

SMOKE TEST

ELK 6.6.2

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
2	LOADING SAMPLE DATA AND VISUALIZING THE DATA IN KIBANA.....	5
2.1	CREATE INDEX PATTERNS FOR SAMPLE ACCOUNT DATA.....	7
2.2	CREATE VISUALIZATION TYPE FOR SAMPLE ACCOUNT DATA.....	8
3	COLLECTING ELASTICSEARCH LOGS USING FILEBEAT.....	11
3.1	INSTALLING AND SETTING UP FILEBEAT	12
3.2	COLLECTING ELASTICSEARCH LOGS IN KIBANA UI	14
3.3	CREATE INDEX PATTERNS NAME FOR ELASTICSEARCH LOGS DATA.....	16
3.4	CREATE VISUALIZATION TYPE FOR ELASTICSEARCH LOGS DATA	17
4	TESTING ELK STACK WITH SAMPLE FLIGHT DATASET	20
4.1	ADD SAMPLE FLIGHT DATA TO KIBANA.....	20
4.2	DISCOVER THE SAMPLE FLIGHT DATASET	21
4.3	VISUALIZE THE SAMPLE FLIGHT DATASET.....	22
4.4	TEST DASHBOARD FOR SAMPLE FLIGHT DATASET	25
4.5	TEST REST API FROM DEV TOOLS	26
4.6	TESTING SQL CLI FOR ELK.....	28

1 INSPECT STATUS OF THE CLUSTER

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

```
[bluedata@bluedata-2541 ~]$ curl http://172.18.0.8:9200/_cat/health
1553251084 10:38:04 sds-demo-cluster green 3 3 10 5 0 0 0 0 - 100.0%
```

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

```
[bluedata@bluedata-2541 ~]$ curl -XGET '172.18.0.8:9200/_cluster/health?pretty'
{
  "cluster_name" : "sds-demo-cluster",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 3,
  "number_of_data_nodes" : 3,
  "active_primary_shards" : 5,
  "active_shards" : 10,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0,
  "task_max_waiting_in_queue_millis" : 0,
  "active_shards_percent_as_number" : 100.0
}
```

1.1 Inspect Cluster Stats

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

```
[bluedata@bluedata-2541 ~]$ curl http://172.18.0.8:9200/_cluster/stats
{"_nodes":{"total":3,"successful":3,"failed":0},"cluster_name":"sds-demo-cluster","cluster_uuid":"8D-0RitLS2S25TxP2rpU-Q","timestamp":1553251342487,"status":"green","indices":{"count":1,"shards":{"total":10,"primaries":5,"replication":1.0,"index":{"shards":{"min":10,"max":10,"avg":10.0},"primaries":{"min":5,"max":5,"avg":5.0},"replication":{"min":1.0,"max":1.0,"avg":1.0}}},"docs":{"count":1,"deleted":0},"store":{"size_in_bytes":10268},"fielddata":{"memory_size_in_bytes":0,"evictions":0},"query_cache":{"memory_size_in_bytes":0,"total_count":0,"hit_count":0,"miss_count":0,"cache_size":0,"cache_count":0,"evictions":0},"completion":{"size_in_bytes":0},"segments":{"count":2,"memory_in_bytes":2374,"terms_memory_in_bytes":1478,"stored_fields_memory_in_bytes":624,"term_vectors_memory_in_bytes":0,"norms_memory_in_bytes":128,"points_memory_in_bytes":8,"doc_values_memory_in_bytes":136,"index_writer_memory_in_bytes":0,"version_map_memory_in_bytes":0,"fixed_bit_set_memory_in_bytes":0},"max_unsafe_auto_id_timestamp":1553126694700,"file_sizes":{},"nodes":{"count":{"total":3,"data":3,"coordinating_only":0},"master":3,"ingest":3},"versions":["6.6.2"],"os":{"available_processors":24,"allocated_processors":24},"names":[{"name":"Linux","count":3}],"pretty_names":[{"pretty_name":"CentOS Linux 7 (Core)","count":3}],"mem":{"total_in_bytes":202164760576,"free_in_bytes":95627595776,"used_in_bytes":106537164800,"free_percent":47,"used_percent":53},"process":{"cpu":{"percent":0},"open_file_descriptors":{"min":333,"max":336,"avg":334},"jvm":{"max_uptime_in_millis":139730032,"versions":[{"version":"1.8.0_131","vm_name":"Java HotSpot(TM) 64-Bit Server VM","vm_version":"25.131-b11","vm_vendor":"Oracle Corporation","count":3}],"mem":{"heap_used_in_bytes":1296806928,"heap_max_in_bytes":3113877504,"threads":194},"fs":{"total_in_bytes":96605306880,"free_in_bytes":91653144576,"available_in_bytes":91653144576},"plugins":{},"network_types":{"transport_types":{"security4":3},"http_types":{"security4":3}}}}[bluedata@bluedata-2541 ~]$
```

2 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.

```
ssh -i <your pem keypair> bluedata@<ip_address>
```

```
[root@yav-344 ~]# ssh -i KeyPairs/4.pem bluedata@10.39.250.35
Warning: Permanently added '10.39.250.35' (ECDSA) to the list of known hosts.
Last login: Wed Jul  3 22:22:24 2019
[bluedata@bluedata-8475 ~]$
```

Execute the following command to download the sample account dataset:

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

```
[bluedata@bluedata-8475 ~]$ curl -O https://download.elastic.co/demos/kibana/gettingstarted/7.x/accounts.zip
% Total    % Received % Xferd Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left  Speed
100 57700  100 57700    0     0    155k      0  0:00:01  0:00:01  0:00:00  155k
[bluedata@bluedata-8475 ~]$
```

Execute the following command to unzip the sample account dataset:

```
unzip accounts.zip
```

```
[bluedata@bluedata-8475 ~]$ unzip accounts.zip
Archive:  accounts.zip
  inflating: accounts.json
[bluedata@bluedata-8475 ~]$ ls
accounts.json  accounts.zip  vagent.bin
[bluedata@bluedata-8475 ~]$
```

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
```

```
[bluedata@bluedata-8475 ~]$
[bluedata@bluedata-8475 ~]$ curl -H 'Content-Type: application/x-ndjson' -XPOST '10.39.250.2:9200/bank/account/_b
ulk?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:

```
{
  "index" : {
    "_index" : "bank",
    "_type" : "account",
    "_id" : "990",
    "_version" : 1,
    "result" : "created",
    "_shards" : {
      "total" : 2,
      "successful" : 2,
      "failed" : 0
    },
    "_seq_no" : 210,
    "_primary_term" : 1,
    "status" : 201
  }
},
{
  "index" : {
    "_index" : "bank",
    "_type" : "account",
    "_id" : "995",
    "_version" : 1,
    "result" : "created",
    "_shards" : {
      "total" : 2,
      "successful" : 2,
      "failed" : 0
    },
    "_seq_no" : 196,
    "_primary_term" : 1,
    "status" : 201
  }
}
]
}
[bluedata@bluedata-8475 ~]$
```

