logocover

**Smoke test DOCUMENT**

ELK Smoke Test Cases

Date Prepared: July 2019

**Document Information**

|  |  |  |  |
| --- | --- | --- | --- |
| **Project Name** | **ELK Smoke Test Document** | | |
| **Project Owner** |  | **Document Version No** | 1.0 |
| **Quality Review Method** | By email/HP SharePoint |  |  |
| **Prepared By** |  | **Preparation Date** | July 2019 |
| **Reviewed By** | Refer to version history | **Review Date** |  |

**Table of Contents**

[1 INSPECT STATUS of the Cluster 4](#_Toc15649539)

[2 Loading sample data and Visualizing the data IN Kibana 5](#_Toc15649540)

[2.1 Create Index Patterns for sample account data 7](#_Toc15649541)

[2.2 Create visualization type for sample account data 9](#_Toc15649542)

[3 COLLECTING ELASTICSEARCH LOGS USING FILEBEAT 11](#_Toc15649543)

[3.1 Installing and setting up Filebeat 12](#_Toc15649544)

[3.2 Collecting Elasticsearch logs in Kibana UI 15](#_Toc15649545)

[3.3 Create Index patterns name for Elasticsearch logs data 16](#_Toc15649546)

[3.4 Create visualization type for Elasticsearch logs data 18](#_Toc15649547)

[4 TESTING ELK STACK WITH SAMPLE FLIGHT DATASET 20](#_Toc15649548)

[4.1 Add sample flight data to Kibana 20](#_Toc15649549)

[4.2 Discover the sample flight dataset 21](#_Toc15649550)

[4.3 Visualize the sample flight dataset 23](#_Toc15649551)

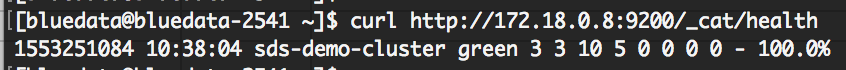
[4.4 Test Dashboard for sample flight dataset 25](#_Toc15649552)

[4.5 Test REST API from Dev Tools 27](#_Toc15649553)

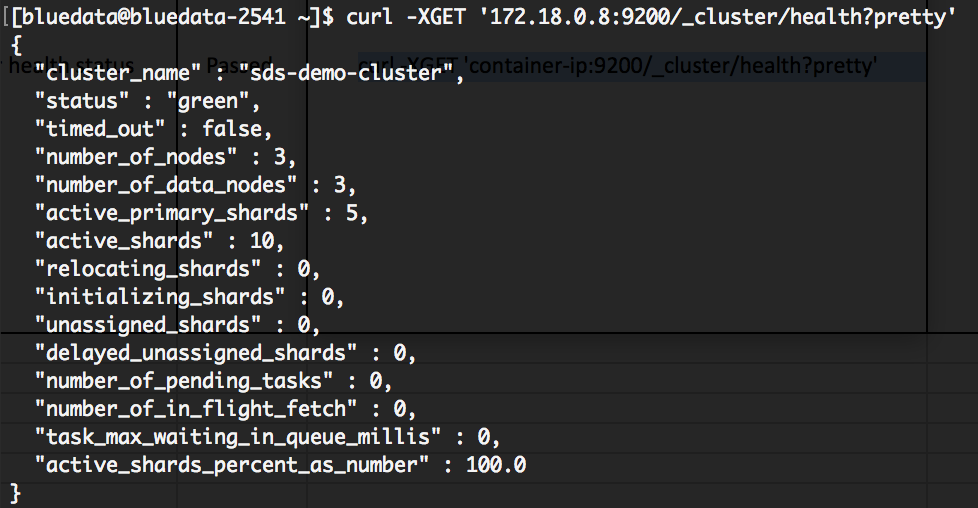
[4.6 Testing SQL CLI for ELK 29](#_Toc15649554)

# INSPECT STATUS of the Cluster

curl http://<container-ip>:9200/\_cat/health

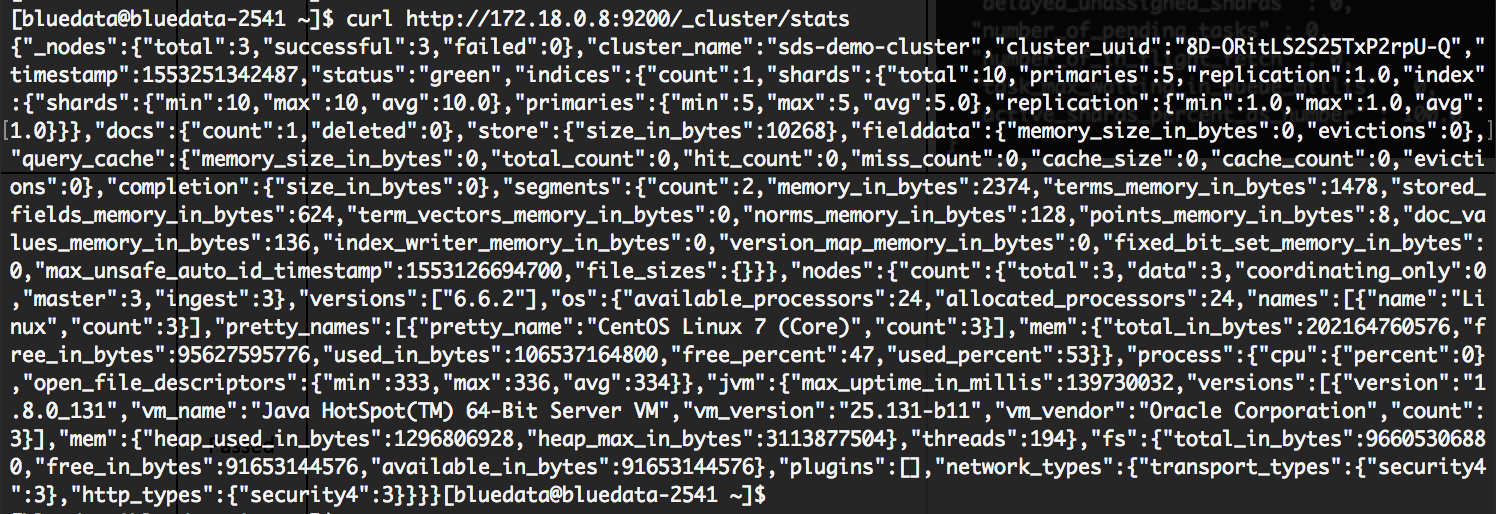


curl -XGET '<container-ip>:9200/\_cluster/health? pretty'



Inspect Cluster Stats:

curl http://<container-ip>:9200/\_cluster/stats

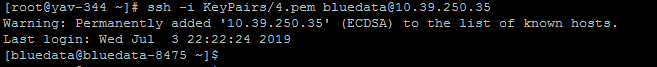


# Loading sample data and Visualizing the data IN Kibana

Here we will load the sample dataset and visualize the data in Kibana UI

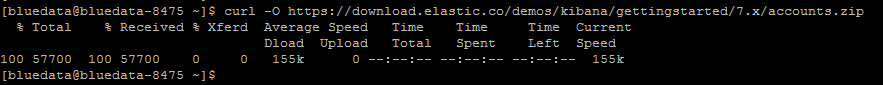
Loading the sample account dataset

Go to the Elasticsearch master node



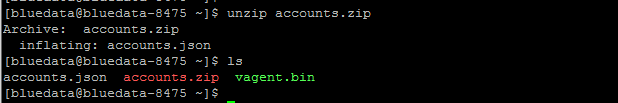
Execute the following command to download the sample account dataset

**curl -O https://download.elastic.co/demos/kibana/gettingstarted/7.x/accounts.zip**



Execute the following command to unzip the sample account dataset

**unzip accounts.zip**

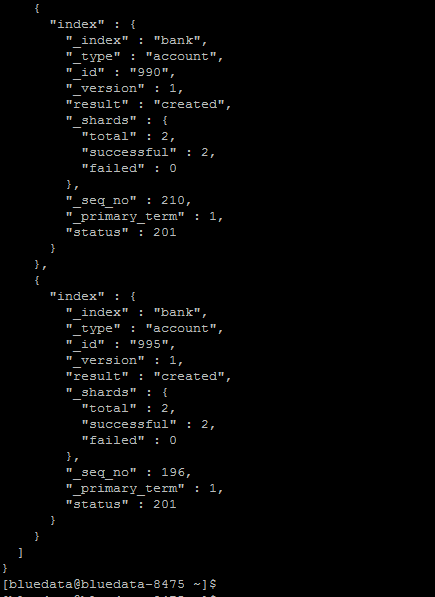


Execute the following command to load the sample data into Elasticsearch data host

**curl -H 'Content-Type: application/x-ndjson' -XPOST ‘<IP\_Address>:9200/bank/account/\_bulk?pretty' --data-binary @accounts.json**

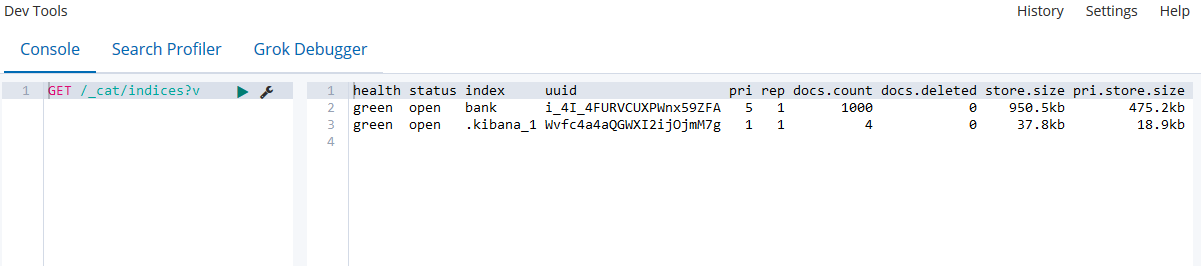


It will take some time to load the sample account data into Elasticsearch data host. You will see the result as given below



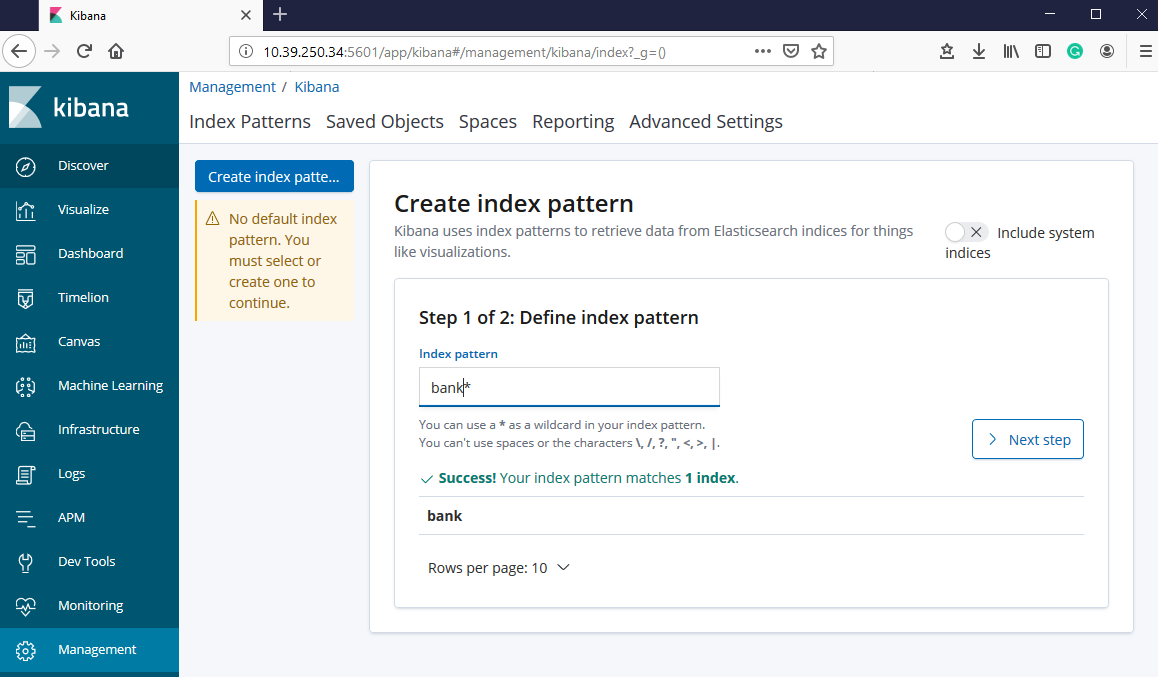
Go to the Kibana UI then click on Dev Tools section, and execute the following command to verify if bank index is created from the sample account dataset

