SMOKE TEST

ELK 6.6.2

Date Prepared: July 2019

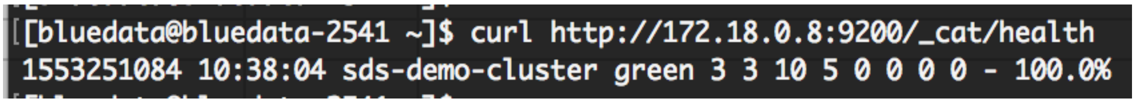
Document Information

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

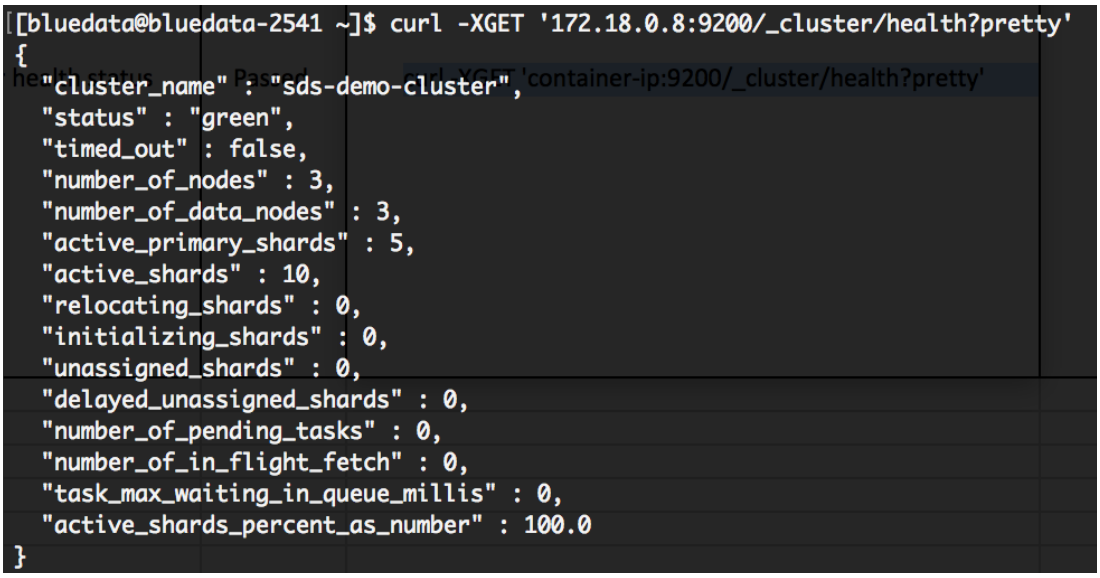
1 INSPECT STATUS OF THE CLUSTER

```
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%
```

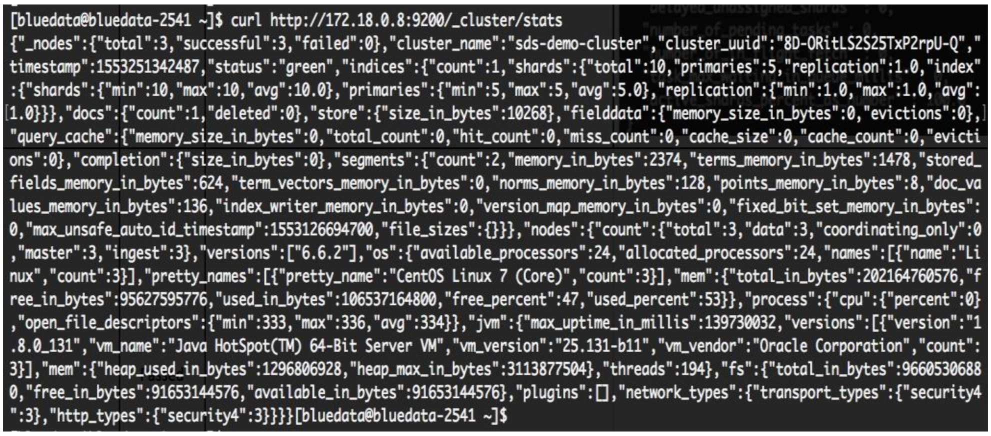
```
curl -XGET '<container-ip>:9200/_cluster/health? pretty'
```



```
[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-ORitLS2S25TxP2rpU-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,"evicti
ons":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_va
lues_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":"Li
nux","count":3}],"pretty_names":[{"pretty_name":"CentOS Linux 7 (Core)","count":3}],"mem":{"total_in_bytes":202164760576,"f
ree_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":9660530688
0,"free_in_bytes":91653144576,"available_in_bytes":91653144576},"plugins":[],"network_types":{"transport_types":{"security4
":3},"http_types":{"security4":3}}}}[bluedata@bluedata-2541 ~]$
```

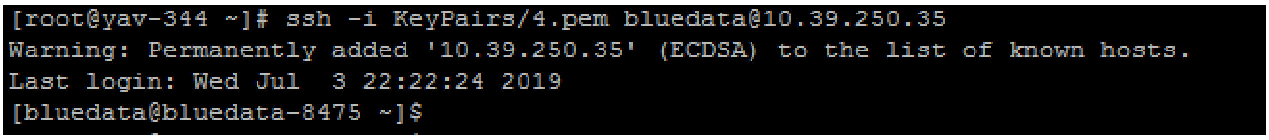
2 LOADING SAMPLE DATA AND VISUALIZING THE DATA IN KIBANA

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.

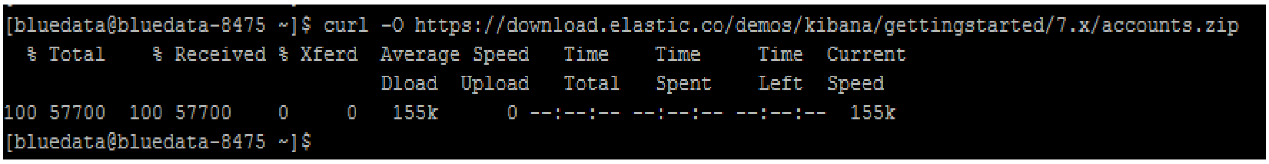
```
ssh -i <your pem keypair> bluedata@<ip_address>
```



```
[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:

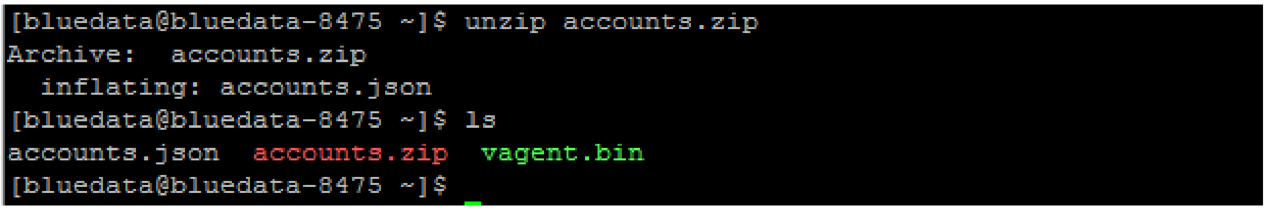
```
curl -O
https://download.elastic.co/demos/kibana/gettingstarted/7.x/accounts.zip
```



```
[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 --:--:-- --:--:-- --:--:--  155k
[bluedata@bluedata-8475 ~]$
```

Execute the following command to unzip the sample account dataset:

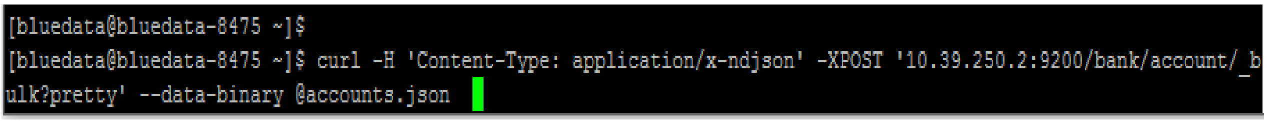
```
unzip accounts.zip
```



```
[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 ~]$
```

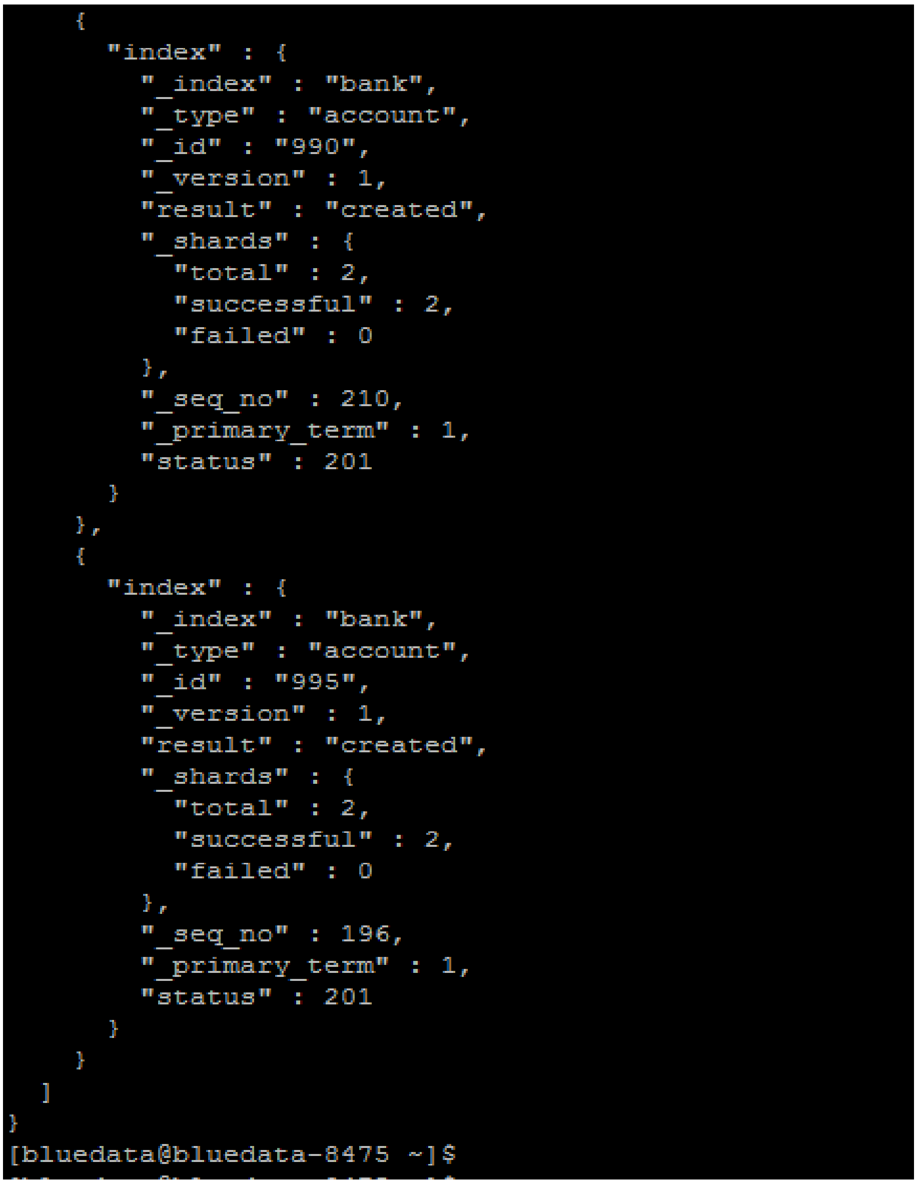
Execute the following command to load the sample data into Elasticsearch data host

```
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
```

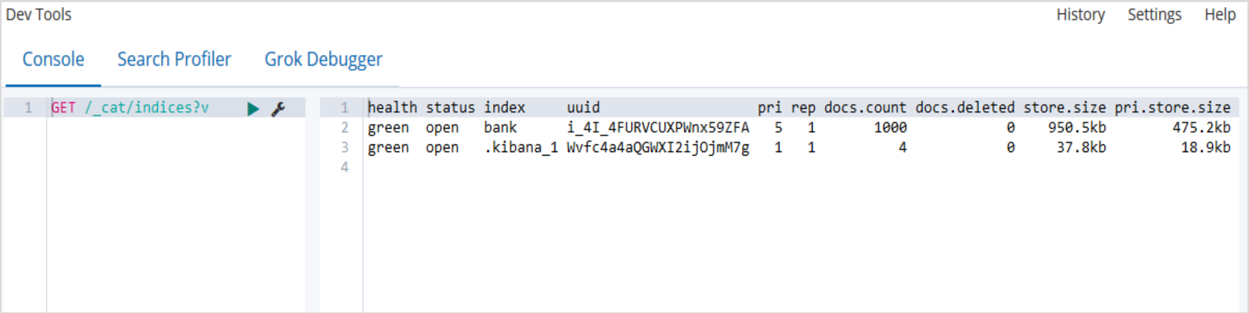
It will take some time to load the sample account data into Elasticsearch data host. You will see the result as given below:



```
    {
      "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
```

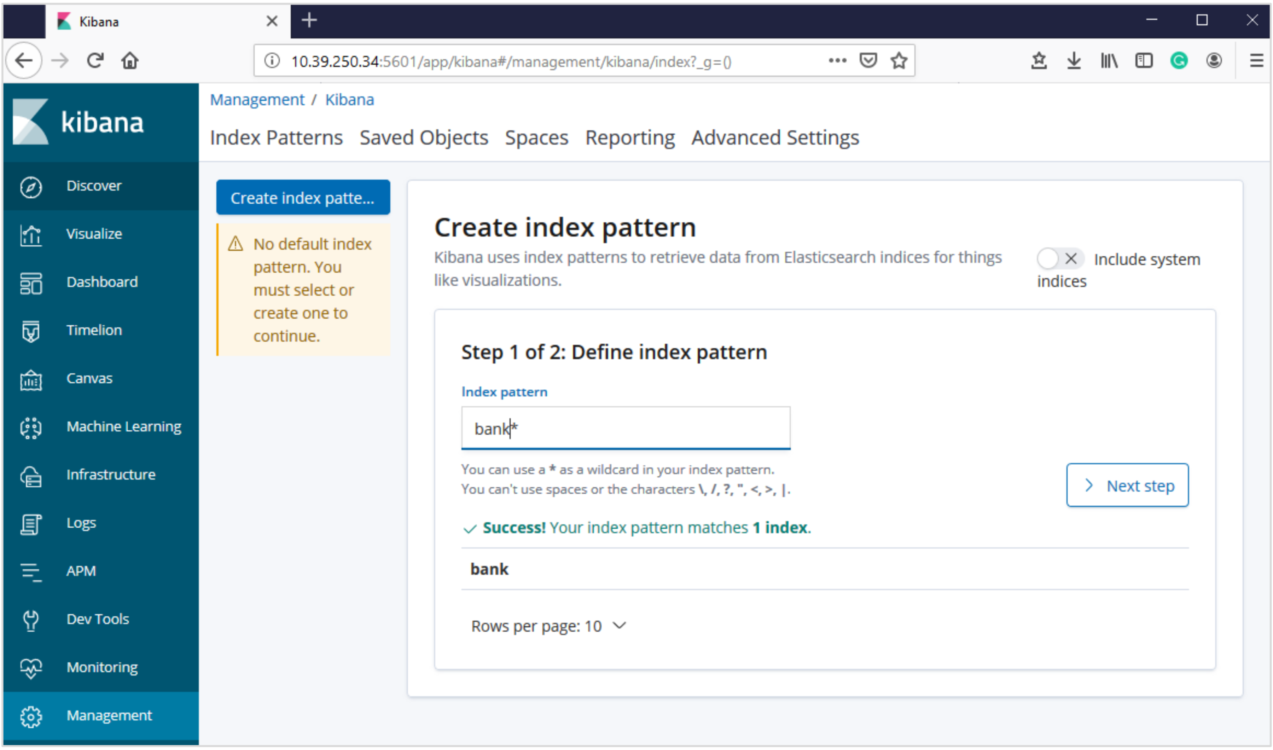