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
```

Dev Tools

History Settings Help

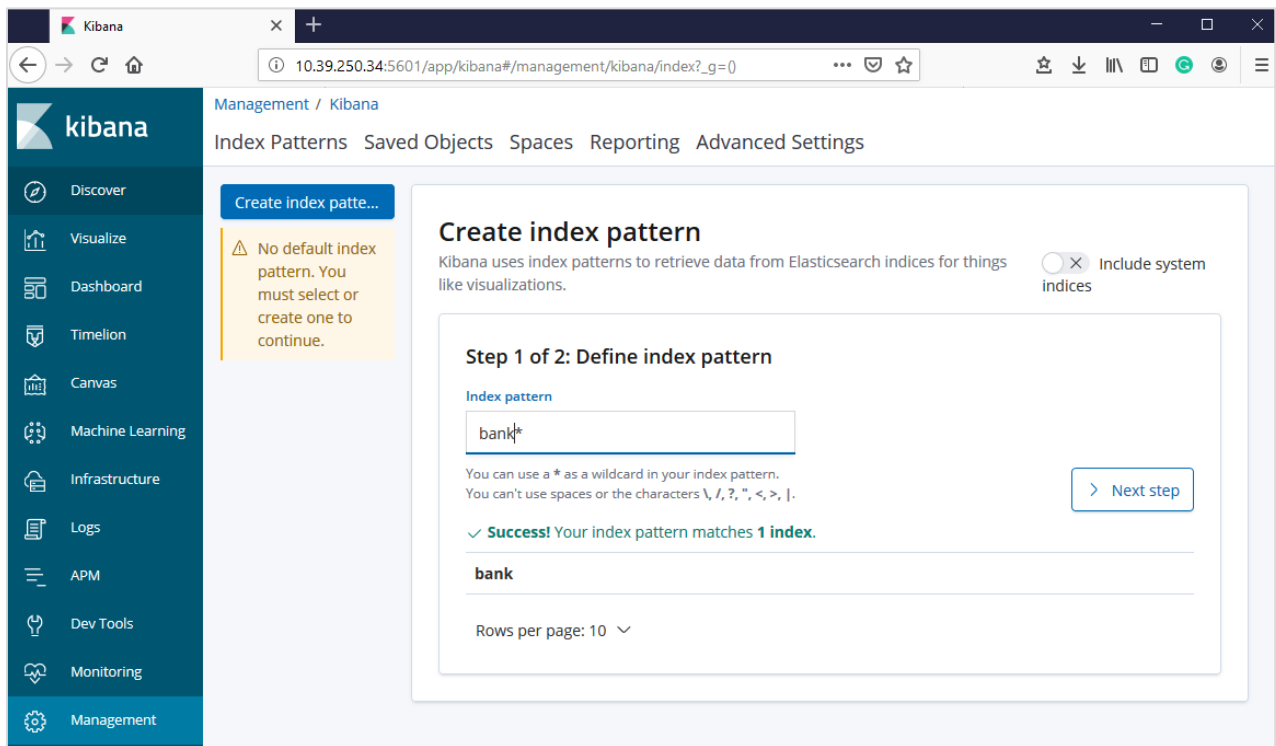
Console Search Profiler Grok Debugger

1 GET /_cat/indices?v

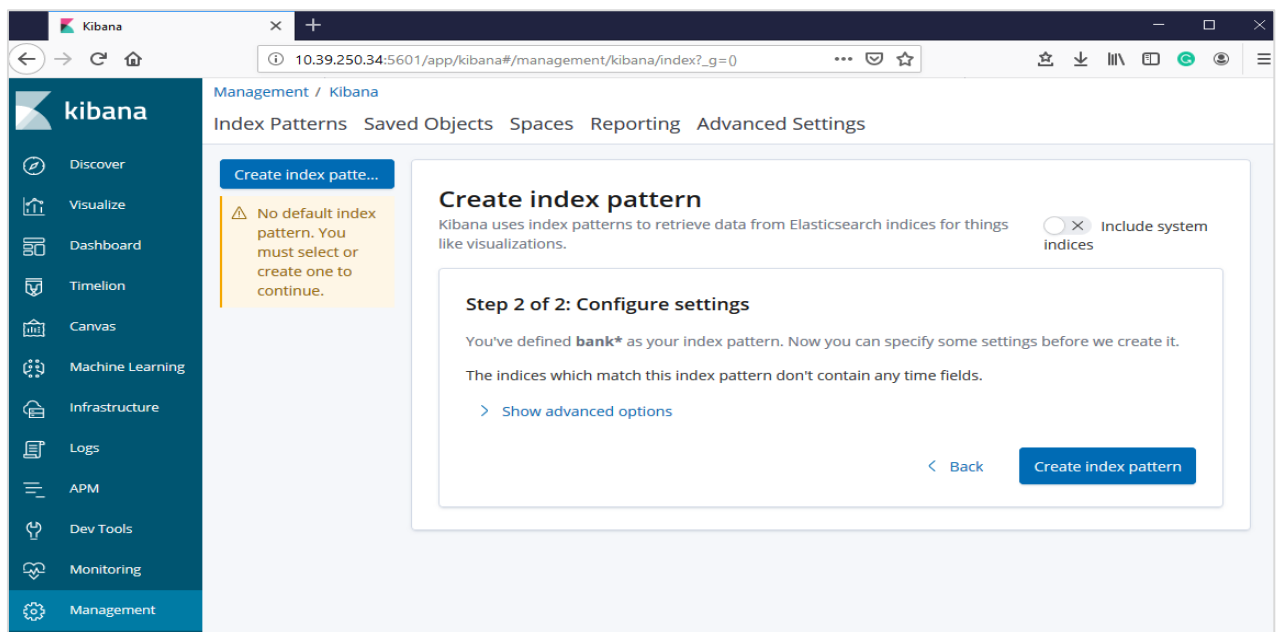
1	health	status	index	uuid	pri	rep	docs.count	docs.deleted	store.size	pri.store.size
2	green	open	bank	i_4I_4FURVCUXPWnx59ZFA	5	1	1000	0	950.5kb	475.2kb
3	green	open	.kibana_1	Wvfc4a4aQGWXI2ij0jmM7g	1	1	4	0	37.8kb	18.9kb
4										

2.1 Create Index Patterns for sample account data

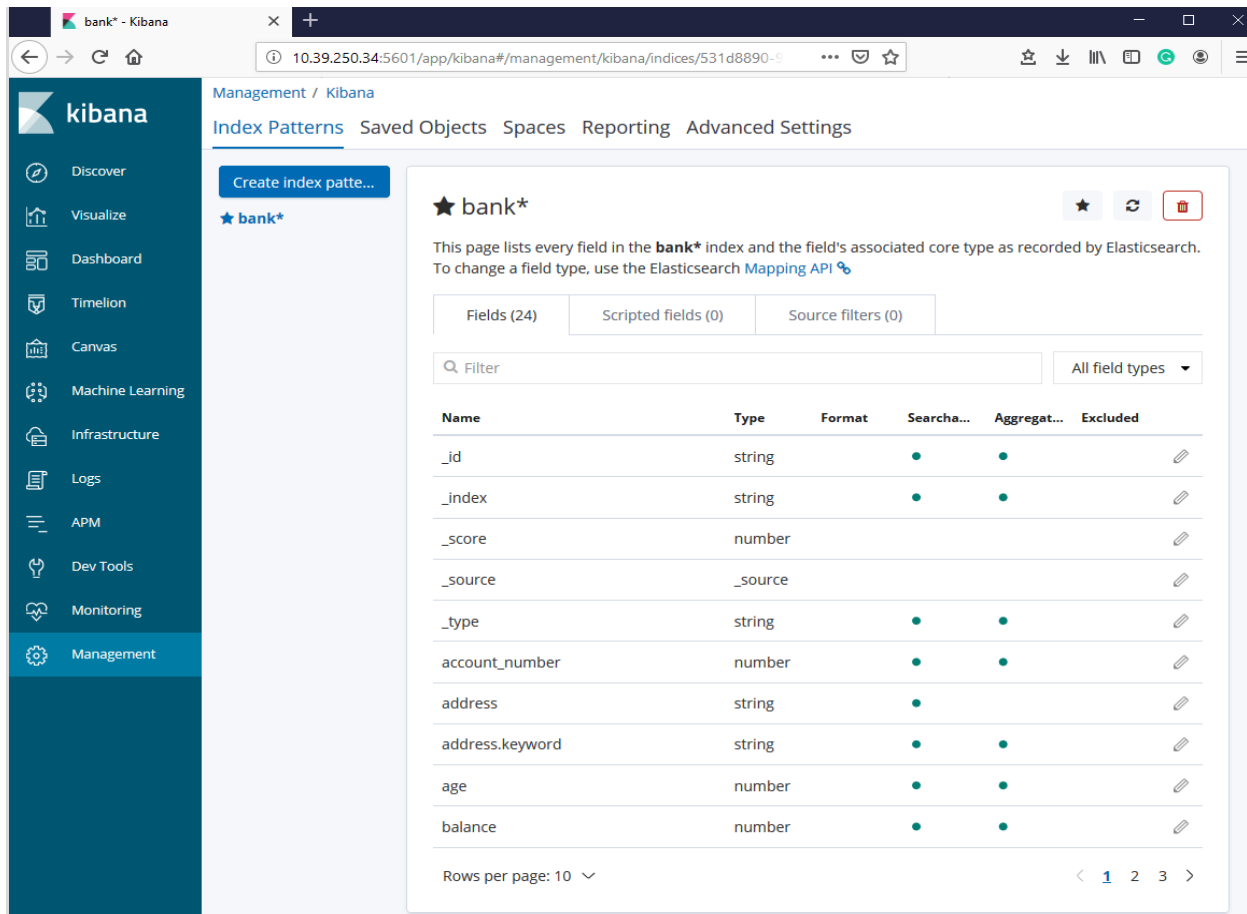
Go to the Management section and then click on Index Patterns on Kibana.



Define index patterns then click on Next step.



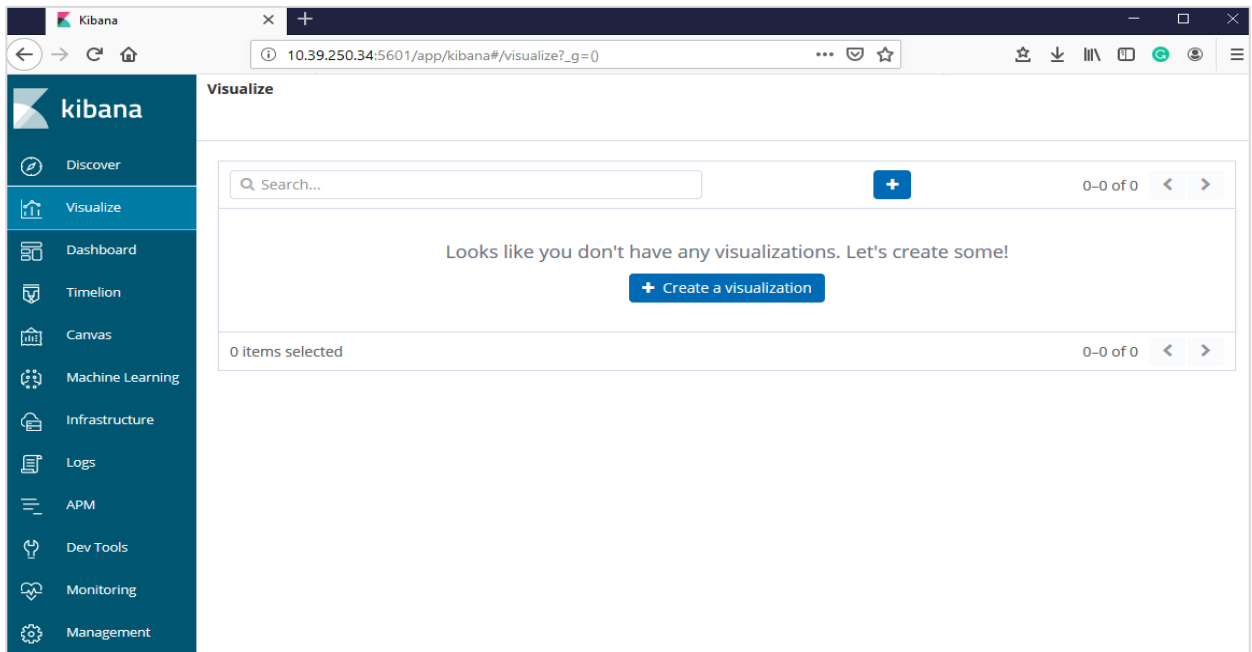
Click on Create Index Patterns.



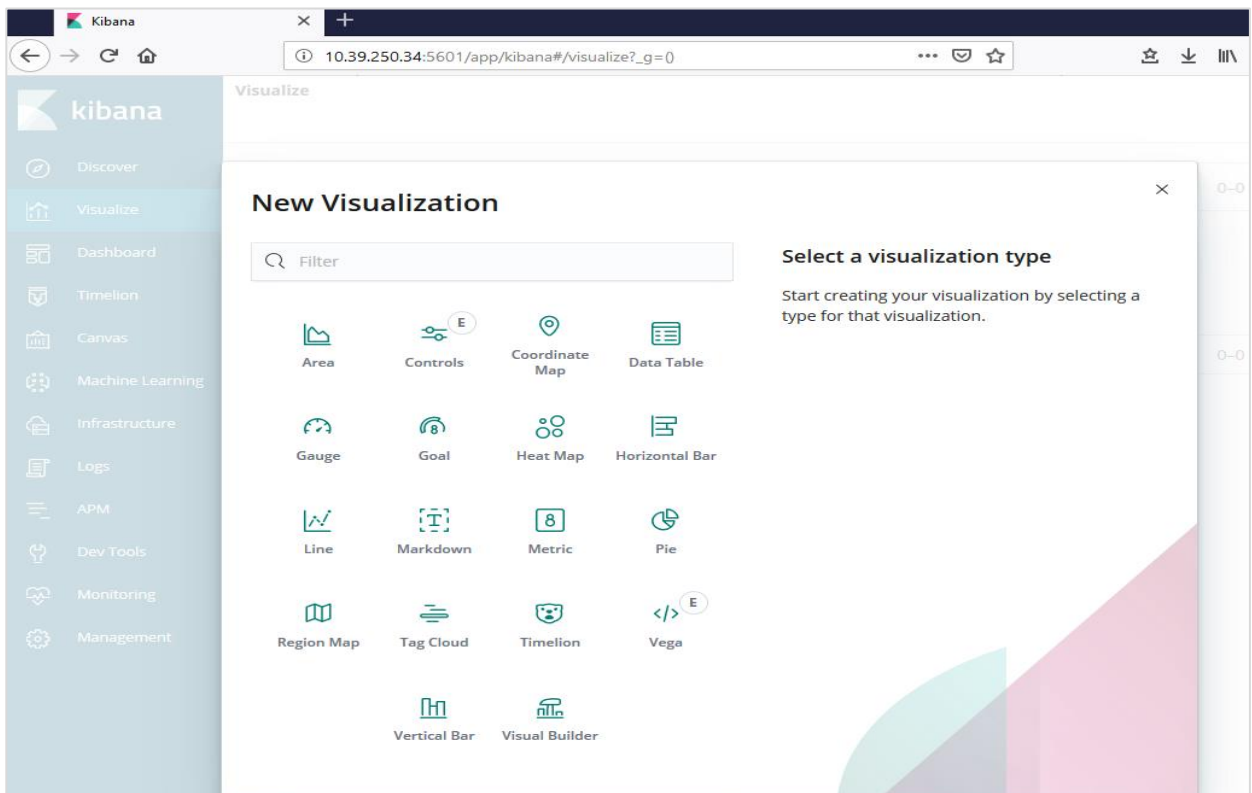
New index pattern is created successfully.

2.2 Create visualization type for sample account data

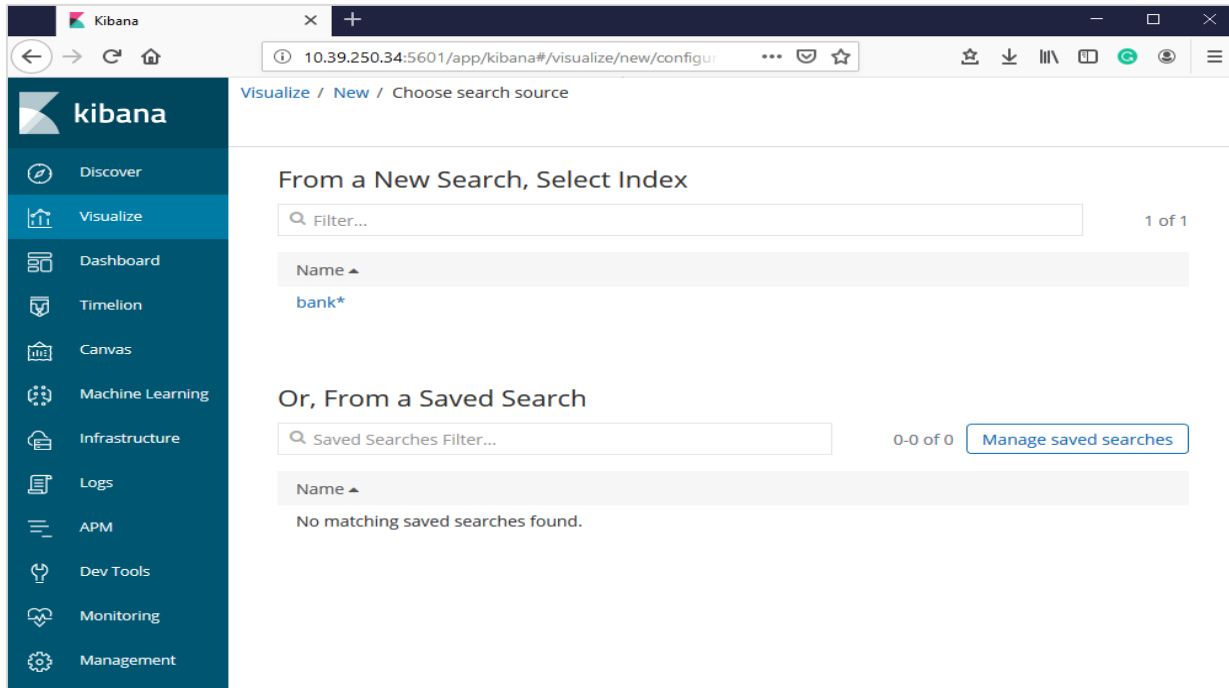
Click on Visualize section on Kibana UI.



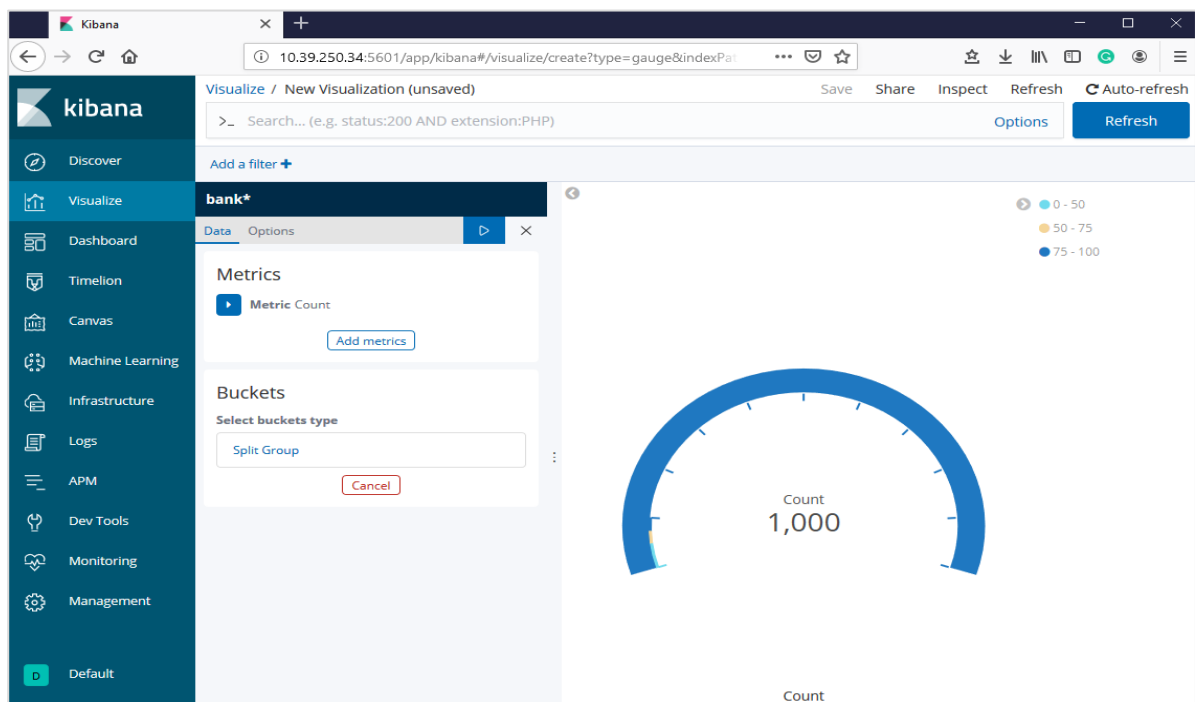
Click on + sign to create new visualization type for sample account data.



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



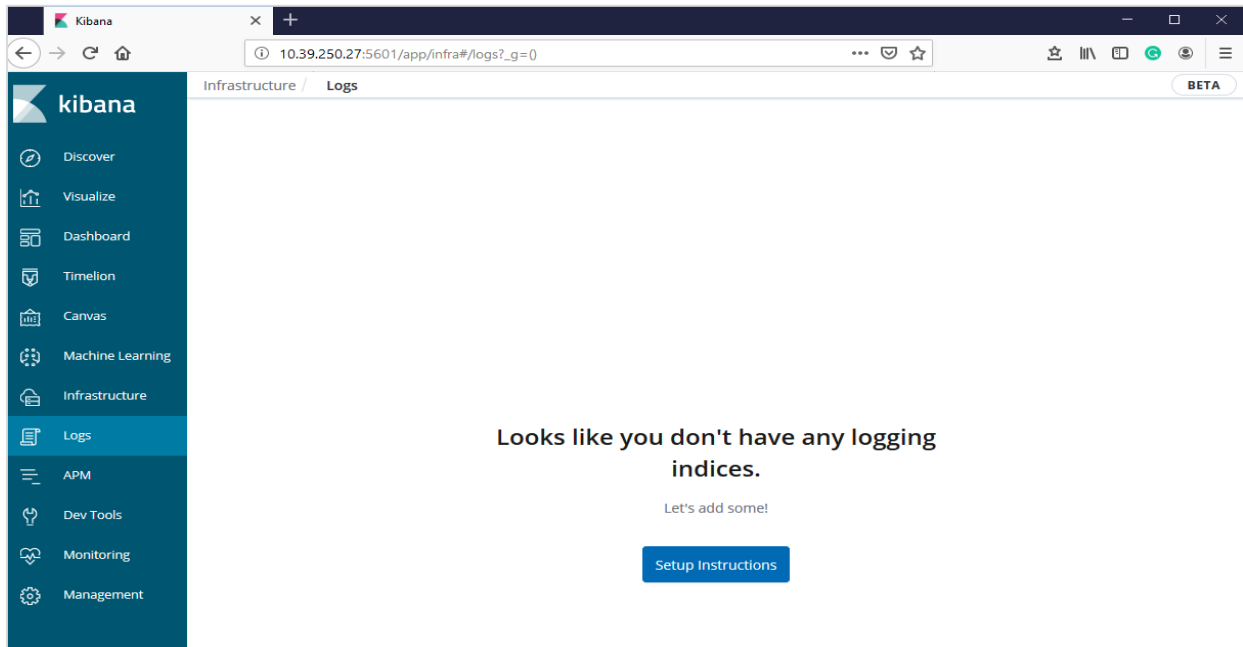
Select bank* to create gauge visualization for sample account data.



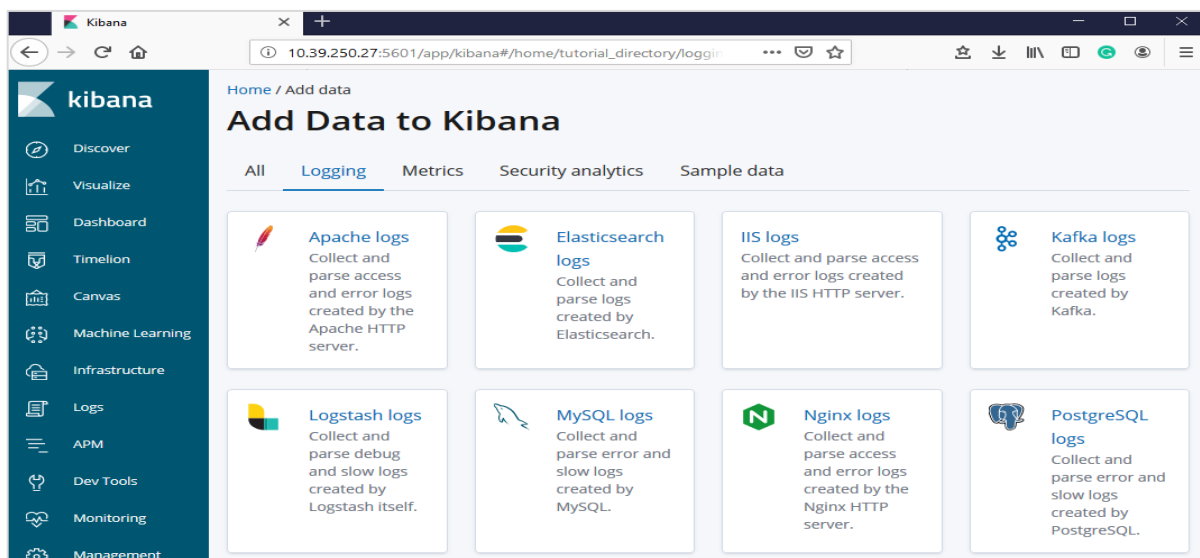
Gauge visualization is created for sample account data successfully.

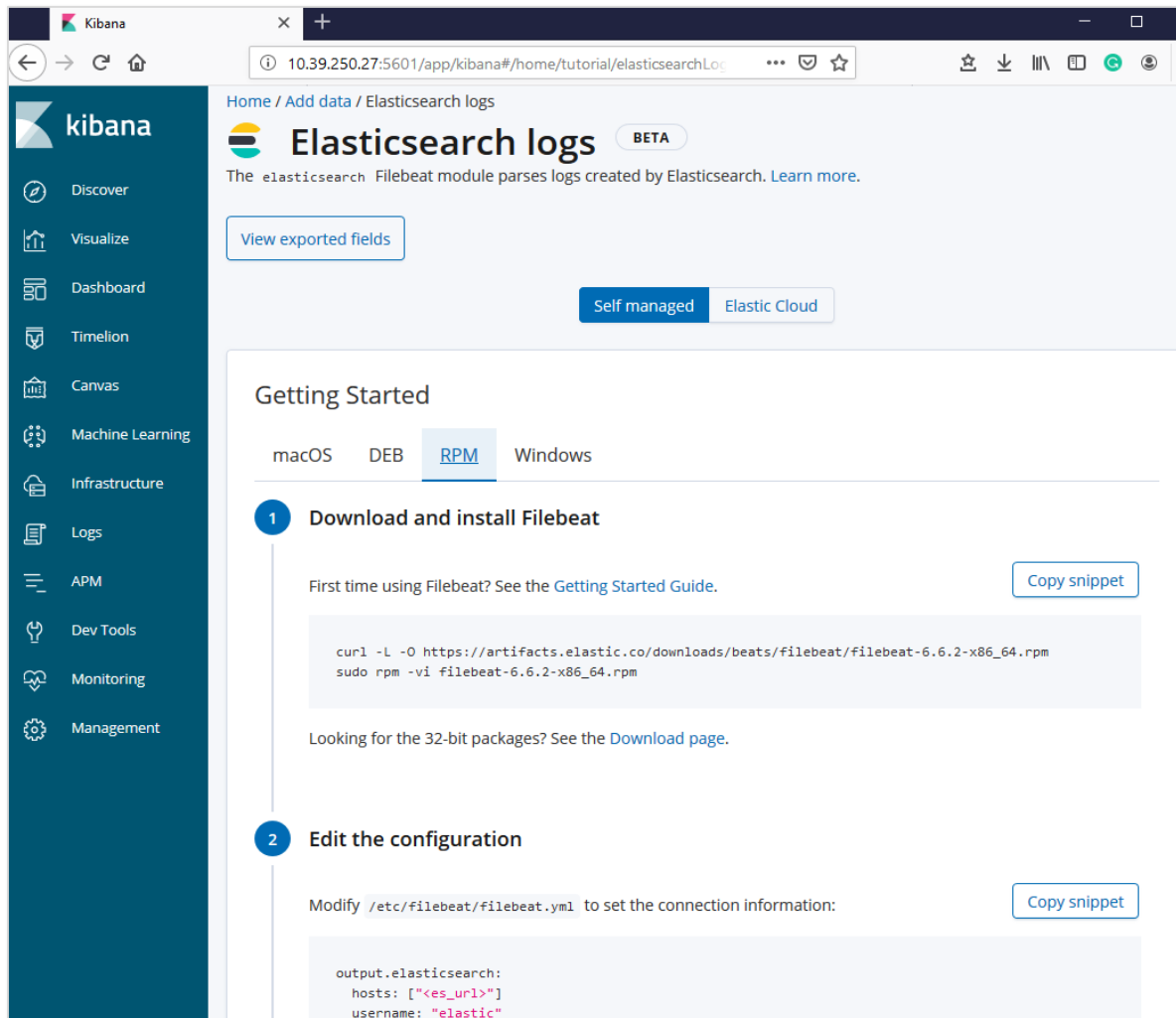
3 COLLECTING ELASTICSEARCH LOGS USING FILEBEAT

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.

3.1 Installing and setting up Filebeat

Go to the Elasticsearch master node for installing Filebeat.

