2.optional.MysqlXADataSource` For MS-SQL, you can enter `com.microsoft.sqlserver.jdbc.SQLServerXADataSource` For Oracle, you can enter `oracle.jdbc.xa.client.OracleXADataSource` or `oracle.jdbc.pool.OracleConnectionPoolDataSource`
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.

Table continues

Name	Description
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.
TLS	The check box that indicates whether the JDBC data source may use TLS-secured communication. Selecting this check box enables TLS when a database server is accepting TLS connections. The JDBC driver provided by database vendor determines which TLS version is used. Clear this check box if the server does not support TLS.
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 page field descriptions

Use this page to run maintenance tests. You can access this page on System Manager by navigating to **Elements › Avaya Breeze® › System Tools and Monitoring › Maintenance Tests**. For more information about maintenance tests, see *Maintaining and Troubleshooting Avaya Breeze® platform*.

Name	Description
Select Avaya Breeze® to test	The name of the Avaya Breeze® platform instance that you are testing. Select the instance from the drop-down menu.
Test Description	The name of the maintenance test.
Test Result	An indication of whether the test was successful or failed.
Test Result Time Stamp	The time when the test was 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 page field descriptions

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

Name	Description
Media Server	The name of the Avaya Aura® Media Server instance.

Table continues

Name	Description
Overload Status	The status of Avaya Aura® Media Server. This column displays: • ✓ when Avaya Aura® Media Server is not overloaded. • ✗ when Avaya Aura® Media Server is overloaded.
License Mode	The license mode of the Avaya Aura® Media Server instance: • **licensed** • **unlicensed**
Lock Mode	The operational state of Avaya Aura® Media Server: • **locked** • **unlocked**
Authentication	This columm indicates whether Avaya Breeze® platform is able to authenticate with Avaya Aura® Media Server.
Avaya Breeze Server	The name of the Avaya Breeze® platform server. The system will not display the value for: • The Avaya Breeze® platform servers prior to Release 3.3. • The Avaya Breeze® platform servers that are not reachable.
Connection Status	The connection status of Avaya Breeze® platform with Avaya Aura® Media Server. This column displays: • ✓ when Avaya Breeze® platform is able to connect with Avaya Aura® Media Server. • ✗ when Avaya Breeze® platform is unable to connect with Avaya Aura® Media Server. **Connection Disabled** is displayed when the **Select AAMS by Breeze server Location - Priority 2** cluster attribute is selected and the location of the Avaya Breeze® platform server is different than the location of Avaya Aura® Media Server.

Reliable Eventing Groups page field descriptions

You can access the Reliable Eventing Groups page on System Manager by navigating to **Elements › Avaya Breeze® › Reliable Eventing Administration › Dashboard**.

Comments on this document?

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 page field descriptions

This page is displayed when you click **New** or **Edit** on the Reliable Eventing Groups page.

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.

Table continues

Name	Description
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® platform brokers. • **Standalone**: If you select this option, you must assign minimum one Avaya Breeze® platform broker.
Assigned Brokers section	
Name	The name of Avaya Breeze® platform server.
Version	The version of the Avaya Breeze® platform server.
Description	The description of the Avaya Breeze® platform server.
Unassigned Brokers section	
Name	The name of Avaya Breeze® platform server.
Version	The version of the Avaya Breeze® platform server.
Description	The description of the Avaya Breeze® platform 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 page field descriptions

You can access this page on System Manager by navigating to **Elements › Avaya Breeze® › Server Administration**. Use this page to:

- Add or edit an Avaya Breeze® platform server.
- Shut down or restart an Avaya Breeze® platform server.
- Assign trust and identity certificates to the Avaya Breeze® platform servers.

- Access information about the service status and maintenance tests for each Avaya Breeze® platform server.

Column name	Description
Name	The name of the Avaya Breeze® platform server. Click the name to navigate to the Avaya Breeze® Instance Editor page.
Cluster Name	The name of the cluster to which the Avaya Breeze® platform server belongs.
Service Install Status	The status of the installed services. • ✔ indicates that all services have been installed. • ⚠ indicates that the service is in the process of installing or uninstalling. • ✖ indicates that the service has not downloaded properly or is not installed. • - - - - indicates that there is no connection. When you click on the installation status icon, the Service Status page is displayed. This page provides more information about the service, and also provides options to reinstall or start the service.
Tests Pass	Maintenance test results. A green check mark indicates the test or tests passed. A red X indicates a test failed. • ✔ indicates that the test passed. • ✖ indicates that the test failed. • - - - - indicates that there is no connection. When you click on the status icon, the Maintenance Tests page is displayed.
Alarms	The number of alarms raised for the Avaya Breeze® platform server. This value is in the format <critical + major alarm count>/<minor alarm count>/<warning alarm count>.
System State	The current state of the Avaya Breeze® platform server. The system states are: • Accepting • Denying • - - - - (No connection)
Security Module	The state of the security module. The states are: Up, Down, and - - - (unknown). • Up • Down

Table continues

Comments on this document?

Column name	Description
	• - - - - (No connection)
Activity	The sum of active call, HTTP, and other custom-defined sessions of the snap-ins installed on the Avaya Breeze® platform server.
License Mode	The license mode of the Avaya Breeze® platform server. All Avaya Breeze® platform servers must be in compliance with the license file, including the major release and the total number of Avaya Breeze® platform servers. The possible license modes are: • **License Normal Mode**: A valid license file is installed. License errors are not found. The complete functionality is present for the Avaya Breeze® platform instance. • **License Error Mode**: License error is seen in this mode. The Avaya Breeze® platform instance is in a 30 day grace period. Complete functionality is available during the grace period. System Manager displays this warning icon along with the date and time of the grace period expiration. • **License Restricted Mode**: The Avaya Breeze® platform instance enters this mode after the 30 day grace period expires. The Avaya Breeze® platform server goes into the Deny New Service mode. The server automatically returns to service when you install a valid license file. For more information about license errors, see *Maintaining and Troubleshooting Avaya Breeze® platform*.
Overload Status	The overload status of the Avaya Breeze® platform server. • indicates that the server is not in an overloaded state. • indicates that the server is in an overloaded state. • - - - - indicates that there is no connection.
Version	The version of the Avaya Breeze® platform software that is installed on the Avaya Breeze® platform server.
Last Reboot Status	The status of the last cluster reboot operation.

Button or menu option	Description
Edit	Launches the Avaya Breeze® Instance Editor page and enables you to edit the the selected Avaya Breeze® platform server.

Table continues

Button or menu option	Description
New	Launches the Avaya Breeze® Instance Editor page and enables you to add a new Avaya Breeze® platform server.
Delete	Deletes the selected Avaya Breeze® platform server.
System State › Accept New Service	Allows incoming call requests for the selected Avaya Breeze® platform server.
System State › Deny New Service	Blocks incoming call requests for the selected Avaya Breeze® platform server.
Shutdown System › Shutdown	Shuts down the selected Avaya Breeze® platform server.
Shutdown System › Reboot	Reboots the selected Avaya Breeze® platform server.

Icon	Description
	Indicates that the Avaya Breeze® platform server is one of the lookup servers.
	Indicates that the Avaya Breeze® platform server is the active load balancer.
	Indicates that the Avaya Breeze® platform server is the active load balancer, but it is unable to connect to the standby server.
	Indicates that the Avaya Breeze® platform 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 that the Avaya Breeze® platform server is the active server in a cluster database.
S	Indicates that the Avaya Breeze® platform server is the standby server in a cluster database.

Services page field descriptions

You can access this page on System Manager by navigating to **Elements › Avaya Breeze® › Service Management › Services**. Use this page to load, install, uninstall, start, stop, and delete a snap-in.

Column 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 cannot 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.
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® platform 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® platform clusters. The element manager raises a critical alarm. If you install the license file the snap-in returns to the

Table continues

Column name	Description
	License Normal mode. You must manually re-install the snap-in to any cluster from which the snap-in was uninstalled. • **Not Applicable**: For services that do not require a license file.
Avaya Signed	Indicates whether the snap-in is Avaya signed. The column displays a green tick mark if the snap-in is 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 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. For Avaya Snapp Store, go to https://www.devconnectmarketplace.com/marketplace/ and navigate to **Avaya Snapp Store**.
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® platform 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® platform 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.

Table continues

Button	Description
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.
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

Service Databases page field descriptions

You can access the Service Databases page on System Manager by navigating to **Elements › Avaya Breeze® › Service Management › Service Databases**. 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.

Table continues

Button	Description
Delete	Deletes the selected database.

Service Ports page field descriptions

You can access the Service Ports page on System Manager by navigating to **Elements › Avaya Breeze® › Configuration › Service Ports**. Use this page to change the assignment of service ports.

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.

Option	Description
Service	The list of Avaya-developed snap-ins that have default ports specified. Select the snap-in for which you want to modify the port configuration.
Cluster	The list of clusters that are available.

Selected Service Ports

Column 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.

Column 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 page field descriptions

You can access the Service Profile Configuration page on System Manager by navigating to **Elements › Avaya Breeze® › Configuration › Service Profiles**. Use this page to create, edit, or delete a service profile.

Column 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.

Table continues

Button	Description
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 36

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 section

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

The following tabs are available in the Services in this Service Profile section:

- All Services tab
- Service Invocation Details tab

All Services tab descriptions

This tab lists all services that you have added to a service profile.

Column 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 tab descriptions

This tab includes the following sections:

- Calling Service Invocation Order

- Called Service Invocation Order
- Service Not in an Invocation Order

Column 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. This column is displayed in the Calling Service Invocation Order amd Called Service Invocation Order sections.
Name	The name of each service in the service profile.
Version	The version of each service in the service profile.
Description	A description of the service.

Available Service to Add to this Service Profile section

Column 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. When you add a service to a service profile, it is displayed in the Services in this Service Profile section.
Name	The name of each service that can be added to the service profile.
Description	A description of each service 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® platform 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® platform sever.

Table continues

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

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

SNMP MIB Download page field descriptions

When you load a snap-in on System Manager, Avaya Breeze® platform generates a zip file. You can download this zip file from the SNMP MIB Download page, which you can access by navigating to **Elements › Avaya Breeze® › System Tools and Monitoring › SNMP MIB**.

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

Button	Description
Download	Downloads the SNMP MIB zip file.

System Resource Monitoring page field descriptions

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

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

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

Chapter 15: Deployment operations

This section includes deployment procedures that must be performed exclusively using the System Manager web console. For more information about deployment, see *Deploying Avaya Breeze® platform*.

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

Before you begin

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

Procedure

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

Administering an Avaya Breeze® platform instance

About this task

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

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

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

Before you begin

Ensure that you have the following:

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

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

- An Avaya Breeze® platform management FQDN that is registered in DNS.
- The IPv4 or IPv6 address including the IPv4 network mask or IPv6 Network prefix length, and IPv4 or IPv6 default gateway for the Avaya Breeze® platform **Security Module**.
- The SIP entity name associated to the Avaya Breeze® platform **Security Module**.

Procedure

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

   UCID Network Node ID is a unique, numeric node ID that is assigned to each Avaya Breeze® platform server provisioned.
5. In the Management Network Interface **FQDN or IPv4 Address** field, type the IP address or FQDN of the Avaya Breeze® platform **Management Network Interface**.
6. **(Optional)** In the Management Network Interface **FQDN or IPv6 Address** field, type the IPv6 address or FQDN of the Avaya Breeze® platform **Management Network Interface**.
7. In the Security Module fields, type the required addresses for the IPv4 or IPv6 SIP Entity Address, Network Mask or Network prefix length, and Default Gateway used for the SIP (Security Module) network.
8. Click **Commit** to save your changes.

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

For more information, see "Creating a new cluster".

d. Click **Cluster State › Accept New Service**.

For more information, see "Accepting new service".

Administering Avaya Aura® Media Server URI

Before you begin

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

Procedure

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

Chapter 16: Maintenance operations

This section includes maintenance procedures that can be performed exclusively from the Avaya Breeze® platform element of System Manager. For more information about maintenance procedures, see *Maintaining and Troubleshooting Avaya Breeze® platform*.

Modifying the logging configuration

About this task

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

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

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

Procedure

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

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

Downloading the Avaya Breeze® platform SNMP MIB

About this task

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

Procedure

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

Tip:

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

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

Running maintenance tests

Procedure

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

Viewing the current usage of a cluster

Procedure

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

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

Viewing the peak usage of a cluster

Procedure

1. In System Manager, click **Elements › Avaya Breeze®**.
2. Click **System Tools And Monitoring › System Resource Monitor**.
3. In the **Cluster** field, select the cluster for which you want to view the peak usage.
4. In the **Time Period** field, select one of the following:

- **Today**
- **Yesterday**
- **2 Days Ago**
- **3 Days Ago**
- **4 Days Ago**
- **5 Days Ago**
- **6 Days Ago**

5. Click **View Peak Usage**.

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

Resetting the peak usage of a cluster

Procedure

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

Chapter 17: Certificate management

Avaya Breeze® platform certificate deployment is managed by Avaya Aura® System Manager through 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® platform server.
- Add or remove trusted certificates on the Avaya Breeze® platform server.
- Replace or renew identity certificates on the Avaya Breeze® platform server signed by the Avaya Aura® System Manager CA.
- Replace identity certificates on the Avaya Breeze® platform server signed by a third party CA.

Before attempting to make certificate changes in Avaya Breeze® platform, review your solution to understand which network elements will be affected. This will require planning and network audits before deploying new certificates. Typically, certificate changes include the following types of stages:

- 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® platform 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 Session Manager.

Note:

Avaya Breeze® platform is initially deployed with certificates generated by the System Manager CA that lack necessary values in the SAN for the SIP and HTTPS certificates. Avaya Breeze® platform does not know its security module IP/FQDN at time of deployment. The user is required to update the SIP and HTTPS certificates from the System Manager GUI to include the security module IP/FQDN in the SAN field. Other Avaya Aura® servers now require this information when establishing trust with Avaya Breeze® platform.

Caution:

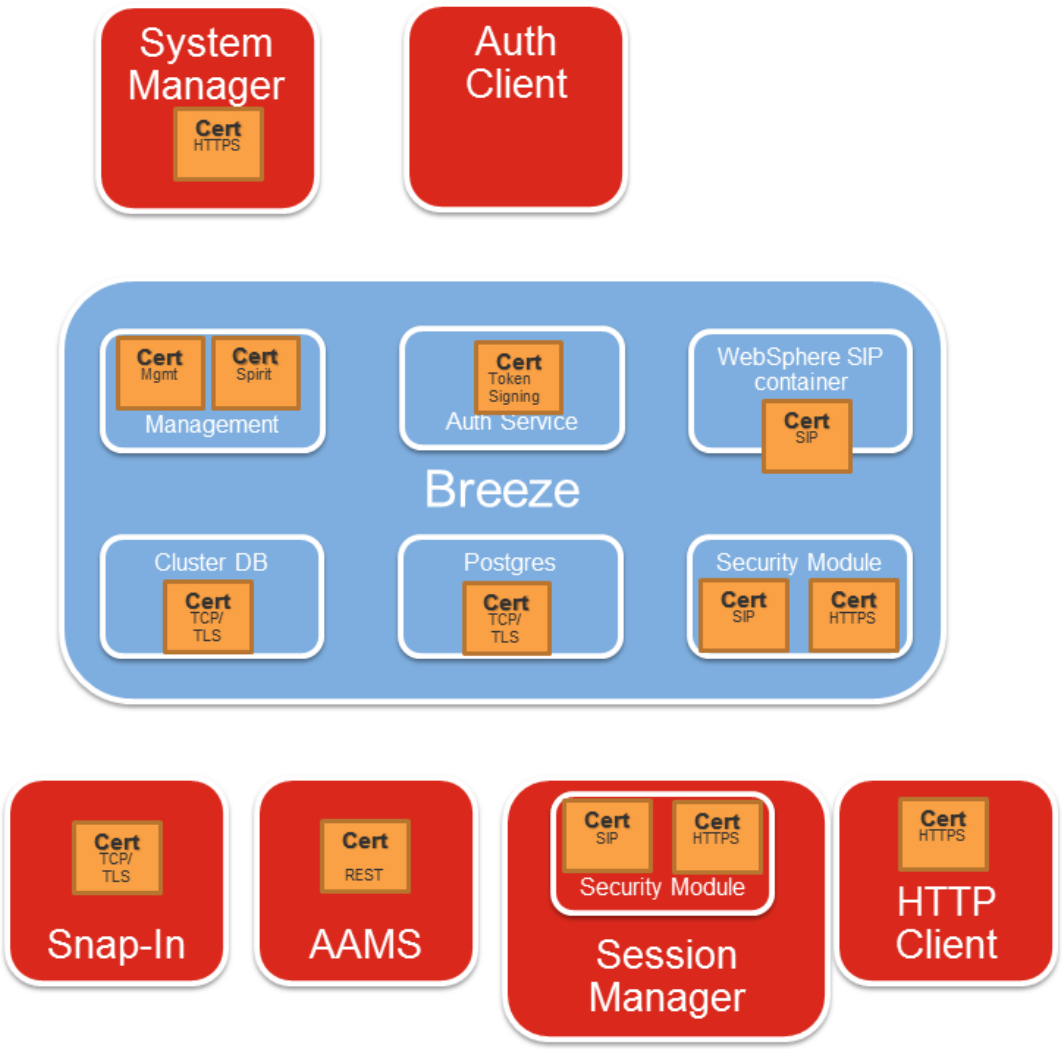
Any changes to these interfaces can cause major service interruptions.

The near-end and far-end entities can use certificates to authenticate each other, and each side presents its identity certificate during TLS negotiation. If one side does not trust the signer of the other side's identity certificate, 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. The root CA certificate must be stored in the entity's trusted list, which is also known as a Trust Store.

Warning:

To change the identity certificate of an Avaya Breeze® platform 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 certificate.

The following diagram depicts the identity certificate on Avaya Breeze® platform, and its TLS connections to other elements in the network. Only a small subset of elements is represented.



Avaya Breeze® platform does not support elliptical curve ciphers.

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® platform, 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 pre-installed 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 in the SIP and HTTP certificates.

Related links

Replacing an identify certificate with a System Manager CA certificate on page 157

Identity certificate descriptions

Multiple identity certificates exist on Avaya Breeze® platform.

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® platform.	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® platform and external servers. For example, Session Manager.	SIP	Default port 5061 on Avaya Breeze® platform. Other ports also supported.	Yes	Any product that needs a SIP TLS link to Avaya Breeze® platform.
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.

Table continues

Service name	To/from	Protocol	Port	Support 2048 key length and SHA2 signature	Notes
SPIRIT	SAL server on System Manager	HTTPS	Avaya Breeze® platform ephemeral port 22 connections to SMGR port 443 (HTTPS)	Yes	
Management (JBOSS)	Connections between System Manager and Avaya Breeze® platform for management. For example, RMI/JMX and DRS replication.	JMX, RMI, HTTPS	JMX for DRS. Avaya Breeze® platform port 2009 RMI Avaya Breeze® platform port 11099, JMX Avaya Breeze® platform port 11100 HTTPS port 443 on SMGR	Yes	Use for both Internal communication and for external access from some snap-ins.
CDB	Connections to Avaya Breeze® platform local cluster DB	TCP/TLS	Port 5433 on Avaya Breeze® platform	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® platform local Postgres DB	TCP/TLS	Port 5432 on Avaya Breeze® platform	Yes	

Demo certificates

As of Release 3.8.1, Avaya Breeze® platform no longer supports demo certificates for fresh deployments. If your existing deployment uses demo certificates, replace them with certificates signed by the System Manager CA. In many cases, existing TLS communications will break until the System Manager root CA certificate is installed on the far-end truststore.

In earlier releases, Avaya Breeze® platform 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).

Determining whether you are using a demo identity certificate

Procedure

1. In System Manager, click **Services › Inventory › Manage Elements**.
2. Select the Avaya Breeze® platform 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

About this task

You can view identity certificates in System Manager.

Procedure

1. In System Manager, click **Services › Inventory › Manage Elements**.
2. Select Avaya Breeze® platform instance.
3. Click **More Actions › Configure Identity Certificates**.
4. Click **View**.

Replacing an identify certificate with a System Manager CA certificate

About this task

You can replace an Avaya Breeze® platform identity certificate with a certificate 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 certificate. Failure to do so can result in a loss of communication between devices.

Note:

Avaya Breeze® platform is initially deployed with certificates generated by the System Manager CA that lack necessary values in the SAN for the SIP and HTTPS certificates. The user is required to update the SIP and HTTPS certificates from the System Manager GUI to include the security module IP/FQDN in the SAN field. Other Avaya Aura® servers now require this information when establishing trust with Avaya Breeze® platform.

Procedure

1. In System Manager, click **Services › Inventory › Manage Elements**.
2. Select the appropriate Avaya Breeze® platform 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 `securitymodule_sip` or `securitymodule_http` identity certificates, enter the hostname or IP address of the security module.

