



Avaya Context Store Snap-in Reference

© 2015-2019, Avaya Inc.
All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/LicenseInfo), UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

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

License types

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

Heritage Nortel Software

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

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE

AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://WWW.MPEGLA.COM).

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: <https://support.avaya.com> or such successor site as designated by Avaya.

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: Introduction	9
Purpose.....	9
Prerequisites.....	9
How to navigate this document.....	9
Chapter 2: Context Store Snap-in services and features	11
Context Store overview.....	11
Data model mapping.....	12
Context lease time.....	12
Sensitive data.....	12
Context Store architecture overview.....	13
Avaya Breeze™ overview.....	14
Topology.....	15
Context Store services.....	16
Context Store Manager.....	17
Context Store REST.....	18
Context Store SOAP	19
Context Store Query	19
Context Store Screen Pop.....	20
Context Store Notify.....	21
Context Store Rules.....	22
Context Store Event Streams.....	22
Context Store Java SDK.....	23
Context Store JavaScript SDK.....	24
Context Store features.....	25
External Data Mart.....	25
Context aliasId for additional indexing.....	38
Audit trail.....	38
Upsert method.....	40
Pluggable Data Connector.....	40
ContextStoreTasks Type for Engagement Designer.....	41
Authorization.....	41
Scalability overview.....	42
Chapter 3: Interoperability	47
Avaya product compatibility	47
Hardware requirements.....	47
Software requirements	49
Chapter 4: Licensing	50
License requirements.....	50
Configuring Context Store licenses.....	50

Chapter 5: Context Store Deployment	52
Certified deployment scenarios.....	52
Key customer configuration information.....	52
Context Store deployment checklist.....	53
Verifying the status of Avaya Breeze™ servers.....	57
Loading a snap-in service.....	57
Configuring a cluster and installing mandatory services.....	58
Cluster attributes field descriptions.....	60
Installing the optional Context Store services.....	64
Verifying a successful deployment.....	65
Assigning permissions to an authorization client.....	65
Geo redundancy and External Data Mart deployment	66
Enabling Geo redundancy in Context Store.....	66
Enabling External Data Mart persistence.....	68
Enabling External Data Mart provisioning.....	69
Deploying Context Store PDC on Orchestration Designer.....	70
Deploying ContextStoreTask Type.....	71
Overview of ContextStoreTasks Type deployment.....	71
Installing ContextStoreTasks Type SVAR on Engagement Designer.....	72
Context Store Upgrade overview.....	72
Context Store uninstallation and deletion.....	73
Context Store uninstallation overview.....	73
Deleting a Context Store cluster.....	73
Uninstalling an optional snap-in service.....	74
Deleting a snap-in service.....	75
Chapter 6: Administering Context Store	76
Configuring attributes for a service.....	76
ContextStoreManager attribute descriptions.....	76
ContextStoreRest attribute descriptions.....	83
ContextStoreScreenPop attribute descriptions.....	84
ContextStoreNotify attribute descriptions.....	86
ContextStoreRules attribute descriptions.....	87
ContextStoreQuery attribute descriptions.....	88
ContextStoreSoap attribute descriptions.....	89
Chapter 7: High availability	90
High availability within a cluster.....	90
Geo redundancy.....	91
Context Store Geo redundancy overview.....	91
Third party load balancer configuration requirement.....	92
Architecture.....	93
Service preservation.....	94
Session preservation.....	95
Notifications in geo redundant architecture.....	95

Failover support.....	97
Chapter 8: Performance	99
Capacity and scalability specification.....	99
Chapter 9: Security	100
Overview.....	100
Secure space.....	100
Configuring space security.....	101
Selecting TLS version for a snap-in service.....	101
Certificate-based authentication.....	102
Port utilization.....	103
Chapter 10: Troubleshooting	104
Troubleshooting overview.....	104
Alarms.....	104
Overview.....	104
ContextStoreManager_CS_EVT_1.....	105
ContextStoreManager_CS_EVT_2.....	105
ContextStoreManager_CS_EVT_3.....	106
ContextStoreManager_CS_EVT_4.....	107
ContextStoreManager_CS_EVT_5.....	107
Events.....	108
Overview.....	108
CSAUD_5.....	108
CSAUD_7.....	109
CSAUD_8.....	109
CSAUD_10.....	110
CSAUD_11.....	110
CSAUD_13.....	110
Logging.....	111
Context Store log files.....	111
Frequently asked questions.....	112
Where do I find documentation for Context Store?.....	112
Where can I get documentation and help for products related to Context Store?.....	113
Where do I get plugins, SDKs, and sample resources for Context Store?.....	113
Applicability of Context Store licenses.....	114
How do I verify if Context Store is successfully deployed?.....	115
How do I determine the appropriate size for my Context Store deployment?.....	115
How do I verify if Context Store is successfully connected to the External Data Mart?.....	116
How do I determine the appropriate size for my External Data Mart deployment?.....	116
What JDBC driver is required to use the External Data Mart feature.....	117
How do I submit requests to the ContextStoreRest interface if access through external ReST client is blocked?.....	117
Problems with data grid deployment.....	118
How do I verify if connection between geo-redundant clusters is successfully established?.....	119

Does Context Store require runtime configuration changes?.....	120
Why is the ContextStoreRest interface returning 503 Service Temporarily Unavailable for all my requests?.....	120
Why is ContextStoreRest interface blocking all requests with throttled error message?.....	121
Why can't I set the state of my cluster to Accept New Service?.....	121
What is the maximum lease time permitted for a context?.....	122
What are the Context Store limits for data and throughout?.....	122
Why can't I access Context Store from a web client?.....	123
Why is Customer Journey unable to retrieve data?.....	124
Why is the External Data Mart not working?	124
How can I carry out a health check in Context Store interfaces?.....	126
How to I perform troubleshooting for unavailable customer journey?.....	126
Do we have a canned solution we use to link CC Elite to Context Store?.....	127
Why am I seeing a BAD_REQUEST response when using ContextStoreTask Types in an Engagement Designer workflow?.....	127
Context data at rest. Is data encrypted while in the Context Store?.....	127
Context Store Request is still being served over HTTPS even though cluster security is disabled.....	128
Chapter 11: Related resources	129
Documentation.....	129
Finding documents on the Avaya Support website.....	131
Training.....	131
Support.....	131

Chapter 1: Introduction

Purpose

This document describes the Context Store Snap-in characteristics and capabilities, including feature descriptions, interoperability, and performance specifications. The document also provides instructions on deploying, configuring, and troubleshooting the Context Store services.

For information about Avaya Breeze™, Avaya Aura® System Manager, and Avaya Engagement Designer, see the respective product documentation at the Avaya Support website: <http://www.avaya.com/support>.

This document is intended for anyone who wants to install, configure, and administer Context Store.

Prerequisites

- Users who want to deploy and administer the Context Store services must have a working knowledge of Avaya Breeze™ and System Manager.
- Users who want to deploy Context Store must have means to access the Avaya PLDS to be able to download the Context Store services.
- Developers who want to use the Context Store services and SDKs must have a working knowledge of the technologies and products referenced in the document.
- Users who want to use Context Store Pluggable Data Connector (PDC) must have access to Avaya Aura® Orchestration Designer.
- Users who want to use Context Store Task Type must have access to Avaya Engagement Designer.

How to navigate this document

You can navigate back and forth within the PDF file using keyboard shortcut keys in Adobe Acrobat Reader. For example, you might click a link to a related topic while following a procedure and might want to go back to the original location or topic on which you clicked the link.

Follow these simple keyboard shortcuts to navigate this document easily:

- To navigate back to the original topic, press `Alt` and the `Left Arrow` keys together.
- To go to the previous page, press the `Left Arrow` key.
- To go to the next page, press the `Right Arrow` key.
- To go to the first page, press the `Home` key.
- To go to the last page of the document, press the `End` key.

Chapter 2: Context Store Snap-in services and features

Context Store overview

Context Store provides a flexible and easy integration among different applications, providing a centralized solution to store context information. Many applications can use the abstract context concepts that Context Store provides.

A context entry in Context Store has the following main elements:

- **contextId**: A text field that contains a unique identification for the context. You can specify the contextId while adding the context entry in Context Store. If you do not specify a contextId while creating a context, the system generates a unique id.
- **data**: The data field in a context entry is an abstract map with multiple key/value pairs. Keys in the data field must be unique. Multiple identical keys in the same request results in the values being overwritten with the last key. To provide a better structure and organization of context data, Context Store also supports inner maps in context data fields.
- **groupId**: An optional text field that creates a logical group of related context entries. You can specify the groupId while adding the context entry in Context Store or while updating an existing context entry.
- **aliasId**: An optional field that contains unique identifications for the aliases associated with a Context object. You can specify aliasId/aliasIds while adding the context entry in Context Store or you can update an existing context entry to have aliasIds.
- **routingId (rid)**: A parameter used in a Geo-redundant deployment to route requests by the load balancer. If you specify a value for the rid parameter, Context Store assigns the value to the routingId. The default value is 0. The rid query parameter for a request, if provided, cannot be left blank.
- **topic**: An optional text field that can be used to specify the topic of this Context object which can be used later for filtering when querying Context data in the External Data Mart. You can specify the topic while adding the context entry in Context Store or while updating an existing context entry.

Data model mapping

Context Store maps your data model into the Context Store data model. While mapping your data model into the Context Store abstract model of key/value pairs in Context Store, you must consider the following factors:

- Context size: Context Store uses a high performance in-memory data grid. To take advantage of this environment and to achieve high performance, keep the context size minimal. For more information see, [Capacity and scalability specification](#) on page 99.
- Pointers rather than actual data: Use Context Store as a centralized solution to share information and not to store data. For example, use Context Store to store the location and name of a user's picture, not to store the actual picture.
- Structure: Use the inner-map structure of Context Store to structure the data properly.

Context lease time

Context Store preserves a context entry for a specific time defined as the *lease time* of the context. Any Context Store client can renew this lease time, or time-to-live, at any moment. The clients can also define the context lease time while creating a context and specify different lease time values for different scenarios.

A Context Store client can also provide the lease query parameter, but leave the value blank. In this case, Context Store uses the default configured lease for the context object.

Be aware when planning to use the External Data Mart Provisioning feature, that provisioned Context objects are stored in the data-grid with infinite lease time.

Note that Context Store supports retrieval of expired Context data, if that data was persisted to the External Data Mart. The retrieved data is written back into the data-grid (with default lease). This optional feature is enabled via the Enable Retrieval From Database attribute of the ContextStoreRest service.

To use the Context Store in-memory data grid efficiently, you must evaluate the contexts' lease time requirements before implementing Context Store. This analysis helps to understand the memory requirements and usage, and to provide a Context Store solution that can store all information as long as required.

For details about the average latency of a request, see [Capacity and scalability specification](#) on page 99. To store information for a longer duration, you can use an external database.

Sensitive data

Context Store supports customer-encrypted data. The keys in the key/values pairs must not be encrypted as character restrictions apply on these identifiers. For more information on character restrictions, see ReST API documentation. While creating a context entry, the Context Store

clients can mark context values as sensitive. Context Store does not include the sensitive values in logs, alarms, and reports.

*** Note:**

The ReST API documentation can be accessed by browsing to an instance of the Context Store ReST snap-in by typing `http://clusterIP/services/ContextStoreRest/`. You can access this online documentation over HTTP and HTTPS on Firefox, Microsoft Edge, or Chrome browsers; Internet Explorer is not supported. A copy of the full API documentation is provided in the appendix section of *Avaya Context Store Snap-in Developer Guide*.

Context Store architecture overview

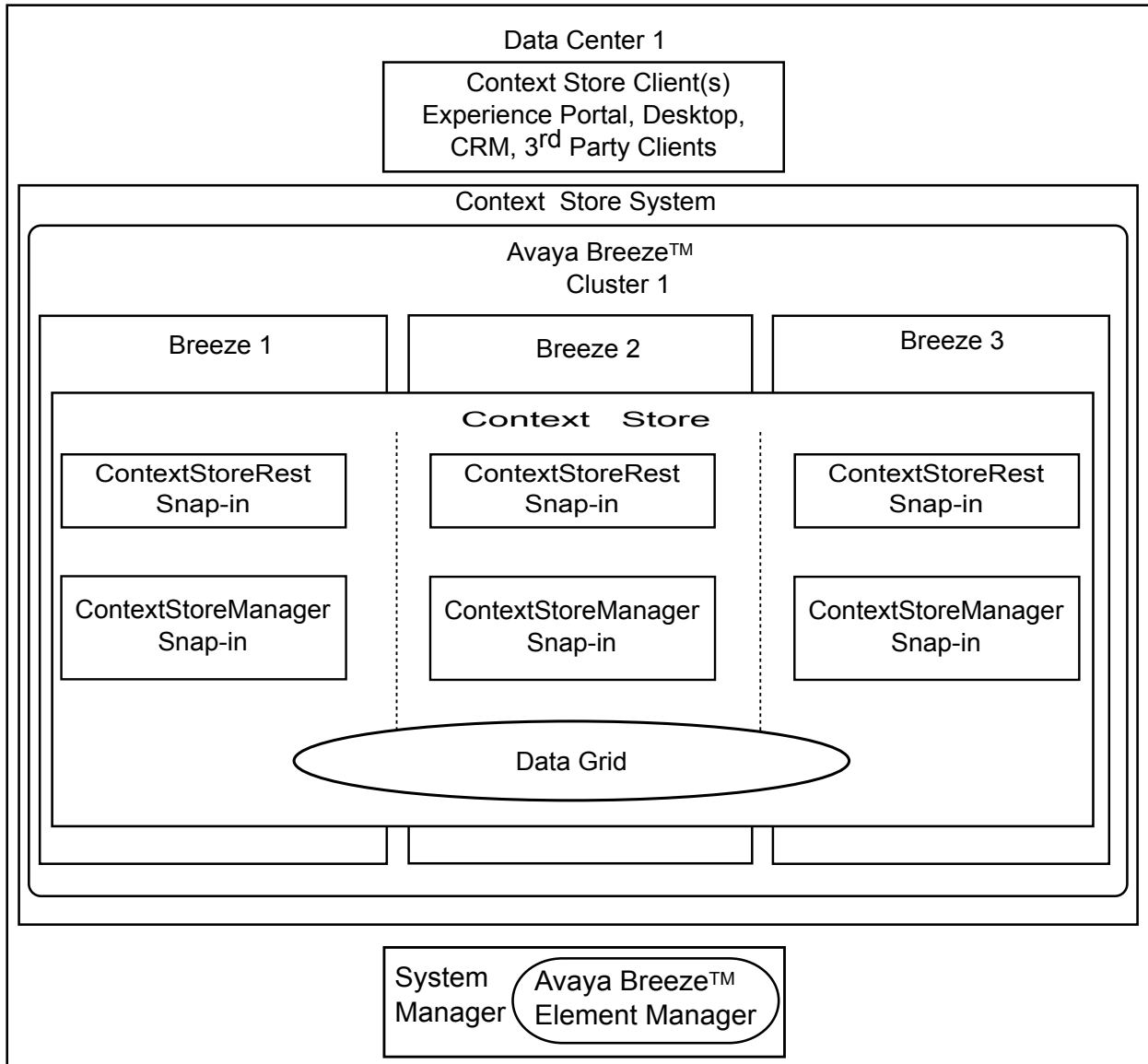
Avaya Context Store Snap-in provides a centralized data cache to the applications in a contact center. Using a distributed cache, Context Store offers a scalable, reliable, and fault-tolerant system to store context information. Context Store also provides services for making changes to the context information. You must deploy Context Store as a service on the applicable release of Avaya Breeze™. For more information on a supported line-up, see *Avaya Context Store Snap-in Release Notes*. A high availability (HA) deployment requires an Avaya Breeze™ cluster containing a minimum of two Avaya Breeze™ nodes.

Context Store offers the following functionality:

- A standard RESTful Web Service API to third-party components to set and get context information.
- Storage of context information using multiple key-value data.
- Storage of context information using external identifiers, such as the UCID generated by Session Border Controllers.
- Scalable solution with high availability using a distributed cache.
- Management and monitoring services through the integration of Avaya Breeze™.
- Security through the integration of Avaya Breeze™.

Context Store offers the flexibility to be deployed on Avaya Breeze™ nodes of varying sizes. You can deploy Context Store on a single node or on a cluster of up to five nodes.

The following diagram shows the high-level architecture for the Context Store configuration of a cluster with three instances of Avaya Breeze™. This is a sample illustration. You can have a single-node cluster or cluster of up to five nodes.



Avaya Breeze™ overview

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

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

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

Avaya Breeze™ provides:

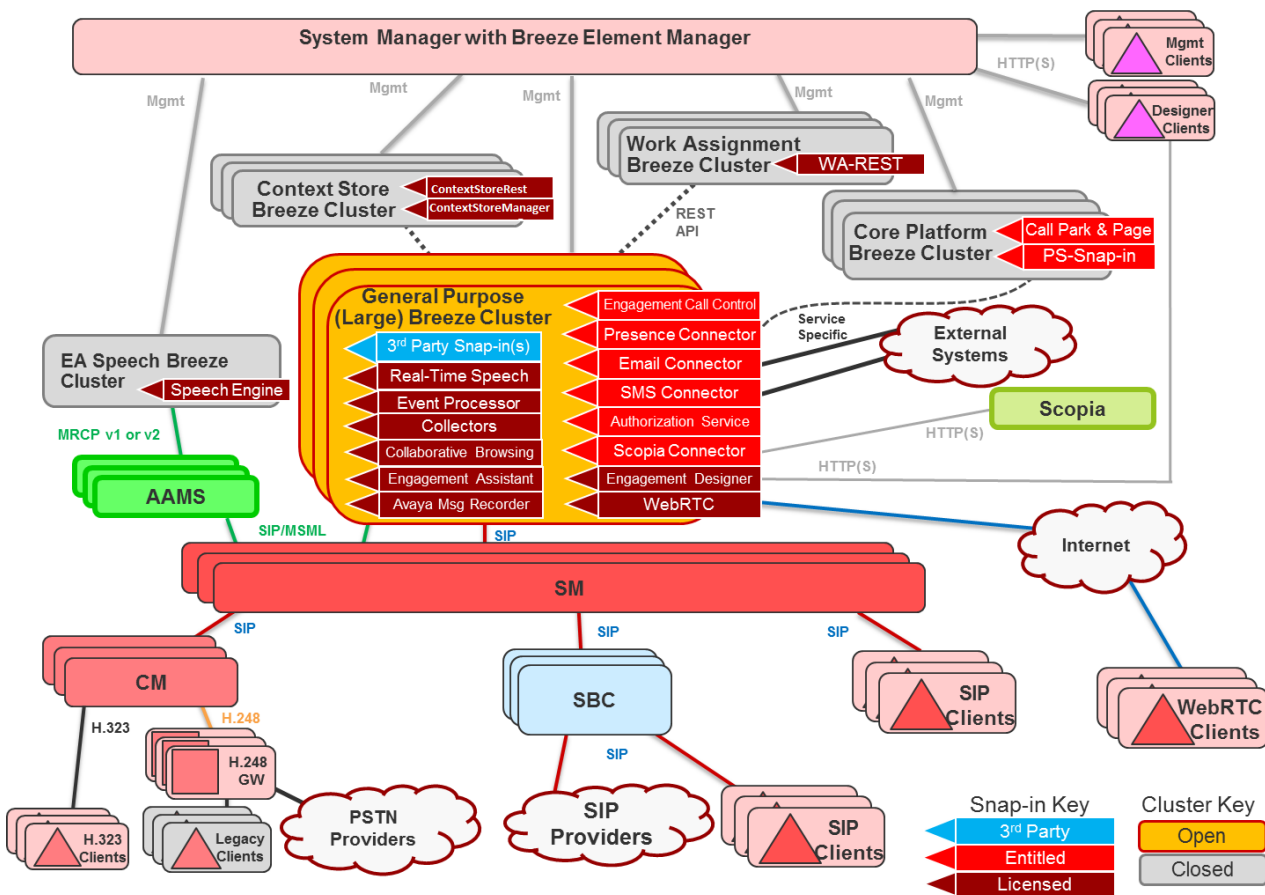
- Unified Communications and Contact Center customers and Business Partners the ability to deliver capabilities using the skill sets of enterprise and cloud application developers.
- A robust Software Development Kit (SDK) with an easy-to-use API. Developers need not understand the details of call processing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

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

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

Topology

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



Context Store services

Context Store provides the following snap-in services:

- Context Store Manager (ContextStoreManager)
- Context Store Rest (ContextStoreRest)
- Context Store Screen Pop (ContextStoreScreenPop)
- Context Store Notify (ContextStoreNotify)
- Context Store Rules (ContextStoreRules)
- Context Store Event Streams (Streams)
- Context Store SOAP (ContextStoreSoap)
- Context Store Query (ContextStoreQuery)

You must install these services from the Avaya Breeze™ **Element Manager** page in System Manager to the Context Store cluster. The system installs the services in all the Avaya Breeze™ servers that are in the Context Store cluster.

Related links

- [Context Store Manager](#) on page 17
- [Context Store REST](#) on page 18
- [Context Store SOAP](#) on page 19
- [Context Store Query](#) on page 19
- [Context Store Screen Pop](#) on page 20
- [Context Store Notify](#) on page 21
- [Context Store Rules](#) on page 22
- [Context Store Event Streams](#) on page 22

Context Store Manager

ContextStoreManager initializes the configuration of Context Store, External Data Mart, the data grid spaces for Context Store, alarming, Event streaming, and Geo redundancy.

When you install the ContextStoreManager snap-in service on Avaya Breeze™, the system deploys a ContextStoreManager service in each Avaya Breeze™ server in the cluster. The service creates the base for Context Store.

Although the ContextStoreManager snap-in service is deployed on every node, only one node is elected to be the Master ContextStoreManager, which handles functions such as alarms. If the node elected to be Master ContextStoreManager fails, another node is immediately elected.

Note:

Using System Manager, you must create a simple network management protocol (SNMP) target profile and assign the profile to your network monitoring system (NMS).

Related links

- [Context Store services](#) on page 16
- [Configuring a cluster and installing mandatory services](#) on page 58
- [ContextStoreManager attribute descriptions](#) on page 76

Data grid

Context Store uses an in-memory data grid for storing the context entries for a specific time. Using the ContextStoreManager service of Context Store, you can specify for how long you want the context entries to be present in the data grid. In addition to providing a storage space, the data grid functionality provides the following advantages to Context Store:

- Efficiency by providing an in-memory data cache for a fast and reliable response in any operation on context data
- Scalability by distributing load across all available resources through the built-in scalability features
- High availability by hot backup for zero downtime
- Consistency by maintaining data integrity with 100% transactional data handling

For more information, see [Context lease time](#) on page 12.

Context Store REST

Context Store implements a RESTful web services interface, the ContextStoreRest service, to provide the required services to the clients.

The ContextStoreRest service focuses on system resources, including addressing and transferring of resource states. ContextStoreRest identifies the resources using HTTP or HTTPS URLs and returns the output to the clients using JavaScript Object Notation (JSON).

Using the contextId, or optionally an aliasId, through the ContextStoreRest snap-in service, you can create, read, update and delete context entries and values. You can also group related context entries together by assigning a groupId when the context entry is created or updating an existing context entry with a groupId.

The required fields for Context Store object are as follows:

- contextId: A unique identifier for the context. If you do not specify a contextId while creating a context, the system generates a unique id. A contextId can be of maximum 255 characters.
- data: Represented as key/value pairs.

Basic request example

* Note:

On multiple node deployments, ContextStoreRest requests must be submitted through the clusterIP, which ensures that the requests are load balanced across all the servers in a cluster. For single node deployments, enter the Avaya Breeze™ node security IP instead of the cluster IP.

Request name	URL	HTTP request type	Content
Create a new context object	<code>https://clusterIP/services/ContextStoreRest/cs/contexts/</code>	POST	<code>{"contextId":"sampleContext", "data": {"key1":"value1","key2":"value2","key3":"value3"}}</code>
Retrieve an existing context object	<code>https://clusterIP/services/ContextStoreRest/cs/contexts/sampleContext</code>	GET	

For more information about ContextStoreRest, and the complete API documentation, see *Avaya Context Store Snap-in Developer Guide*.

Related links

[Context Store services](#) on page 16

[Configuring a cluster and installing mandatory services](#) on page 58

[ContextStoreRest attribute descriptions](#) on page 83

Context Store SOAP

Context Store SOAP is an optional snap-in service that provides the required Context Store services to the clients. All the Context Store operations available through the ContextStoreRest interface are also available through this Simple Object Access Protocol (SOAP)-compliant interface. A Web Service Definition Language (WSDL) file and schema define the ContextStoreSoap interface.

Both the ContextStoreRest and SOAP interfaces are deployed on the same Avaya Breeze™ cluster. Context Store routes the requests received through the SOAP interface to the ContextStoreRest interface on the local Avaya Breeze™ node. The ContextStoreSoap snap-in sends the SOAP XML envelopes to the clients as defined by the schema in the snap-in WSDL.

You can download the ContextStoreSoap WSDL from <http://clusterIP/services/ContextStoreSoap/wsd/cs/Cs.wsd>.

Note:

In a geo-redundant deployment, you cannot download the ContextStoreSoap WSDL through the IP address of a customer-provided geo load balancer. You must download the WSDL directly from either of the clusters in the configuration and then update with the IP address of the geo load balancer.

Avaya Aura® Contact Center (AACC) uses Context Store SOAP interface as a web interface to send and receive context data. The SOAP interface is compatible with the Database Integration Wizard (DIW) application of AACC. So the SOAP web service calls can be invoked from the AACC script.

ContextStoreSoap snap-in is installed as an SVAR file. For more information, see the Installing the optional Context Store services topic.

For more information about ContextStoreSoap and the complete API documentation, see *Avaya Context Store Snap-in Developer Guide*.

Related links

[Context Store services](#) on page 16

[ContextStoreSoap attribute descriptions](#) on page 89

[Installing the optional Context Store services](#) on page 64

Context Store Query

Context Store Query (ContextStoreQuery) is an optional snap-in service that you can use to retrieve context data that is unavailable in the Context Store data grid from an external data mart (EDM).

The ContextStoreQuery snap-in provides a REST interface to collect all associated context data from the EDM in the JSON format. Using the ContextStoreQuery REST interface, you can generate audit trails or retrieve instances of context data from the context data stored in the

associated EDM database. With this collected data, you can visualize a customer journey represented by an interaction with a touchpoint.

You must configure the **EDM: Database username** and **EDM: Database password** attributes to retrieve information from an EDM. Misconfigured or incorrect details (e.g. incorrect password) will result in errors in the system.

The ContextStoreQuery snap-in is installed as an SVAR file. For more information, see the [Installing the optional Context Store services](#) topic.