GET /\_cat/indices?v

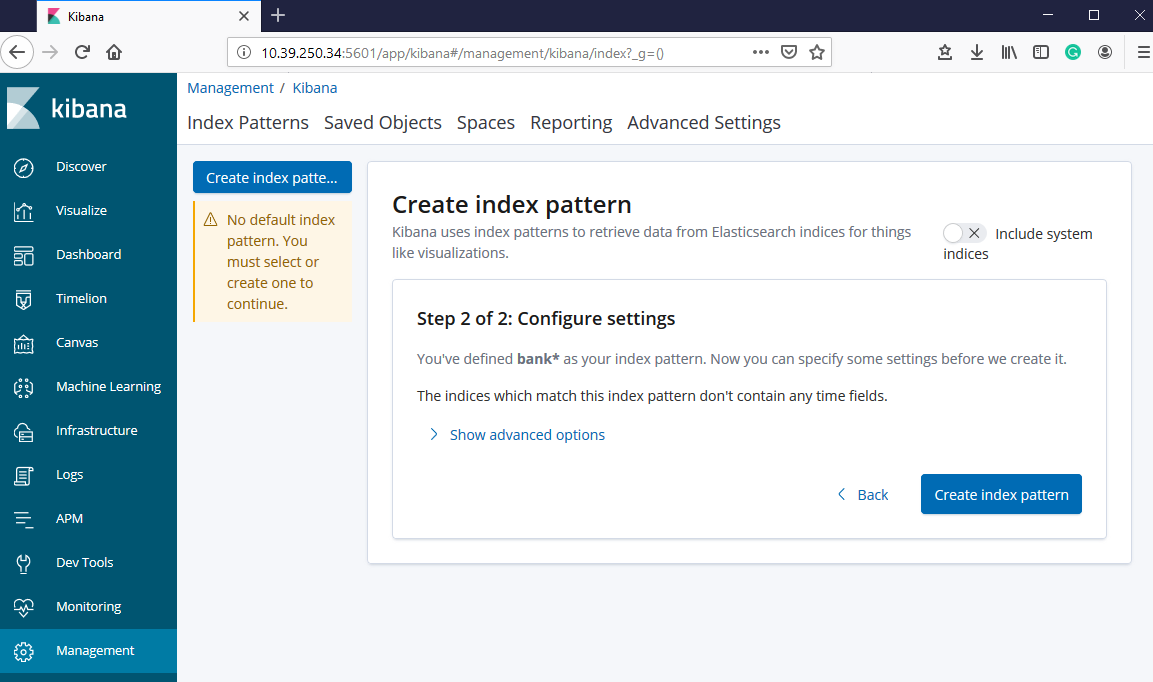


## Create Index Patterns for sample account data

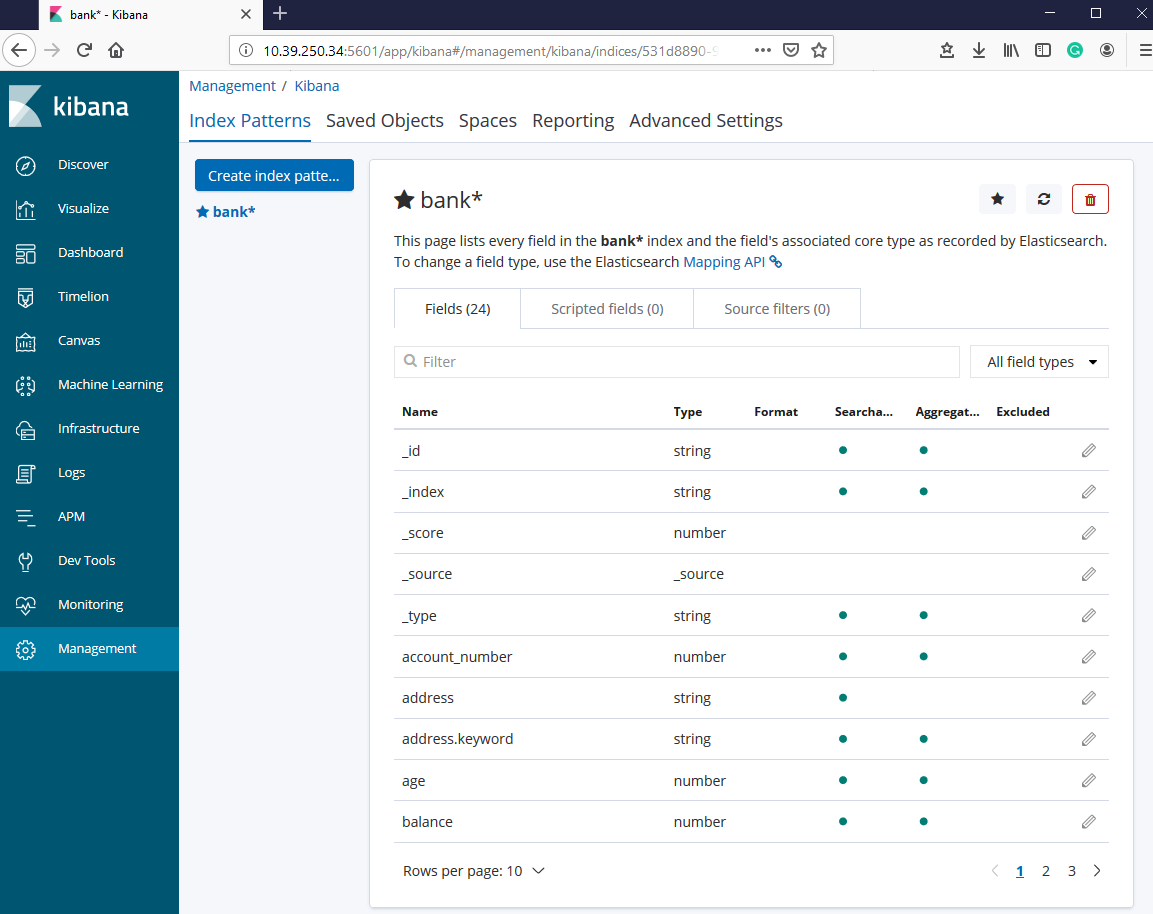
Go to the Management section and then click on Index Patterns on Kibana.



Define index patterns then click on Next step.



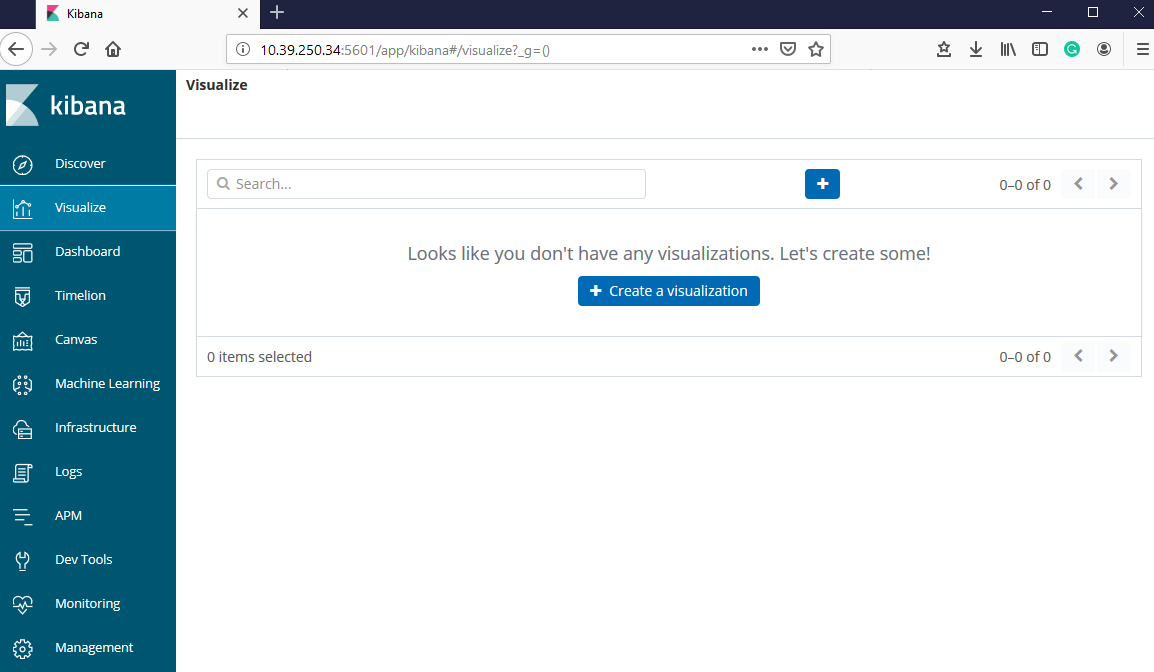
Click on Create Index Patterns.



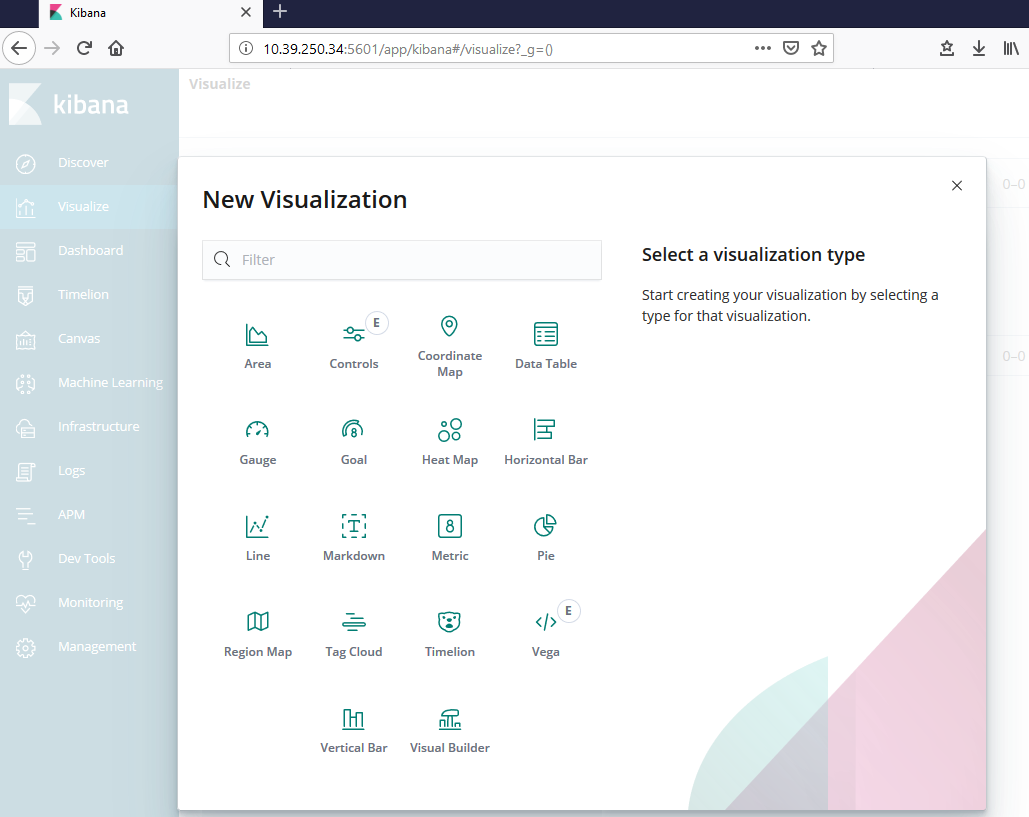
New index pattern is created successfully.

## Create visualization type for sample account data

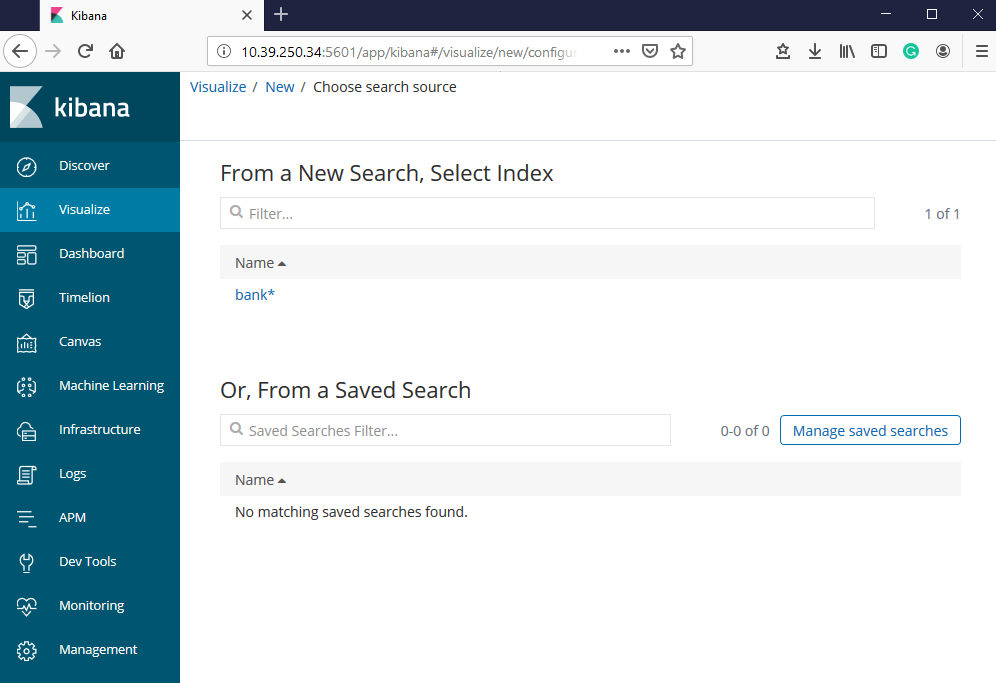
Click on Visualize section on Kibana UI.



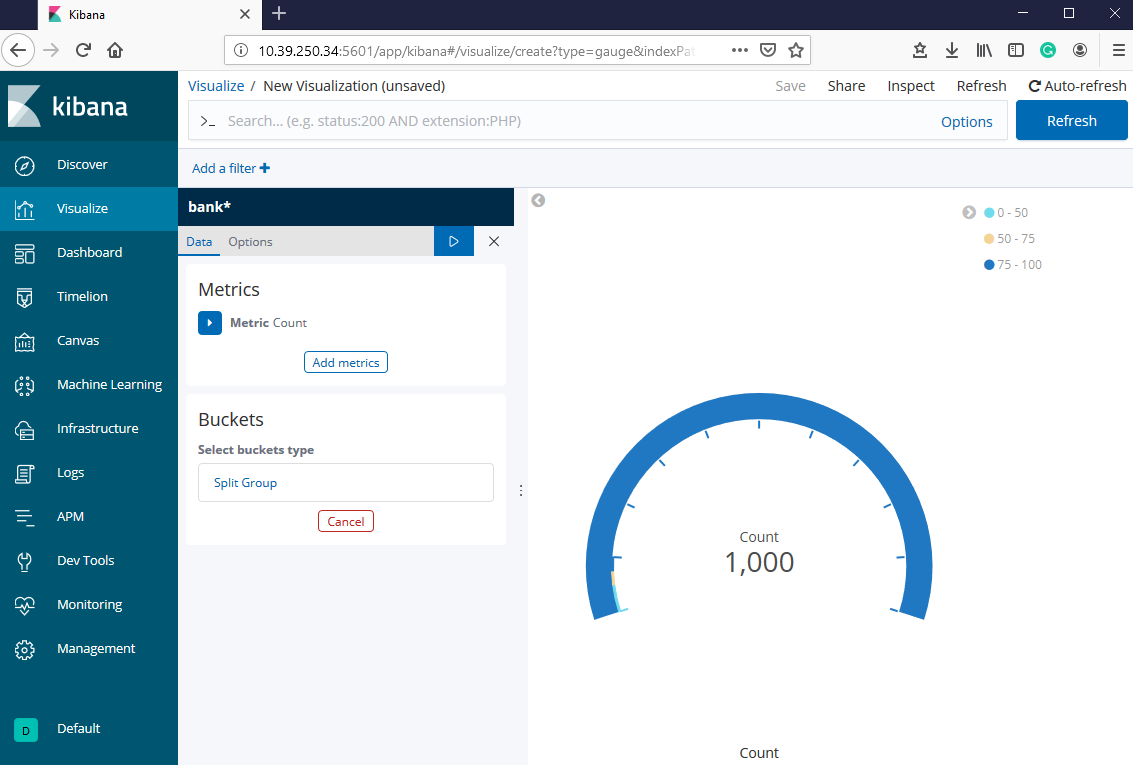
Click on + sign to create new visualization type for sample account data



Click on Gauge to create gauge visualization for sample account data.