```
ssh -i <your pem keypair> bluedata@<ip_address>
```

```
[root@yav-344 ~]# ssh -i KeyPairs/4.pem bluedata@10.39.250.30
Warning: Permanently added '10.39.250.30' (ECDSA) to the list of known hosts.
Last login: Tue Jul  2 21:08:33 2019
[bluedata@bluedata-7226 ~]$ ls
vagent.bin
[bluedata@bluedata-7226 ~]$
```

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
```

```
[bluedata@bluedata-7226 ~]$ sudo curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-6.6.2-x86_64.rpm
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 11.2M  100 11.2M    0     0  9.7M      0  0:00:01  0:00:01 --:--:--  9.7M
[bluedata@bluedata-7226 ~]$ sudo rpm -vi filebeat-6.6.2-x86_64.rpm
warning: filebeat-6.6.2-x86_64.rpm: Header V4 RSA/SHA512 Signature, key ID d88e42b4: NOKEY
Preparing packages...
filebeat-6.6.2-1.x86_64
```

Execute the following command to install Filebeat.

```
sudo rpm -vi filebeat-6.6.2-x86_64.rpm
```

```
[bluedata@bluedata-7226 ~]$ sudo rpm -vi filebeat-6.6.2-x86_64.rpm
warning: filebeat-6.6.2-x86_64.rpm: Header V4 RSA/SHA512 Signature, key ID d88e42b4: NOKEY
Preparing packages...
filebeat-6.6.2-1.x86_64
[bluedata@bluedata-7226 ~]$ ls
filebeat-6.6.2-x86_64.rpm  vagent.bin
[bluedata@bluedata-7226 ~]$
```

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

```
sudo vi /etc/filebeat/filebeat.yml
```

```
[bluedata@bluedata-7226 ~]$
[bluedata@bluedata-7226 ~]$ sudo vi /etc/filebeat/filebeat.yml
[bluedata@bluedata-7226 ~]$
```

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

```
##### Kibana #####
# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:

# Kibana Host
# Scheme and port can be left out and will be set to the default (http and 5601)
# In case you specify and additional path, the scheme is required: http://localhost:5601/path
# IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
host: "10.39.250.27:5601"

##### Outputs #####
# Configure what output to use when sending the data collected by the beat.

#----- Elasticsearch output -----
output.elasticsearch:
# Array of hosts to connect to.
hosts: ["10.39.250.28:9200", "10.39.250.30:9200"]
```

Execute the following command to enable Elasticsearch module:

```
sudo filebeat modules enable elasticsearch
```

```
[bluedata@bluedata-7226 ~]$  
[bluedata@bluedata-7226 ~]$ sudo filebeat modules enable elasticsearch
```

Execute the following command to setup Filebeat:

```
sudo filebeat setup
```

```
[bluedata@bluedata-7226 ~]$ sudo filebeat setup  
Loaded index template  
Loading dashboards (Kibana must be running and reachable)  
Loaded dashboards  
Loaded machine learning job configurations
```

Execute the following command to start Filebeat:

```
sudo service filebeat start
```

```
[bluedata@bluedata-7226 ~]$ sudo service filebeat start  
Starting filebeat (via systemctl): [ OK ]
```

