**KIBANA**

Kibana is an open-source tool for analytics and visualization platform designed to work with Elastic search. We use Kibana to search, view, and interact with data stored in Elastic search indices. We can easily perform advanced data analysis and visualize our data in variety of charts, tables, and aps.

**Key points:**

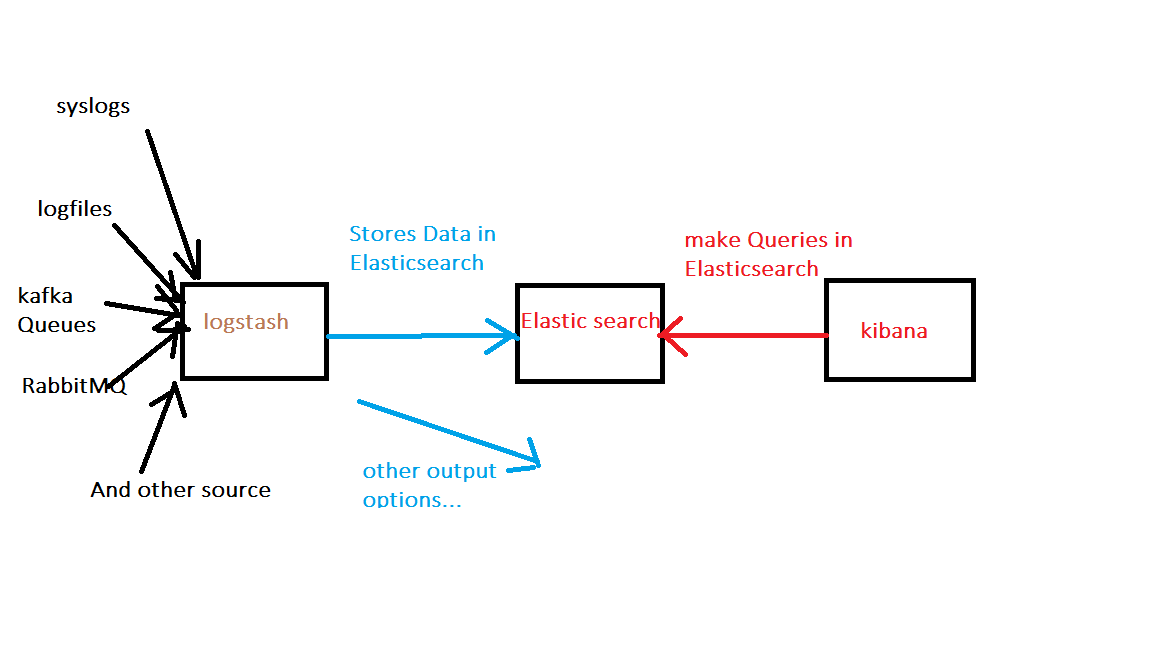
* Kibana enables the searching & interactions with data in elastic search.
* Kibana allows performing advance analytics and creation of report.
* Kibana enables creation and sharing of dynamic dashboards that get updates in real time.

**Introduction to ELK stack:**

ELK stack is the combination of three open source too i.e., Elasticsearch, Logstash & Kibana for log analysis.

1. **Elasticsearch:** is a highly scalable open-source search and analysis engine. It allows you to store, search, and analyze big volumes of data quickly and in near real time. It is generally used as the underlying engine/ technology that powers applications that have complex search features and requirements.
2. **Logstash:** is an open-source data collection engine with real-time pipelining capabilities. Logstash can dynamically unify data from disparate sources and normalize the data for diverse advanced downstream analytics and visualization use cases. **Basically, tool for collecting and monitoring logs from remote machine and is the data pipeline for Elasticsearch.**
3. **Kibana:** is an open-source data visualization and exploration tool used for log and time-series analytics, application monitoring, and operational intelligence use cases. It offers powerful and easy-to-use such as histograms, line graphs, pie charts, heat-maps, and built-in geospatial support.

How Do they work together?