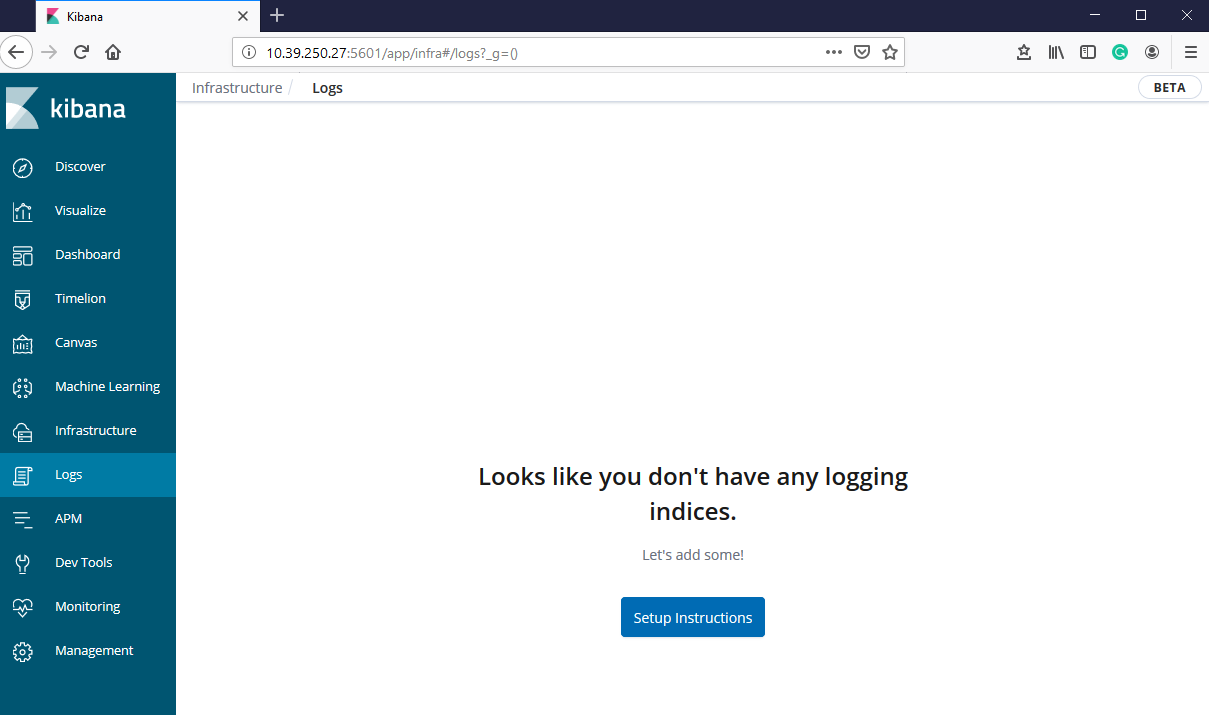
Select bank\* to create gauge visualization for sample account data



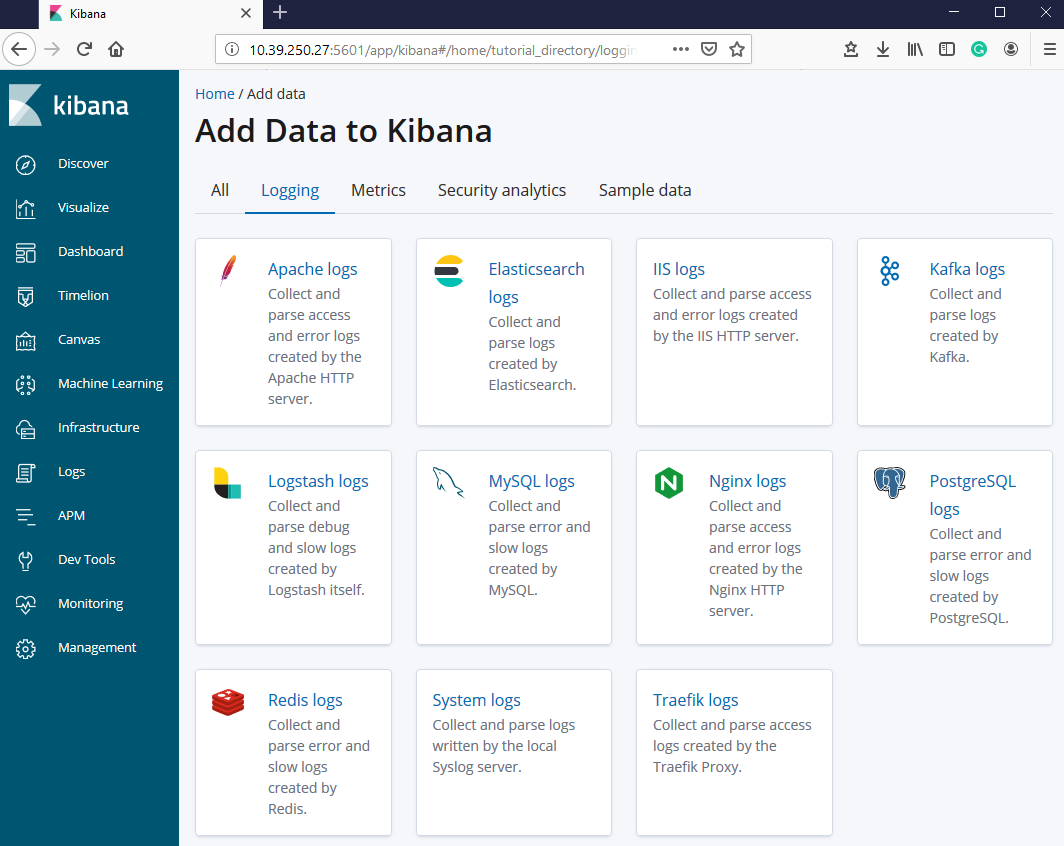
Gauge visualization is created for sample account data successfully.

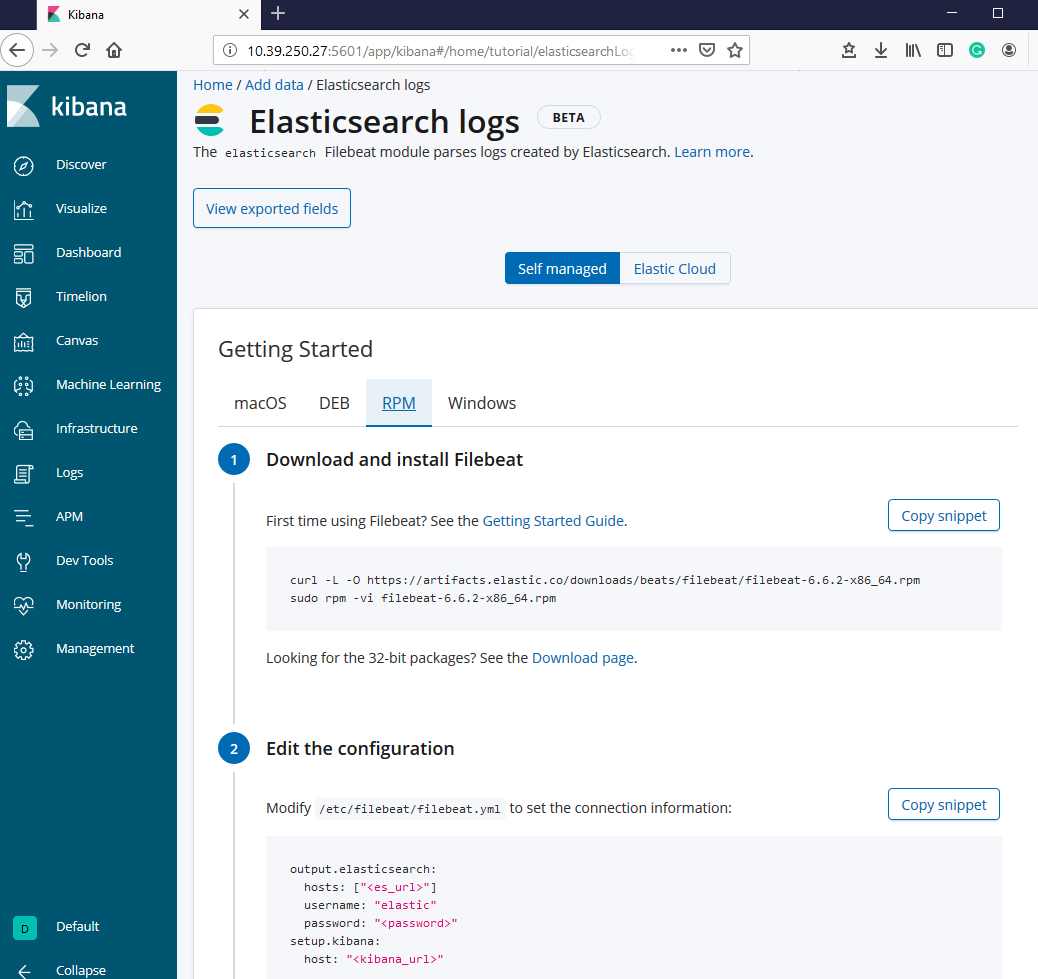
# COLLECTING ELASTICSEARCH LOGS USING FILEBEAT

We will use Kibana UI to get information about how to install Filebeat for collecting Elasticsearch logs. Click on the Logs section then click on Setup Instruction



Click on Elasticsearch logs box. Here you will see the instruction for installing Filebeat.

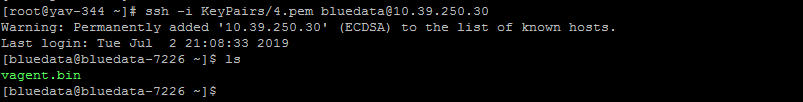




Here you can see the installation and setup process of Filebeat for Elasticsearch logs

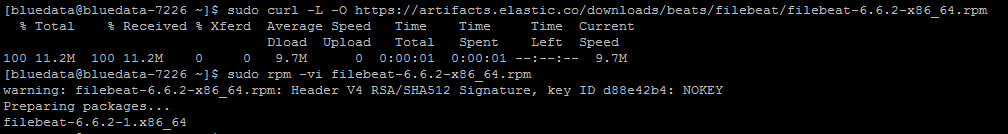
## Installing and setting up Filebeat

Go to the Elasticsearch master node for installing Filebeat.



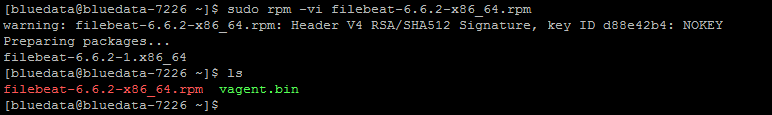
Execute the following command to download the rpm for Filebeat

**sudo curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-6.6.2-x86\_64.rpm**



Execute the following command to install Filebeat

**sudo rpm -vi filebeat-6.6.2-x86\_64.rpm**

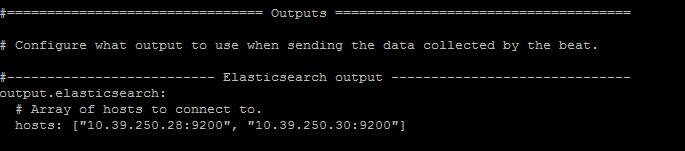
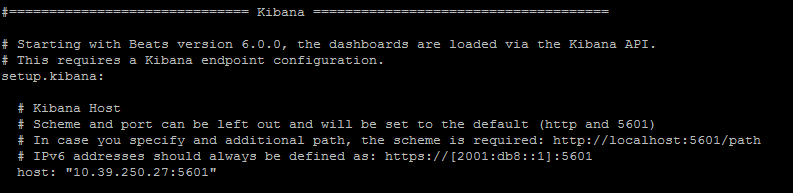


Modify /etc/filebeat/filebeat.yml to set the connection information:

**sudo vi /etc/filebeat/filebeat.yml**



Enter IP address for Kibana and Elasticsearch hosts in filebeat.yml file



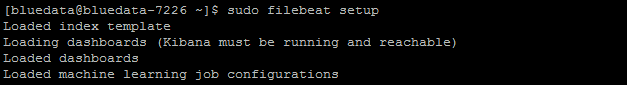
Execute the following command to enable Elasticsearch module

**sudo filebeat modules enable elasticsearch**



Execute the following command to setup Filebeat

**sudo filebeat setup**



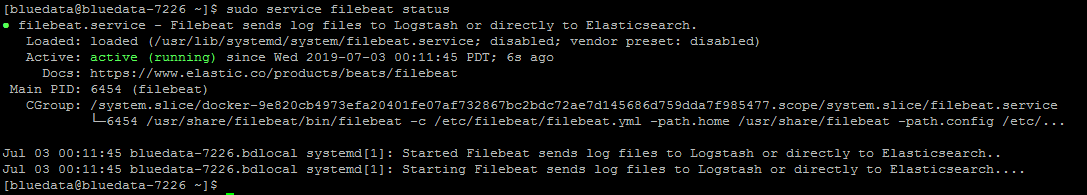
Execute the following command to start Filebeat

**sudo service filebeat start**



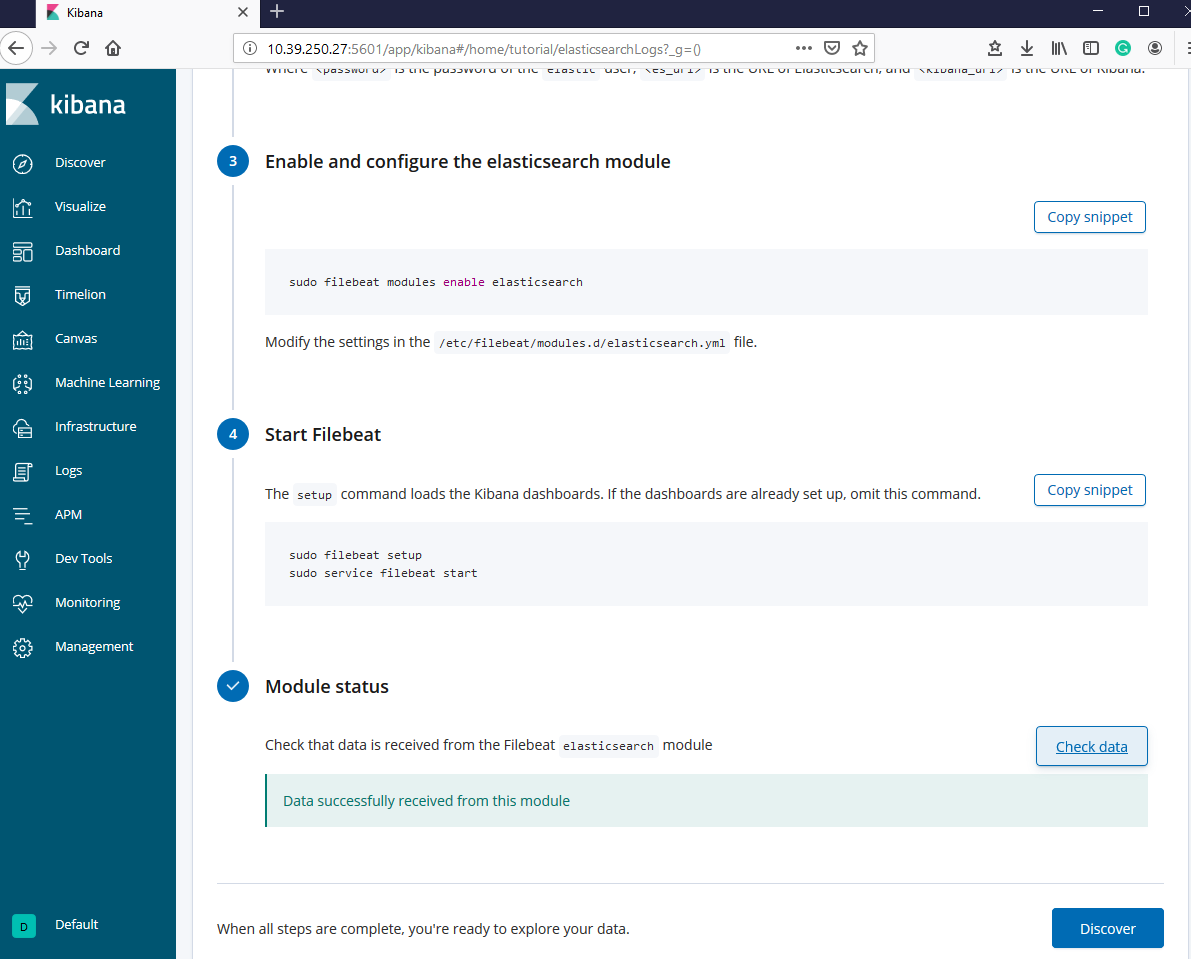
Execute the following command to check the status for Filebeat