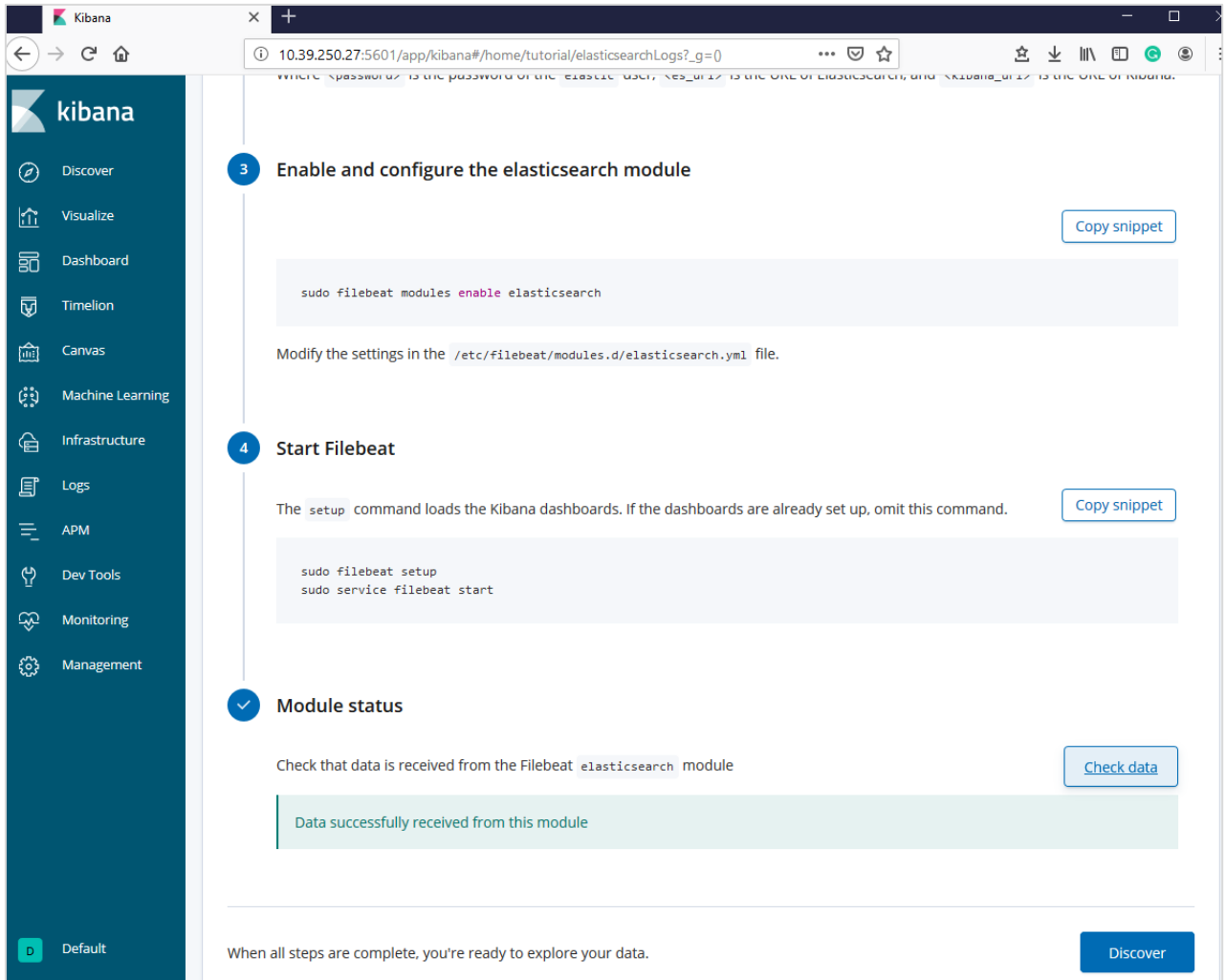
Execute the following command to check the status for Filebeat:

```
sudo service filebeat status
```

```
[bluedata@bluedata-7226 ~]$ sudo service filebeat status  
• filebeat.service - Filebeat sends log files to Logstash or directly to Elasticsearch.  
  Loaded: loaded (/usr/lib/systemd/system/filebeat.service; disabled; vendor preset: disabled)  
  Active: active (running) since Wed 2019-07-03 00:11:45 PDT; 6s ago  
    Docs: https://www.elastic.co/products/beats/filebeat  
 Main PID: 6454 (filebeat)  
   CGroup: /system.slice/docker-9e820cb4973efa20401fe07af732867bc2bdc72ae7d145686d759dda7f985477.scope/system.slice/filebeat.service  
           └─6454 /usr/share/filebeat/bin/filebeat -c /etc/filebeat/filebeat.yml -path.home /usr/share/filebeat -path.config /etc/...  
  
Jul 03 00:11:45 bluedata-7226.bdlocal systemd[1]: Started Filebeat sends log files to Logstash or directly to Elasticsearch..  
Jul 03 00:11:45 bluedata-7226.bdlocal systemd[1]: Starting Filebeat sends log files to Logstash or directly to Elasticsearch...  
[bluedata@bluedata-7226 ~]$
```

3.2 Collecting Elasticsearch logs in Kibana UI

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



Kibana

10.39.250.27:5601/app/kibana#/home/tutorial/elasticsearchLogs?_g=()

3 Enable and configure the elasticsearch module

Copy snippet

```
sudo filebeat modules enable elasticsearch
```

Modify the settings in the `/etc/filebeat/modules.d/elasticsearch.yml` file.

4 Start Filebeat

The `setup` command loads the Kibana dashboards. If the dashboards are already set up, omit this command.

Copy snippet

```
sudo filebeat setup
sudo service filebeat start
```

Module status

Check that data is received from the Filebeat `elasticsearch` module

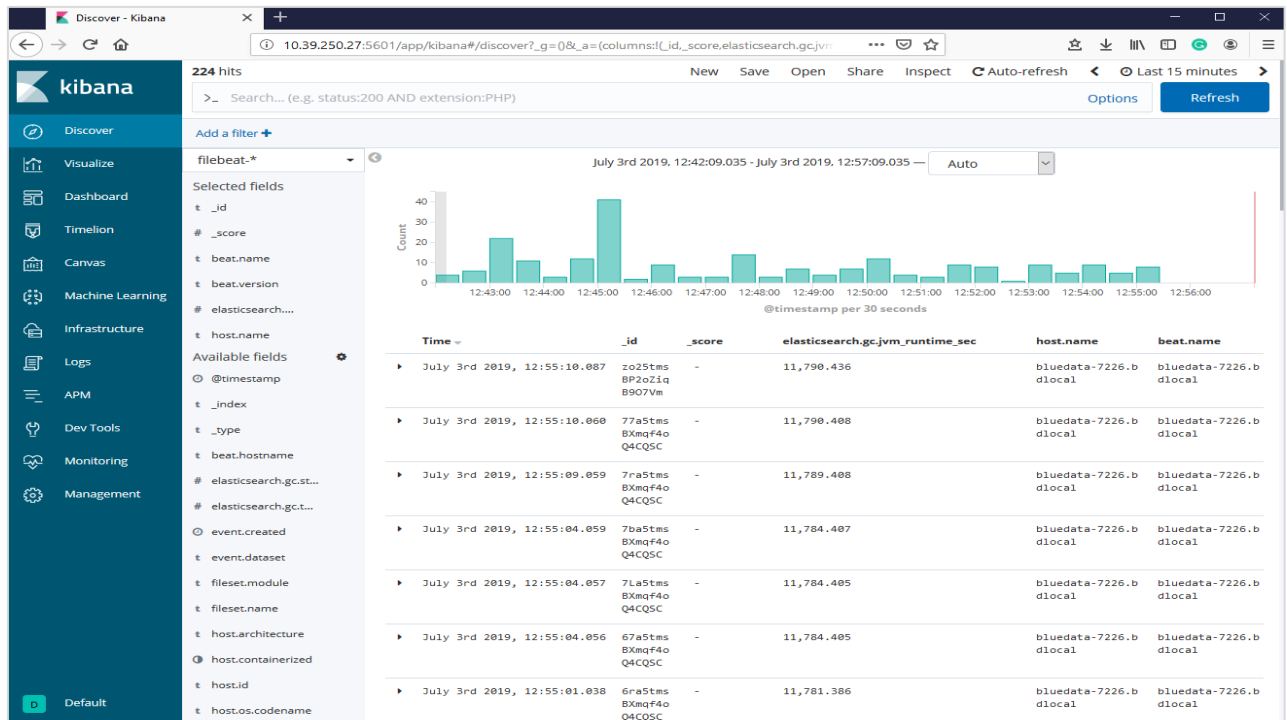
Check data

Data successfully received from this module

When all steps are complete, you're ready to explore your data.

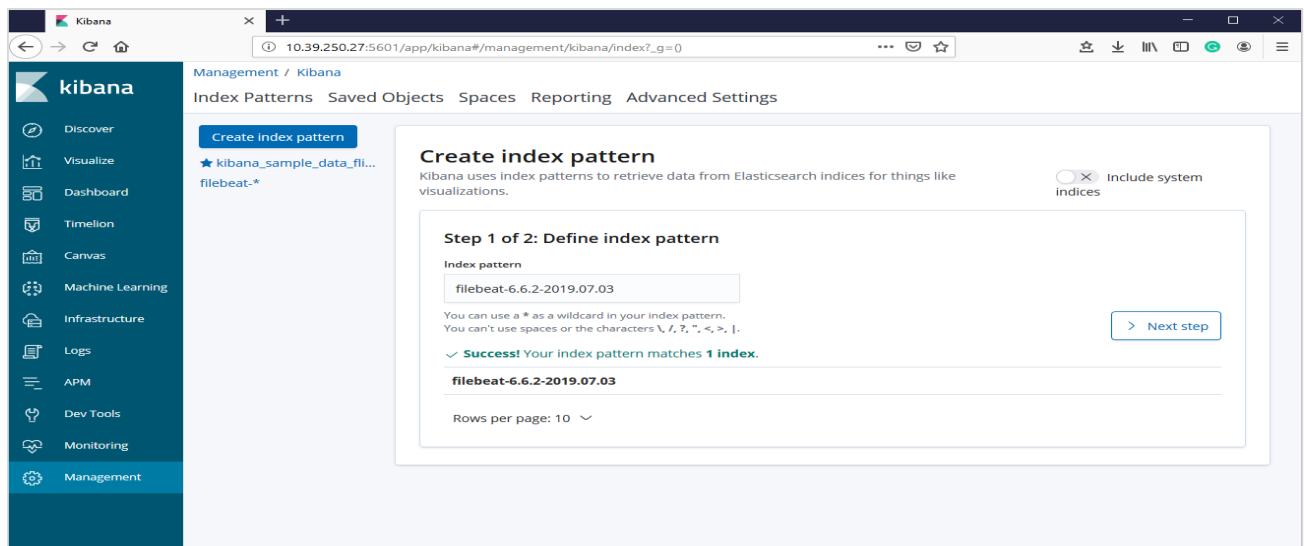
Discover

Click on Discover to explore your Elasticsearch log data.



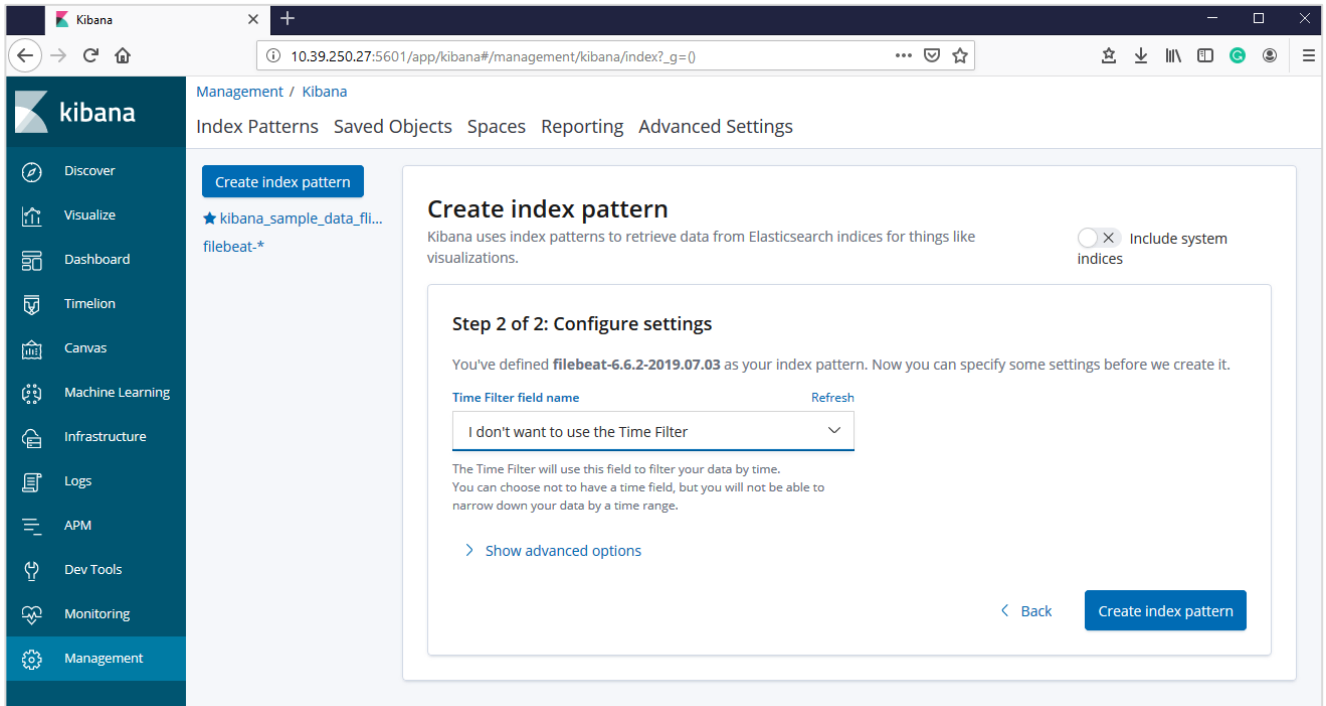
3.3 Create Index patterns name for Elasticsearch logs data

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

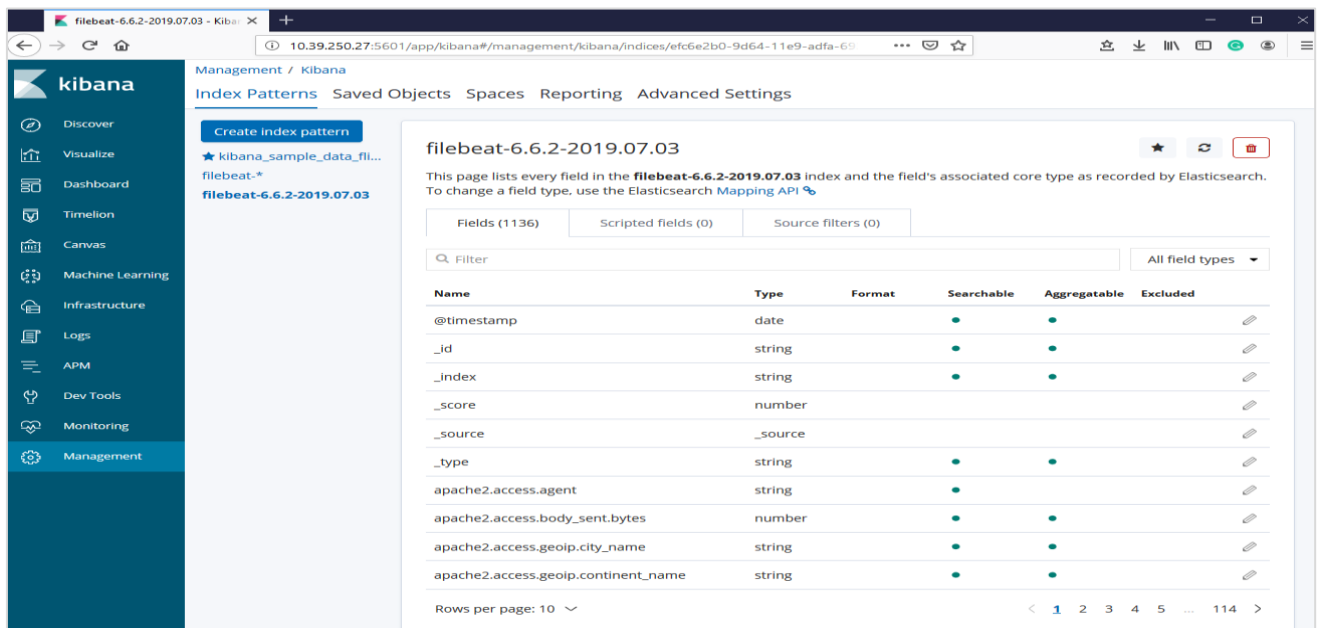


The screenshot shows the Kibana Management interface. The left sidebar contains navigation options: Discover, Visualize, Dashboard, Timelion, Canvas, Machine Learning, Infrastructure, Logs, APM, Dev Tools, Monitoring, and Management. The main view displays the 'Create index pattern' dialog. The dialog has a title 'Create index pattern' and a description 'Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.' There is a checkbox 'Include system indices' which is currently unchecked. The 'Index pattern' field contains 'filebeat-6.6.2-2019.07.03'. Below the field, there is a success message: 'Success! Your index pattern matches 1 index.' and the index pattern 'filebeat-6.6.2-2019.07.03' is displayed. The 'Rows per page' is set to 10.