```
GET /_cat/indices?v
```

```
health status index     uuid                   pri rep docs.count docs.deleted store.size pri.store.size
green  open   bank      i_4I_4FURVCUXPWnx59ZFA   5   1       1000            0    950.5kb        475.2kb
green  open   .kibana_1 Wvfc4a4aQGWXI2ijOjmM7g   1   1          4            0     37.8kb         18.9kb
```

2.1 Create Index Patterns for sample account data

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



No default index pattern. You must select or create one to continue.

Create index pattern

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

Step 1 of 2: Define index pattern

Index pattern: bank*

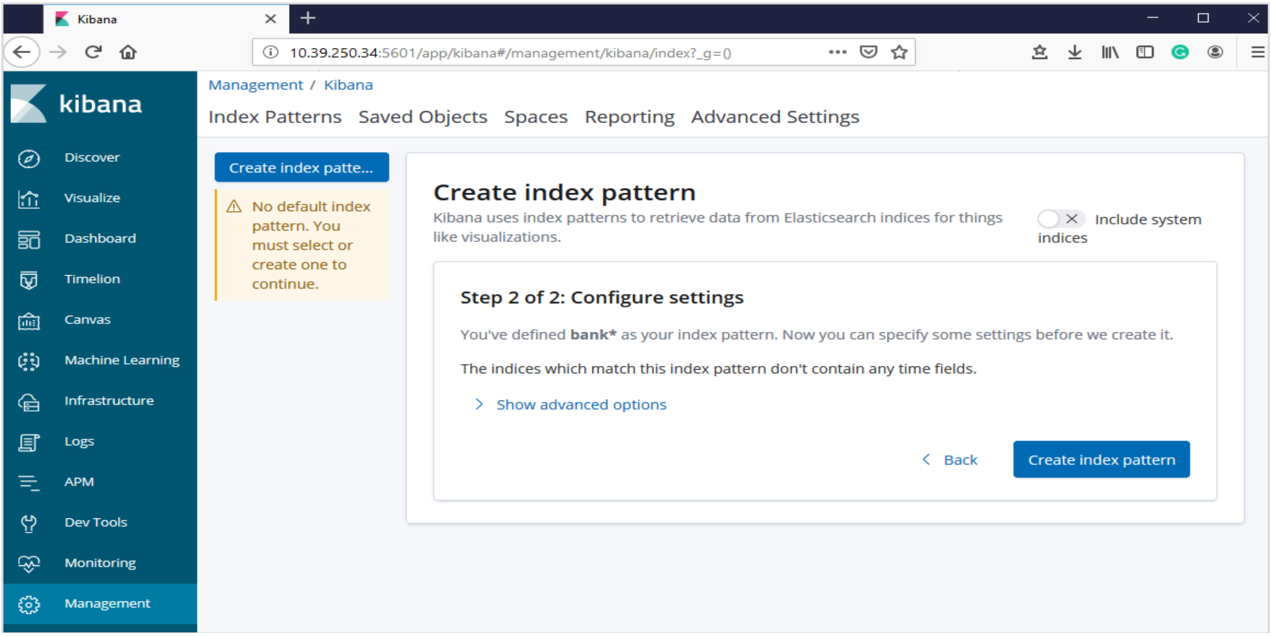
You can use a * as a wildcard in your index pattern.
You can't use spaces or the characters \, /, ?, ", <, >, |.

✓ **Success!** Your index pattern matches **1 index**.

bank

Rows per page: 10

Define index patterns then click on Next step.



No default index pattern. You must select or create one to continue.

Create index pattern

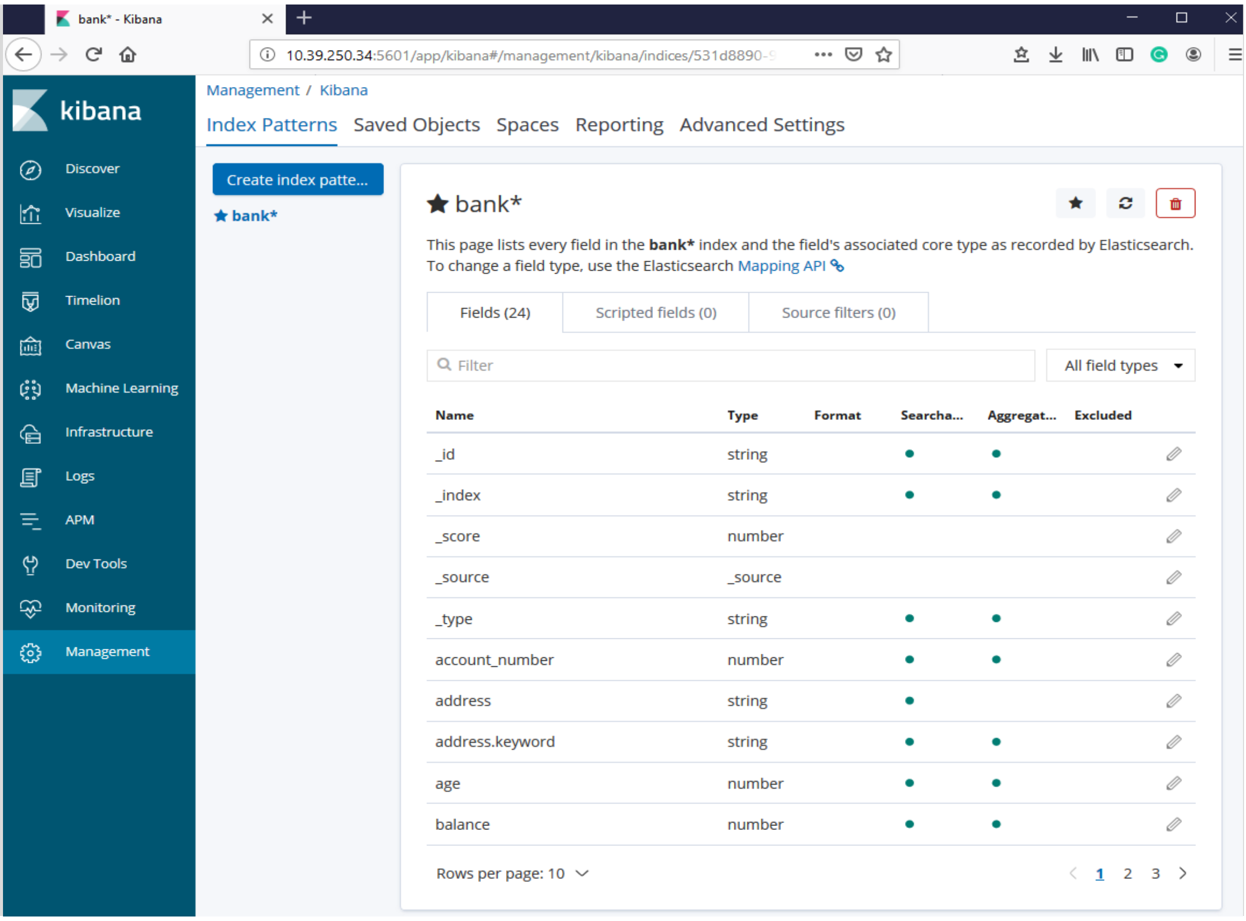
Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.

Step 2 of 2: Configure settings

You've defined **bank*** as your index pattern. Now you can specify some settings before we create it.

The indices which match this index pattern don't contain any time fields.

Click on Create Index Patterns.



★ bank*

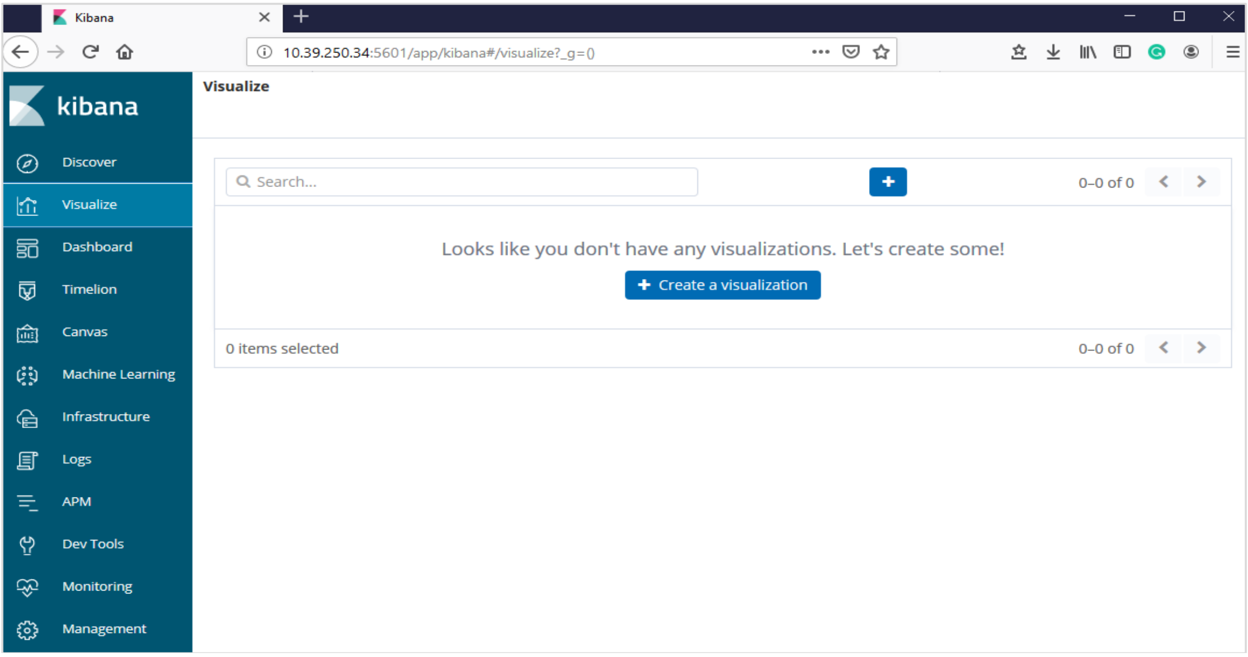
This page lists every field in the **bank*** index and the field's associated core type as recorded by Elasticsearch. To change a field type, use the Elasticsearch Mapping API

Name	Type	Format	Searcha...	Aggregat...	Excluded
_id	string		●	●	
_index	string		●	●	
_score	number				
_source	_source				
_type	string		●	●	
account_number	number		●	●	
address	string		●		
address.keyword	string		●	●	
age	number		●	●	
balance	number		●	●	

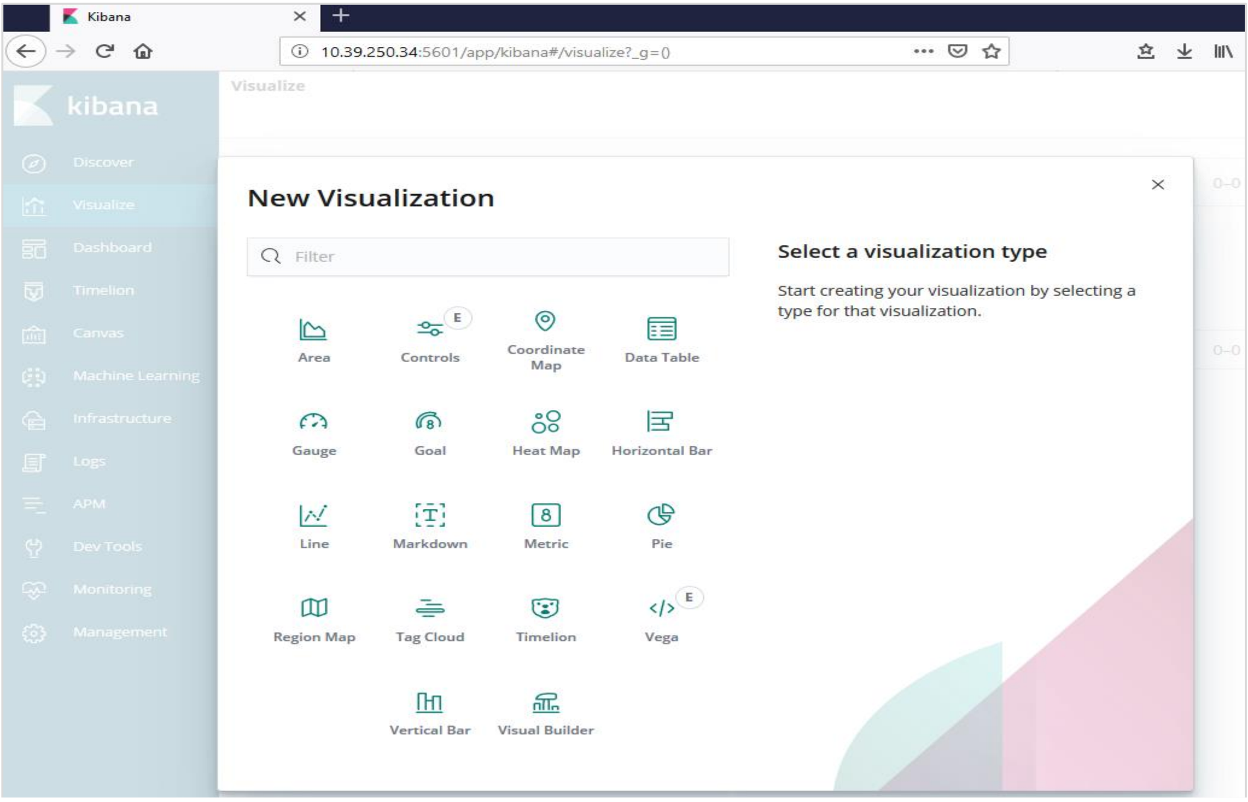
New index pattern is created successfully.

2.2 Create visualization type for sample account data

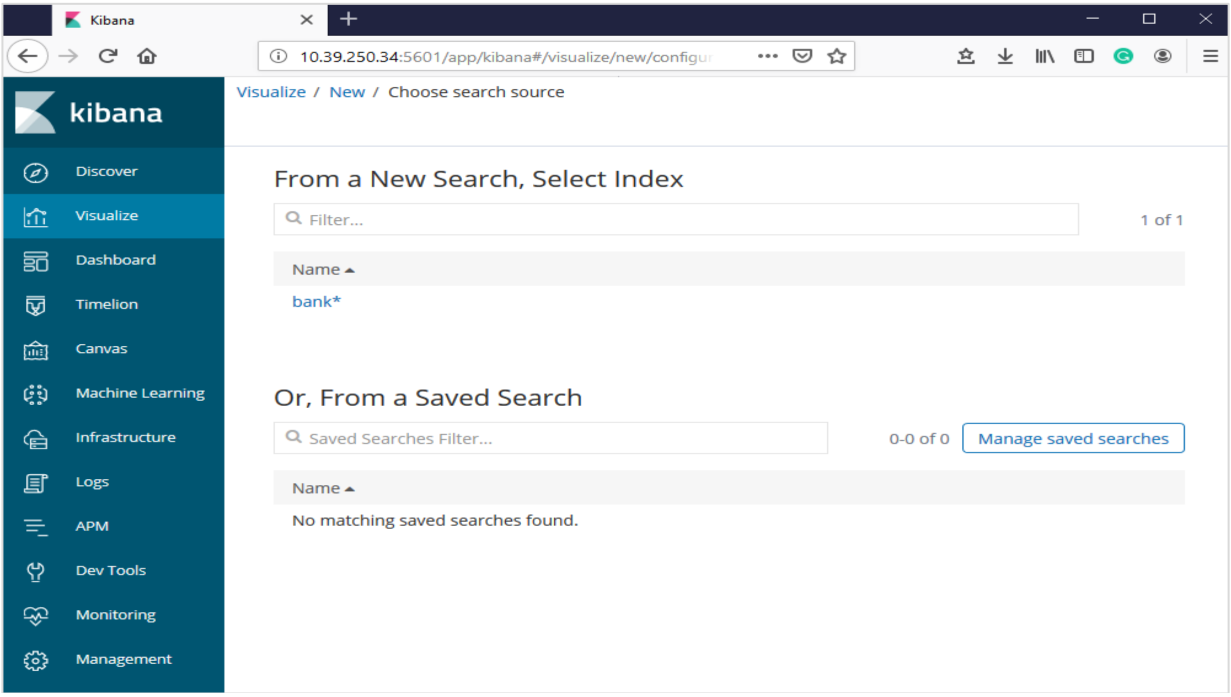
Click on Visualize section on Kibana UI.



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



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



Visualize / New / Choose search source

From a New Search, Select Index

1 of 1

Name

bank*

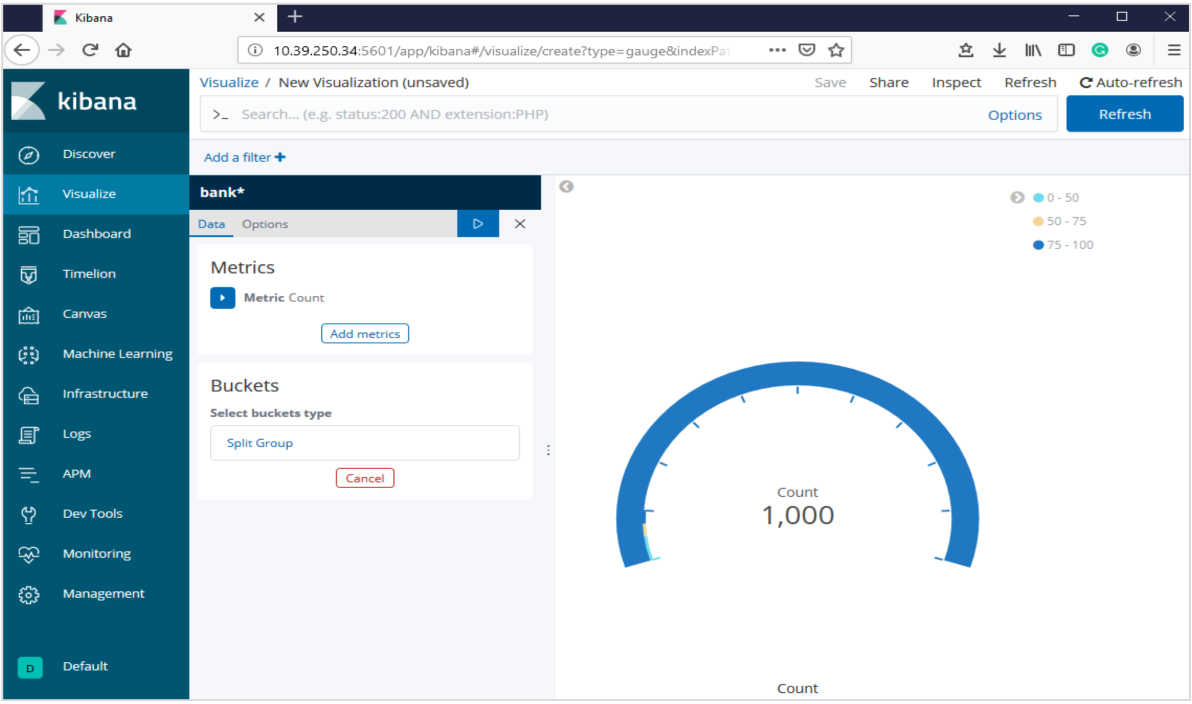
Or, From a Saved Search

0-0 of 0

Name

No matching saved searches found.

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



Visualize / New Visualization (unsaved)

bank*

Metrics

Metric Count

Buckets

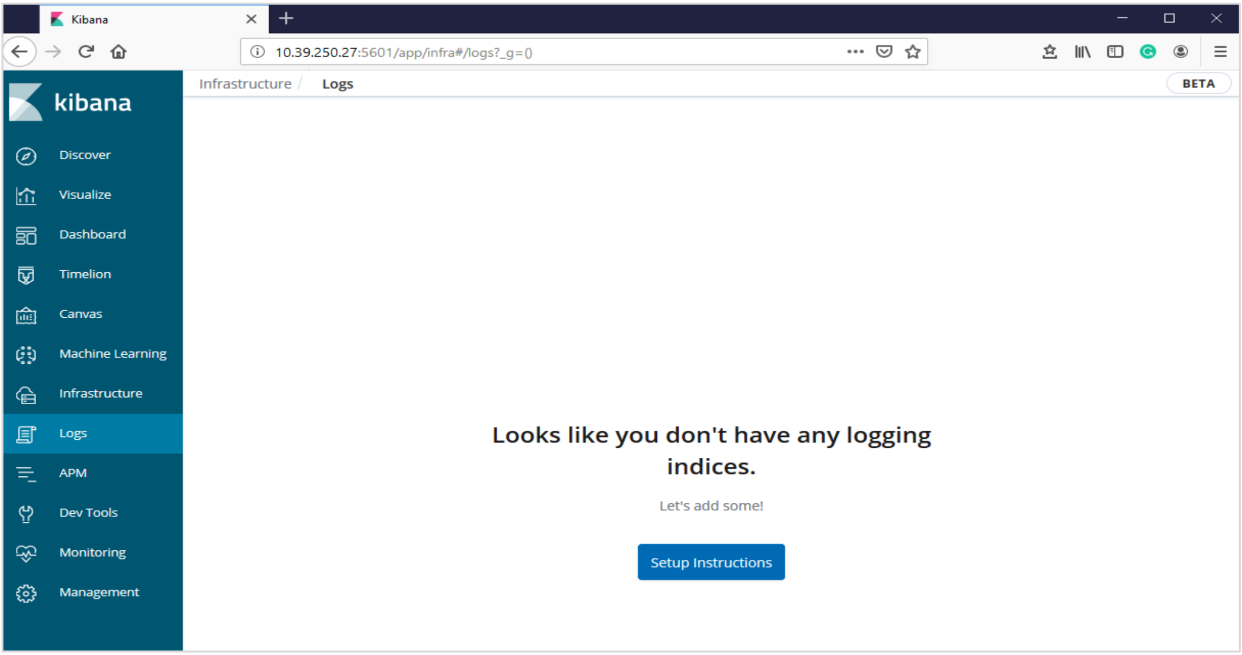
Select buckets type

Split Group

Gauge visualization is created for sample account data successfully.

3 COLLECTING ELASTICSEARCH LOGS USING FILEBEAT

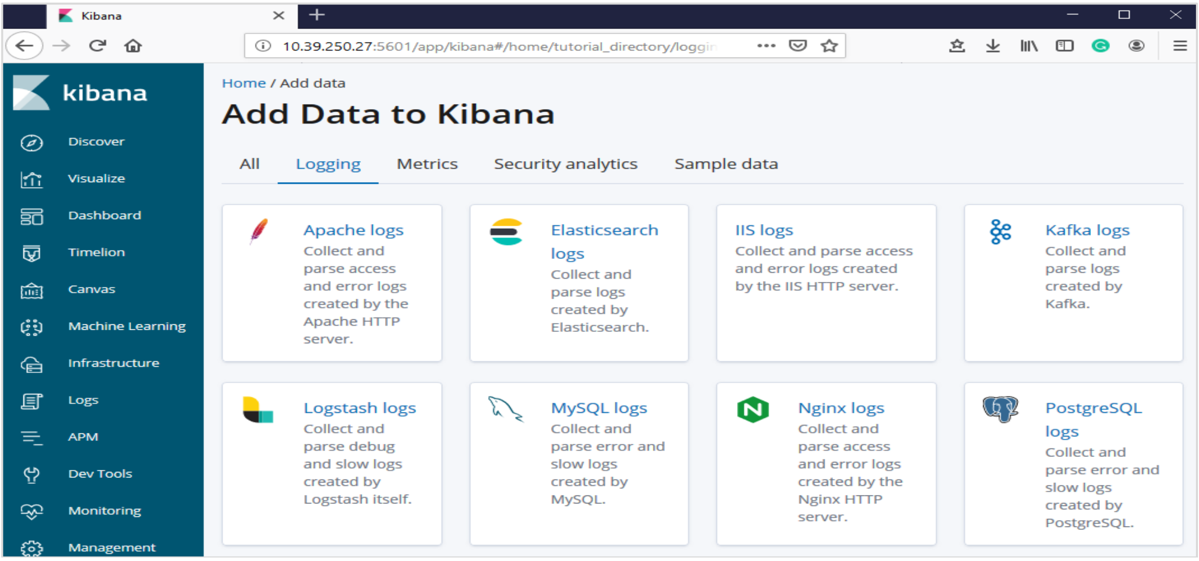
We will use Kibana UI to get information about how to install Filebeat for collecting Elasticsearch logs. Click on the Logs section then click on Setup Instruction.



Looks like you don't have any logging indices.

Let's add some!

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



Add Data to Kibana

Apache logs
Collect and parse access and error logs created by the Apache HTTP server.

Elasticsearch logs
Collect and parse logs created by Elasticsearch.

IIS logs
Collect and parse access and error logs created by the IIS HTTP server.

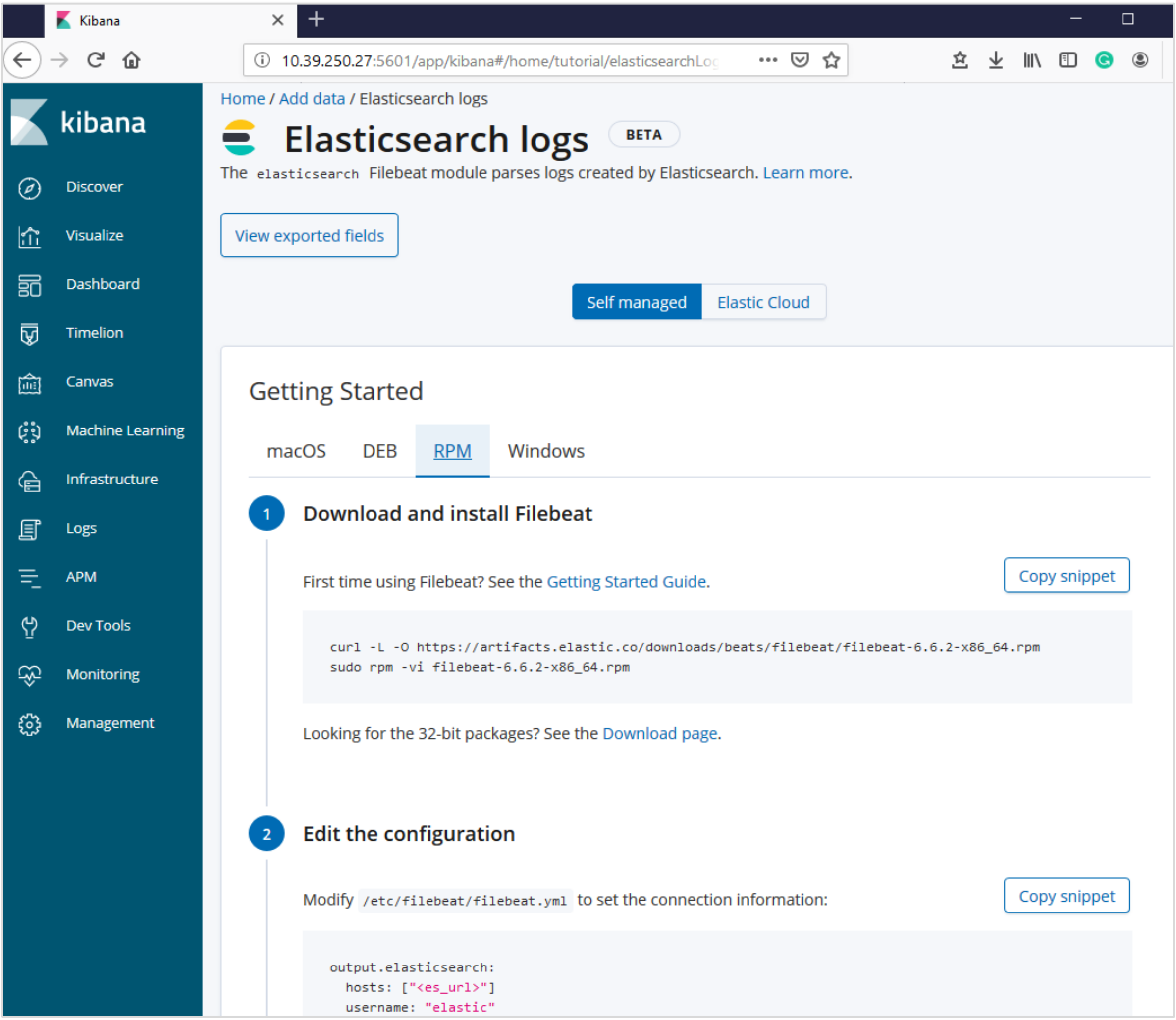
Kafka logs
Collect and parse logs created by Kafka.

Logstash logs
Collect and parse debug and slow logs created by Logstash itself.

MySQL logs
Collect and parse error and slow logs created by MySQL.

Nginx logs
Collect and parse access and error logs created by the Nginx HTTP server.

PostgreSQL logs
Collect and parse error and slow logs created by PostgreSQL.



Home / Add data / Elasticsearch logs

Elasticsearch logs BETA

The `elasticsearch` Filebeat module parses logs created by Elasticsearch. Learn more.

Getting Started

1 Download and install Filebeat

First time using Filebeat? See the Getting Started Guide.

