Task 1: Create a Kibana Dashboard, with ElasticSearch Queries on a Sample Dataset, using the ELK stack.

Introduction

ElasticSearch is a distributed, multitenant-capable full-text search engine with a web interface and schema-free JSON documents. It can be used to search any kind of document, and distributed means that indices are divided into shards and each shard can have zero or more replicas. Each ElasticSearch node hosts one or more shards. ElasticSearch is developed alongside the data collection and log-parsing engine Logstash and the visualisation platform Kibana. All three technologies: ElasticSearch, Logstash and Kibana make up the "ELK stack".

When creating a Dashboard in Kibana, we ingest the data from a data source, here a sample dataset, using Logstash, store it using ElasticSearch and display metrics from the data using Kibana. This process is integrated into the Kibana web interface, and the visualisations when they display the data, use ElasticSearch queries in the backend to get the specific data to display.

Information about the Dataset

The dataset that I used is a sample dataset of sales of products in supermarket chain. It has about 1000 entries, across three branches in three different cities.

The fields in the dataset are:

- Invoice ID
- Branch
- City
- Customer Type
- Gender
- Product Line
- Unit Price
- Quantity
- Tax 5%
- Total
- Date
- Time
- Payment Method
- COGS (Cost of Goods Sold)
- Gross Margin Percentage
- Gross Income
- Rating

Work Done By:

Aseem Athale

athaleaseem@gmail.com