Define index pattern then click on Next step.



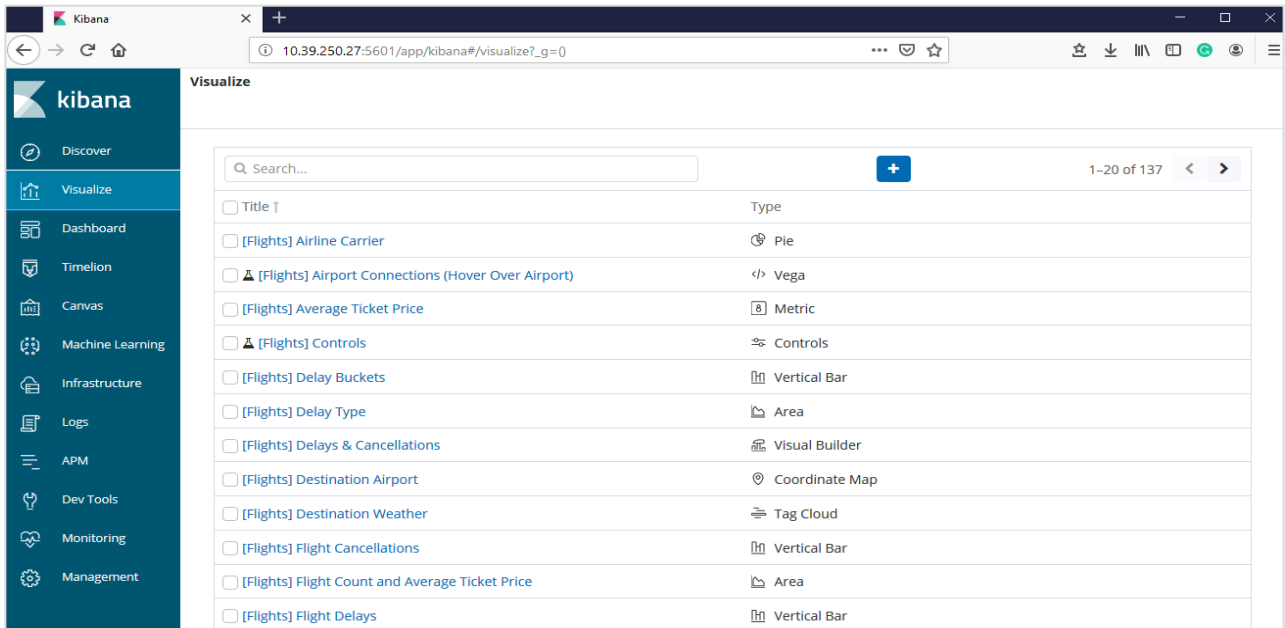
Click on Create index pattern to define time filter field name for your index pattern



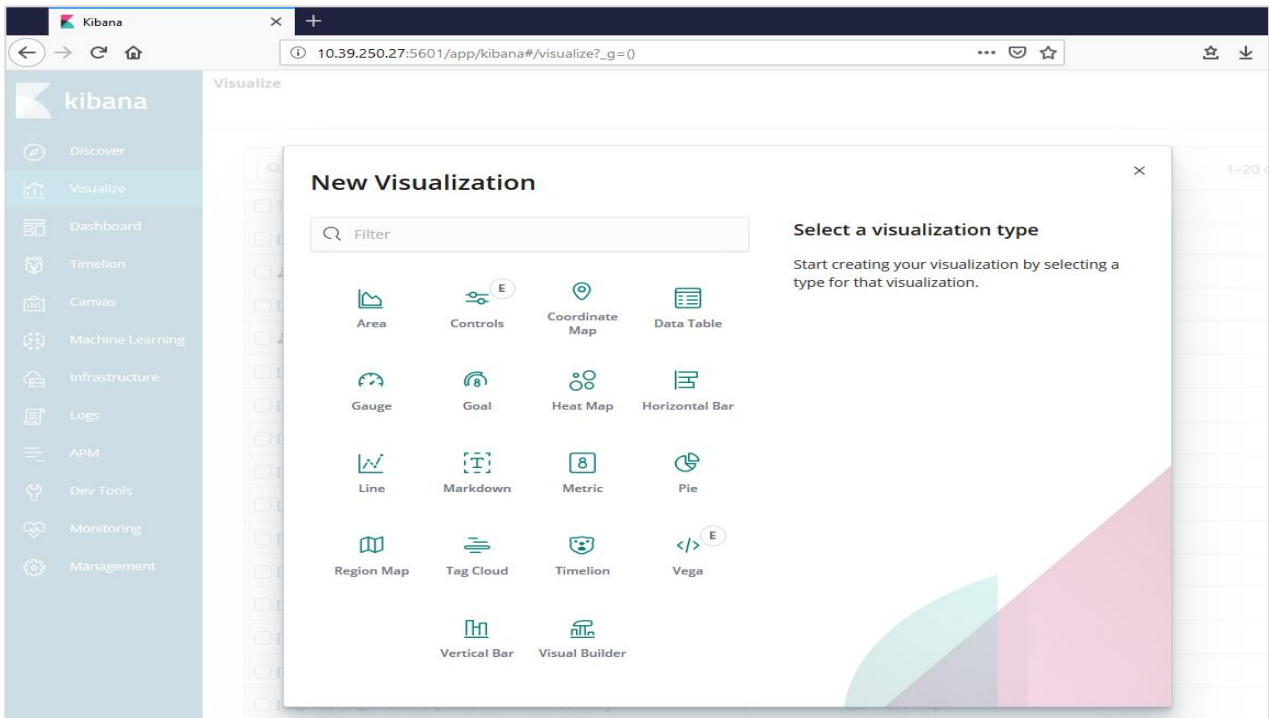
New index pattern is created successfully.

3.4 Create visualization type for Elasticsearch logs data

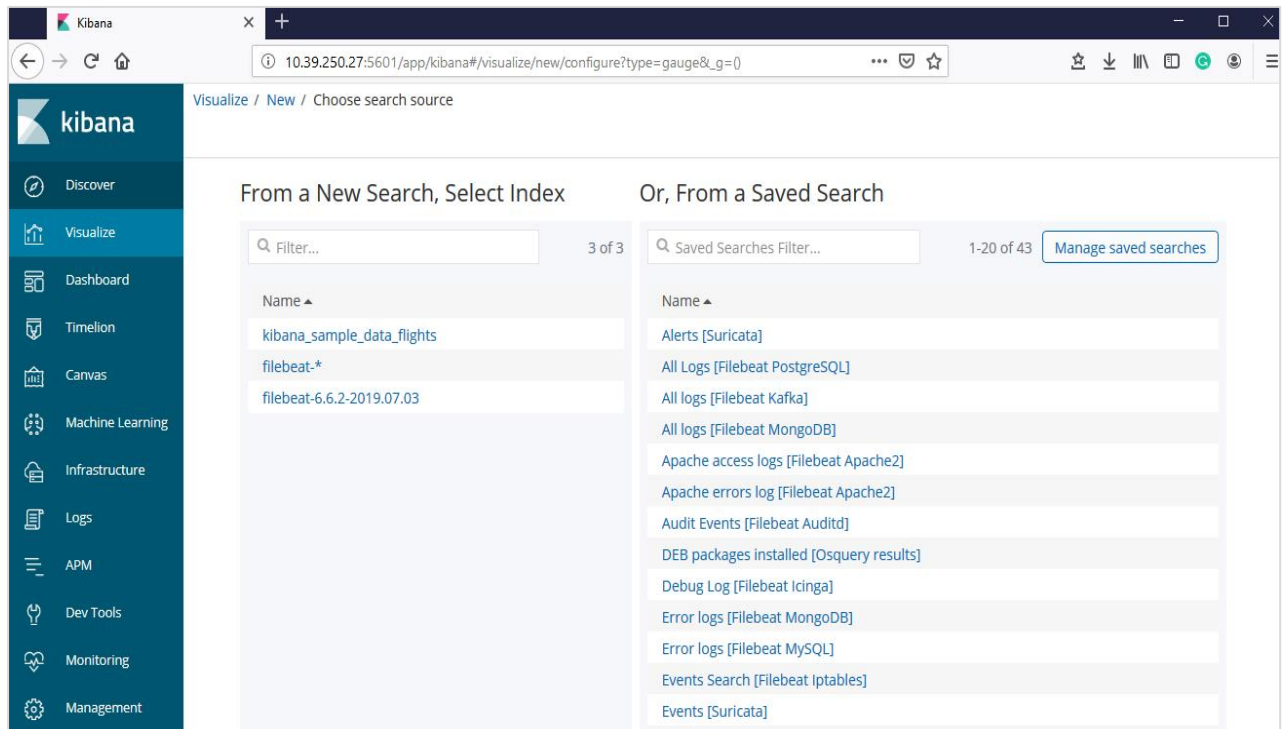
Click on Visualize section on Kibana UI.



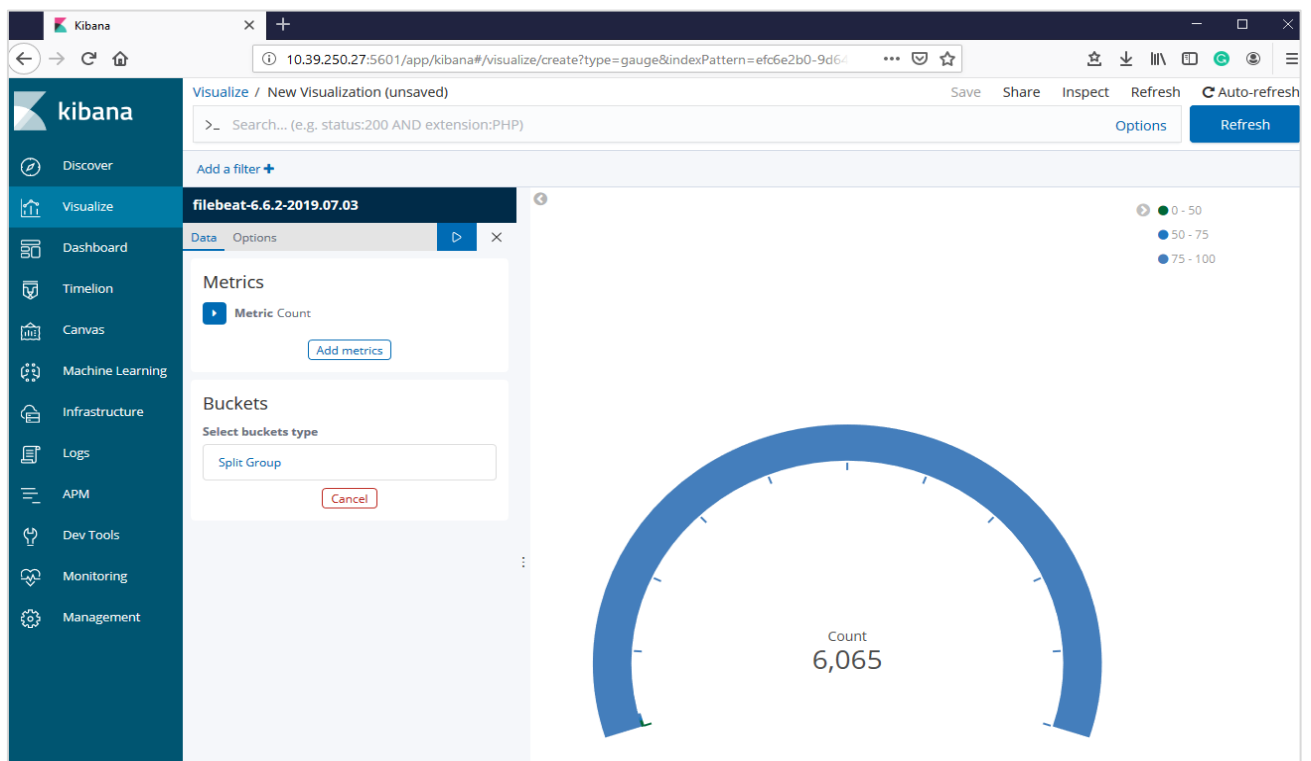
Click on + sign to create new visualization type for Elasticsearch logs data.



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.