```
curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-6.6.2-x86_64.rpm
sudo rpm -vi filebeat-6.6.2-x86_64.rpm
```

Looking for the 32-bit packages? See the Download page.

2 Edit the configuration

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

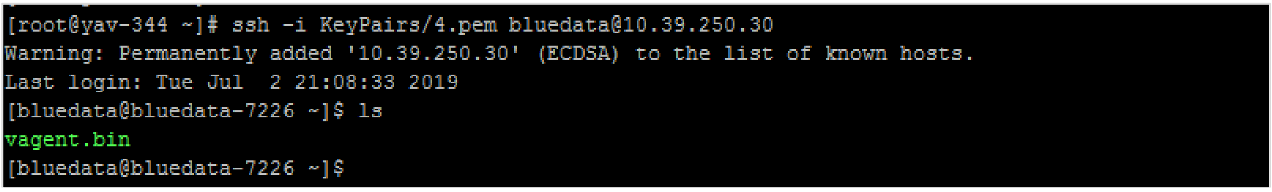
```
output.elasticsearch:
  hosts: ["<es_url>"]
  username: "elastic"
```

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.

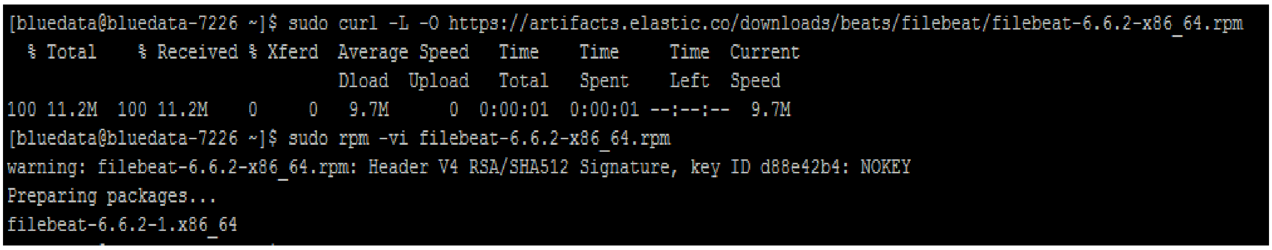
```
ssh -i <your pem keypair> bluedata@<ip_address>
```



```
[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

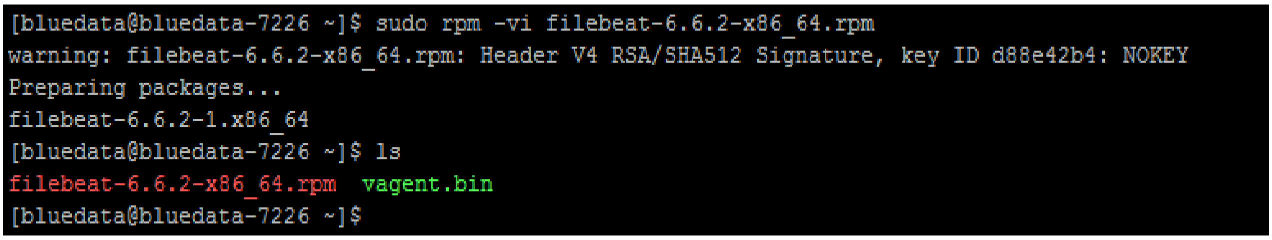
```
sudo curl -L -O
https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-6.6.2-
x86_64.rpm
```



```
[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.

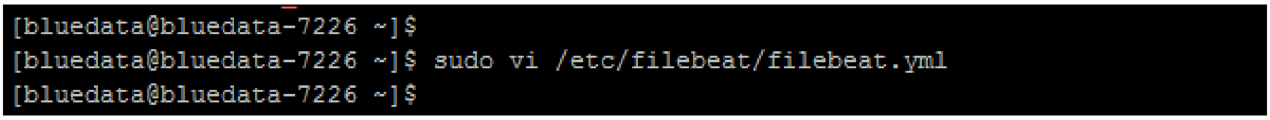
```
sudo rpm -vi filebeat-6.6.2-x86_64.rpm
```



```
[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 ~]$
```

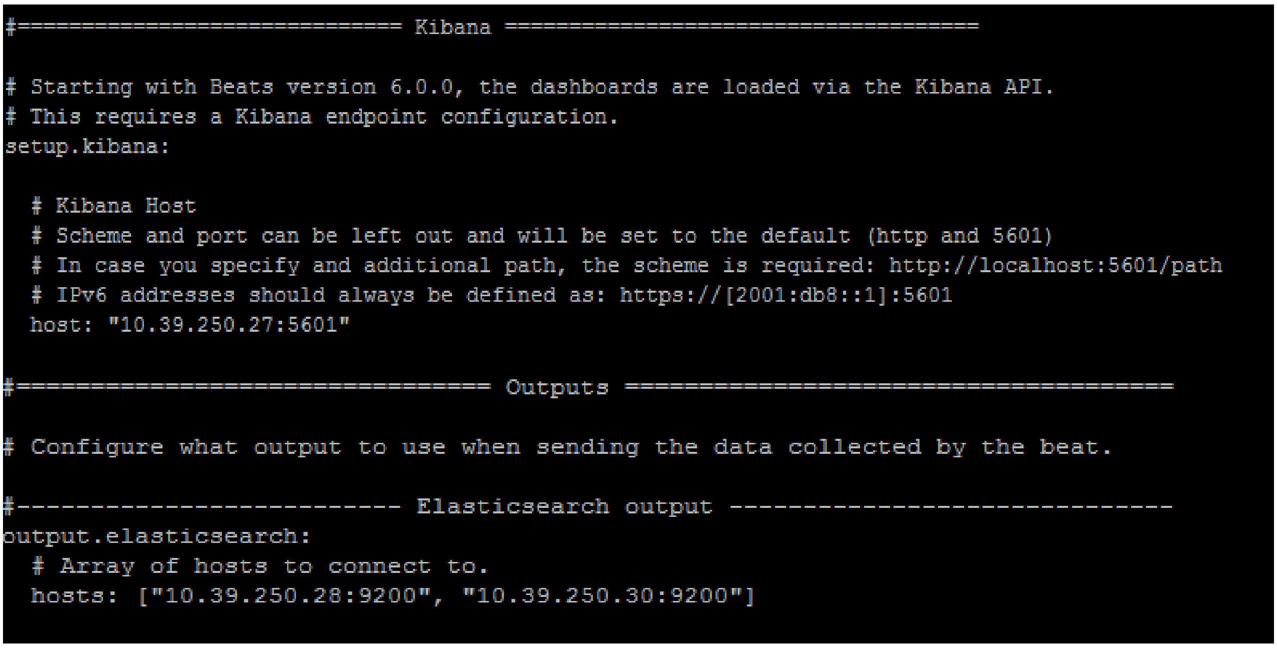
Modify /etc/filebeat/filebeat.yml to set the connection information:

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



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

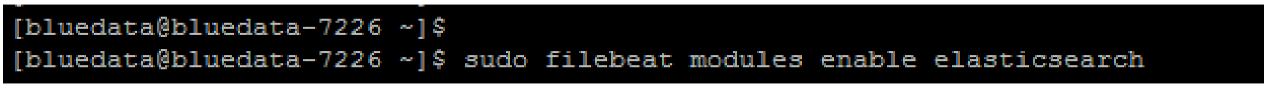
Enter IP address for Kibana and Elasticsearch hosts in filebeat.yml file.