   The address is the same as the SIP entity address. Where possible, use hostnames instead of IP addresses.
10. Select **RSA** for the **Key Algorithm**.
11. Select **2048** or **4096** as the **Key Size**.
12. For the `securitymodule_sip` or `securitymodule_http` identity certificate, select the **DNS Name** check box and enter the Fully Qualified Domain Name of the security module interface.

    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).

    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** checkbox 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`.

    RFC5922 recommends Subject Alternative Name (SAN) extension entries of the URI type and the SIP scheme over DNS type entries. Avaya SIP Endpoints currently only support the DNS type entries. Use both DNS and URI entries to cover third party SIP devices which may require them.

15. Click **Commit**.

Replacing an identify certificate with a third party CA certificate

About this task

You can replace an Avaya Breeze® platform identity certificate with a certificate issued by a third party CA. A third party CA can be a commercial vendor, such asVeriSign or Symantec, or an enterprise-run CA maintained by your 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 certificate. Failure to do so can result in a loss of communication between devices.

Before you begin

Make sure you have the following:

- An identity certificate with the correct attributes that is signed by the third party CA. This certificate must be in the PKCS#12 format. The identity certificate attributes are described in the sections below. For example, for the SIP certificate, see Security Module SIP identity certificate attributes on page 165.
- 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. In System Manager, click **Services › Inventory › Manage Elements**.
2. Select the appropriate Avaya Breeze® platform 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.

   For example, **Security Module SIP** or **Security Module HTTPS**.
5. Click **Replace**.
6. On the Replace Identity Certificate page, select **Import third party PKCS#12 file**.
7. When prompted to select a file, navigate to the third party signed certificate.
8. Enter the password in the **Password** field.
9. Click **Retrieve Certificate**.

10. 10. Click **Commit**.

Activating a new identity certificate

About this task

To activate a new identity certificate, an Avaya Breeze® platform reboot is required, which is service impacting.

Procedure

1. In System Manager, click **Elements › Avaya Breeze®**.
2. Select an Avaya Breeze® platform instance.
3. Select **Shutdown System › Reboot**.
4. Click **Confirm**.

CSR generation

Avaya Breeze® platform does not provide a UI interface to generate a CSR to replace its identity certificates. An alternate tool, such as OpenSSL, needs to be used to generate the CSR.

The high-level steps to replace Avaya Breeze® platform identity certificates using a CSR are:

- Generate a CSR and its corresponding private key using OpenSSL or a similar tool, such as Microsoft Server. Make sure the CSR contains the correct certificate attributes.
- Send the CSR to the PKI administrator to get it signed by the third party CA. The result is a signed identity certificate.
- Package the identity certificates and private key into PKCS#12 container using OpenSSL or a similar tool.
- Import the PKCS#12 certificate and private key onto Avaya Breeze® platform.

Related links

Replacing an identify certificate with a third party CA certificate on page 159

Generating a CSR and private key using OpenSSL

About this task

This section describes the procedure to generate a private key and a CSR with OpenSSL. This example describes how to replace the security module SIP identity certificate. A similar procedure needs to be followed to replace other identity certificates.

Procedure

1. Log in to Avaya Breeze® platform using an SSH connection..
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.

The following example is for a security module SIP identity certificate.

```
$ 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 CAs 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 this case, only use the DNS type entry with the corresponding 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 is asm1.key. The private key is protected with a passphrase. Remember this passphrase because 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 decrypt TLS traffic or impersonate the Avaya Breeze® platform.

```
$ 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. Ensure that the CSR contains the correct attributes by running 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.

Bundling 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 onto Avaya Breeze® platform.

This procedure is a continuation of the previous procedure about generating a CSR and private key. It assumes the identity certificate file is asm1_signed.pem and the private key is asm1.key.

Before you begin

- Obtain an identity certificate from the PKI administrator.
- The identity certificate must be in PEM format. If it is in a different format, you can use OpenSSL to change it to PEM.

Procedure

1. Copy the asm1_signed.pem to Avaya Breeze® platform and place it in `/home/cust/`.
2. Log into Avaya Breeze® platform using an SSH connection.

3. Run the following OpenSSL command to generate the PKCS#12 file. It would prompt for:

```
$ 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:
```

   You are prompted for the private key passphrase and a new password to to protect the PKCS#12 file. This password is required when installing the identity certificate through System Manager.

   The generated PKCS#12 container file is asm1.p12.

4. Download the generated PKCS#12 container file and install it on Avaya Breeze® platform.

   For more information, see Replacing an identify certificate with a third party CA certificate on page 159.

5. Delete the private key asm1.key from the Avaya Breeze® platform server to avoid it get compromised.

   The following is the path to the private key: `$ rm /home/cust/asm1.key`

Identity certificate expiration alarms

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 Manager automatically renews these identity certificates 30 days before they expire. For identity certificates signed by a third party CA, the PKI administrator must replace or renew them prior to expiration.

Automically renewed System Manager certificates

An alarm warns you when an identity certificate signed by the System Manager root CA is about to expire. 60 days before the identity certificate expires, the OP_MMTC20048 alarm is displayed.

When the identity certificate is automatically renewed, the OP_TMAG20500 alarm is displayed. When you see this alarm, reboot the cluster for the server to pick up the updated certificate. When the reboot is complete, the OP_TMAG20501 alarm is displayed.

Third party identity certificates

Avaya Breeze® platform notifies you of certificate expiration by generating alarms. The following alarms are generated when 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 information about alarms and the expiration process, see *Maintaining and Troubleshooting Avaya Breeze® platform*.

Related links

Rebooting a cluster on page 16

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
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

Table continues

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

(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.

Attribute	Value	Required
	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

[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 certificate attributes

Attribute	Value	Required
Subject	`CN={breeze-fqdn}`	Required
Validity	validity period	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.

Attribute	Value	Required
Authority Key Identifier	hash	Required [11]
Subject Key Identifier	hash	Recommended
Key Usage	`digitalSignature`	Required
	`nonrepudiation`	Required
	`keyEncipherment`	Required
	`dataEncipherment`	Required
Extended Key Usage	`keyAgreement`	Required
	`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
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 with a certificate issued by the System Manager CA

About this task

This procedure describes how to replace an Avaya Breeze® platform SIP identity certificate with a certificate signed by the System Manager CA. For example, if you are using a demo certificate, you can replace it with an identity certificate signed by the System Manager CA.

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

[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.

Procedure

1. Obtain the System Manager root CA certificate.
2. Deploy the System Manager root CA certificate on peer devices that connect SIP TLS to Avaya Breeze® platform.
   a. Identify all the peer servers that connect to Avaya Breeze® platform through SIP over TLS.

      An example of a peer server is Session Manager.
   b. Deploy the System Manager root CA certificate following the peer server documentation on how to deploy the trusted CA certificate on the respective Trust Stores.
3. Replace the SIP identity certificate with a certificate issued by the System Manager CA,
4. Activate the new SIP identity certificate.
5. Verify that the SIP TLS connections are now using the new identity certificate.
6. In System Manager, click **Elements › Session Manager › System Status › SIP Entity Monitoring**.
7. Verify that the link status is UP for Avaya Breeze® platform entities that are TLS connected.

Related links

Replacing an identify certificate with a System Manager CA certificate on page 157

Activating a new identity certificate on page 160

Replacing an identity certificate issued by a third party CA

About this task

Use this procedure to replace an identity certificate issued by a CA other than the System Manager CA. A third party CA can be a commercial vendor, such as VeriSign or Symantec, or an enterprise-run CA maintained by your IT department. You can use this procedure when your third party identity certificate is about to expire and you need to replace it.

Procedure

1. Obtain the new SIP identity certificate through a CSR or a PKCS#12 container.
2. Deploy the trusted third party root CA certificate on Avaya Breeze® platform.
   a. Obtain the root CA certificate from the third party CA PKI administrator.
   b. Add the root CA certificate into the Avaya Breeze® platform SECURITY_MODULE_SIP and WEBSPHERE trust stores.
3. Deploy the trusted third party root CA certificate on peer devices that connect SIP TLS to Avaya Breeze® platform.
   a. Identity all the peer devices that connect to Avaya Breeze® platform through SIP over TLS. For example, Session Manager.
   b. Obtain the root CA certificate.

c. Follow the peer device documentation on how to deploy the trusted CA certificates into their respective Trust Stores.

4. Replace the SIP identity certificate with a third party CA certificate.
5. Activate the new SIP identity certificate.
6. Verify the SIP TLS connections are now using the new identity certificate.
7. In System Manager, click **Elements › Session Manager › System Status › SIP Entity Monitoring**.
8. Verify that the link status is UP for Avaya Breeze® platform entities that are TLS connected.

Related links

Replacing an identify certificate with a third party CA certificate on page 159

Activating a new identity certificate on page 160

Obtaining the new SIP identity certificate through a CSR

About this task

When replacing an identity certificate issued by a third party CA, you can obtain the new SIP identity certificate through a CSR.

Procedure

1. Generate a CSR on Avaya Breeze® platform.
2. Send the CSR to the third party CA PKI administrator to get it signed.
3. Obtain the signed SIP identity certificate in PEM format.
4. Bundle the SIP identity certificate and the private key into a PKCS#12 container.

Obtaining the new SIP identity certificate through a PKCS#12 container

About this task

When replacing an identity certificate issued by a third party CA, you can obtain the new SIP identity certificate through a PKCS#12 container.

Procedure

1. Obtain a SIP identity certificate from the third party CA PKI administrator.
2. Obtain the associated private key bundled in a PKCS#12 container.
3. Verify that the SIP identity certificate has the attributes described in Security Module SIP identity certificate attributes on page 165.

Trust management

Multiple Trust Stores exist on Avaya Breeze® platform. 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
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® platform and external devices (e.g. Communication Manager, SBC, SIP Endpoints, etc.)	SIP
WEBSPHERE	Used by the WebSphere SIP container for validating the identity certificate of the Security Module 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.	SIP
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. In System Manager, click **Services › Inventory › Manage Elements**.
2. Select an Avaya Breeze® platform instance.
3. Click **More Actions › Configure Trusted Certificates**.
4. On the Trusted Certificates page, 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. In System Manager, click **Services › Inventory › Manage Elements**.
2. Select an Avaya Breeze® platform instance.
3. Click **More Actions › Configure Trusted Certificates** .
4. On the Trusted Certificates page, click **Add**.
5. To import a certificate from a file:
   a. Click **Import from file**.
   b. Click **Browse** and locate the file.
   c. Click **Retrieve Certificate**.
   d. Click **Commit**.
6. To import a certificate in the PEM format:
   a. Select **Import as PEM Certificate**.
   b. Locate the PEM certificate.
   c. Open the certificate using Notepad.
   d. Copy the entire contents of the file. You must include the start and end tags:
      -----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE----.
   e. Paste the contents of the file in the box provided at the bottom of the page.
   f. Click **Commit**.
7. To import certificates from existing certificates:
   a. Click **Import from existing**.
   b. Select the certificate from the Global Trusted Certificate section.
   c. Click **Commit**.
8. To import certificates using TLS:
   a. Click **Import using TLS**.
   b. Enter the IP Address of the location in the **IP Address** field.
   c. Enter the port of the location in the **Port** field.
   d. Click **Retrieve Certificate**.
9. Click **Commit**.

Removing trusted CA certificates

Procedure

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

Exporting an Avaya Breeze® platform certificate

Procedure

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

Exporting the System Manager root CA certificate

About this task

When Avaya Breeze® platform 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® platform, such as Communication Manager or SIP devices. This section describes how to obtain the System Manager root CA certificate.

Procedure

1. In 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.

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

Peer certificate validation

All the Avaya Breeze® platform TLS services support validation of peer identity certificates that have a SHA2 signature and a public key length of 2048 bits. Avaya Breeze® platform verifies that the peer identity certificate can 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® platform 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® platform applies the following validations:

1. Mutual TLS authentication: During the TLS handshake, the SIP entity and Avaya Breeze® platform 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® platform behavior depends on the version and its configuration:

- For Avaya Breeze® platform 3.0.0 and earlier, the Enable TLS Endpoint Certificate Validation setting on the Avaya Breeze® platform Administration page controls the validation:

- If Enable TLS Endpoint Certificate Validation is checked, Avaya Breeze® platform 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® platform 3.0.1 and later, the TLS Endpoint Certificate Validation setting on the Avaya Breeze® platform Administration page controls the validation performed on the client certificate. Avaya Breeze® platform 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

CRL limitations

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® platform is registered. On the **Security › Configuration › Security Configuration** page, set the **Certification Recovation Validation** field to **NONE**.

If an outgoing HTTP proxy is set up, CRL download might not work. In this case, you must download the CRL list and then update it on System Manager at **Home › Services › Security › Configuration › CRL Download**.

Certificate revocation management

Avaya Breeze® platform verifies that certificates are valid and not contained on a CRL. If a certificate is on a CRL, Avaya Breeze® platform will not allow a secure connection to be created using that certificate, and the certificate must be updated.

Troubleshooting guidelines for common certificate issues

Certificate expired

The lifespan of identity certificates is usually shorter than CA certificates. When you attempt to use a certificate that is no longer valid, the TLS connection fails with the certificate_expired (45) description in the TLS Alert message. You can see this with a Wireshark capture on the specific port.

Some services will fail to start if the identity certificate they use has expired. For more information, see the 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 the 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 can fail with the unsupported_certificate(43) description in the TLS Alert message. The certificate attributes that are usually mis-configured are those in the Key Usage and Extended Key Usage extensions.

Certificate not yet valid

A newly generated identity certificate with a current “Valid From” date and time might 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 18: Communication Manager administration

If you have a snap-in that uses the Remove Snap-in From Call feature, ensure that you configure Communication Manager.

Administering Communication Manager

Procedure

1. Log in to the Communication Manager CLI interface.
2. Type `system-parameters features`.
3. In the **SIP Endpoint Managed Transfer** field, type `n`.
4. Save the changes.
5. If the endpoints are on different Communication Manager, do the following:
   a. Type `change locations`.
   b. In the **Proxy Selection Route Pattern** field, type the route pattern assigned on the Route Pattern screen.
   c. Save the changes.

Appendix A: CEnetSetup

CLI commands

CEnetSetup or AvayaNetSetup command

Use the `CEnetSetup` or `AvayaNetSetup` command to change the OVA properties specified during deployment.

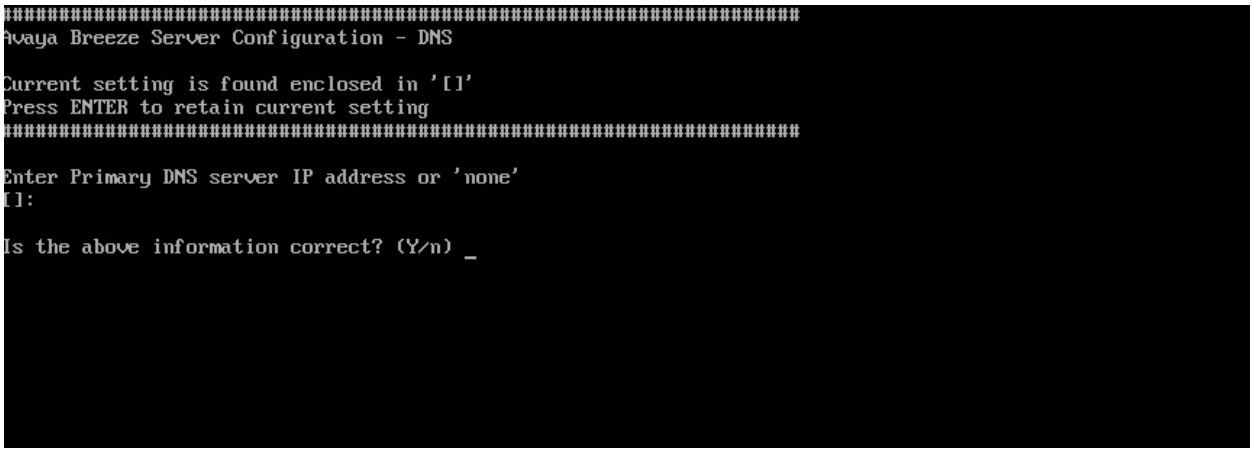
If you change the time zone or time and date settings using one of these commands, set the Avaya Breeze® platform node to the Deny New Service state and reboot it at your earliest convenience to ensure that the change is propagated through all software components. You can select the Deny New Service cluster state on the Cluster Administration page.

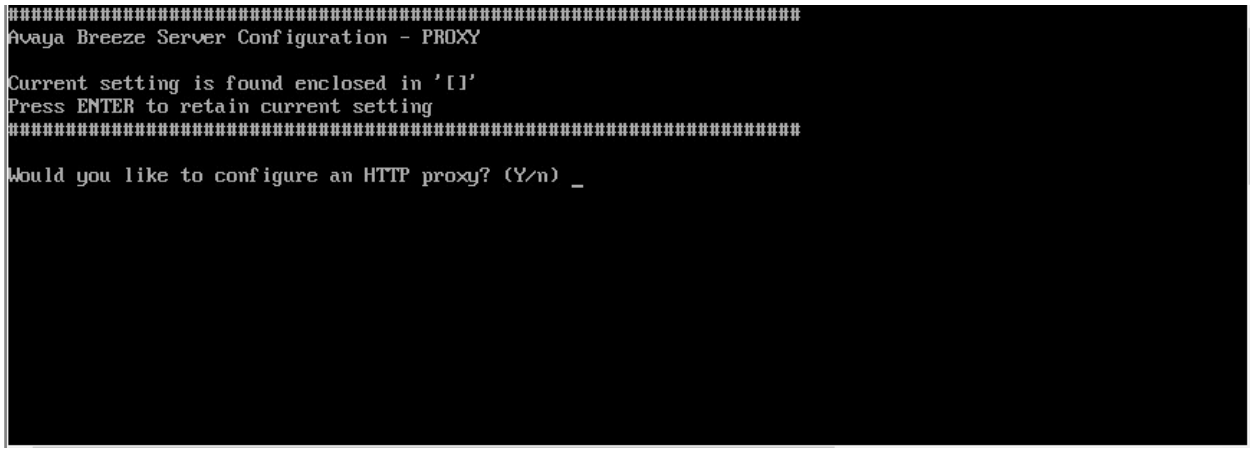
If you are changing the management interface IP address (server IP address), use the VM console (not a session supported by **ssh**).

For information about configuring Avaya Breeze® platform after changing the IP address or FQDN using the `CEnetSetup` or `AvayaNetSetup` commands, see *Deploying Avaya Breeze® platform*.