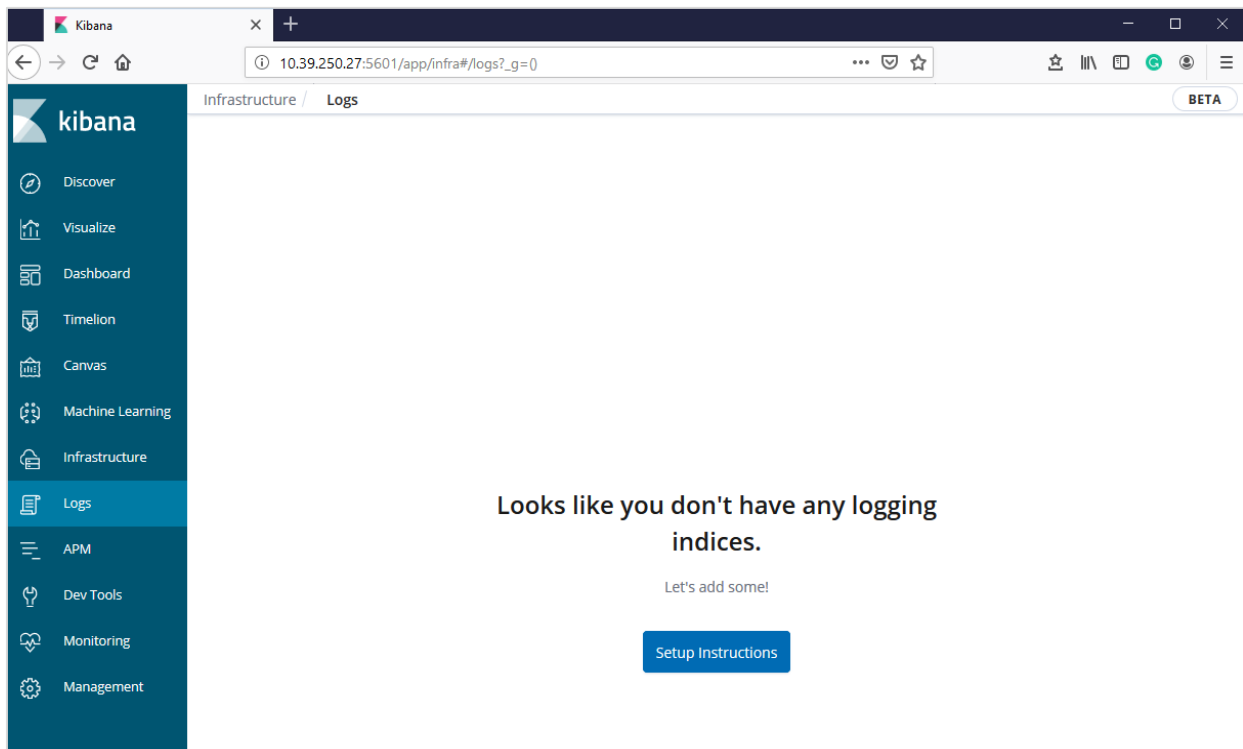


Gauge visualization is created for Elasticsearch logs data successfully.

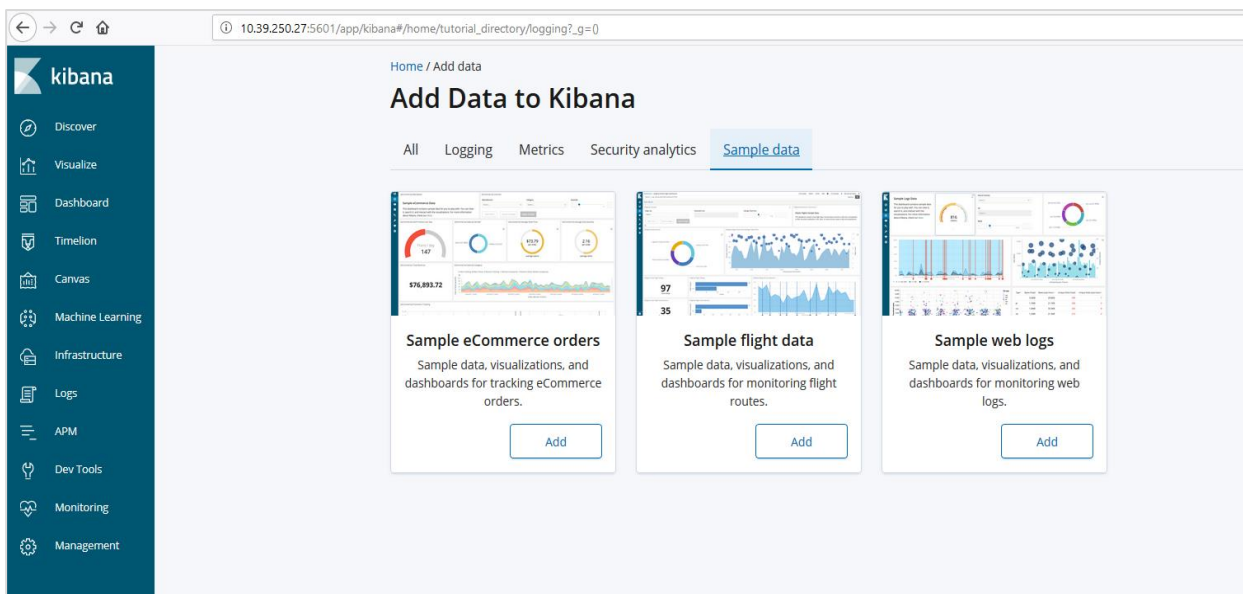
4 TESTING ELK STACK WITH SAMPLE FLIGHT DATASET

4.1 Add sample flight data to Kibana

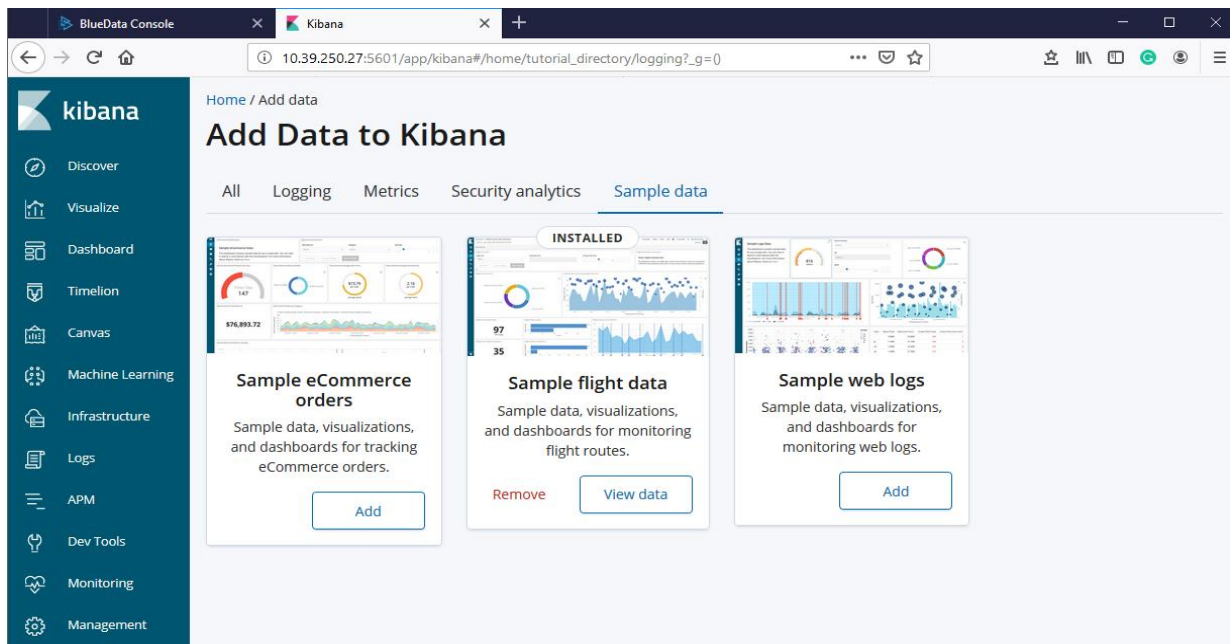
We will use Kibana UI to add sample flights dataset and test the ELK stack.



Click on Add to install sample flight data in Kibana.

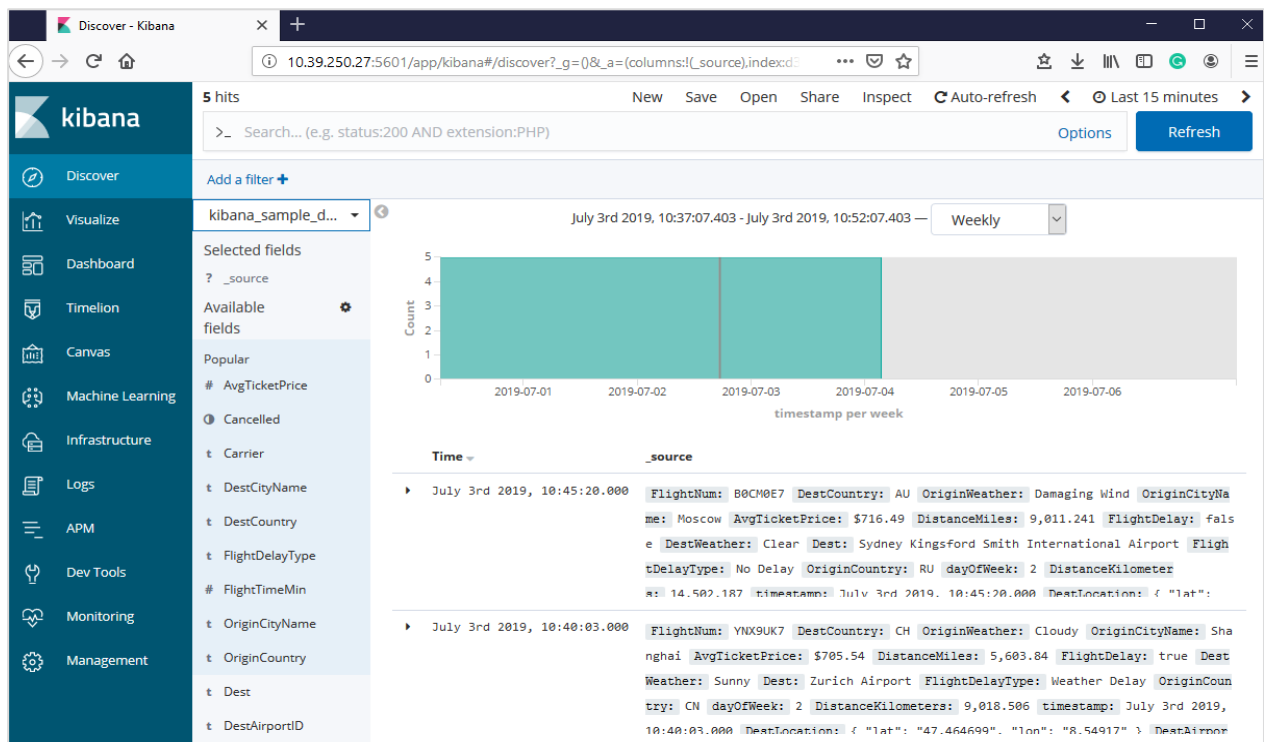


Click on View data to check the data in sample flight data and you can also remove sample flight data anytime from Kibana.



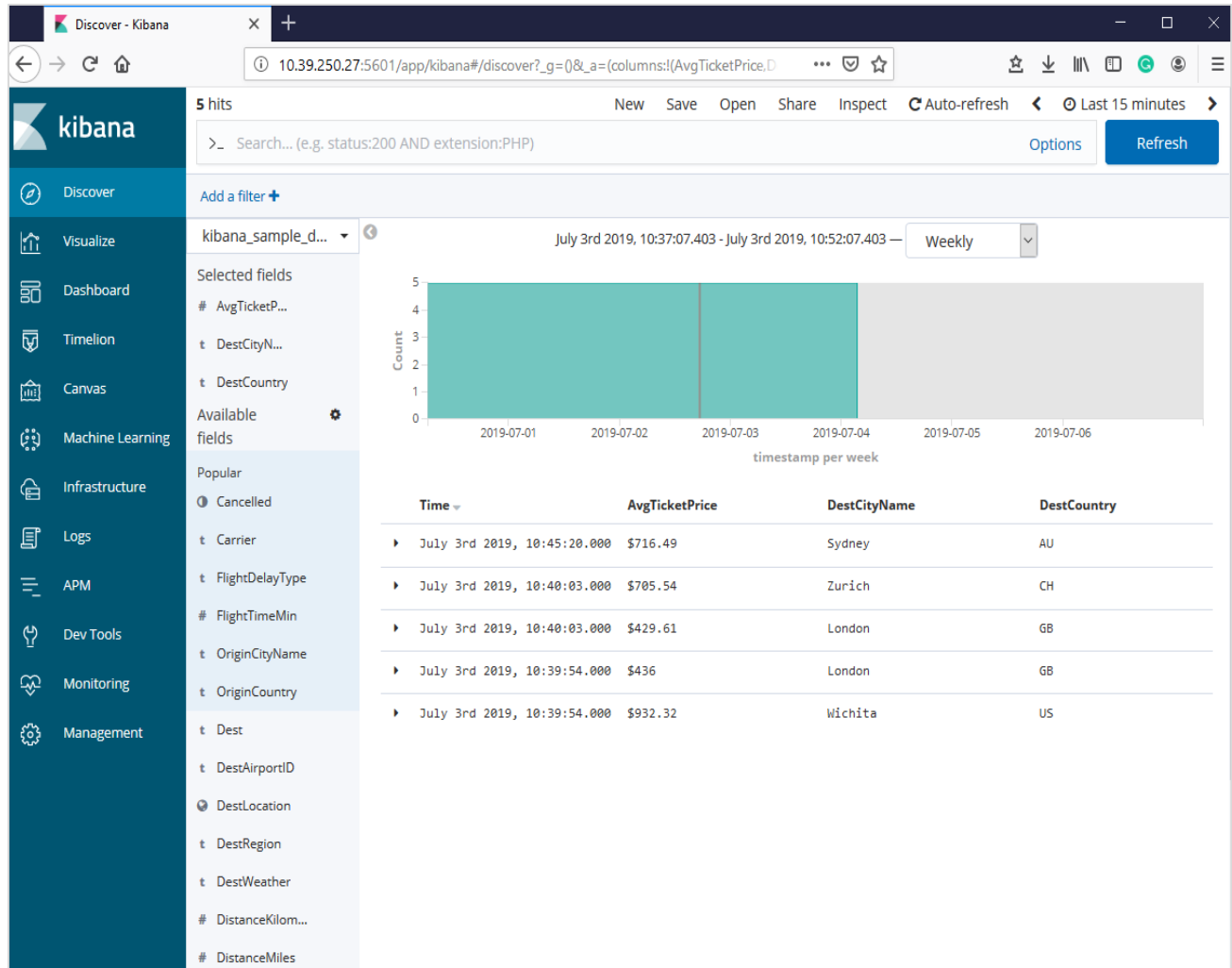
4.2 Discover the sample flight dataset

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.

