Applications Log Analysis and IS Policy Dashboard

Drubus Technologies Private Limited

Knowledge Document

By: Rishika Chaudhary

1. Installation of the required software

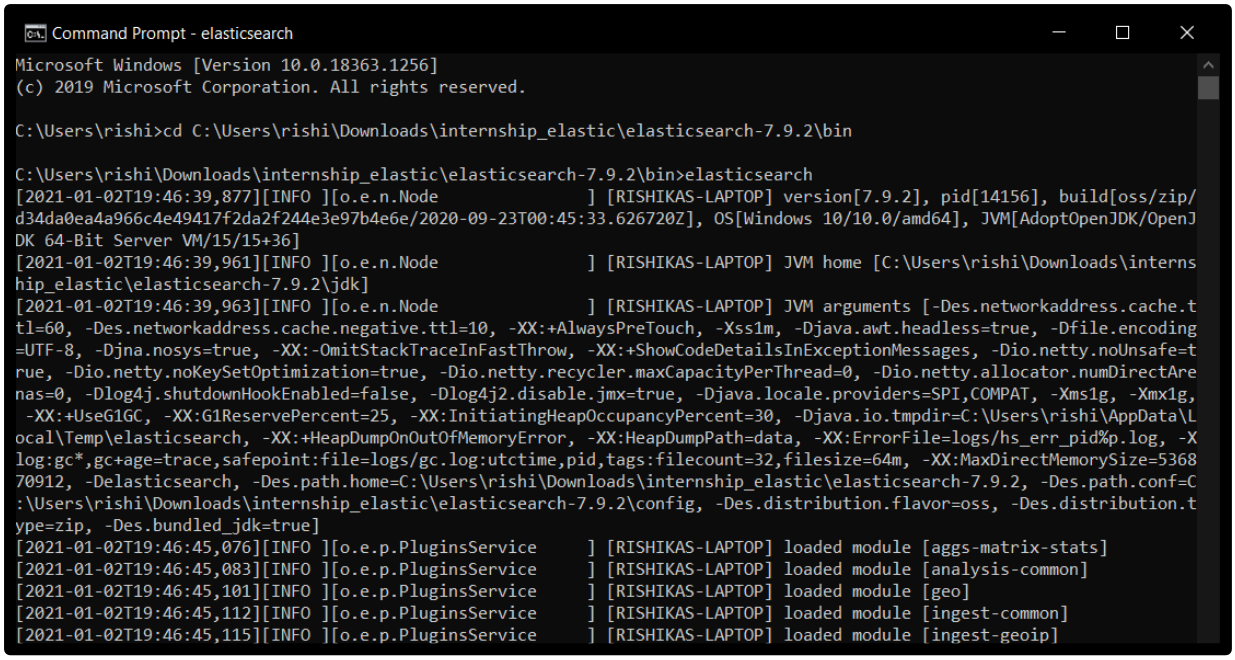
   Primary software used:
   ELASTIC SEARCH, LOGSTASH AND KIBANA

