# Elasticsearch - A Beginner's Guide

## 1. What is Elasticsearch?

Elasticsearch is an open-source search and analytics engine based on Apache Lucene. It is commonly used for log analysis, full-text search, and real-time data monitoring. It allows you to store, search, and analyze large volumes of data quickly and efficiently.

## 2. When to Use Elasticsearch

- Log and event data (e.g., server logs)
- Application performance monitoring
- Product or document search (e.g., e-commerce)
- Real-time analytics (e.g., user behavior tracking)

## 3. Installation (Linux/macOS)

1. Install Java (Elasticsearch requires Java 11+).
2. Download Elasticsearch from https://www.elastic.co/downloads/elasticsearch
3. Extract and run:
   tar -xzf elasticsearch-x.y.z.tar.gz
   cd elasticsearch-x.y.z
   ./bin/elasticsearch
4. Access: http://localhost:9200

## 4. Installing Kibana

1. Download Kibana from https://www.elastic.co/downloads/kibana
2. Extract and run:
   tar -xzf kibana-x.y.z.tar.gz
   cd kibana-x.y.z
   ./bin/kibana
3. Access: http://localhost:5601

## 5. Example: Indexing Data

Use the following command with curl or Postman:

```
curl -X POST "localhost:9200/products/_doc/1" -H 'Content-Type: application/json' -d'{
  "name": "Laptop",
  "price": 1299.99,
  "stock": 12
}'
```

### 6. Querying Data

```
curl -X GET "localhost:9200/products/_search" -H 'Content-Type: application/json' -d'{
  "query": {
    "match": {
      "name": "Laptop"
    }
  }
}'
```

### 7. Visualization with Kibana

Once Kibana is running:

- Go to 'Discover' to search your indexed data
- Create visualizations and dashboards with charts and filters
- Use DevTools to run and test queries in a friendly interface

### 8. Recommended Data Formats

Elasticsearch works best with JSON data. Ideal data formats include:

- Server logs (e.g., Apache, Nginx)
- JSON-formatted API responses
- CSV transformed to JSON for ingestion via Logstash

# Elasticsearch - A Beginner's Guide

## 9. Using Logstash to Ingest Data

Example Logstash pipeline config to import logs:

```
input {
  file {
    path => "/path/to/access.log"
    start_position => "beginning"
  }
}
filter {
  grok {
    match => { "message" => "%{COMBINEDAPACHELOG}" }
  }
}
output {
  elasticsearch {
    hosts => ["localhost:9200"]
    index => "weblogs"
  }
  stdout { codec => rubydebug }
}
```

## 10. Resources

- Official site: https://www.elastic.co/
- Elasticsearch documentation: https://www.elastic.co/guide/en/elasticsearch/reference/index.html
- Kibana tutorials: https://www.elastic.co/guide/en/kibana/index.html