Automated Safeguards for ElastiCache - Redis

Amazon ElastiCache is a managed service used to deploy, run, and scale popular open source compatible in-memory data stores. Customers can build data-intensive apps or improve the performance of your existing apps by retrieving data from high throughput and low latency in-memory data stores.

> **Note**
>
> ElastiCache for Redis is HIPAA Eligible, but ElastiCache for Memcached is not. ElastiCache for Redis is the only allowed caching engine at this time.

Amazon ElastiCache can scale-out, scale-in, and scale-up to meet fluctuating application demands. Write and memory scaling is supported with sharding. Replicas provide read scaling.

ElastiCache is priced based on the instances used, allowing for scaling the cache layer. See Amazon ElastiCache Pricing for details.

Amazon ElastiCache can be used to significantly improve latency and throughput for many read-heavy application workloads (such as social networking, gaming, media sharing and Q&A portals) or compute-intensive workloads (such as a recommendation engine) by allowing you to store the objects that are often read in cache. Moreover, with Redis's support for advanced data structures, you can augment the database tier to provide features (such as leaderboard, counting, session and tracking) that are not easily achievable via databases in a cost-effective way.

Amazon ElastiCache for Redis is a great choice for implementing a highly available, distributed, and secure in-memory cache to decrease access latency, increase throughput, and ease the load off your relational or NoSQL databases and applications. ElastiCache can serve frequently requested items at sub-millisecond response times, and enables you to easily scale for higher loads without growing the costlier backend databases. Database query results caching, persistent session caching, and full-page caching are all popular examples of caching with ElastiCache for Redis. Learn how to build a caching application with ElastiCache for Redis.

Amazon ElastiCache for Redis gives you a fast in-memory data store to build and deploy machine learning models quickly. Use ElastiCache for Redis for use cases such as fraud detection in gaming and financial services, real-time bidding in ad-tech, and matchmaking in dating and ride sharing to process live data and make decisions within tens of milliseconds. Learn how Coffee Meets Bagel uses ElastiCache for real-time machine learning-based dating recommendations.

See Amazon ElastiCache for Redis Features for details.

ClearDATA Automated Safeguards for ElastiCache ensure that all of the compliance requirements are met for all newly created ElastiCache instances. ClearDATA reviews newly created instances to ensure the storage is encrypted and the communication between the instances is encrypted. If these settings are not properly configured, the instance will be deleted shortly after creation.

> **Note**
>
> ElastiCache for Redis versions 3.2.6, and 4.0.10+ are the only versions that support the necessary encryption standards. If a Redis version other than the ones listed is chosen, it will be considered non-compliant and terminated.

Compliance Guidance

Encrypted Storage

HIPAA Technical Safeguard 45 CFR 164.312(a)(2)(iv) requires encryption and decryption as an addressable standard and strongly suggests that you implement a mechanism to encrypt and decrypt electronic protected health information (ePHI). ClearDATA's interpretation of this regulation is that all storage must be encrypted. Amazon ElastiCache for Redis at-rest encryption is a feature that ClearDATA will enforce use of to increase data security by encrypting on-disk data during sync and backup or snapshot operations. See ElastiCache for Redis At-Rest Encryption for details.

Remediation

If the encryption option is not properly selected when the ElastiCache cluster is provisioned the cluster will be immediately deleted.

Encrypted Connections

HIPAA Technical Safeguard 45 CFR 164.312(a)(2)(iv) requires encryption and decryption as an addressable standard and strongly suggests that you implement a mechanism to encrypt and decrypt electronic protected health information (ePHI). ClearDATA's interpretation of this regulation is that all connections between ElastiCache instances must use a TLS encrypted connection, ensuring the data transmitted from node to node is encrypted. Amazon ElastiCache in-transit encryption is a feature that ClearDATA will enforce use of that allows you to increase the security of your data at its most vulnerable points—when it is in transit from one location to another. See ElastiCache for Redis In-Transit Encryption (TLS) for details.

Remediation

If the encryption option is not properly selected when the ElastiCache cluster is provisioned the cluster will be immediately deleted.

Shared Responsibility

Customers are responsible for configuring the Redis AUTH token. Amazon ElastiCache for Redis clusters (single/multi node) that contain PHI must provide a Redis AUTH token to enable authentication of Redis commands. Customers should provide a strong token for Redis AUTH with following constraints:

- Must be only printable ASCII characters Amazon Web Services
- Must be at least 16 characters and no more than 128 characters in length
- Cannot contain any of the following characters: '/', "", or "@"

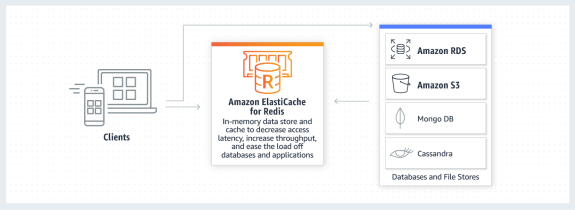
This token must be set from within the Request Parameter at the time of Redis replication group (single /multi node) creation and can be updated later with a new value.

Please contact your ClearDATA team for a copy of the Responsibilities Matrix.

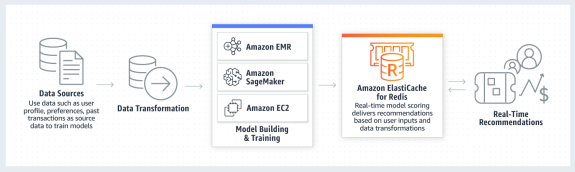
Exclusion

Disabling automated remediation at done the cluster level. Please contact ClearDATA Support to request that an exclusion be placed to allow for the cluster to be created.

Caching



Machine Learning



Users can be added to the **Safeguards-ElastiCache** group to gain access to create and manage RDS instances.

RACI

Item	ClearDATA	Customer
Enforcement of Automated Safeguards	RA	IC
Create Redis AUTH token	IC	RA
Ensure any service excluded from automated remediation does not contain any PHI/PII	IC	RA
Create, configure, manage, and maintain ElastiCache clusters	C	RA