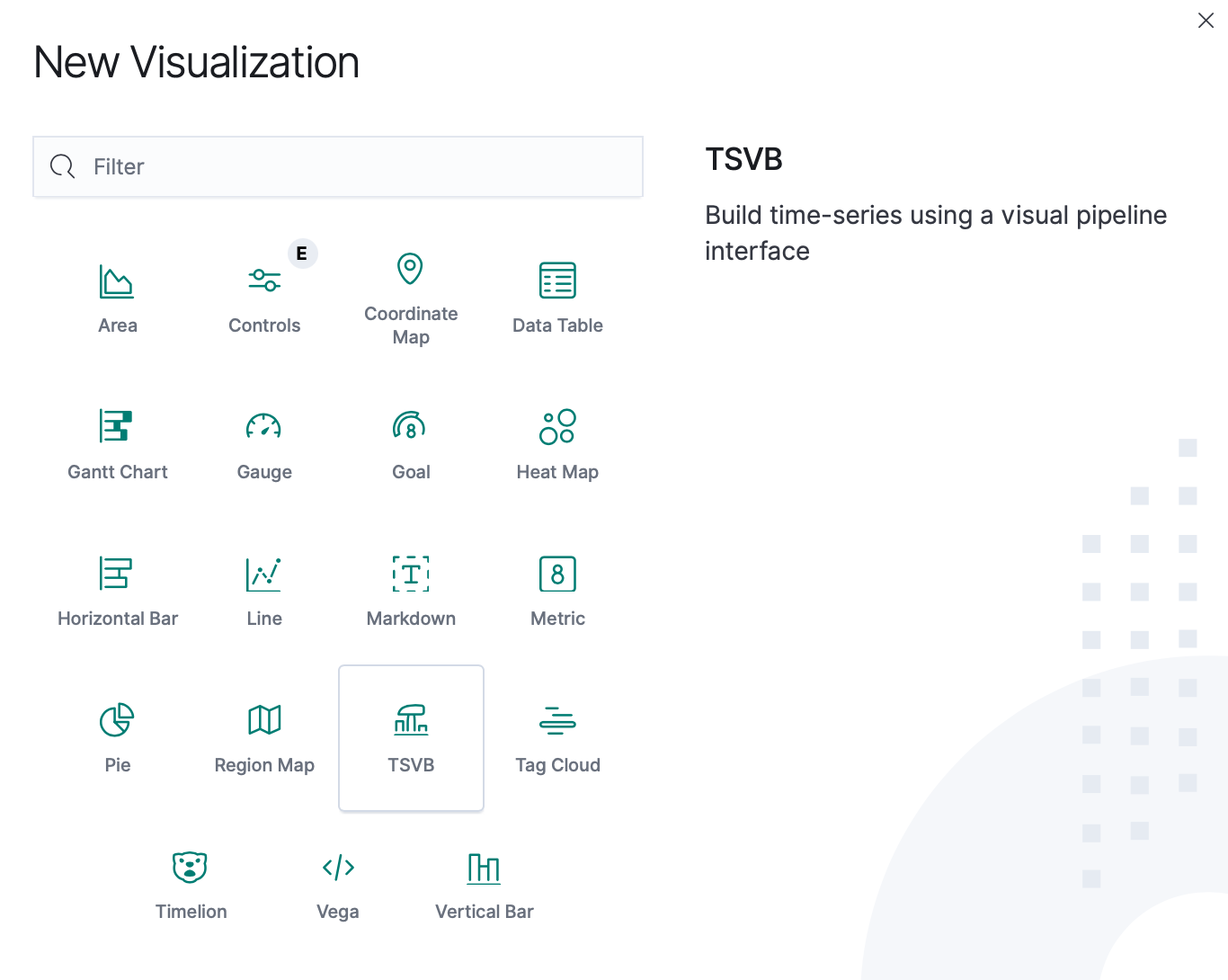
**Kibana Interfaces:**

1. **Discover**
2. **Visualize**
3. **Dashboard**
4. **Timelion**
5. **Dev Tools**
6. **Management**

**Discover:** We can explore our data from the Discover page. We can submit search queries, filter the search results, and view document data. You can also see the number of documents that match the search query and get field values statistics. If a time fields is configured for the selected index pattern, the distribution of documents over time is displayed in histogram at the top of the page.