The supported databases are:

- PostgreSQL
- Microsoft SQL Server
- Oracle

*** Note:**

To retrieve context audit trails using the ContextStoreQuery snap-in, you must enable the Audit Trail feature using the applicable ContextStoreManager attribute.

Retrieving customer interaction details with ContextStoreQuery snap-in

You can retrieve customer interaction details using a contextId or a groupId. Use contextId to retrieve a single customer journey and use groupId to retrieve multiple customer journeys. You can also retrieve the latest context entry in EDM.

Related links

[Context Store services](#) on page 16

[Customer journey visualization](#) on page 35

[Audit trail](#) on page 38

[ContextStoreQuery attribute descriptions](#) on page 88

[Installing the optional Context Store services](#) on page 64

Context Store Screen Pop

ContextStoreScreenPop is an optional service which you can use to either view, add, or update the data stored in Context Store in a format that you prefer. ContextStoreScreenPop uses both predefined and user defined rules to process the available data. The snap-in then returns the processed information to the clients in the specified format. Context Store supports the following formats for returning data: HTML, XML, JSON, URL, REDIRECT, WA, and MAILTO. You can configure these output formats to view the context data in a web browser.

ContextStoreScreenPop provides a rules engine with which you can manipulate the view of context data stored in Context Store. To configure the rules, all you must do is add the rule in System Manager, and the rules engine updates the rule set. The rules engine can change the output format, and filter the results based on the keys in the context. For more information about how to create user-configurable rules or make use of the existing predefined rules, see *Avaya Context Store Snap-in Developer Guide*.

The ContextStoreScreenPop URLs can easily integrate with other applications, such as Avaya One-X Agent. For information for how to configure ContextStoreScreenPop with Avaya one-X[®] Agent, see *Avaya Context Store Snap-in Developer Guide*.

Related links

[Context Store services](#) on page 16

[Installing the optional Context Store services](#) on page 64

[ContextStoreScreenPop attribute descriptions](#) on page 84

Context Store Notify

ContextStoreNotify is an optional service in Context Store, using which you can receive notifications for any change in a context entry. The ContextStoreNotify service uses the ContextStoreRest service to send an event trigger to up to five registered subscribers through the REST interface. To use this service, you must:

- Obtain a suitable client that can handle REST messages.
- Create a service on your application server so that the client can handle the REST event messages.
- Subscribe for the ContextStoreNotify service by configuring the ContextStoreNotify attributes in System Manager.

To subscribe for a notification, you must configure the ContextStoreNotify attributes using the System Manager Cluster attributes page and provide the URI of the endpoint that you want to configure for receiving notifications.

You can also provide the following optional filters:

- The tenantId of the contexts for which you want to receive notifications.
- The groupId of the contexts for which you want to receive notifications.

You can configure up to five subscriptions. You can enable or disable a subscription by specifying a value of true or false for the attribute *enabled*. You can disable or enable a subscription dynamically. However, to change any other configuration of a subscription, you must first disable the subscription, make the changes, and then enable the subscription again.

If Context Store cannot send the notification to the client endpoint for any reason, Context Store retries to send the same notification to the same endpoint up to three times in a one– minute period. After the third try, if Context Store is still unable to send the notification, Context Store disables the subscription for that endpoint. To enable that subscription again, you must first disable the subscription by setting the ContextStoreNotify attribute *enabled* as *false* (a snap-in itself cannot update an attribute value in System Manager). After you verify that the endpoint is available for receiving notifications, you can enable the subscription by setting the value of the *enabled* attribute to *true*.

Related links

[Context Store services](#) on page 16

[ContextStoreNotify attribute descriptions](#) on page 86

[Installing the optional Context Store services](#) on page 64

Context Store Rules

ContextStoreRules is an optional service snap-in with which you can integrate Context Store with CRM systems by triggering an Engagement Designer workflow.

Context Store provides a flag to determine if the data must be sent to the rules engine. The rules engine then determines the workflow that must be triggered by raising the Avaya Breeze™ event that the workflow is listening for.

You can load the CRM integration ContextStoreRules snap-in using the standard System Manager SVAR loading mechanism. The CRM Integration ContextStoreRules snap-in has:

- User-defined business rules to determine if it must trigger a rule and which Avaya Breeze™ event it must raise.
- Rules that you can trigger using the following ContextStoreRest API calls, if you add the parameter rules=true to the URL:
 - Create Context (POST)
 - Update Context (PUT)

You can define five rules and trigger five independent workflows based on the rules.

To configure the CRM integration snap-in, you must create a unique Avaya Breeze™ event and an Engagement Designer workflow. You must also configure the Engagement Designer cluster to allow HTTP requests. For more information about CRM integration, see *Avaya Context Store Snap-in Developer Guide* and *Avaya Engagement Designer Developer's Guide*.

Related links

[Context Store services](#) on page 16

[Installing the optional Context Store services](#) on page 64

[ContextStoreRules attribute descriptions](#) on page 87

Context Store Event Streams

With the Event Streams feature, Context Store provides more fine-grained and personalized event notifications than the ContextStoreNotify feature. Users, such as an agent or agent supervisor, can register for customized event streams. The users can filter the event streams by identifiers of the context, such as contextId, or specific keys or key/value pairs that the context object contains. The users can register for the event streams using a web interface. Context Store delivers the applicable event notifications to the users through the same interface. A sample JavaScript web interface is provided for the Event Streams feature. For more information about the Event Streams feature and the usage of the web interface, see *Avaya Context Store Snap-in Developer Guide*.

To use the Event Streams feature, you must install the Streams SVAR on the Context Store cluster and enable the feature using the **Event Stream: Enable Event Streaming** field on the

ContextStoreManager page. For more information about installing the SVAR file, see [Installing the optional Context Store services](#) on page 64.

The Event Streams feature requires space in the data grid to operate. Hence, while enabling the Event Streams feature, you must reduce the maximum memory allocation in the **ContextStoreSpace DataGrid Settings** field by 6 GB. You must also restart the cluster after reducing the memory allocation.

Feature restrictions

Context Store does not support filtering event notifications by aliasIds. The limitation is because of the inability to filter by complex objects, such as json objects.

The number of users or streams must be limited to five registered streams. You can either have five users with one stream each or fewer users with multiple streams each.

The Event Streams feature is supported only on environments equal to or greater than 64 GB x 3 nodes.

You cannot enable the feature on systems on which traffic is running.

Related links

[Context Store services](#) on page 16

[ContextStoreManager attribute descriptions](#) on page 76

[Installing the optional Context Store services](#) on page 64

Context Store Java SDK

Context Store provides a Java SDK to facilitate the access to the Context Store services. The Context Store Java SDK provides a client library for users to write software that will interact with a deployed Context Store system.

The Context Store Java SDK is a zip file and is distributed through Avaya DevConnect at http://www.devconnectprogram.com/site/global/products_resources/avaya_breeze/avaya_snap_ins/context_store/overview/index.gsp.

The directory structure of the Context Store Java SDK, ContextStore <version> SDK.zip, is as follows:

```
CS Event Stream Client
├─ app
│  ├─ assets
│  ├─ css
│  ├─ font
│  ├─ js
│  └─ scripts
├─ browser components
├─ boiler_plate_client.html
├─ index.html
├─ README.txt
CS ReST
├─ CS ReST Clients
│  └─ cs-rest-csharp-client (rest clients for testing purposes only)
│     └─ packages
│        └─ SimpleClient
│           └─ README.txt
```

```
    - SimpleClient.sln
  | CS SDK
  | | CS SDK API
  | | | conf (logging configuration file)
  | | | examples (an example integration class using the SDK)
  | | | lib (the dependencies that are required to use the SDK)
  | | | - cs-sdk-api-<version>-SNAPSHOT.jar
  | | | - cs-sdk-api-<version>-SNAPSHOT-javadoc.jar
  | | | - developer_guide.html
  | | | .....- LICENSE.txt
  | | | | CS SDK Docs (the SDK documentation)
  | | | | - developer_guide.html
```

Access to Context Store through the Java SDK requires client authentication. Authentication is established using certificates. The Java SDK requires users to supply the following system properties at runtime: Keystore location, Keystore password, Truststore location, and Truststore password.

For more information about the guidelines for the Context Store SDK use, see *Avaya Context Store Snap-in Developer Guide*.

Context Store JavaScript SDK

Context Store provides a JavaScript SDK to facilitate access to the Context Store services. The JavaScript SDK provides a client library using which users can write software that interacts with a deployed Context Store system through the ContextStoreRest interface.

The SDK provides service interfaces using the created instance of the AvayaDataStoreClient class. With the JavaScript SDK, you can access all Context Store operations that are available through ContextStoreRest.

The Context Store JavaScript SDK is a .js file within a zip file and is distributed through Avaya DevConnect at http://www.devconnectprogram.com/site/global/products_resources/avaya_breeze/avaya_snap_ins/context_store/overview/index.gsp.

The zip file contains:

- AvayaDataStoreClient-<version>.min.js: The Context Store JavaScript SDK library
- test_app directory: The directory that contains a sample client for accessing the Context Store JavaScript SDK
- README.txt: Instructions for SDK usage
- License.txt: User license

For more information about JavaScript API operations and guidelines for Context Store JavaScript SDK usage, see *Avaya Context Store Snap-in Developer Guide*.

Context Store features

External Data Mart

External Data Mart overview

External Data Mart (EDM) is an optional feature of the ContextStoreManager snap-in service. Using EDM, you can connect and persist data from Context Store to an external, customer-provided database. To use this feature, you must install any of the databases that Context Store supports, create the required tables, and configure the relevant parameters in the ContextStoreManager section.

! **Important:**

If you make any configuration changes in EDM after installation, you must disable the **EDM: Enable persistence to database** field and enable the field again after reconfiguring the EDM.

Context Store provisioning and persistence of data to EDM

While both Context Store provisioning and the persistence of data to EDM features share the same **ContextStoreManager** EDM attributes, they operate independently of one another. You can enable either Context Store provisioning or persistence of data to EDM or both on a cluster.

- Provisioning Context Store with data from the database: The Context Store space queries the database on start-up for entries in the database and writes them into its data grid with infinite leases.
- Persistence of data to an external database: The EDM Mirror Service listens to the replication channel of the Context Store data grid and adds entries to database for every operation on a flagged context.

***** **Note:**

- The EDM Mirror Service captures any context added to Context Store, including the contexts added using the provisioning feature, and persists the operation table of the EDM database.

***** **Note:**

If the EDM is unreachable by the EDM Mirror Service, the EDM redo logs will save approximately 30 minutes of context data from before the time that the EDM is reconnected. The configuration for the EDM Mirror Service Redo Log attribute is provided for different deployment scenarios in the *Data-grid Configuration Settings – ContextStoreManager Attributes* section of the *Context Store Release Notes*.

- If you have enabled both the EDM persistence and EDM provisioning features, the system writes the provisioned context data into the CS_OPERATION table each time the cluster is restarted. That means that there will be near-identical entries in the CS_OPERATION table, the only differentiation being the time-stamp of the object.

Supported databases

Context Store supports the following three databases for External Data Mart:

- PostgreSQL 9.1 and later
- Oracle 11g and later
- Microsoft SQL Server 2008 and later

When you install ContextStoreManager, External Data Mart tries to validate the database tables *CS_OPERATION*, *CS_PROVISION* and *GENERATED_KEYS* in the external database that you have configured. If the tables are not present or if the tables do not match the required database schema, the installation of the External Data Mart feature fails. If External Data Mart fails to install, Context Store raises an alarm to System Manager.

External Data Mart provisioning

With the EDM provisioning feature, you can replicate contexts to an external database and use the replicated contexts to redeploy a pre-populated CS data grid. To facilitate such provisioning, you must create contexts with the "`persistTo`": "`CS_PROVISION`" flag set.

Context Store stores the contexts that contain the provisioning flag into the provisioning table of the external data mart. When you reboot Context Store, the contexts that are stored in the `CS_PROVISION` table are brought back into the data grid from the external data mart.

An operation on a context in the data grid updates the provisioning table in the external data mart with the latest version of the context.

Provisioned context data

When you reboot Context Store, the data grid is empty. If the **EDM: Enable Provisioning from database** field is set to `true` in the ContextStoreManager attributes, Context Store queries the `CS_PROVISION` table in the EDM database for context entries. Then the system performs a pump-up of the provisioned data to populate the data grid.

Context Store supports retrieving 10 contexts from the external data mart per second.

This feature is designed for automatically provisioning vital operational information into the data-grid. It is not intended as a means to pump-up all general context data from external sources.

If a configured external data mart is unavailable or the operation times out, Context Store attempts the operation for a fixed number of times. The multiple attempts are to ensure that potential networking difficulties are addressed. For more information about enabling the EDM provisioning feature in Context Store, see the *Enabling External Data Mart* topic. For more information about EDM provisioning, see *Avaya Context Store Snap-in Developer Guide*.

Database requirements and planning

You must configure the External Data Mart feature while configuring the ContextStoreManager service. Consider the following factors before you configure External Data Mart:

- Database: You must install a database server that Context Store supports.

*** Note:**

The Context Store database owner requires a minimum of 100 connections to the external database.

- Network:
 - The database must be in the same LAN as the Avaya Breeze™ host where you have installed Context Store.
- Database user: You must create a user account for Context Store to connect to the database. The user account must have permissions to read and write database entries for Context Store.

*** Note:**

- If you are using the Microsoft SQL server: The db user configured for the EDM feature must have database ownership or the system administrator privileges for this connection to be successful. Also, from the security profile of the database user, you must set the Context Store database as the default database.
- Database space: You must plan the space requirements for your database. You cannot modify the database and External Data Mart configurations after you install the ContextStoreManager service. The average size of a context is 2 KB in raw JSON data. However, this size might differ significantly depending on your configuration.
- Create database tables: You must create the required database tables before you install External Data Mart. Ensure to create the database tables in the correct database that you intend to use with Context Store.
- Verification: After you create the database tables, perform the following tasks to verify the database and the tables:
 - Test the database connection.
 - Log in to the database and verify if you have created the database tables successfully.
 - Test if the user account that you have created for Context Store has the required permissions.

For the specific instructions on the verification process, see the documentation of your database.

Creating database tables for External Data Mart

About this task

External Data Mart supports PostgreSQL, Oracle, and Microsoft SQL Server. To use the External Data Mart feature, you must use any of these three databases and create the required database tables. For more information about External Data Mart, see [External Data Mart overview](#) on page 25.

*** Note:**

If you are using the Microsoft SQL server: The db user configured for the EDM feature must have database ownership or the system administrator privileges for this connection to be

successful. Also, from the security profile of the database user, you must set the Context Store database as the default database.

Procedure

1. Log in to the external database that you are using for External Data Mart using the database user account you have created for Context Store.
2. Create database tables for External Data Mart.

 **Note:**

The SQL scripts for database schema creation and update are also available from the DevConnect portal.

Depending on the database that you have, enter the relevant commands provided in the following table:

Database	Commands
PostgreSQL	<p>If the tables <i>CS_OPERATION</i>, <i>CS_PROVISION</i> and <i>GENERATED_KEYS</i> exist, drop the tables:</p> <pre>DROP TABLE IF EXISTS CS_OPERATION CASCADE; DROP TABLE IF EXISTS CS_PROVISION CASCADE; DROP TABLE IF EXISTS GENERATED_KEYS CASCADE;</pre> <p>Create the tables:</p> <pre>CREATE TABLE CS_OPERATION (PERSIST_CONTEXT_UID INT8 NOT NULL, CONTEXT_ID VARCHAR(255) NOT NULL, ROUTING_ID VARCHAR(255) NOT NULL, TENANT_ID VARCHAR(255), DATA_JSON TEXT, IDENTIFIER VARCHAR(255), META_JSON TEXT, GROUP_ID VARCHAR(255), OPERATION_TYPE VARCHAR(10), UPDATE_DATE TIMESTAMP NOT NULL, SCHEMA_JSON TEXT, TOUCHPOINT VARCHAR(255), TIMESTAMP VARCHAR(255), PRIMARY KEY (PERSIST_CONTEXT_UID)); CREATE TABLE CS_PROVISION (SPACE_ID VARCHAR(255) NOT NULL, CONTEXT_ID VARCHAR(255) NOT NULL, ROUTING_ID VARCHAR(255) NOT NULL, TENANT_ID VARCHAR(255), DATA_JSON TEXT, IDENTIFIER VARCHAR(255), META_JSON TEXT, GROUP_ID VARCHAR(255), OPERATION_TYPE VARCHAR(10), UPDATE_DATE TIMESTAMP NOT NULL, SCHEMA_JSON TEXT, TOUCHPOINT VARCHAR(255), TIMESTAMP VARCHAR(255), PRIMARY KEY (SPACE_ID)); CREATE INDEX CS_OPERATION_CONTEXT_ID_IDX ON CS_OPERATION (CONTEXT_ID); CREATE INDEX CS_OPERATION_GROUP_ID_IDX ON CS_OPERATION (GROUP_ID); CREATE INDEX CS_OPERATION_ROUTING_ID_IDX ON CS_OPERATION (ROUTING_ID); CREATE INDEX CS_OPERATION_TOUCHPOINT_IDX ON CS_OPERATION (TOUCHPOINT); CREATE INDEX CS_OPERATION_TIMESTAMP_IDX ON CS_OPERATION (TIMESTAMP); CREATE INDEX CS_OPERATION_GRP_QRY_IDX ON CS_OPERATION (GROUP_ID, TOUCHPOINT); CREATE INDEX CS_PROVISION_CONTEXT_ID_IDX ON CS_PROVISION (CONTEXT_ID);</pre>

Database	Commands
	<pre>CREATE INDEX CS_PROVISION_ROUTING_ID_IDX ON CS_PROVISION (ROUTING_ID); CREATE INDEX CS_PROVISION_TOUCHPOINT_IDX ON CS_PROVISION (TOUCHPOINT); CREATE INDEX CS_PROVISION_TIMESTAMP_IDX ON CS_PROVISION (TIMESTAMP); CREATE INDEX CS_PROVISION_GRP_QRY_IDX ON CS_PROVISION (GROUP_ID, TOUCHPOINT); CREATE TABLE GENERATED_KEYS (PK_COLUMN VARCHAR(255),VALUE_COLUMN INT4);</pre>

Database	Commands
Oracle	<p>If the tables <i>CS_OPERATION</i>, <i>CS_PROVISION</i> and <i>GENERATED_KEYS</i> exist, drop the tables:</p> <pre>DROP TABLE CS_OPERATION CASCADE CONSTRAINTS; DROP TABLE CS_PROVISION CASCADE CONSTRAINTS; DROP TABLE GENERATED_KEYS CASCADE CONSTRAINTS;</pre> <p>Create the tables:</p> <pre>CREATE TABLE CS_OPERATION (PERSIST_CONTEXT_UID NUMBER(19,0) NOT NULL, CONTEXT_ID VARCHAR2(255 CHAR) NOT NULL, ROUTING_ID VARCHAR2(255 CHAR) NOT NULL, TENANT_ID VARCHAR2(255 CHAR), DATA_JSON CLOB, IDENTIFIER VARCHAR2(255), META_JSON CLOB, GROUP_ID VARCHAR2(255 CHAR), OPERATION_TYPE VARCHAR2(10 CHAR), UPDATE_DATE TIMESTAMP NOT NULL, SCHEMA_JSON CLOB, TOUCHPOINT VARCHAR2(255 CHAR), TIMESTAMP VARCHAR2(255 CHAR), PRIMARY KEY (PERSIST_CONTEXT_UID)); CREATE TABLE CS_PROVISION (SPACE_ID VARCHAR2(255 CHAR) NOT NULL, CONTEXT_ID VARCHAR2(255 CHAR) NOT NULL, ROUTING_ID VARCHAR2(255 CHAR) NOT NULL, TENANT_ID VARCHAR2(255 CHAR), DATA_JSON CLOB, IDENTIFIER VARCHAR2(255), META_JSON CLOB, GROUP_ID VARCHAR2(255 CHAR), OPERATION_TYPE VARCHAR2(10 CHAR), UPDATE_DATE TIMESTAMP NOT NULL, SCHEMA_JSON CLOB, TOUCHPOINT VARCHAR2(255 CHAR), TIMESTAMP VARCHAR2(255 CHAR), PRIMARY KEY (SPACE_ID)); CREATE INDEX CS_OPERATION_CONTEXT_ID_IDX ON CS_OPERATION (CONTEXT_ID); CREATE INDEX CS_OPERATION_GROUP_ID_IDX ON CS_OPERATION (GROUP_ID); CREATE INDEX CS_OPERATION_ROUTING_ID_IDX ON CS_OPERATION (ROUTING_ID); CREATE INDEX CS_OPERATION_TOUCHPOINT_IDX ON CS_OPERATION (TOUCHPOINT); CREATE INDEX CS_OPERATION_TIMESTAMP_IDX ON CS_OPERATION (TIMESTAMP); CREATE INDEX CS_OPERATION_GRP_QRY_IDX ON CS_OPERATION (GROUP_ID, TOUCHPOINT); CREATE INDEX CS_PROVISION_CONTEXT_ID_IDX ON CS_PROVISION (CONTEXT_ID); CREATE INDEX CS_PROVISION_ROUTING_ID_IDX ON CS_PROVISION (ROUTING_ID); CREATE INDEX CS_PROVISION_TOUCHPOINT_IDX ON CS_PROVISION (TOUCHPOINT); CREATE INDEX CS_PROVISION_TIMESTAMP_IDX ON CS_PROVISION (TIMESTAMP); CREATE INDEX CS_PROVISION_GRP_QRY_IDX ON CS_PROVISION (GROUP_ID,</pre>

Database	Commands
	<pre>TOUCHPOINT); CREATE TABLE GENERATED_KEYS (PK_COLUMN VARCHAR2 (255 CHAR), VALUE_COLUMN NUMBER (10, 0));</pre>

Database	Commands
Microsoft SQL Server	<p>If the tables <i>CS_OPERATION</i>, <i>CS_PROVISION</i> and <i>GENERATED_KEYS</i> exist, drop the tables:</p> <pre>DROP TABLE CS_OPERATION; DROP TABLE CS_PROVISION; DROP TABLE GENERATED_KEYS;</pre> <p>Create the tables:</p> <pre>CREATE TABLE CS_OPERATION (PERSIST_CONTEXT_UID NUMERIC(19,0) NOT NULL, CONTEXT_ID VARCHAR(255) NOT NULL, ROUTING_ID VARCHAR(255) NOT NULL, TENANT_ID VARCHAR(255), DATA_JSON TEXT, IDENTIFIER VARCHAR(255), META_JSON TEXT, GROUP_ID VARCHAR(255), OPERATION_TYPE VARCHAR(10) NULL, UPDATE_DATE DATETIME NOT NULL, SCHEMA_JSON TEXT, TOUCHPOINT VARCHAR(255), TIMESTAMP VARCHAR(255), PRIMARY KEY (PERSIST_CONTEXT_UID)); CREATE TABLE CS_PROVISION (SPACE_ID VARCHAR(255) NOT NULL, CONTEXT_ID VARCHAR(255) NOT NULL, ROUTING_ID VARCHAR(255) NOT NULL, TENANT_ID VARCHAR(255), DATA_JSON TEXT, IDENTIFIER VARCHAR(255), META_JSON TEXT, GROUP_ID VARCHAR(255), OPERATION_TYPE VARCHAR(10) NULL, UPDATE_DATE DATETIME NOT NULL, SCHEMA_JSON TEXT, TOUCHPOINT VARCHAR(255), TIMESTAMP VARCHAR(255), PRIMARY KEY (SPACE_ID)); CREATE INDEX CS_OPERATION_CONTEXT_ID_IDX ON CS_OPERATION (CONTEXT_ID); CREATE INDEX CS_OPERATION_GROUP_ID_IDX ON CS_OPERATION (GROUP_ID); CREATE INDEX CS_OPERATION_ROUTING_ID_IDX ON CS_OPERATION (ROUTING_ID); CREATE INDEX CS_OPERATION_TOUCHPOINT_IDX ON CS_OPERATION (TOUCHPOINT); CREATE INDEX CS_OPERATION_TIMESTAMP_IDX ON CS_OPERATION (TIMESTAMP); CREATE INDEX CS_OPERATION_GRP_QRY_IDX ON CS_OPERATION (GROUP_ID, TOUCHPOINT); CREATE INDEX CS_PROVISION_CONTEXT_ID_IDX ON CS_PROVISION (CONTEXT_ID); CREATE INDEX CS_PROVISION_ROUTING_ID_IDX ON CS_PROVISION (ROUTING_ID); CREATE INDEX CS_PROVISION_TOUCHPOINT_IDX ON CS_PROVISION (TOUCHPOINT); CREATE INDEX CS_PROVISION_TIMESTAMP_IDX ON CS_PROVISION (TIMESTAMP);</pre>

Database	Commands
	<pre>CREATE INDEX CS_PROVISION_GRP_QRY_IDX ON CS_PROVISION (GROUP_ID, TOUCHPOINT);</pre> <pre>CREATE TABLE GENERATED_KEYS (PK_COLUMN VARCHAR(255), VALUE_COLUMN INT);</pre>

Configuring Additional Databases

Additional databases

Context Store provides only the PostgreSQL database by default. However, you can configure Context Store to write to other databases, if the database has a JDBC-compatible driver. You must load the jar file to System Manager and then configure the drivers in the **ContextStoreManager** page.

You need licence to use some JDBC drivers. You must provide a licensed driver and load it into the Context Store cluster.

For more information about configuring the drivers, see [ContextStoreManager attribute descriptions](#) on page 76. For more information about enabling External Data Mart, see [Enabling External datamart in Context Store](#) on page 68.

Loading JDBC driver to System Manager

Procedure

1. On the System Manager web console, click **Home > Elements > Avaya Breeze > Configuration > JDBC Providers**.
2. Click **New** and enter information in the required fields.
3. Click **Select the jar file** to select the JDBC jar file.

The driver appears on the list of **Available JDBC drivers**.

4. On the System Manager web console, click **Avaya Breeze > Service Management > Services**.
5. Select the driver.
6. Click **Install** and select the Context Store cluster.
7. Click **Commit** to install the jar file to the cluster.

Related links

[JDBC Providers field description](#) on page 34

JDBC Providers field description

Name	Description
Name	The name of your JDBC driver.

Table continues...

Name	Description
Driver Name	The name of the JDBC driver class. <ul style="list-style-type: none"> • Oracle: <ul style="list-style-type: none"> - oracle.jdbc.driver.OracleDriver • Microsoft: <ul style="list-style-type: none"> - com.microsoft.sqlserver.jdbc.SQLServerDriver
Description	The description of the JDBC driver.

Customer journey visualization

Context Store's audit trail data, when stored in the External Data Mart, can be used to produce a visualization of a Customer's journey. Each journeyElement displayed in the graph represents an individual interaction with the customer. Click on any icon to view the drill-down view of an interaction.

