

Kibana overview

Kibana is to visualize the Elasticsearch data and navigate the Elastic Stack. Select the way to give shape to the data by starting with one question to find out where the interactive visualization will lead. Begin with the classic charts (histograms, line graphs, pie charts, sunbursts, and so on) or design visualization and add Geodata to any map. Searching Elasticsearch for specific log messages or strings within these messages is the bread and butter of Kibana. There is a new querying language called KQL (Kibana Querying Language). These are some stuff I perform for usage instruction. But there is a lot on the links.

- Discover
- Visualize
- Dashboard
- Settings

How to open Kibana

Step 1: - Login to the Azure portal

Step 2:- Turn on all the VMS and ELK VM to

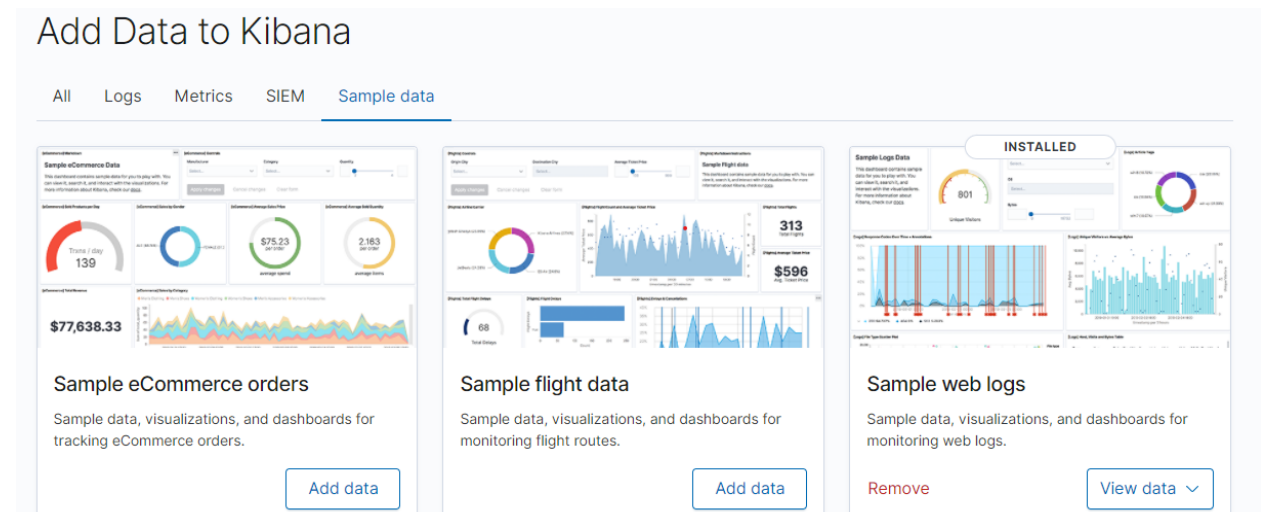
Step 3: - Open a Browser and paste the link in this pattern [ELK-public-IP]:5601/app/kibana:

Step 4:- Once logged in the Kibana dashboard will open

Add Sample Data

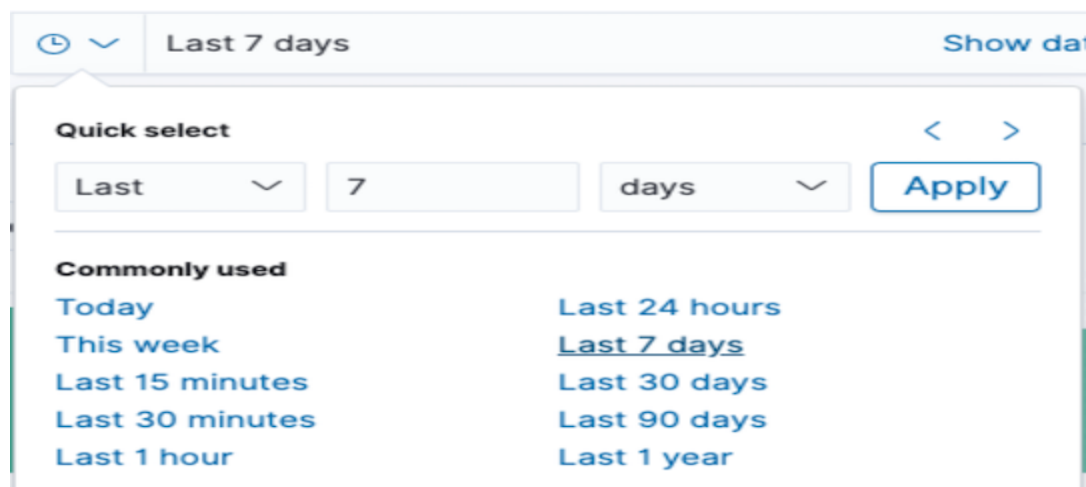
Sample data help to Visualize and investigate the functions of Kibana

1. On the home page, click Try our sample data.



Explore the Data

Data will be displayed over time and a table that lists the fields for each document that matches the index pattern. Able to filter the Data in timely manner



Viewing the Data

Through this kibana dashboard collection panels can be used to view and analyze the data. Panels contain visualizations, Interactive controls, Text, and more.