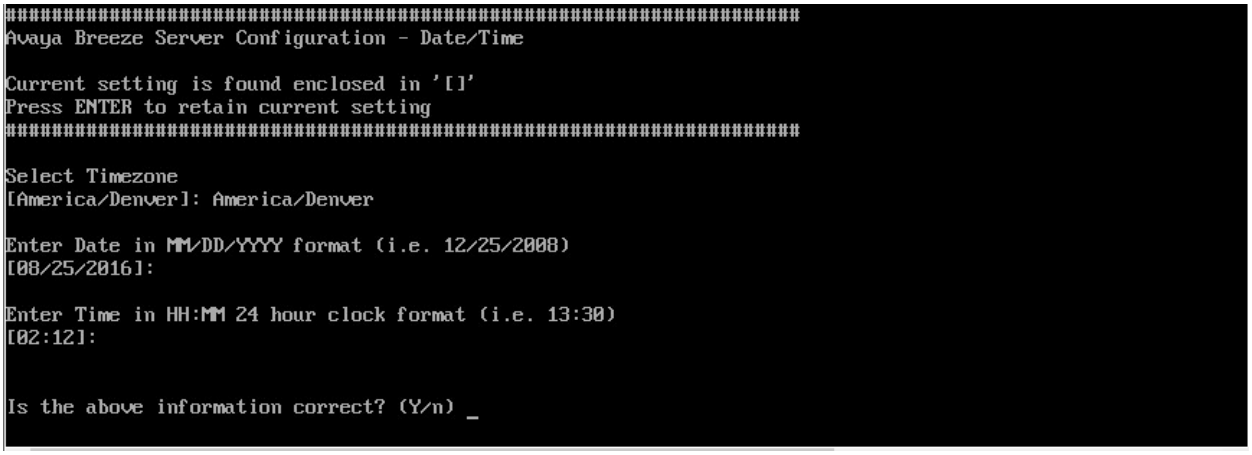
Sample output

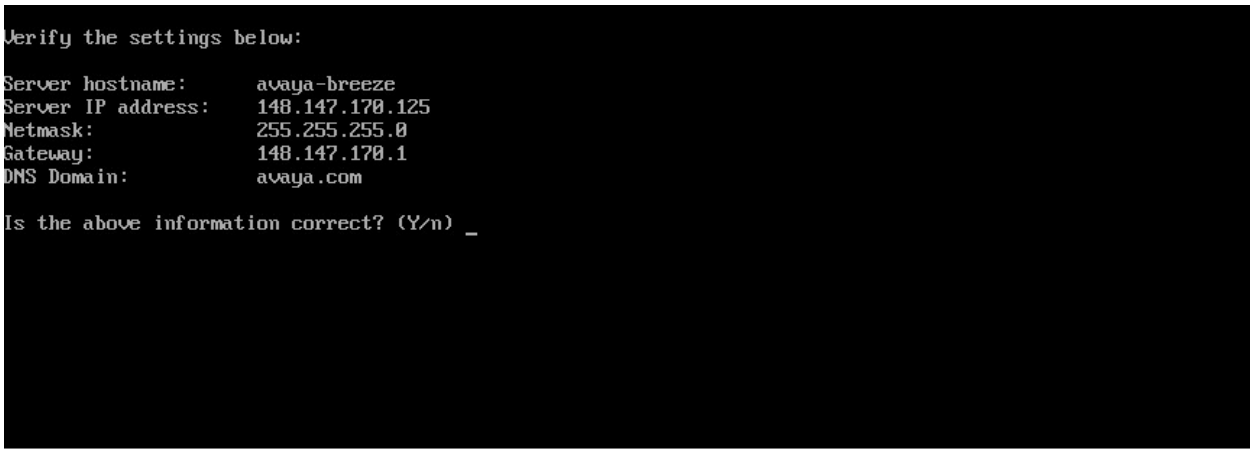







Avaya Timezone Selection
America/Belem
America/Belize
America/Blanc-Sablon
America/Boa_Vista
America/Bogota
America/Boise
America/Buenos_Aires
America/Cambridge_Bay
America/Campo_Grande
America/Cancun
America/Caracas
America/Catamarca
America/Cayenne
America/Cayman
America/Chicago
America/Chihuahua
America/Coral_Harbour


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) _





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® platform 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: Apache Directory Studio Configuration

Configuring an LDAP provider and a SAML provider

Supported OAuth 2.0 identity providers

Avaya Breeze® platform supports the following OAuth 2.0 identity providers (IdPs):

- ADFS 2012
- ADFS 2016
- ADFS 2019
- Azure
- Okta
- OneLogin
- Shibboleth
- SimpleSAML
- Symantec Access Manager (SAM)

Configuring LDAP providers

This section provides example configuration procedures for Apache Directory Studio. This section is purely for reference.

Prerequisites

Java 7.0 or newer. Oracle's JDK is recommended.

Installing Apache Directory Studio

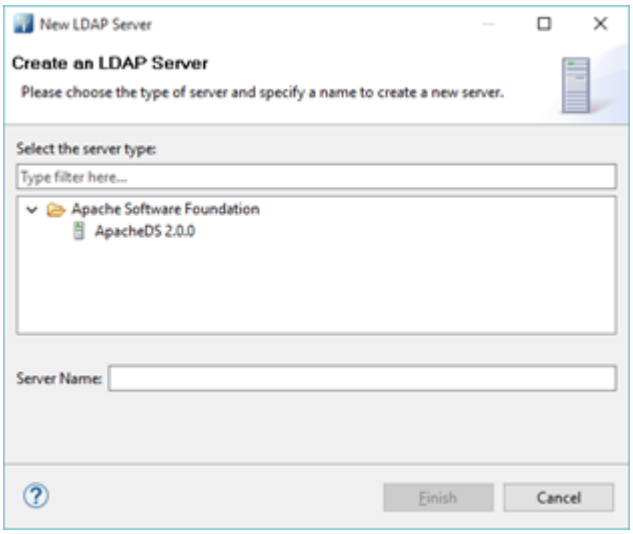
Procedure

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.

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**.

Creating SSL Certificates for LDAP Server

Creating an end entity

Procedure

1. In 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.

Creating the LDAP Server certificate

Procedure

1. In 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.

Downloading the CA that signed the certificate

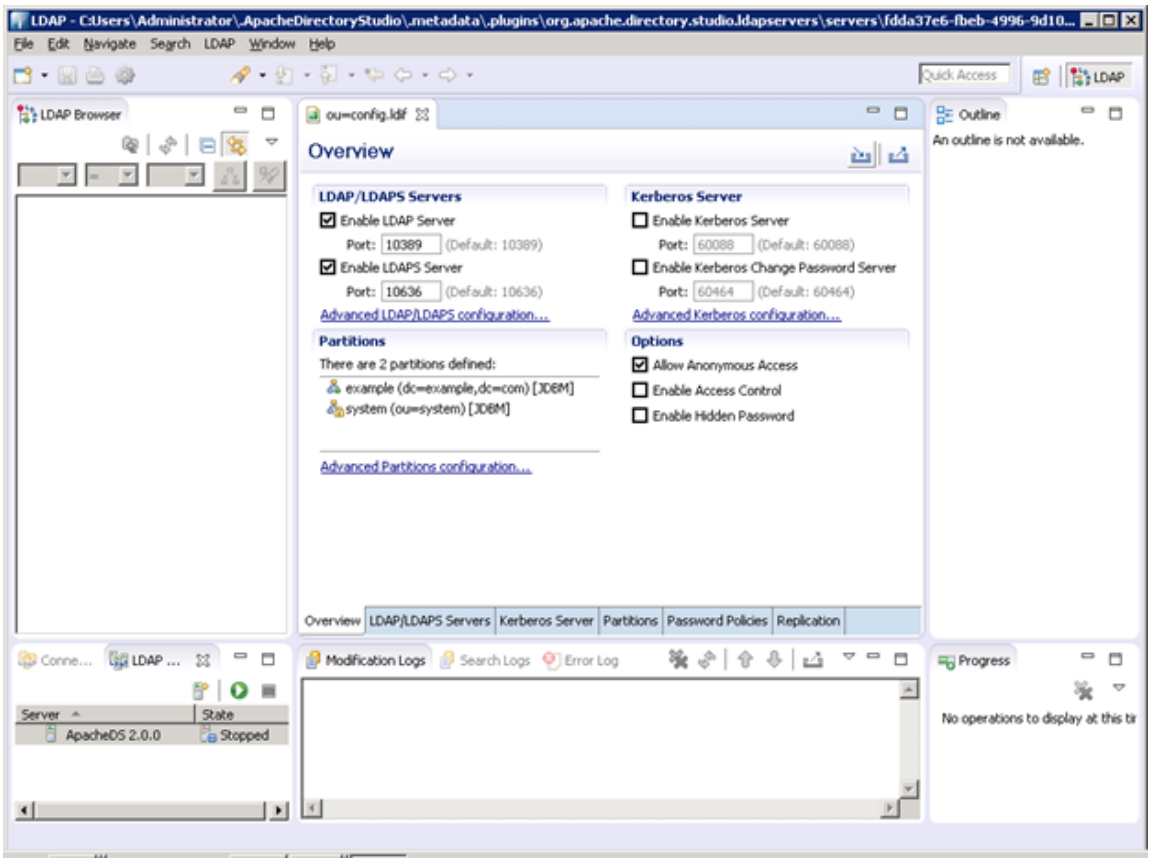
Procedure

1. In 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.

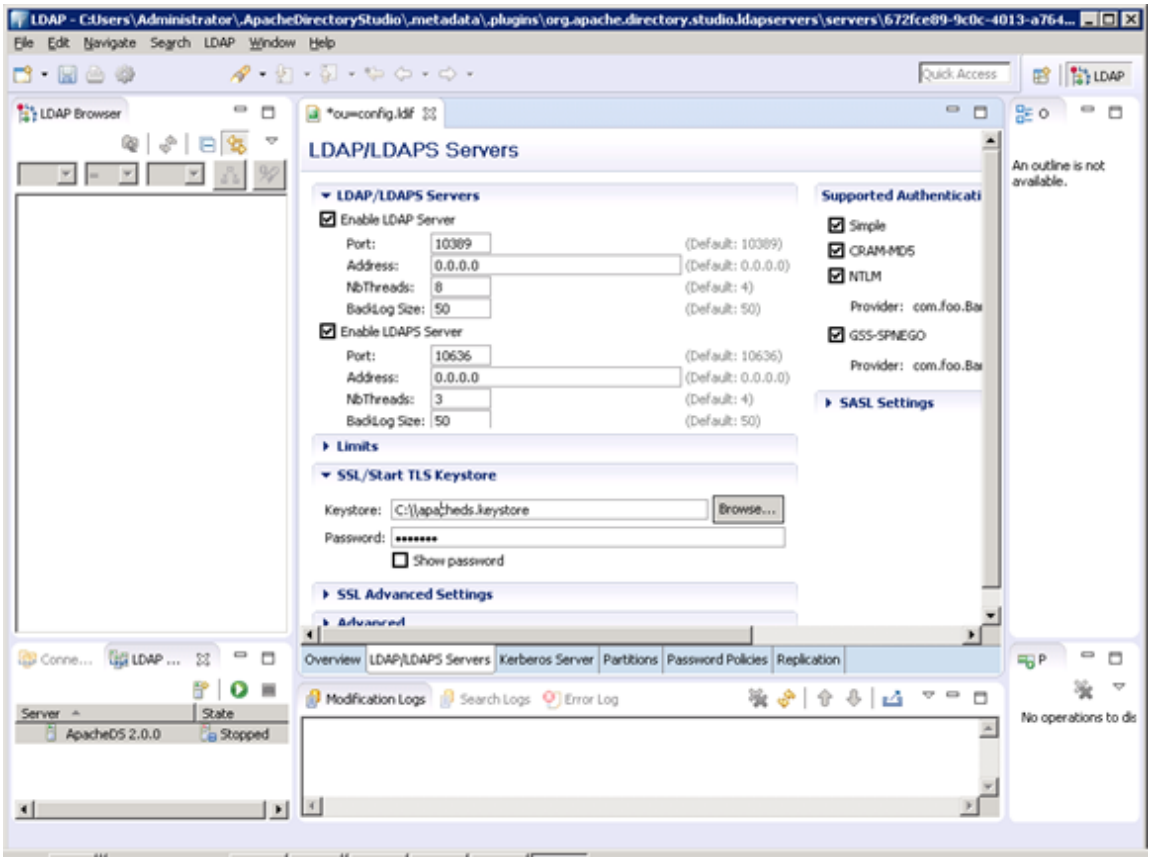
Editing the configuration

Procedure

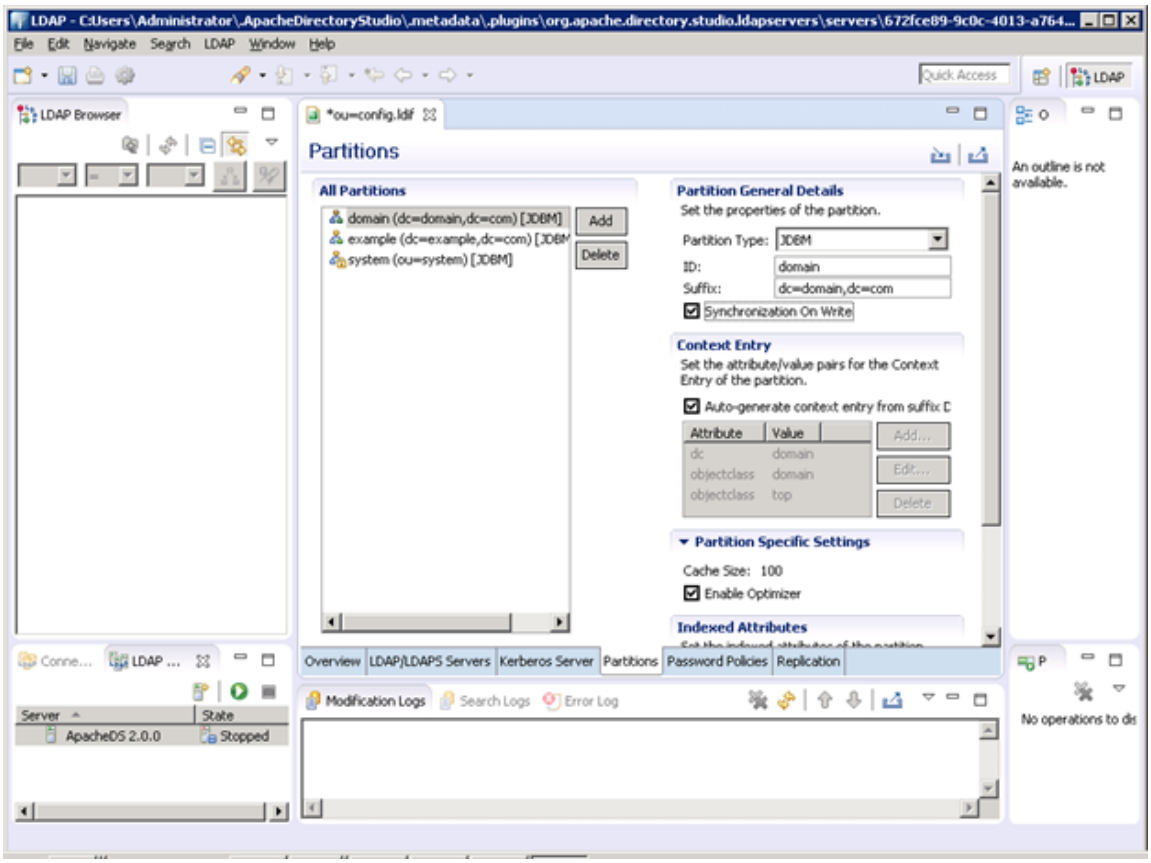
1. On Apache Directory Studio, in the Servers view, double-click the server or press **F3**.



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:

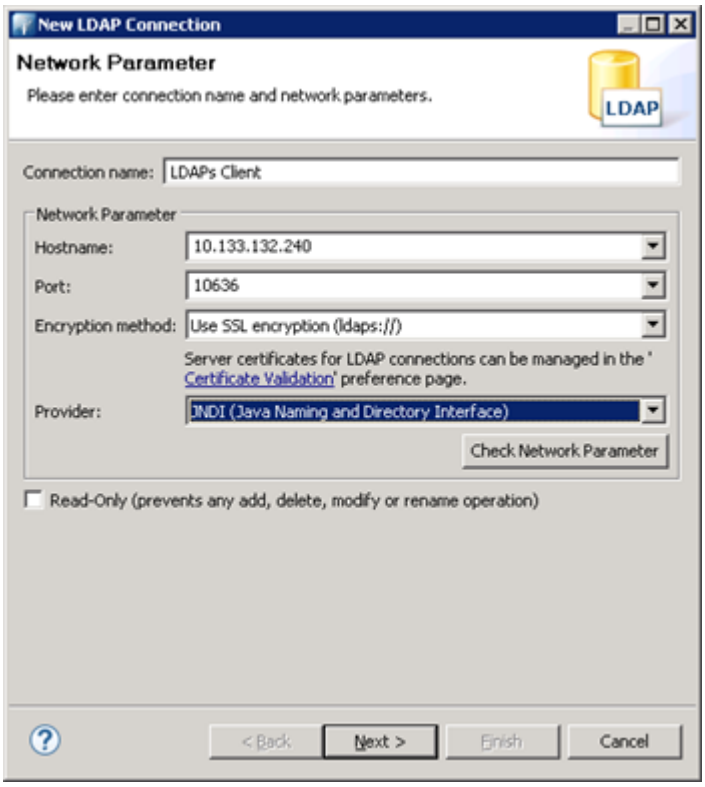


5. Press **Ctrl+s** to save the configuration.

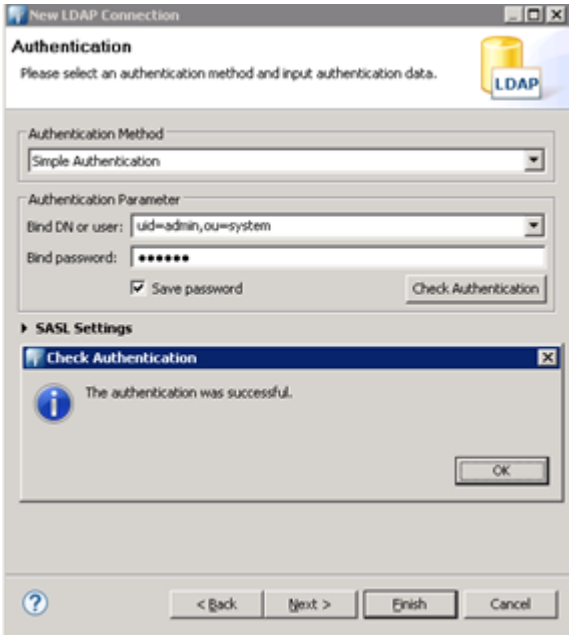
Creating a new LDAP Client

Procedure

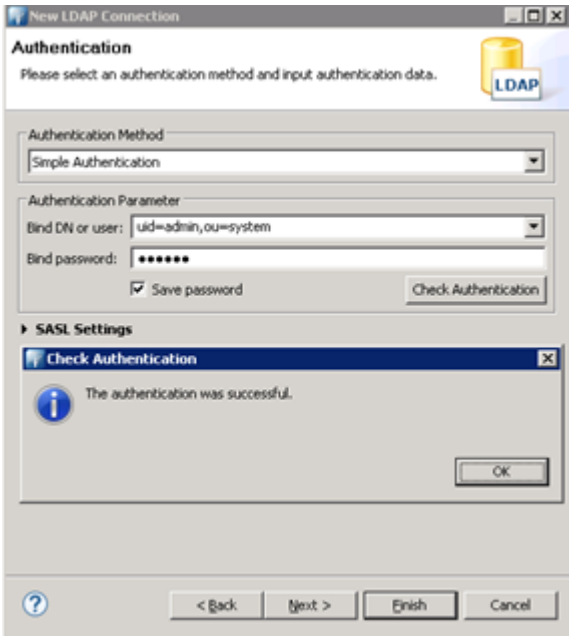
1. On Apache Directory Studio, in the LDAP menu, click **New Connection** and enter the required information.