```
#============================== 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:

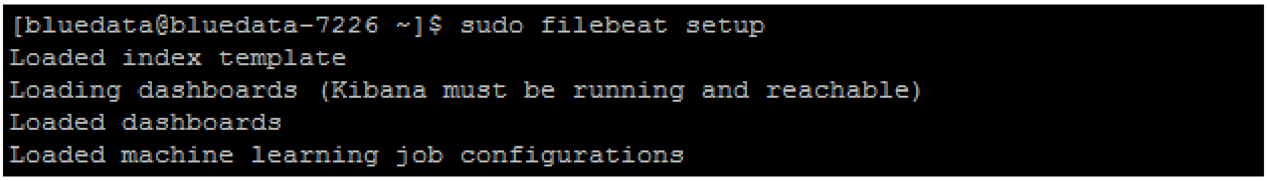
```
sudo filebeat modules enable elasticsearch
```



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

Execute the following command to setup Filebeat:

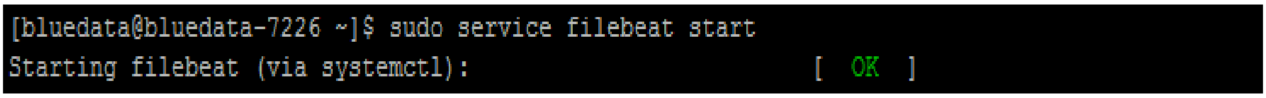
```
sudo filebeat setup
```



```
[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:

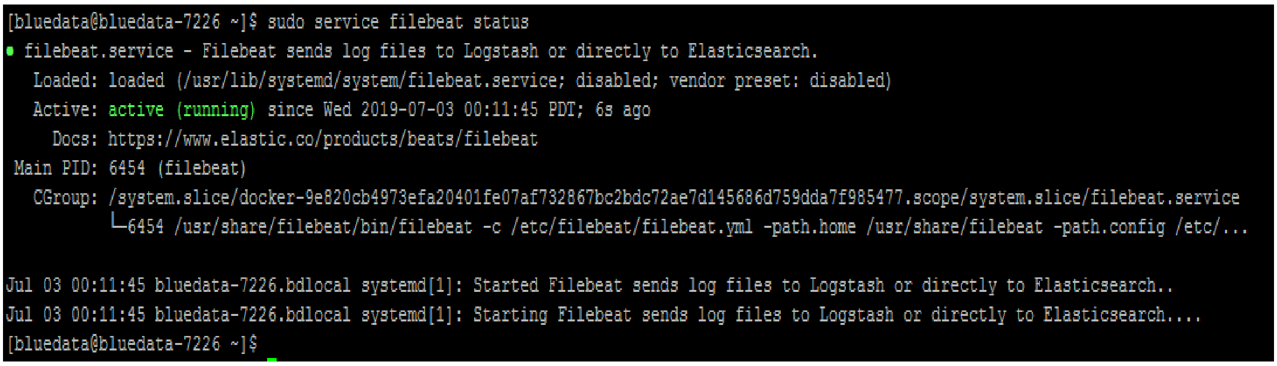
```
sudo service filebeat start
```



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

Execute the following command to check the status for Filebeat:

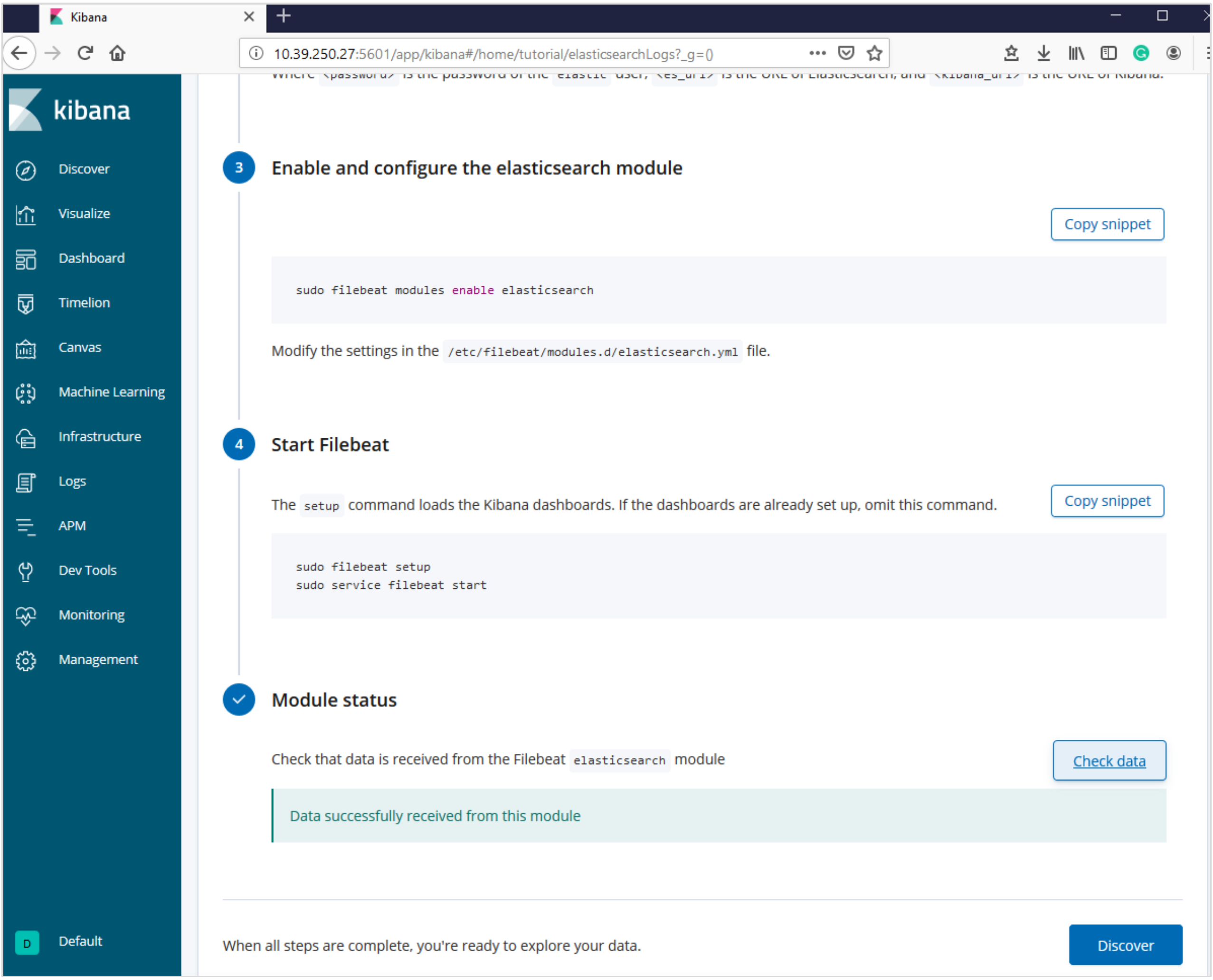
```
sudo service filebeat status
```



```
[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.



where `<password>` is the password of the `elastic` user, `<es_url>` is the URL of Elasticsearch, and `<kibana_url>` is the URL of Kibana.

