Automated Safeguards for Elasticsearch

Amazon Elasticsearch provides a managed service of the open source Elastic stack. Elasticsearch allows for scalable search, has near real-time search, and supports multitenancy. Elasticsearch also includes components such as a data-collection and log-parsing engine called Logstash, and an analytics and visualization platform called Kibana. The service offers open-source Elasticsearch APIs, managed Kibana, and integrations with Logstash and other AWS Services, enabling you to securely ingest data from any source and search, analyze, and visualize it in real time.

Pricing Guidelines

Amazon Elasticsearch is priced based on usage, depending on the cluster size and instance type. Please see the Amazon Elasticsearch Pricing page for full details

Amazon Elasticsearch allows you to create a fully managed Elasticsearch cluster in minutes, with no software to install. Amazon Elasticsearch Service offers acces to open-source Elasticsearch APIs, managed Kibana, and integration with Logstash, so you can continue to use your existing code and data ingestion and visualization tools. The service also offers built-in integrations with other AWS services such as Amazon Kinesis Data Firehose, AWS IoT, and Amazon CloudWatch Logs for data ingestion; AWS CloudTrail for auditing; Amazon VPC, AWS KMS, Amazon Cognito, and AWS IAM for security. Amazon Elasticsearch is also scalable, highly available, and secure to host even the most sensitive data.

See the Amazon Elasticsearch Features page for a list of features, and the .Amazon Elasticsearch Developer Guide for details.

Automated Safeguards

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

Compliance Guidance

ClearDATA Automated Safeguards for Amazon Elasticsearch ensure that all of the compliance requirements are met for all newly created Elasticsearch clusters. ClearDATA reviews newly created clusters to ensure the storage is encrypted, the communication between the cluster nodes is encrypted, and the cluster is not publicly available. If these settings are not properly configured, the cluster will be deleted shortly after creation.

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. All Amazon Elasticsearch clusters must be encrypted upon provisioning in order to be deemed compliant. Please see Encryption of Data at Rest for Amazon Elasticsearch Service f or details.

Remediation

If the encryption option is not properly selected when the Elasticsearch 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 Elasticsearch nodes must use a TLS encrypted connection, ensuring the data transmitted from node to node is encrypted. Please see https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/ntn.html for details.

Remediation

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

Public Access

HIPAA Technical Safeguard 45 CFR § 164.312(e)(1) requires implementation technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. ClearDATA evaluates the Elasticsearch clusters to ensure they are not publicly accessible, which could lead to unintended data access. Please see VPC Support for Amazon Elasticsearch Service Domains for details.

Remediation

If the public access option is not properly selected when the Elasticsearch cluster is provisioned the cluster will be immediately deleted.

Shared Responsibility

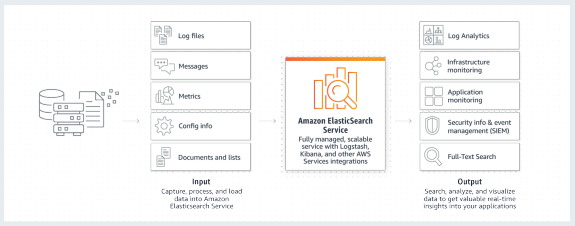
ClearDATA will ensure that all Elasticsearch clusters created in accounts with Automated Safeguards meet the requirements outlined above under Compliance Guidance. If an Elasticsearch cluster is created and found to violate any of the items listed, the cluster will be terminated and an alert will be sent to the ClearDATA SNS topic with details of the violation.

Customers are responsible for adhering the to guidelines listed above when creating Elasticsearch clusters that may contain sensitive data.

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.



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

Item	ClearDATA	Customer
Enforcement of Automated Safeguards	RA	IC
Deploy Elasticsearch clusters in accordance with the compliance guidelines listed above	C	RA
All Elasticsearch, Logstash, or Kibana configuration, monitoring, and management	C	RA
Ensure any service excluded from automated remediation does not contain any PHI/PII	IC	RA
Configure the ElasticSearch domain policy to limit access to required connection points and users, ensuring it is not available to any area it should not be made available.	IC	RA