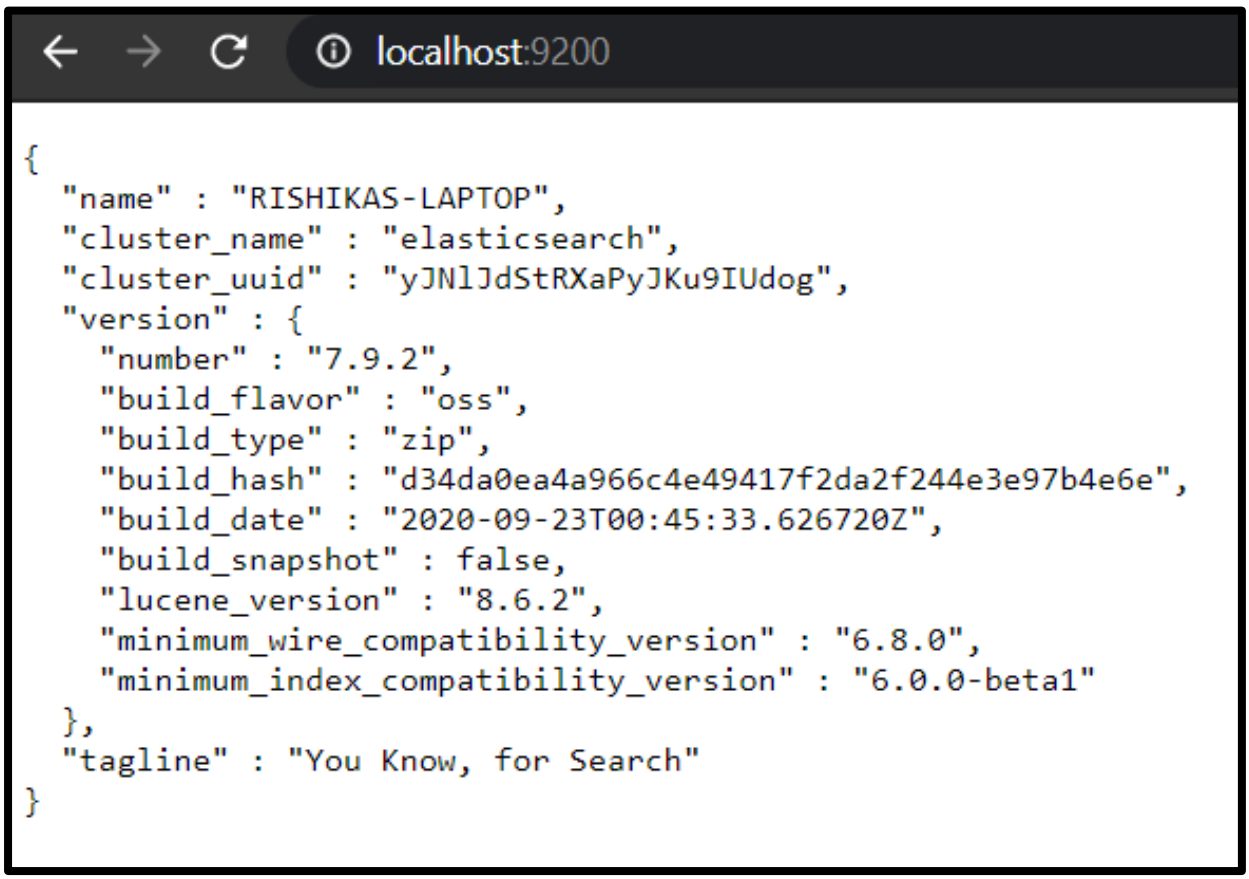
   1.1. Installing Elastic Search

   Elasticsearch is a highly scalable open-source full-text search and analytics engine. It allows you to store, search, and analyse big volumes of data quickly and in near real time. It is generally used as the underlying engine/technology that powers applications that have complex search features and requirements.

   - Go to the official site of elastic.co, search to set up elastic search
   - Choose the latest version of the software, and choose Windows.
   - Zip file will download, unzip the file in a folder.
   - Go to the unzipped folder named elastic search, copy the path of the bin folder.
   - Open the command prompt, copy the path there and run elastic search.
   - Run the local host 9200, and you can see if elastic search is running.
   - https://www.elastic.co/guide/en/elasticsearch/reference/current/setup.html
   - https://www.youtube.com/watch?v=8iXZTS7f_hY

Above links will help us download elastic search on windows, same can be done on MAC and linux, the steps are available on the official site of elastic search.


Command Prompt - elasticsearch
Microsoft Windows [Version 10.0.18363.1256]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Users\rishi>cd C:\Users\rishi\Downloads\internship_elastic\elasticsearch-7.9.2\bin
C:\Users\rishi\Downloads\internship_elastic\elasticsearch-7.9.2\bin>elasticsearch
[2021-01-02T19:46:39,877][INFO][o.e.n.Node] [RISHIKAS-LAPTOP] version[7.9.2], pid[14156], build[oss/zip/d34da0ea4a966c4e49417f2da2f244e3e97b4e6e/2020-09-23T00:45:33.626720Z], OS[Windows 10/10.0/amd64], JVM[AdoptOpenJDK/OpenJDK 64-Bit Server VM/15/15+36]
[2021-01-02T19:46:39,961][INFO][o.e.n.Node] [RISHIKAS-LAPTOP] JVM home [C:\Users\rishi\Downloads\internship_elastic\elasticsearch-7.9.2\jdk]