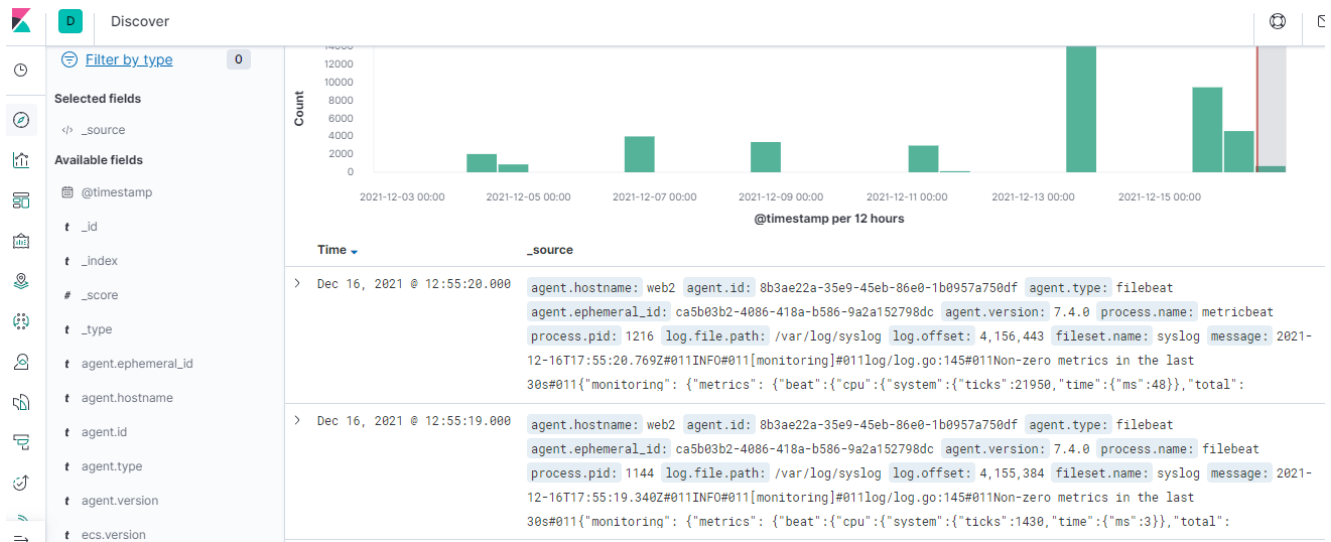
Create a visualization panel

Create a treemap panel that shows the top sales regions and manufacturers, then add the panel to the dashboard.

1. In the toolbar, click Edit.
2. On the dashboard, click Create visualization.

Time Stamps

Through Kibanana can check the data on a timely basis. Inspect Each value and the files that are receiving thorough telemetry.



Inspecting Each Data

Below it shows can inspect and able to download the data

[Logs] Unique Visitors vs. Average Bytes

View: Data 



Download CSV 

timestamp per 3 hours	Avg. Bytes	Unique Visitors	Count
2021-12-09 12:00	5,577.2	5	5
2021-12-09 15:00	7,448	1	1
2021-12-09 18:00	321	1	1
2021-12-09 21:00	6,100.1	10	10
2021-12-10 00:00	5,820.52	24	25
2021-12-10 03:00	4,779.475	61	61
2021-12-10			

Filters
co
KQL
Today
Show dates

Filters	co
geopip.continent_code.keyword	Filter results that contain geopip.continent_code.keyword
geopip.continent_code	Filter results that contain geopip.continent_code
geopip.country_code2.keyword	Filter results that contain geopip.country_code2.keyword
geopip.country_code2	Filter results that contain geopip.country_code2
geopip.country_code3.keyword	Filter results that contain geopip.country_code3.keyword
geopip.country_code3	Filter results that contain geopip.country_code3
geopip.country_name.keyword	Filter results that contain geopip.country_name.keyword
geopip.country_name	Filter results that contain geopip.country_name
geopip.dma_code	Filter results that contain geopip.dma_code
geopip.postal_code.keyword	Filter results that contain geopip.postal_code.keyword
geopip.postal_code	Filter results that contain geopip.postal_code
geopip.region_code.keyword	Filter results that contain geopip.region_code.keyword
geopip.region_code	Filter results that contain geopip.region_code

t auth

t bytes

t clientip

t geopip.city_name

t geopip.continent_code

t geopip.country_code2

t geopip.country_code3

t geopip.country_name

geopip.dma_code

vl1&q1&q2&pbx=1&bv=on.2,or,gc,r,pw,r,qf,cf,os&bkt=2414&bin=261" Mozilla/5.0 (iPhone; CPU iPhone

> May 27, 2019 @ 23:52:50.000 bytes: 65 agent: "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; YTB720; GTB7.2; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)" request: /category/electronics @version: 1 path: /home/ubuntu/apache-daily-access.log message: 200.48.47.210 - [27/May/2019:28:53:00] "GET /category/electronics HTTP/1.1" 200 65 "/category/office" Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; YTB720; GTB7.2; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)" request: /category/electronics @version: 1 path: /home/ubuntu/apache-daily-access.log message: 200.129.182.89 - [27/May/2019:28:46:20 +0000] "GET /category/electronics HTTP/1.1" 200 65 "/category/games" Mozilla/5.0 (iPhone; CPU iPhone OS 5_0_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9A405 Safari/7534.48.3" @timestamp: May 27, 2019 @ 23:46:20.000

May 27, 2019 @ 23:59:59.999 — Auto

timestamp per 30 minutes

<https://www.elastic.co/guide/en/kibana/current/discover.html>
<https://www.elastic.co/guide/en/kibana/current/index.html>