Context Store uses the ContextStoreQuery snap-in to request for customer data stored in an external data mart (EDM). The Context Store Customer Journey application, hosted on the ContextStoreQuery snap-in, uses the ContextStoreQuery API to retrieve the data from the EDM and visualize the data by contextId or groupId.

A multi session journey is when a groupId is used to link disparate contexts into a single journey. You can navigate through a multi session journey using interaction cards displayed at the bottom of the visualization. The interaction cards indicate the start and end of an interaction and the number and type of interactions.

The standalone Context Store Customer Journey application provides the option to choose between two data sources:

- The ContextStoreQuery Snap-in: Data is retrieved from an external database.
- Audit Trail: Audit trail metadata is retrieved from CS data grid.

The ContextStoreQuery snap-in has access to data at each interaction with a touchpoint. You can click the interaction points to view the data. Audit trail does not have access to the underlying data and shows only the touchpoints and timestamps.

Storing audit trail data in Context Store

To visualize the data stored in Context Store, you must associate a touchpoint with each operation on a context object.

For example, Post: `http(s)://clusterIP/services/ContextStoreRest/cs/contexts/?touchpoint=web`

Each interaction has a timestamp associated with it. If you enabled the External Data Mart (EDM) feature and the persistToEDM flag is set to True for a Context Store operation, the data at the time of each update is stored in the EDM database. The ContextStoreQuery snap-in can later retrieve the data stored in this manner.

Viewing customer interactions

The Customer Journey application provides the following options to view and filter customer data:

- Use the mouse wheel to zoom in and out. Zoom is centered at the mouse point.
- Click and drag the mouse pointer towards left or right to see information on a scrolling window.
- Hover the mouse pointer over an interaction to see a tooltip about the interaction.
- Click an interaction to view data. After a data card is opened, you can also filter the data..
- Click a touchpoint label to filter all associated interactions.
- Hover the mouse pointer over a path segment to see interval and data delta, if exists..
- Search interaction data using the input field..
- Timeline navigation cards are displayed below the timeline to aid navigation of interactions. You can:
 - Click these cards to bring the interactions for this session into view.
 - Click a selected card to deselect it and return to the original timeline view.

* Note:

- Zooming and panning are not enabled in the drilled-in view.
- The Customer Journey application cannot predict the distribution of interactions. Therefore, some interactions might overlap. The Customer Journey application provides timeline navigation cards and the zoom functionality to address this issue. The application retrieves data as stored in the database; users should use accordingly.

You can select the available date range to view the customer journey. The interactions from the previous 1 to 60 days can be viewed.

Each interaction point in the journey is indicated with a touchpoint icon. You can click a particular icon to view the details of the interaction.

* Note:

If the touchpoint is undefined for a specific Context Store operation, you cannot view the interaction details.

The visualization displays icons for the following touchpoints:

- Web
- Email
- Webvoice
- Voice
- Chat
- Social
- Survey
- Chatbot

- CRM
- SMS
- APP

When you use other touchpoints than those listed here, the Context Store Customer Journey application displays the first two letters of the touchpoint string instead of the icons.

Related links

[Viewing customer journey on a standalone Customer Journey application](#) on page 37

[Audit trail](#) on page 38

[Context Store Query](#) on page 19

Viewing customer journey on a standalone Customer Journey application

About this task

In this release, Google Chrome is the only supported browser for viewing customer journey on the standalone Context Store Customer Journey application.

Procedure

1. Go to `http(S)://clusterIP/services/ContextStoreQuery/`
2. On the top right of the Context Store UI, click the **Configuration** icon.
The Context Store Customer Journey application displays the Cluster Configuration window.
3. In the **Cluster IP** field, enter the IP address of your Context Store cluster.
4. Select **context Id** or **group Id**.
5. In the **Id** field, enter the appropriate Id for the data you want to view customer journey.
6. In the **Routing Id** field, enter the routingId of the context entry for which you want to view customer journey.
7. In the **Select Data Source** field, select **Audit Trail** or **ContextStoreQuery**.
From ContextStoreQuery, you can retrieve context data from each interaction point. Audit trail does not have access to the underlying data and shows only the touchpoints and timestamps.
For details on the usage of the Customer Journey application, see the “Viewing customer interactions” section.
8. Click **Save**.

Related links

[Customer journey visualization](#) on page 35

Context aliasId for additional indexing

You can use the Context alias feature to retrieve the same context object using alternative identifiers. Context aliasIds provide more flexibility in retrieving and updating context objects.

A context object can be indexed using the usual contextId and groupId. The object can also be indexed with context aliasIds such as a customer account number, a billing authorization number, and a mobile phone number. A customer object can be retrieved using any of these aliasIds to retrieve the context object.

Context aliasIds are subject to the same restrictions as all other context identifiers such as permissible characters, length, and must be unique in the data grid.

You can add up to three aliasIds for any one context object. In addition to defining aliasIds when a context object is first created, you can add and delete aliasIds post creation. For more information about adding, updating, or deleting an aliasId, see *Avaya Context Store Snap-in Developer Guide*.

Note:

If you add three aliasIds for a context, you must reduce your context data size to 1.5 KB to achieve the same capacity as that certified through performance tests. The performance tests test with 2KB context objects.

Each aliasId for a context must be unique within the context object, and the Context Store data grid. The same aliasId can exist in each cluster in a Geo solution, but the routingId distinguishes them from one another. Any attempt to duplicate an existing aliasId or retrieve a context using an unknown aliasId results in error messages.

The aliasing capability impacts the performance of Context Store, in particular latency, due to the increased number of lookups and data comparison required to find the correct object in the data grid. For more information, see [Capacity and scalability specification](#) on page 99.

Using aliasId as a request parameter

When creating a context, you can specify up to three aliasIds as parameters in the requests. For all other “by aliasId” operations, provide only the aliasId which identifies to the context on which an operation is to be executed.

For more information about the usage of the aliasId feature, see *Avaya Context Store Snap-in Developer Guide*.

Audit trail

With the Audit trail feature, you can find out a certain configured number of Context Store operations performed on a context during the lifecycle of the context. If you opt for the ContextStoreQuery snap-in, you can collect all associated context data from an external data mart (EDM) through ContextStoreRest interface. Using this interface, you can generate audit trails or retrieve instances of context data from the historical context data stored in the associated EDM.

Audit trail records all successful interactions with a context and stores the information inside the context object as an extra field. If you enable the Audit trail feature, you can find out which

application created or updated the context. You can also track the operation types, such as Create, Read, Update, Delete, and Upsert, that were performed on the context. The audit entry of a context also provides information such as the time at which the operations were performed and the version of the context.

After you enable the Audit trail feature, the ContextStoreRest API accepts touchpoint, which is any application that can interact with ContextStoreRest APIs, as a parameter for each interaction. The touchpoint parameter is an alphanumeric ID.

If you enabled the Audit trail feature, but did not provide the touchpoint parameter as part of the Rest URL, then the system still records the audit entry with the value `undefined`.

The versionId of a context increases with each interaction, such as Update, Get, Put, and Delete, with a context.

For more information about the touchpoint parameter, see *Avaya Context Store Snap-in Developer Guide*.

If you want to retrieve audit trail data from an EDM, you must configure the EDM database username and EDM database password in the system.

ReST URL paths

You can retrieve the audit entries of a context using the contextId or aliasId of the context. When you provide the correct parameters, the system displays the audit data. For example, the URL to retrieve audit data using contextId is `https://clusterIP/services/ContextStoreRest/cs/contexts/audit/{contextId}?rid={routingId}`. *Avaya Context Store Snap-in Developer Guide* has more detailed usage examples.

Setting a limit on audit entries

The number of audit entries for the context objects can reduce the number of contexts that you can store in the Context Store data grid. Therefore, you must set a limit on the number of audit entries that can exist for a context.

Setting the audit entry limit to 0 means that the audit feature is disabled. To enable the feature, set the number of audit entries for a context by selecting a value ranging between 1 and 50. If you set the limit to 10, then Context Store records the 10 most recent interactions as entries for the context. When the number of audit entries reaches the maximum limit, the system removes the oldest audit entry each time a new entry is added.

Note:

If you enable the Audit trail feature in a geo-redundant deployment, the CS Audit: Event limit attribute must be set identically in both clusters.

Audit trail and capacity planning

The number of audit entries configured for a context affects the size of the context object and the number of contexts in the data grid. Therefore, you must consider the size of the audit data trail while planning the Context Store capacity.

For more information about Audit trail and capacity planning, see *Avaya Context Store Snap-in Developer Guide*.

Related links

[Customer journey visualization](#) on page 35

[Context Store Query](#) on page 19

Upsert method

With the Upsert method, Context Store either updates an existing context with new data or creates a new context if it does not exist in the data grid. Combining the two operations into a single request reduces the number of API calls.

However, due to the nature of Upsert operations, it is computationally more expensive to complete an Upsert request than to do a single create or update request.

You can perform the Upsert operations using aliasIds. You can also set the lease time of a context with the Upsert method. Context Store applies the lease time that you provide to the context in both Create and Update operations.

Certain fields of the context metadata are immutable by design. You cannot modify the immutable fields of an existing context using the Upsert method. However, if you create a new context with the Upsert method, you can define the properties for the new context .

Note:

There is a performance consideration for Upsert that should be taken into account. A single Upsert operation is more computationally expensive than its corresponding POST or PUT request and can take up to three times longer to complete. Hence, if you are using the Upsert method, the total number of requests per second supported will be reduced as per the number of the Upsert request used per second.

For detailed usage information of Upsert operation, see the *Avaya Context Store Snap-in Developer Guide*.

Pluggable Data Connector

Context Store provides a Pluggable Data Connector (PDC) to integrate Avaya Aura® Experience Portal with the ContextStoreRest service. Experience Portal uses call flows created in Avaya Aura® Orchestration Designer. When you install the Context Store PDC in Orchestration Designer, a Context Store Connector node is available in Orchestration Designer. You can drag the Context Store Connector node into call flows to integrate Context Store into the flow.

You can also configure the Context Store Connector node to perform actions such as creating, getting, updating, or deleting context information using either contextId or aliasId. For more information on using the pluggable data connector, see *Avaya Context Store Snap-in Developer Guide*.

ContextStoreTasks Type for Engagement Designer

ContextStoreTasks Type is the service in Engagement Designer (ED) that interfaces with Context Store. Engagement Designer is an Avaya Breeze™ snap-in that business analysts and other non-developers can use to create workflow definitions that describe and execute business processes.

The ContextStoreTasks Type enables all the Context Store operations to be run from within a workflow in ED. You can perform Add, Update, Retrieve, and Delete operations for both contexts and values using ContextStoreTasks Type.

Note:

The ContextStoreTasks Type SVAR is compatible only with the same version Context Store and Engagement Designer.

For more information about installing ContextStoreTasks Type and performing CS operations using ContextStoreTasks Type, see *Avaya Context Store Snap-in Developer Guide*.

Authorization

Context Store provides authorized access to context data using the Avaya Breeze™ Authorization Service (AS) snap-in.

An administrator authorizes different user groups and applications with specific access levels. This user-privilege mapping is stored in the AS snap-in and a bearer token is generated for the user or application.

When the user or application requires access to Context Store, they must supply the authorization token with the Context Store request. If the user or application is accessing Context Store for the first time, the authorization token must be requested from the AS snap-in. When the Web Filter / Token Validator component of Context Store receives a request, it verifies the existence and validity of the authorization token. If the token exists in the ContextStore data grid, Context Store returns the data requested according to the access level that the user or application is granted

Privilege levels

Context Store supports two features or access levels: Privileged and Standard. For each feature, you can have four values:

Value	Definition
Create	Applies to all ContextStoreRest Post requests.
Delete	Applies to all ContextStoreRest Delete requests
Read	Applies to all ContextStoreRest Get requests
Update	Applies to all ContextStoreRest Put requests

Generating bearer tokens

Four Rest methods are available for generating bearer tokens.

Name	Rest method	URL	Headers
Get token	GET	https://clusterIP/ services/ ContextStoreRest/cs/ contexts/token/	
Get token by scope	GET	https://clusterIP/ services/ ContextStoreRest/cs/ contexts/token/scope/	scope
Get token by user	GET	https://clusterIP/ services/ ContextStoreRest/cs/ contexts/token/username/	<ul style="list-style-type: none"> • user name • password
Get token for user by scope	GET	https://clusterIP/ services/ ContextStoreRest/cs/ contexts/token/username/ scope/	<ul style="list-style-type: none"> • scope • user name • password

Related links

[Assigning permissions to an authorization client](#) on page 65

[ContextStoreRest attribute descriptions](#) on page 83

Scalability overview

Context Store provides scalability by supporting varied deployment types to suit all purposes.

The scalability feature facilitates the deployment of Context Store on Avaya Breeze™ nodes of varying sizes. You can deploy Context Store on a single node or on a cluster of up to five nodes. Deployments with single node or low resources are for non-mission-critical environments, such as customer trials and lab deployments. The scalability options are as follows:

- Scale Out feature: Provides customers the option to deploy Context Store on a single-node cluster or on a cluster containing from two nodes up to a maximum of five nodes.
- Scale Up feature: Supports incremental memory allocations for Avaya Breeze™ nodes and provides the option to store data in the grid for longer lease duration.

Related links

[Addition or removal of nodes overview](#) on page 43

[Scale out](#) on page 43

[Scaling out Avaya Breeze cluster](#) on page 44

[Scale up](#) on page 45

[Scaling up Avaya Breeze cluster](#) on page 46

Addition or removal of nodes overview

Context Store provides the option to add or remove Avaya Breeze™ nodes in the deployed Context Store setup. This feature is only supported in a multi-node cluster. You can add only one node at a time. When you add or remove nodes, ensure that:

- No traffic runs through the system
- No Geo replication is in operation

*** Note:**

Context Store does not support scaling out dynamically. After adding or removing a node to the cluster, you must shut down all the nodes and start the nodes simultaneously.

The resources of a node must be identical to the other nodes in the cluster. After adding a node and allocating resources to the node, you must manually update the cluster configuration in System Manager before shutting down the nodes. Updating the configuration ensures that the cluster utilizes the new resources.

*** Note:**

When adding or removing nodes, ensure that all external clients that you create or manage are able to handle the changes to capacity or throughput. The maximum requirements for the external clients and connections do not exceed the requirements in the previous Context Store releases. You must provide adequate bandwidth and performance for the external clients.

Related links

[Scalability overview](#) on page 42

Scale out

The Context Store Scale out feature allows you to have a single-node deployment or add additional nodes to an existing multi-node deployment. With an increase in the number of nodes and resources associated with the nodes, you can maintain contexts for longer lease duration or use nodes with smaller footprint to use the capacity.

*** Note:**

Context Store does not support scaling out dynamically. After adding a node to the cluster, you must shut down all the nodes and restart the nodes simultaneously.

By using the Scale out feature, you can:

- Deploy Context Store on one node only. In a single node deployment, load balancing is not enabled and therefore a cluster IP address is not required. Context Store uses the security module IP address of the node for traffic.
- Deploy Context Store on a cluster of two to five nodes. Context Store supports high availability in this configuration.
- Scale the clusters in Geo redundant deployments. Context Store clusters that are connected as part of a Geo deployment must contain the same number of nodes. All the nodes in both

the clusters must have the same amount of memory. If a node is added to one cluster, a replica node must be added to the second cluster.

For high availability, Context Store supports a maximum of one failed node regardless of how many nodes are assigned to the cluster. To avoid service interruption, the remaining nodes must be able to support the throughput and capacity of the contribution of the failed node.

Related links

[Scalability overview](#) on page 42

Scaling out Avaya Breeze™ cluster

Before you begin

Identify the cluster configuration that you want to achieve. For example, if your current cluster has three nodes of 64 GB each and, you wish to scale out to five nodes of 64 GB each, configure the following fields as per the requirements of a five-node cluster:

- ContextStore ManagerSpace DataGrid Settings
- ContextStoreSpace DataGrid Settings
- Context Store DataGrid type
- EDM: Mirror Service container size
- GEO: Gateway Service container size
- EDM: Mirror Service redo log size
- CS Threshold attributes

Ensure that all your nodes have identical resources, such as CPU, memory, and hard disk. For more information, see [Context Store deployment checklist](#) on page 53.

Procedure

1. Deploy a new Avaya Breeze™ node with the required CPU and memory configuration.
2. On the System Manager web console, click **Home** > **Elements** > **Avaya Breeze** > **Cluster Administration**.
3. Select the cluster that you want to scale out and select the **Deny New Service** state in the **Cluster State** list.
4. Select the cluster again and click **Edit**.
5. On the Cluster Editor window, go to the **Servers** tab.
6. Add the Avaya Breeze™ node from the **Unassigned Servers** list.
7. Click **Commit**.

The system prompts you to ensure that all Avaya Breeze™ server restarts are complete before placing the cluster into the **Accept New Service** state.

8. Click **OK**.

The system starts installing the assigned services to the newly added server.

9. Repeat this procedure for all the nodes.
10. Shut down all the nodes.
11. Power on all the nodes simultaneously.
12. On the **Cluster Administration** page, verify that the services are installed for the cluster.
13. Click **Show** on the new cluster to verify if the system has added the servers to the cluster.

The system displays the Avaya Breeze™ servers as part of the Context Store cluster.

14. Select the check box of the cluster.
15. From the **Cluster State** drop-down menu, select **Accept New Service**.
16. Click **Continue** in the **Accept New Service** dialog box.

The system displays the **Accepting** state in the **Servers State** column.

Related links

[Scalability overview](#) on page 42

Scale up

The Context Store Scale up feature provides the functionality to increase the memory allocations from 8 GB to 128 GB so that contexts can be stored in the data grid for longer lease durations. Ensure that all nodes in your cluster have identical resources, such as memory, CPU, and hard disks.

By using the Scale up feature, you can:

- Deploy Context Store on Avaya Breeze™ nodes that have memory ranging from 8 GB to 128 GB.
- Support production environments deployed on a cluster of Avaya Breeze™ nodes that have memory ranging from 16 GB to 128 GB.

* Note:

Context Store does not support single-node deployments for production environments as Context Store does not support high availability or Geo redundancy in single-node deployments.

- Support deployments with smaller footprints. You can deploy Context Store on Avaya Breeze™ nodes that have smaller CPU core allocations for non-mission critical environments.
- Support multiple options for hard disk allocations for the Avaya Breeze™ nodes in Context Store to facilitate deployments with reduced footprints and requirements. Large hard disks are not required for non-mission-critical environments as maintaining logs for long periods is not required. In addition, the quantity of logs is reduced as the supported throughput is lowered in such a deployment.

For more information about CPU, hard disk and memory allocations see the *Certified Deployments section in Avaya Context Store Snap-in Release Notes*.

Related links

[Scalability overview](#) on page 42

Scaling up Avaya Breeze™ cluster

Procedure

1. On the System Manager web console, click **Home** > **Elements** > **Avaya Breeze** > **Cluster Administration**.
2. Select the cluster that you want to scale up and click **Deny New Service** in the **Cluster State** list.
3. On the System Manager web console, click **Home** > **Elements** > **Avaya Breeze** > **Configuration** > **Attributes** > **Service Clusters** > **ContextStoreManager**.
4. Change the values in the following fields according to the cluster set up that you want to scale up to:
 - a. Change the values in the **ContextStore ManagerSpace DataGrid Settings** field.
 - b. Change the values in the **ContextStoreSpace DataGrid Settings** field.
 - c. Change the values in the **Context Store DataGrid type** field
 - d. Change the values in the **EDM: Mirror Service container size** field.
 - e. Change the values in the **GEO: Gateway Service container size** field.
 - f. Change the values in the **EDM: Mirror Service redo log size** field.
 - g. Change the values for the CS Threshold attributes.
5. Shut down all the Avaya Breeze™ nodes.
6. Using VSphere Client, increase the memory, hard disk and CPU allocations according to the deployment that you want to achieve .

*** Note:**

The CPU, hard disk and memory settings must be the same for all the nodes in the cluster. In a Geo redundant set up, both the clusters must be identical.

7. Power on all the nodes simultaneously.
8. Select the check box of the cluster.
9. From the **Cluster State** drop-down menu, select **Accept New Service**.
10. Click **Continue** in the **Accept New Service** dialog box.

The system displays the **Accepting** state in the **Servers State** column.

Example

Related links

[Scalability overview](#) on page 42

Chapter 3: Interoperability

Avaya product compatibility

The Context Store snap-in is compatible with the following Avaya products:

Avaya product	Version
Avaya Aura [®] System Manager	8.0
Avaya Breeze [™]	3.5
Avaya Aura [®] Experience Portal	7.2 and 7.2.1 (FP)
Avaya Aura [®] Orchestration Designer	7.2 and 7.2.1 (FP)
Avaya one-X [®] Agent	2.5, 2.5.2, 2.5.4, and 2.5.5
Intelligent Customer Routing	7.0.1
Avaya Engagement Designer	3.5
Avaya Oceana [™] Solution	3.5
Avaya Workspaces	3.5

Hardware requirements

This topic provides information about the Context Store hardware requirements. For information about the Avaya Breeze[™] requirements, see the *Interoperability chapter in Avaya Breeze[™] Overview and Specification*.

The requirements specified here are not applicable to all deployment options. For more information about the hardware requirements of the certified deployment scenarios, see *Certified Deployments section in Avaya Context Store Snap-in Release Notes*.

ESXi host server

Context Store supports a range of deployment options from a single node cluster to an Avaya Breeze[™] cluster with a maximum of five nodes. As a failover strategy to ensure maximum availability of the solution, Avaya recommends that at least two Avaya Breeze[™] servers be deployed. The servers must be on different VMware ESXi hosts. To guarantee service availability and to ensure high availability of the solution, it is recommended that three servers be used. If you install any or all three Avaya Breeze[™] servers on the same host, then the failure of the host impacts multiple Avaya Breeze[™] servers. The failure of multiple servers prevents Context Store

from using a backup server during failover and hence impacts the overall availability of the solution.

*** Note:**

The specifications provided here are for a reference implementation. This is the implementation on which Context Store's capacity and performance figures have been certified. Equivalent performance cannot be guaranteed in environments which do not meet the hardware and network requirements stated here.

- Processor: For the specified best performance, the processor should have at least 8 dedicated, non-hyper-threaded cores, equivalent to a 2.9 GHz Xeon processor.

To ensure that the Context Store solution can support published capacity figures and availability, Avaya recommends that you reserve the processor to achieve maximum traffic rate with low latencies, especially when Context Store is recovering from a failure. Without dedicated cores, Context Store competes with other Virtual Machines on the same VMWare ESXi host for crucial resources at times of maximum throughput or recovery, resulting in poor performance or loss of data.

- Hyper-Threading must not be enabled. Context Store does not support VM features that sub divide the processing power of the core, because it does not expect to have to compete with external processes during max capacity or failover where Context Store requires additional processing overhead to ensure no service interruption.
- vMotion must not be enabled: Context Store has not certified this feature, and hence it is recommended that this feature not be used during the running of Context Store.
- For best performance, Network should:
 - Support at least Gigabit Ethernet
 - Have a response time of less than 250 milliseconds between hosts.
 - Be able to handle a transfer rate of 48 mb/sec
 - Have all hosts on the same Data Center, on the same subnet and on the same high quality LAN, so no latencies are incurred in the solution.

*** Note:**

Use of VLAN is not recommended, because capacity testing executed on a VLAN environment resulted in poor performance. Frequent connection issues were also seen within the cluster, between geo-redundant clusters, and to an External Data Mart.

- Have a dedicated 1 GB channel with a minimum of 300 MB bandwidth being available for Session Replication between the Context Store clusters, if Context Store's Geo Redundancy feature is used.
- Storage: Must at least be 15000 RPM SATA hard disks.

Guest virtual machines

*** Note:**

The specifications provided here change according to the deployment. For the details about certified deployment scenarios, see *Certified Deployments section in Avaya Context Store Snap-in Release Notes*.

Each guest virtual machine for Context Store must meet the following criteria, which is dependent on the deployment scenario. For details about the Avaya tested hardware requirements based on

the deployment scenarios, see *Certified Deployments section in Avaya Context Store Snap-in Release Notes*.

- Processor: 4 to 8 dedicated cores
 - All Context Store nodes in production environment require 8 dedicated, non-hyper-threaded cores. The CPU resource reservation must be at least 18960 MHz for each node. If Profile 1, 2, or 3 is selected when deploying the Avaya Breeze™ OVA, the CPU reservation must be increased manually by editing the virtual machine settings after deployment.
- RAM: 8 to 128 GB RAM
- Hard disk: 50 GB to 300 GB

 **Important:**

If you use a SAN, the performance of the SAN must meet the above specifications.

Each guest virtual machine must also be thick provisioned and be on the same subnet.

Software requirements

The Context Store software requirements are based on the Avaya Breeze™ and System Manager requirements. For information about Avaya Breeze™ requirements, see the *Interoperability chapter in Avaya Breeze™ Overview and Specification*. For information about Avaya Aura® System Manager requirements, see *Deploying Avaya Aura® System Manager in Virtualized Environment*.

Chapter 4: Licensing

License requirements

Use of the Context Store software requires a valid Context Store license file and Avaya Breeze™ license file.

Context Store uses the snap-in service licensing feature provided by Avaya Breeze™. All Context Store SVAR files contain a digital signature which is verified by the Avaya Breeze™ Element Manager.

Platform and snap-in licenses must be installed on the WebLM server of System Manager, which manages the Platform and snap-in licenses.

A single license, containing information for each licensed feature, applies to all Context Store snap-in services.

Note that the following Context Store features have additional associated license costs:

- Context Store GEO Redundancy
- Context Store Java SDK
- ContextStoreScreenPop

Configuring Context Store licenses

Before you begin

- Ensure that you have obtained the Context Store license from Avaya PLDS.
- Ensure that the Avaya Breeze™ license is installed on System Manager.

In System Manager, click **Elements > Avaya Breeze > Server Administration** to see the current status of each Avaya Breeze™ server platform license.

About this task

This task provides information about configuring Context Store license in System Manager.

Procedure

1. On the System Manager Home page, select **Services > Licenses**.
2. Select **Install License**.
3. Browse to the location of the Context Store license.

4. Select the license file and click **Install**.

The system installs the license file.

In the left navigation pane, the system displays CONTEXT_STORE under **Licensed Products**.

5. To verify if the license file is installed successfully:
 - a. Click **Elements > Avaya Breeze > Service Management > Services**.
 - b. In the **License mode** column, verify that the column displays a check mark for the Context Store node.

The following licensing modes apply to all Avaya Breeze™ and Context Store licenses

- Normal: Context Store has a valid license file for normal operation of Context Store.
- Error: Context Store is operating in 30 day grace period. All the functionalities of Context Store are still available. However, to get Context Store back to the normal mode, you must install a valid license file before the grace period expires.
- Restricted: Context Store has exceeded its 30 day grace license period and has no access to Avaya Breeze™.

