ELK Stack Documentation

Table of Contents

1. Introduction to ELK Stack

The ELK Stack is a powerful combination of three open-source tools: Elasticsearch, Logstash, and Kibana. This stack is commonly used for log and event data analysis, offering robust capabilities in searching, analysing, and visualising large datasets.

Elasticsearch: A distributed, RESTful search and analytics engine. It is used to store and index data, providing fast and scalable search capabilities.

Logstash: A server-side data processing pipeline that ingests, processes, and transforms data before sending it to Elasticsearch.

Kibana: A web-based user interface for visualising and managing data in Elasticsearch. It allows users to create dynamic dashboards and perform real-time data analysis.

2. Kibana Dashboard

2.1. Overview

Kibana provides a user-friendly interface to interact with Elasticsearch data. Dashboards in Kibana allow you to combine multiple visualizations and saved searches into a single, interactive view.

2.2. Creating a Sample E-commerce Sales Dashboard

To create a sample E-commerce Sales Dashboard, follow these steps:

Access Kibana:
Open your web browser and navigate to the Kibana URL.

Go to Dashboard:
In Kibana, navigate to the "Dashboard" section.

Create Dashboard:
Click on the "Create Dashboard" button and give it a meaningful name.

Add Visualisations:
Use the "Add" button to add visualisations such as bar charts, pie charts, or line charts.

Configure Filters:
Apply filters to focus on specific data. For example, create a filter for the taxful total price range.

Save Dashboard:
Save your dashboard for future use.

3. Elasticsearch Queries

3.1. Basic Query Structure
Elasticsearch queries are structured in JSON format. The basic structure includes the query field, where you define your search criteria.

3.2. Example Query
json
Copy code

```
GET kibana_sample_data_ecommerce/_search
{
  "query": {
    "range": {
      "taxful_total_price": {
        "gte": 50,
        "lte": 100
      }
    }
  }
}
```

This example retrieves documents from the kibana_sample_data_ecommerce index where the taxful_total_price falls between 50 and 100.

4. CRUD Operations in Elasticsearch

4.1. Creating Documents

To create a document in Elasticsearch, use the index API:

json
Copy code

```
POST your_index/_doc/1
{
  "field1": "value1",
  "field2": "value2"
}
```

4.2. Retrieving Documents

Retrieve a document by its ID using the get API:

json
Copy code

```
GET your_index/_doc/1
```

4.3. Updating Documents

Update a document using the update API:

json
Copy code

```
POST your_index/_update/1
{
  "doc": {
    "field1": "new_value"
  }
}
```

4.4. Deleting Documents

Delete a document by its ID using the delete API:

json
Copy code

```
DELETE your_index/_doc/1
```

This documentation provides a brief overview of ELK Stack, guidance on creating a Kibana dashboard, sample Elasticsearch queries, and CRUD operations. For more detailed information, refer to the official documentation of each component.

https://www.loom.com/share/21f489255bba433c91992974333d6984?sid=5ffbd6de-4763-45a8-99c1-5487ac91b431