2. Add the CA certificate and click **Next**.



3. Enter the following information, and click **Check Authentication**.

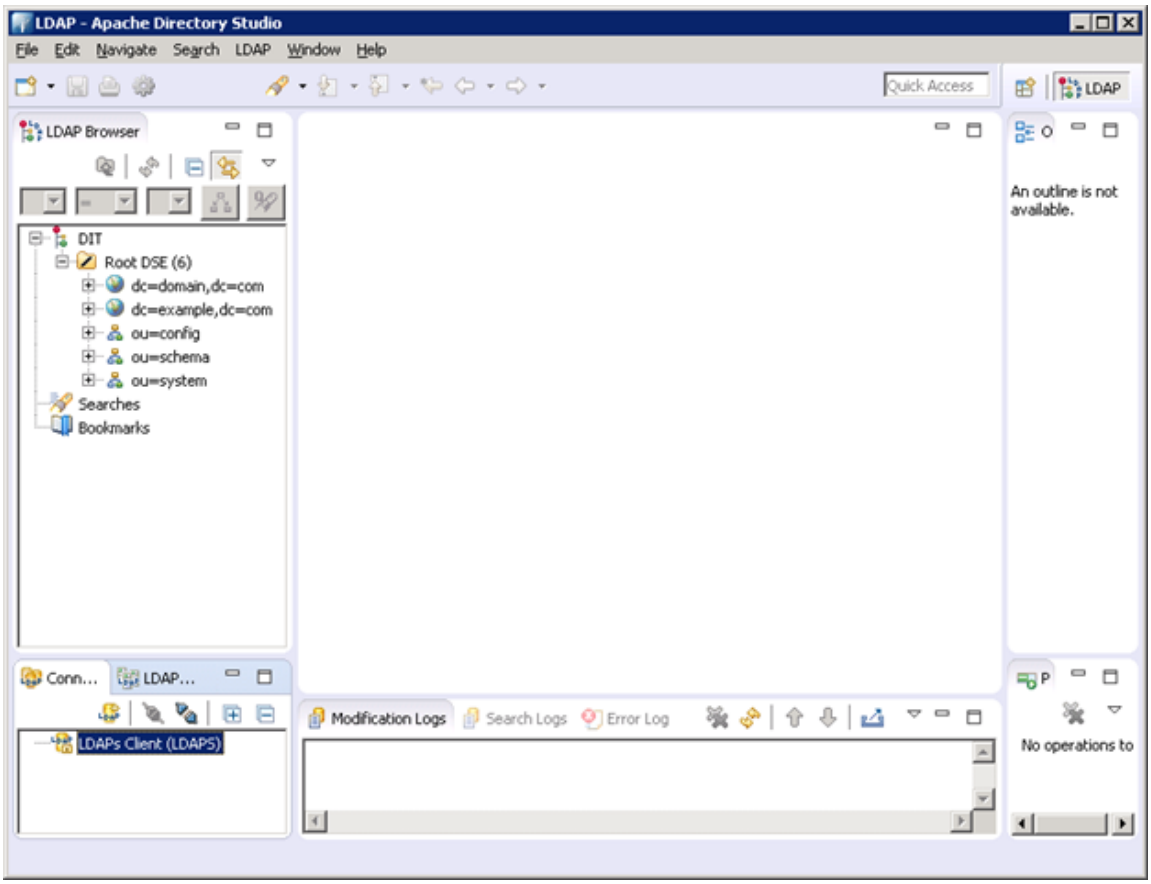


4. Click **Finish**.

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:

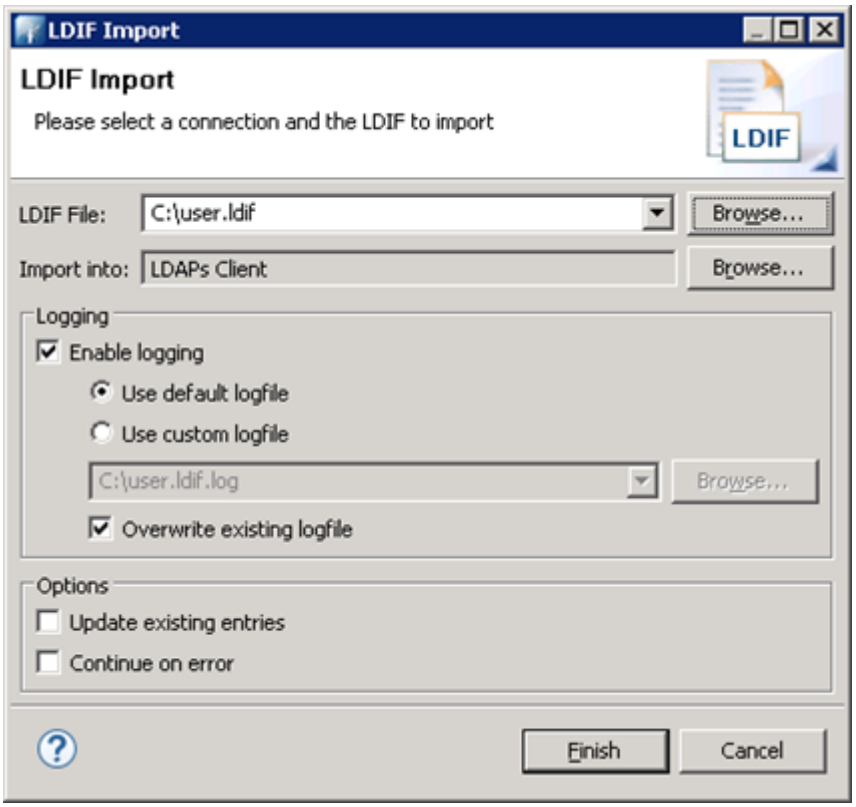
```
dn: ou=people,dc=domain,dc=com
objectClass: top
objectClass: organizationalUnit
ou: people



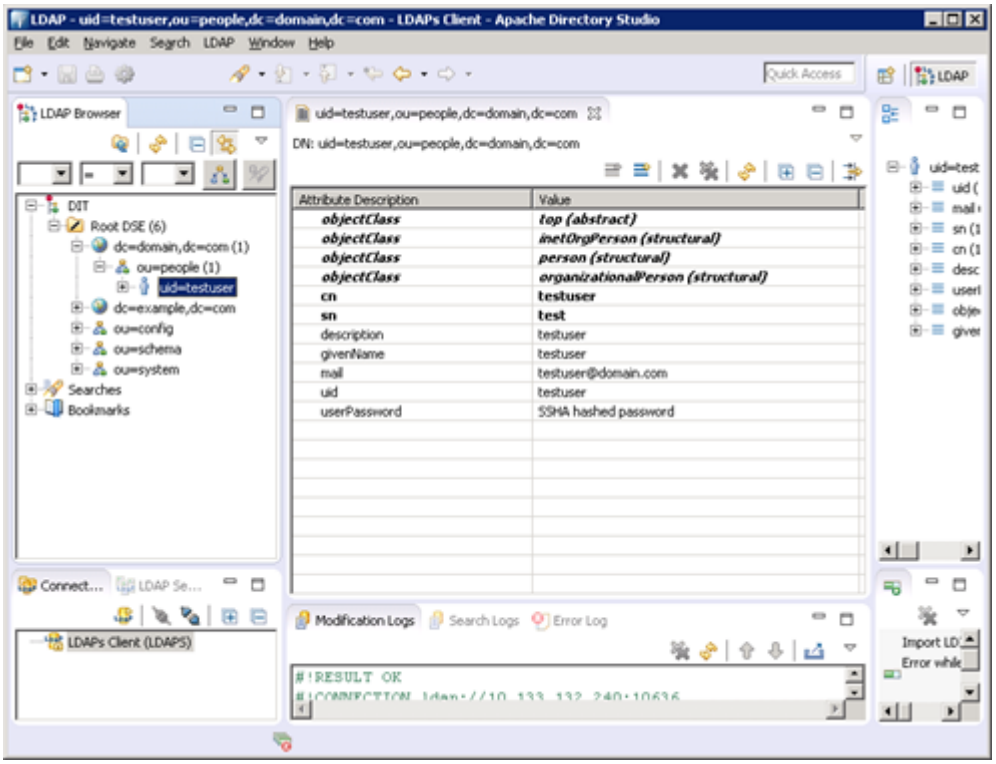
dn: uid=testuser,ou=people,dc=domain,dc=com
objectClass: top
objectClass: inetOrgPerson
objectClass: person
objectClass: organizationalPerson
cn: testuser
description: testuser
givenName: testuser
mail: testuser@domain.com
sn: test
uid: testuser
userPassword: 123456
```

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.