For more information on licensing modes and licensing for Avaya Breeze™, see the Avaya Breeze™ documentation.

Avaya Breeze™ licensing audit runs every 9 minutes. Any license changes including install or uninstall actions on the WebLM server takes time to reflect on the user interface. The latest license information thus takes a maximum of 9 minutes to reflect in the Avaya Breeze™ Element Manager.

Chapter 5: Context Store Deployment

Certified deployment scenarios

Avaya provides 13 tested/certified deployment scenarios for Context Store, in addition to sizings certified for the Avaya Oceana™ Solution. The hardware requirements, number of nodes, supported features, settings, and capacity specifications differ as per the deployment scenarios.

The support for additional features, such as, AliasIds, ContextStoreNotify, Audit trail, Geo redundancy, External Data Mart, and Event streams, is dependent on the hardware resources allocated to the cluster.

*** Note:**

The additional memory resources required for the Event Streams feature are not included in these figures. If this optional feature is deployed, the ContextStoreSpace DataGrid size must be reduced by 6GB.

This document provides the minimum hardware requirements required for the External Data Mart, Geo Redundancy, and ContextStoreNotify features.

Related links

[Capacity and scalability specification](#) on page 99

Key customer configuration information

This topic lists the information that you must have before you install and configure the Context Store snap-in services.

You need the following information to install and configure the Context Store snap-in services. Record the information in this worksheet before beginning the installation.

Requirement	Notes	Your value
The name of the Context Store SVAR files that are available on PLDS.		
The location of the Context Store SVAR files that you have downloaded from PLDS.		

Table continues...

Requirement	Notes	Your value
The instances of Avaya Breeze™ in System Manager, on which you plan to install Context Store. These Avaya Breeze™ servers must be dedicated for Context Store.		
The IP address of the cluster	The Cluster IP must be on the same subnet as the Security Module IP of the Avaya Breeze™ instances. Do not specify the IP address of any of the Avaya Breeze™ servers that you plan to add to the cluster. * Note: For single node deployments, you do not require the IP address of the cluster.	
Digital certificates for authentication using mutual TLS	For more information about certificates and authentication, see the <i>Security</i> chapter in this document.	
Identify the configuration attributes for the Context Store services	For more information about configuring attributes, see the chapter <i>Administering Context Store</i> .	

Context Store deployment checklist

* **Note:**

ContextStore space fails to deploy if you try to contact an EDM with incorrect login details or there are connection issues. If this happens, you must disable the **EDM: Enable provisioning from database** field and enable the field again after providing correct login details.

Task	Notes	✓
<ul style="list-style-type: none"> Identify the Avaya Breeze™ servers to use in the Context Store cluster. Ensure that the Avaya Breeze™ servers are synchronized Ensure that the Avaya Breeze™ servers have passed the Avaya Breeze™ tests. Ensure that the Avaya Breeze™ license is installed on System Manager. Ensure that the NMS server is configured with System Manager as the target SNMP Profile. 	<p>Verifying the status of Avaya Breeze servers on page 57</p> <p>For more information about creating and managing SNMP target profiles, see <i>Administering Avaya Aura® System Manager</i> available at http://support.avaya.com.</p>	
<ul style="list-style-type: none"> Register the fully qualified domain names (FQDNs) of System Manager, Avaya Breeze™ host names, and security IP address with the domain name system (DNS) server. Ensure that System Manager can resolve the host name of the Avaya Breeze™ servers. 		
Download the Context Store snap-in services.	For more information, see <i>Avaya Context Store Snap-in Release Notes</i> .	
Download the Context Store license.	For more information, see <i>Avaya Context Store Snap-in Release Notes</i> .	
Load the required SVAR files in System Manager:	For more information, see Loading a snap-in service on page 57.	
<p>If you plan to use an External Data Mart:</p> <ul style="list-style-type: none"> Set up an external database on a separate server. The external database must meet the Context Store requirements. Create the database tables for the External Data Mart feature. 	<p>Database requirements and planning on page 26</p> <p>Creating database tables for External Data Mart on page 27</p>	
<p>Define a cluster from the Avaya Breeze™ > Cluster Administration page in System Manager, and assign the instances of Avaya Breeze™ to the cluster.</p>	<p>The system installs the ContextStoreManager service when you create a cluster.</p> <p>The system also installs the selected optional services, which you add to the cluster deployment.</p> <p>For more information, see Setting up a cluster on page 58.</p>	

Table continues...

Task	Notes	✓
Configure the ContextStore ManagerSpace DataGrid Settings , ContextStoreSpace DataGrid Settings and other ContextStoreManager and ContextStoreRest attributes of the services in the System Manager Service Clusters tab.	<p>! Important:</p> <p>If you plan to use External Data Mart or GEO redundancy features, to avoid the need to restart the cluster, configure the applicable data grid type before adding servers to a new cluster as this cannot be changed dynamically once the data grid has been deployed on the servers.</p> <p>! Important:</p> <p>If you plan to use the external data mart feature, configure</p> <p>If you plan to enable the Geo redundancy feature, see Enabling geo redundancy on page 66.</p> <p>For more information, see ContextStoreManager attribute descriptions on page 76.</p>	
Load the Context Store license in System Manager.	Configuring Context Store licenses on page 50	
Optional: Manually install the ContextStoreScreenPop services.	ContextStoreScreenPop is an optional service. You can manually deploy this service to the cluster after the initial installation of mandatory services. Installing a Context Store service on page 64	
Optional: Configure the ContextStoreScreenPop attributes in System Manager.		
Optional: Manually install the ContextStoreNotify services.	ContextStoreNotify is an optional service. You can manually deploy this service to the cluster after initial installation of mandatory services. Installing a Context Store service on page 64	
Optional: Configure the ContextStoreNotify attributes in System Manager.		

Table continues...

Task	Notes	✓
Optional: Manually install the Streams services.	Event streams is an optional service. You can manually deploy this service to the cluster after the initial installation of mandatory services. Installing a Context Store service on page 64	
Optional: Configure the Streams attributes in System Manager.	ContextStoreManager attribute descriptions on page 76	
Optional: Manually install the ContextStoreRules services.	ContextStoreRules is an optional service. You can manually deploy this service to the cluster after the initial installation of mandatory services. Installing a Context Store service on page 64	
Optional: Configure the ContextStoreRules attributes in System Manager.	ContextStoreRules page field descriptions on page 87	
Optional: Deploy PDC on Orchestration Designer.	PDC Plug-in deployment overview on page 70	
Optional: Manually install the ContextStoreSoap snap-in.	ContextStoreSoap is an optional service. You can manually deploy this service to the cluster after the initial installation of mandatory services. Installing a Context Store service on page 64	
Optional: Configure the ContextStoreSoap attributes in System Manager.		
Context Store Standalone - Optional: Oceana - Mandatory: Manually install the ContextStoreQuery snap-in.	ContextStoreQuery is an optional service for Context Store standalone, it is a mandatory service for Oceana. You can manually deploy this service to the cluster after the initial installation of mandatory services. Installing a Context Store service on page 64	
On installation of ContextStoreQuery - mandatory: Configure the ContextStoreQuery attributes in System Manager.	The correct configuration must be configured for ContextStoreQuery (e.g. correct database username and password). Failure to do so will result in errors in the system.	
Verify the installation.	Verifying a successful deployment on page 65.	
Optional: Verify the installation of optional services.	Verifying a successful deployment on page 65.	

Verifying the status of Avaya Breeze™ servers

Before you begin

Identify the Avaya Breeze™ servers on which you plan to install the snap-in services.

About this task

This topic provides the basic procedures for verifying the status of the Avaya Breeze™ servers. For detailed procedures, see *Deploying Avaya Breeze™*.

Procedure

1. Ensure that the Avaya Breeze™ servers are in the synchronized state:
 - a. On the System Manager web console, navigate to **Home > Services > Replication**.
 - b. Locate the Avaya Breeze™ node in the **Replica Group** list.
 - c. In the **Synchronization Status** column, verify that the Avaya Breeze™ status is **Synchronized**.

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

2. Ensure that the Avaya Breeze™ servers are passing the tests:
 - a. On the System Manager web console, click **Elements > Avaya Breeze > System Tools > Maintenance Tests**.
 - b. Select the Avaya Breeze™ servers and perform all tests.
 - c. Ensure that all tests are successful.
3. On the System Manager web console, click **Elements > Avaya Breeze > Server Administration**.

Ensure that:

- For the Avaya Breeze™ servers the **System State** column displays the **Denying** state.
- The **License Mode** column displays a green check mark.

Loading a snap-in service

Procedure

1. On the System Manager web console, click **Home > Elements > Avaya Breeze > Service Management > Services**.
2. Click **Load**.
3. On the Load Service window, click **Choose File**.
4. Select the snap-in service svar file that you want to load.

5. Click **Load**.

The system displays the Accept End User License Agreement window.

6. Click **Accept**.

Configuring a cluster and installing mandatory services

Before you begin

- Identify the Avaya Breeze™ servers on which you plan to install Context Store. These servers must be dedicated to Context Store only.
- Add the Avaya Breeze™ servers to System Manager. For more information, see *Deploying Avaya Breeze™*.
- Verify the status of the Avaya Breeze™ servers.
- Ensure that System Manager can resolve the host name of the Avaya Breeze™ servers. Register the fully qualified domain names (FQDNs) of System Manager, Avaya Breeze™ host names, and security IP address with the domain name system (DNS) server.
- Download the following Context Store SVAR files from PLDS:
 - ContextStoreManager
 - ContextStoreRest

*** Note:**

For more information about downloading the software from PLDS, see *Deploying Avaya Breeze™*.

About this task

This topic provides information about setting up an Avaya Breeze™ cluster for Context Store and installing the ContextStoreManager and ContextStoreRest services. ContextStoreRest is not a mandatory service, but is required if you need to interact with the data grid that ContextStoreManager deploys.

The cluster provides high availability and scaling by distributing the services across multiple Avaya Breeze™ servers. With this distribution of services, the system achieves throughput and avoids interruption if a failure occurs. The clients access the services through a cluster IP address that supports high availability. For more information about clustering, see *Deploying Avaya Breeze™*.

*** Note:**

You can enable load balancer only after adding nodes to your Context Store cluster.

Procedure

1. On the System Manager web console, click **Elements > Avaya Breeze > Service Management > Services**.
2. On the Services page, load the mandatory service ContextStoreManager. For more information about loading a service, see *Administering Avaya Breeze™*.

3. On the System Manager web console, click **Elements > Avaya Breeze > Cluster Administration**.
4. On the **Cluster Administration** page, click **New**.
5. Enter the following details for the cluster in the **General** tab of the **Cluster Editor** page:
 - **Cluster Profile:** Select **Context Store** from the drop-down menu.
 - **Cluster Name:** Enter a unique cluster name. The name can be any string such as ContextStore.
 - **Important:**
 - Ensure that no spaces are included in string.
 - **Cluster IPv4:** The Cluster IP must be on the same subnet as the Security Module IP of the Avaya Breeze™ servers. Ensure that you do not specify the IP address of any of the Avaya Breeze™ servers that you plan to add to the cluster.
 - **Note:**
 - For single node deployments, do not enter the IP address of the cluster. Requests must instead be submitted directly to the Security Module IP address of the node.
 - **Description:** Enter a description for the cluster.
6. In the **Cluster Attributes** section, specify the attributes for the cluster that you are creating.

For more information about the cluster attributes, see the topic *Cluster attributes field descriptions*.
7. On the **Cluster Editor** page, select the **Services** tab.

The system displays the Context Store services that you have loaded and configured through the Services page.

By default, the system automatically adds the mandatory service, ContextStoreManager, to the **Assigned Services** list. The **Available Services** list displays the optional services that are available for you to add to the Context Store cluster. Ensure that you configure the optional services and then attempt to install the optional services.
8. Click **the plus sign (+)** on any service in the **Available Services** list to add the service to the cluster.
9. Click **Commit**.

The system prompts you to ensure that all Avaya Breeze™ server restarts are complete before placing the cluster into the **Accept New Service** state.
10. Configure the attributes of the ContextStoreManager service.

For more information about configuring attributes, see the chapter *Administering Context Store*.
11. Configure the required and applicable attributes of the Context Store services.

12. On the **Cluster Editor** page, select the **Servers** tab.

The system displays all Avaya Breeze™ servers in the **Unassigned Servers** section.

13. Add the three identified Context Store nodes to the Context Store cluster.

Click the plus sign (+) on the node to add the node to the cluster.

The system adds the Avaya Breeze™ servers to the **Assigned Servers** section.

14. Click **Commit**.

15. Click **OK**.

16. On the **Cluster Administration** page, verify that the services are installed for the cluster.

17. Click **Show** on the new cluster to verify if the system has added the servers to the cluster.

18. Select the check box of the new cluster.

19. From the **Cluster State** drop-down menu, select **Accept New Service**.

20. Click **Continue** in the **Accept New Service** dialog box.

The system displays the **Accepting** state in the **Servers State** column.

Next steps

Install optional services.

Enable the installed optional services.

Related links

[Cluster attributes field descriptions](#) on page 60

Cluster attributes field descriptions

For more information about setting cluster attributes, see the *Administering Avaya Breeze™*.

Basic Attributes




Name	Description	Default value	Change to
Cluster Profile	Type of profile for the cluster.	Not selected	Context Store  Important: Ensure that you set this value to Context Store.

Table continues...

Name	Description	Default value	Change to
Cluster Name	Name of the cluster	None	Any name describing the cluster.  Important: Ensure that no spaces are included in string. This field is mandatory.
Cluster Group	Select the cluster group from the drop-down list.		
Cluster IPv4	IP address for the cluster	None	The designated cluster IP for this Context Store cluster. This field is mandatory for the Load Balancing feature.  Note: This field is not applicable for a single-node deployment.
Cluster Fully Qualified Domain Name			
Enable Cluster Database	This check box is disabled by default. Not applicable to Context Store.	Not set	You must not select this check box.
Enable Database Auto Switchover	This check box is selected by default. Not applicable to Context Store.	Set	Do not update.
Description		None	Any text describing the cluster. This field is optional.

Cluster Attributes

Name	Description	Default value	Change to
Authorization Service Address		None	Do not update

Table continues...



Name	Description	Default value	Change to
Default SMS Connector Service			
Grid Heap Size for LU		-Xms64m -Xmx256m	Xms64m -Xmx384m
Grid password	Specify a password for grid security.	None	
Use secure grid?	If selected, grid security is enabled.	Not set	
HTTP or HTTPS limit on connections	Number of http/https connections.	3000	Do not update
HTTP or HTTPS traffic rate limit in bytes/sec	Http/https traffic rate in bytes per second.	4000000	Do not update
HTTP Load Balancer backend server max failure response timeout period (seconds)		15	Do not update
Max number of failure responses from HTTP Load Balancer backend server		2	Do not update
Network connection timeout to HTTP Load Balancer backend server (seconds)		10	Do not update
Only allow secure web communications		Enabled	The administrator or user can decide whether to disable this attribute or leave it as enabled.
Is Load Balancer enabled?	<p>Select this check box to enable load balancing for the cluster.</p> <p>If you do not select this check box, load balancing will not be available on the cluster.</p> <p> Note:</p> <p>You must enable load balancer only after adding nodes to your Context Store cluster.</p>	Not set	<p>Select check box to enable the load balancer.</p> <p>You must enable the check box.</p> <p> Note:</p> <p>This field is not applicable for a single-node deployment.</p>

Table continues...

Name	Description	Default value	Change to
Is session affinity enabled?	Not applicable to Context Store.		Do not update
Trusted addresses for converting to use X-Real-IP for session affinity	Not applicable to Context Store.		Do not update
The maximum number of Avaya Breeze servers allowed in a Cluster	Max number of Avaya Breeze servers allowed in an a cluster. This field is not editable.	5	
Default identity for special make call cases			
Media server shuffle out timer (seconds)			
Limit on the memory (GB) to allocate for base processes			
Percent of memory to allocate base processes			
Percent of memory to allocate for WAS			
Limit on the memory (GB) to allocate for WAS			
Minimum TLS Version for Non-SIP Traffic			
Minimum TLS Version for SIP Call Traffic			
List of required snap-ins including minimum version	Lists snap-ins required for a Context Store cluster. This field is not editable.	"ContextStoreManager-1.0.0.0",	
Default SIP Domain	Not applicable to Context Store.		Do not update
Use secure signaling for platform initiated SIP calls	Not applicable to Context Store.		
Preferred Minimum Session Refresh Interval (secs)	Not applicable to Context Store.		Do not update

Table continues...

Name	Description	Default value	Change to
Use early pre-answer media?	Not applicable to Context Store.		Do not enable
Use short replication interval?	Not applicable to Context Store.		Do not enable

Related links

[Configuring a cluster and installing mandatory services](#) on page 58

Installing the optional Context Store services

Before you begin

Download the optional services that you want to install from PLDS.

Record the information mentioned in the [Key customer configuration information](#) on page 52.

About this task

Two approaches to installing optional services are as follows:

- Deploy the optional services manually after creating a cluster.
- Deploy the optional services as part of creating a cluster.

This task provides basic details about manually installing the optional Context Store snap-in services. For detailed procedures about installing snap-in services, see *Deploying Avaya Breeze™*.

* Note:

The mandatory snap-in service, ContextStoreManager, is installed when you create a cluster.

Procedure

1. On the System Manager web console, click **Elements > Avaya Breeze**.
2. In the left navigation pane, click **Service Management > Services**.
3. On the **Services** page, select and load the optional Context Store services. For more information about loading a service, see *Administering Avaya Breeze™*.
4. On the **Services** page, select and install the Context Store service.
For more information about installing a service, see *Administering Avaya Breeze™*.
5. Configure the attributes of the Context Store services as described in [Configuring attributes for a service](#) on page 76.

Verifying a successful deployment

Procedure

Open your web browser and type the following URL:

```
https://clusterIP/services/<Service name>/
```

Where:

- *clusterIP* is the IP address of the Context Store cluster where the service that you want to verify is running
- *<Service name>* is the service that you want to verify: For example, ContextStoreManager.

* Note:

You must enter the service names as they are displayed in the **Name** column on the Service Management page.

Ensure that you have configured certificate authentication on the browser. For more information, see [Certificate-based authentication](#) on page 102.

The web browser displays a confirmation message if the service that you are trying to verify is successfully installed in the specified cluster. If you are verifying ContextStoreRest service, On the ContextStoreRest service's verification page, the API's documentation and live test client is available.

Assigning permissions to an authorization client

Before you begin

- Configure LDAP user and synchronize it with System Manager
- Import LDAP server certificate.

For more information about configuring LDAP user, synchronizing the user with System Manager, and importing LDAP server certificate, see *Deploying Avaya Oceana™ Solution*.

Procedure

1. On the System Manager web console, click **Home > Elements > Avaya Breeze > Configuration > Authorization**.

The system displays the Authorization Clients tab.

2. Select the CS cluster name and click **Edit Grants**.
3. Click **New**.

The system displays the Create Grants for Authorization Client: <client name> screen.

4. Select the resource from the **Resource Name** drop-down list.
5. Select the version of the resource cluster from the **Resource Cluster** drop-down list.

6. Select the feature that the resource cluster wants to advertise from the **Feature** drop-down list.
7. Click the **Select** check box corresponding to the value you want to select.
8. Click **Commit**.

Related links

[Authorization](#) on page 41

[ContextStoreRest attribute descriptions](#) on page 83

Geo redundancy and External Data Mart deployment

The Geo redundancy and External Data Mart features have no dependencies or restrictions on each other; either or both of these optional features can be enabled on a Context Store cluster.

To use the Geo redundancy feature, you must:

1. Manage the Context Store clusters from the same System Manager.
2. Individually enable Geo redundancy for each cluster in the Context Store set up.
3. Allocate identical resources to the clusters in a geo-redundant deployment.

For more information, see [Enabling Geo redundancy in Context Store](#) on page 66.

To use the External Data Mart feature, you must:

1. Identify and configure the external database to which context data is saved.
 2. Individually enable the External Data Mart for each cluster in the Context Store set up.
- For the External Data Mart connection, **EDM: Enable Persistence to database**
 - For the Geo-Redundancy connection, **GEO: Enable session preservation**

For more information, see [Enabling External datamart in Context Store](#) on page 68.

To use Context Store without Geo redundancy and External Data Mart, follow the procedure mentioned in [Configuring a cluster and installing mandatory services](#) on page 58.

Related links

[Enabling Geo redundancy in Context Store](#) on page 66

[Enabling External Data Mart persistence](#) on page 68

[Enabling External Data Mart provisioning](#) on page 69

Enabling Geo redundancy in Context Store

Before you begin

- Ensure you have configured two Context Store clusters.

- Create and download the keystore, from the **Security > Certificate > Authority** page in the System Manager web console. For more information about certificates, see the *Certificate Based Authentication* chapter in the *Avaya Context Store Snap-in Developer Guide*.

About this task

This topic provides information about enabling session preservation and thereby achieve Geo redundancy in Context Store. The same keystore certificate is applied to both clusters.

You must perform this procedure on each Avaya Breeze™ node in both the Context Store clusters.

Procedure

1. To configure secure data replication between clusters, put the keystore certificate in `/opt/Avaya/dcm/gigaspace/security/` directory of each Avaya Breeze™ node in both clusters:

The certificate enforces SSL encryption on the replication channel. For more information about the certificate based authentication and creation of the keystore certificate, see *Avaya Context Store Snap-in Developer Guide*.

* Note:

The replication does not work without the SSL encryption.

If an Avaya Breeze™ node is upgraded or redeployed, the configuration steps for Geo redundancy security must be repeated.

2. Enable the Geo redundancy feature and configure attributes:
 - a. On the System Manager web console, click **Elements > Avaya Breeze > Configuration > Attributes**.
 - b. Select **Service Clusters** and select the cluster and the service **ContextStoreManager** from the drop-down list of services.
 - c. Enter `true` in the **GEO: Enable session preservation** field.
 - d. Configure all the other geo redundancy attributes in the **Geo Redundancy Configuration** group.
3. Configure the ContextStoreManager service data grid:

* Note:

The **ContextStore DataGrid Type** attribute must be set to GEO or PROVISIONED-GEO to use the Geo Redundancy feature. EDM provisioning is an optional Context Store feature. To learn more about this feature, see *External Data Mart Provisioning* section in this document.

- a. Set the applicable values for **DataGrid Settings** and **Gateway Service container size** for the deployment size

See the *Certified Deployments* section in *Avaya Context Store Snap-in Release Notes* for applicable values.

- b. Click **Commit**.

4. If necessary, restart all the Avaya Breeze™ servers in the Context Store cluster.

*** Note:**

Cluster restart is required only if the DataGrid type has changed. All other geo-redundancy-related configuration is dynamic and can be updated by disabling, updating, and then re-enabling the feature.

5. Enter `true` in the **Cluster Deny Service on two node outage** field if Geo load balancer is configured to automatically detect a compromised cluster.
6. Repeat these steps on the second cluster.

Next steps

After you configure and restart the second Context Store cluster, confirm that replication is active between both the Context Store spaces by creating a context object in one cluster and retrieving the context object from the other cluster.

*** Note:**

If you must restart a cluster, clear the **Cluster Deny Service on two node outage** check box before the restart. To enable the attribute, select the **Cluster Deny Service on two node outage** check box again after the restart. If you enable the Cluster Deny Service on two node outage attribute before the other nodes have started up and joined the cluster, the action triggers throttling on the cluster.

Configure the load balancer for geo redundancy.

Related links

[Geo redundancy and External Data Mart deployment](#) on page 66

[Third party load balancer configuration requirement](#) on page 92

Enabling External Data Mart persistence

Before you begin

Ensure that you create the database table(s) before enabling the External Data Mart feature. For more information about creating database tables, see [Creating database tables for External Data Mart](#) on page 27

Procedure

1. On the System Manager web console, click **Elements > Avaya Breeze > Configuration > Attributes**.
2. Click the **Service Clusters** tab.

*** Note:**

To use only one EDM in the geo-redundant solution, you must disable EDM from the other cluster in the **Service Cluster** tab.

3. From the **Service** drop-down menu, select **ContextStoreManager**

4. Enter `true` in the **EDM: Enable Persistence to database** field.
5. Configure the other EDM attributes. All attributes related to External Data Mart configuration are prefixed with **EDM:**.
6. Configure the ContextStoreManager service data grid:
 - a. Set the applicable values for **DataGrid Settings** and **Mirror Service container size** for the deployment size

See the *Certified Deployments* section in *Avaya Context Store Snap-in Release Notes* for applicable values.
 - b. Click **Commit**.

Next steps

Confirm that the external data mart is active by creating a context object in the cluster and verifying that it has been written to the database.

Related links

[Geo redundancy and External Data Mart deployment](#) on page 66

Enabling External Data Mart provisioning

Before you begin

Ensure that you create the database table(s) before enabling the External Data Mart provisioning feature. For more information about creating database tables, see [Creating database tables for External Data Mart](#) on page 27

About this task

You cannot enable the EDM provisioning feature at runtime. You must restart the cluster to redeploy the data grid with the updated configuration.

Note:

EDM: Enable Provisioning from database is an optional attribute. Provisioning is a separate, optional EDM feature than EDM Persistence (which is used for Customer Journey).

Procedure

1. On the System Manager web console, click **Elements > Avaya Breeze > Configuration > Attributes**.
2. Click the **Service Clusters** tab.
3. From the **Service** drop-down menu, select **ContextStoreManager**
4. Enter `true` in the **EDM: Enable Provisioning from database** field.
5. Configure the other EDM attributes. All attributes related to External Data Mart configuration are prefixed with **EDM:**.

6. Configure the ContextStoreManager service data grid:
 - a. Set the applicable values for **DataGrid Settings**, **EDM: Mirror Service redo log size**, and **Mirror Service container size** for the deployment size.

See the *Certified Deployments* section in *Avaya Context Store Snap-in Release Notes* for applicable values.
 - b. Click **Commit**.
7. If necessary, restart all the Avaya Breeze™ servers in the Context Store cluster.

 **Note:**

Cluster restart is required only if the DataGrid type has changed. All other geo-redundancy-related configuration is dynamic and can be updated by disabling, updating, and then re-enabling the feature.

Next steps

Confirm that the provisioning was successful by using ContextStoreRest to retrieve a context object from the data-grid, that existed in the CS_PROVISION table in the database.

Related links

[Geo redundancy and External Data Mart deployment](#) on page 66

Deploying Context Store PDC on Orchestration Designer

Before you start deploying PDC on Orchestration Designer, ensure that you have:

- Installed Orchestration Designer 6.0 or later in the system where you want to deploy Context Store PDC. The Orchestration Designer software is available on <http://www.avaya.com/devconnect>.
- The latest Context Store PDC. The Context Store PDC is available on Avaya DevConnect Program at http://www.devconnectprogram.com/site/global/products_resources/avaya_breeze/avaya_snap_ins/context_store/overview/index.gsp.
- The sample application that uses the Context Store PDC. The sample application is available on Avaya DevConnect Program at http://www.devconnectprogram.com/site/global/products_resources/avaya_breeze/avaya_snap_ins/context_store/overview/index.gsp.