3 Enable and configure the elasticsearch module

```
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.

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

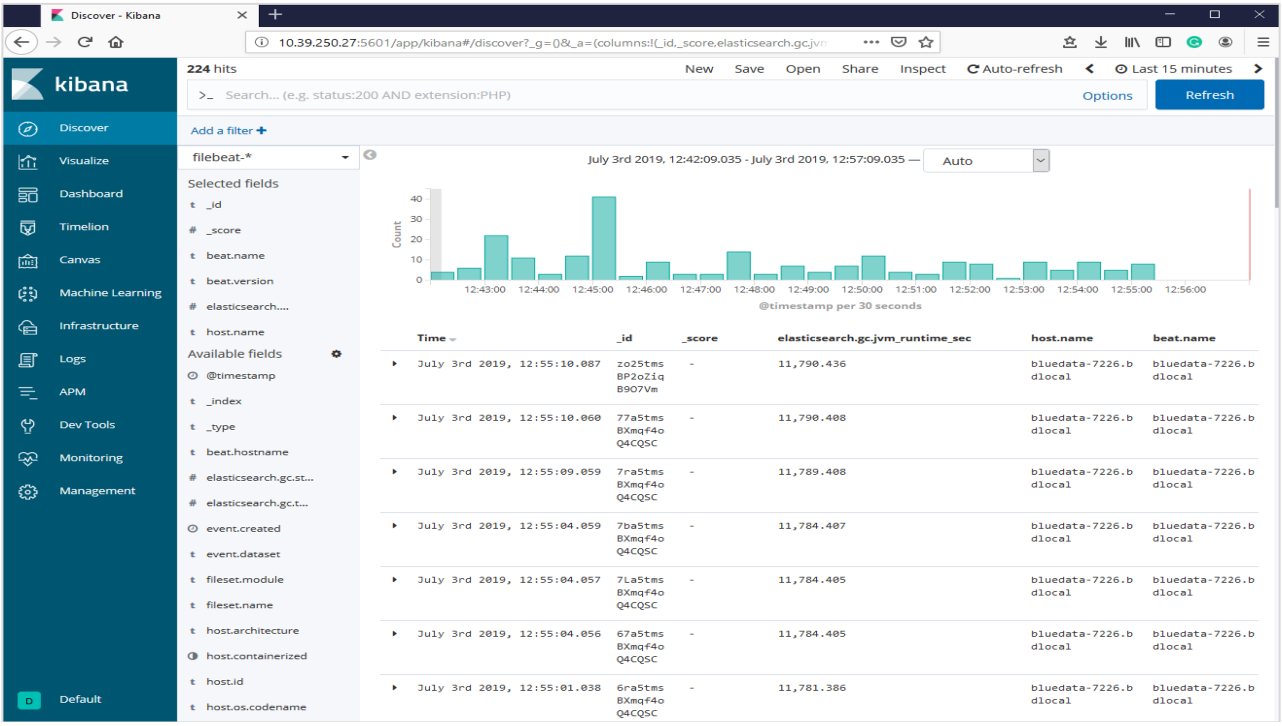
✓ Module status

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

Data successfully received from this module

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

Click on Discover to explore your Elasticsearch log data.



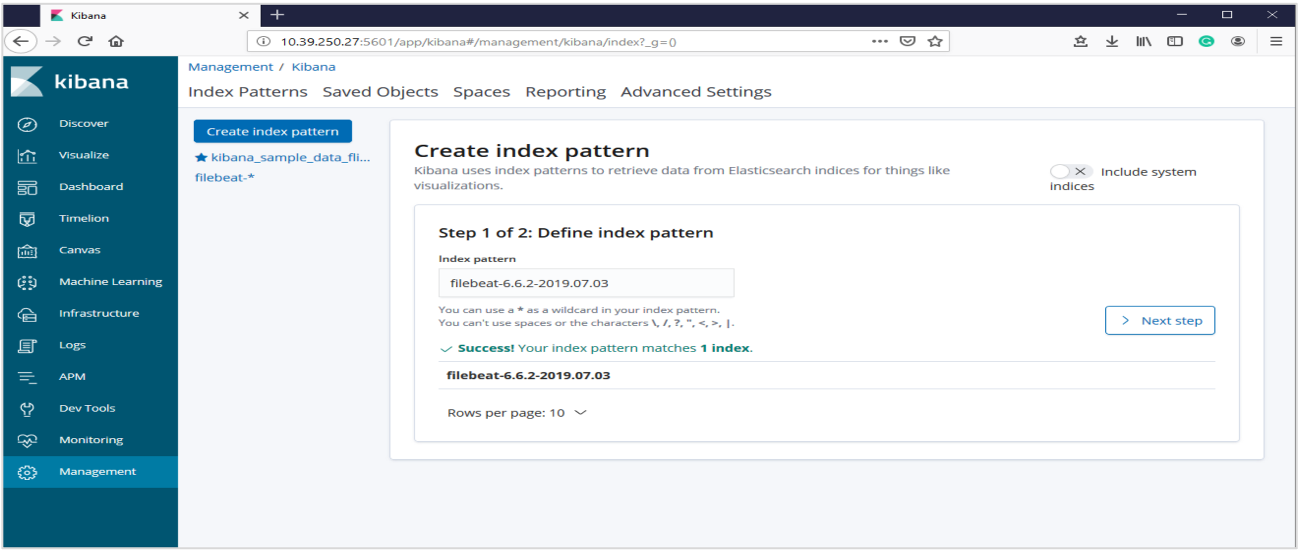
224 hits

July 3rd 2019, 12:42:09.035 - July 3rd 2019, 12:57:09.035 —

Time	_id	_score	elasticsearch.gc.jvm_runtime_sec	host.name	beat.name
July 3rd 2019, 12:55:10.087	zo25tmsBP2oZiqB9O7Vm	-	11,790.436	bluedata-7226.bdlocal	bluedata-7226.bdlocal
July 3rd 2019, 12:55:10.060	77a5tmsBXmqf4oQ4CQSC	-	11,790.408	bluedata-7226.bdlocal	bluedata-7226.bdlocal
July 3rd 2019, 12:55:09.059	7ra5tmsBXmqf4oQ4CQSC	-	11,789.408	bluedata-7226.bdlocal	bluedata-7226.bdlocal
July 3rd 2019, 12:55:04.059	7ba5tmsBXmqf4oQ4CQSC	-	11,784.407	bluedata-7226.bdlocal	bluedata-7226.bdlocal
July 3rd 2019, 12:55:04.057	7La5tmsBXmqf4oQ4CQSC	-	11,784.405	bluedata-7226.bdlocal	bluedata-7226.bdlocal
July 3rd 2019, 12:55:04.056	67a5tmsBXmqf4oQ4CQSC	-	11,784.405	bluedata-7226.bdlocal	bluedata-7226.bdlocal
July 3rd 2019, 12:55:01.038	6ra5tmsBXmqf4oQ4CQSC	-	11,781.386	bluedata-7226.bdlocal	bluedata-7226.bdlocal

3.3 Create Index patterns name for Elasticsearch logs data

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



Create index pattern

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

Step 1 of 2: Define index pattern

Index pattern

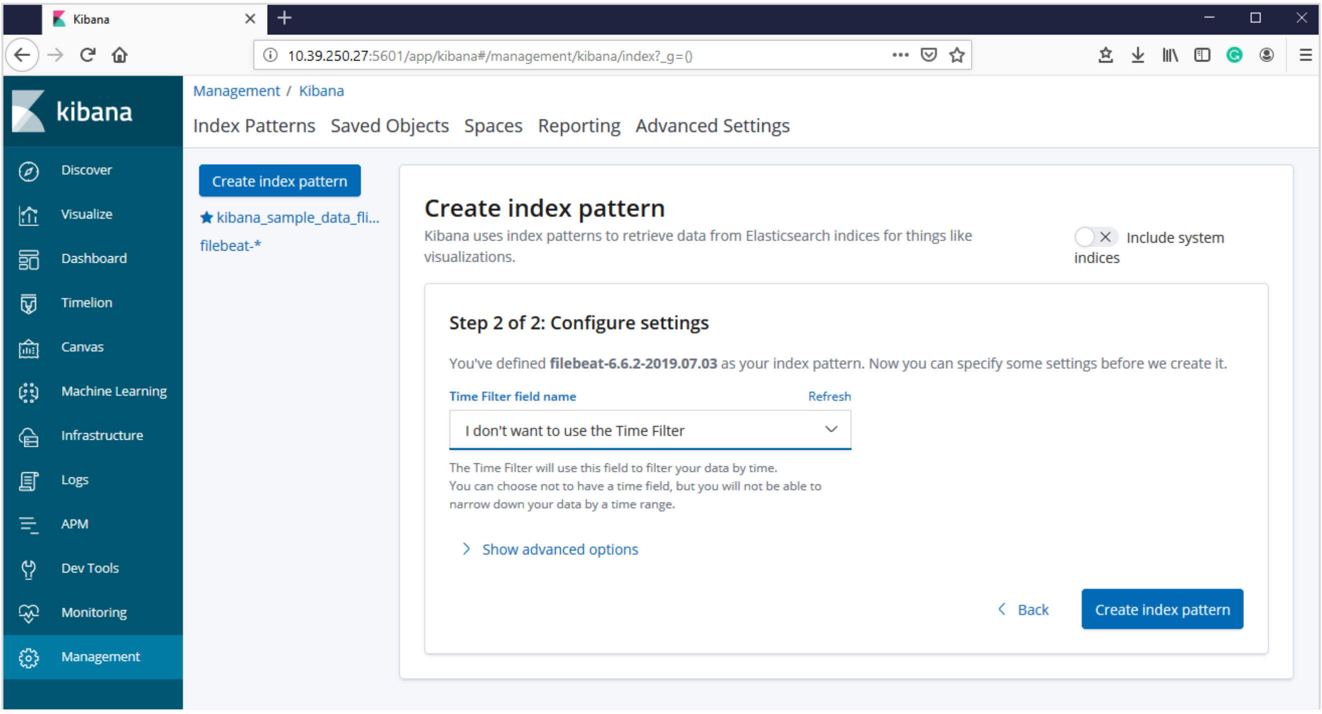
filebeat-6.6.2-2019.07.03

You can use a * as a wildcard in your index pattern.
You can't use spaces or the characters \, /, ?, ", <, >, |.

✓ **Success!** Your index pattern matches **1 index**.

filebeat-6.6.2-2019.07.03

Define index pattern then click on Next step.



Create index pattern

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

Include system indices

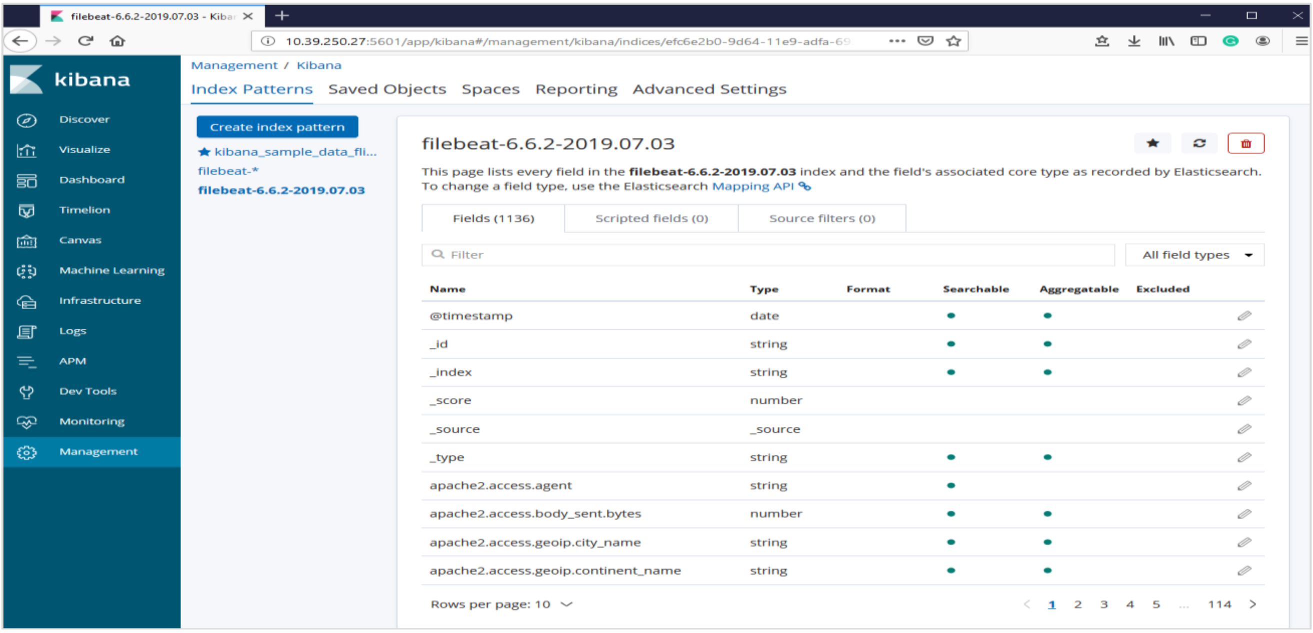
Step 2 of 2: Configure settings

You've defined **filebeat-6.6.2-2019.07.03** as your index pattern. Now you can specify some settings before we create it.

Time Filter field name: I don't want to use the Time Filter

The Time Filter will use this field to filter your data by time. You can choose not to have a time field, but you will not be able to narrow down your data by a time range.

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



filebeat-6.6.2-2019.07.03

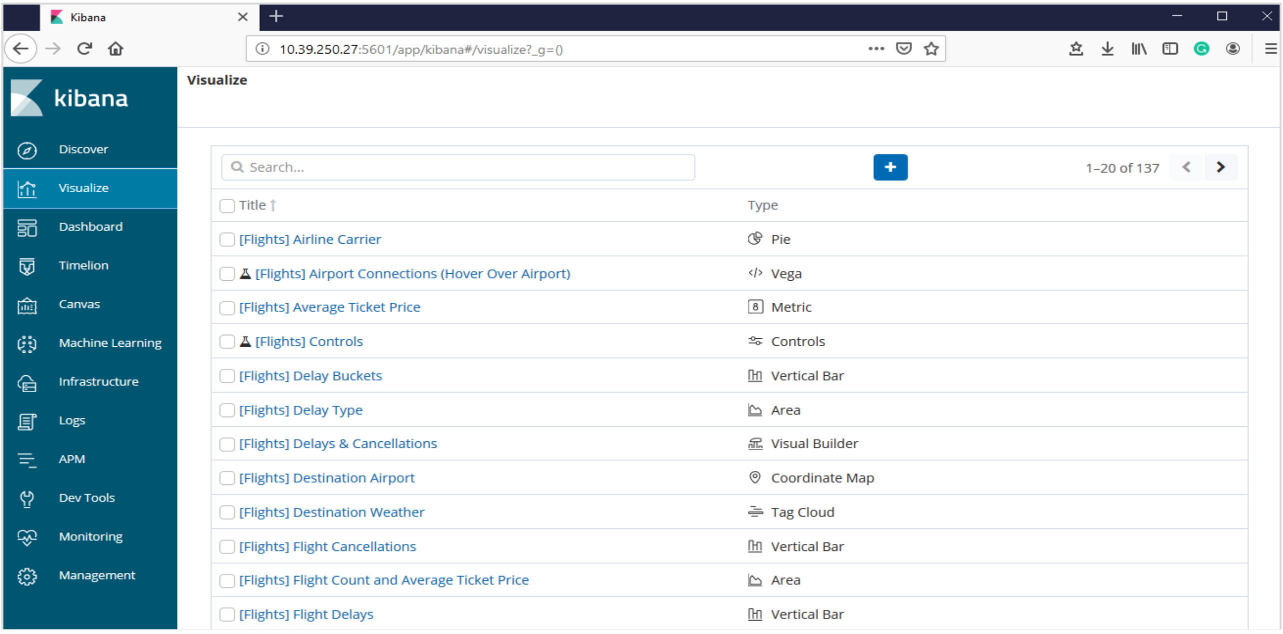
This page lists every field in the **filebeat-6.6.2-2019.07.03** index and the field's associated core type as recorded by Elasticsearch. To change a field type, use the Elasticsearch Mapping API

Name	Type	Format	Searchable	Aggregatable	Excluded
@timestamp	date		●	●	
_id	string		●	●	
_index	string		●	●	
_score	number				
_source	_source				
_type	string		●	●	
apache2.access.agent	string		●		
apache2.access.body_sent.bytes	number		●	●	
apache2.access.geoip.city_name	string		●	●	
apache2.access.geoip.continent_name	string		●	●	

New index pattern is created successfully.

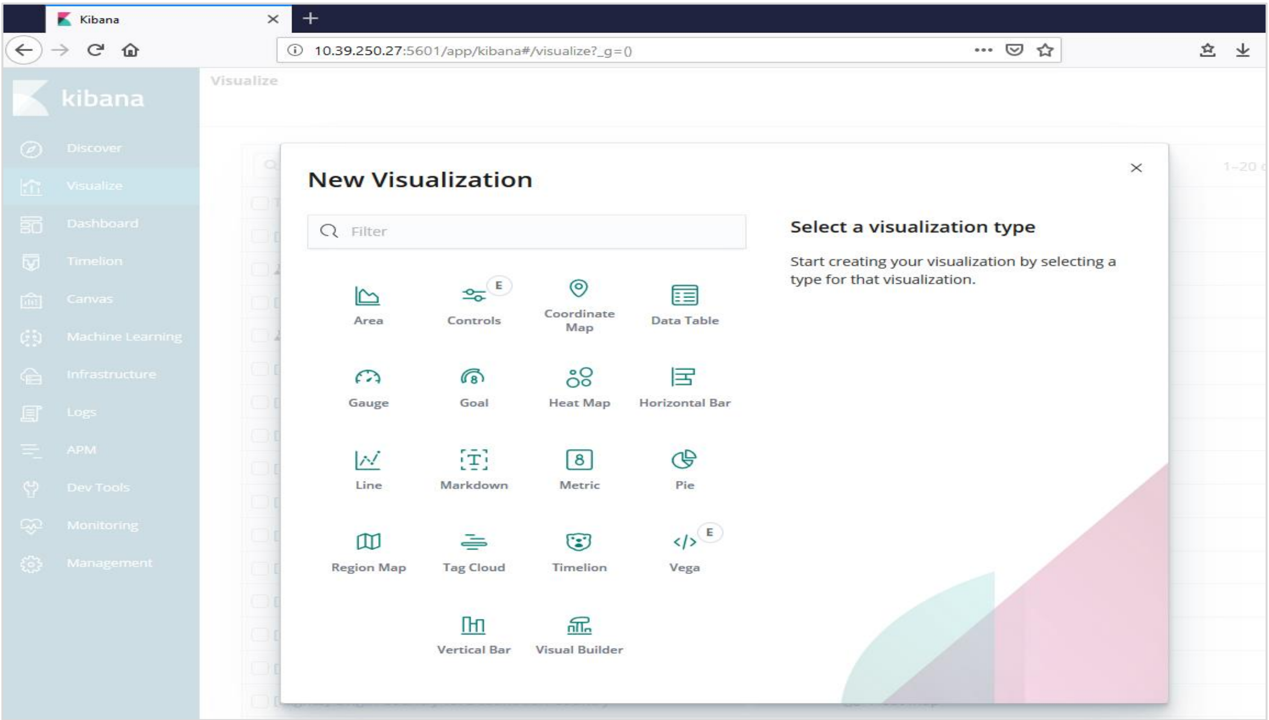
3.4 Create visualization type for Elasticsearch logs data

Click on Visualize section on Kibana UI.



Title ↑	Type
[Flights] Airline Carrier	Pie
[Flights] Airport Connections (Hover Over Airport)	Vega
[Flights] Average Ticket Price	Metric
[Flights] Controls	Controls
[Flights] Delay Buckets	Vertical Bar
[Flights] Delay Type	Area
[Flights] Delays & Cancellations	Visual Builder
[Flights] Destination Airport	Coordinate Map
[Flights] Destination Weather	Tag Cloud
[Flights] Flight Cancellations	Vertical Bar
[Flights] Flight Count and Average Ticket Price	Area
[Flights] Flight Delays	Vertical Bar

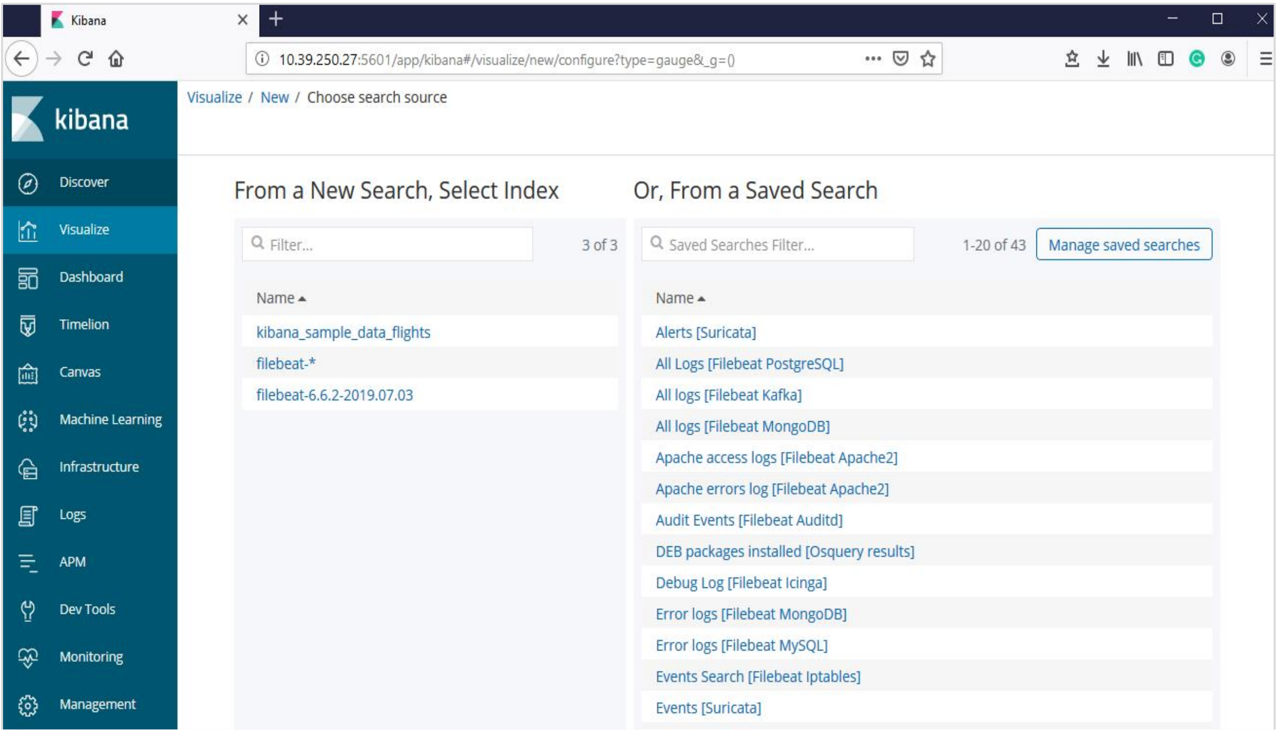
Click on + sign to create new visualization type for Elasticsearch logs data.



Select a visualization type

Start creating your visualization by selecting a type for that visualization.

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



From a New Search, Select Index

Filter... 3 of 3

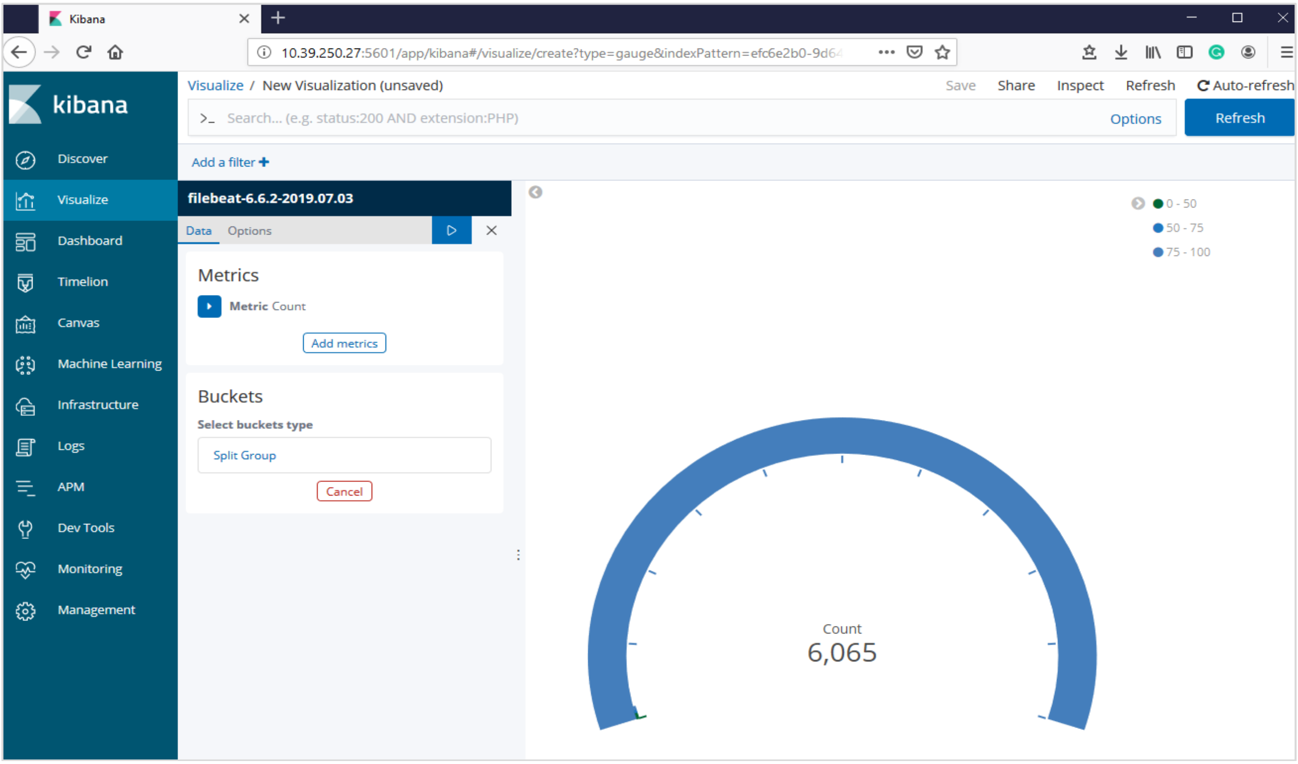
Name ▲
kibana_sample_data_flights
filebeat-*
filebeat-6.6.2-2019.07.03

Or, From a Saved Search

Saved Searches Filter... 1-20 of 43 Manage saved searches

Name ▲
Alerts [Suricata]
All Logs [Filebeat PostgreSQL]
All logs [Filebeat Kafka]
All logs [Filebeat MongoDB]
Apache access logs [Filebeat Apache2]
Apache errors log [Filebeat Apache2]
Audit Events [Filebeat Auditd]
DEB packages installed [Osquery results]
Debug Log [Filebeat Icinga]
Error logs [Filebeat MongoDB]
Error logs [Filebeat MySQL]
Events Search [Filebeat Iptables]
Events [Suricata]

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



filebeat-6.6.2-2019.07.03

Metrics
Metric Count

Buckets
Select buckets type
Split Group

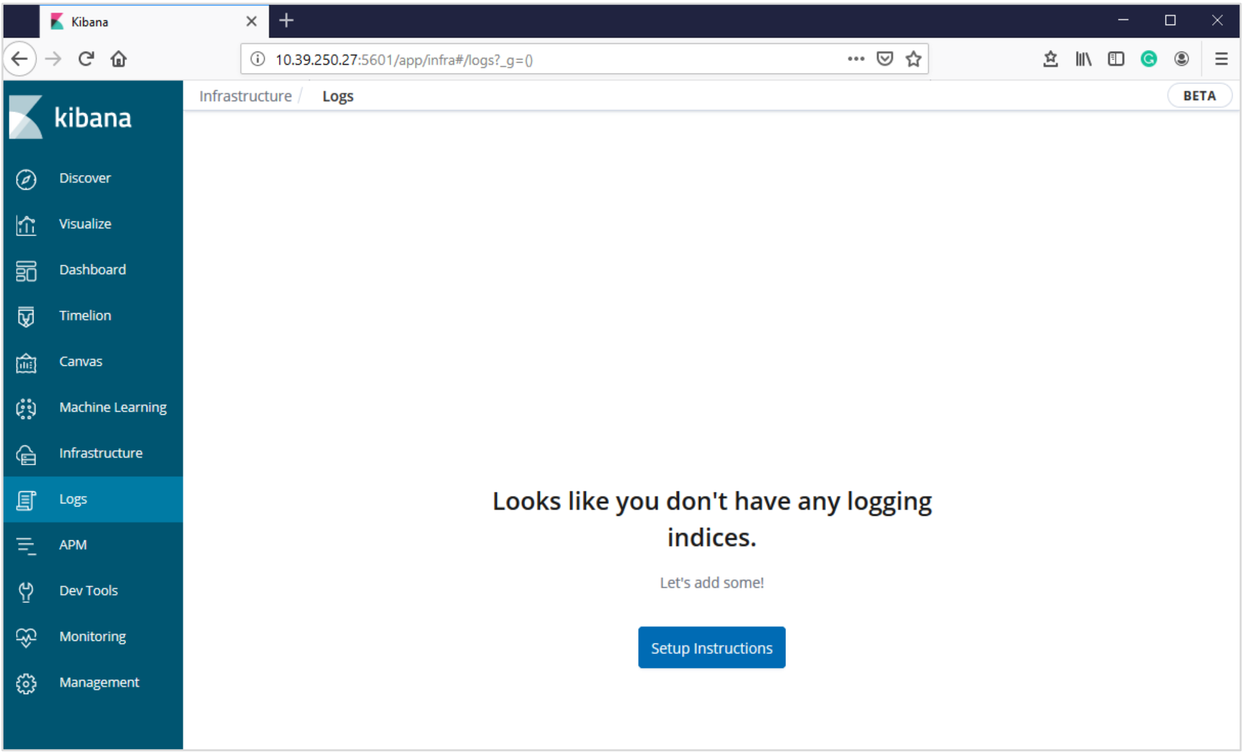
Count
6,065

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

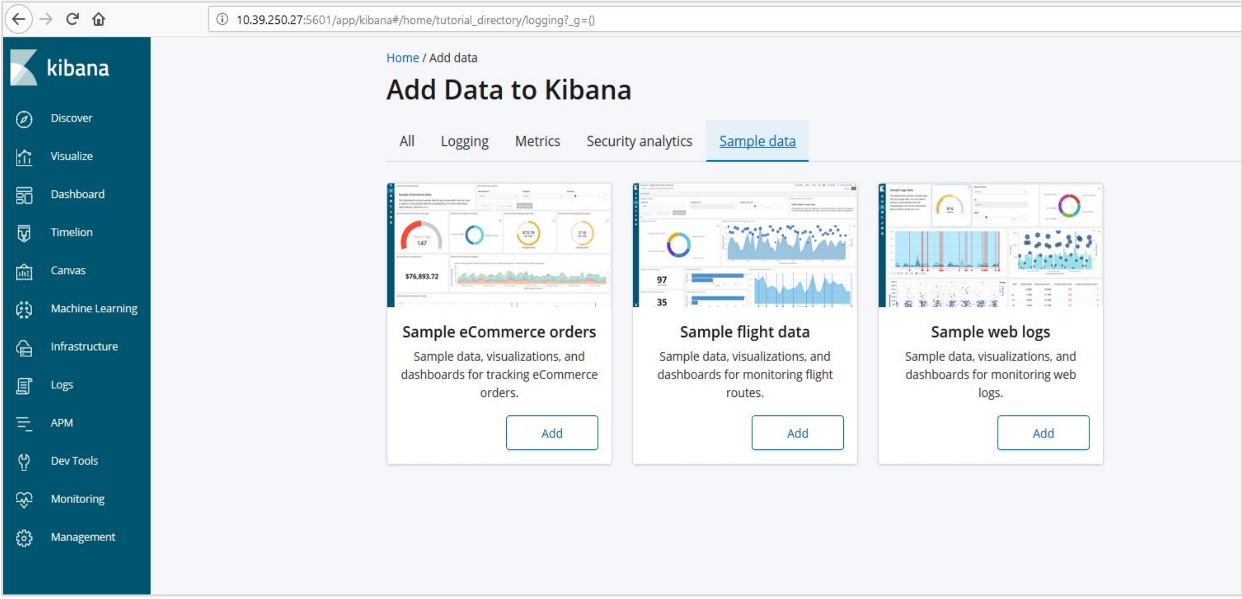
We will use Kibana UI to add sample flights dataset and test the ELK stack.



Looks like you don't have any logging indices.

Let's add some!

Click on Add to install sample flight data in Kibana.



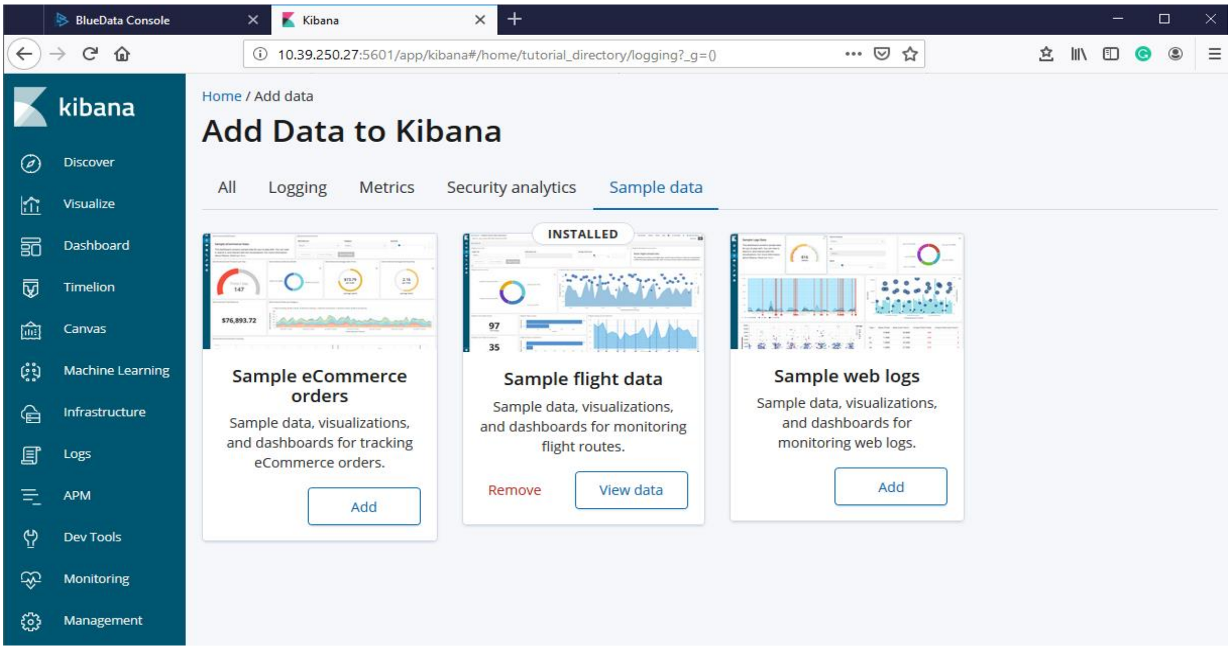
Add Data to Kibana

Sample eCommerce orders
Sample data, visualizations, and dashboards for tracking eCommerce orders.

Sample flight data
Sample data, visualizations, and dashboards for monitoring flight routes.

Sample web logs
Sample data, visualizations, and dashboards for monitoring web logs.

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



Add Data to Kibana

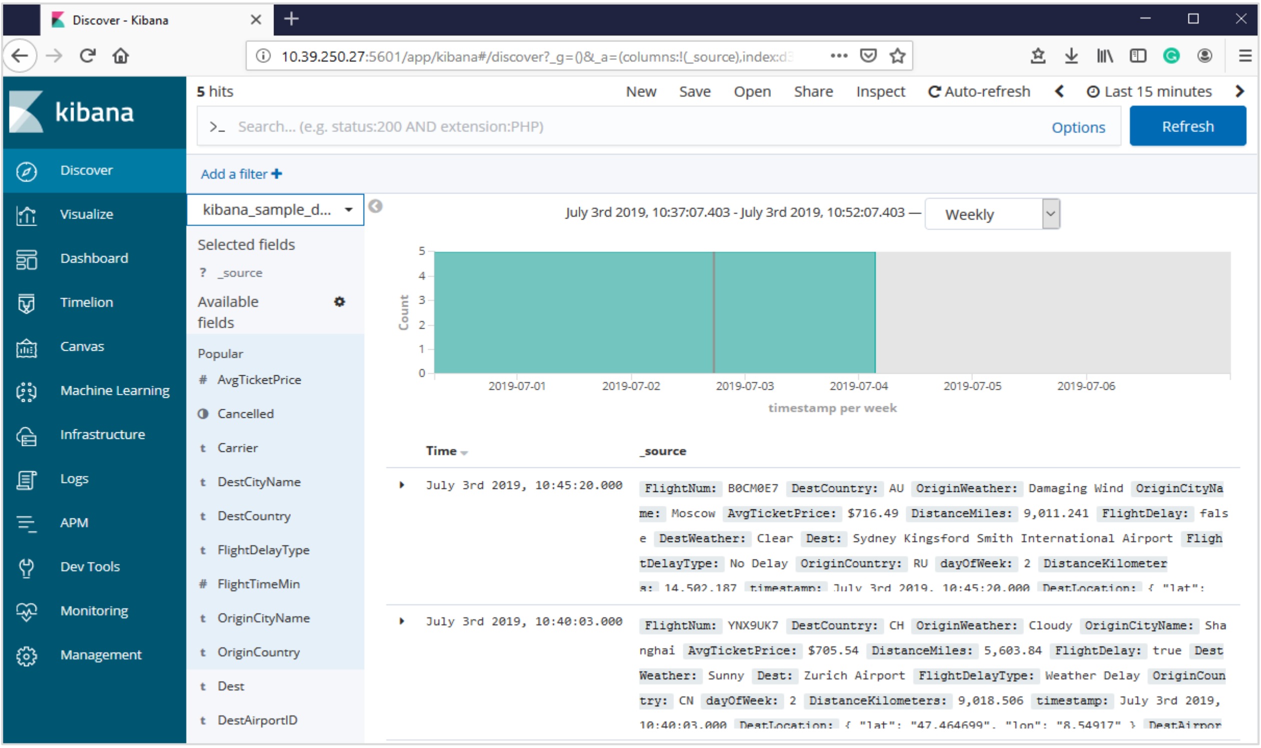
Sample eCommerce orders
Sample data, visualizations, and dashboards for tracking eCommerce orders.

Sample flight data
Sample data, visualizations, and dashboards for monitoring flight routes.

Sample web logs
Sample data, visualizations, and dashboards for monitoring web logs.

4.2 Discover the sample flight dataset

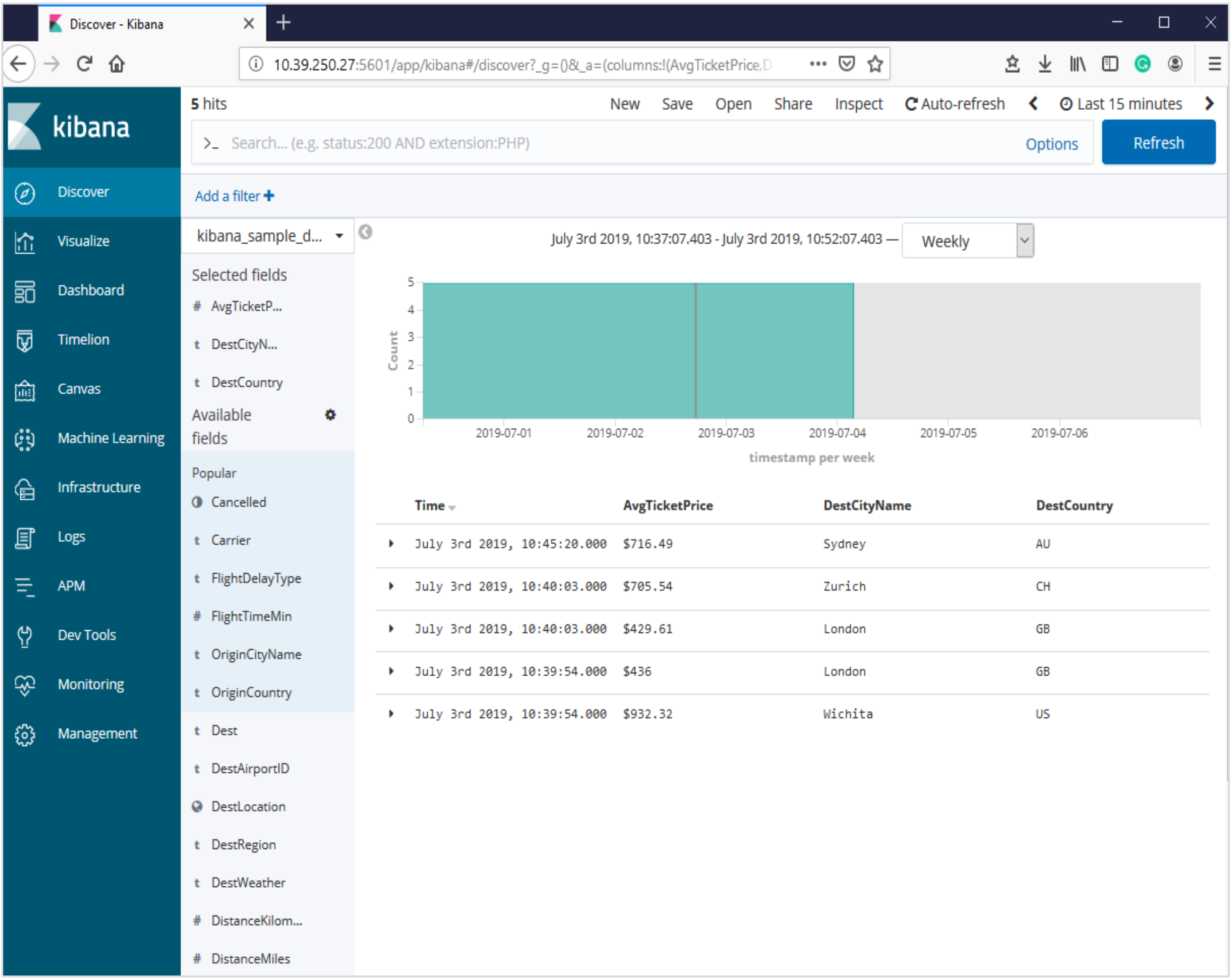
Click on Discover section in Kibana UI.



Time	_source
July 3rd 2019, 10:45:20.000	FlightNum: B0CM0E7 DestCountry: AU OriginWeather: Damaging Wind OriginCityName: Moscow AvgTicketPrice: $716.49 DistanceMiles: 9,011.241 FlightDelay: false DestWeather: Clear Dest: Sydney Kingsford Smith International Airport FlightDelayType: No Delay OriginCountry: RU dayOfWeek: 2 DistanceKilometers: 14,502.187 timestamp: July 3rd 2019, 10:45:20.000 DestLocation: { "lat":
July 3rd 2019, 10:40:03.000	FlightNum: YNX9UK7 DestCountry: CH OriginWeather: Cloudy OriginCityName: Shanghai AvgTicketPrice: $705.54 DistanceMiles: 5,603.84 FlightDelay: true DestWeather: Sunny Dest: Zurich Airport FlightDelayType: Weather Delay OriginCountry: CN dayOfWeek: 2 DistanceKilometers: 9,018.506 timestamp: July 3rd 2019, 10:40:03.000 DestLocation: { "lat": "47.464699", "lon": "8.54917" } DestAirpor

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.

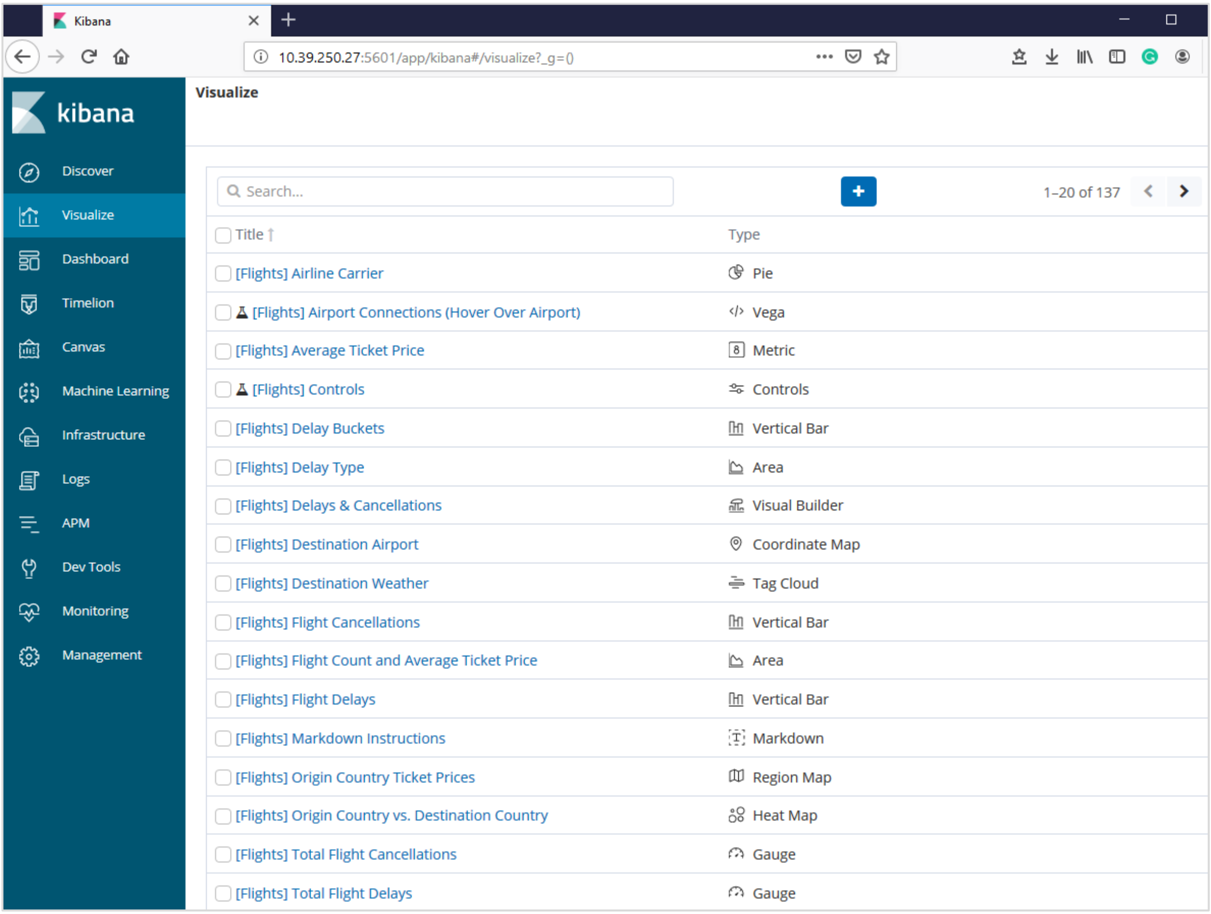


Time	AvgTicketPrice	DestCityName	DestCountry
July 3rd 2019, 10:45:20.000	$716.49	Sydney	AU
July 3rd 2019, 10:40:03.000	$705.54	Zurich	CH
July 3rd 2019, 10:40:03.000	$429.61	London	GB
July 3rd 2019, 10:39:54.000	$436	London	GB
July 3rd 2019, 10:39:54.000	$932.32	Wichita	US

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

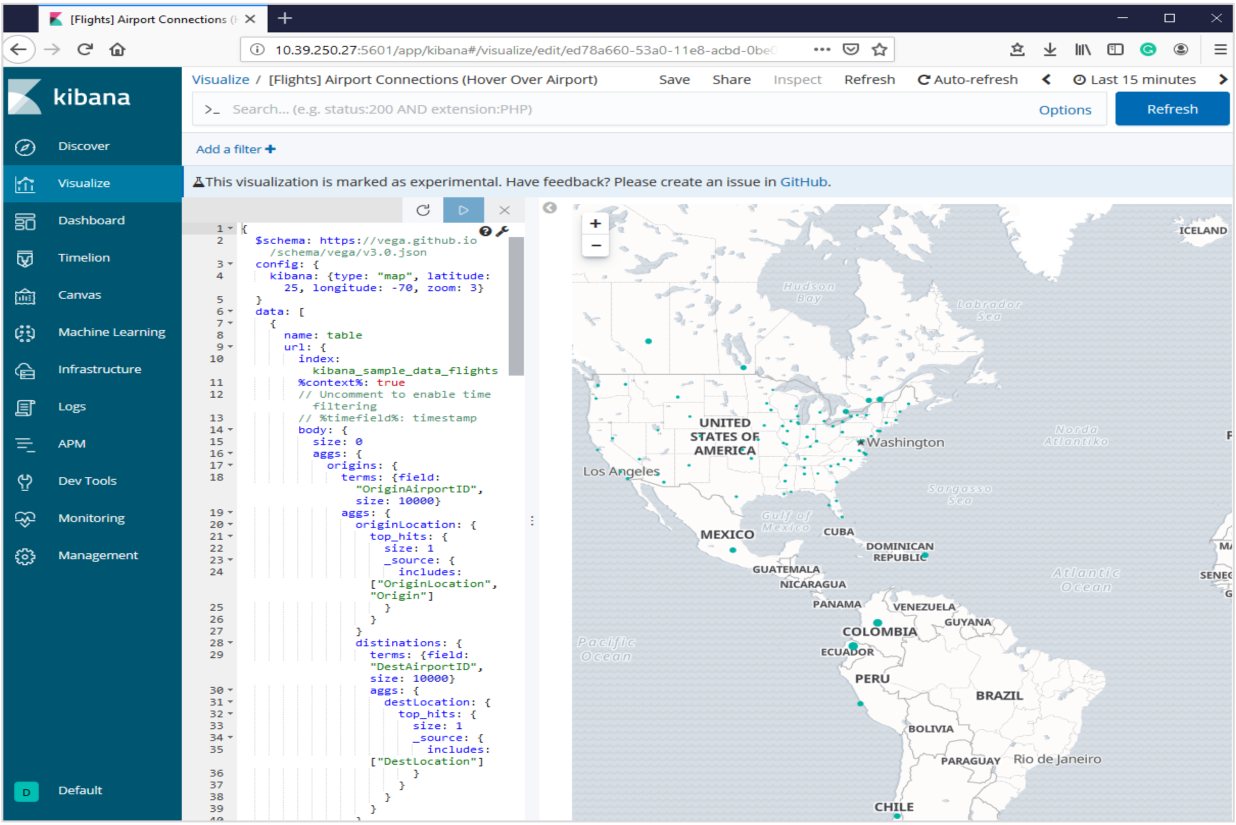
4.3 Visualize the sample flight dataset

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



□ Title ↑	Type
□ [Flights] Airline Carrier	Pie
□ [Flights] Airport Connections (Hover Over Airport)	Vega
□ [Flights] Average Ticket Price	Metric
□ [Flights] Controls	Controls
□ [Flights] Delay Buckets	Vertical Bar
□ [Flights] Delay Type	Area
□ [Flights] Delays & Cancellations	Visual Builder
□ [Flights] Destination Airport	Coordinate Map
□ [Flights] Destination Weather	Tag Cloud
□ [Flights] Flight Cancellations	Vertical Bar
□ [Flights] Flight Count and Average Ticket Price	Area
□ [Flights] Flight Delays	Vertical Bar
□ [Flights] Markdown Instructions	Markdown
□ [Flights] Origin Country Ticket Prices	Region Map
□ [Flights] Origin Country vs. Destination Country	Heat Map
□ [Flights] Total Flight Cancellations	Gauge
□ [Flights] Total Flight Delays	Gauge

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



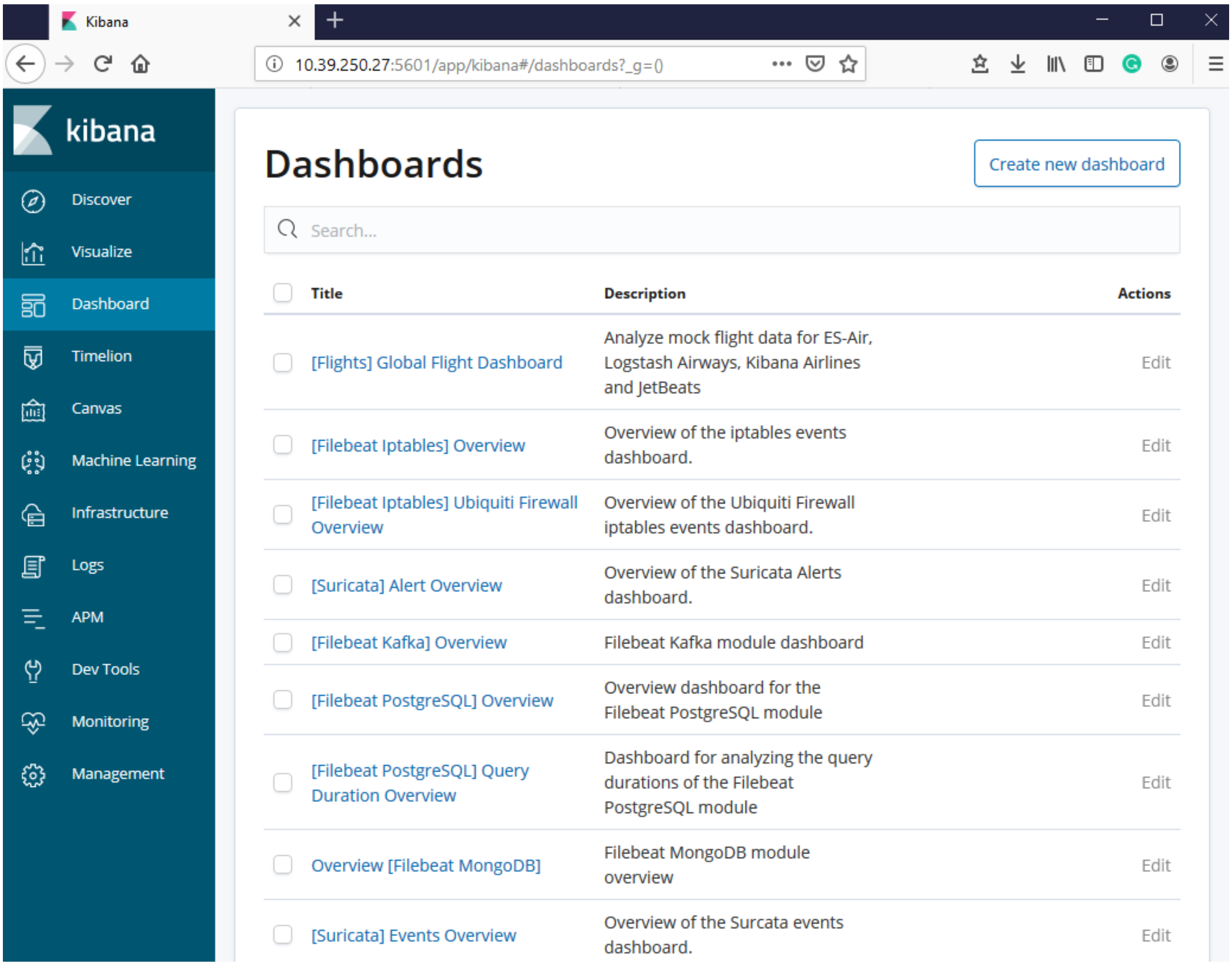
This visualization is marked as experimental. Have feedback? Please create an issue in GitHub.