**sudo service filebeat status**

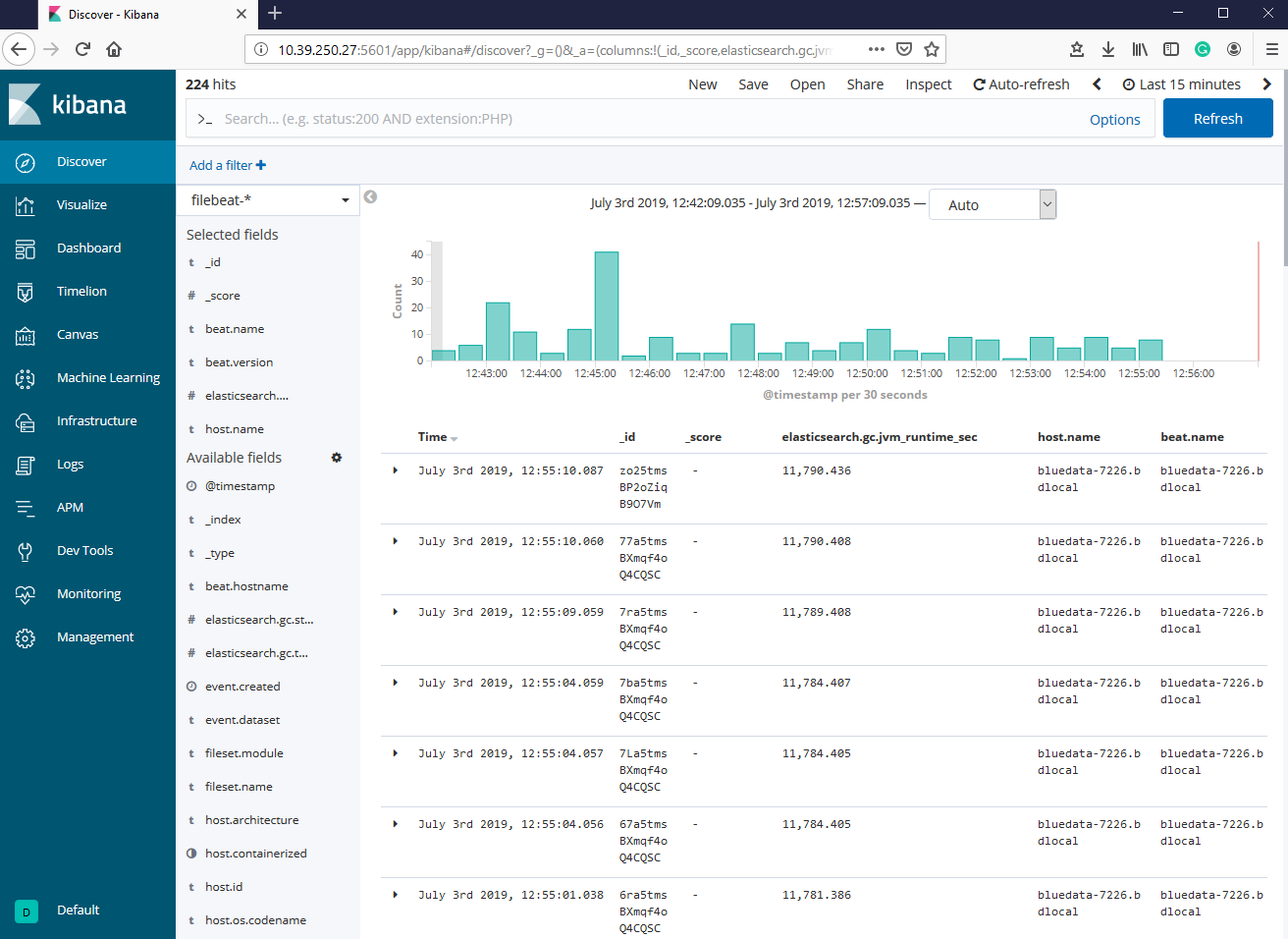


## Collecting Elasticsearch logs in Kibana UI

Go to the Elasticsearch logs section in Kibana UI and click on Check data button.

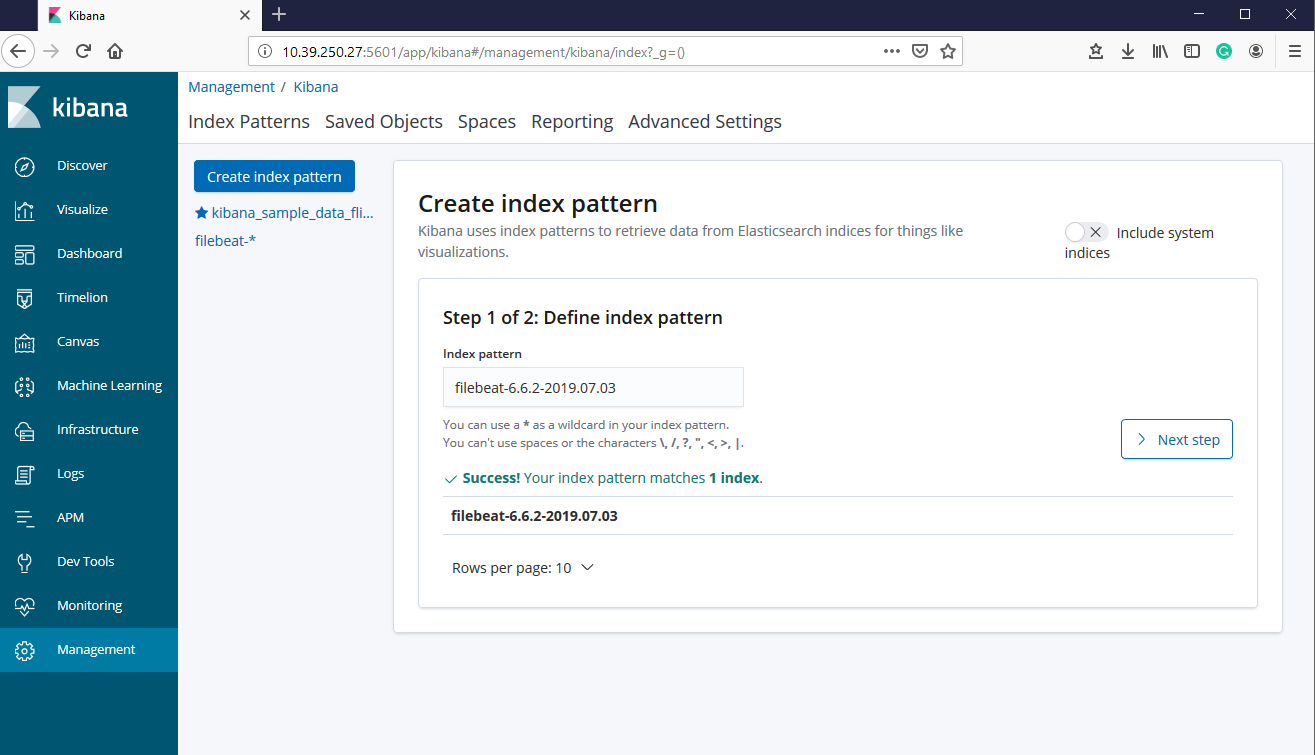


Click on Discover to explore your Elasticsearch log data

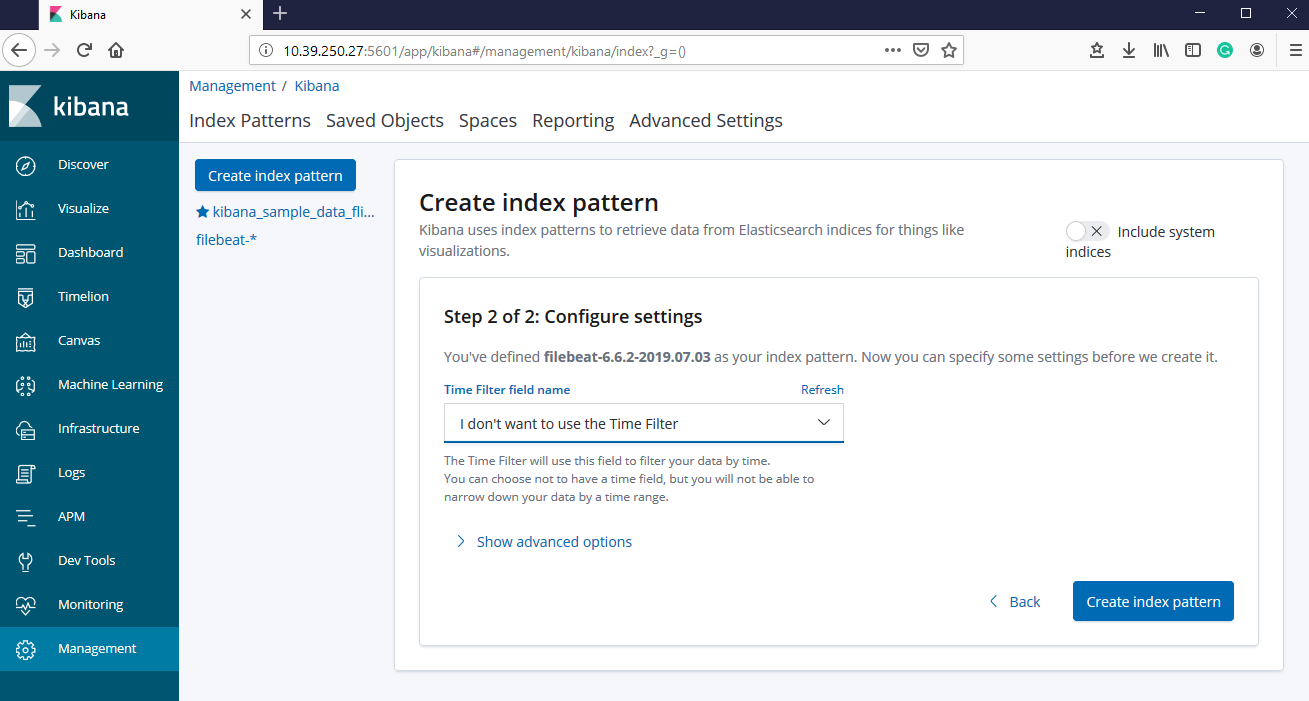


## Create Index patterns name for Elasticsearch logs data

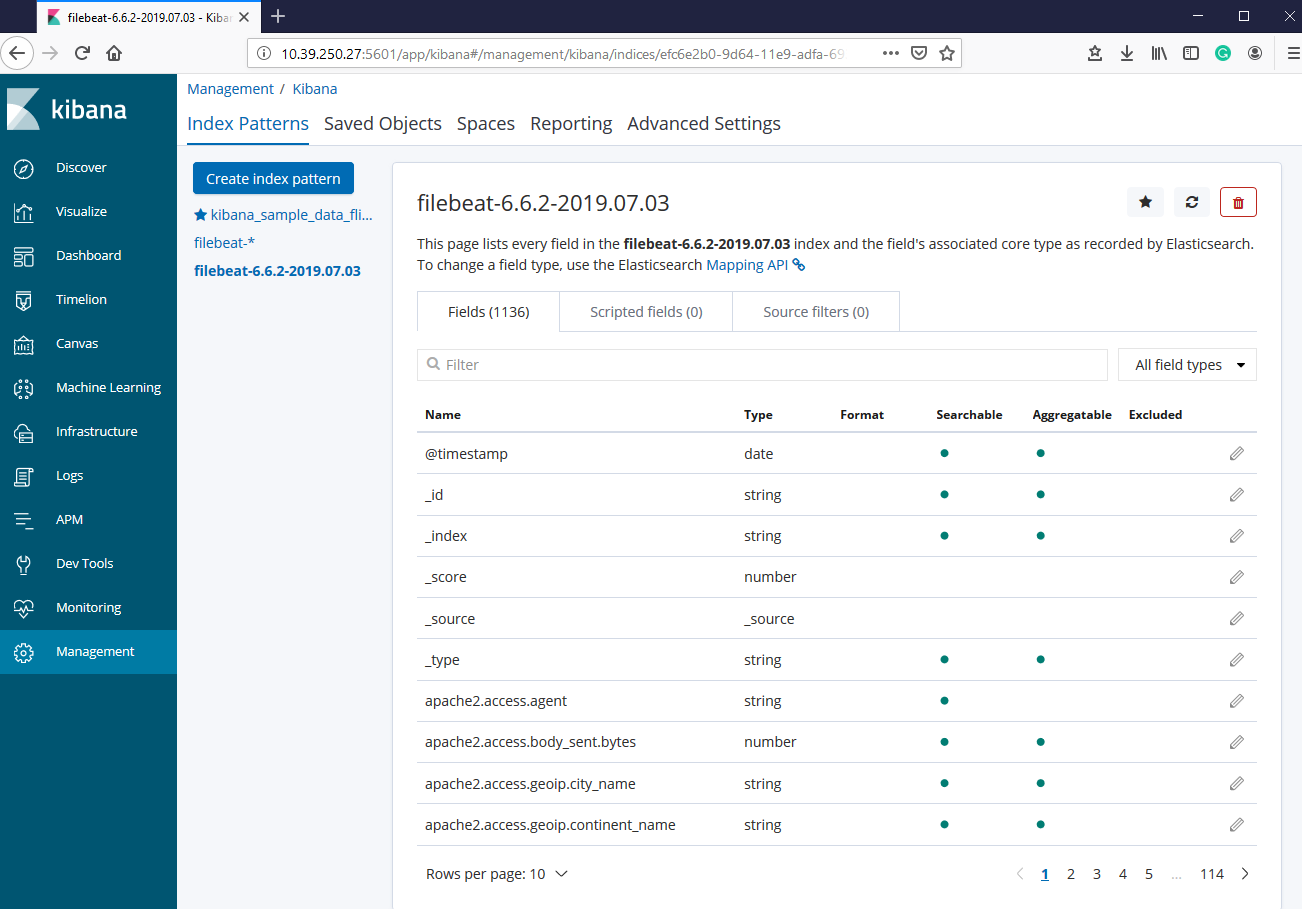
Go to the Management section and then click on Index Patterns.



Define index pattern then click on Next step.