You must also ensure that the machine where you plan to install Context Store PDC can resolve the cluster IP address. If DNS is not set up in the machine, you must add the cluster IP address in the *hosts* file.

For more information about Orchestration Designer, see *Avaya Aura® Orchestration Designer Developer's Guide*.

For more information about installing and using the PDC, see *Avaya Context Store Snap-in Developer Guide* available on <http://www.avaya.com/devconnect>.

Avaya Context Store Snap-in Developer Guide provides detailed information about the following tasks:

- Configuring Orchestration Designer to use Tomcat.
- Configuring certificates for the Context Store PDC.
- Running the Test project.
- Configuring the Context Store PDC.
- Using the Context Store connector in the workflow.
- Creating the variables and getting the output variables.

Deploying ContextStoreTask Type

Overview of ContextStoreTasks Type deployment

Before you install ContextStoreTasks Type for Engagement Designer, ensure that you have:

- Context Store.
- Engagement Designer.

*** Note:**

The Engagement Designer cluster and the Context Store cluster must be managed by the same System Manager.

Install Engagement Designer into the General Purpose cluster. For more information about installing Engagement Designer, see *Avaya Engagement Designer snap-in Reference*.

*** Note:**

If the Engagement Designer cluster has multiple nodes, you must select the **Is session affinity enabled?** check box for the Engagement Designer cluster while creating the cluster.

Engagement Designer, ContextStoreTasks Type is an SVAR file. When the Engagement Designer cluster has reached the Installed state, upload the ContextStoreTasksType Bundle through the Engagement Designer Administration console.

For more information about accessing the Engagement Designer Administration or Design consoles, see *Getting Started with Avaya Engagement Designer*.

Related links

[Context Store deployment checklist](#) on page 53

Installing ContextStoreTasks Type SVAR on Engagement Designer

Before you begin

Deploy Engagement Designer.

Procedure

1. Download the ContextStoreTasks Type SVAR file from PLDS.
2. Open the following URL in a web browser.

```
https://Applicable-ED-IP-ADDRESS/services/EngagementDesigner/admin.html
```

For more information on accessing the Engagement Designer Admin console, see *Getting Started with Avaya Engagement Designer*.

3. Click the Bundles tab.
4. Click **Upload Bundle**.
5. Click **Choose File**.
6. Browse and select the ContextStoreTasks Type SVAR file.
7. Click **Upload**.

The system uploads the file.

 **Note:**

Uninstall any older versions of ContextStoreTasks Type before proceeding with the next step.

8. Click the check box corresponding to the ContextStoreTasks Type SVAR file and click **Deploy Bundle**.

You should now be able to see the Context Store bundle in the Engagement Designer Design console.

Context Store Upgrade overview

To upgrade a Context Store snap-in service in Avaya Breeze™ you must install a new version of the snap-in service. For detailed procedure and information about upgrading various Context Store snap-in services, see *Avaya Context Store Snap-in Release Notes*.

Context Store uninstallation and deletion

Context Store uninstallation overview

The options are:

- Delete a Context Store cluster: To uninstall the mandatory Context Store services (ContextStoreManager), you must delete the Context Store cluster.
- Uninstall a snap-in service: For optional snap-in services, you can uninstall a service snap-in: When you uninstall a service, the system does not remove the attributes from the Avaya Breeze™ PostgreSQL database.
- Delete a snap-in service: When you delete a service, the system removes the attributes from the Avaya Breeze™ PostgreSQL database.

 **Note:**

To completely uninstall Context Store and the data grid, you must delete the services so that the configuration information is removed from the Avaya Breeze™ server database.

Deleting a Context Store cluster

Procedure

1. On the System Manager web console, click **Elements > Avaya Breeze > Cluster Administration**.
2. Select the Context Store clusters that you want to delete.
3. On the **Cluster State** list, select **Deny New Service**, if the clusters are in **Accepting** state.
4. On the Warning box, click **Continue**.
The states of the selected clusters change to **Denying**.
5. Click **Delete**.
6. On the Warning box, click **Continue**.

Next steps

Verify that the Context Store cluster was deleted successfully:

1. On the Cluster Administration page of System Manager web console, verify that the clusters that you deleted in the above procedure have been removed from the list.
2. On the Services page of System Manager web console, verify that the status of the Context Store services have been changed from **Installed** to **Loaded**.

Uninstalling an optional snap-in service

About this task

This task provides information about uninstalling an optional service snap-in.

 **Note:**

- When you uninstall a service, the system does not remove the attributes from the Avaya Breeze™ PostgreSQL database.
- The system preserves the data grid and the entries written to spaces until the lease times expire.

Procedure

1. On the Avaya Aura® System Manager web console, click **Elements** > **Avaya Breeze**.
2. In the left navigation pane, click **Cluster Administration**.
3. On the Cluster Administration page, select the check box for the cluster and then click **Edit**.
4. On the Cluster Editor page, perform the following steps:
 - a. Click the **Services** tab.
The system displays the list of services installed in the cluster.
 - b. Click the checkbox for the service that you want to uninstall.
 - c. Click **Uninstall**.

Next steps

To verify that the service is uninstalled, click **Elements** > **Avaya Breeze** and perform the following steps:

1. On the Server Administration page, verify that the **Service Install Status** for the service is **Uninstalling**.

 **Note:**

- After the service is uninstalled, the **State** of the service is **Loaded**.
2. On the Services page, verify that the **State** of the service is **Loaded**.
3. On the Cluster Administration page, perform the following steps:
 - a. Click **Show**.
 - b. Click the required server and verify that the Service Status page does not display the uninstalled service.

Deleting a snap-in service

Before you begin

Before deleting a service snap-in, you must ensure that the service snap-in is uninstalled.

For more information, see [Uninstalling a service snap-in](#) on page 74.

About this task

This task provides information about deleting a service snap-in. When you delete a service, the system removes the attributes from the Avaya Breeze™ Postgres database.

Note:

Delete all the previous version of Context Store services. Also, note down the existing attributes configurations, so that you can refer to it during the new installation.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze** > **Service Management** > **Services**.
2. On the Services page, perform the following steps:
 - a. Verify that the **State** of the service is **Loaded**.
 - b. Select the service that you want to delete and then click **Delete**.
 - c. In the dialog box, select the **Please Confirm** check box to confirm the deletion.
 - d. Click **Delete**.

Next steps

To verify that the service is deleted, click **Elements** > **Avaya Breeze** and perform the following steps:

1. Click **Service Management** > **Services**.
2. Verify that the Services page does not display the deleted service.

Chapter 6: Administering Context Store

Configuring attributes for a service

About this task

Use this procedure to configure values for a Context Store service. The configuration is a one-time activity that you must perform after installing a service.

Important:

If you plan to use External Data Mart or GEO redundancy features, to avoid the need to restart the cluster, configure the applicable data grid type before adding servers to a new cluster as this cannot be changed dynamically once the data grid has been deployed on the servers.

Procedure

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

The table displays all the attributes that you can configure for the service, including a description of each attribute.

5. For the attribute 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.

ContextStoreManager attribute descriptions

After configuring the following ContextStoreManager attributes which control the data grid you must restart all servers in the cluster:

- ContextStore DataGrid type

- ContextStore ManagerSpace DataGrid Settings
- ContextStoreSpace DataGrid Settings
- Event Stream: Enable Event Streaming

If you enable the Event Streams feature, ContextStoreSpace DataGrid must be reduced by 6G. Therefore to enable the Event Streams feature on an existing data grid, you must restart the cluster to deploy the smaller ContextStoreSpace DataGrid .

Context Store supports runtime configuration/re-configuration of ContextStoreManager’s “GEO:” and “EDM:” attributes. You must disable the applicable enablement attribute for the feature and enable it again after modifying or adding connection details:

- For the External Data Mart connection, **EDM: Enable Persistence to database**
- For the Geo-Redundancy connection, **GEO: Enable session preservation**

*** Note:**

The **ContextStore DataGrid Type** or **ContextStoreSpace DataGrid Settings** attributes cannot be changed dynamically. If this value is not already set to GEO or PROVISIONED-GEO type, you must remove the existing data-grid, and therefore, restart the cluster.

Field	Description
License Features	
FEAT_CS_EXPIRATION	Context Store expiration feature.
VALUE_CS_AEP_CONNECTOR	Context Store AEP connector.
VALUE_CS_API	Context Store API
VALUE_CS_GEO_REDUNDANT_1	Context Store Geo Redundancy
VALUE_CS_SERVER	Context Store server
VALUE_CS_USERS	Context Store users
Startup Configuration	
ContextStore DataGrid type	<p>Mandatory attribute</p> <p>The type of Context Store data grid. Four options are available:</p> <ul style="list-style-type: none"> • STANDARD: A single cluster deployment with non-provisioned data grid • GEO: A geo-redundant deployment with non-provisioned data grid • PROVISIONED: A single cluster deployment with provisioned data grid • PROVISIONED-GEO: A geo-redundant deployment with provisioned data grid <p>STANDARD is the default deployment.</p>

Table continues...

Field	Description
ContextStore ManagerSpace DataGrid Settings	<p>Mandatory attribute</p> <p>A comma-separated list of three numbers: {memoryCapacityPerContainer},{maximumMemoryCapacity},{maximumRelocationsPerMachine}.</p> <p>The default values are <i>1,2,1</i></p> <p>The system interprets a numeric value only as gigabytes. You can specify megabytes with an <i>m</i> or <i>mb</i> after the number. For example, 2MB.</p> <p>For values specific to your deployment type, see the <i>Certified Deployments section in Avaya Context Store Snap-in Release Notes</i>.</p>
ContextStoreSpace DataGrid Settings	<p>Mandatory attribute</p> <p>A comma-separated list of three numbers: {memoryCapacityPerContainer},{maximumMemoryCapacity},{maximumRelocationsPerMachine}.</p> <p>The default values are <i>8,118,1</i></p> <p>The system interprets a numeric value only as gigabytes. You can specify megabytes with an <i>m</i> or <i>mb</i> after the number. For example, 1MB.</p> <p>For values specific to your deployment type, see the <i>Certified Deployments section in Avaya Context Store Snap-in Release Notes</i>.</p>
External Data Mart Configuration	
EDM: Mirror Service redo log size	<p>The amount of context data to store for retry if disconnected from the External Data Mart (EDM). The system discards the oldest data when this size limit is reached.</p> <p>Range: 10000 to 250000</p> <p>The default value is <i>60000</i>.</p> <p>The configuration for this attribute provided for different deployment scenarios in the <i>Data-grid Configuration Settings – ContextStoreManager Attributes section of the Context Store Release Notes</i> is designed to store approximately 30 minutes of data.</p>
EDM: Enable Persistence to database	<p>Setting this to <code>true</code> enables persistence of context data to the customer-provided External Data Mart. The accepted values are:</p> <ul style="list-style-type: none"> • <code>true</code>: Enables persistence to the external data mart. • <code>false</code>: Disables persistence to the external data mart <p>The default value is <i>false</i>.</p>

Table continues...


Field	Description
EDM: Enable Provisioning from database	<p>Setting this to 'true' will enable provisioning of context data from the customer-provided External Data Mart. The accepted values are:</p> <ul style="list-style-type: none"> • true: Enables provisioning to the external data mart. • false: Disables provisioning to the external data mart <p>The default value is <i>false</i>.</p>
EDM: Database type	<p>The type of EDM database. The accepted values are:</p> <ul style="list-style-type: none"> • PostgreSQL • Microsoft SQL Server • Oracle Database
EDM: Database host	The host for the EDM database.
EDM: Database port	The port for the EDM database.
EDM: Database username	<p>User name for the External Data Mart database connection.</p> <p>You cannot update this attribute dynamically.</p>
EDM: Database password	<p>Password for the External Data Mart database connection.</p> <p>You cannot update this attribute dynamically.</p>
EDM: Database name	Name of the database used as External Data Mart
EDM: Mirror Service container size	<p>Memory required for the External Data Mart Mirror Service deployment.</p> <p>The default value is <i>1</i>.</p> <p>The system interprets a numeric value only as gigabytes. You can specify megabytes with an <i>m</i> or <i>mb</i> after the number. For example, 2m.</p> <p>For values specific to your deployment type, see the <i>Certified Deployments</i> section in <i>Avaya Context Store Snap-in Release Notes</i>.</p>
Run-Time Service Configuration	
Cluster Deny Service on two node outage	<p>Determines whether to deny or accept service when two nodes in a cluster are unavailable. If disabled, the last remaining node continues to attempt service requests. The accepted values are:</p> <ul style="list-style-type: none"> • true: If two nodes in a cluster are unavailable, the third node also denies service. • false: Even if two nodes in a cluster are unavailable, the third node tries to serve incoming requests. <p>The default value is, <i>false</i>.</p> <p> Note:</p> <p>This attribute is not applicable for one or two-node deployments.</p>

Table continues...

Field	Description
<p>CS Audit: Event limit</p>	<p>Configure the limit of event entries in the audit trail of context objects.</p> <ul style="list-style-type: none"> • Range: 0 to 50 • Default value: 50 <p>You can update this attribute dynamically. Changes you make do not become effective on a context until the next interaction with that object.</p> <p>* Note:</p> <p>If you enable the Audit trail feature in a geo-redundant deployment, the CS Audit: Event limit attribute must be set identically in both clusters.</p>
<p>CS Default Lease Time</p>	<p>Default lease time, in seconds, for context data to live in the in-memory data cache Context Store automatically removes a context if the context remains in Context Store for the lease period without any change.</p> <p>This attribute specifies the default lease time that Context Store uses when you do not specify any lease time for a context entry.</p> <ul style="list-style-type: none"> • Range: 1 to 86400 • Default value: 7200 <p>For values specific to your deployment type, see the <i>Certified Deployments section in Avaya Context Store Snap-in Release Notes</i>.</p> <p>* Note:</p> <p>CS Default Lease Time is not applicable to the contexts in the CS_PROVISION table. The contexts in the CS_PROVISION table has an infinite lease time and remain in the data grid permanently until the contexts are deleted manually.</p>
<p>CS Maximum Lease Time</p>	<p>Maximum lease time, in seconds, for context data. The system logs warnings for leases longer than this value.</p> <p>If the average lease time for the cluster exceeds this value, Context Store raises an error event. If a context is created or updated with a lease time that exceeds this value, Context Store logs only a warning.</p> <ul style="list-style-type: none"> • Range: 1 to 86400 • Default value: 14400 <p>You can update this attribute dynamically.</p>

Table continues...



Field	Description
CS Threshold: Instance High Requests per Second	<p>High threshold on Context Store instance requests per second. Must be greater than related Minima. If the requests per second for an instance exceeds this value, the Context Store instance rejects the further requests and raises an event.</p> <ul style="list-style-type: none"> • Range: 1 to 650 • Default value: 65 <p>You can update this attribute dynamically.</p> <p>For values specific to your deployment type, see the <i>Certified Deployments section in Avaya Context Store Snap-in Release Notes</i>.</p>
CS Threshold: Instance Low Requests per Second	<p>Low threshold on Context Store instance requests per second. Must be lower than related Maxima. If the requests per second for an instance exceeds this value, the Context Store instance raises an event, without rejecting any further requests.</p> <ul style="list-style-type: none"> • Range: 1 to 650 • Default value: 55 <p>You can update this attribute dynamically.</p> <p>For values specific to your deployment type, see the <i>Certified Deployments section in Avaya Context Store Snap-in Release Notes</i>.</p>
CS Threshold: Max Error Rate	<p>Threshold for maximum tolerated Context Store request error rate in percentage</p> <ul style="list-style-type: none"> • Range: 1 to 100 • Default value: 20 <p>You can update this attribute dynamically.</p>
CS Threshold: Max Latency	<p>Threshold for maximum tolerated Context Store request latency in milliseconds. When the average latency exceeds the value you have specified in this field, Context Store raises an event.</p> <ul style="list-style-type: none"> • Range: 1 to 5000 • Default value: 250 <p>You can update this attribute dynamically.</p> <p> Note:</p> <p>The average latency of a request in an hour is less than 250 milliseconds with a maximum latency of two seconds.</p>

Table continues...

Field	Description
CS Threshold: Service High Requests per Second	<p>High threshold on Context Store service requests per second. Must be greater than related Minima. If the service requests per second for a Context Store cluster exceeds the value you have specified in this attribute, Context Store rejects the further service requests and also raises an event.</p> <ul style="list-style-type: none"> • Range: 1 to 1240 • Default value: 105 <p>You can update this attribute dynamically.</p> <p>For values specific to your deployment type, see the <i>Certified Deployments section in Avaya Context Store Snap-in Release Notes</i>.</p>
CS Threshold: Service Low Requests per Second	<p>Low threshold on Context Store service requests per second. Must be lower than related Maxima. If the service requests per second for a Context Store cluster exceeds the value you have specified in this attribute, Context Store raises and alarm, without rejecting the further service requests.</p> <ul style="list-style-type: none"> • Range: 1 to 1240 • Default value: 85 <p>You can update this attribute dynamically.</p> <p>For values specific to your deployment type, see the <i>Certified Deployments section in Avaya Context Store Snap-in Release Notes</i>.</p>
Geo Redundancy Configuration	
GEO: Enable session preservation	<p>Setting this to 'true' enables Geo-Redundancy between configured Context Store clusters. The accepted values are:</p> <ul style="list-style-type: none"> • true: Enables geo redundancy • false: Disables geo redundancy <p>The default value is <i>false</i>.</p>
Geo: Gateway Service container size	<p>Memory required for Geo-Redundancy Gateway Service deployment. The system interprets a numeric value only as gigabytes. You can specify megabytes with an <i>m</i> or <i>mb</i> after the number. For example, 2m.</p> <p>For values specific to your deployment type, see the <i>Certified Deployments section in Avaya Context Store Snap-in Release Notes</i>.</p> <p>The default value is <i>1</i>.</p>
GEO: Keystore file name	Certificate name of the geo redundancy keystore.
GEO: Keystore password	Password of the geo redundancy keystore.
GEO: Target cluster Id	Name of the target cluster on the geo redundant site
Streams Configuration	

Table continues...

Field	Description
Event Stream: Enable Event Streaming	<p>Setting this to 'true' enables clients to subscribe for personalized events from Context Store.</p> <p>The default value is <i>false</i>.</p> <p>Enable this parameter for the Event Streams feature to work.</p> <p> Note:</p> <p>If you want to enable the Event Streams feature, ensure that there is 6 GB memory on the Avaya Breeze™ cluster.</p>
Supplier	
Supplier Id	<p>The supplier Id that Avaya provides.</p> <p>The default value is <i>10000000</i>.</p>
Advanced Configuration	
Enable Centralized Logging	<p>This value indicates that centralized logging is needed by the snap-in. Enables centralized logging after the snap-in is installed.</p>

Related links

[Context Store Event Streams](#) on page 22

[Configuring a cluster and installing mandatory services](#) on page 58

ContextStoreRest attribute descriptions


Field	Description
Advanced Configuration	
Authorization Service Address	<p>The fully qualified domain name (FQDN) of the node/cluster where Authorization Service is installed</p> <p>Enter the FQDN or IP of the node/cluster where the Authorization Service is installed.</p> <p> Note:</p> <p>If the Authorization service is installed on the Context Store cluster, you need not set this attribute.</p>
Enable Breeze Authorization Service	<p>Setting this to 'true' enables authorization against the Breeze Authorization Service. The accepted values are:</p> <ul style="list-style-type: none"> • true: Enables authorization against the Breeze Authorization Service • false: Disables authorization against the Breeze Authorization Service <p>The default value is <i>false</i>.</p>

Table continues...

Field	Description
Require user for Breeze Authorization Service	Setting this to 'true' enforces user access only for Breeze Authorization Service. If you enable this attribute, the system disables the Get Token and Get Token by Scope API methods. The accepted values are: <ul style="list-style-type: none"> • true • false The default value is <i>false</i> .
Enable Centralized Logging	This value indicates that centralized logging is needed by the snap-in. Enables centralized logging after the snap-in is installed.
External Data Mart Configuration	
Enable Retrieval From Database	Setting this to 'true' will enable retrieval of Context data from the External Data Mart when expired in Context Store Space.
Supplier	
Supplier Id	The supplier Id that Avaya provides.
License Features	
FEAT_CS_EXPIRATION	Context Store expiration feature.
VALUE_CS_AEP_CONNECTOR	Context Store AEP connector.
VALUE_CS_API	Context Store API
VALUE_CS_GEO_REDUNDANT_1	Context Store Geo Redundancy
VALUE_CS_SERVER	Context Store server
VALUE_CS_USERS	Context Store users

Related links

- [Assigning permissions to an authorization client](#) on page 65
- [Authorization](#) on page 41
- [Configuring a cluster and installing mandatory services](#) on page 58
- [Context Store REST](#) on page 18

ContextStoreScreenPop attribute descriptions

Field	Description
License Features	
FEAT_CS_EXPIRATION	Context Store expiration feature.

Table continues...

Field	Description
VALUE_CS_AEP_CONNECTOR	Context Store AEP connector.
VALUE_CS_API	Context Store API
VALUE_CS_GEO_REDUNDANT_1	Context Store Geo Redundancy
VALUE_CS_SERVER	Context Store server
VALUE_CS_USERS	Context Store users
Rules Configuration	
Base for URL	<p>You must provide this path if you set the override format as URL. You must specify a valid URL to which the system can pass parameters.</p> <p>The default URL is that of a demonstrative CSS file of Context Store. Replace the default URL with the URL of the CSS file.</p> <p>The default URL is: <code>http://127.0.0.1/?</code></p>
CSS for HTML	<p>You must provide this path if you set the override format as HTML. This path must point to a valid CSS file.</p> <p>The default URL is that of a demonstrative CSS file of Context Store. Replace the default URL with the URL of the CSS file.</p> <p>The default URL is: <code>/services/ContextStoreScreenPop/demo/css/demo.css</code></p>
Identifier Delimit Character	<p>Use this field to specify the character that delimits the UCID. Context Store extracts the contextId based on the value that you specify for this attribute and the default setting for the UCID delimit position.</p> <p>For example, if the values of:</p> <ul style="list-style-type: none"> • The default setting for the UCID delimit character = \. • The UCID = 1111111.222222.333333.444444 <p>Then Context Store detects the contextId as 333333.</p>
Identifier Delimit Position	<p>This setting is the occurrence of the UCID delimiter that marks the start of a contextId in a UCID string. The next instance of the delimiter marks the end of the contextIdn.</p> <p>The default setting for the UCID delimit position = 2</p>

Table continues...

Field	Description
Identifier Parsing Position	Use this field to detect a UCID from a string that contains the id. The valid value for this attribute must contain a comma separated list of two positive integers. The first integer is the start location of the id and the second number is the end location of the id. The default value is: 0,10.
JavaScript for HTML	The JavaScript file that must be included when selecting the html format. Provide the http link to where the JavaScript file is hosted.
Rules	
User Rule 01 - 20	You can enter customized rules for ContextStoreScreenPop. The system supports up to 20 user defined rules. This field is empty by default. Select the Override Default check box to enter the user defined rule.
Common Configuration	
Supplier ID	Avaya-provided supplier Id.

Related links

[Context Store Screen Pop](#) on page 20

ContextStoreNotify attribute descriptions

Name	Description
License Features	
FEAT_CS_EXPIRATION	Context Store expiration feature.
VALUE_CS_AEP_CONNECTOR	Context Store AEP connector.
VALUE_CS_API	Context Store API
VALUE_CS_GEO_REDUNDANT_1	Context Store Geo Redundancy
VALUE_CS_SERVER	Context Store server
VALUE_CS_USERS	Context Store users
Subscription <i>number</i>	
Where <i>number</i> is the serial number of subscription. One subscription is for one client. You can have a maximum of five subscriptions	
Subscription <i>number</i> enabled	<ul style="list-style-type: none"> true: Enables the subscription false: Disables the subscription

Table continues...

Name	Description
License Features	
Subscription <i>number</i> endpointURI	This attribute is for configuring the receiver endpoint for ContextStoreNotify. Specify the full URI of the endpoint that will receive notifications for this subscription.
Subscription <i>number</i> tenantId	This attribute filters the notifications you receive. Only the contexts created with the specified tenantId will trigger notification for this subscription.
Subscription <i>number</i> groupId	This attribute filters the notifications you receive. Only the contexts with the specified groupId will trigger notification for this subscription.
Common Configuration	
Supplier ID	Avaya-provided supplier Id.

Related links

[Context Store Notify](#) on page 21

ContextStoreRules attribute descriptions

Name	Description
License Features	
FEAT_CS_EXPIRATION	Context Store expiration feature.
VALUE_CS_AEP_CONNECTOR	Context Store AEP connector.
VALUE_CS_API	Context Store API
VALUE_CS_GEO_REDUNDANT_1	Context Store Geo Redundancy
VALUE_CS_SERVER	Context Store server
VALUE_CS_USERS	Context Store users
Rule <i>number</i>	
Where <i>number</i> is the serial number of the rule.	
Rule 01: Eventing Connector Family	Enter the Family value you entered when creating the event.
Rule 01: Eventing Connector Type	Enter the Type value you entered when creating the event.
Rule 01: Eventing Connector URL	Enter the HTTP location of the Eventing Connector where the ED Workflow is installed.

Table continues...

Name	Description
License Features	
Rule 01: Eventing Connector Version	Rules Eventing Connector Version for rule 01. This should match the Family value you entered when creating the event.
Rule 01: Eventing Rule Priority	Enter priority for Rule 01. <ul style="list-style-type: none"> • This should be a number between 1 and 5. • Only one rule can fire and the priority determines which rule will fire when the context matches multiple rules.
Rule 01: Identifier	Enter a name for Rule 01. This should be an alphanumeric string.
Rule 01: Key	Enter the key for Rule 01.
Rule 01: Operator	Enter operator for Rule 01. This must be set to '=='
Rule 01: Value	Enter a value for Rule 01.
Common Configuration	
Supplier ID	Avaya-provided supplier Id.

Related links

[Context Store Rules](#) on page 22

ContextStoreQuery attribute descriptions

Field	Description
License Features	
FEAT_CS_EXPIRATION	Context Store expiration feature.
VALUE_CS_AEP_CONNECTOR	Context Store AEP connector.
VALUE_CS_API	Context Store API
VALUE_CS_GEO_REDUNDANT_1	Context Store Geo Redundancy
VALUE_CS_SERVER	Context Store server
VALUE_CS_USERS	Context Store users
External Data Mart Configuration	
EDM: Database username	Password of the customer-provided External Data Mart database

Table continues...