[2021-01-02T19:46:39,963][INFO][o.e.n.Node] [RISHIKAS-LAPTOP] JVM arguments [-Des.networkaddress.cache.ttl=60, -Des.networkaddress.cache.negative.ttl=10, -XX:+AlwaysPreTouch, -Xss1m, -Djava.awt.headless=true, -Dfile.encoding=UTF-8, -Djna.nosys=true, -XX:-OmitStackTraceInFastThrow, -XX:+ShowCodeDetailsInExceptionMessages, -Dio.netty.noUnsafe=true, -Dio.netty.noKeySetOptimization=true, -Dio.netty.recycler.maxCapacityPerThread=0, -Dio.netty.allocator.numDirectArenas=0, -Dlog4j.shutdownHookEnabled=false, -Dlog4j2.disable.jmx=true, -Djava.locale.providers=SPI,COMPAT, -Xms1g, -Xmx1g, -XX:+UseG1GC, -XX:G1ReservePercent=25, -XX:InitiatingHeapOccupancyPercent=30, -Djava.io.tmpdir=C:\Users\rishi\AppData\Local\Temp\elasticsearch, -XX:+HeapDumpOnOutOfMemoryError, -XX:HeapDumpPath=data, -XX:ErrorFile=logs/hs_err_pid%p.log, -Xlog:gc*,gc+age=trace,safepoint:file=logs/gc.log:utctime,pid,tags:filecount=32,filesize=64m, -XX:MaxDirectMemorySize=536870912, -Delasticsearch, -Des.path.home=C:\Users\rishi\Downloads\internship_elastic\elasticsearch-7.9.2, -Des.path.conf=C:\Users\rishi\Downloads\internship_elastic\elasticsearch-7.9.2\config, -Des.distribution.flavor=oss, -Des.distribution.type=zip, -Des.bundled_jdk=true]
[2021-01-02T19:46:45,076][INFO][o.e.p.PluginsService] [RISHIKAS-LAPTOP] loaded module [aggs-matrix-stats]
[2021-01-02T19:46:45,083][INFO][o.e.p.PluginsService] [RISHIKAS-LAPTOP] loaded module [analysis-common]
[2021-01-02T19:46:45,101][INFO][o.e.p.PluginsService] [RISHIKAS-LAPTOP] loaded module [geo]
[2021-01-02T19:46:45,112][INFO][o.e.p.PluginsService] [RISHIKAS-LAPTOP] loaded module [ingest-common]
[2021-01-02T19:46:45,115][INFO][o.e.p.PluginsService] [RISHIKAS-LAPTOP] loaded module [ingest-geoip]