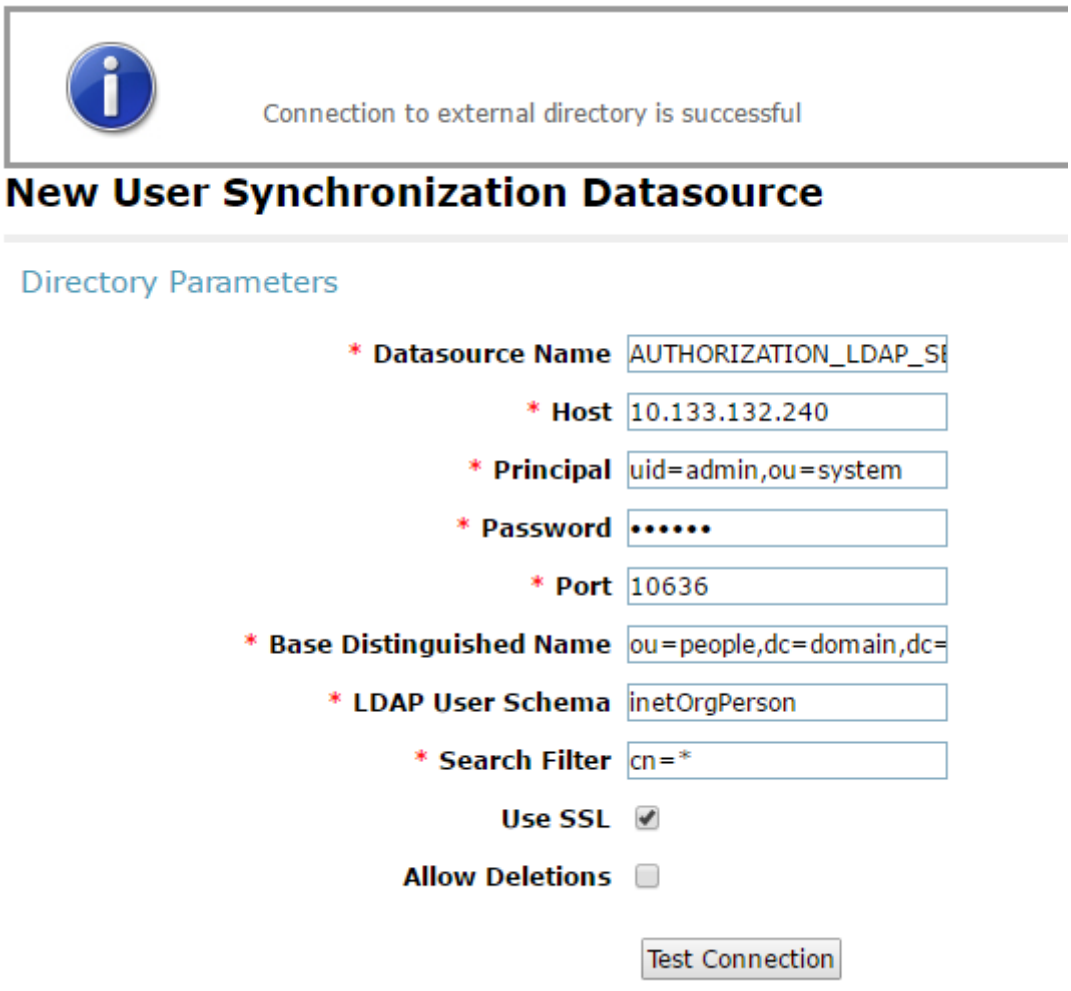


System Manager directory synchronization

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
```

Performing directory synchronization

Procedure

1. In 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.

Active Directory Configuration

This section provides example configuration procedures for Active Directory. This section is purely for reference.

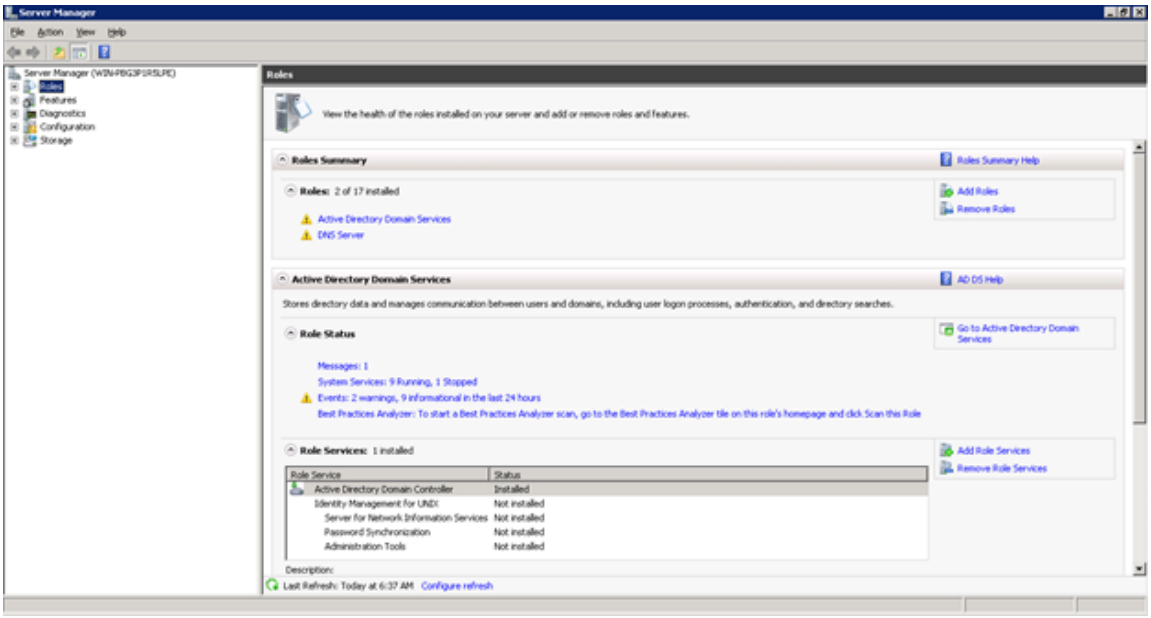
Enabling SSL on Windows Server 2008

Installing and configuring Active Directory

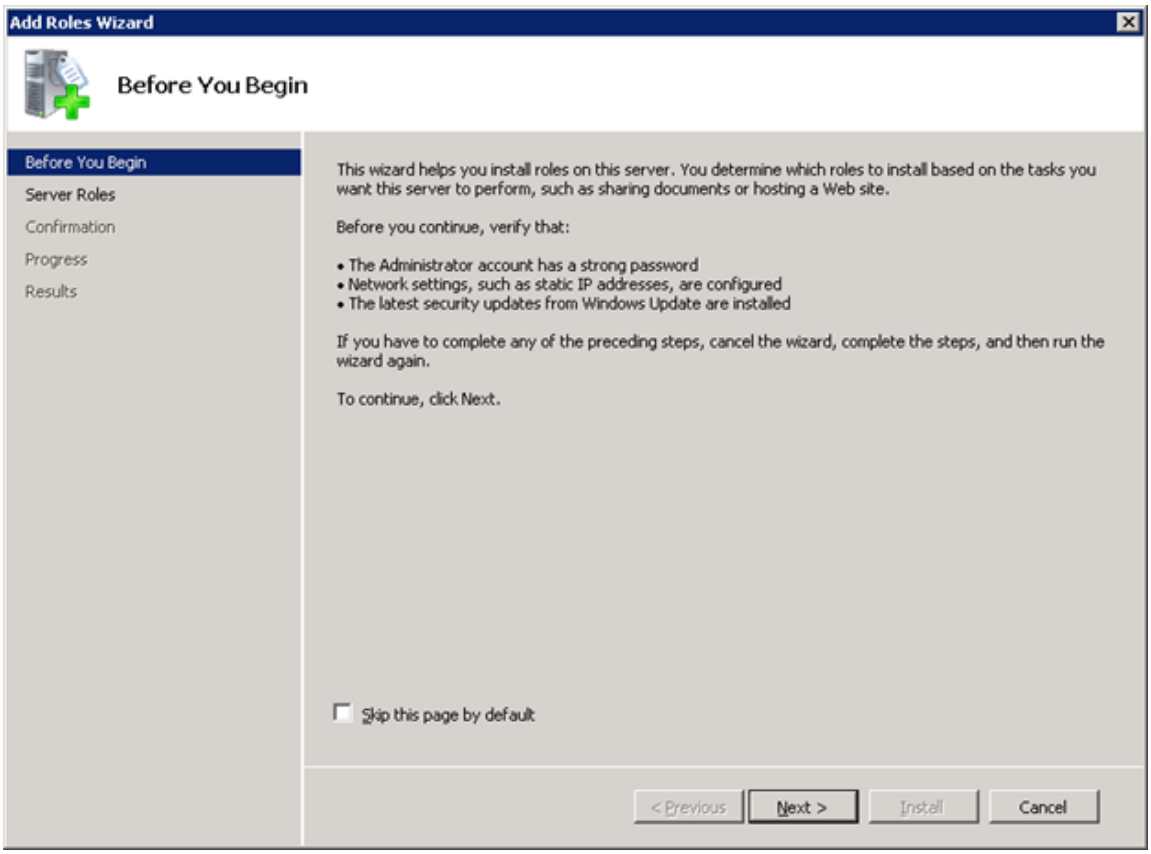
Procedure

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.

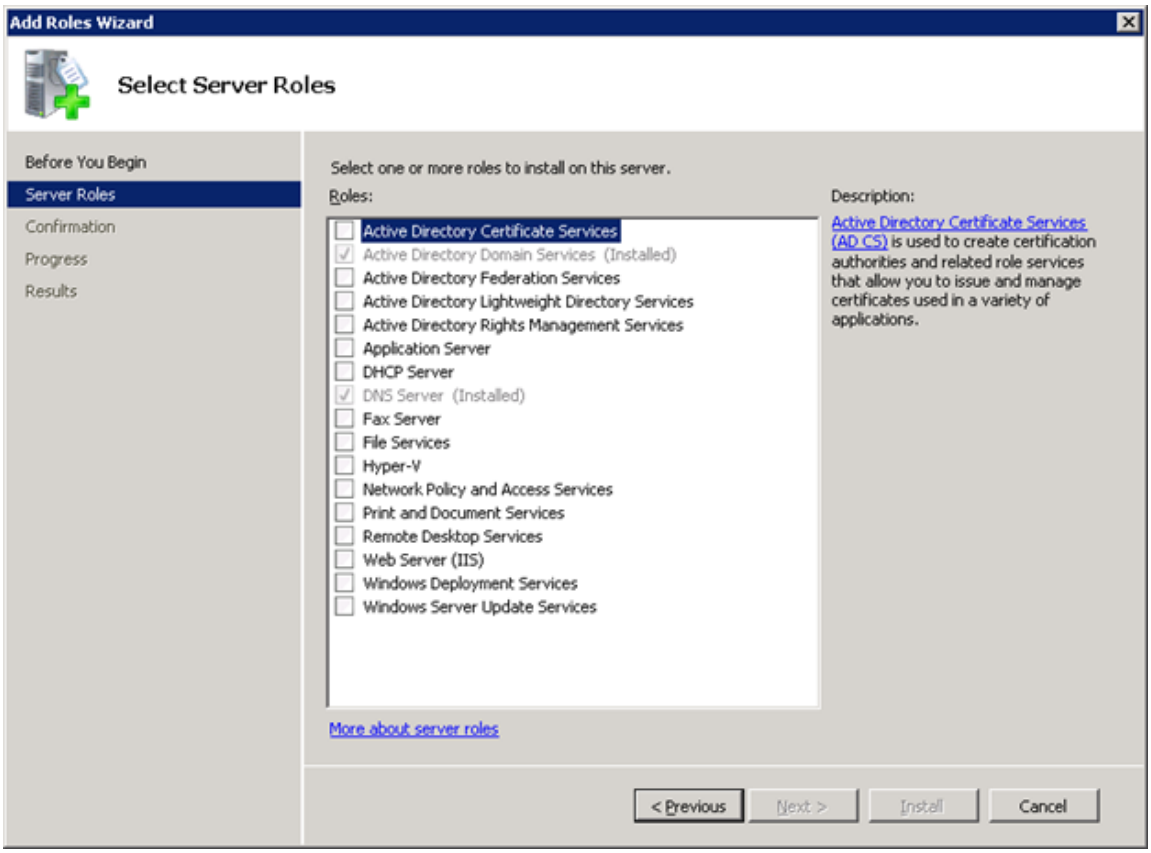




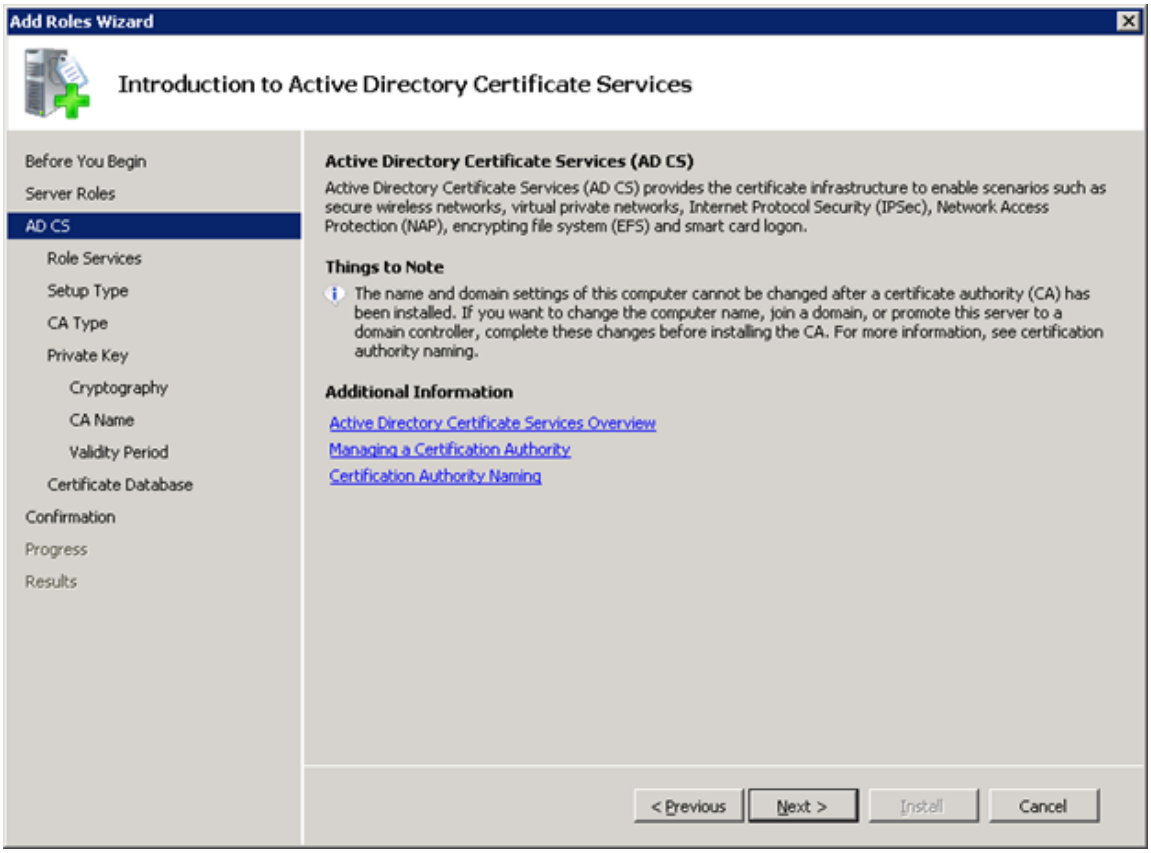
3. Click **Add Roles** in the **Roles Summary** section.



4. Click **Next** to proceed further to install **Active Directory Certificate Services**.

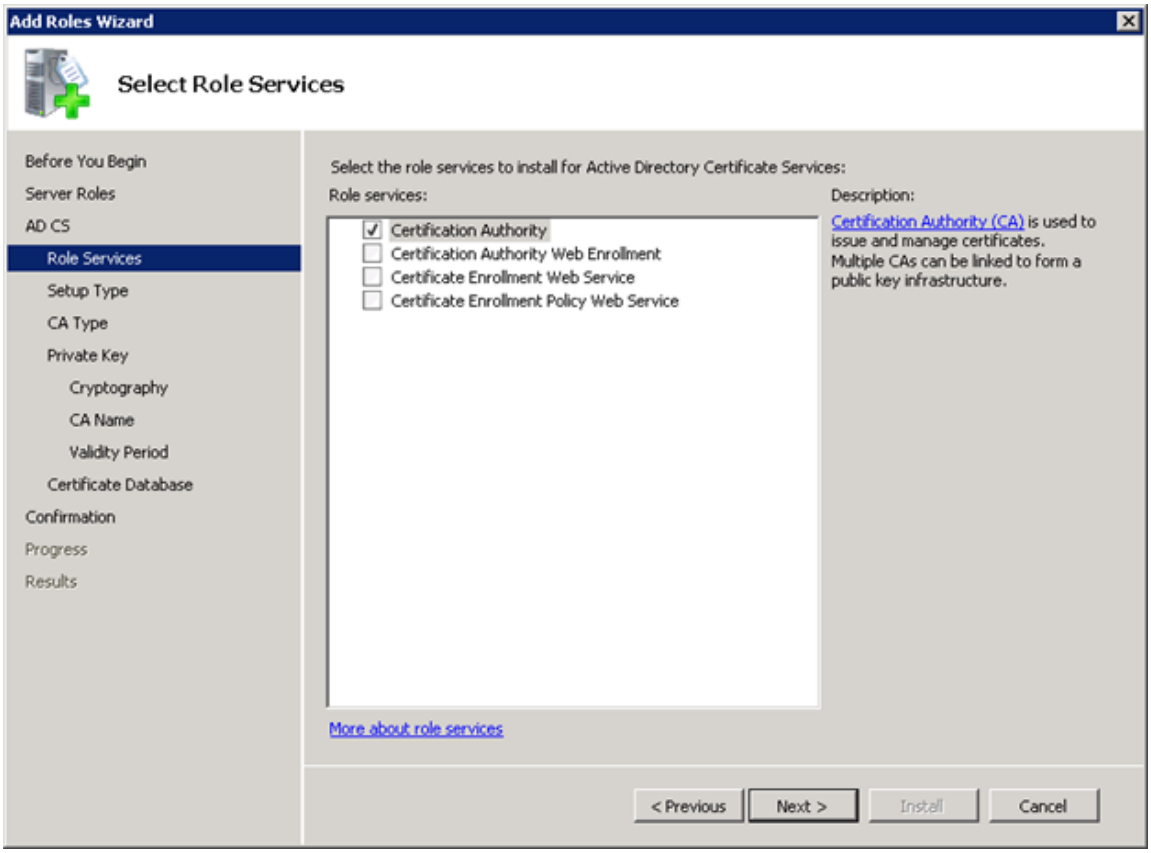


5. Click the **Active Directory Certificate Services** check box.
6. Click **Next**.



This window provides the introduction to Active Directory Certificate Services.

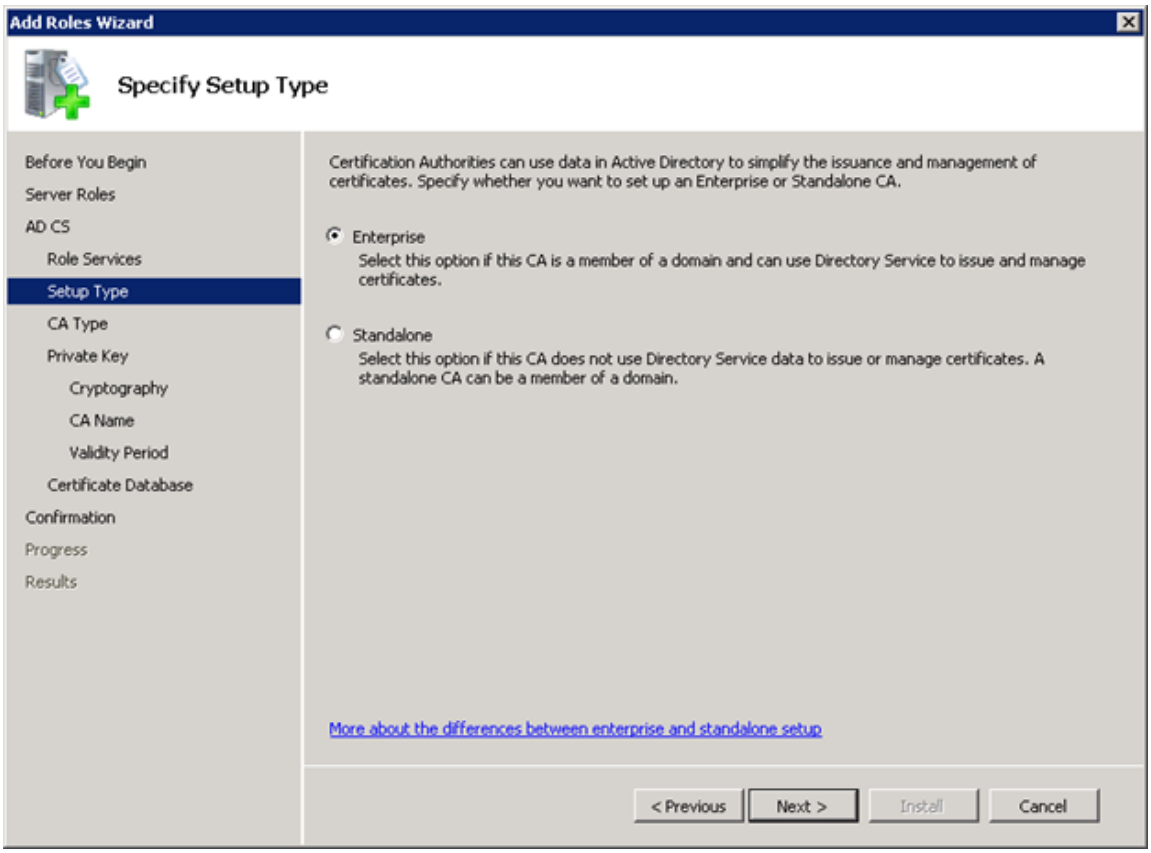
7. Click **Next**.



By default the first check box will be enabled.

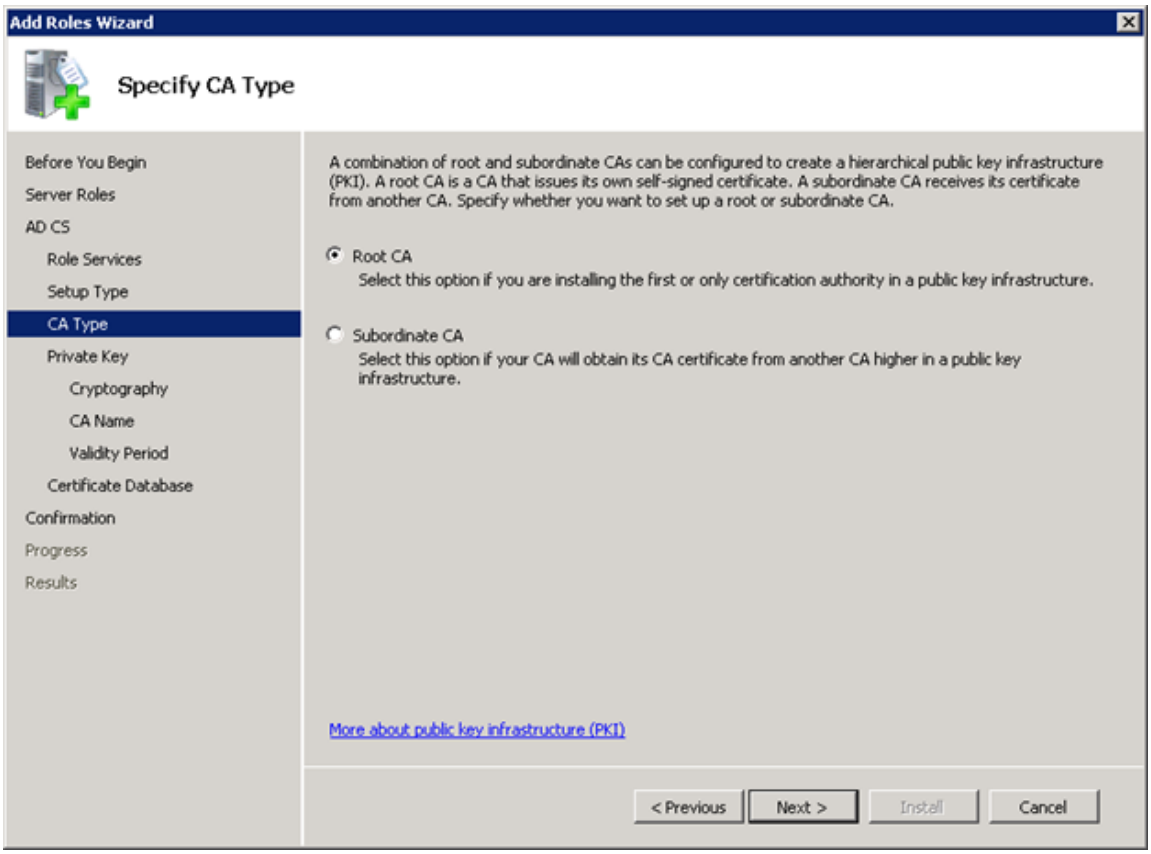
8. Click **Next**.

This window specifies set up type for the role installation.



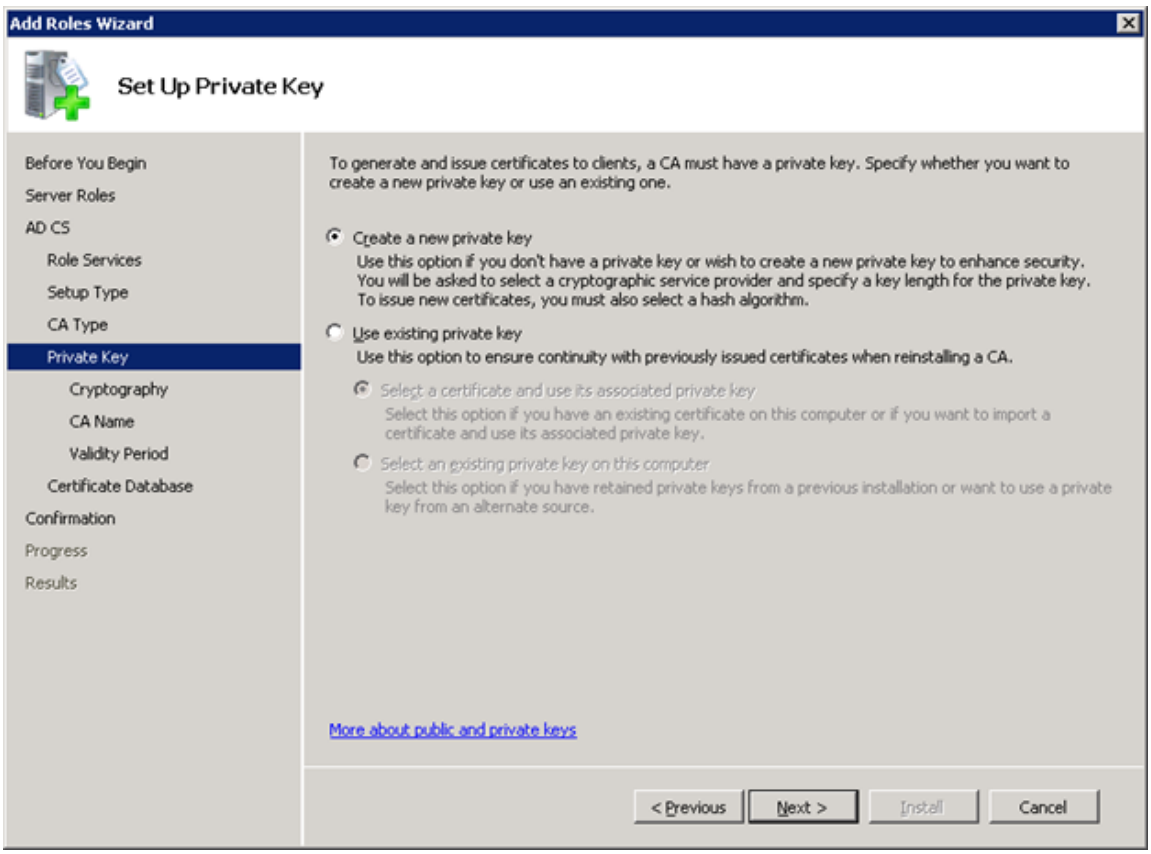
9. Click **Next**.

   The next window focuses on CA type to create hierarchical public key infrastructure.

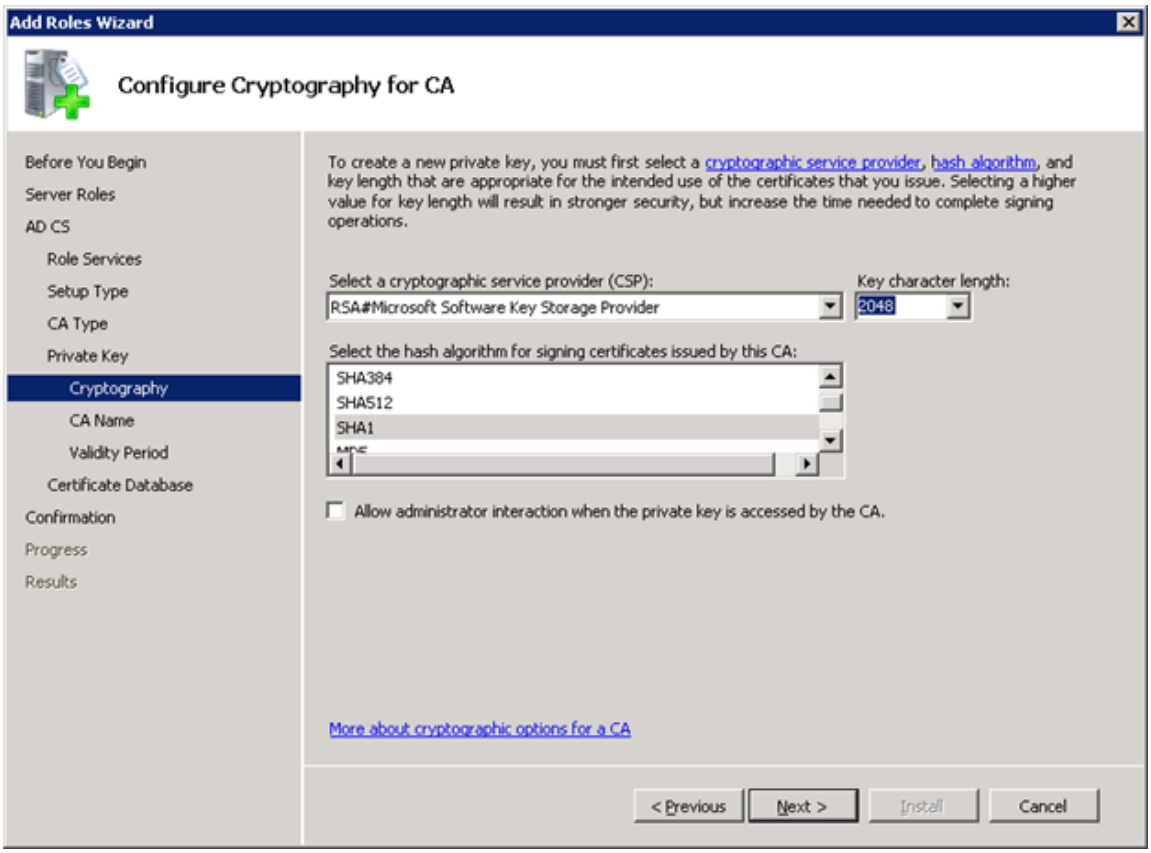


10. Click **Next**.

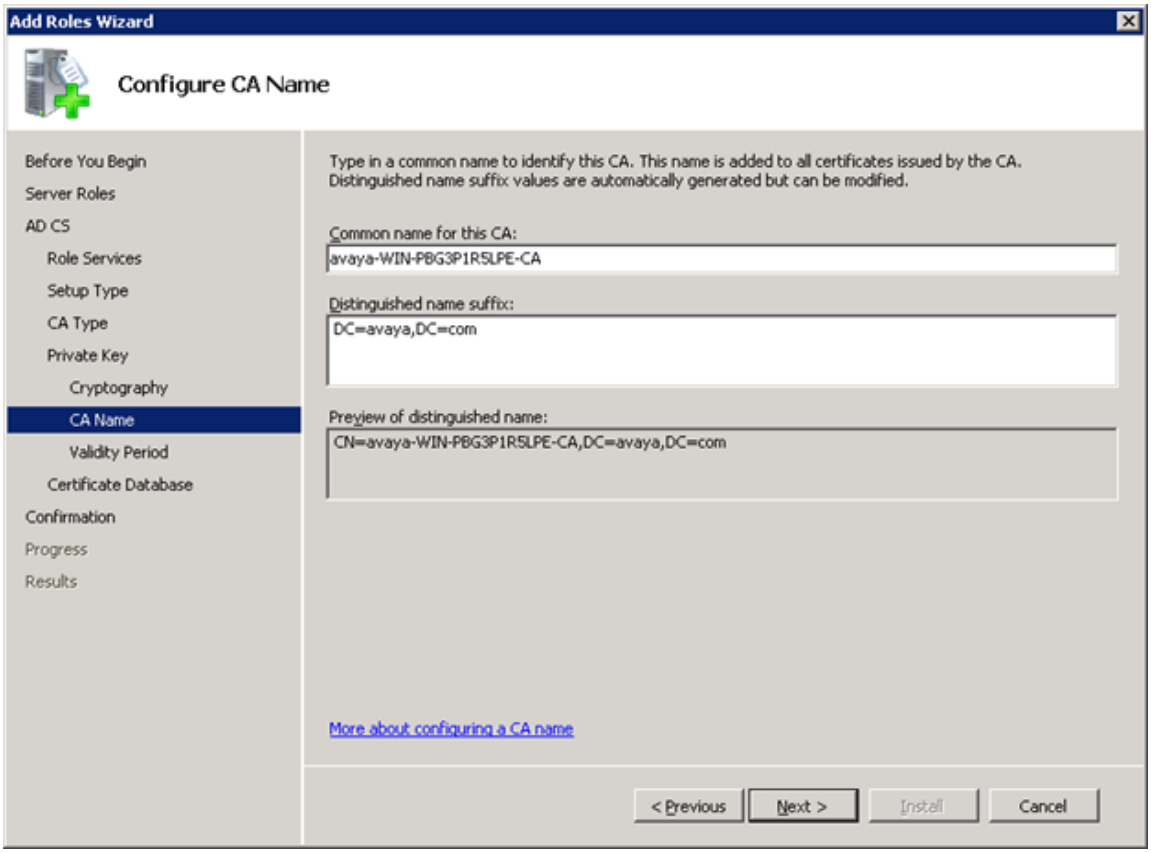
    This window focuses on Private Key generation and issues certificate to clients.



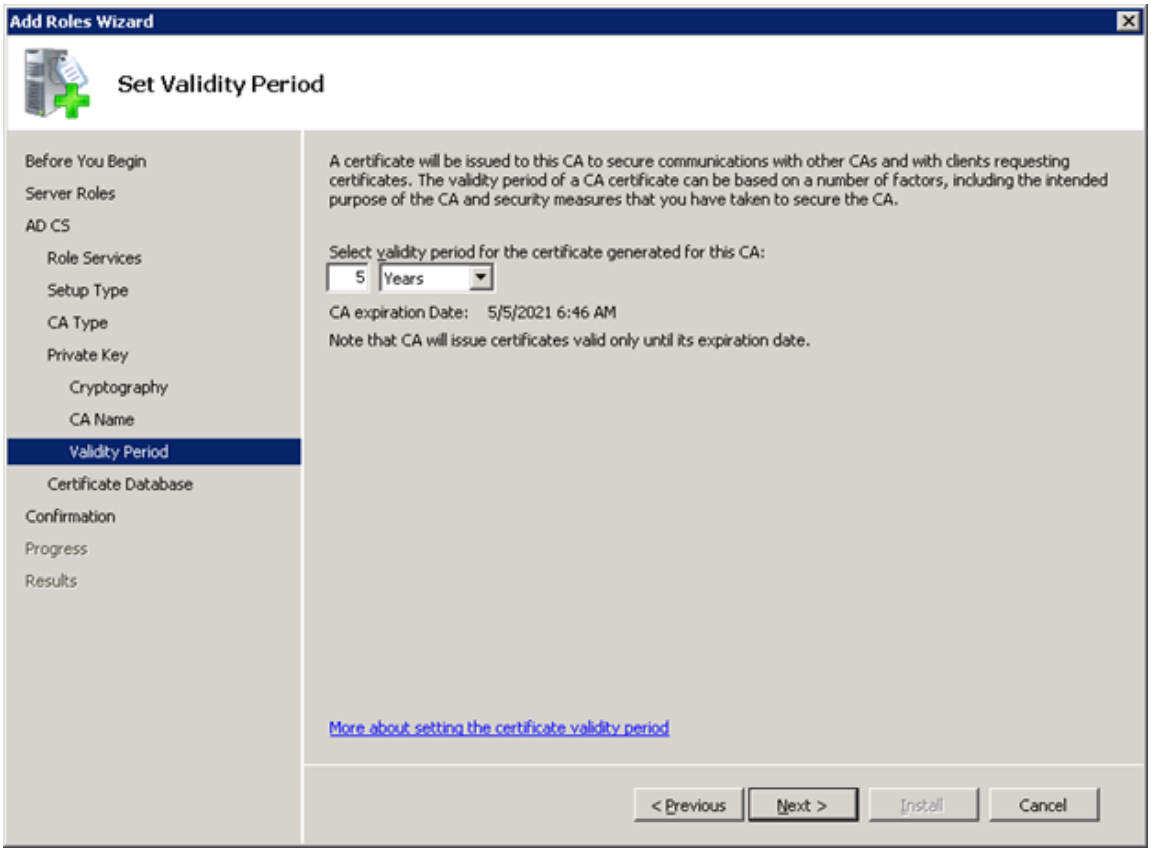
11. Click **Next**.



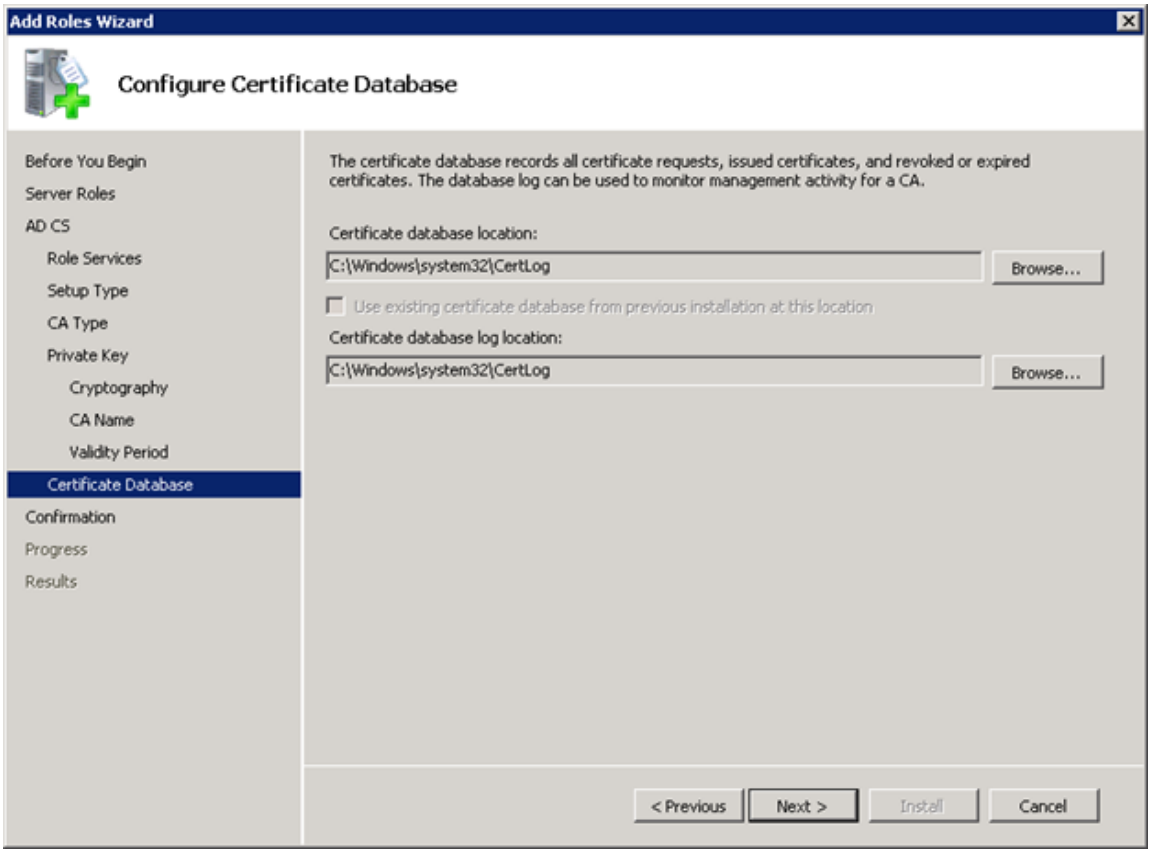
12. Click **Next**.
13. Configure the CA name and click **Next**.



14. Set the validity of the CA certificate, and click **Next**.

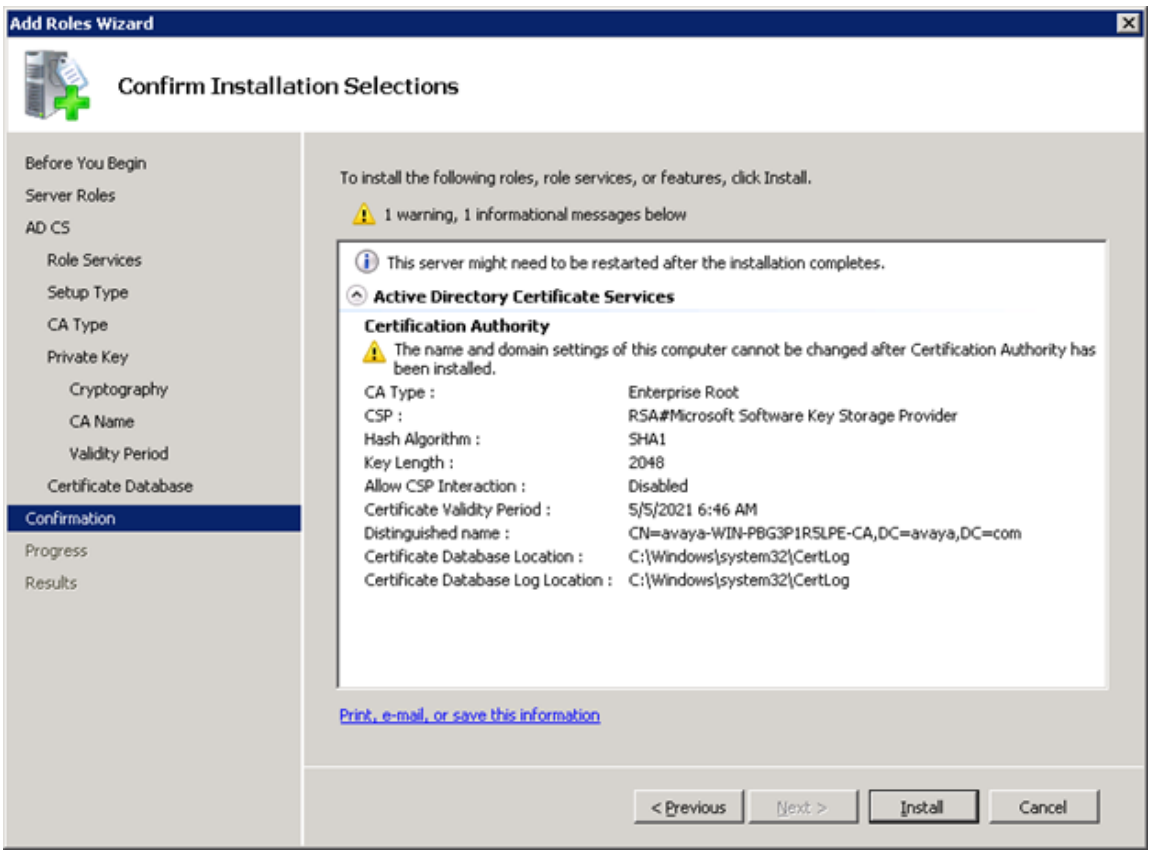


15. Configure the Certificate database.

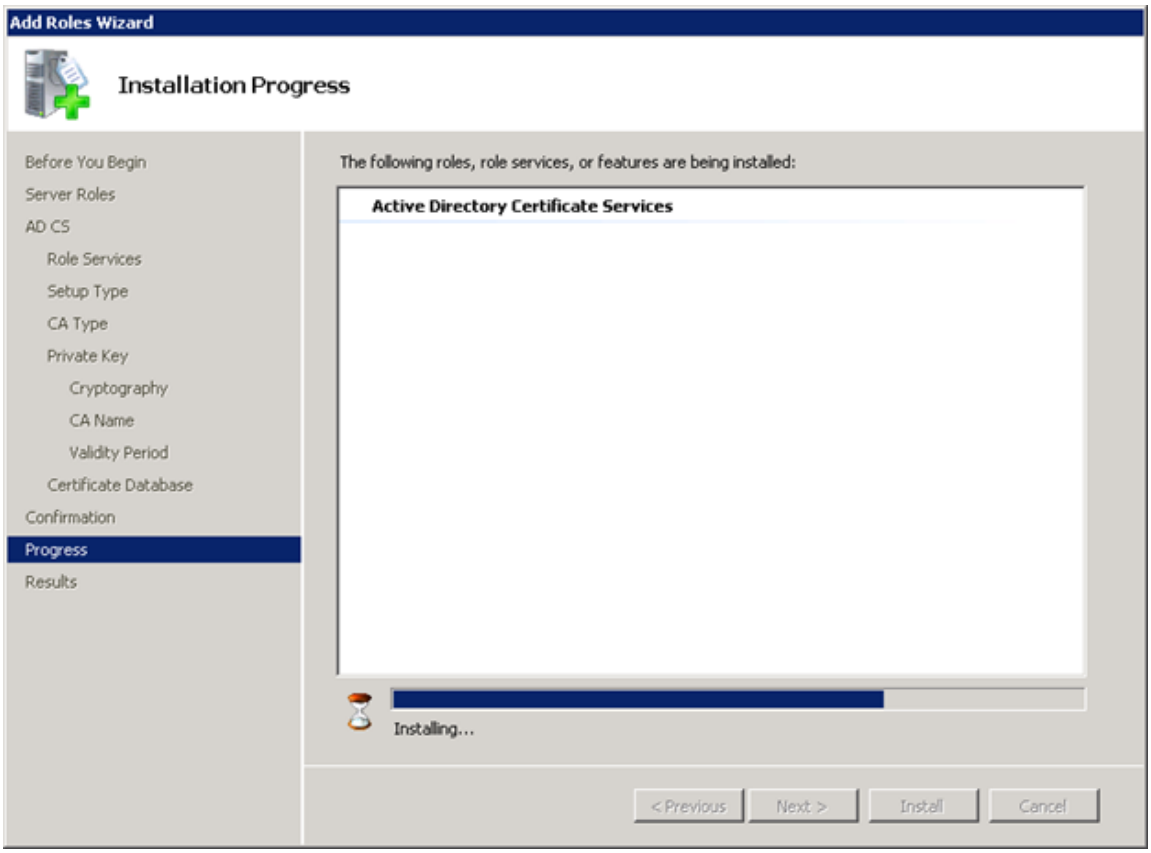


16. Click **Next**.

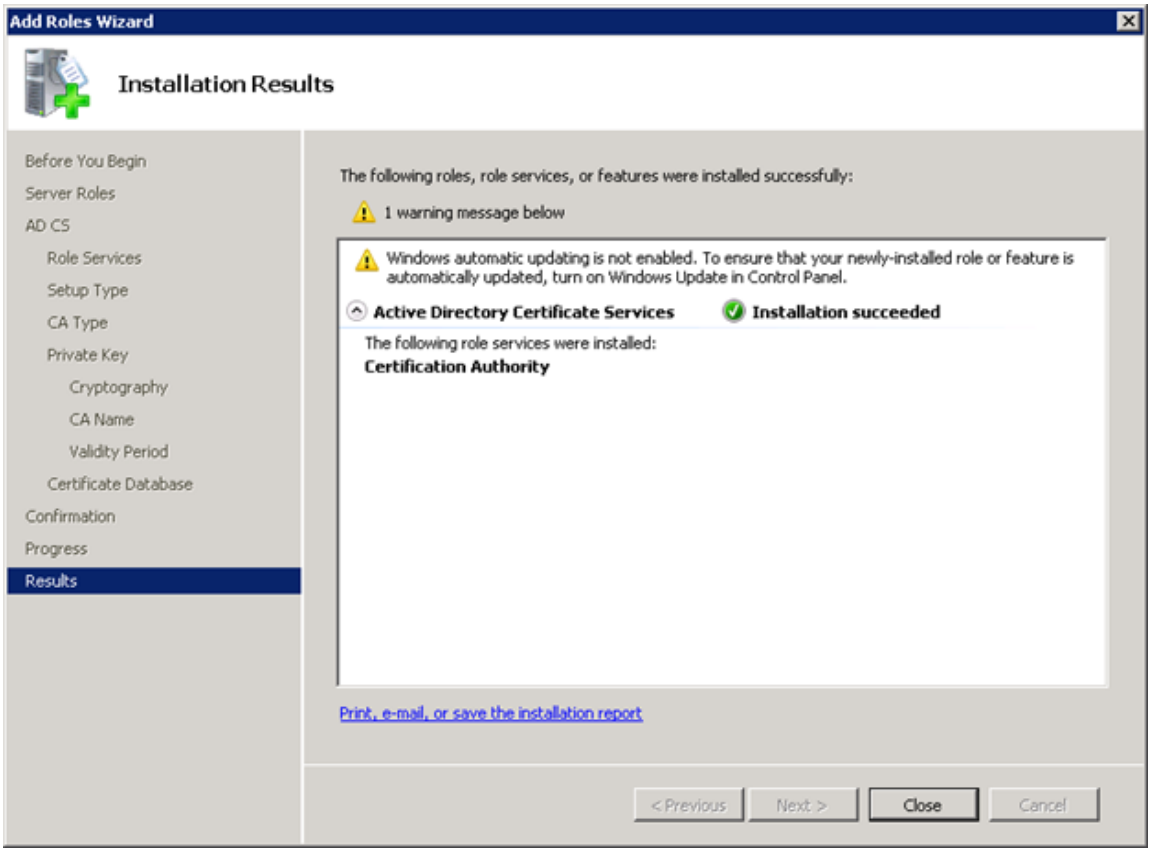