**Visualize:** Visualize enables you to create new visualizations of the data in your Elasticsearch indices.

Below page is the visualize page, here we can see the visualization types.



In the visualization creation process, select the metric aggregation for the visualization’s Y axis and select a bucket aggregation for the visualizations X axis. Based on our requirement we can add metrics and buckets by selecting add options. Here I have selected add metrics option.

**Dashboard:** A kibana dashboard displays a collection of saved visualizations. You can arrange and resize the visualizations as needed and save dashboards to they be reloaded and shared.

**Dashboard creation process:**

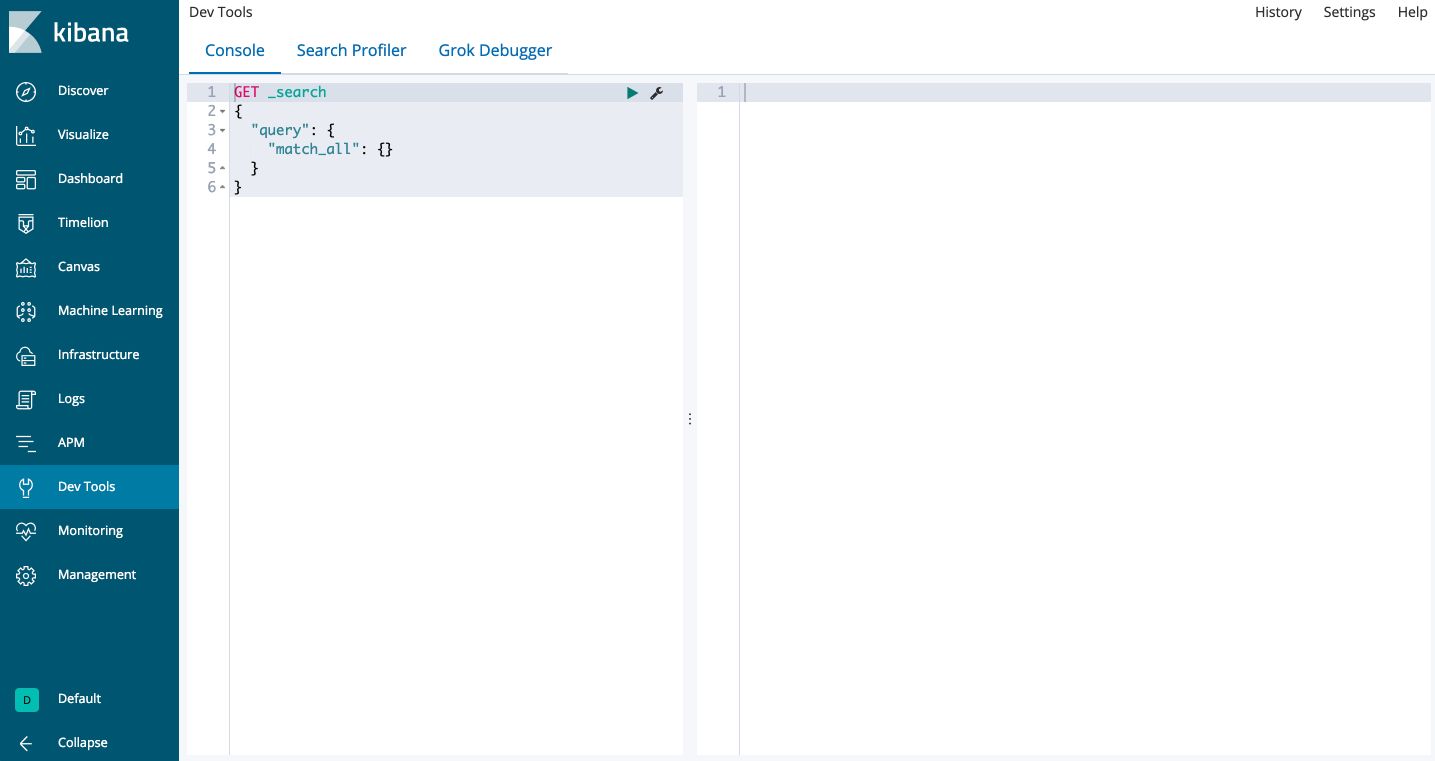
We can create the dashboards by clicking create a dashboard option or clicking ‘+’ symbol.