```
{
  $schema: https://vega.github.io/schema/vega/v3.0.json
  config: {
    kibana: {type: "map", latitude: 25, longitude: -70, zoom: 3}
  }
  data: [
    {
      name: table
      url: {
        index: kibana_sample_data_flights
        %context%: true
        // Uncomment to enable time filtering
        // %timefield%: timestamp
        body: {
          size: 0
          aggs: {
            origins: {
              terms: {field: "OriginAirportID", size: 10000}
              aggs: {
                originLocation: {
                  top_hits: {
                    size: 1
                    _source: {
                      includes: ["OriginLocation", "Origin"]
                    }
                  }
                }
                distinations: {
                  terms: {field: "DestAirportID", size: 10000}
                  aggs: {
                    destLocation: {
                      top_hits: {
                        size: 1
                        _source: {
                          includes: ["DestLocation"]
                        }
                      }
                    }
                  }
```

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

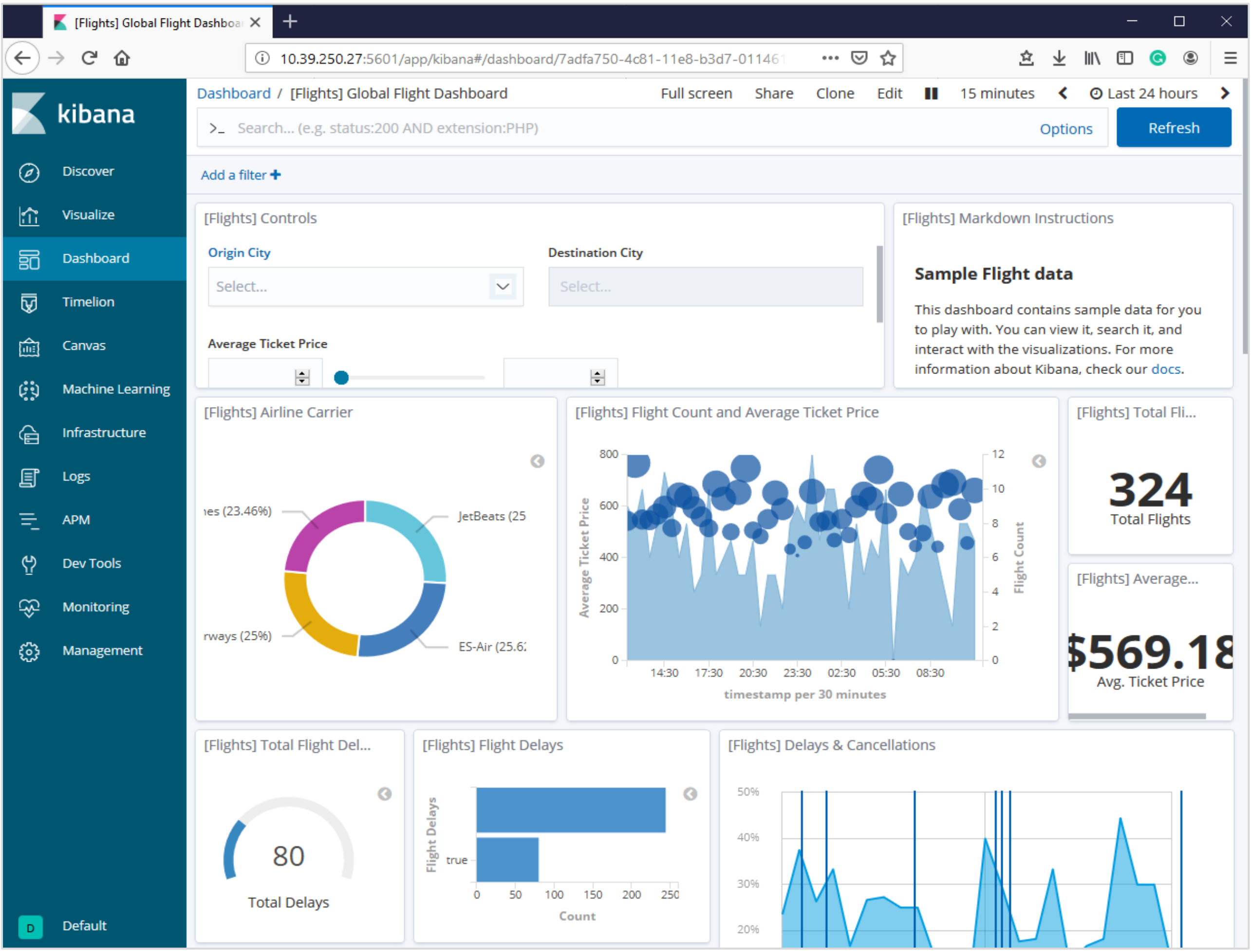
Click on Dashboard section to check dashboard for sample flight dataset. Here we have Global Flight Dashboard for sample flight dataset.



Dashboards

□ Title	Description	Actions
□ [Flights] Global Flight Dashboard	Analyze mock flight data for ES-Air, Logstash Airways, Kibana Airlines and JetBeats	Edit
□ [Filebeat Iptables] Overview	Overview of the iptables events dashboard.	Edit
□ [Filebeat Iptables] Ubiquiti Firewall Overview	Overview of the Ubiquiti Firewall iptables events dashboard.	Edit
□ [Suricata] Alert Overview	Overview of the Suricata Alerts dashboard.	Edit
□ [Filebeat Kafka] Overview	Filebeat Kafka module dashboard	Edit
□ [Filebeat PostgreSQL] Overview	Overview dashboard for the Filebeat PostgreSQL module	Edit
□ [Filebeat PostgreSQL] Query Duration Overview	Dashboard for analyzing the query durations of the Filebeat PostgreSQL module	Edit
□ Overview [Filebeat MongoDB]	Filebeat MongoDB module overview	Edit
□ [Suricata] Events Overview	Overview of the Surcata events dashboard.	Edit

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

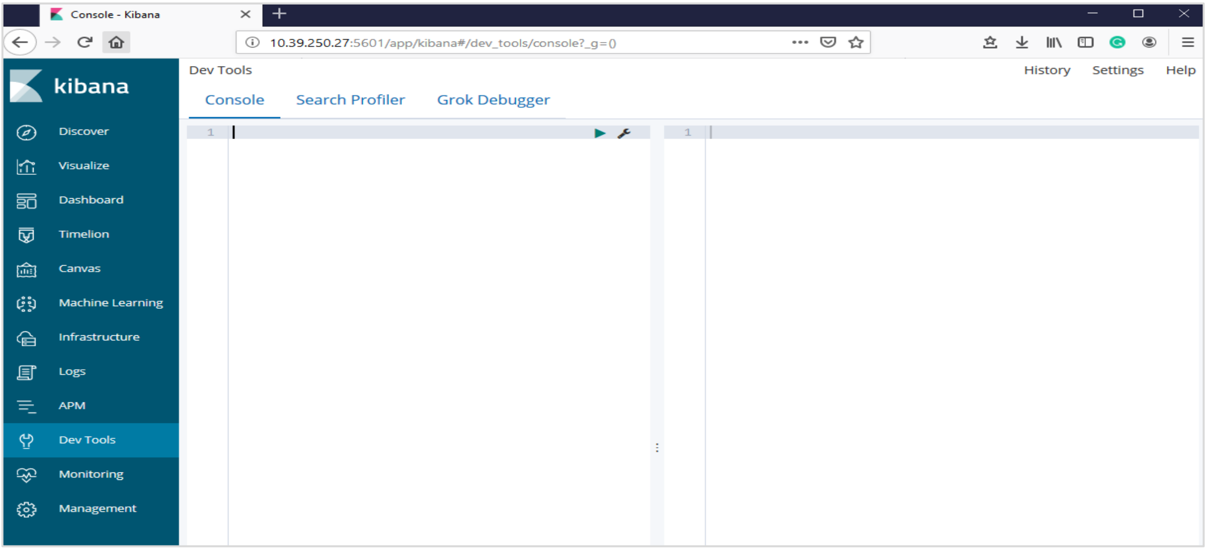


Sample Flight data

This dashboard contains sample data for you to play with. You can view it, search it, and interact with the visualizations. For more information about Kibana, check our docs.

4.5 Test REST API from Dev Tools

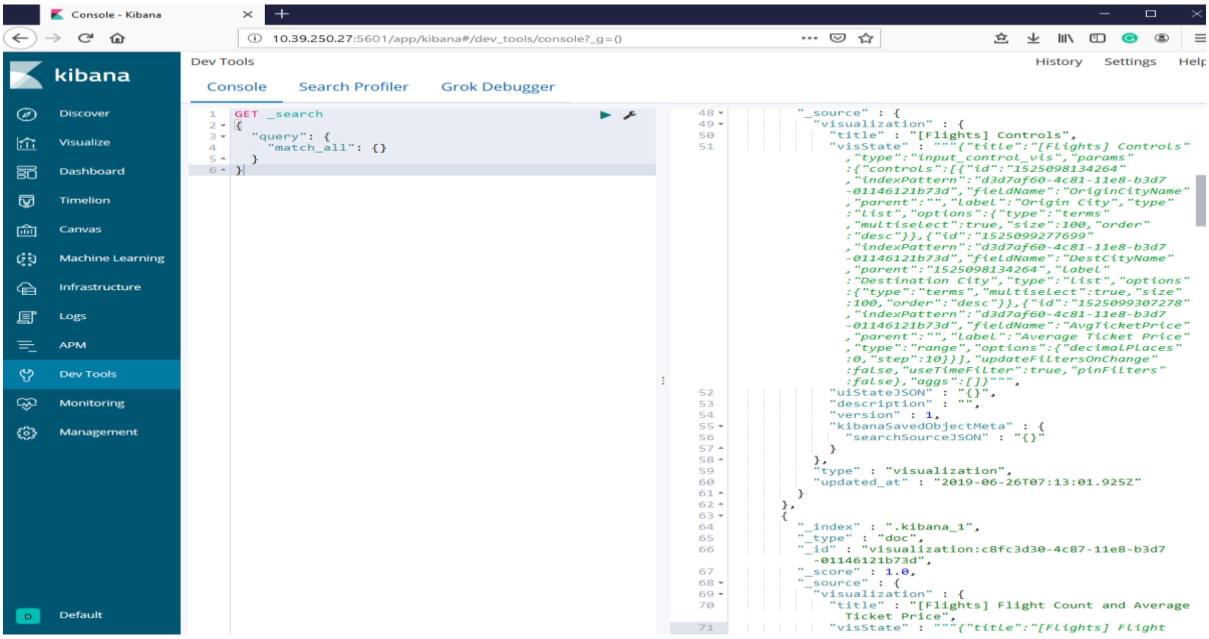
Click on Dev Tools in Kibana UI.



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": {}
  }
}
```