Field	Description
EDM: Database password	Password of the customer-provided External Data Mart database.
Common Configuration	
Supplier Id	The supplier Id that Avaya provides.
Advanced Configuration	
Enable Centralized Logging	This value indicates that centralized logging is needed by the snap-in. Enables centralized logging after the snap-in is installed.

Related links

[Context Store Query](#) on page 19

ContextStoreSoap attribute descriptions

Field	Description
DEFAULT_GROUP	
Supplier Id	The supplier Id that Avaya provides.
License Features	
FEAT_CS_EXPIRATION	Context Store expiration feature.
VALUE_CS_AEP_CONNECTOR	Context Store AEP connector.
VALUE_CS_API	Context Store API
VALUE_CS_GEO_REDUNDANT_1	Context Store Geo Redundancy
VALUE_CS_SERVER	Context Store server
VALUE_CS_USERS	Context Store users

Related links

[Context Store SOAP](#) on page 19

Chapter 7: High availability

High availability within a cluster

*** Note:**

- Context Store does not support high availability for single-node deployments. If the single node fails, you cannot recover the data.
- For a cluster with more than one node, Context Store supports data preservation for only one node failure. For more information about multiple node failure and high availability, see *Avaya Context Store Snap-in Developer Guide*.

Context Store uses Avaya Breeze™ and data grid to achieve high availability. For High availability, the Context Store cluster must consist of two or more Avaya Breeze™ nodes that are dedicated for Context Store. Context Store creates a data grid across the Avaya Breeze™ servers in the cluster where you deploy Context Store, so that the servers can operate in an active/active mode.

To achieve high availability, Context Store data grid uses the following techniques:

- Self healing: The Context Store data grid has self healing and disaster recovery capabilities that minimize the chances of a downtime. The data grid also preserves its states so that, in case of a system failure, you can recover the data grid in its latest state.
- Data sharing: All the servers in a Context Store cluster shares the same data grid. Even if one server is unavailable, the other servers in the Context Store cluster can use the data present in the data grid.
- Data partition and redundancy: Context Store partitions the data that is present in the data grid and distributes the data across different machines. This distributed structure enables the system to hold more data than the capacity of a single machine and also helps attain high availability. The system keeps a backup of data from each partition so that if one source becomes unavailable, Context Store can retrieve the same data from the backup location.

The Context Store cluster is accessible through a cluster IP address that is maintained by a highly available load balancer. The load balancer distributes HTTP requests across each of the Avaya Breeze™ servers in the cluster. If one of the servers in the Context Store cluster is unavailable, Context Store can still work without loss of data and significant impact to its performance.

However, unavailability of two servers might result in loss of data and failing HTTP requests. If two servers are unavailable in a cluster, restart the cluster to clear old context data and restore Context Store to a known state. When the cluster is restored to a known state, data replication in the cluster is not accurate for updates that occur during the failover period. The data and EDM on the other cluster, which services the contexts during failover, is accurate.

*** Note:**

You can enable load balancer only after adding nodes to your Context Store cluster.

Server failure

If any of the servers in the cluster are unavailable, Context Store redirects the client requests to the primary partition. If the primary partition is unavailable, Avaya Breeze™ determines a new primary partition to direct the client requests. Context Store might have an increased response time during this negotiation process, until a new primary partition is assigned.

Server restoration

When an unavailable server becomes available, Avaya Breeze™ readjusts the partitions to accommodate the new server. If the server that becomes available contains a primary partition, Avaya Breeze™ determines a new primary partition to serve the client requests. Context Store might have an increased response time during this negotiation process, until a new primary partition is assigned.

Geo redundancy

Context Store Geo redundancy overview

Context Store Geo redundancy is an architecture that you can configure to enhance high availability of Context Store. Using Context Store Geo redundancy, you can have two Context Store clusters in active/active mode. These Context Store clusters can be either in the same data center or in two different data centers. To ensure a successful failover, you must add the two Context Store clusters to the same System Manager.

Context Store supports Geo redundancy with two Data centers only.

To enable Context Store Geo redundancy, you must:

- Configure the *Context Store Geo* attributes: For more information, see [Geo redundancy and External Data Mart deployment](#) on page 66.
- Use a load balancer: You must provide and configure a highly available load balancer for the two Context Store clusters. The load balancer must provide:
 - A common address: Both the Context Store clusters must be reachable through a common address. For the third party applications that you integrate with Context Store, use this common address to access the clusters. You must use only the common address, and not the individual cluster IP address, to access the Context Store clusters.
 - Load balancing: The load can be distributed between the clusters as per your requirements, however, the traffic must be routed on the *rid parameter*, the *routingId* field of a context object. You cannot route requests using round robin, least busy server, or any other mechanism other than routing on the *rid parameter*.

For routing the requests and distributing the traffic between the clusters, Context Store uses an optional field, *rid parameter*, in each REST request. If you do not specify a value for the rid parameter, the load balancer routes the request to the default Context Store cluster. Due to the replication of the same context entry in the two clusters, Context Store uses a combination of the rid parameter and the contextId to uniquely identify a context entry.

The two geographically redundant Context Store clusters support the same traffic as one non geo redundant Context Store cluster supports.

Avaya Engagement Designer does not support the geo redundancy feature, rid parameter, of Context Store.

For more information about load balancer for a geo-redundant deployment and a reference configuration, see *Avaya Context Store Snap-in Developer Guide*.

Third party load balancer configuration requirement

For a third-party load balancer to route traffic correctly between two or more Context Store clusters, the following mandatory steps must be configured on the load balancer:

- Ensure that the traffic is routed on the rid parameter.

Each request for a particular context must be routed to the same Context Store cluster. To achieve this, Context Store uses an optional field, *rid parameter*, in each REST request. For example, all requests with rid parameter=1 must be directed to the nondefault cluster and any other requests must be sent to the default cluster. Requests for the same context must go to the same Context Store cluster as the time lag for replication between the two Context Store clusters is not instantaneous. You cannot route requests using round robin, least busy server, or any other mechanism other than routing on the rid parameter. You must ensure that each request for a particular context has the same rid parameter.

- If the load balancer receives responses with any of the following codes: 500, 502, 503, and 504, the load balancer must mark the Context Store cluster as down and redirect all subsequent requests to the other Context Store cluster. The 500 code signifies that only one of the Avaya Breeze™ nodes in the Context Store cluster is operational and it cannot process requests.
- The load balancer must be able to forward the Context Store https requests. If the load balancer requires authentication, load the certificates in the load balancer. For more information about certificates, see [Certificate-based authentication](#) on page 102.

Related links

[Failover scenarios](#) on page 92

Failover scenarios

The following section displays the failover scenarios in geo redundancy:

- When a Context Store cluster is down, requests that are routed to the cluster will be redirected to the other cluster. This might result in GET requests going to a cluster which

does not contain that context. For example, the request will fail in the following sequence of events:

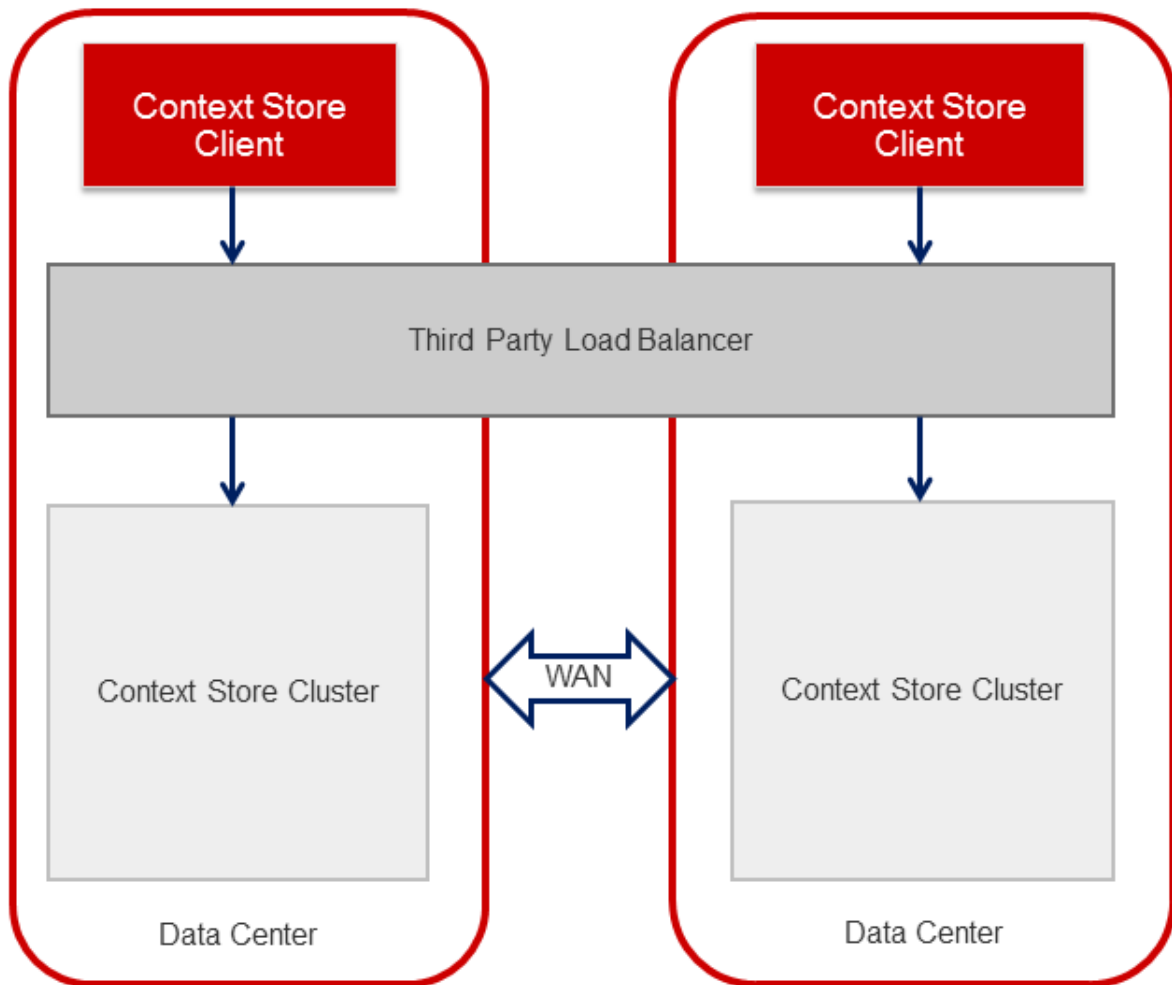
1. Context A is saved to cluster 1.
 2. Cluster 1 goes down before context A has been replicated to cluster 1.
 3. The load balancer attempts to route the GET request for context A to cluster 2.
- When a cluster is shut down and restarted, existing data on the active cluster is not replicated to the other cluster. For example, the following data is not replicated:
 1. Shut down cluster 1.
 2. Create new contexts on cluster 2 and update existing contexts on cluster 2.
 3. Restart cluster 1
 4. Only the newly created contexts on cluster 2 are replicated to cluster 1.

Related links

[Third party load balancer configuration requirement](#) on page 92

Architecture

The following diagram depicts the architecture of a Context Store geo redundant deployment:



Two Context Store clusters are deployed at two different data centers. All requests to Context Store are routed through a third party load balancer that is common between the two Context Store clusters. The load balancer can communicate with both the clusters at any time. The clusters are connected through WAN. The load balancer can reside on either data center.

Service preservation

Context Store geo redundancy provides service preservation through load balancing of requests across the two Context Store clusters, with both the clusters in active state simultaneously. These Context Store clusters can be in two separate LANs, connected by a WAN link. However, because the replication of data between the two Context Store clusters is not instantaneous, you must route all requests for a specific context to the same cluster.

If you enable the option *Cluster Deny Service on 2 node outage* from the ContextStoreManager attributes, the third Avaya Breeze™ server in a Context Store cluster stops processing requests when the other two servers stop working. The third server then returns 500's as the status code, and the load balancer routes the traffic to the other cluster.

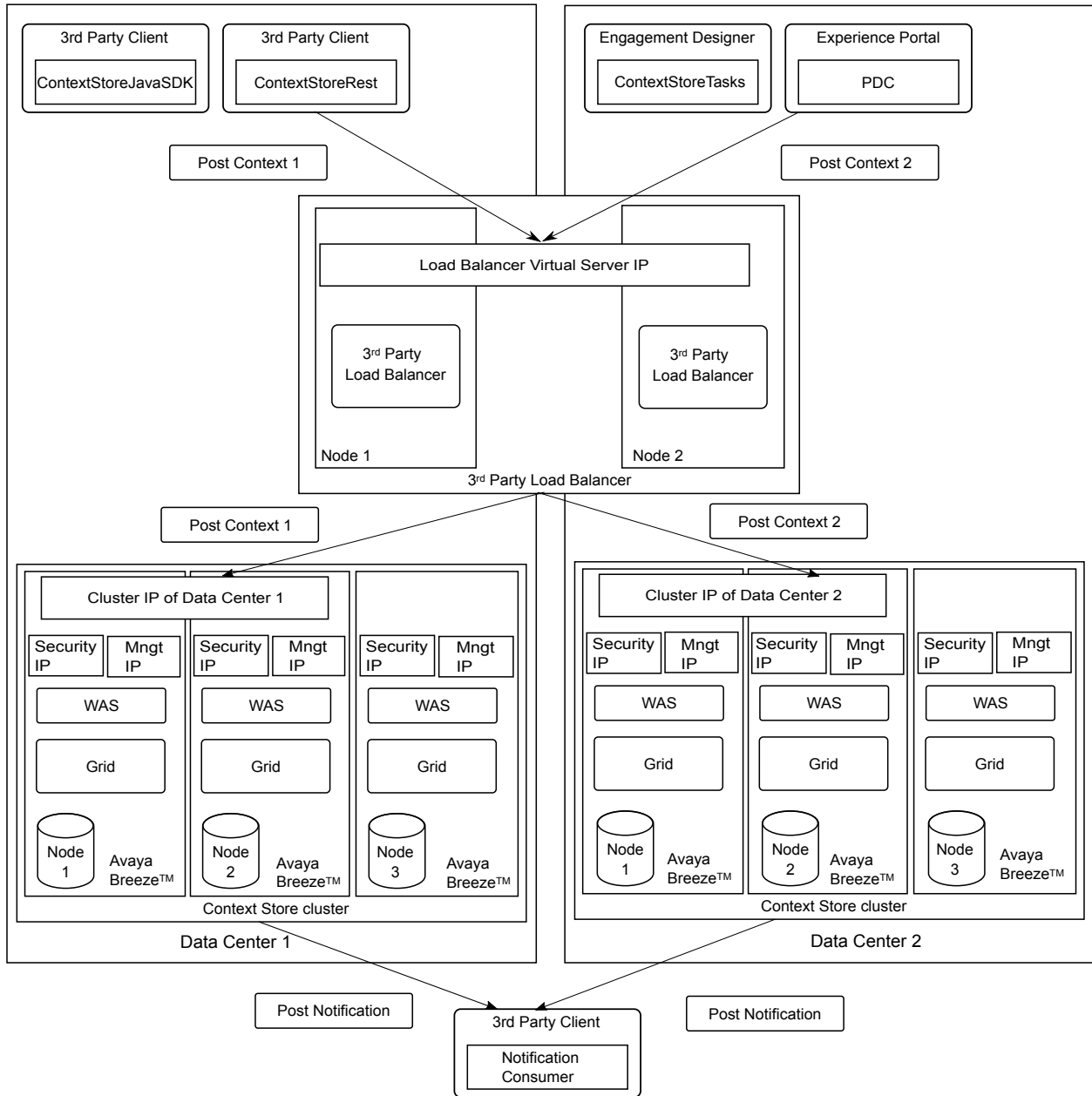
Session preservation

Context Store geo redundancy incorporates bi-directional replication of state and data across the two Context Store clusters to ensure preservation of session, in case of a cluster failure. The bi-directional replication strategy stores backup of all contexts in each Context Store cluster, so that if a cluster or a datacenter is unavailable, you can continue working with the backed up context.

Notifications in geo redundant architecture

In a geo redundant architecture, Context Store uses the same notification subscription details on each cluster, so that you receive notifications from any of the two clusters. If the Context Store cluster to which you have sent your request is unavailable, Context Store reroutes your request to the other available cluster. The cluster then processes your request and generates the notifications. The following diagram depicts the working of ContextStoreNotify in a Context Store geo redundant architecture.

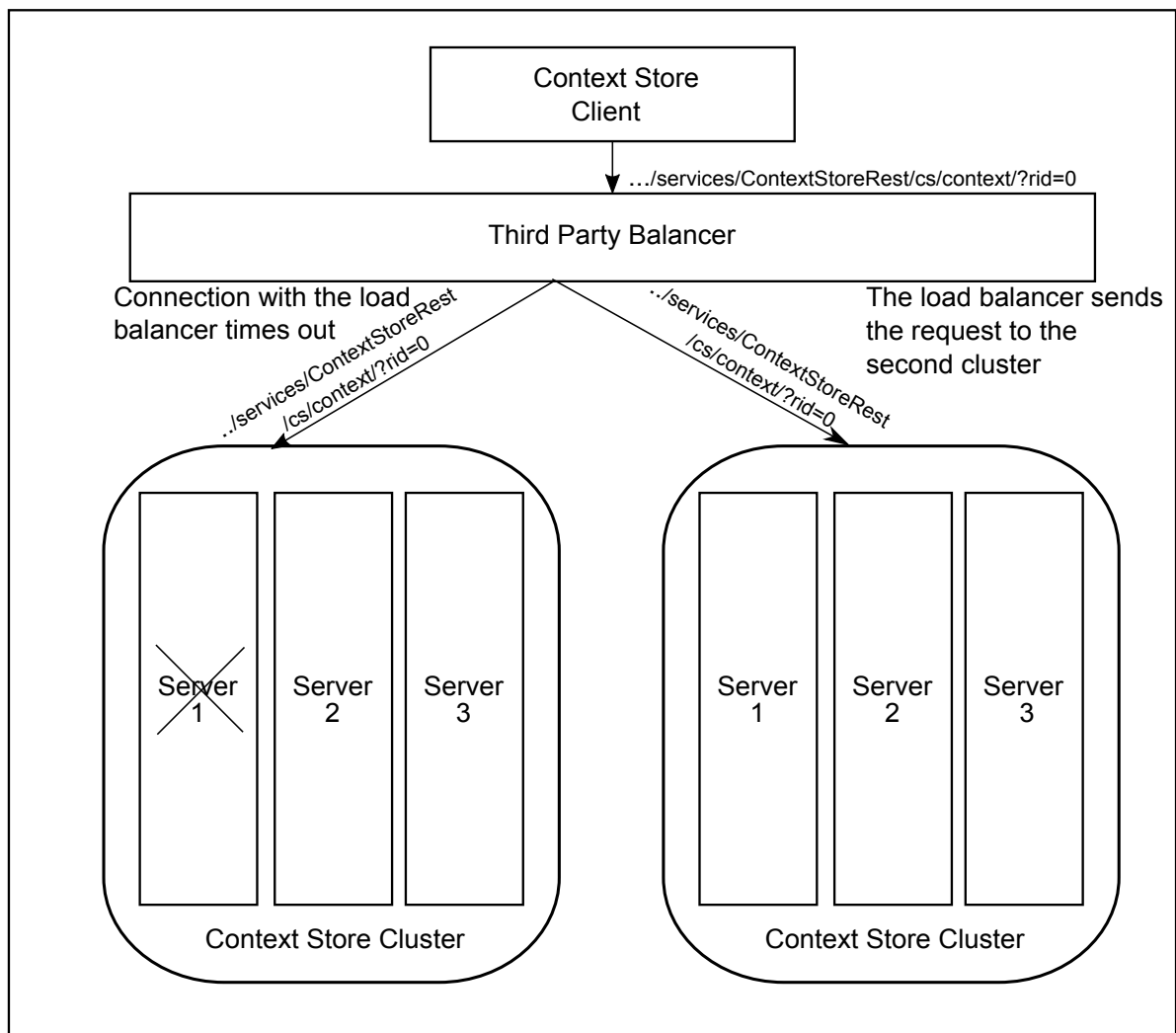
High availability



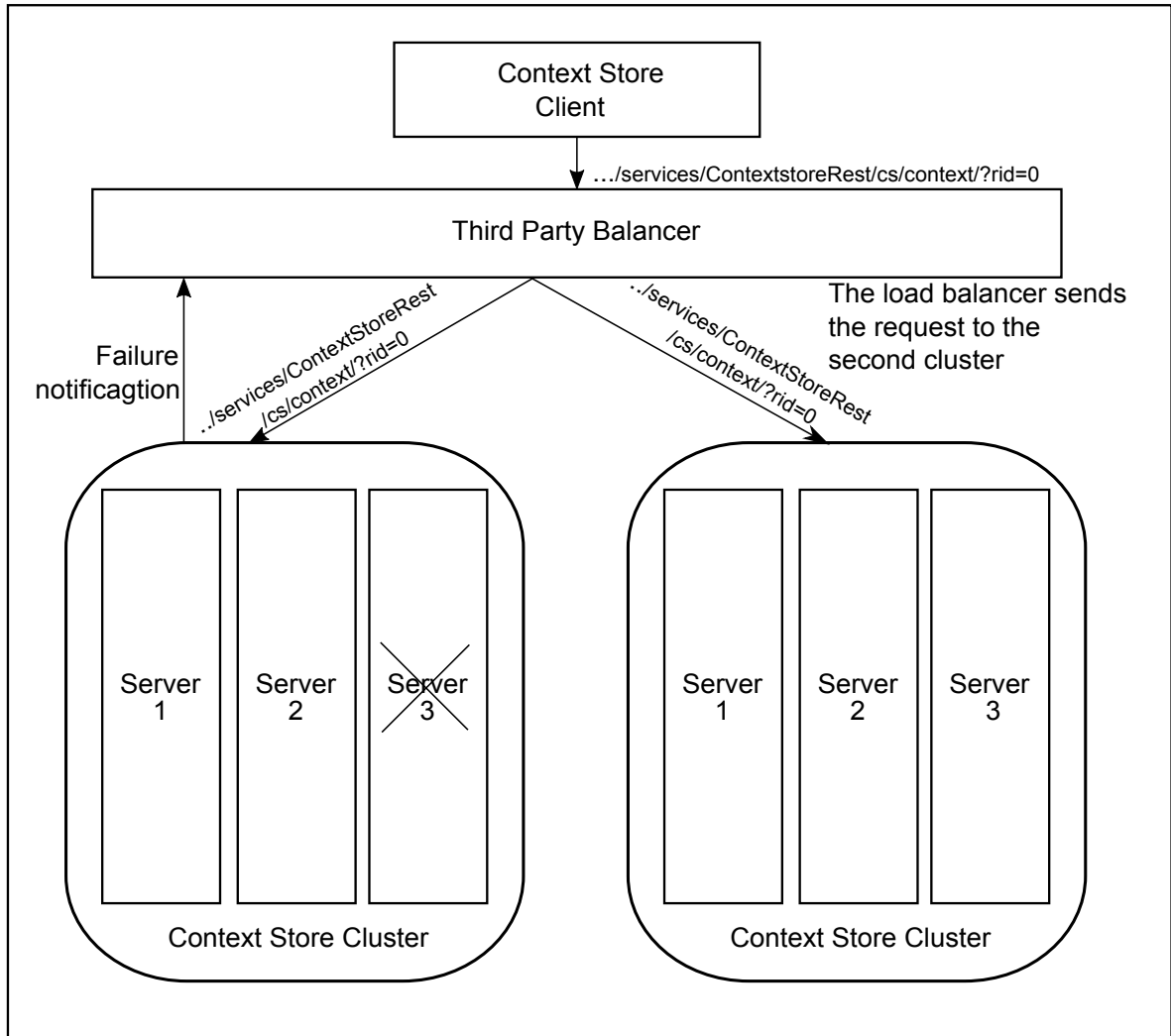
Failover support

In a Context Store geo redundant setup, the load balancer detects that a cluster is unavailable, the load balancer routes the incoming requests to the available cluster. The geo redundant architecture supports the following failover scenarios:

- Both servers are unavailable: If the two Avaya Breeze™ servers in a Context Store cluster are unavailable, the cluster IP address is also unavailable. The geo redundant load balancer detects the failure and routes all requests to the remaining active cluster.



- Either of the Avaya Breeze™ servers and the other server of a Context Store cluster is unavailable, the remaining server detects the failure and returns a status code of 500. Upon receiving the failure information from the remaining server, the load balancer routes all requests to the other cluster in the geo redundant system.



- All three servers are unavailable: If all three Avaya Breeze™ servers in a Context Store cluster are unavailable, the geo redundant load balancer routes all requests to the remaining Context Store cluster in the geo redundant system.

For the reference implementation, the Nginx load balancer running on the Geo cluster will automatically detect if a Context Store cluster is back in service. There are no manual steps required for the Load Balancer to reintroduce a Context Store cluster back into receiving requests.

Chapter 8: Performance

Capacity and scalability specification

This topic provides the capacity specification for the Avaya certified deployment scenarios. Avaya has used these values as a benchmark for capacity verification.

Key considerations:

- The standard storage capacity of a context is 2 KB in raw JSON data. Note that the object might be significantly larger when stored in the data grid depending on the complexity of the object. When you enable optional features, which require memory resources, the size of the Context objects, lease time, or throughput must be decreased to achieve the certified performance. Also, when you use the aliasId feature, the 2 KB standard context must be reduced to 1.5 KB to achieve the certified performance level, in terms of throughput and lease time. Enabling the Audit feature also has an impact on Context Store capacity. You must reduce the context size based on the number of audit entries enabled. For more information, see *Avaya Context Store Snap-in Developer Guide*.
- The average latency of a request in an hour is less than 250 milliseconds with a maximum latency of two seconds regardless of the deployment size. Latency is the time interval between the client request and the Context Store response, in milliseconds.
- Context Store supports a maximum of three aliasIds.
- For production environments which require the Geo redundancy feature, each cluster must contain two or more Avaya Breeze™ nodes with 16 GB of memory and 8 cores allocated to each node.
- If you want to enable the Event streams feature, you require 6 GB memory on the Avaya Breeze™ cluster.
- For production deployments that are not certified with five notifications, if you increase the number of notification clients to five, the request per second capacity will be reduced to half.

 **Note:**

From Release 3.2 of Context Store, performance is tested with only one notification client.

For the capacity certified for each Avaya certified deployments, see the *Certified Deployments section in Avaya Context Store Snap-in Release Notes*.

Chapter 9: Security

Overview

Context Store uses Avaya Breeze™ to provide all security configurations for access to its services. Avaya Breeze™ provides configuration for HTTPS, Mutual TLS (Client Certificate Challenge), Cross Origin Resource Sharing (CORS), Whitelists, and Trust Certificates. In addition, System Manager provides a flexible platform for administering certificates and authorities.