    This window displays the complete summary to begin the installation.



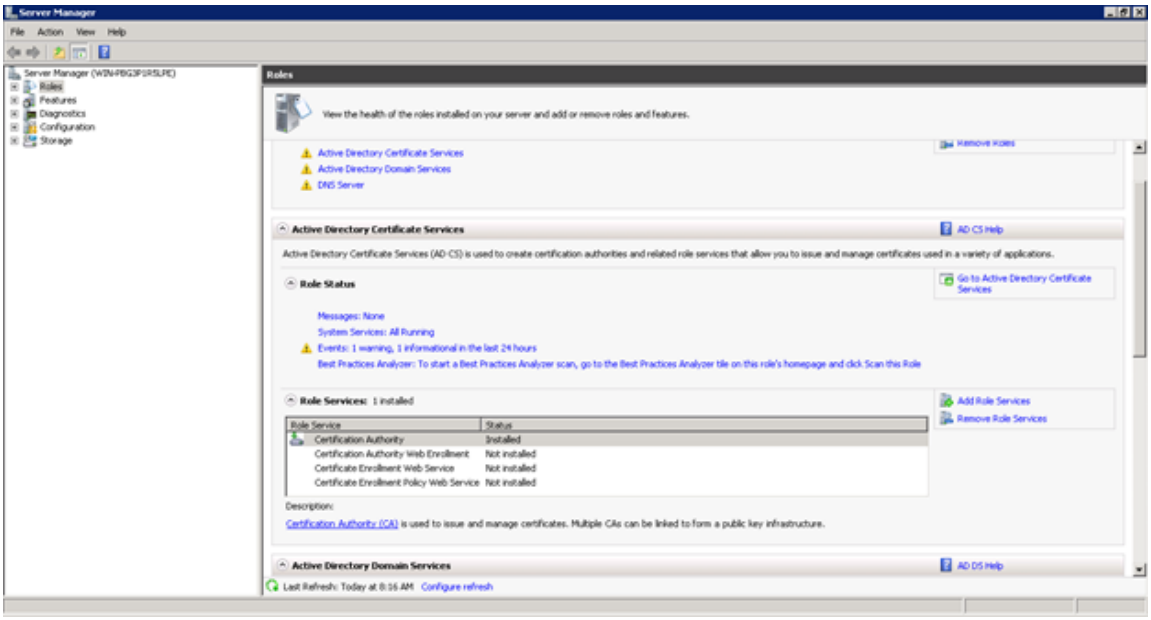
17. Click **Install**.



After the installation is completed, the following window is displayed.

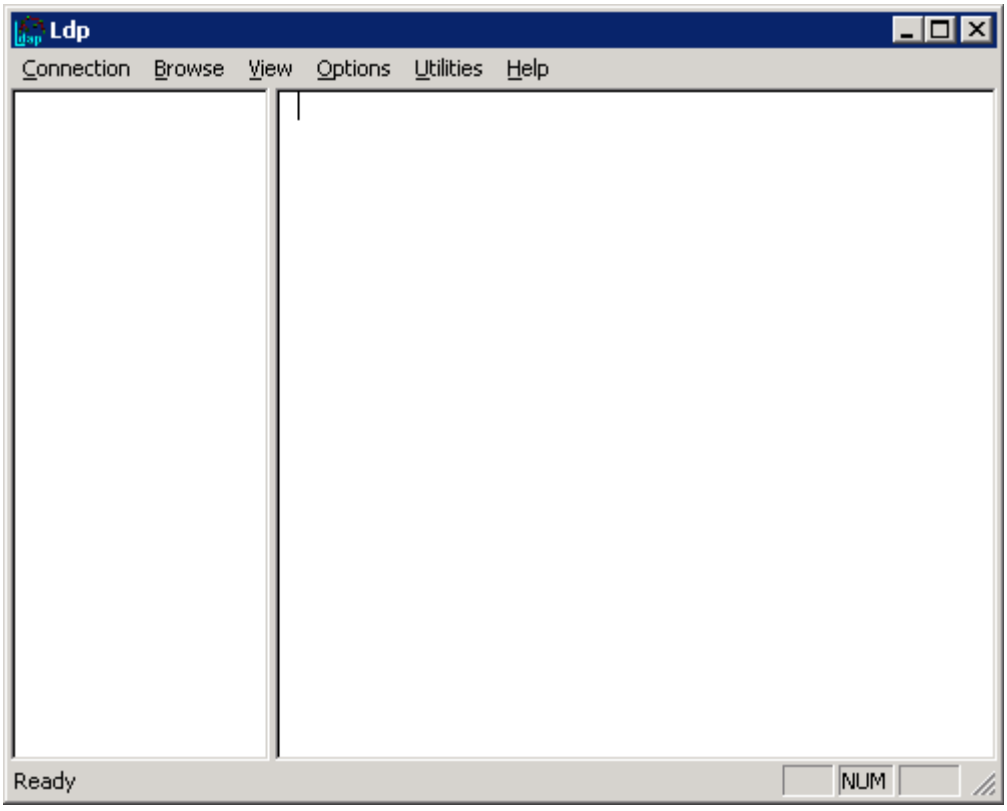


18. In the Server Manager window, you can see that the Certificate service has been installed successfully.

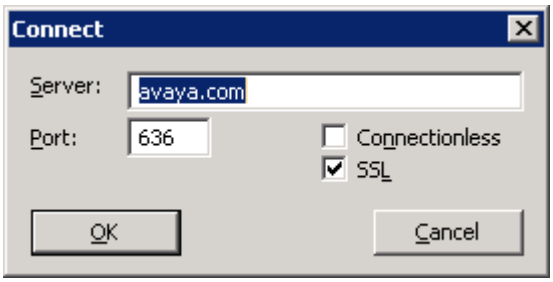


In the Role Services section, you can see the status of the service being shown as installed. After installation it is recommended to restart the Windows Server machine.

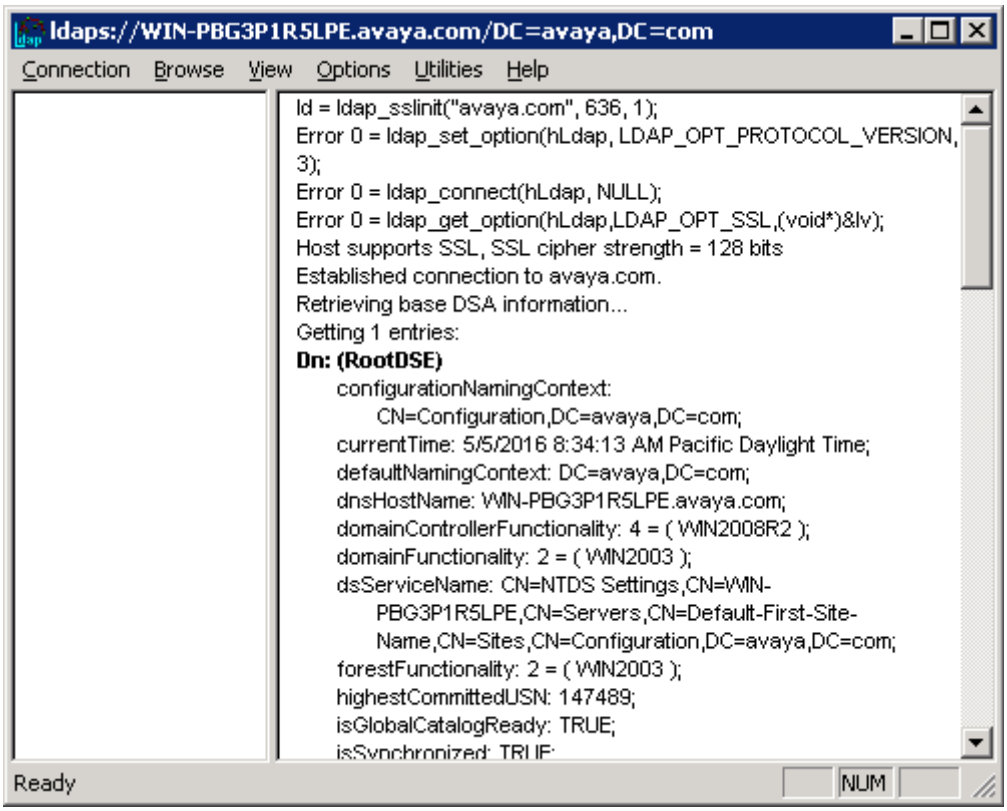
19. To check whether SSL is being enabled on Active directory, type `ldp.exe` in search programs and files.



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.



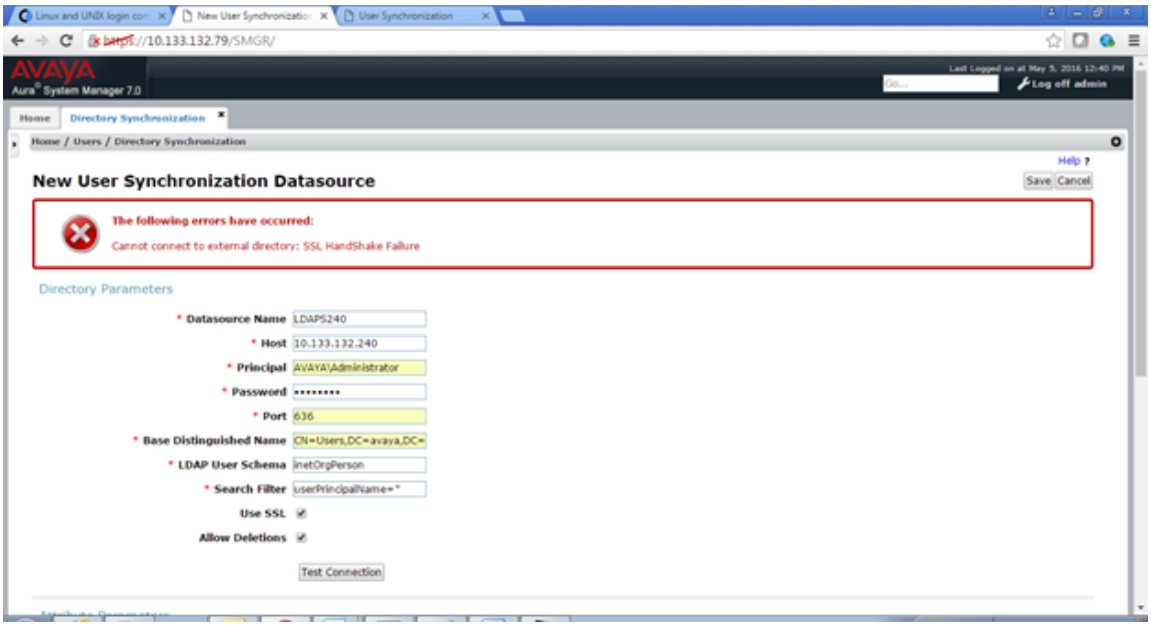
Active Directory now supports SSL.



Performing directory synchronization

Procedure

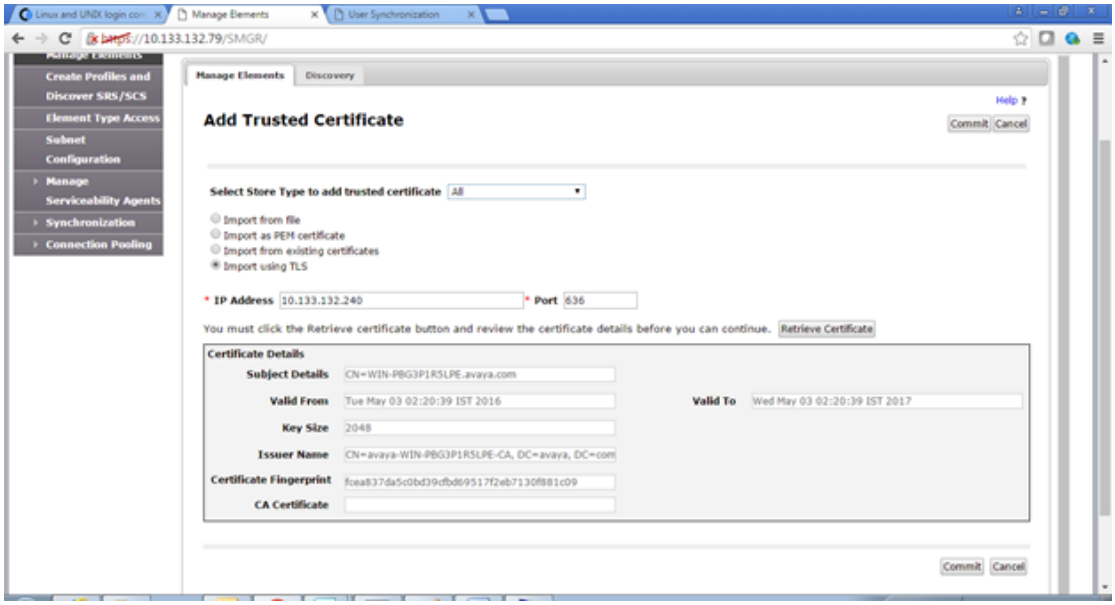
1. In System Manager, click **Users › Directory Synchronization**.
2. Add a new data source and enter the following LDAP server details, and click **Test Connection**.
   - **DS Name**
   - **Host**
   - **Principal**
   - **Port**
   - **Base DN**
   - **LDAP User Schema**
   - **Search Filter**
   - **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.

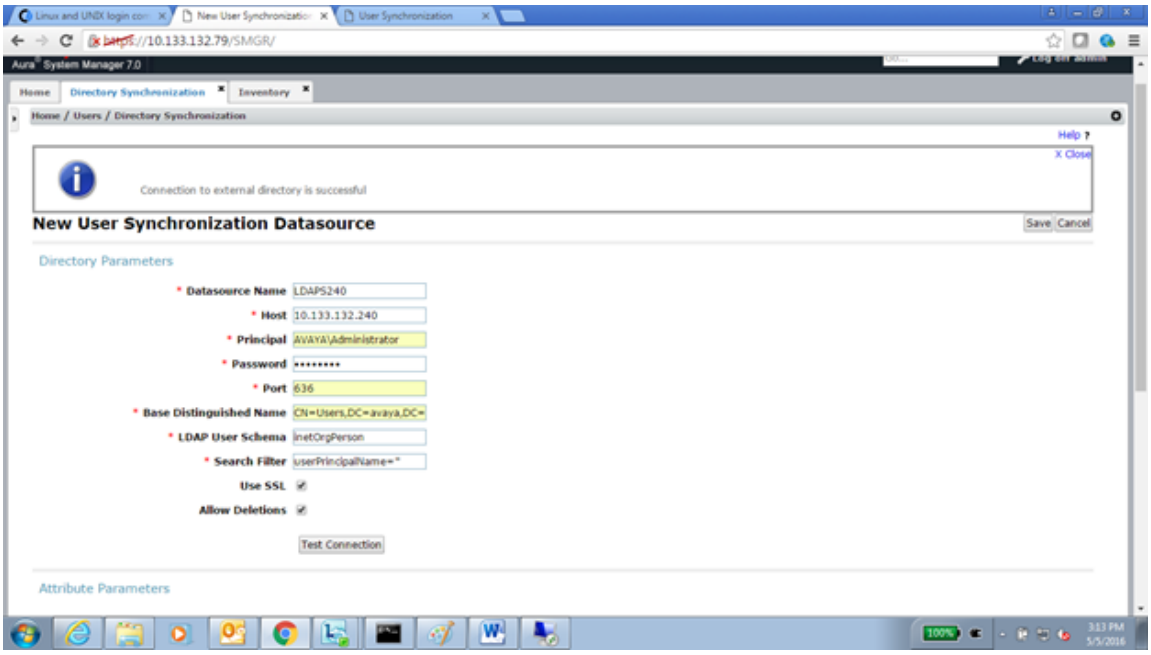
3. To resolve we need to import the Certificate:
   a. Navigate to **Services › Inventory › Manage Elements**.
   b. Select the System Manager instance and click **More Actions › Configured Trusted Certificates**.
   c. Click **Add**.
   d. Select the **Import using TLS** field.



   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.



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`.

Open LDAP configuration

This section provides example configuration procedures for OpenLDAP. This section is purely for reference.

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.

a. 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}xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

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
```