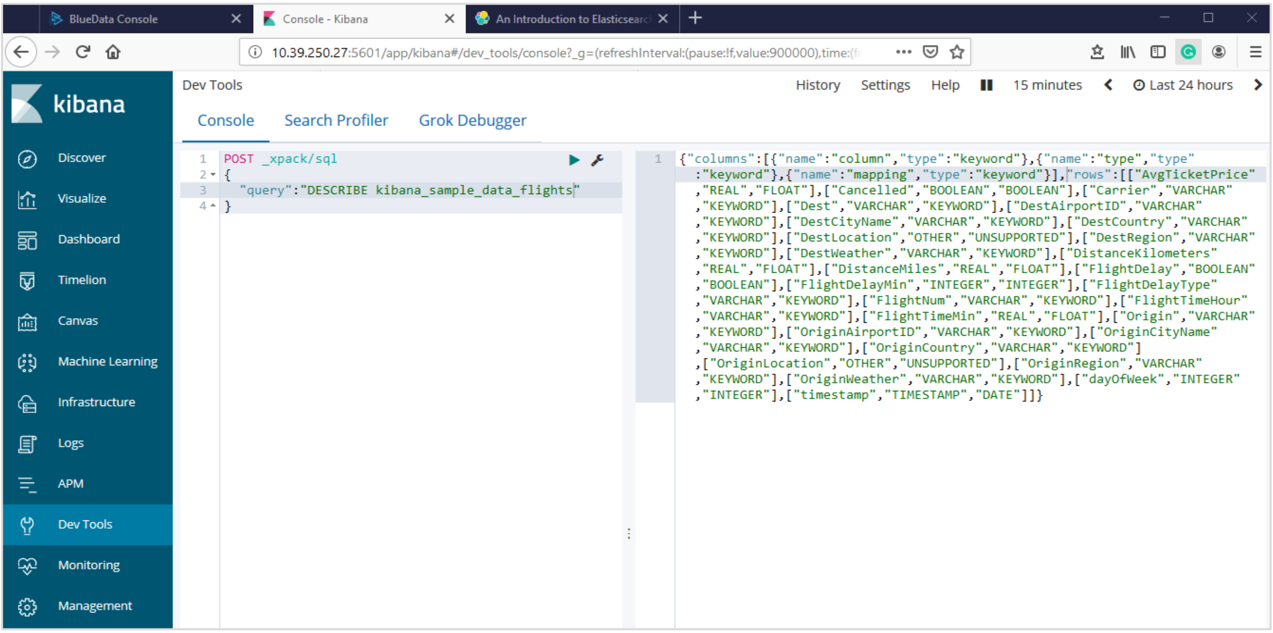


```
GET _search
{
  "query": {
    "match_all": {}
  }
}
```

```
          "_source" : {
            "visualization" : {
              "title" : "[Flights] Controls",
              "visState" : """{"title":"[Flights] Controls"
                ,"type":"input_control_vis","params"
                :{"controls":[{"id":"1525098134264"
                ,"indexPattern":"d3d7af60-4c81-11e8-b3d7
                -01146121b73d","fieldName":"OriginCityName"
                ,"parent":"","label":"Origin City","type"
                :"list","options":{"type":"terms"
                ,"multiselect":true,"size":100,"order"
                :"desc"}},{"id":"1525099277699"
                ,"indexPattern":"d3d7af60-4c81-11e8-b3d7
                -01146121b73d","fieldName":"DestCityName"
                ,"parent":"1525098134264","label"
                :"Destination City","type":"list","options"
                :{"type":"terms","multiselect":true,"size"
                :100,"order":"desc"}},{"id":"1525099307278"
                ,"indexPattern":"d3d7af60-4c81-11e8-b3d7
                -01146121b73d","fieldName":"AvgTicketPrice"
                ,"parent":"","label":"Average Ticket Price"
                ,"type":"range","options":{"decimalPlaces"
                :0,"step":10}}],"updateFiltersOnChange"
                :false,"useTimeFilter":true,"pinFilters"
                :false},"aggs":[]}""",
              "uiStateJSON" : "{}",
              "description" : "",
              "version" : 1,
              "kibanaSavedObjectMeta" : {
                "searchSourceJSON" : "{}"
              }
            },
            "type" : "visualization",
            "updated_at" : "2019-06-26T07:13:01.925Z"
          }
        },
        {
          "_index" : ".kibana_1",
          "_type" : "doc",
          "_id" : "visualization:c8fc3d30-4c87-11e8-b3d7
            -01146121b73d",
          "_score" : 1.0,
          "_source" : {
            "visualization" : {
              "title" : "[Flights] Flight Count and Average
                Ticket Price",
              "visState" : """{"title":"[Flights] Flight
```