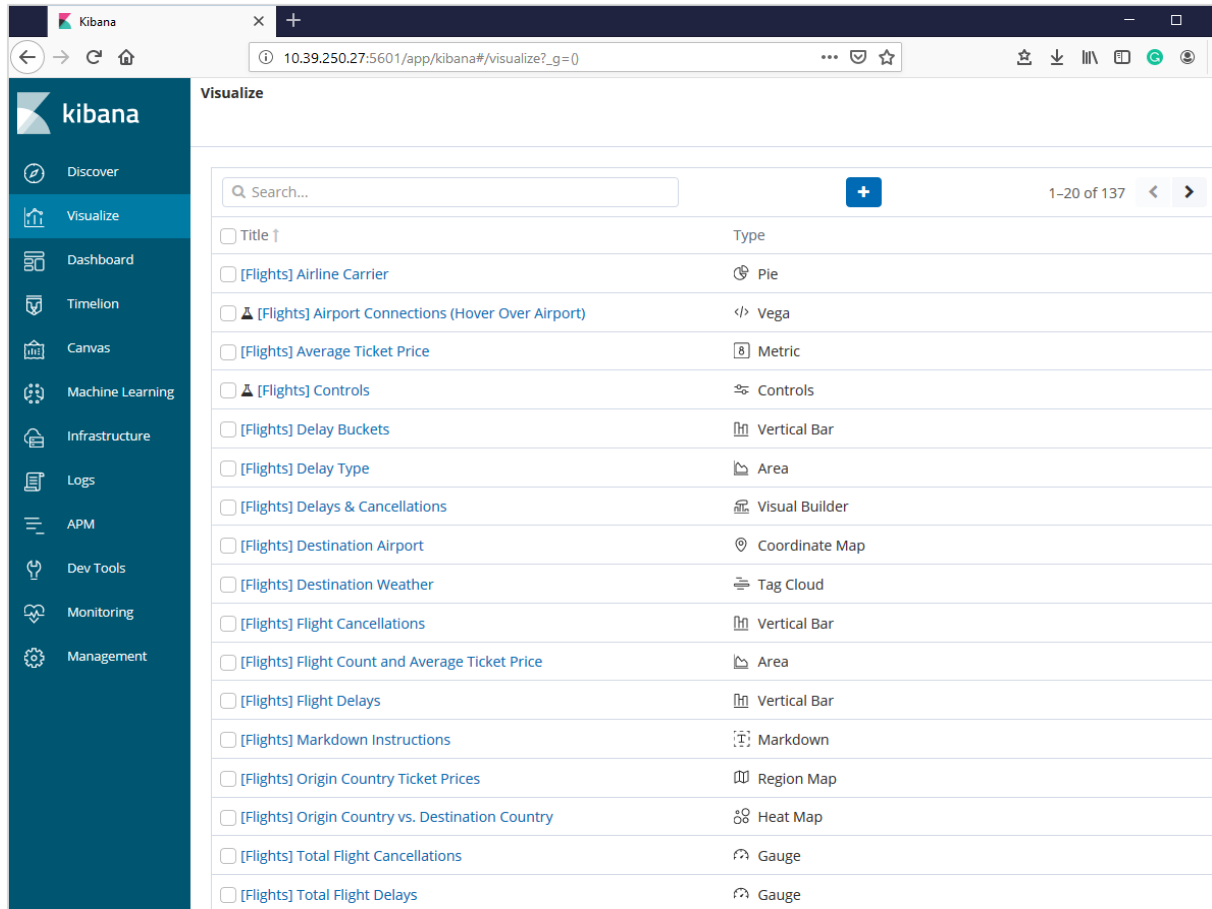
Let's select some of the field, which is available.



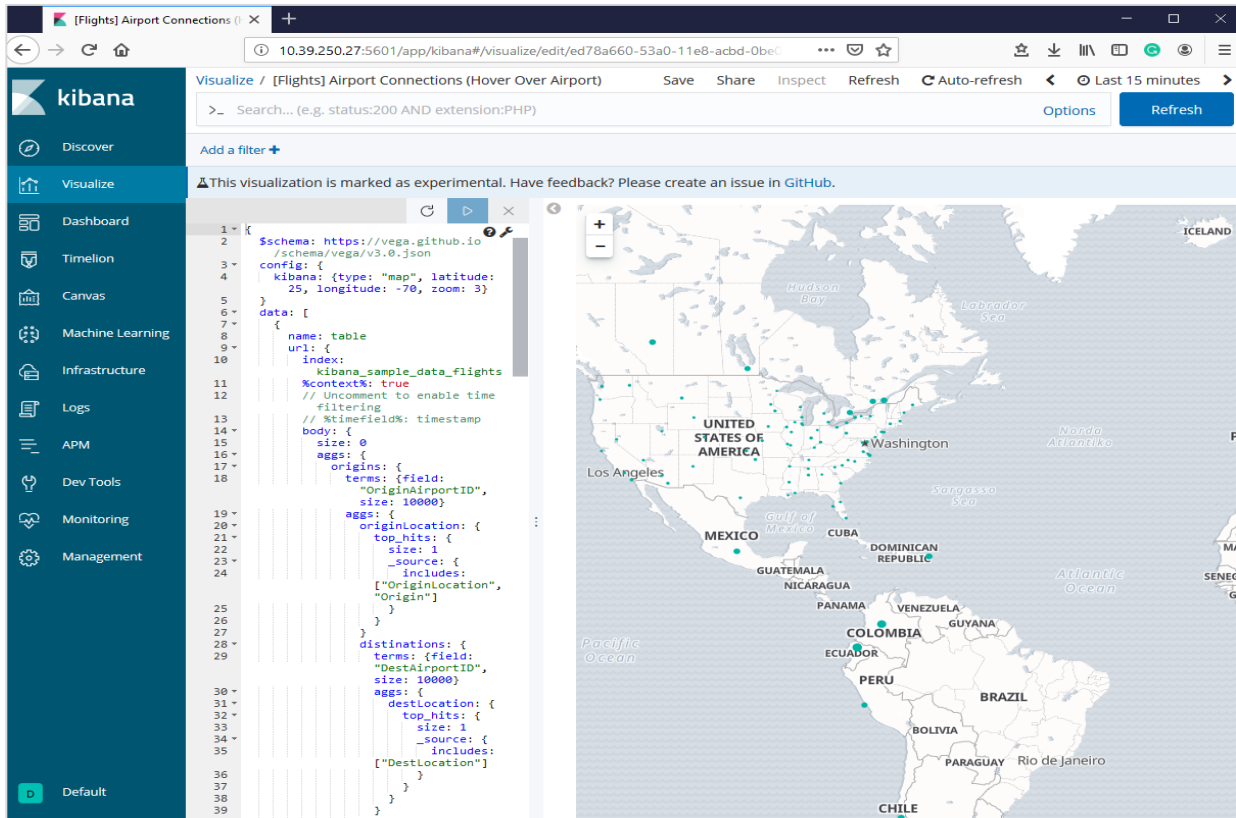
Here selected fields are avgticketprice, destcityname and destcountry. You can see the filtered output based on the fields you selected.

4.3 Visualize the sample flight dataset

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



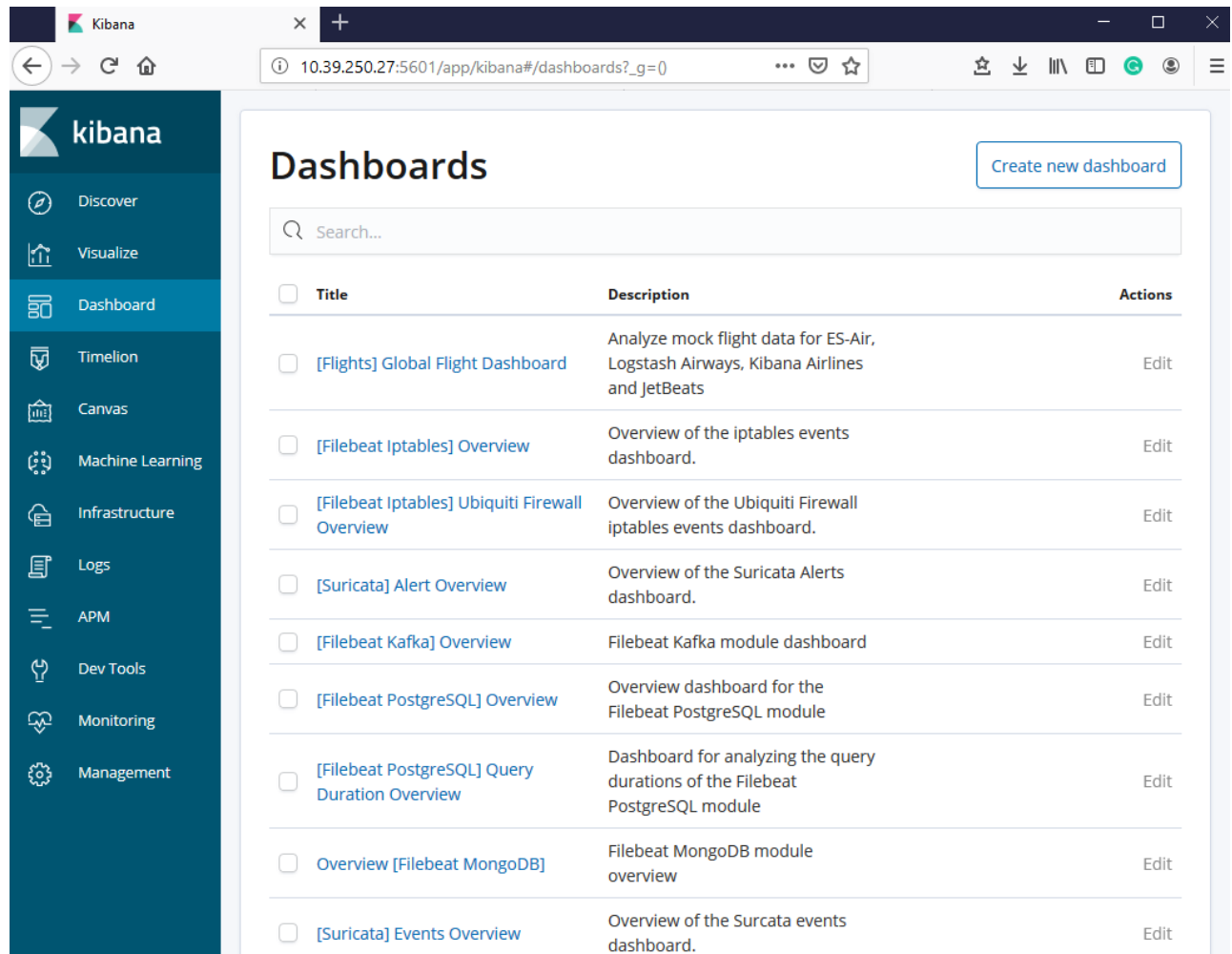
Here you can see the visualization type available for sample flight dataset. Select any visualization type to explore the sample flights dataset.



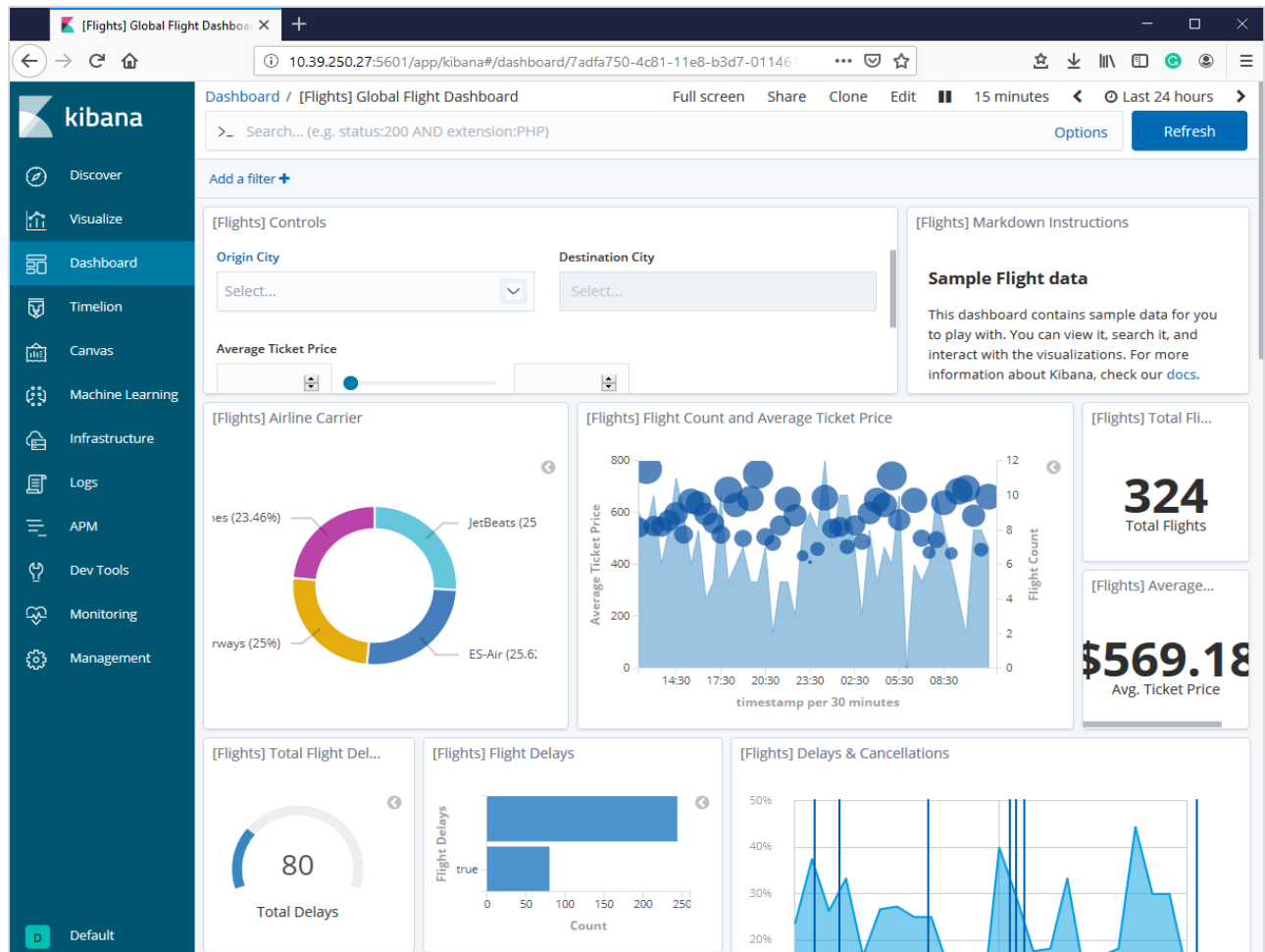
Here we have selected the [Flights] Airport Connections (Hover Over Airport) visualization, which has Vega visualization type. When you will do hover over airport you will see how many connections that airport has.

