Elasticsearch Training

# Day 1: Introduction to Elasticsearch and Hands-On Setup

## Learning Objectives:

Understand the core concepts of Elasticsearch, including documents, indices, and clusters.

Learn about the Elasticsearch architecture and its role in the ELK Stack.

Successfully install and configure Elasticsearch on a local environment or cloud platform.

## Hands-On Activities:

Install Elasticsearch on a local machine or cloud environment.

Create a basic index and populate it with sample data.

Use the Elasticsearch REST API to perform basic CRUD operations.

Explore the Elasticsearch cluster health and status.

# Day 2: Indexing and Mapping

## Learning Objectives:

Master the process of creating and managing indices.

Grasp the importance of mappings and their impact on search performance.

Differentiate between dynamic and explicit mappings.

## Hands-On Activities:

Create multiple indices with different settings and mappings.

Index sample data into the created indices.

Experiment with different field types and their implications.

dynamic vs. explicit mappings on indexing and search.

# Day 3: Advanced Search Queries

## Learning Objectives:

Become proficient in using Elasticsearch Query DSL.

Construct complex search queries to retrieve specific data.

Utilize full-text search capabilities effectively.

Implement filtering, sorting, and pagination for optimized search results.

## Hands-On Activities:

Build various search queries using the Query DSL.

Experiment with different query types (match, term, range, etc.).

Implement full-text search with different analyzers and tokenizers.

Optimize search performance through filtering, sorting, and pagination.

# Day 4: Aggregations and Analytics

## Learning Objectives:

Understand the concept of aggregations in Elasticsearch.

Apply metric, bucket, and pipeline aggregations to analyze data.

Leverage aggregations for data exploration and insights.

## Hands-On Activities:

Create different types of aggregations (terms, histogram, average, etc.).

Combine multiple aggregations to answer complex questions.

Visualize aggregation results using tools like Kibana.

Analyze sample datasets using aggregations to uncover trends and patterns.

# Day 5: Data Ingestion and Best Practices

## Learning Objectives:

Learn how to ingest data into Elasticsearch using Logstash and Beats.

Create and configure ingest pipelines for data transformation.

Implement data enrichment processes.

Understand best practices for Elasticsearch deployment and security.

Monitoring Elasticsearch clusters

Securing Elasticsearch clusters

Setting up role-based access control (RBAC)

## Hands-On Activities:

Set up Logstash to ingest data from various sources.

Create ingest pipelines to preprocess data before indexing.

Configure Beats ingestion.

Securing Elasticsearch clusters.