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

```
POST _xpack/sql
{
  "query":"DESCRIBE kibana_sample_data_flights"
}
```

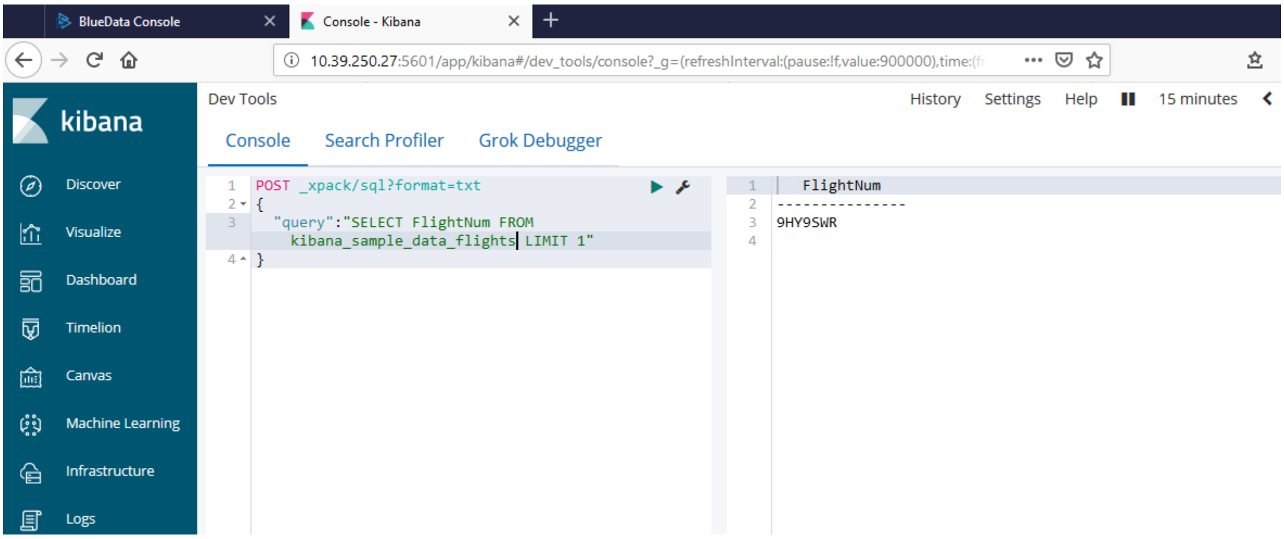


```
POST _xpack/sql
{
  "query":"DESCRIBE kibana_sample_data_flights"
}
```

```
{"columns":[{"name":"column","type":"keyword"},{"name":"type","type"
  :"keyword"},{"name":"mapping","type":"keyword"}],"rows":[["AvgTicketPrice"
  ,"REAL","FLOAT"],["Cancelled","BOOLEAN","BOOLEAN"],["Carrier","VARCHAR"
  ,"KEYWORD"],["Dest","VARCHAR","KEYWORD"],["DestAirportID","VARCHAR"
  ,"KEYWORD"],["DestCityName","VARCHAR","KEYWORD"],["DestCountry","VARCHAR"
  ,"KEYWORD"],["DestLocation","OTHER","UNSUPPORTED"],["DestRegion","VARCHAR"
  ,"KEYWORD"],["DestWeather","VARCHAR","KEYWORD"],["DistanceKilometers"
  ,"REAL","FLOAT"],["DistanceMiles","REAL","FLOAT"],["FlightDelay","BOOLEAN"
  ,"BOOLEAN"],["FlightDelayMin","INTEGER","INTEGER"],["FlightDelayType"
  ,"VARCHAR","KEYWORD"],["FlightNum","VARCHAR","KEYWORD"],["FlightTimeHour"
  ,"VARCHAR","KEYWORD"],["FlightTimeMin","REAL","FLOAT"],["Origin","VARCHAR"
  ,"KEYWORD"],["OriginAirportID","VARCHAR","KEYWORD"],["OriginCityName"
  ,"VARCHAR","KEYWORD"],["OriginCountry","VARCHAR","KEYWORD"]
  ,["OriginLocation","OTHER","UNSUPPORTED"],["OriginRegion","VARCHAR"
  ,"KEYWORD"],["OriginWeather","VARCHAR","KEYWORD"],["dayOfWeek","INTEGER"
  ,"INTEGER"],["timestamp","TIMESTAMP","DATE"]]}
```

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"
}
```



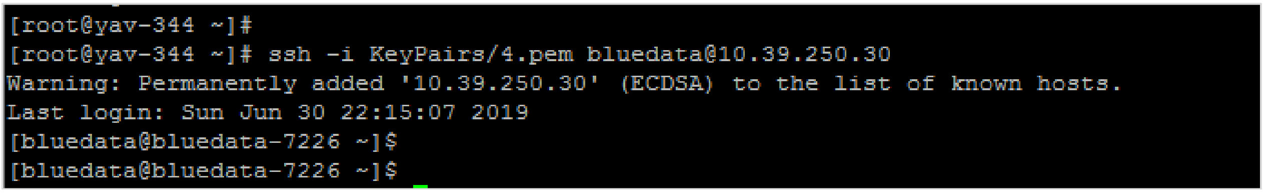
```
POST _xpack/sql?format=txt
{
  "query":"SELECT FlightNum FROM
    kibana_sample_data_flights LIMIT 1"
}
```

```
   FlightNum
---------------
9HY9SWR
```

4.6 Testing SQL CLI for ELK

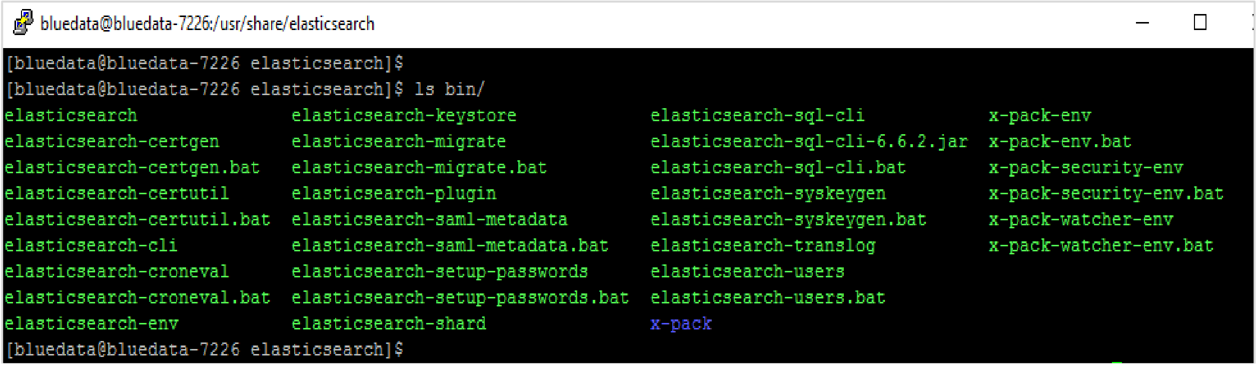
Go inside the container where Elasticsearch is installed.

```
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 ~]$
```

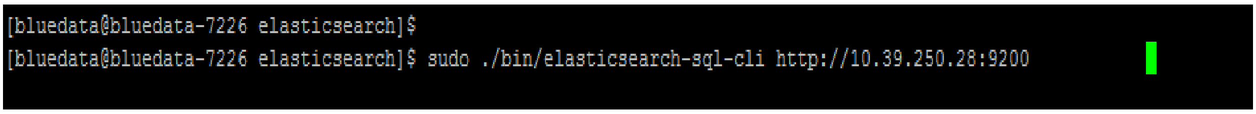
Go to the directory (/usr/share/elasticsearch) where Elasticsearch is installed then use ls command. We will be using elasticserach-sql-cli.



```
[bluedata@bluedata-7226 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]$
```

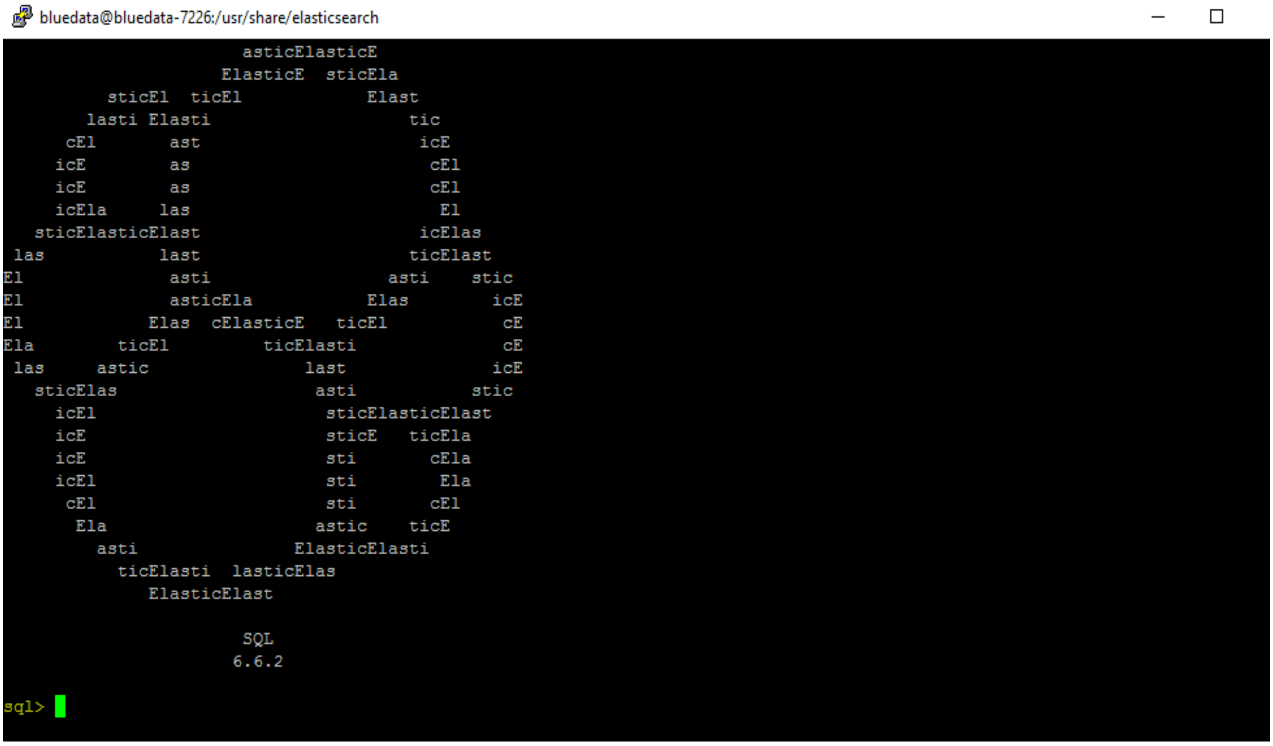
Execute the following command to open SQL CLI, which is installed with Elasticsearch. You can pass the URL of the Elasticsearch instance as a first parameter.

```
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
```

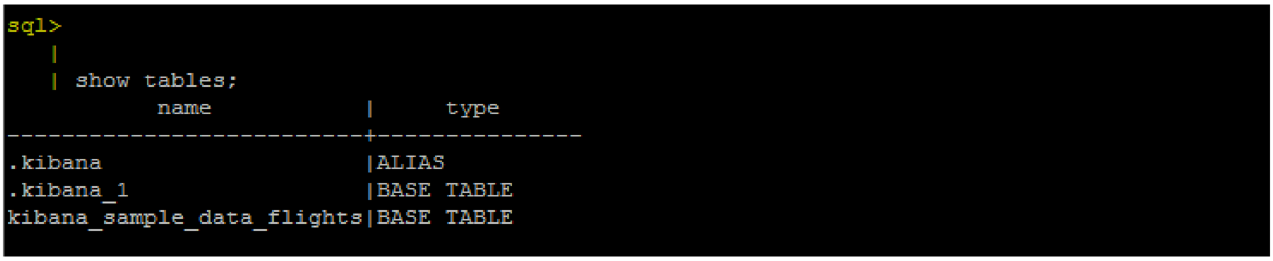
After executing above command, you will see the SQL CLI as given below:



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

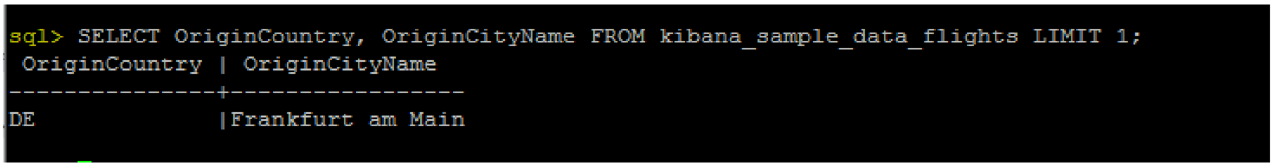
```
                       asticElasticE
                     ElasticE  sticEla
          sticEl  ticEl                Elast
        lasti Elasti                     tic
      cEl       ast                       icE
     icE        as                         cEl
     icE        as                         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
```