Performing System Manager directory synchronization

Procedure

1. In 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**.

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® platform Authorization Service must be installed.
- The Service Provider metadata of the Avaya Breeze® platform 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® platformnode.
8. On the Specify Display Name screen, enter a name.
   a. 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. In 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 is 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 integrated to use the Avaya Breeze® platform Authorization Code Grant flow.
- Use the Authorization Sample snap-ins provided in the Avaya Breeze® platform 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.

Configuration of Azure Active Directory as a SAML provider

The topics in this section describe how to enable SAML authentication with Microsoft Azure Active Directory.

Use these steps to:

- Set up an application on Microsoft Azure Active Directory.
- Integrate Microsoft Azure Active Directory (acting as a SAML identity provider) with the Avaya Breeze® platform Authorization Service (acting as a SAML service provider).

Prerequisites

- You must have a Microsoft Azure account.
- Avaya Breeze® platform Authorization Service must be installed.

Adding a new Microsoft Azure application

About this task

Set up a new application on Microsoft Azure Active Directory for integration with the Avaya Breeze® platform Authorization Service.

Before you begin

- You must have a Microsoft Azure account.
- Avaya Breeze® platform Authorization Service must be installed.

Procedure

1. Log in to Microsoft Azure.
2. Search for "Azure Active Directory".
3. Under Services, click **Azure Active Directory**.
4. Under Manage, click **Enterprise applications**.
5. Click **+ New application**.
6. Click **Create your own application**.
7. Enter your application name in **What's the name of your app?**.
8. Select **Integrate any other application you don't find in the gallery (Non-gallery)** and click **Create**.
9. Click **Assign users and groups**.
10. Click **+ Add user/group**.
11. Under Users, click **None Select**.
12. Search for the user to assign and click **Select**.
13. Click **Assign** to assign the selected user.
14. Next to Home, click the name of the Microsoft Azure application that you created.

    The Add New Application page .
15. Under Getting Started, click **Set up single sign on**.
16. Click **SAML**.
17. To download the service provider metadata for the node, use the node URL.

    The node URL is in the following format:

    ```
    https://<Asset_FQDN>:9443/services/AuthorizationService/spmetadata
    ```
18. Click **Updated metadata file** with upload the node `spmetadata` file.
19. Under SAML Signing Certificate, next to Federation Metadata XML, click **Download** and save the XML metadata.
20. Modify the downloaded federation metadata XML file.
    a. Keep `EntityDescriptor` and `IDPSSODescriptor` and remove the other elements (`Signature`, `RoleDescriptor`).
    b. Add the following between `SingleLogoutService` and `SingleSignOnService`:

```
<NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
```

21. Repeat steps 2 through 20 to add Microsoft Azure applications for other nodes.
22. Next to Home, click the name of a Microsoft Azure application that you created, and click **All applications** to list all the Microsoft Azure active directory applications you created.

Configuring Microsoft Azure SAML authorization in Avaya Breeze® platform

Procedure

1. On System Manager, click **Elements › Avaya Breeze® › Configuration › Authorization › Authentication Mechanism** and select the **Authorization Mechanism type**.
2. Click **Change Authentication Mechanism**.
3. In **Authentication Mechanism**, select **SAML**.
4. Under Change Authentication Method Type, set the following values:
   - **Select Authentication Mechanism**: SAML
   - **Should SAML requests be signed**: (Leave it as is)
   - **Attribute Used as UserID**: Can be one of the following, based on your Microsoft Azure account:

     ```
     http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
     http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
     http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
     http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn
     ```

   - **Authentication Context**: Password Protected Transport
   - **Authentication Context Comparison Type**: exact
   - **Identity Provider Metadata File**: `breeze1.xml` or `breeze2.xml`

Configuring Microsoft Azure Active Directory on Avaya Breeze® platform service providers

Procedure

1. On System Manager, click **Elements › Avaya Breeze® › Configuration › Attributes › Service Globals › Authorization Service**.
2. Under Authorization Attributes, next to Allow Public Clients, select **Override Default**.
3. Use POSTMAN to save the `breeze1.xml` file to the Avaya Breeze® platform node.
   a. The URL to use looks like the following:

      ```
      https://<Asset_FQDN>:9443/services/AuthorizationService/idpmetadata
      ```

   b. The POST body should contain the contents of the `breeze1.xml` file.
4. Repeat step 3 for the other Avaya Breeze® platform node.

Restarting the SAML profile in Avaya Breeze® platform

Procedure

1. On System Manager, click **Elements › Avaya Breeze® › Configuration › Attributes › Service Globals › Authorization Service**.
2. Under **SAML Attributes**, select **Undeploy** for the SAML Profile and click **Commit**.

   Wait about one minute after undeploying the profile.
3. Under **SAML Attributes**, select **Deploy** for the SAML Profile and click **Commit**.

Configuring Azure authorization service after Breeze upgrade

Procedure

1. Install only the latest version of Authorization Service.
   a. Uninstall all the earlier versions of Authorization Service.
   b. Install the latest version of Authorization Service.

      Only one version of Authorization Service can be installed at a time.
2. Update or install identity certificate.
   a. On System Manager, click **Elements › Avaya Breeze® › Cluster Administration**.
   b. Select the cluster and click **Certificate Management › Update /Install Identity certificate (Authorization Service)**.

      Because the metadata is changed, you must exchange it again to update using the latest metadata. Service provider metadata must be generated for all nodes in a cluster separately.
   c. Delete all the relying agents created earlier for the respective Avaya Breeze® platform nodes.
   d. Repeat steps 1 to 4 in Adding a new Microsoft Azure application on page 220.
   e. Click your application.
   f. To configure the new service provider metadata for the identity provider, repeat steps 15 to 20 in Adding a new Microsoft Azure application on page 220.

Configuration of Okta as a SAML provider

The topics in this section describe how to enable SAML authentication with Okta active directory.

Use these steps to:

- Set up an application on Okta active directory.
- Integrate the Okta active directory (acting as a SAML identity provider) with the Avaya Breeze® platform Authorization Service (acting as a SAML service provider).

Prerequisites

- You must have an Okta account at https://developer.okta.com/signup/.

- Avaya Breeze® platform Authorization Service version 3.6.0.1 or later must be installed.

Adding a new Okta application for each Avaya Breeze® platform node

About this task

Create an Okta application for every Avaya Breeze® platform node in your cluster. Repeat this task for every node.

Before you begin

- You must have an Okta account at https://developer.okta.com/signup/.
- Avaya Breeze® platform Authorization Service version 3.6.0.1 or later must be installed.

Procedure

1. Log in to Okta.
2. Create an application in Okta for the Breeze node.
   a. On the Okta menu, click **Applications › Applications**, then click **Create App Integration**.
   b. On the Create a new app integration page, select **SAML 2.0** and click **Next**.
   c. On the Create SAML Integration page, in **App name** enter the Avaya Breeze® platform SIP Entity FQDN or IP and click **Next**.
3. On the Create SAML Integration page, do the following in the General section.
   a. Download the SP metadata XML file from the Avaya Breeze® platform node using the following URL.

      ```
      https://<my.breeze.sip.entity.fqdn.or.ip>:9443/services/AuthorizationService/
      spmetadata
      ```

   b. Open the downloaded metadata XML file and record the values for:
      - `EntityDescriptor entityID`
      - `AssertionConsumerService Location`
4. On the Create SAML Integration page, enter the following in the Configure section.
   a. In **Single Sign on URL**, enter the `AssertionConsumerService Location` value.
   b. In `Audience URI (SP Entity ID)`, enter the `EntityDescriptor entityID` value.
   c. In **Name ID Format**, select **Transient**.
   d. In **Application username**, select **Email**.
5. Scroll down to the **Attribute Statements (optional)** section and enter the following.
   a. For **Name**, enter "email".
   b. For **Value**, enter "user.email".
6. Scroll down and click **Next**.
7. On the next Create SAML Integration page, select **I'm a software vendor. I'd like to integrate my app with Okta** and click **Finish**.

Assigning users to each Okta application

Procedure

1. On the Applications page, click **Assign Users to App**.
2. On the Assign Applications page:
   a. Select **Application & Label** to select all Okta applications (nodes).
   b. Select **Person & Username** to select all users.
   c. Click **Next**.
3. **(Optional)** To add test users, click **Directory › People** and click **Add Person**.

   To add new users to each application, repeat the previous steps.
4. On the Assign Applications page, click **Confirm Assignments**.

Downloading IdP metadata from each Okta application

About this task

Repeat these steps for every Avaya Breeze® platform node in your cluster.

Procedure

1. On the Okta menu, click **Applications › Applications**.
2. Click the **my.breeze.sip.entity.fqdn.or.ip** link.
3. On the my.breeze.sip.entity.fqdn.or.ip page, click the **Sign On** tab.
4. Right-click the **Identity Provider metadata** link and select **Save Link As**.

   Save the metadata to a file. For example: `idp-my.breeze.sip.entity.fqdn.or.ip.xml`.

Configuring SAML authentication on System Manager

Procedure

1. Log in to System Manager.
2. Click **Elements › Avaya Breeze® › Configuration › Authorization › Authentication Mechanism**.
3. Select the **Authorization Mechanism type** and click **Change Authentication Mechanism**.
4. Under Change Authentication Method Type, set the following values.
   - **Select Authentication Mechanism**: SAML
   - **Should SAML requests be signed**: (Leave it as is)
   - **Attribute Used as UserID**: `email`.
   - **Authentication Context**: Password Protected Transport
   - **Identity Provider Metadata File**: Click **Choose File** and select any Okta applications IdP metadata XML file that was downloaded.
5. Click **Save**.

Configuring Okta on Avaya Breeze® platform

About this task

Repeat this task for every Avaya Breeze® platform node in your cluster.

Procedure

1. Use POSTMAN to save the IdP metadata file (`idp-my.breeze.sip.entity.fqdn.or.ip.xml`) specific to each Avaya Breeze® platform node in your cluster.

   Use the following URL when posting the contents of the IdP metadata file to POSTMAN.

   ```
   https://<my.breeze.sip.entity.fqdn.or.ip>:9443/services/AuthorizationService/idpmetadata
   ```

2. Include the body of the IdP metadata file in the body of the POST and select **XML**.

   You may need to disable SSL certificate verification or set the right trust certificates in POSTMAN.

3. Verify that the POST was successful and includes “Status: 200 OK” and “Identity provider configuration saved” in the response.