4.4 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.

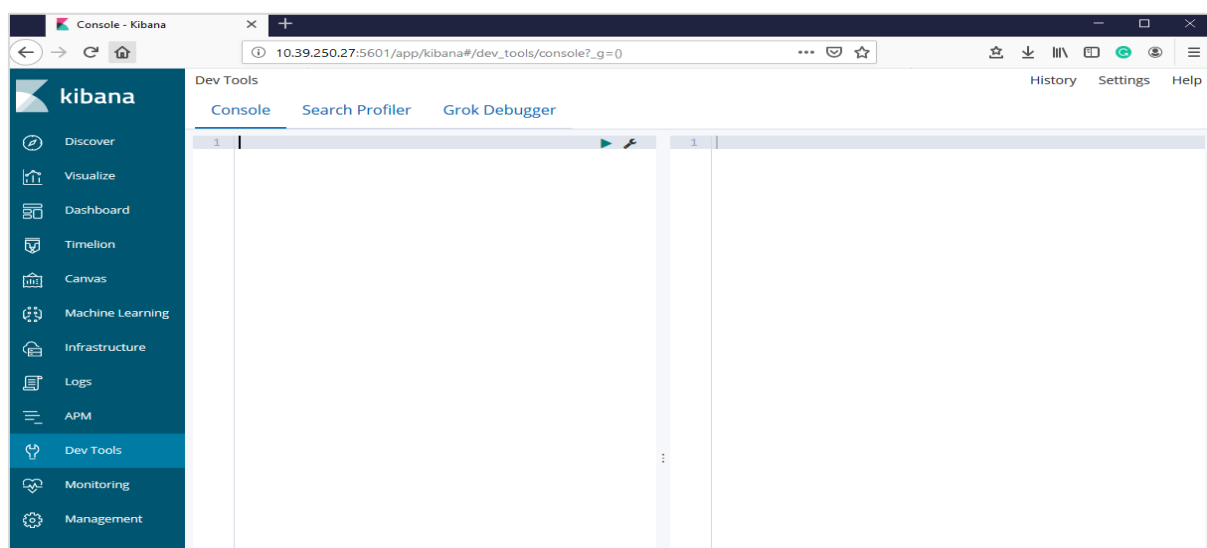


Click on Global Flight Dashboard to explore dashboard for sample flight dataset.



4.5 Test REST API from Dev Tools

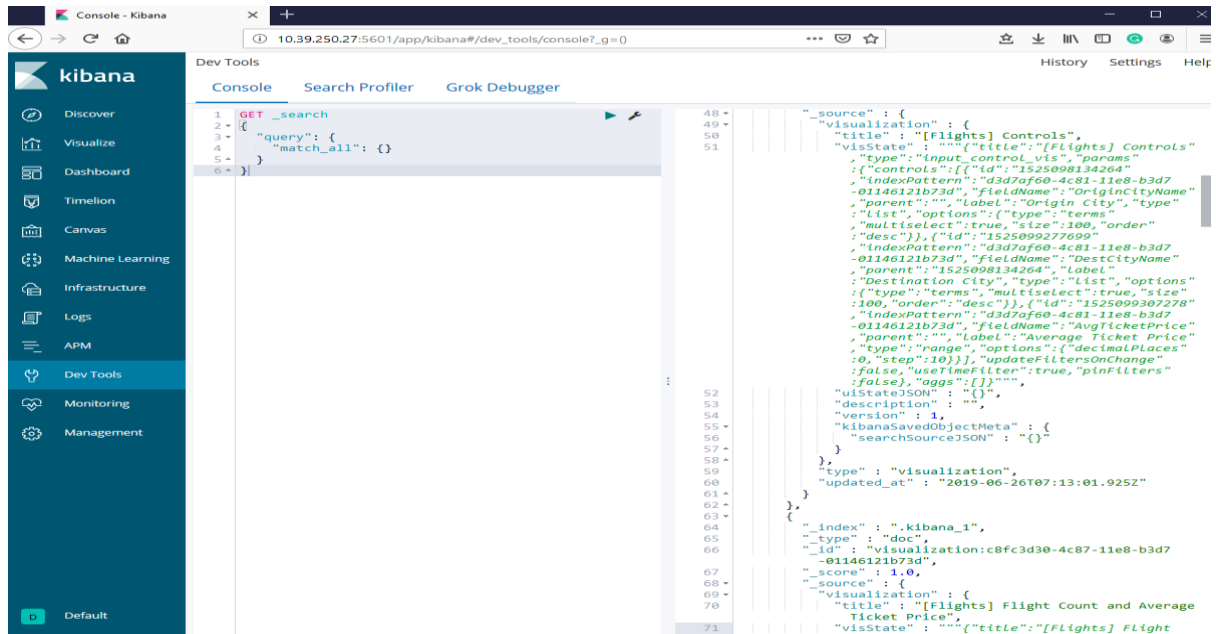
Click on Dev Tools in Kibana UI.



Note: Here you can run your REST API commands.

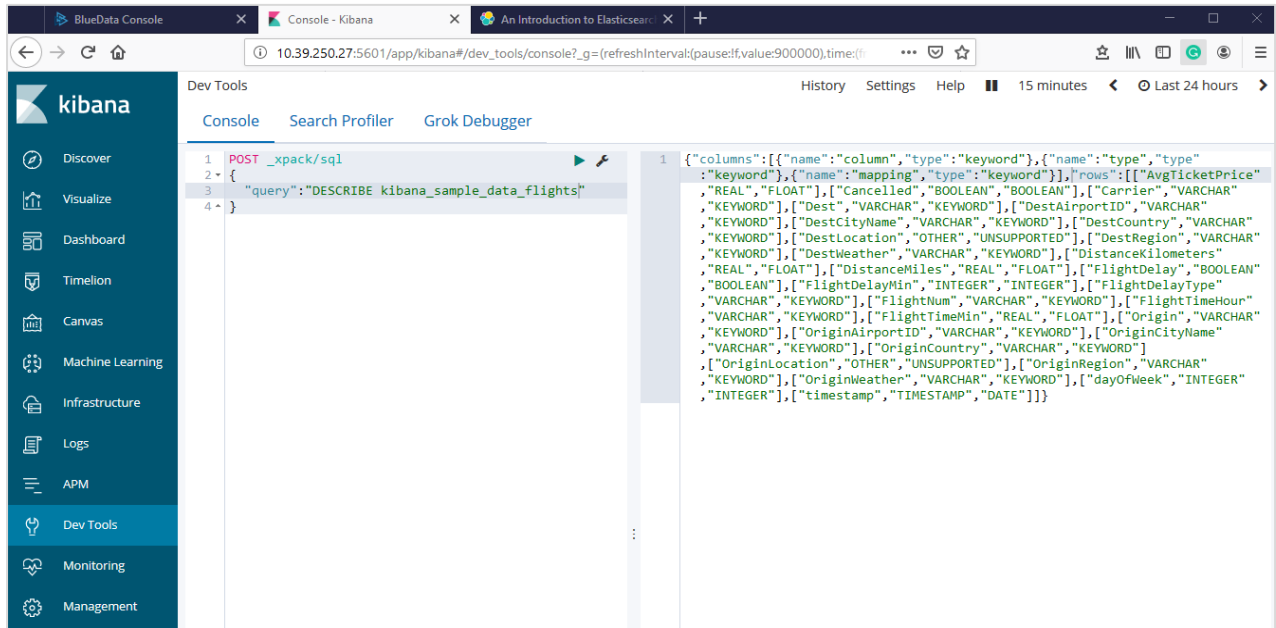
Use following REST command to check whether Sample flight data added to Kibana.

```
GET _search
{
  "query": {
    "match_all": {}
  }
}
```



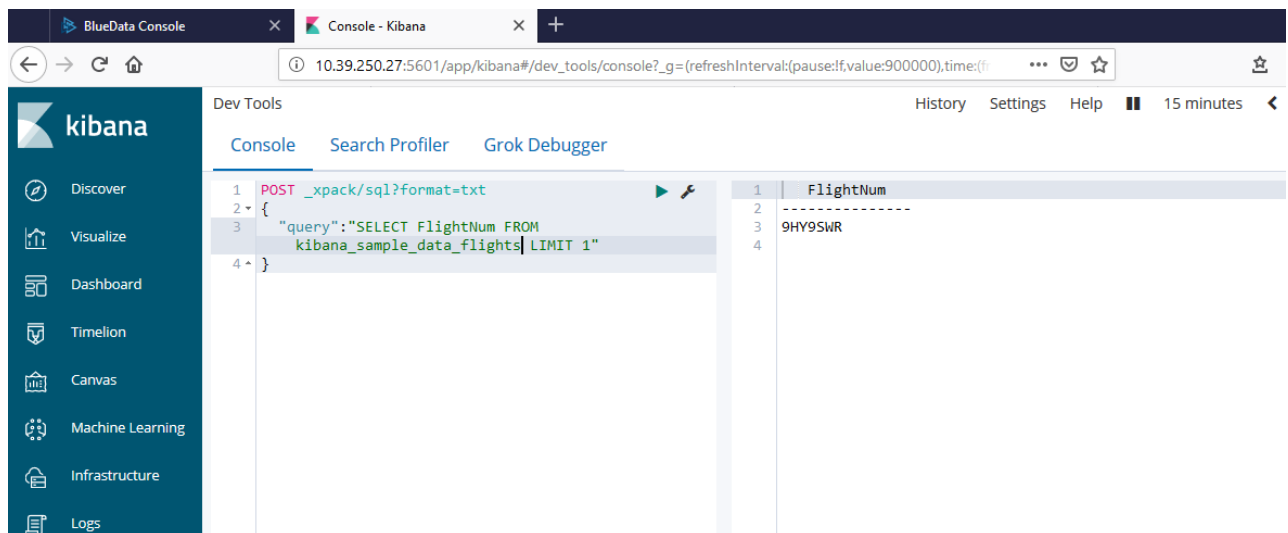
Use the following command to describe what is inside the sample flight dataset.

```
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"
}
```



4.6 Testing SQL CLI for ELK

Go inside the container where Elasticsearch is installed.

```
ssh -i <your pem keypair> bluedata@<ip_address>
```

```
[root@yav-344 ~]#  
[root@yav-344 ~]# ssh -i KeyPairs/4.pem bluedata@10.39.250.30  
Warning: Permanently added '10.39.250.30' (ECDSA) to the list of known hosts.  
Last login: Sun Jun 30 22:15:07 2019  
[bluedata@bluedata-7226 ~]$  
[bluedata@bluedata-7226 ~]$
```

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

```
bluedata@bluedata-7226:/usr/share/elasticsearch  
[bluedata@bluedata-7226 elasticsearch]$  
[bluedata@bluedata-7226 elasticsearch]$ ls bin/  
elasticsearch          elasticsearch-keystore          elasticsearch-sql-cli          x-pack-env  
elasticsearch-certgen  elasticsearch-migrate           elasticsearch-sql-cli-6.6.2.jar x-pack-env.bat  
elasticsearch-certgen.bat elasticsearch-migrate.bat       elasticsearch-sql-cli.bat     x-pack-security-env  
elasticsearch-certutil  elasticsearch-plugin            elasticsearch-syskeygen       x-pack-security-env.bat  
elasticsearch-certutil.bat elasticsearch-saml-metadata     elasticsearch-syskeygen.bat   x-pack-watcher-env  
elasticsearch-cli        elasticsearch-saml-metadata.bat elasticsearch-translog        x-pack-watcher-env.bat  
elasticsearch-croneval  elasticsearch-setup-passwords  elasticsearch-users  
elasticsearch-croneval.bat elasticsearch-setup-passwords.bat elasticsearch-users.bat  
elasticsearch-env       elasticsearch-shard             x-pack  
[bluedata@bluedata-7226 elasticsearch]$
```

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
```

```
[bluedata@bluedata-7226 elasticsearch]$  
[bluedata@bluedata-7226 elasticsearch]$ sudo ./bin/elasticsearch-sql-cli http://10.39.250.28:9200
```

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

bluedata@bluedata-7226:/usr/share/elasticsearch

```

      asticElasticE
      ElasticE   sticEla
      sticEl  ticEl      Elast
      lasti Elast
      cEl      ast      tic
      icE      as      cEl
      icE      as      cEl
      icEla    las      El
      sticElasticElast      icElas
      las      last      ticElast
      El      asti      asti      stic
      El      asticEla      Elas      icE
      El      Elas cElasticE ticEl      cE
      Ela      ticEl      ticElasti      cE
      las      astic      last      icE
      sticElas      asti      stic
      icEl      sticElasticElast
      icE      sticE      ticEla
      icE      sti      cEla
      icEl      sti      Ela
      cEl      sti      cEl
      Ela      astic      ticE
      asti      ElasticElasti
      ticElasti lasticElas
      ElasticElast

      SQL
      6.6.2

sql>

```

Execute the following command to check which tables are available

```

sql>
|
| show tables;
      name      |      type
-----+-----
.kibana          |ALIAS
.kibana_1        |BASE TABLE
kibana_sample_data_flights|BASE TABLE

```

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

```

sql> SELECT OriginCountry, OriginCityName FROM kibana_sample_data_flights LIMIT 1;
      OriginCountry | OriginCityName
-----+-----
DE                  |Frankfurt am Main

```