 **Note:**

When enabling the Geo Redundancy feature or using the CS Pluggable Data Connector for Orchestration Designer or a secured client of ContextStoreScreenPop, the CS SDK, or the ContextStoreNotify service, additional security steps (certificates and/or licenses) are required. See individual feature sections for detailed information about required configuration. There are several options available when configuring certificates using System Manager; to help getting started, one particular approach is documented in the *Appendix section of Avaya Context Store Snap-in Developer Guide*.

For more information about security configuration, see *Avaya Breeze™ Overview and Specification* and *Avaya Aura® System Manager Overview and Specification*.

Secure space

With Context Store Secure space, you can secure the data grid with your own unique password. The unique password prevents unauthorized access of the grid by tools. The secure user for the grid is dcmuser. After security is enabled, the username dcmuser and the password that you set in the **Cluster Attributes** page are applied to the data grid.

You can configure Space security when the cluster is being created or by editing the cluster configuration after the cluster is created.

 **Warning:**

When you enable security after creating the cluster, the system deletes the existing unsecured data grid and all data that the grid contains automatically and the data grid is redeployed in secure mode.

Configuring space security

Procedure

1. On the System Manager web console, go to **Elements > Avaya Breeze > Cluster Administration**.
2. If you are creating a new secure cluster, click **New** on the **Cluster Administration** page.
3. If you are securing an existing cluster:
 - a. Select the check box of the cluster that you want to secure and select the **Deny New Service** option from the **Cluster State** drop-down menu.
 - b. On the Warning box, click **Continue**.

The system changes the state of the cluster to *Denying*.
 - c. Click **Edit**.
 - d. Go to **Cluster Attributes > Cluster Editor > General** tab.
 - e. Enter the password that you want to use in the **Grid password** text box.
 - f. Select the **Use secure grid?** check box.
 - g. Click **Commit**.

The system prompts you to ensure that all Avaya Breeze™ server restarts are complete before placing the cluster into the **Accept New Service** state.
 - h. Click **OK**.
 - i. Select the check box of the new/modified cluster.
 - j. From the **Cluster State** drop-down menu, select **Accept New Service**.
 - k. Click **Continue** in the **Accept New Service** dialog box.

The system displays the **Accepting** state in the **Servers State** column.

Selecting TLS version for a snap-in service

About this task

Avaya Breeze™ supports selection of minimum TLS version for SIP and HTTPS service in each cluster. By default, Avaya Breeze™ uses the value of the **Minimum TLS Version** field set in System Manager configuration. If the value of the **Minimum TLS Version** field is TLSv1.1, Avaya Breeze™ uses TLSv1.2. If the value of the **Minimum TLS Version** field is SSLv3, Avaya Breeze™ uses TLSv1.0.

Procedure

1. On the System Manager web console, click **Elements > Avaya Breeze**.
2. In the left navigation pane, click **Cluster Administration**.

3. On the Cluster Administration page, select the check box for the cluster and then click **Edit**.
4. On the Cluster Editor page, perform the following steps:
 - a. Click the **Services** tab.
The system displays the list of services installed in the cluster.
 - b. Select the checkbox next to the snap-in service for which you want to select the TLS version.
 - c. From the **Select TLS Version for the Selected Snap-in(s)**, select the relevant TLS version.
The selected TLS version appears in the TLS version column corresponding the service snap-in.
5. Click **Commit**.
6. Reboot the cluster for the changes to take effect.

Certificate-based authentication

For the Context Store certificate-based authentication, you must perform the following procedures in the System Manager web portal:

- Configure the client certificate challenge in Avaya Breeze™ Element Manager. The configuration is available on the **Avaya Breeze > Configuration > HTTP Security** page.
- Create a client key store.
- Download the Avaya Breeze™ trusted certificate from System Manager.
- Authenticate browsers.

Ensure that client applications that access Context Store operations provide the location and credentials of the client certificate and trusted certificate to establish a secure session with the Context Store cluster.

For information about Avaya Breeze™ certificate-based authentication, see the *Security* chapter in *Avaya Breeze™ Overview and Specification*. For information about Avaya Aura® System Manager certificate-based authentication, see the *Security Enhancement* section in *Avaya Aura® System Manager Overview and Specification*.

Cross Origin Resource Sharing

Cross Origin Resource Sharing (CORS) enables access to Context Store requests that originate from other domains.

The configuration is available on the **Avaya Breeze > Configuration > HTTP Security** page.

*** Note:**

When you enable the client certificate challenge , web clients cannot authenticate through Javascript, that is, Ajax calls. As the browser and the Javascript layer are not connected, the required client certificate is not sent.

Port utilization

For Context Store and Avaya Breeze™ port information, see the applicable Avaya Breeze™ and Context Store Port Matrix documents at <https://support.avaya.com/security>.

Chapter 10: Troubleshooting

Troubleshooting overview

This chapter provides information about the alarms and events that Avaya Context Store Snap-in generates. It also lists the Context Store log files. For information on troubleshooting issues related to Avaya Breeze™, see the *Maintaining and Troubleshooting Avaya Breeze™* guide.

Alarms

Overview

Context Store generates alarms whenever an error occurs.

You can view, search, export, and configure alarms from the System Manager web portal. The alarms information is available in the **Services > Events > Alarms** page in System Manager.

Prerequisites

Using System Manager, you must create a simple network management protocol (SNMP) target profile and assign the profile to your network managing system (NMS).

For more information about creating and managing SNMP target profiles, see *Administering Avaya Aura® System Manager* available at <http://support.avaya.com>.

Alarm status

Context Store alarm statuses are consistent with those of the other snap-ins deployed on Avaya Breeze™. These alarms can have any of the following two statuses:

Status	Description
Raised	An alarm has been generated. Software recovery actions have failed to correct the problem.
Cleared	The problem has been fixed and the alarm has been cleared. This state must be set manually.

Context Store generates two alarm IDs for the same alarm- one when raising the alarm and the other when clearing the alarm. The alarm ID that Context Store generates for clearing an alarm contains *CLR* as a prefix in the original alarm ID that was in *Raised* state.

Alarm severities

Avaya Context Store Snap-in generates alarms with two severity types, as described in the following table:

Severity	Description
Major	All the Context Store alarms in Raised state are of Major severity.
Normal	Context Store generates a clear alarm with Normal severity.

For more information on alarm statuses and severities, see *Maintaining and Troubleshooting Avaya Aura® Avaya Breeze™*.

ContextStoreManager_CS_EVT_1

Event ID	ContextStoreManager_CS_EVT_1
Default event text	Cluster requests per second is greater than the High configured threshold.
Event level	Major
Trigger component	ContextStoreRest: Processing number of requests

Problem description

The REST requests per second is greater than or equal to the configured high threshold for the service or the cluster.

The alarm is cleared automatically when the service request per second is lower than the value in the Context Store attribute **CS Threshold: Service Low Requests per Second**.

Note:

You can configure the high threshold value by updating the ContextStoreManager attribute **CS Threshold: Service High Requests per Second**. The value is 1240.

Proposed solution

Procedure

Contact the support engineer to ensure that the traffic load is minimized.

ContextStoreManager_CS_EVT_2

Event ID	ContextStoreManager_CS_EVT_2
Default event text	Cluster lacks enough ContextStoreRest instances to support the maximum requests/second load.

Event level Major

Trigger component ContextStoreRest: Number of live instances in a cluster

Problem description

Multiple instances of ContextStoreRest failed and Context Store cannot support the service high availability requests for every second.

The system clears the alarm when the number of deployed ContextStoreRest interfaces is equal to or more than 2.

Proposed solution

Procedure

1. Ensure that all the Avaya Breeze™ nodes in the cluster are running.
2. Ensure that all Avaya Breeze™ nodes have network connection access.
3. Ensure that all Avaya Breeze™ nodes have ContextStoreRest snap-in deployed.
4. Ensure that the Avaya Breeze™ cluster has ContextStoreManager snap-in deployed.

ContextStoreManager_CS_EVT_3

Event ID ContextStoreManager_CS_EVT_3

Default event text Cluster lacks enough ContextStoreRest instances to support the maximum requests/second load and be highly available.

Event level Major

Trigger component ContextStoreRest: Number of live instances in a cluster

Problem description

The system cannot support the service high threshold requests per second in the event of another instance failure.

The alarm is cleared when number of REST instances in the cluster is equal to or more than 3.

Proposed solution

Procedure

1. Ensure that all Avaya Breeze™ nodes in the cluster are running.
2. Ensure that all the Avaya Breeze™ nodes have network connection access.
3. Ensure that all Avaya Breeze™ nodes have ContextStoreRest snap-ins deployed.
4. Ensure that the Avaya Breeze™ cluster have ContextStoreManager snap-in deployed.

ContextStoreManager_CS_EVT_4

Event ID	ContextStoreManager_CS_EVT_4
Default event text	Failed to persist item to external data mart.
Event level	Major
Trigger component	ContextStoreManager: EDM deployment

Problem description

System cannot persist information from datagrid to External Data Mart. This error occurs if Context Store cannot perform any of the following:

- Connect to the database configured for External Data Mart.
- Validate schema or data of the database configured for External Data Mart.

The alarm is cleared when the connection with database is restored with External Data Mart.

Proposed solution

Procedure

1. Ensure that Context Store is able to connect to the external database.
2. Ensure that the values that you have specified for the External Data Mart attributes in the ContextStoreManager attributes page are correct. If the values are incorrect:
 - a. Update the values.
 - b. Redeploy ContextStoreManager and ContextStoreRest.
3. Ensure that the database schema is as per the Context Store requirements. If the database schema is incorrect:
 - a. Update the database schema.
 - b. Redeploy ContextStoreManager and ContextStoreRest.

ContextStoreManager_CS_EVT_5

Event ID	ContextStoreManager_CS_EVT_5
Default event text	ContextStoreNotify Subscription Disabled see log for Details.
Event level	Major
Trigger component	ContextStoreNotify

Problem description

This alarm is raised when there is a failure to connect to an endpoint and the subscription of that endpoint is disabled automatically.

Proposed solution

Procedure

1. Check logviewer on System Manager to identify details about the subscription that is disabled.
2. Verify the validity of the endpoint and enable the subscription.

Events

Overview

Context Store generates events for warning purpose only.

You can view the events in Log viewer at the following directory: `Home/Services/Events/Logs/Log Viewer`.

CSAUD_5

Event ID	CSAUD_5
Default event text	Instance requests per second is greater than the configured threshold.
Event level	Warning

Problem description

Context Store creates the `CS_AUDIT_5` event log in System Manager when Context Store operates at the maximum capacity. The system operates at maximum capacity when the request per second is greater than or equal to the value of the ContextStoreManager attribute `CS Threshold: Instance High Requests per Second`.

Proposed solution

Procedure

Contact the support engineer to ensure that the traffic load is minimized.

CSAUD_7

Event ID	CSAUD_7
Default event text	Instance latency is greater than the configured threshold.
Event level	Warning

Problem description

Context Store creates the CSAUD_7 event log in System Manager when the average time for the context data to travel between the client and Context Store exceeds the value that you have specified for the ContextStoreManager attribute *CS Threshold: High Latency*.

Proposed solution

Procedure

1. Ensure that all Avaya Breeze™ nodes in the cluster are running.
2. Ensure that all Avaya Breeze™ nodes have network access.
3. Ensure that all Avaya Breeze™ nodes have ContextStoreRest snap-in deployed.
4. Ensure that all Avaya Breeze™ clusters have ContextStoreManager snap-in deployed.
5. Verify that the context size of the requests is as per the Context Store requirement.

CSAUD_8

Event ID	CSAUD_8
Default event text	Instance error rate is greater than the configured threshold.
Event level	Warning

Problem description

Context Store creates the CSAUD_8 event log in System Manager when the rate of the failed requests returned to the client from Context Store exceeds the threshold value that you have specified in the ContextStoreManager attribute *CS Threshold: High Error Rate*.

Proposed solution

Procedure

1. Ensure that all Avaya Breeze™ nodes in the cluster are running.
2. Ensure that all Avaya Breeze™ nodes have network access.

3. Ensure that all Avaya Breeze™ nodes have ContextStoreRest snap-in deployed.
4. Verify that all Avaya Breeze™ clusters have ContextStoreManager snap-in deployed.
5. Ensure that the traffic load does not exceed the high threshold request per second.

CSAUD_10

Event ID CSAUD_10

Default event text Cluster average lease time is greater than the configured threshold.

Event level Warning

Problem description

Context Store creates the CSAUD_10 event log in System Manager when the average lease time for data stored by Context Store exceeds the threshold value.

Proposed solution

Procedure

No corrective action is required.

CSAUD_11

Event ID CSAUD_11

Default event text Cluster requests per second is greater than the configured Low threshold.

Event level Information

Problem description

Context Store creates the CSAUD_11 event log when cluster requests per seconds is greater than the configured low threshold value.

CSAUD_13

Event ID CSAUD_13

Default event text Instance requests per second is greater than the configured Low threshold.

Event level Warning

Problem description

Context Store creates the `CSAUD_13` event log in System Manager when the instance requests per second is greater than the configured Low threshold.

Proposed solution

Procedure

1. Ensure that all the Avaya Breeze™ nodes in the cluster are in the running state.
2. Ensure that all the Avaya Breeze™ nodes have network access.
3. Ensure that all Avaya Breeze™ nodes have the ContextStoreRest snap-in deployed.
4. Ensure that all Avaya Breeze™ clusters have ContextStoreManager snap-in deployed.

Logging

Context Store log files

The following table describes the log name and location of the logs related to Context Store:

Log name	Location	Description
Context Store <service> logs	<code>/var/log/Avaya/services/<ServiceName>/<ServiceName>.log</code>	Logs related to Context Store services, such as ContextStoreManager, ContextStoreRest, and so on.
External Data Mart logs	<code>/var/log/Avaya/dcm/pu/ContextStoreManager/ContextStoreManager-cs-edm.log</code>	Logs related to the External Data Mart feature.
ASM logs	<code>/var/log/Avaya/sm/asm.log</code>	Logs related to Avaya Breeze for platform APIs and features used by Snap-ins.
Text logs	<code>/var/log/Avaya/sm/TextLog_date_time.log</code>	Provides information on problems that might be blocking services.
Event logs	<code>/var/log/Avaya/services/event.log</code>	Alarms and events raised by Context Store snap-ins.
Data grid logs	<code>/var/log/Avaya/dcm/</code>	Data grid log file location.

Log level configuration

You can adjust the logging level of all snap-in services individually from **Home > Elements > Avaya Breeze > Configuration > Logging**.

Log file configuration

The Context Store service log files are configured, by default, to store up to 10 log files of maximum 10MB each.

This size and number of log files stored, is configurable for each individual Context Store service in the `/opt/Avaya/Common/conf/log4j.properties` file:

- `log4j.appender.<service-name>.MaxFileSize=10MB`
- `log4j.appender.<service-name>.MaxBackupIndex=10`

Frequently asked questions

Where do I find documentation for Context Store?

Context Store documents are available at the Avaya support portal: <https://support.avaya.com/documents>.

For each major release of Context Store there are three documents published:

- Avaya Context Store Snap-in Release Notes
 - Describes new features and feature modifications in the release.
 - Describes prerequisites for installation and upgrade procedures and provides the PLDS ID and MD5 checksum for every available component.
 - Lists known issues that exist in the present release as well as issues which have been resolved in this release since the previous release.
 - Contains the attribute configurations for all certified Context Store deployments.
- Avaya Context Store Snap-in Reference
 - Contains overview information about Context Store and its features.
 - Contains detailed instructions for the deployment and configuration of Context Store.
 - Discusses high availability, performance and security aspects of Context Store.
 - Contains some troubleshooting information
- Avaya Context Store Snap-in Developer Guide
 - Contains detailed usage information for Context Store features and interfaces.
 - Contains tutorial sections for certain features.
 - Provides complete API references for all interfaces to Context Store (ContextStoreRest).

Where can I get documentation and help for products related to Context Store?

Context Store is a Snap-in service that runs on the Avaya Breeze™ platform. Plugins are available to integrate Context Store into Avaya Aura Orchestration Designer callflows (to be run on Avaya Aura® Experience Portal) and Engagement Designer workflows.

Documentation for all Avaya products is available at the Avaya support portal: <https://support.avaya.com/documents>.

DevConnect forums exist to provide support for the following products:

- Avaya Breeze™ forum: <http://www.devconnectprogram.com/forums/forums/show/18.page>
- Avaya Aura Orchestration Designer forum: <http://www.devconnectprogram.com/forums/forums/show/15.page>
- Engagement Designer forum: <http://www.devconnectprogram.com/forums/forums/show/33.page>

Where do I get plugins, SDKs, and sample resources for Context Store?

Sample resources, plugins, and SDKs for Context Store can be downloaded from the Avaya DevConnect portal: https://www.devconnectprogram.com/site/global/products_resources/avaya_breeze/avaya_snap_ins/context_store/overview/index.gsp

In the **Releases > Downloads** section you will find:

- Links to download the documents applicable to the release (Release Notes, Reference Guide and Developer Guide)
- Context Store components which are not distributed as Avaya Breeze™ snap-in services
 - Context Store Java SDK
 - Context Store Pluggable Data Connector for Orchestration Designer / Avaya Aura Experience Portal
- The Capacity Planner Tool for estimating sizes when designing a Context Store deployment
- Sample client applications
 - Event Streams sample application
 - ContextStoreNotify sample consumer
 - Sample workflows for Avaya Engagement Designer
 - Sample workflows for Orchestration Designer / Avaya Aura® Experience Portal
- Sample implementations
 - Example of Audit Trail user interface application

- Example of ScreenPop application which sorts the returned data

Applicability of Context Store licenses

Below is the breakdown of applicable licenses for the Context Store product.

*** Note:**

Numerous Context Store services and features exist but those are currently not charged for and there are no applicable license material codes.

Licensed Feature Name (WebLM)	License Description (Sales/Offer Definition)	Material Code	Free ?	Applicable/Related Feature
Context Store Server	PER SERVER LIC	305220	N	Context Store Snap-In Service. One license required for every server on which Context Store is deployed. For example: 3 per cluster..
Context Store Users	USER LIC	305221	N	ContextStoreScreenPop. One license required for every concurrent user of ContextStoreScreenPop.
Context Store AEP Connector	AEP CONNECTOR LIC	307379	Y	CS Pluggable Data Connector for Avaya Aura Experience Portal. One license required per environment or cluster.
Context Store API	API CLIENT LIC	307390	N	CS SDK This is the license for CS JAVA SDK and is only required if customer wants to build their own custom integrations to CS using the SDK we provide. One license required per environment or cluster.
Context Store GEO Redundancy	GEO REDUNDANCY LIC	380821	N	Geo-Redundant CS Deployment Only one GEO license is required for a cluster to have a license Geo-redundant deployment (which is two linked CS Clusters).
<p>* Note: 385461 is an entitlement license (i.e. no cost) that is not listed in the Offer Definition but is in the ASD tool.</p>				

How do I verify if Context Store is successfully deployed?

The most reliable way to verify deployment is to create and retrieve test Contexts through the ContextStoreRest interface. You can submit requests to the Cluster IP address (which will round-robin request to each available ContextStoreRest instance) or directly to the security module IP address of a server to verify that each is working as expected.

Helpful hint: If you create contexts without specified contextIds with the shortid=true parameter (<http://clusterIP/services/ContextStoreRest/cs/contexts/?shortid=true>), the first 1-3 digits of the returned, auto-generated contextId match the last octet of the security module IP address of the server on which the context was created. So with just a few simple create requests to the cluster IP address, you can verify that each of the servers is processing requests and therefore ContextStoreRest is functioning correctly.

Submit test requests using either a ReST client such as Postman (for Google Chrome) or the live API built-in to ContextStoreRest itself (<http://clusterIP/services/ContextStoreRest/>)

*** Note:**

Sample Postman request collections are available to download from the Context Store DevConnect for all ContextStoreRest operations and features.

How do I determine the appropriate size for my Context Store deployment?

The appropriate size for a Context Store deployment is based on the following variables:

- The average size of context objects created
- The average lease time of the created context objects
- The rate at which new context objects are being created
- The inclusion of additional Context Store features, such as External Data Mart, geo-redundancy, high availability, Context Store Event Streams , Audit Trail, and aliasIds, which themselves have memory requirements.

The Context Store Release Notes, available on Avaya Support site, contains the ContextStoreManager attribute configurations for 13 certified deployments of varying sizes; from a single-node with 8 GB of memory up to a cluster of three nodes with 128 GB of memory each.

You can also download a Capacity Planner Tool that assists you with custom sizing, from <http://www.avaya.com/devconnect>. This tool accepts inputs for the four variables and provides the best-estimate recommendations

Related links

[How do I determine the appropriate size for my External Data Mart deployment?](#) on page 116

How do I verify if Context Store is successfully connected to the External Data Mart?

If you have access to the database itself, the simplest way to verify is:

1. Create a context with the persistToEDM flag set to true =>


```

      {"contextId": "PersistedContext", "persistToEDM": "true", "data":
      {"key1_name": "value1_data"}
```
2. Run an SQL query to search the database for this context =>


```

      select * from
      cs_operation where context_id = 'PersistedContext'
```

If you cannot query the database directly, you can use ContextStoreQuery ReST interface to verify that the context has been written to the External Data Mart =>
 <http://clusterIP/services/ContextStoreQuery/edm/contexts/audit/{contextId}/?data=true>

How do I determine the appropriate size for my External Data Mart deployment?

There is not “one size fits all” answer for External Data Mart (EDM) size. The appropriate size for the EDM is directly linked to the sizing variables listed in “How do I determine the appropriate size for my Context Store deployment?”

You must also consider questions such as, how long the context data will remain in the EDM and will the data be truncated after a certain period of time.

Though the exact details might vary from vendor to vendor, the following table is a rough guide to the amount of disk space consumed by the EDM attached to a system running at high capacity with a large percentage of create and update operations.

Average context size (KB)	Requests per second	GB per hour written to EDM
2	1240	8.35
16	1000	55
32	800	88
64	500	110

Calculating specific quantities when the Audit Trail feature is enabled (required for Customer Journey) is a bit different as it depends entirely on the length of the audit trail stored for each context. The audit trail is the number of interactions with that context during its life span. It also depends on the amount of additional information being stored within the context object.

In an Avaya Oceana™ Solution deployment, you must include the required Avaya Oceana™ Solution service data and the additional customer created data in estimations.

For example, based on analysis of some sample data from an Avaya Oceana™ Solution lab for a voice and chat contact, the minimum context required for Avaya Oceana™ Solution (and assuming three elements created in the Customer Journey), the storage per contact is ~3 KB

Related links

[How do I determine the appropriate size for my Context Store deployment?](#) on page 115

What JDBC driver is required to use the External Data Mart feature

The External Data Mart feature is configured to work with a PostgreSQL database by default. This is an open-source database and therefore the required driver is distributed with the Context Store software.

If you are using an Oracle or Microsoft SQL Server database, Avaya Context Store does not have permission to re-distribute the required drivers. The JDBC driver must therefore be manually loaded into the Breeze Element Manager and then installed on the Context Store cluster. See instructions for doing this in the *Loading JDBC driver to System Manager* section in the *Avaya Context Store Snap-in Reference* guide.

SQL Server

Download Microsoft JDBC Driver 6.0 for SQL Server from <http://www.microsoft.com>:

- Breeze 3.2 and earlier runs on Java 7, therefore the SQL Server JDBC driver selected must support the jre7 version (in Microsoft JDBC Drivers 6.0 for example, this would be the sqljdbc41.jar)
- Breeze 3.3 (and later) runs on Java 8, therefore the SQL Server JDBC driver selected must support the jre8 version (in Microsoft JDBC Drivers 6.0 for example, this would be the sqljdbc42.jar)
- Consult Microsoft JDBC Driver documentation to make sure you have the correct driver for your database version
- Use of an incompatible driver will result in failures in the system and/or SQL exceptions in logs

Oracle

Download the applicable Oracle JDBC Driver from <http://www.oracle.com>.

- The JDBC driver required depends on the database version that is used, you must consult Oracle JDBC Driver documentation to make sure you have the correct driver for your database version.
- Use of an incompatible driver will result in failures in the system and/or SQL exceptions in logs

How do I submit requests to the ContextStoreRest interface if access through external ReST client is blocked?

If customer's network blocks access for ReST clients, such as Postman (for Google Chrome) or the live API built in to ContextStoreRest itself (`http://<IP_ADDRESS>/services/ContextStoreRest/`), submit CURL requests from command line on a computer which has tunnel/proxy access to the environment.

*** Note:**

When you submit the CURL requests from command line, Context Store does not display a status code. An error message or the data requested is displayed.

Create a context

Use the following command to create a context:

```
curl -H "Content-Type: application/json" -X POST -d
'{"contextId":"DemoContext1","groupId":"demo","data":
{"key1_name":"value1_data","key2_name":"value2_data","key3_name":"value3
_data"}}' http://<IP_ADDRESS> /services/ContextStoreRest/cs/contexts/
```

For secured clusters, use the following command to create a context:

```
curl -H "Content-Type: application/json" -X POST -d
'{"contextId":"DemoContext1","groupId":"demo","data":
{"key1_name":"value1_data","key2_name":"value2_data","key3_name":"value3
_data"}}' https:<IP_ADDRESS> /services/ContextStoreRest/cs/contexts/ -k
```

Retrieve a context

Use the following command to retrieve a context:

```
curl http://<IP_ADDRESS> /services/ContextStoreRest/cs/contexts/
DemoContext1/
```

For secured clusters, use the following command to retrieve a context:

```
curl https://<IP_ADDRESS> /services/ContextStoreRest/cs/contexts/
DemoContext1/ -k
```

Problems with data grid deployment

If the resources available in the cluster of Avaya Breeze™ servers is not sufficient for the configured deployment (data grid size plus optional features selected), the deployment fails. For attribute values for each certified deployment, see *Avaya Context Store Snap-in Release Notes*.

If deployment issues occur, check your configuration settings are correct, check the `/var/log/Avaya/services/ContextStoreManager` and `/var/log/Avaya/dcm/gs-esm-<X>` logfiles for errors related to deployment.

The following errors indicate there has been a data-grid deployment failure:

- Instead of the ContextStoreManager status page located at `http://<IP_ADDRESS>/services/ContextStoreManager/`, the following error is displayed: Error 503: Internal error Could not read statistics object, check CSSpace settings. EDM PU deployment failed, check EDM settings, or try accessing the homepage via load balancer IP or other node GEO PU deployment failed, review GEO settings, or try accessing the homepage via load balancer IP or other node.
- A 404 not found response is returned for non-read request. For example, Error 404: `javax.servlet.UnavailableException: Space ContextStoreManagerSpace could not be found in 60000 milliseconds to create a listener.`

- The following error is displayed: Number of retries (100) to create proxy to grid has been exhausted, machine restart required.