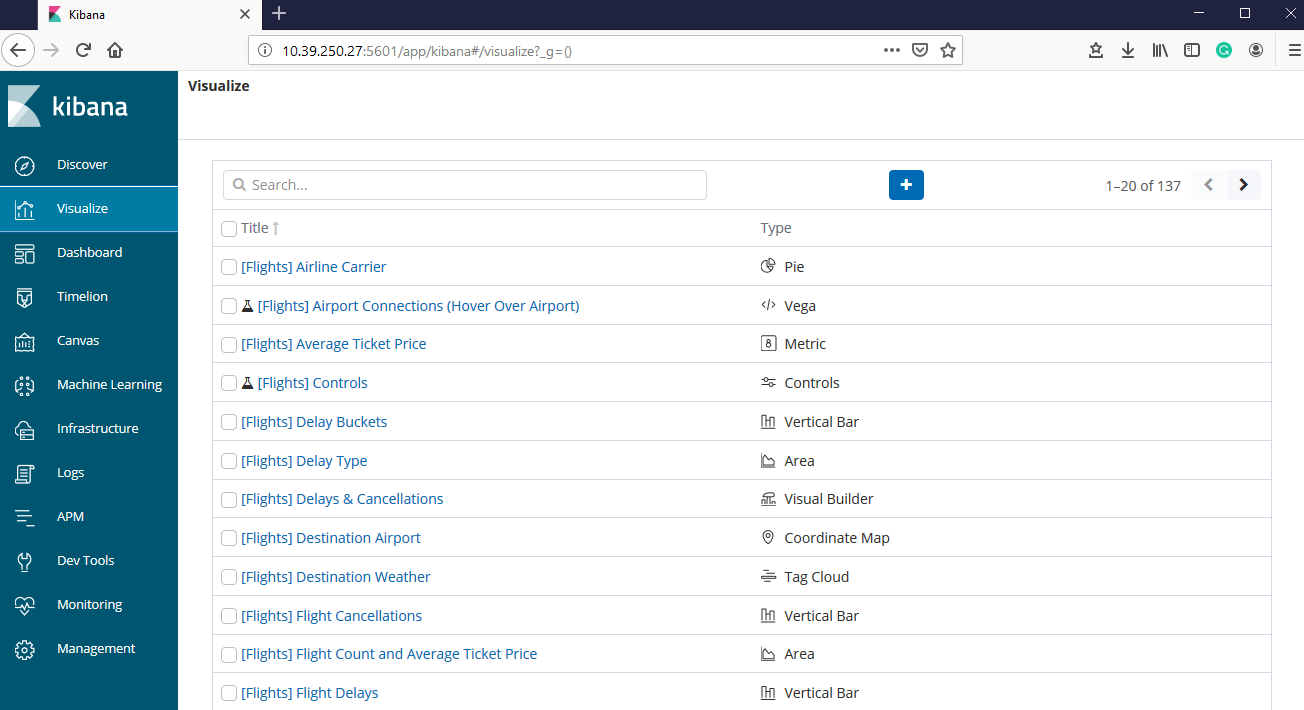
Click on Create index pattern to define time filter field name for your index pattern



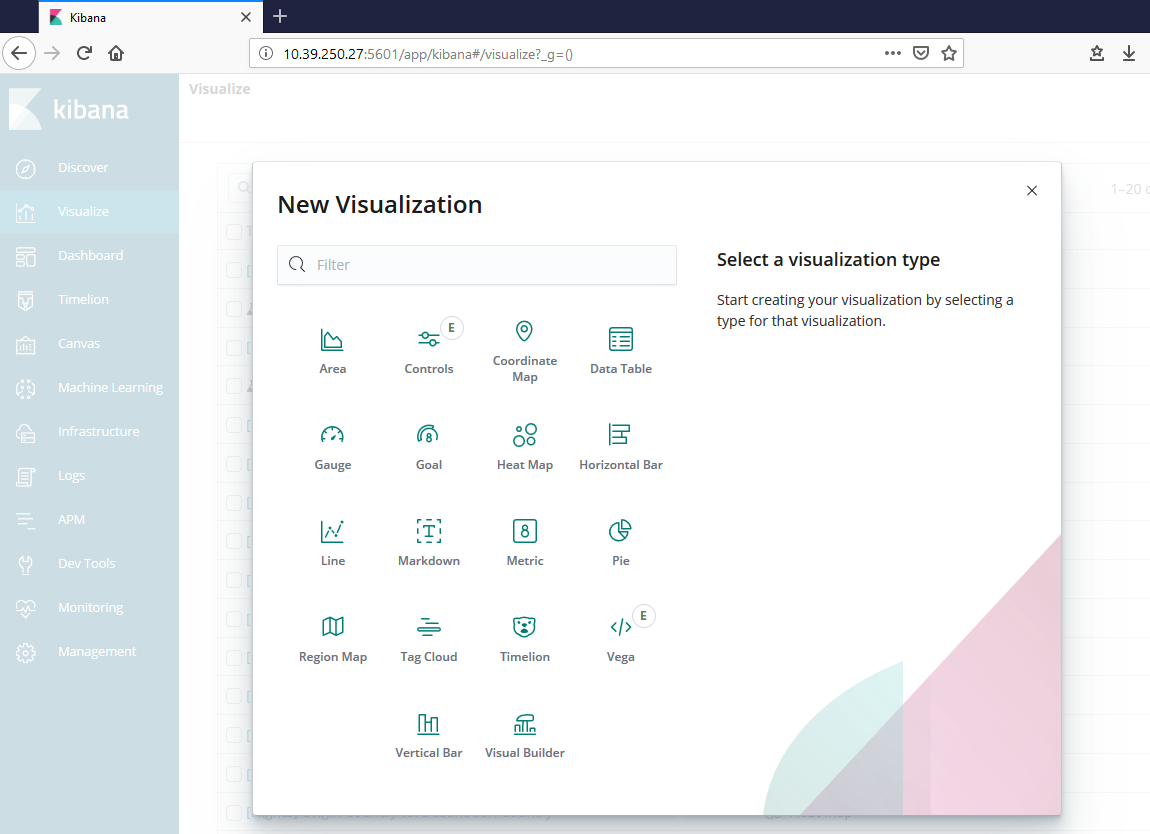
New index pattern is created successfully.

## Create visualization type for Elasticsearch logs data

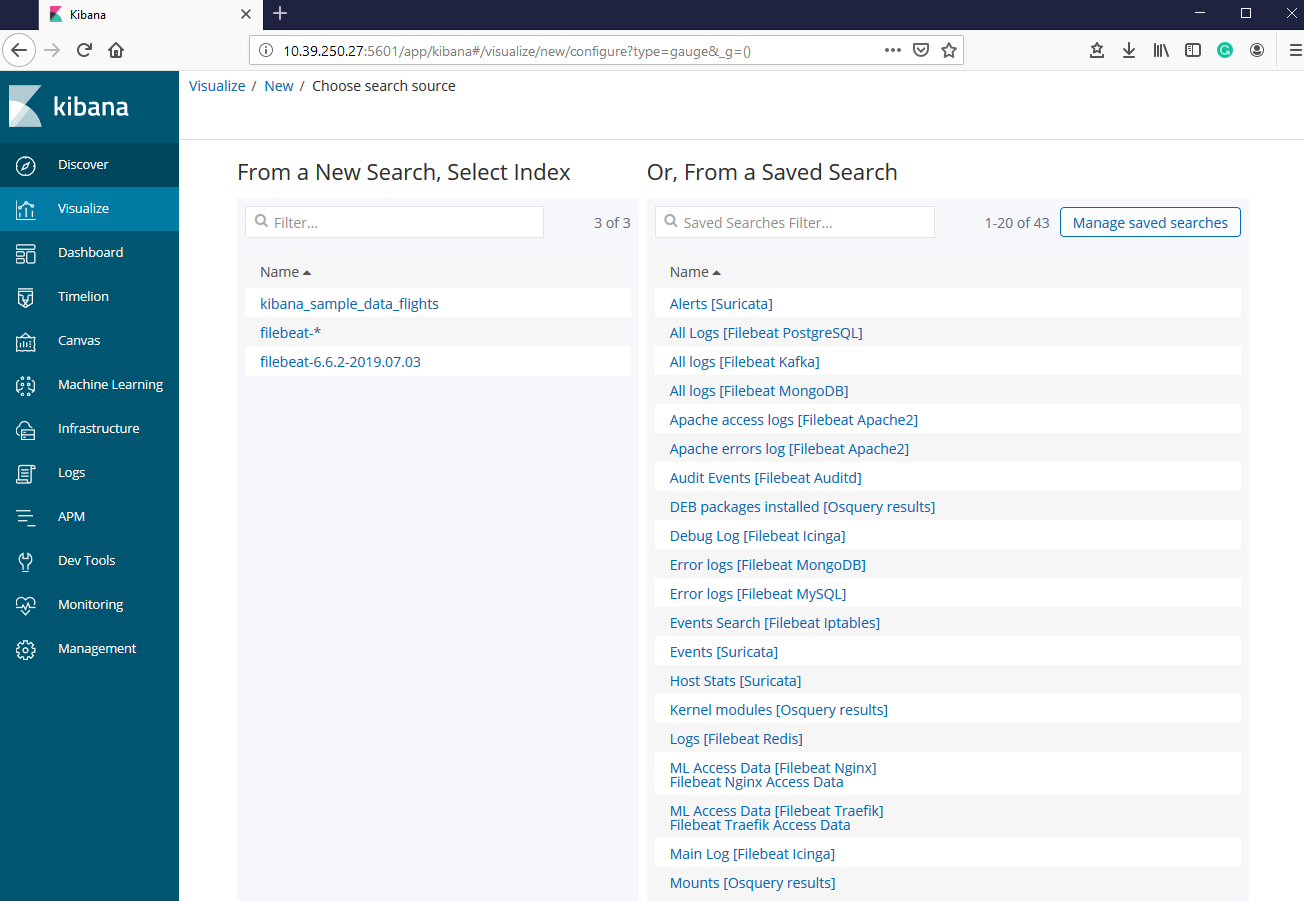
Click on Visualize section on Kibana UI.



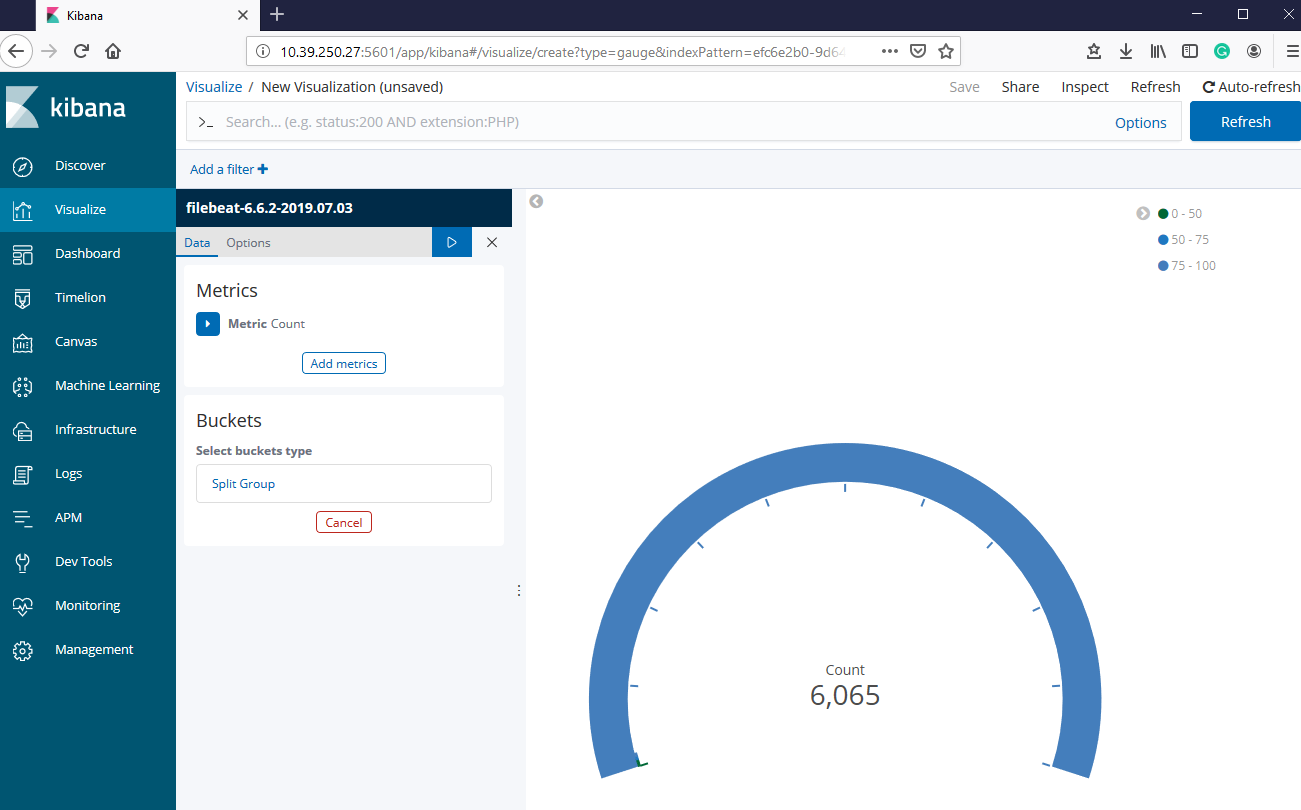
Click on + sign to create new visualization type for Elasticsearch logs data



Click on Gauge to create gauge visualization for Elasticsearch log data.



Select filebeat.6.6.2.2019.07.03 to create gauge visualization for Elasticsearch logs data

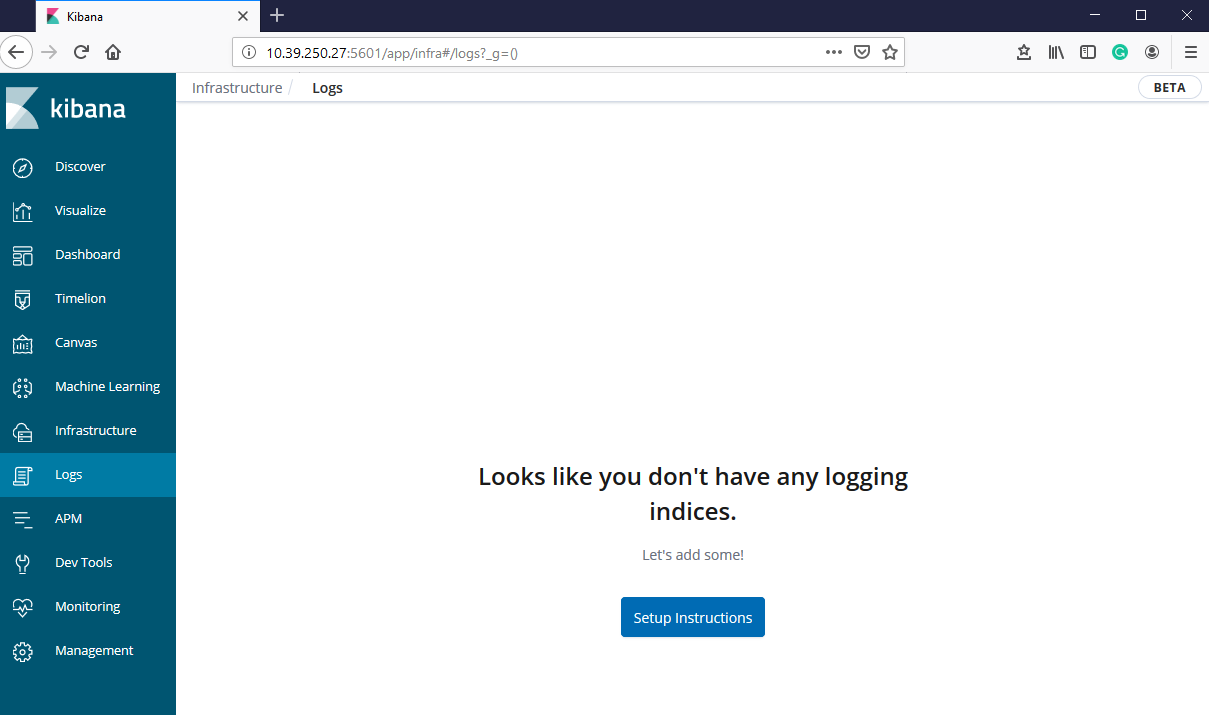


Gauge visualization is created for Elasticsearch logs data successfully.