>Next we will get the below page, here we need to click the add option.

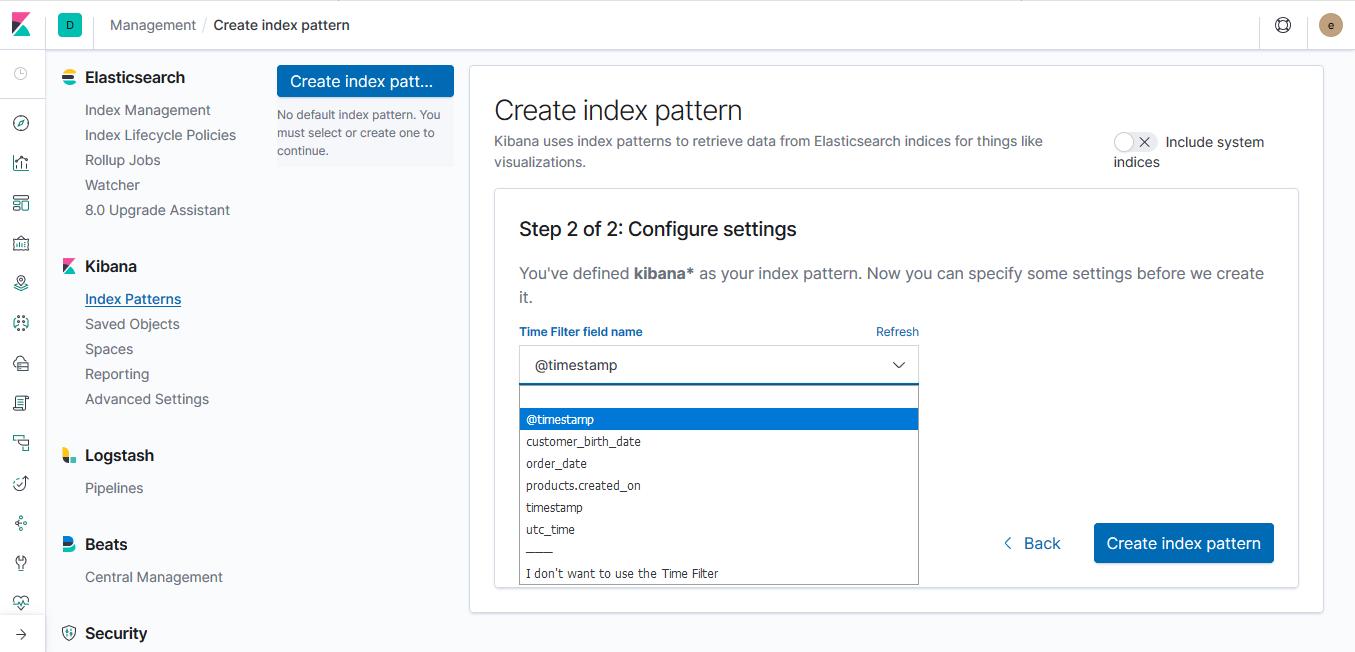
>Next we get the below page, here we can directly add the visualizations to dashboard or we can add new visualization.

>Otherwise we can add saved search to dashboard.

**Dev Tools:** The Dev Tools page contains development tools that you can use to interact with your data in Kibana.



**Management:** is an application is where you perform your runtime configuration of Kibana, including both the initial setup and ongoing configuration of index patterns, advanced settings that tweak the behaviors of kibana itself, and the various “objects” that you can save throughout Kibana such as searches, Visualizations and dashboards.



**Create index pattern:**

Kibana uses index patterns to retrieve data from Elasticsearch indices for things like Visualizations.

**Step1 of 2: Define index pattern**

**Index name**

You can use a \* as wildcard in your index pattern

You can’t use spaces or the characters