*** Note:**

It is imperative that nodes are shut down at the same time to ensure that the data-grid is fully undeployed before the next deployment attempt takes place. The last node standing will keep the data-grid alive. So when nodes have already started back up before that last-man-standing shuts down, the data grid does not get redeployed. This necessity is stated in the documentation, this is what we mean by “simultaneous restart”.

- After a correct fresh start of the cluster, you will see these lines in the ContextStoreManager log file (on whichever node has taken charge of the deployment. Whoever got there first)

```
- grid.EsmGrid INFO - [M:deployElasticSpace][T:null].
  ContextStoreManagerSpace not found, deploying...
- grid.EsmGrid INFO - [M:deployElasticPU][T:null]. ContextStoreSpace
  not found, deploying...
- grid.EsmGrid INFO - [M:deployStateless][T:null]. EDM-Mirror-
  Service is deployed with status BROKEN.
- Followed quickly by manager.AbstractPUManager INFO -
  [M:checkDeploymentStatus][T:null]. [EDM-Mirror-Service] is in
  status [INTACT] a few seconds later
```

- If these deploying messages do not appear on any ContextStoreManager logs since restart and instead you get already deployed messages, you have not restarted the cluster correctly.

```
- grid.EsmGrid INFO - [M:deployElasticSpace][T:null]. space with name
  ContextStoreManagerSpace is already deployed.
- grid.EsmGrid ERROR - [M:deployElasticPU][T:null]. space
  ContextStoreSpace is already deployed.
```

How do I verify if connection between geo-redundant clusters is successfully established?

The easiest way to verify connection between the clusters is to create a context in one cluster and then retrieve it from the other cluster.

1. Create a context on Cluster A.
2. Retrieve the context from Cluster A (to verify it was created successfully)
3. Retrieve the context from Cluster B (to verify it was replicated to the other cluster successfully)
4. Create a context on Cluster B (to verify replication is working in both directions).
5. Retrieve the context from Cluster B.
6. Retrieve the context from Cluster A.

Additionally, you can identify the Grid Services Container (GSC) in each cluster which is hosting the Gateway service used for geo redundancy replication by searching for the term "GEO-Gateway-Service". In that file (in each cluster) you can then easily find the state changes for the Gateway link between the two clusters: `Connection delegator: moved to state: CONNECTED/ DISCONNECTED.`

Does Context Store require runtime configuration changes?

Some aspects of Context Store configuration can be changed dynamically, but not all. See lists below for details.

Changes requiring cluster restart

- Data-grid sizing is not dynamic (ContextStoreManager "Startup Configuration" attributes); you must shut down all the nodes and start the nodes simultaneously if you make changes to the data-grid.
- The Context Store cluster does not support scaling out dynamically. After adding or removing a node to the cluster, you must shut down all the nodes and start the nodes simultaneously.

Changes requiring service reinstall

- ContextStoreQuery - reinstall this service after attributes changes.

Changes requiring that the feature is toggled off and on again

- ContextStoreManager "External Data Mart Configuration" attributes - enable/disable the EDM feature(s) to make configuration changes.
- ContextStoreManager "Geo Redundancy Configuration" attributes - enable/disable the GEO feature to make configuration changes.
- ContextStoreNotify - to make changes to the configuration of a subscription, you must first disable the subscription, make the changes, and then enable the subscription again.

Changes that do not require any action other than the change in attribute value itself

- ContextStoreManager "Run-time Service Configuration"
- ContextStoreManager "Streams Configuration"
- ContextStoreRest "External Data Mart Configuration"
- ContextStoreRest "Advanced Configuration"
- "Enable Centralized Logging" for any service

Why is the ContextStoreRest interface returning 503 Service Temporarily Unavailable for all my requests?

The 503 errors indicate that either the Avaya Breeze™ servers or the cluster which hosts Context Store is in **Denying** state.

On the main Cluster Administration page, select the check box beside the affected cluster and change the **Cluster State** to **Accept New Service**. If the state is already set as expected, try toggling the state to **Deny New Service** and then set it back to **Accept New Service**.

Why is ContextStoreRest interface blocking all requests with throttled error message?

Requests to the ContextStoreRest interface is throttled in the following scenarios:

- Service instance is throttled when request rate on node exceeds threshold or Cluster is throttled when request rate for whole cluster exceeds threshold. Check the following applicable threshold configurations:
 - CS Threshold: Instance High Requests per Second
 - CS Threshold: Instance Low Requests per Second
 - CS Threshold: Service High Requests per Second
 - CS Threshold: Service Low Requests per Second
- Request error rate exceeds the configured threshold. Check the following applicable threshold configurations:
 - CS Threshold: Max Error Rate
- Authorization token provided in request header is not valid (ContextStoreRest is integrated with Breeze Authorization service).
- More than one node is disconnected from the cluster and the "Cluster Deny Service on two node outage" geo-related attribute is enabled.

 **Note:**

If a cluster in a geo-redundant deployment must be restarted, it is recommended that the "Cluster Deny Service on two node outage" attribute is disabled before the restart and then re-enabled afterwards. If this 'two node outage' check is executed before the other nodes have started up and joined the cluster – this will trigger throttling on the cluster.

Why can't I set the state of my cluster to Accept New Service?

If it is not possible to activate the cluster, check the license status of the Avaya Breeze™ servers in the cluster.

On the main Cluster Administration page, check that the License Mode column for each Avaya Breeze™ server used in the affected cluster shows a green check-mark. This means that the license is valid.

What is the maximum lease time permitted for a context?

There is effectively no limit on context lease but it is vital to take lease time into consideration when sizing a Context Store deployment as this can drastically change the amount RAM required in the cluster to store the context data for such a long time.

The default lease time is 2 hours (7200 seconds) and the maximum lease time threshold (above which a warning will be logged but request will not be blocked) is 4 hours (14400 seconds).

Both of these figures can be set anywhere within the range specified in the Context Store documentation. As per the description of lease parameter in the Avaya Context Store Developer Guide, "The valid lease must be in the range 1 to 2147483647." (2147483647 is the maximum value permitted for an integer field such as this.)

In the Capacity Planner tool, configuration sizing options are offered for up to 90 hours or days (though if you're storing data for 90 days, what you need is a database and not Context Store!)

What are the Context Store limits for data and throughput?

The limits in the table below should not be exceeded. These limits are not enforced at an API level.


Limit Type	Limit Value	Comments
Max context size	Recommend 64kb max	<p>500kb is the largest data size to which Context Store has been tested and this size of data is not recommended for regular traffic.</p> <p>Context Store data grid stores all contexts in-memory. Therefore, having control over the maximum amount of memory per context allows system administrators to properly size Context Store environment and prevent clients from over-utilizing memory.</p> <p> Note: The standard context size used for deployment and testing is 2kb.</p>

Table continues...

Limit Type	Limit Value	Comments
Max Contexts	variable, dependent on system resources	<p>The maximum contexts limit is dependent on the memory resources available in Context Store. Within the confines of the system's resources, the maximum number of contexts possible is directly related to the lease time and the context size.</p> <p>Context Store has been engineered to support 1,240 requests per second, writing 2kb context entries with 2 hour lease, on a full spec lab as per the defined system requirements. This equates to just under 9 million context entries (2kb each) stored in memory at any given time (just under 17GB of context data).</p> <p>If the size or lease increases, the maximum number that can be stored in will obviously be reduced.</p>
Max Contexts linked to Group ID	100	
Max Contexts returned by Group ID	100	Note that a group GET operation returns the contextIds and metadata associated with the specified group and not the data itself.
Max lease	variable, dependent on system resources	The maximum lease limit is dependent on the memory resources available in Context Store. Within the confines of the system's resources, the maximum number of contexts possible is directly related to the lease time and the context size.
Min lease	1 second	
Max Instance Reqs/Sec	variable, dependent on system resources	A ContextStoreRest instance will be throttled if the CS Threshold: Instance High Requests per Second limit is breached.
Max Service Reqs/Sec	variable, dependent on system resources	The ContextStoreRest service will be throttled if the CS Threshold: Service High Requests per Second limit is breached.

Why can't I access Context Store from a web client?

Due to JavaScript's same-origin policy, requests from a script stored on a server can only send requests back to that server. When blocked, the JavaScript XMLHttpRequest status = 0

To allow a script to send requests to and receive responses from Context Store, you must enable the **Allow Cross-origin Resource Sharing for all** setting on **Home > Elements > Avaya Breeze > Configuration > HTTP Security > HTTP CORS**

CORS must be enabled when using any web client such as the Streams client, the Customer Journey Visualization application (part of the ContextStoreQuery service) or website integration (using JavaScript SDK or integration with ContextStoreRest interface).

Why is Customer Journey unable to retrieve data?

1. Verify that Cross Origin Resource Sharing (CORS) has been enabled in System Manager through **Avaya Breeze > Configuration > HTTP Security**.
2. Check your External Data Mart configuration as per the attributes configuration provided in the *Why is the External Data Mart not working?* section.

Why is the External Data Mart not working?

The following checks need to be performed to troubleshoot an EDM connection issue to ensure the configuration is correct:

- Check the connection by ensuring that you can ping the database server from the Breeze cluster node.
- Verify the database user specified in the attribute EDM: Username in System Manager has read/write access to the `CS_OPERATION` table and the `CS_PROVISION` table.
- Verify the specified database name matches with the database name specified for the associated attribute in System Manager.
- Check that the JDBC driver in System Manager is under JDBC providers. Postgres does not require a driver to be loaded in System Manager. For Oracle or MS SQL server verify that the driver is compatible with the version of the database.
- Verify the following System Manager attributes are set for ContextStoreManager:

Attribute name	Required Value/Format	Sample value	Notes
EDM: Enable Persistence to database	True or False	True	This must be set to true to enable EDM
EDM: Database type	- PostgreSQL - Oracle - Microsoft SQL Server	PostgreSQL	The type selected must match the database.
EDM: Database host	Host address for External Data Mart database.	10.20.30.40	
EDM: Database port	Port for External Data Mart database.	5432	
EDM: Database Name	Name of the database used as External Data Mart.	csedm	Ensure that the configured database name matches the actual name of the created database.

Table continues...

Attribute name	Required Value/Format	Sample value	Notes
EDM: Username	Username for the External Data Mart database connection	edm_user	
EDM: Password	Username for the External Data Mart database connection	edm_password	Verify in DB admin tool that the DB user has access to the CS_OPERATION table
EDM: Mirror Service container size	Memory required for the External Data Mart Mirror Service deployment. Numeric value only is interpreted as GB. MB can be specified with an 'm' or 'mb' after the number. Example, 128m	128m	If this allocation is invalid then the EDM PU will not deploy.

- Verify the following System Manager attributes are set for ContextStoreQuery:

Attribute name	Value	Sample value	Notes
EDM: Username	<db_username>	edm_user	This is the same value set in ContextStoreManager attributes
EDM: Password	<db_user-password>	edm_password	This is the same value set in ContextStoreManager attributes

- *API Validation*

1. Download and install the POSTMAN web client using the Chrome browser.
2. Download the Context Store Postman Request Collection on DevConnect.
3. Import the `ContextStore3.5.postman_collection.json` file into the POSTMAN client.
4. Within `ContextStore3.5.postman_collection.json`, run **Create Persisted Context**

This runs using the ContextStoreRest interface.
5. Verify that the context is persisted to the database.
6. Use the `ContextStore3.5.postman_collection.json` to check that the context can be retrieved through the ContextStoreQuery interface.

- *Microsoft SQL Server DB User*

If you are using Microsoft SQL Server:

- The db user configured for the EDM feature must have database ownership or the system administrator privileges for this connection to be successful.
- From the security profile of the database user, you must set the Context Store database as the default database for this user.

- *Oracle Database*

If you are using an Oracle Database:

- The Oracle driver being used must be compatible with the version of the Oracle database.
- For Context Store 3.5, the tested and supported Oracle driver version for Context Store 3.5 is ojdbc6 driver version 11.2.0.4, 12.1.0.1, 12.1.0.2 which are all available in Oracle Database JDBC Downloads webpage.
- There should only be one Oracle driver installed on the cluster, if the driver has been changed, the nodes must be rebooted.

How can I carry out a health check in Context Store interfaces?

To check the system health:

In postman use the following GET request:

```
http://clusterIP/services/ContextStoreRest/cs/contexts/cs_status_check/
```

If the data grid is in good health, the system displays 200 OK response along with either of the following messages:

- Context Store cluster is UP.
- There is an issue with the Context Store cluster.

You can execute this health check from other Context Store interfaces as well:

- ContextStoreScreenPop: `http://clusterIP/services/ContextStoreScreenPop/cs/pop/cs_status_check`
- ContextStoreSoap: **Get Status** operation
- CS PDC: **Check Context Store status** operation
- Java SDK: `checkCSStatus()` method
- JavaScript SDK: `getContextStoreStatus()` method

How to I perform troubleshooting for unavailable customer journey?

- Verify that the basic Context Store functionality is working. For more information, see [How do I verify if Context Store is successfully deployed?](#) on page 115.

- Verify that persistence of your Context data to the External Data Mart is working. For more information, see [How do I verify if Context Store is successfully connected to the External Data Mart?](#) on page 116.
- For multi-session Customer Journey, a matching groupId must be set for each associated Context object. You can see this groupId value in the Contexts metadata.
 - ReST request to check Context metadata (note, the full ContextStoreRest API is available in the Context Store Developer Guide) `http://CLUSTER_IP/services/ContextStoreRest/cs/contexts/meta/WorkRequestId`
- Verify that you can retrieve the Journey data through the ContextStoreQuery interface itself, leaving Visualization UI out of the equation first to simplify troubleshooting.
 - ReST request to ContextStoreQuery to retrieve Journey information `http://CLUSTER_IP/services/ContextStoreQuery/edm/contexts/audit/groups/context/WorkRequestId`

Do we have a canned solution we use to link CC Elite to Context Store?

No. There is no direct interaction available between Contact Center Elite and Context Store. For voice calls, Avaya Aura Experience Portal (or any alternative IVR) is what writes related data into Context Store. Context Store offers a wide variety of interfaces, SDKs and plugins which can be used to do this.

Why am I seeing a BAD_REQUEST response when using ContextStoreTask Types in an Engagement Designer workflow?

It is possible that the incorrect inputs are being passed to the ContextStoreTask Type. Review the online Engagement Designer Help for the ContextStoreTask by clicking the **Help** icon on the Task or download the sample flows from the Avaya Context Store Snap-in section of <http://www.devconnectprogram.com>

Context data at rest. Is data encrypted while in the Context Store?

Context Store supports customer encrypted data. See [Sensitive data](#) on page 12. There is no provision for encryption as a service. Be aware that the context data is never at rest as the Context Store data-grid is in memory only, so data is never written to disk. When the cluster is shutdown or restarted, all data disappears from memory. Additionally, the Breeze cluster can be configured to use as a secure data-grid. The password is set via cluster attributes.

Context Store Request is still being served over HTTPS even though cluster security is disabled

To disable security on a Context Store Cluster, do the following:

- Set the Context Store Cluster state to deny
- Disable security on the Context Store Cluster
- Set the Context Store Cluster state to accept new service.

If a browser is used, ensure that the browsing data is cleared.

Chapter 11: Related resources

Documentation

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

Title	Use this document to understand:	Audience
Installing		
<i>Deploying Avaya Breeze™</i>	The procedures on deploying the Avaya Breeze™ services.	<ul style="list-style-type: none"> • System administrators • Services and Support personnel • Avaya Professional Services • Implementation engineers
Avaya Breeze™ Overview and Specification	Avaya Breeze™ requirements.	Anyone who wants to have a high-level understanding of Avaya Breeze™ features, functions, capacities, and limitations.
<i>Deploying Avaya Aura® System Manager on VMware® in Virtualized Environment</i>	The procedures for deploying the Avaya Aura® System Manager virtual application in Avaya Aura® Virtualized Environment.	<ul style="list-style-type: none"> • Implementation Engineers • Field Technicians • Business Partners • Solution Providers • Customers
Maintaining		
<i>Avaya Context Store Snap-in Release Notes</i>	The known issues, patches, and workarounds specific to Context Store.	<ul style="list-style-type: none"> • Avaya Professional Services • Implementation engineers
Avaya Breeze™ Port Matrix document	Avaya Breeze™ port information.	<ul style="list-style-type: none"> • Implementation Engineers • Field Technicians • Business Partners • Solution Providers • Customers

Table continues...

Related resources

Title	Use this document to understand:	Audience
Avaya Context Store Port Matrix document	Context Store port information.	<ul style="list-style-type: none"> • Implementation Engineers • Field Technicians • Business Partners • Solution Providers • Customers
Maintaining and Troubleshooting Avaya Breeze™	Avaya Breeze™ alarm statuses and severities.	Anyone who needs information about maintaining and troubleshooting Avaya Breeze™ .
Administering		
<i>Avaya Context Store Snap-in Developer Guide</i>	Developer information for all applicable Context Store features and how to write applications using the Context Store REST Interfaces.	<ul style="list-style-type: none"> • Business process analysts • Developers • Services and Support personnel • Avaya Professional Services
<i>Administering Avaya Breeze™</i>	The procedures to administer and configure the Avaya Breeze™ services.	<ul style="list-style-type: none"> • System administrators • Services and Support personnel
<i>Administering Avaya Aura® System Manager</i>	The procedures to administer and configure System Manager.	<ul style="list-style-type: none"> • System administrators • Services and Support personnel
<i>Avaya Aura® Orchestration Designer Developer's Guide</i>	How to write software using Orchestration Designer that interacts with Context Store.	<ul style="list-style-type: none"> • Business process analysts • Developers
<i>Avaya Aura® System Manager Overview and Specification</i>	Avaya Aura® System Manager certificate-based authentication.	Anyone who wants to have a high-level understanding of System Manager features, functions, capacities, and limitations.
<i>Avaya Engagement Designer Developer's Guide</i>	How to write software using Avaya Engagement Designer that interacts with Context Store. Detailed usage information for the Context Store Task Type for Engagement Designer is documented in the <i>Avaya Context Store Snap-in Developer Guide</i> .	<ul style="list-style-type: none"> • Business process analysts • Developers

Related links

[Finding documents on the Avaya Support website](#) on page 131

Finding documents on the Avaya Support website

Procedure

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

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

7. Click **Enter**.

Related links

[Documentation](#) on page 129

Training

The following courses are available on the Avaya Learning website at www.avaya-learning.com. Enter the course code in the **Search** field, and click **Go** to search for the course.

Course code	Course title
2519W	Introducing Avaya Context Store Snap-in (Self-paced, On-demand)

Support

Go to the Avaya Support website at <http://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. 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.

Index

Numerics

503 Service Temporarily Unavailable requests [120](#)

A

acquire license [50](#)

activate the cluster [121](#)

additional databases

 JDBC driver [34](#)

administer

 grants to authorization client [65](#)

alarms

 event 1 [105](#)

 event 2 [105](#)

 event 3 [106](#)

 event 4 [107](#)

 event 5 [107](#)

 overview

 status

 severities [104](#)

aliasId [38](#)

appropriate size

 context store deployment [115](#)

 external data mart deployment [114](#), [116](#)

architecture [13](#)

 Avaya Breeze [13](#), [50](#)

 Context Store [13](#), [50](#)

attributes [27](#), [76](#)

 cluster [60](#)

Attributes

 ContextStoreRules [87](#)

Audit trail

 audit entry [38](#)

 capacity planning [38](#)

 setting limit [38](#)

authentication [100](#), [102](#)

authorize

 clients [41](#)

Avaya Breeze [9](#), [47](#), [49](#)

Avaya Breeze cluster

 scaling up [46](#)

average latency [99](#)

B

bi-directional data [95](#)

C

canned solution

 CC Elite and Context Store [127](#)

can't access Context Store

 web client [123](#)

capacity [52](#), [99](#)

certified deployment [52](#)

checklist [53](#)

client [23](#)

cluster [58](#)

 scaling out [44](#)

cluster attributes [60](#)

cluster delete [73](#)

cluster state

 Accept New Service [121](#)

configuration

 external datamart [27](#)

configuration requirement [92](#)

configure [58](#), [66](#), [68](#)

 attributes [76](#)

 secure space [101](#)

connection issues

 EDM [124](#)

 External Data Mart [124](#)

context

 maximum lease time [122](#)

context alias [38](#)

context store [11](#)

Context Store

 JavaScript SDK [24](#)

 runtime configuration [120](#)

Context Store connection

 External Data Mart [116](#)

context store data

 encryption [127](#)

Context Store interfaces

 health check [117](#), [126](#)

Context Store limits

 data [122](#)

ContextStoreManager [17](#)

 parameters [76](#)

ContextStoreManager_CS_EVT_1 [105](#)

ContextStoreManager_CS_EVT_2 [105](#)

ContextStoreManager_CS_EVT_3 [106](#)

ContextStoreManager_CS_EVT_4 [107](#)

ContextStoreManager_CS_EVT_5 [107](#)

ContextStoreQuery

 audit trail [19](#)

 parameters [88](#)

ContextStoreQuery snap-in

 customer journey visualization [19](#)

Context Store related products

 finding documentation and help [113](#)

context store request

 cluster security disabled [126](#), [128](#)

ContextStoreRest [18](#)

ContextStoreRest (*continued*)

- parameters [83](#)

ContextStoreRest interface

- throttled error messages [121](#)

ContextStoreRest interface returns

- 503 Service Temporarily Unavailable requests [120](#)

ContextStoreRules

- attributes [87](#)

ContextStoreScreenPop

- parameters [84](#)

Context Store service [64](#)

ContextStoreSoap

- parameters [89](#)

ContextStoresoap snap-in

- geo redundancy [19](#)

ContextStoreSpace

- Context Store Manager [18](#)
- snap-in [18](#)

ContextStoreTasks Type [41](#)

- deployment
 - ContextStoreTasks Type [71](#)
- overview [41, 71](#)

ContextStoreTask Type

- install [72](#)

context time [12](#)

CPU usage [99](#)

CRM

- integration [22](#)

CS Geo notifications [95](#)

customer journey

- interactions [37](#)
- unable to retrieve data [124](#)
- view [37](#)

customer journey visualization

- audit trail [35](#)
- ContextStore Query Snap-in [35](#)

D

database

- JDBC driver [34](#)

database planning [26](#)

database prerequisites [26](#)

database tables [27](#)

database

- MSSQL
 - Oracle [34](#)

data grid [17](#)

data model [12](#)

data replication [95](#)

delete [75](#)

delete a cluster [73](#)

deleting service snap-ins [75](#)

deployment [42, 43, 45, 58, 64–66, 68](#)

- checklist [52, 53](#)
- configuration [52](#)
- configuration information [52](#)

design [13](#)

documentation

- Context Store [112](#)

E

EDM [25, 27](#)

- provisioning [26](#)

EDM connection issues [124](#)

EDM provisioning

- enable [69](#)

enable

- audit trail [38](#)

Enable

- EDM provisioning [69](#)

enabling CORS [123](#)

event

- CSAUD_10 [110](#)
- CSAUD_11 [110](#)
- CSAUD_13 [110](#)
- CSAUD_5 [108](#)
- CSAUD_7 [109](#)
- CSAUD_8 [109](#)

events

- overview
- status
- warning [108](#)

Event streams

- events
 - event streams [22](#)

Experience Portal

- AEP [40](#)
- OD [40](#)
- Orchestration Designer [40](#)

external database

- provision [26](#)

external datamart [26](#)

external data mart [25](#)

- enable [68](#)

External Data Mart

- provisioning [26](#)

External Data Mart connection issues [124](#)

F

failover [92, 97](#)

- scenarios [92](#)

finding Context Store

- documentation [112](#)
- plugins, SDK, and sample resources [113](#)

finding documentation and help

- Context Store related products [113](#)

G

geo [91](#)

Index

geo redundancy	43, 66, 91	new features	38
enable	66	node	42, 43, 45
geo redundant architecture	93	notification	95
goal	11	Notify	
H		agents	22
HA	90, 91	O	
hardware	47	overview	14, 16
high availability	90	Context Store Manager	72
I		ContextStoreRest	72
install	64	P	
install license	50	parameters	
Integration		ContextStoreManager	76
CRM	22	ContextStoreNotify	86
J		ContextStoreQuery	88
Java	23	ContextStoreRest	83
JavaScript SDK		ContextStoreScreenPop	84
client library	24	ContextStoreSoap	89
JDBC driver		PDC	40
external data mart feature	117	deploy	70
JDBC providers		plugins	113
field description	34	plugins, SDK, and sample resources	
K		Context Store	113
key value pair		ports	103
SDK	20	problems	
UCID	20	data grid deployment	118
L		R	
lease time	12	related documentation	129
license	50	requirements	47, 49
Load		REST interface	18
snap-in service	57	S	
svar file	57	sample resources	113
load balancer	92	scalability	99
logs	111	scale up	42, 43, 45
M		scaling out	
mapping	12	Avaya Breeze cluster	44
maximum lease time		scaling up	
context	122	cluster	46
memory	99	Screen Pop	20
N		Screen Pop clients	20
navigate		SDK	23, 113
go back to original location	9	Secure space	
		space security	100
		security	100, 103
		sensitive data	12
		service HA	94
		service preservation	43, 66
		services	
		ContextStoreNotify	21

services (*continued*)

- snap ins [16](#)
- session HA [95](#)
- skills [9](#)
- snap in [16](#)
- soap interface
 - ContextStoresoap api [19](#)
 - soap api [19](#)
- solution [11](#), [109](#)
- solution overview [11](#)
- space security
 - configure [101](#)
- status [57](#)
- support [131](#)
- support failover [97](#)
- synchronized
 - Avaya Breeze servers [57](#)
 - servers [57](#)
- system manager [9](#), [47](#), [49](#)

T

- Third party load balancer
 - configuration [92](#)
- time to live [12](#)
- time-to-live [12](#)
- TLS [102](#)
- Topology [15](#)
- touchpoint [38](#)
- Training
 - Context Store [131](#)
- troubleshooting
 - overview [104](#)

U

- unable to retrieve data
 - customer journey [124](#)
- uninstall [73](#)
- uninstallation [73](#), [74](#), [101](#)
- uninstalling service snap-ins [74](#), [101](#)
- upgrade [72](#)
- Upsert method
 - aliasid [40](#)
 - contextId [40](#)
 - create [40](#)
 - update [40](#)
 - versionId [40](#)

V

- verification [65](#)
- verify
 - Context Store interfaces [117](#), [126](#)
- verify deletion [73](#)
- verifying

- verifying (*continued*)
 - connection between geo-redundant clusters [119](#)
 - Context Store connection to External Data Mart [116](#)
 - Context Store deployment [115](#)
- verifying connection between geo-redundant clusters [119](#)
- view
 - customer interactions [37](#)
 - customer journey [37](#)
- virtual machines [47](#)

W

- WebLM [50](#)