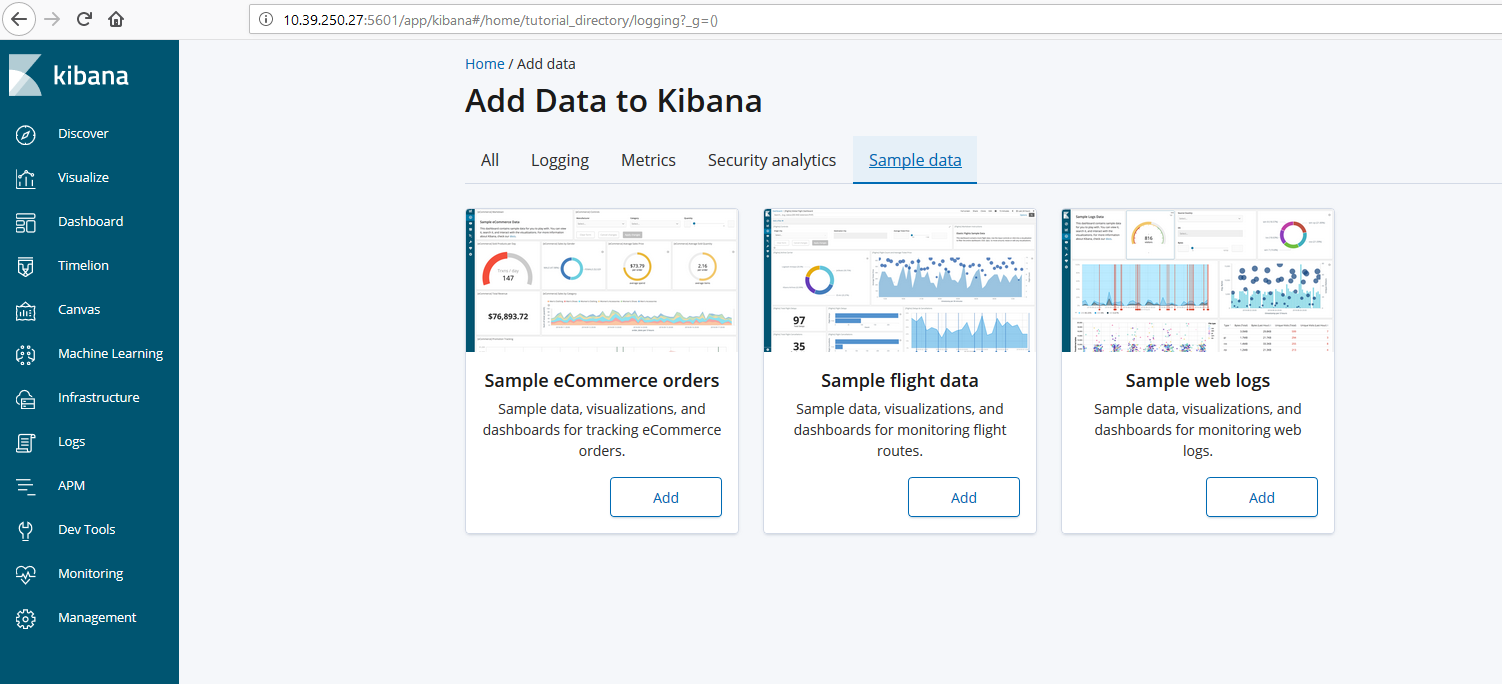
# TESTING ELK STACK WITH SAMPLE FLIGHT DATASET

## Add sample flight data to Kibana

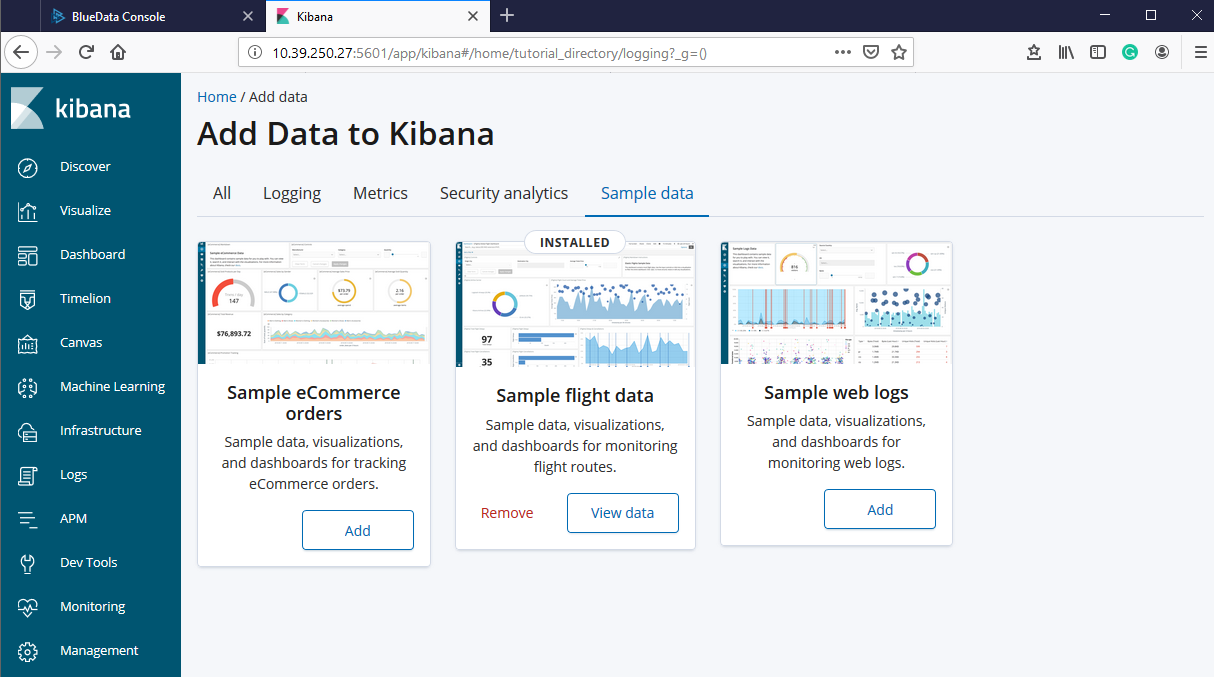
We will use Kibana UI to add sample flights dataset and test the ELK stack



Click on Add to install sample flight data in Kibana

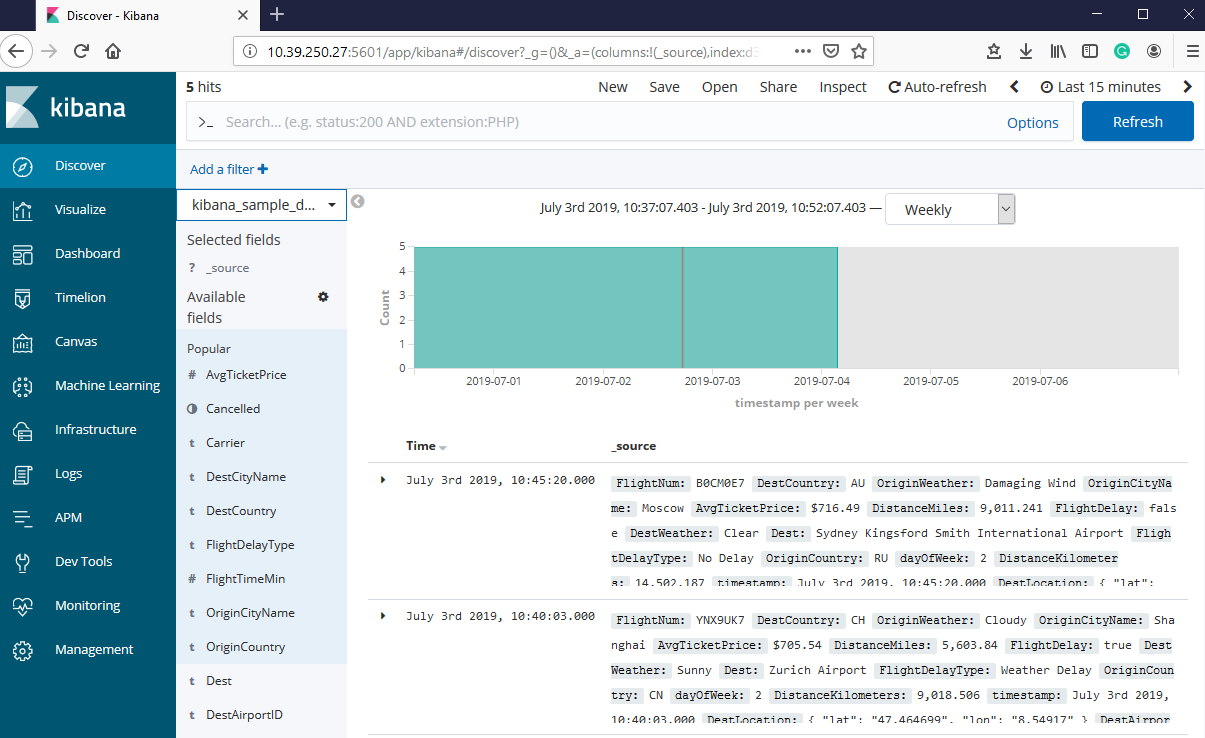


Click on View data to check the data in sample flight data and you can also remove sample flight data anytime from Kibana



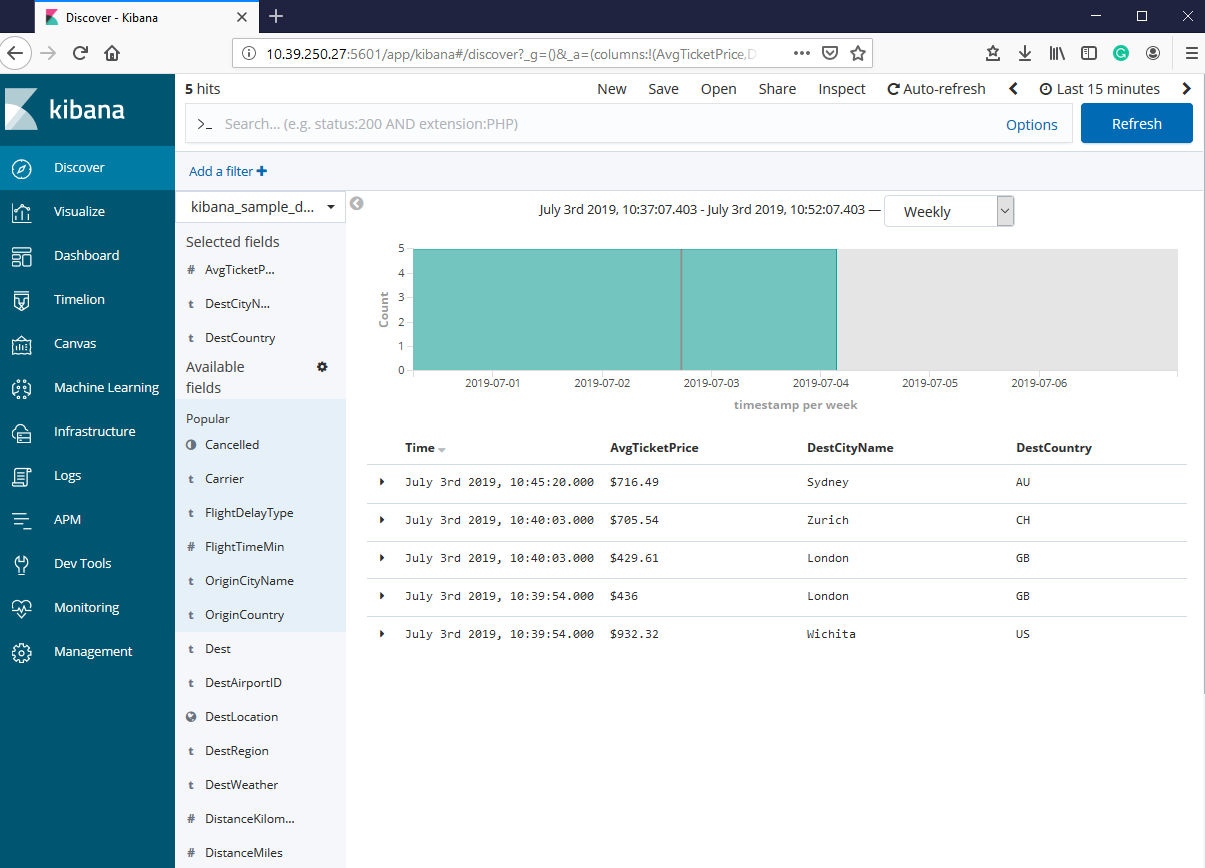
## Discover the sample flight dataset

Click on Discover section in Kibana UI



Here you can see selected fields and available fields for kibana\_sample\_data\_flights. By adding available fields into selected fields, we can get filtered results.

