Elasticsearch and AWS Integration

What is Elasticsearch?

Elasticsearch is a distributed search and analytics engine built on Apache Lucene. It's widely used for log analytics, full-text search, business and operational intelligence. Elastic NV changed its license model in 2021, leading to the creation of OpenSearch by AWS, a fully open-source alternative.

How does Elasticsearch work?

You send JSON documents via API or tools like Logstash. Elasticsearch stores and indexes these documents. You can query them using APIs or visualize with Kibana.

Key Benefits

- 1. Fast time-to-value: Easy REST APIs and JSON.
- 2. High performance: Distributed and parallel processing.
- 3. Tooling: Integrated with Kibana, Beats, Logstash.
- 4. Near real-time: Read/write in <1s.
- 5. Multi-language support.

AWS Services for Elasticsearch

- 1. Amazon OpenSearch Service Managed, scalable, secure search engine.
- 2. Amazon Managed Grafana Visualize OpenSearch data.
- 3. AWS Data Pipeline Schedule and move data into OpenSearch.
- 4. AWS Lambda Event-driven processing for indexing.
- 5. Amazon Kinesis Real-time streaming to OpenSearch.
- 6. Amazon CloudWatch Monitor OpenSearch clusters.

Elasticsearch on AWS Diagram

Elasticsearch and AWS Integration