Restarting the SAML profile in System Manager

Procedure

1. Log in to System Manager.
2. **Elements › Avaya Breeze® › Configuration › Attributes › Service Clusters**.
3. Click “Cluster” and select your cluster.
4. Undeploy the SAML profile.
5. Scroll down to the SAML Attributes.
6. On the SAML Profile row, select **Override Default**.
7. For Effective Value, select **Undeploy**.
8. Scroll down and click **Commit**.

   Wait at least one minute for the changes to take effect.
9. Redeploy the SAML profile.

   Repeat the previous steps, but for Effective Value select **Deploy**.

   Wait at least three minute for the changes to take effect.

Appendix C: Documentation for Collaboration Environment

Additional information

The following resources provide additional information.

Documentation

See the following related documents at https://support.avaya.com. Many documents are also available at https://documentation.avaya.com.

Overview

Title	Use this document to:	Audience
Avaya Breeze® platform Overview and Specification	Understand the Avaya Breeze® platform, customer requirements, and design considerations.	Sales engineers Programmers System administrators Services and support personnel
Avaya Aura® System Manager Overview and Specification	Understand System Manager customer requirements and design considerations.	Sales engineers Programmers System administrators Services and support personnel

Table continues

Title	Use this document to:	Audience
Avaya Aura® Media Server Overview and Specification	Understand Avaya Aura® Media Server customer requirements and design considerations.	Sales engineers Programmers System administrators Services and support personnel

Deploying

Title	Use this document to:	Audience
Deploying Avaya Breeze® platform	Deploy and configure Avaya Breeze® platform. This is the main deployment document for Avaya Breeze® platform. The deployment documents for other environments are listed below.	Implementation engineers Support personnel System administrators
Deploying Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform	Deploy Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform.	Implementation engineers Support personnel System administrators
Quick Start to deploying the HelloWorld Snap-in	Install, configure, and test an Avaya Breeze® platform snap-in service, specifically the HelloWorld call intercept snap-in.	Programmers System administrators
Planning for Deploying Avaya Aura® applications	Understand deployment options for various Avaya Aura® applications.	Services and support personnel System administrators

Table continues

Title	Use this document to:	Audience
Deploying and Updating Avaya Aura® Media Server Appliance	Deploy and configure Avaya Aura® Media Server when it is installed on customer-provided servers.	System administrators Services and support personnel
Deploying Avaya Aura® System Manager in Infrastructure as a Service Environment	Deploy and configure Avaya Aura® System Manager in an IaaS environment. A separate document is also available for deploying System Manager in a virtualized environment.	System administrators Services and support personnel

Administering

Title	Use this document to:	Audience
Administering Avaya Breeze® platform	Administer Avaya Breeze® platform and snap-ins.	System Administrators Services and Support personnel
Implementing and Administering Avaya Aura® Media Server	Deploy and configure Avaya Aura® Media Server.	System administrators Services and support personnel
Administering Avaya Aura® System Manager	Administer Avaya Aura® System Manager.	System Administrators Services and support personnel
Administering Avaya Aura® Session Manager	Administer Avaya Aura® Session Manager.	System Administrators Services and support personnel

Table continues

Title	Use this document to:	Audience
Administering Avaya Session Border Controller	Administer Avaya SBC.	System Administrators Services and support personnel

Maintaining and troubleshooting

Title	Use this document to:	Audience
Upgrading Avaya Breeze® platform	Upgrade Avaya Breeze® platform.	Services and support personnel
Maintaining and Troubleshooting Avaya Breeze® platform	Troubleshoot Avaya Breeze® platform.	Services and support personnel System administrators
Troubleshooting Avaya Aura® System Manager	Troubleshoot System Manager.	Services and support personnel
Troubleshooting Avaya Aura® Session Manager	Troubleshoot Avaya Aura® Session Manager.	Services and support personnel

Programming

The following developer documents are available on Avaya DevConnect .

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

Table continues

Title	Use this document to:	Audience
Avaya Breeze® platform FAQ and Troubleshooting for Snap-in Developers	Troubleshoot Avaya Breeze® platform snap-in developer issues.	Programmers
Avaya Breeze® platform API Javadocs	Understand API classes and uses.	Programmers

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support › Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.

   For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click to display the search results.

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at https://documentation.avaya.com. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the Avaya Support website.

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.

- Click **Languages** ( ) in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.

  You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click **<** or **>** next to the document title to navigate to the previous topic or the next topic.
- Click **Share** ( ) to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** ( ). You can add the topic and its subtopics or add the entire publication.
- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

  You can do the following:

  - Create, rename, and delete a collection.
  - Set a collection as the default or favorite collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collections that others have shared with you.
- Click **Watch** ( ) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

  You can do the following:

  - Enable **Email notifications** to receive email alerts.
  - Unwatch the selected content or all topics.
- Send feedback for a topic.

Training

The following courses are available on the Avaya Learning website at https://www.avaya-learning.com. After logging in to the website, enter the course code or the course title in the **Search** field, and click **Go** to search for the course.

Course code	Course title
43750W	Selling Avaya Custom and Integration Solutions
30210W	Avaya Breeze® platform Overview for Design
30810W	Designing the Avaya Breeze® Solution Part 1 of 2
30820W	Designing the Avaya Breeze® Solution Part 2 of 2
39220W	Avaya Breeze® Release 3.8 Details for Pre-Sales
39240W	Avaya Breeze® UC Snap-ins Release 3.8 Details for Pre-Sales
2016W	Avaya Breeze® platform Fundamentals
20240W	Programming Avaya Breeze® platform Snap-ins Using Java SDK
20250W	Creating Avaya Breeze® platform Workflows Using Engagement Designer
20260W	Creating Advanced Avaya Breeze® platform Workflows Using Engagement Designer
7016W	Avaya Breeze® platform Implementation and Support
71300V	Integrating Avaya Aura® Communication Applications
72300V	Supporting Avaya Aura® Communication Applications

Viewing Avaya Mentor videos

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

About this task

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

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Select Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

> **Note:**
>
> Videos are not available for all products.

Developer resources

Avaya DevConnect provides resources for Avaya Breeze® platform developers. You must register to access the DevConnect website.

Basic DevConnect membership is free and gives you access to the following information and resources:

- Programming and product documentation
- Sample applications
- Videos
- Webinar recordings
- Forums

Upgraded membership options offer developer-oriented technical support and other program services.

Use a browser to navigate to the Avaya Breeze® platform DevConnect website at https://www.avaya.com/breezedeveloper.

Support

Platform support

Go to the Avaya Support website at https://support.avaya.com/ for the most up-to-date documentation and product notices. You can also search for release notes, service packs, and patches. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Product documentation is also available on the Avaya Documentation Center at https://documentation.avaya.com.

Developer support

Go to the Avaya DevConnect website at http://www.avaya.com/breezedeveloper to access the Avaya Breeze® platform API, SDK, sample applications, developer-oriented technical documentation, and training materials.

Using the Avaya InSite Knowledge Base

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

- Up-to-date troubleshooting procedures and technical tips.
- Information about service packs.
- Access to customer and technical documentation.
- Information about training and certification programs.
- Links to other pertinent information.

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

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

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support › Products**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. Select the release number, if applicable.
6. Click the **Technical Solutions** tab to view articles for resolving technical issues.

Index

A

AAMS priority settings 120
activating a new identity certificate 160
Active Directory 198
Active Directory Configuration 198
add
  trusted CA certificates 172
Add Data Source in SMGR 197
Adding
  LDAP Attribute Rule 217
  new Relying Party 215
  UPN Custom Rule 216
adding an external Authorization Client
  Authorization client 57
administering
  Avaya Breeze® platform 146
  Communication Manager 177
Administration
  Geographic redundancy 73
administration
  Communication Manager 177
alarming
  geographic redundancy 77
Allow Cross-origin Resource Sharing for all 65
Apache Directory Studio 188, 188
application sequences
  assigning a user 48
  creating 38
  description 38
  origination 48
  termination 48
application, creating 38
assigning a user
  to an application sequence 48
assigning and editing grants for authorization 56
assigning instance
  clusters 16
assigning ports field descriptions 139
assigning service ports for snap-ins 71
assigning to users
  service profile 51, 50
Attribute Configuration page description 85
attributes
  clusters 85
  configure 34
  configuring 33, 85
  description 36
  management 167
  SPIRIT 167
authentication 55
authentication
  OAuth 58
  SAML 61
authentication mechanism 63
Authentication mechanism 91
Authorization Client 88, 89
Authorization Clients
  Avaya Breeze Authorization Client 56
  External Authorization Client 57
authorization clients 56
Authorization Configuration field descriptions
  field descriptions 87
authorization resources 55
authorization service 55
authorization service
  getting service provider metadata 61
Authorization Service 91
authorized clients 55
Avaya Breeze Authorization Client 56
Avaya Breeze certificate 173
Avaya InSite Knowledge Base 234
AvayaNetSetup 178
Azure authentication 219, 220, 221, 221, 222, 222

B

backup 27
backup
  cluster database 25
  field descriptions 94
Backup and Restore Status 94
Backup Storage Configuration
  field descriptions 95
batch file 211
Broker Destination Status page
  field descriptions 96
bundle
  deleting 46
  installing on a cluster 45
  load 45
  uninstalling 46
Bundle Details and Installation Status 101
bundle installation 45
bundles 45
bundles
  field descriptions 98
  installation status 102
bundling into a PKCS #12 container
  identity certificate

private key ... 163

C

CA ... 190
call-intercept snap-in
deployment checklist ... 28
testing ... 39
cancel ... 26
CEnetSetup ... 178
certificate management ... 152
certificate revocation ... 175
certificate signing request ... 82, 170
certificate troubleshooting ... 175
Certificate validations ... 173
Certificate validations for SIP TLS connections ... 174
certificates ... 152
certificates issued by System Manager ... 154
certificates not on a CRL ... 175
change ... 67
changes ... 10
check_breeze_status.sh ... 182
cli commands ... 178
client certificate challenge
HTTPS ... 64
client certificate for HTTP security ... 121
cluster
administration ... 12
install bundle ... 45
reboot ... 16
restore ... 26
cluster database ... 23
cluster database
backup ... 25
Cluster DB Backup field descriptions ... 109
cluster editor
field descriptions ... 110
clusters
assigning server ... 16
create ... 12
delete ... 16
field description ... 110
load balancing ... 22
new ... 12
removing servers ... 19
view ... 12
view attributes ... 12
Clusters
assign snap-ins ... 20
configuring snap-in attributes ... 34
delete servers ... 18
installing snap-ins ... 20
snap-ins ... 20
uninstall snap-ins ... 21
clusters attributes
editing ... 14
collection
delete ... 230
edit ... 230
generating PDF ... 230
sharing content ... 230
common issues
certificates ... 175
configure cluster level service attributes ... 33
Configure features field descriptions
field descriptions ... 90
configure global level service attributes ... 33
configure service attributes ... 33
configure service attributes
service profiles ... 33
configuring
Azure ... 219, 220, 221, 221, 222, 222
Okta ... 224, 224, 224, 225, 225, 222, 223
SAML authentication example ... 215, 219, 222
snap-in attributes ... 33, 34
Configuring
SAML Authentication ... 218
configuring attributes
global ... 34, 85
service profile ... 85
snap-ins ... 33
Configuring attributes at cluster level ... 34
configuring service invocation ... 37
configuring service ports ... 71
configuring snap-in attributes
clusters ... 34
content
publishing PDF output ... 230
searching ... 230
sharing ... 230
sort by last updated ... 230
watching for updates ... 230
Create Grant ... 89
creating
an application ... 38
an application sequence ... 38
new administered user ... 50
service profile ... 36
creating a new cluster ... 12
CRL limitations ... 175
CSR ... 82
CSR and Private Key generation via OpenSSL ... 160
CSR generation ... 160
current usage ... 150
custAccounts ... 181

D

data source
delete ... 69

edit ... 68
default SIP CA ... 132
delete
a service profile ... 140
service ... 136
deleting a JDBC data source ... 69
Deleting a Reliable Eventing destination
Eventing destination ... 53
Deleting a Reliable Eventing group
Eventing group ... 53
Deleting an external Authorization Client
Authorization client ... 57
deleting clusters ... 16
deleting JDBC provider resources ... 67
deleting services ... 43
Deleting the Bundle ... 44
deleting the bundle ... 46
Demo certificates ... 157
deployment ... 146
deployment checklist
call-intercept snap-in ... 28
non-call-intercept snap-in ... 28
destination status ... 96
Determining whether you are using a demo identity certificate ... 157
DevConnect ... 233
dial pattern
Callable Services ... 40
directory synchronization ... 198, 215, 209
Disabling
revocation checks ... 217
document changes ... 10
documentation center ... 230
documentation center
finding content ... 230
navigation ... 230
documentation portal ... 230
downloading
SNMP MIB ... 149
Downloading
Active Directory Federation Services metadata file ... 218

E

Edit Grants ... 88
Edit Keys ... 91
Editing a JDBC data source ... 68
Editing a Reliable Eventing group
Eventing group ... 53
editing cluster attributes ... 14
editing JDBC provider resource ... 67
Editing the configuration ... 190
enabling
SAML profile for authorization ... 63
Enabling
SAML Profile ... 219
enabling database
cluster ... 23
end entity ... 189
EULA ... 32
event catalog configuration
field description ... 97
event catalog configuration field descriptions ... 97
Event catalog editor
page description ... 98
Event catalog editor field descriptions ... 98
eventing ... 52
example
enabling SAML authentication ... 215
explicit user administration ... 50
External Authorization Client ... 57

F

Fault management
geographic redundancy ... 77
field descriptions ... 93
field descriptions
Attribute Configuration ... 85
Avaya Breeze® platform ... 91
bundles ... 98
Bundles ... 101
cluster administration ... 102
Cluster DB Backup ... 109
dependencies ... 101
HTTP Security ... 121
Implicit User Profile Rule Editor ... 124
Implicit User Profiles ... 123
Install Trusted Certificate ... 125
installation status ... 102
Maintenance Tests ... 129
Reliable Eventing Group Editor ... 131
server administration ... 132
Service Databases ... 138
Service Profile Configuration ... 140
Service Profile Editor ... 141
Service Status ... 142
Services page ... 136
SNMP MIB Download page ... 143
field descriptions, cluster editor ... 110
finding content on documentation center ... 230

G

Geographic Redundancy ... 73
Geographic Redundancy
replication
restoration ... 78
System Verification Tests ... 79
terminology ... 73, 79
geographic redundancy ... 75
Geographic Redundancy replication ... 78

Geographic Replication data restoration 78
getting
service provider metadata for authorization service 61
global attributes 34, 85

H

HTTP CORS security
administering 65
configuring 65
HTTP load balancing 21
HTTP security 64
HTTP Security page description 121
HTTPS security
whitelist 64

I

identity certificate 168, 83
identity certificate
replacing 157
replacing 159
identity certificates 155
identity certificates
viewing 157
Identity Certificates lifecycle 164
identity provider 62
identity providers 188
idle server 20
IdP configuration 62
IdP support 188
implicit sequencing 48
implicit sequencing
description 38
implicit user pattern 41
Implicit User Profile Rule Editor page descriptions . 124
Implicit User Profiles page description 123
insert bulk users 211
install
service 136
trust certificates 24
install status
service 93, 142, 132
Install Trusted Certificate page description 125
Installation status
field descriptions 102
installing the bundle 45

J

JDBC data source 66
JDBC data source
adding 68
change 68
delete 69
edit 68
field descriptions 127
modify 68
query validation 69
remove 69
JDBC Data Source Editor
field descriptions 128
JDBC data source field descriptions 127
JDBC provider editor
field descriptions 126
JDBC provider resource
adding 66
edit 67
field descriptions 125
JDBC provider resources
delete 67
remove 67
JDBC providers 125
JDBC resource providers 66

K

KB
Support site 234

L

LDAP 58
LDAP Authentication 58
LDAP Client 192
LDAP server 189
LDAP server certificate 59
LDAP Server certificate 59, 60, 190
LDAP users 194
legacy 65
load
service 136
load a service 136
load balancing 22
load balancing
restrictions 21
validations 21
load bundle 45
load snap-ins 32
loading a bundle 45
loading snap-ins
service 32
location settings 120
logging
geographic redundancy 77
logging configuration 149

M

maintenance
from System Manager 149
maintenance operations 149
maintenance test
broker 54

maintenance tests 129, 132
maintenance tests
on-demand 150
Maintenance Tests page descriptions 129
Management and SPIRIT identity certificates attributes 167
managing JDBC providers 66
managing JDBC resources 66
mandatory applications 38
manual switch over 19
Media Server Monitoring, field descriptions 129
MIB download 143, 149
migration 27
modify 67

N

new administered user
creating 50
new cluster
field description 110
New External Authorization Client field descriptions
field description 88
non-call-intercept snap-in
deployment checklist 28
testing 40

O

OAuth 2.0 188
Obtaining new SIP Identity Certificate 170
Okta authentication 224, 224, 224, 225, 225, 222, 223
onfiguring identity provider 62
Open LDAP 211
Open LDAP configuration 211
origination application sequence 48
overview 11, 11

P

peak usage 150
peak usage
reset 151
peer certificate validation 173
PKCS#12 container 170
preferred version
setting 35
priority settings
Avaya Aura Media Server 120
media server 120
private key 81
purge 26

R

reboot system 132
regenerating keys 57
reliable eventing 52
Reliable Eventing group
creating 52
Reliable Eventing Group Editor field descriptions .. 131
Reliable Eventing Groups field descriptions
field descriptions 130
Reliable Eventing status 53
Removing 18
removing servers from a cluster
validations 19
Removing trusted CA certificates 173
replacing an identify certificate with a third party CA issued certificate 159
replacing an identify certificate with an System Manager CA issued certificate 157
replacing an Identity Certificate 169
replacing identity certificate 168
replacing with a System Manager certificate ... 157
replacing with a third party certificate 159
reserving ports field descriptions 139
Resource server
features 55
Resource Server 90
Resources servers tab
servers tab 89
restore 26
restore
field descriptions 94
revocation 175
routing 120
routing policy
callable services 40

S

SAML 58
SAML attribute 218
SAML authentication 61
SAML authentication
configuration example 215, 219, 222
SAML profile 63
sample configuration
database providers 69
searching for content 230
Searching service profiles 38
security 64, 81
security
HTTP 121
trust certificates 24
trusted certificates 125, 132
Security Module HTTP identity certificate attributes 166
Security Module SIP identity certificate attributes .. 165
Server Administration page description 132
service

attributes ... 33
delete ... 43
snap-in ... 41
stop ... 42
service checksum ... 142
Service instances tab
instances tab ... 90
service invocation
configure ... 37
service ports
assign ... 71
change ... 71
configure ... 71
Presence ... 71
services ... 71
snap-ins ... 71
Service ports
field descriptions ... 139
service profile
adding services ... 141
adding snap-ins to new ... 36
assigning to users ... 51, 50
assigning users ... 49
attributes ... 85
Callable Services ... 41
creating ... 36, 141, 140
deleting ... 140
description ... 36
implicit user pattern ... 41
modifying ... 141, 140
selecting snap-in version ... 36
uses ... 36
Service Profile Configuration page descriptions ... 140
Service Profile Editor page description ... 141
service profiles
service invocation ... 37
Service profiles
search ... 38
users assigned ... 38
service provider
getting metadata for authorization service ... 61
Service Status page description ... 142
services
adding to service profile ... 141
configuring attributes for a service profile ... 33
delete ... 136
deleting from service profile ... 141
install ... 136
load ... 136
reinstall ... 142
uninstall ... 42
services in a service profile list ... 93
setting up load balancing ... 22
sharing content ... 230
shutdown system ... 132
SIP entity location ... 120
SIP identity certificate ... 170
snap-in
installation ... 35
loading ... 32
start ... 41
stop ... 42
snap-in attributes
configuring ... 33, 34
snap-in install status ... 35
snap-in ports ... 139
Snap-ins
clusters ... 20
snap-ins
uninstall from clusters ... 21
SNMP MIB
downloading ... 149
SNMP MIB Download page descriptions ... 143
sort documents ... 230
standby server ... 20
starting a service ... 41
starting a snap-in ... 41
stopping a service ... 42
Stopping a snap-in ... 42
Store types ... 24
support ... 233
System Manager
identity certificates ... 154
System Manager root CA certificate ... 173
System Resource Monitoring
field descriptions ... 143
system state ... 132

T

termination application sequence ... 48
testing call-intercept snap-in ... 39
testing non-call-intercept snap-in ... 40
testing the connection
data source ... 69
third party CA ... 169
training ... 231
trust certificates ... 24
trust management ... 170
trusted CA certificates ... 171
trusted certificates ... 125, 132

U

uninstall
services ... 42
uninstalling a service ... 42
Uninstalling snap-ins ... 21
uploading a bundle ... 45
URI
administering ... 148

user
administration 48
user authentication 58
User login experience 58

V

videos 232
View Authorized Clients 90
viewing cluster attributes 12
Viewing identity certificates 157

W

watchlist 230
whitelist for HTTP security 121