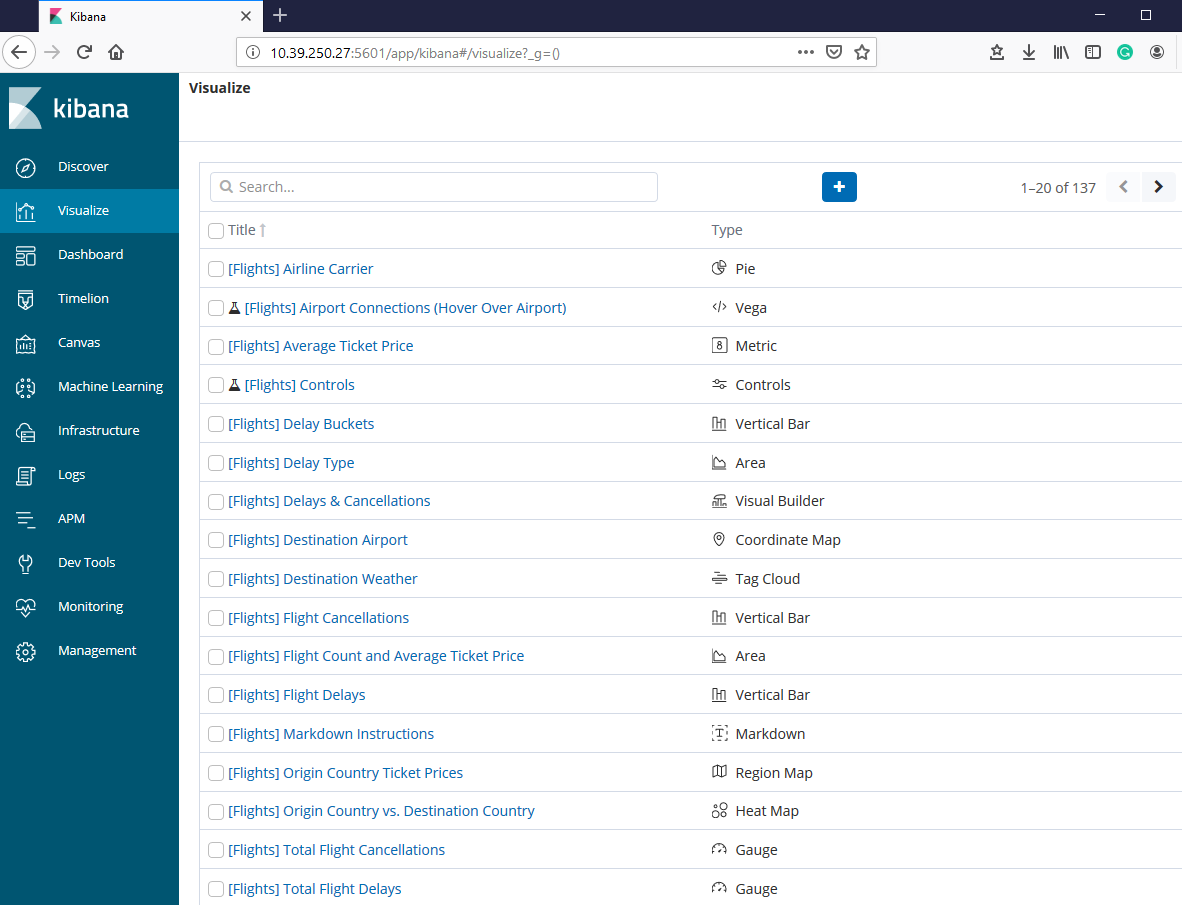
Let’s select some of the field, which is available.



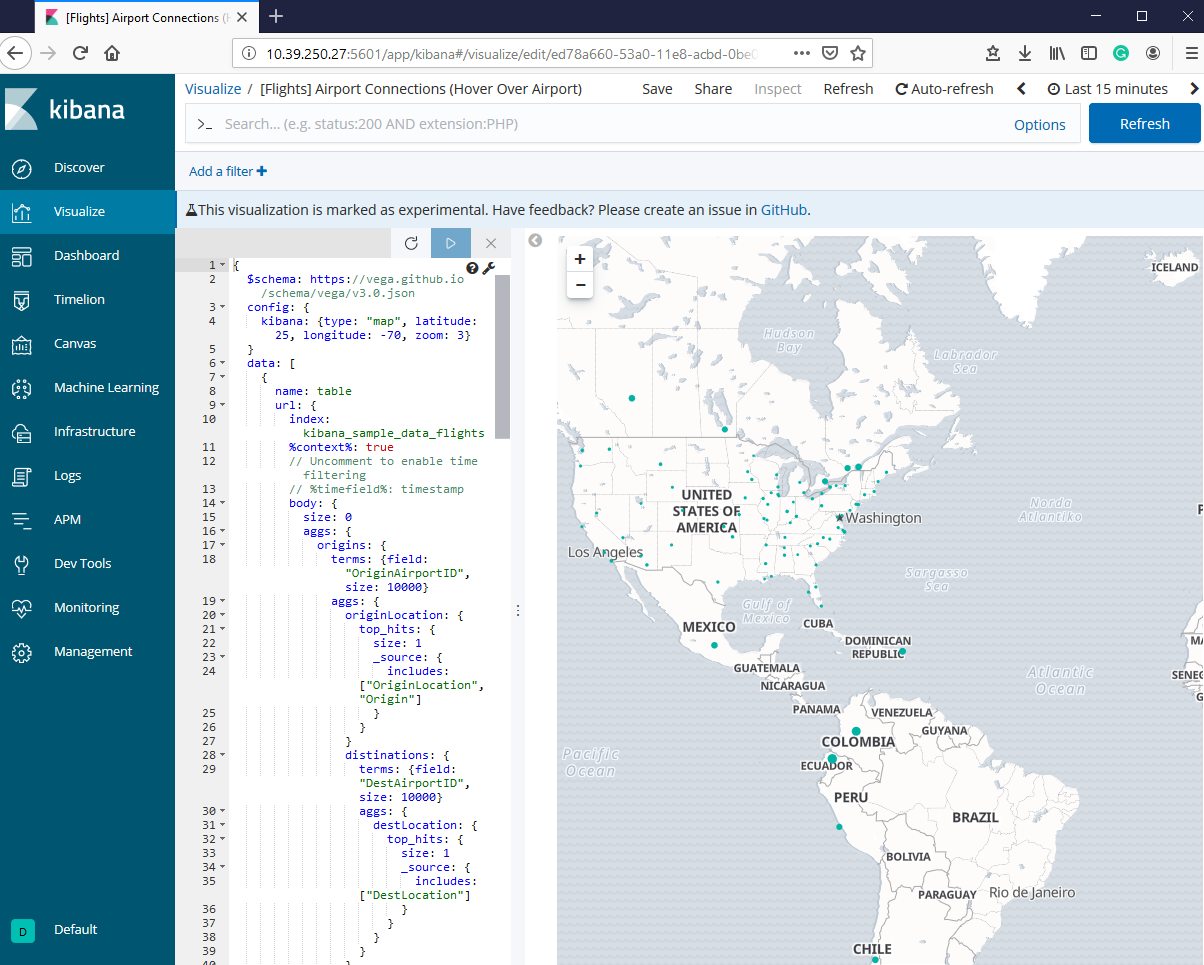
Here selected fields are avgticketprice, destcityname and destcountry. You can see the filtered output based on the fields you selected.

## Visualize the sample flight dataset

Click on Visualize to check available visualization type for sample flight dataset



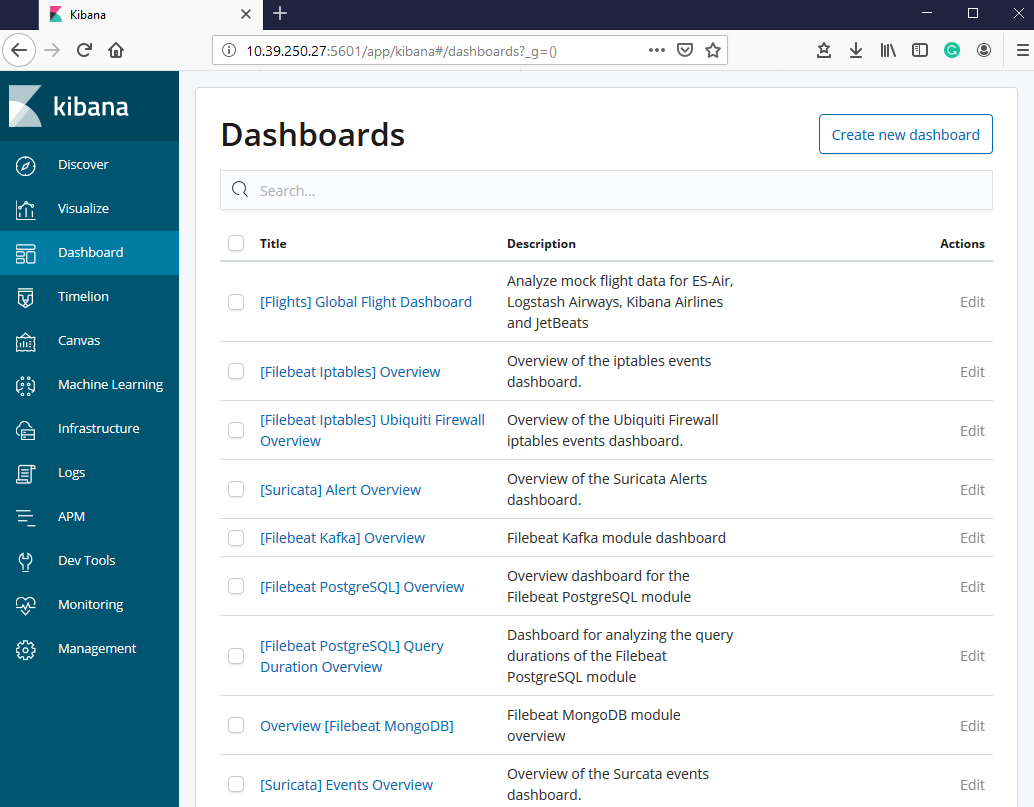
Here you can see the visualization type available for sample flight dataset. Select any visualization type to explore the sample flights dataset.



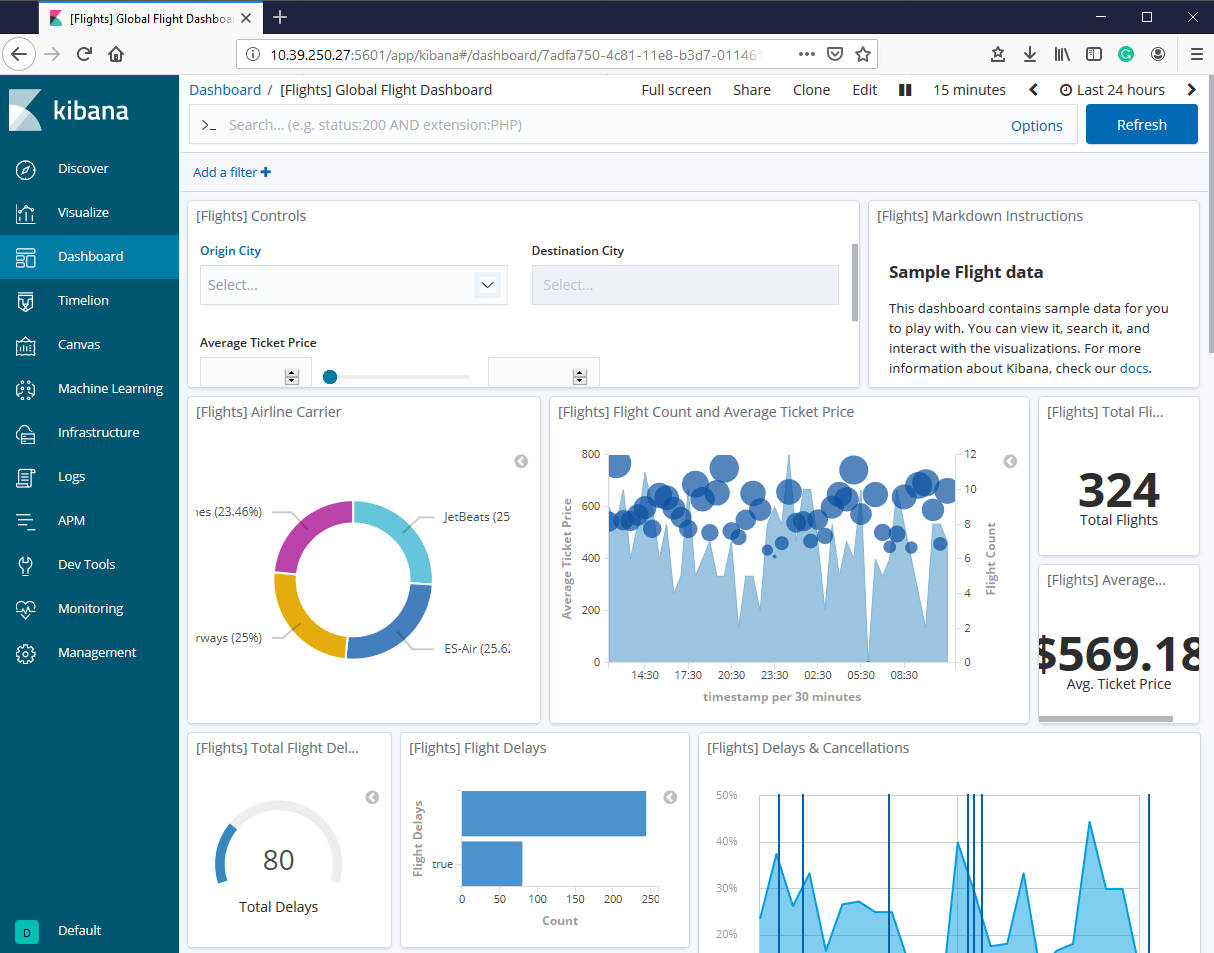
Here we have selected the [Flights] Airport Connections (Hover Over Airport) visualization, which has Vega visualization type. When you will do hover over airport you will see how many connections that airport has.

## Test Dashboard for sample flight dataset

Click on Dashboard section to check dashboard for sample flight dataset. Here we have Global Flight Dashboard for sample flight dataset.

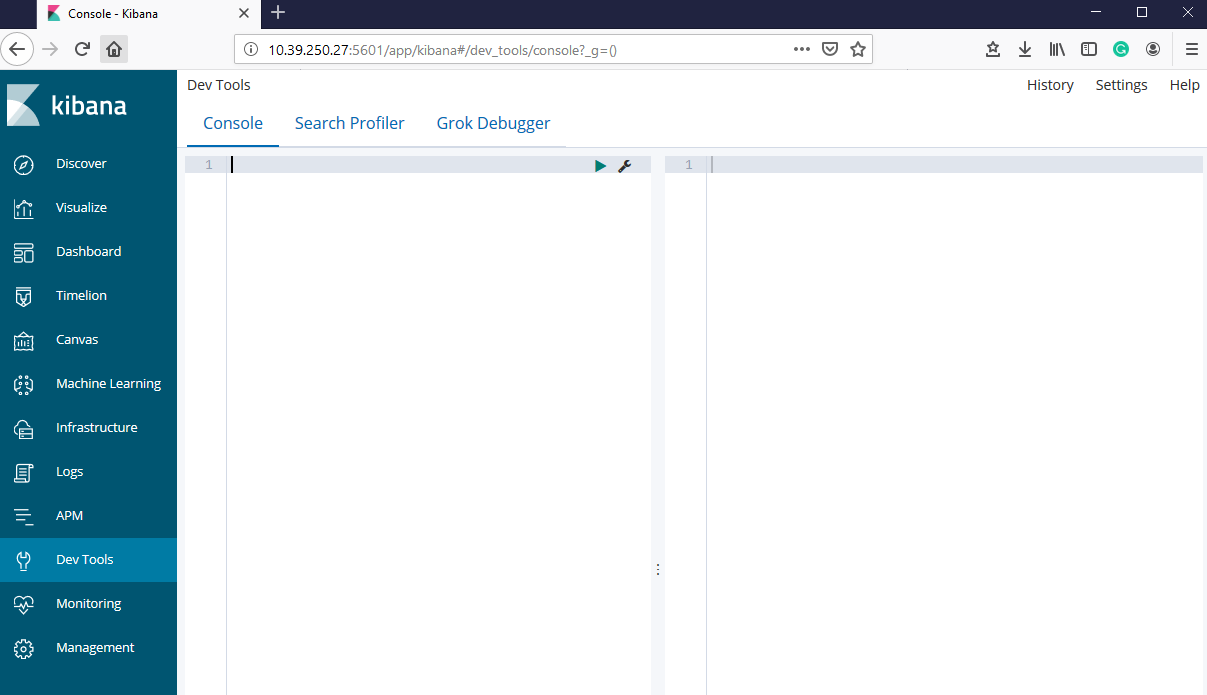


Click on Global Flight Dashboard to explore dashboard for sample flight dataset.



## Test REST API from Dev Tools

Click on Dev Tools in Kibana UI



Note: Here you can run your REST API commands

Use following REST command to check whether Sample flight data added to Kibana

GET \_search

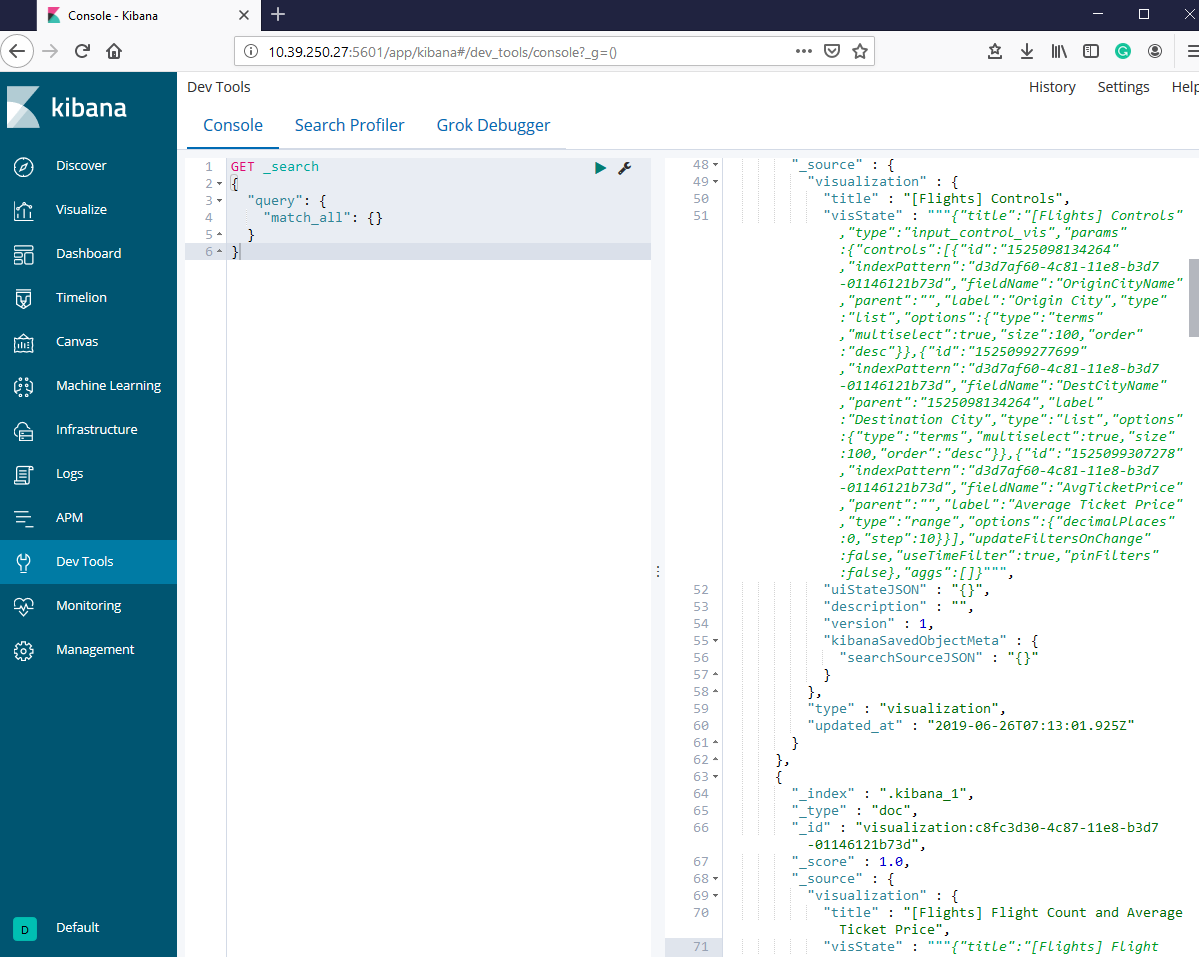
{

"query": {

"match\_all": {}

}

}



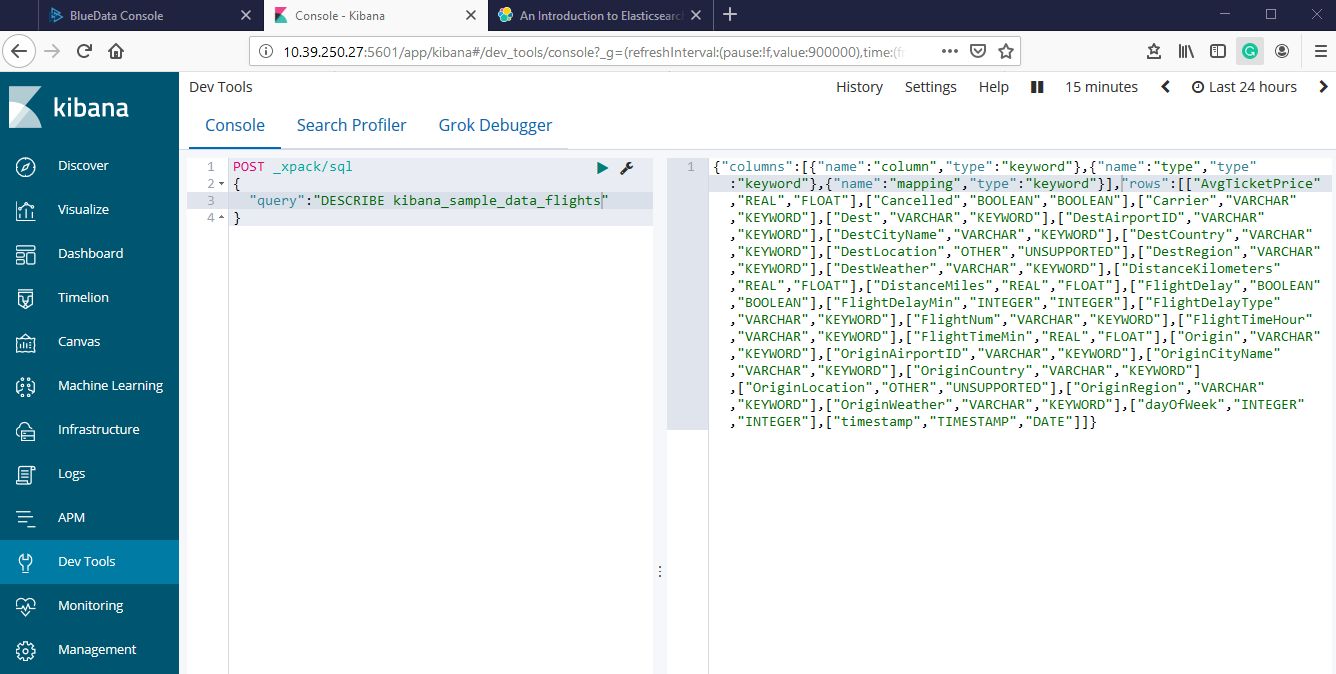
Use the following command to describe what is inside the sample flight dataset

POST \_xpack/sql

{

"query":"DESCRIBE kibana\_sample\_data\_flights"

}



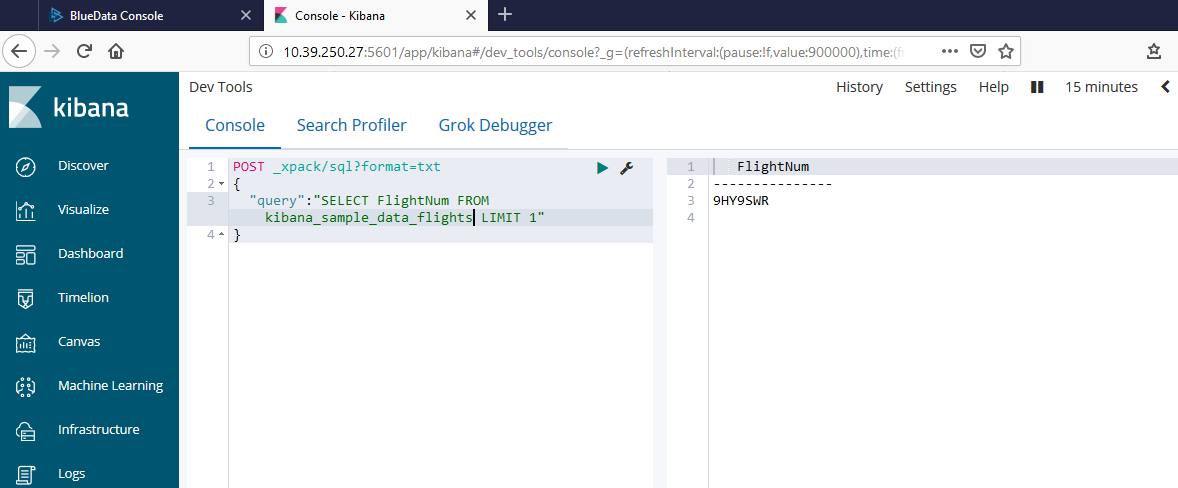
Use following command to run SELECT query in sample flight dataset

POST \_xpack/sql?format=txt

{

"query":"SELECT FlightNum FROM kibana\_sample\_data\_flights LIMIT 1"

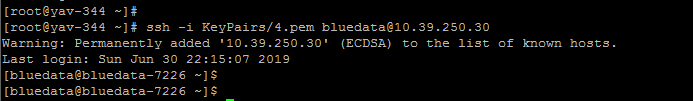
}



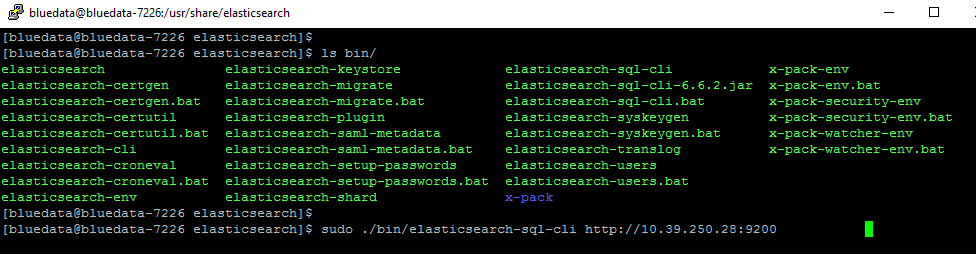
## Testing SQL CLI for ELK

Go inside the container where Elasticsearch is installed

**ssh -i <your pem keypair> bluedata@<ip address>**

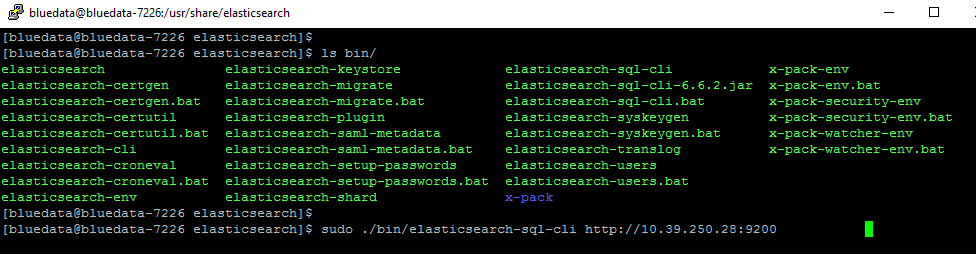


Go to the directory (/usr/share/elasticsearch) where Elasticsearch is installed then use ls command. We will be using elasticserach-sql-cli

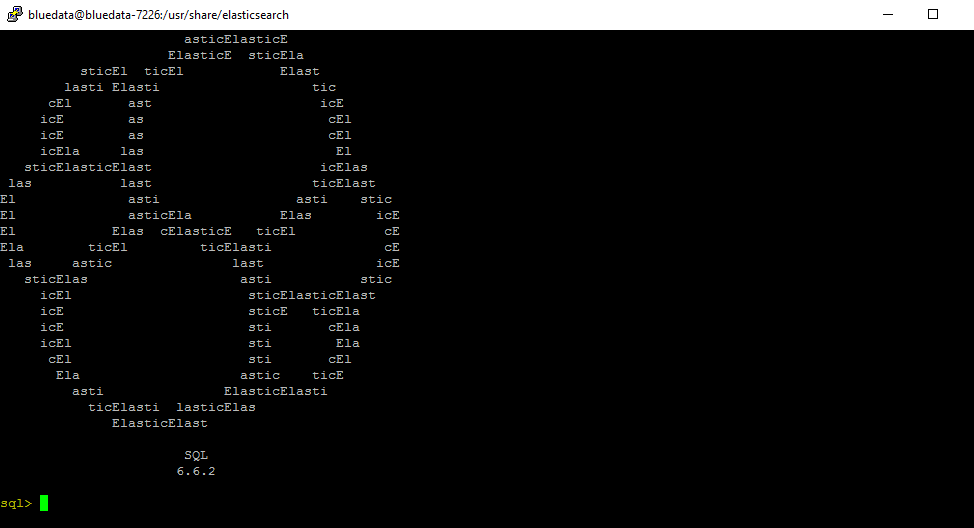


Execute the following command to open SQL CLI, which is installed with Elasticsearch. You can pass the URL of the Elasticsearch instance as a first parameter

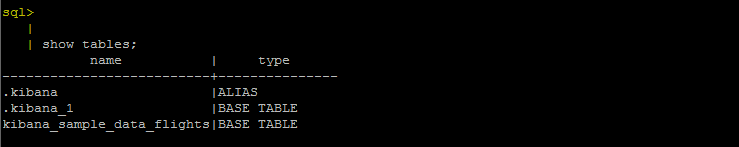
**sudo ./bin/elasticsearch-sql-cli http://<ip-address of elastics search node>:9200**



After executing above command, you will see the SQL CLI as given below



Execute the following command to check which tables are available



Execute the following command to run simple SELECT query in sample flights data table