localhost:9200
{
"name" : "RISHIKAS-LAPTOP",
"cluster_name" : "elasticsearch",
"cluster_uuid" : "yJNlJdStRXaPyJKu9IUdog",
"version" : {
"number" : "7.9.2",
"build_flavor" : "oss",
"build_type" : "zip",
"build_hash" : "d34da0ea4a966c4e49417f2da2f244e3e97b4e6e",
"build_date" : "2020-09-23T00:45:33.626720Z",
"build_snapshot" : false,
"lucene_version" : "8.6.2",
"minimum_wire_compatibility_version" : "6.8.0",
"minimum_index_compatibility_version" : "6.0.0-beta1"
},
"tagline" : "You Know, for Search"
}

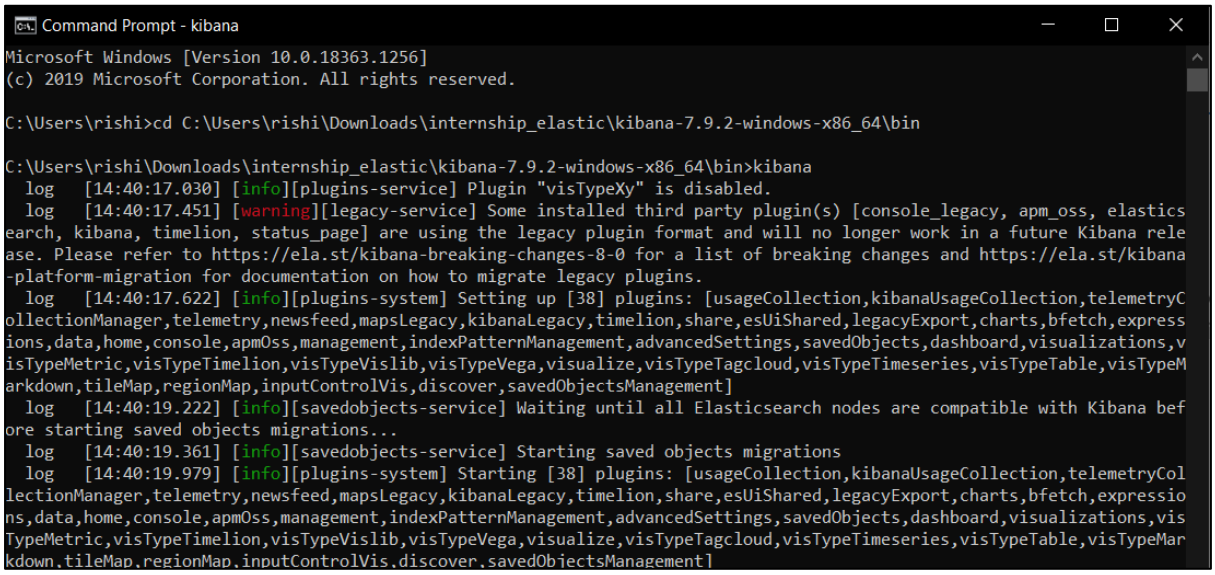
1.2. Installing Kibana

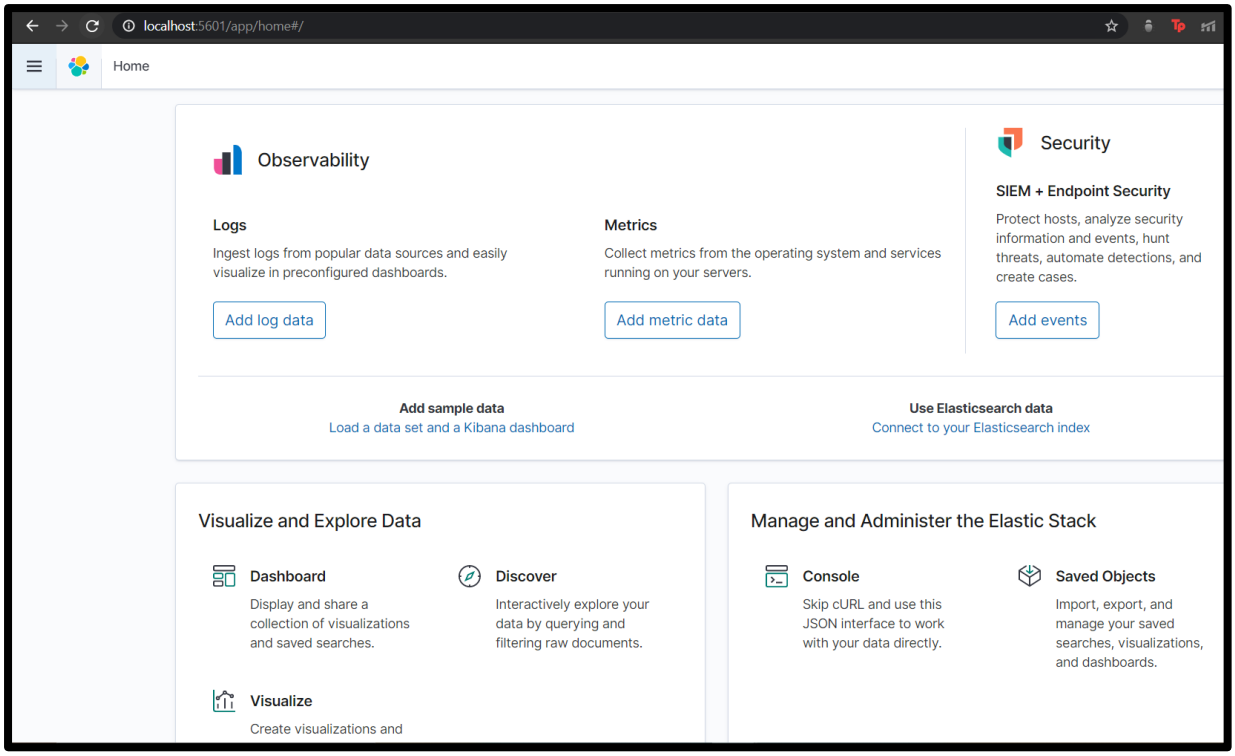
Kibana is an open-source frontend application that sits on top of the Elastic Stack, providing search and data visualization capabilities for data indexed in Elasticsearch. Commonly known as the charting tool for the Elastic Stack (previously referred to as the ELK Stack after Elasticsearch, Logstash, and Kibana), Kibana also acts as the user interface for monitoring, managing, and securing an Elastic Stack cluster — as well as the centralized hub for built-in solutions developed on the Elastic Stack.

- Follow same steps as above, download the zipped file and unzip it.
- Copy the bin path from the unzipped kibana folder.
- Run it on the command prompt and search for local host 5601.
- If you see the interface of kibana on the server, then it has been connected with elastic search and is ready to use.
- https://www.elastic.co/guide/en/kibana/current/install.html
- https://www.youtube.com/watch?v=qvHJ8lLAdXs

Note:

Build flavor of elastic search is **'oss'**, Kibana should have the same flavor, otherwise it would not connect with the search engine. Careful while selecting the version also, both should have the same version number, in this case it was **7.9.2.**





1.3. Installing Logstash

Logstash is a free and open server-side data processing pipeline that ingests data from a multitude of sources, transforms it, and then sends it to your favourite "stash."

- Follow the same steps as above to install Logstash on your systems.
- The zip file for the latest version would be available on elastic.co.
- Certain changes might have to be made in the config file, which can be modified using the links given below.
- Logstash helps in the mapping which would be required when uploading our log files into the search engine.
- https://www.elastic.co/guide/en/logstash/current/installing-logstash.html
- https://www.youtube.com/watch?v=WGNHLcG_OrQ

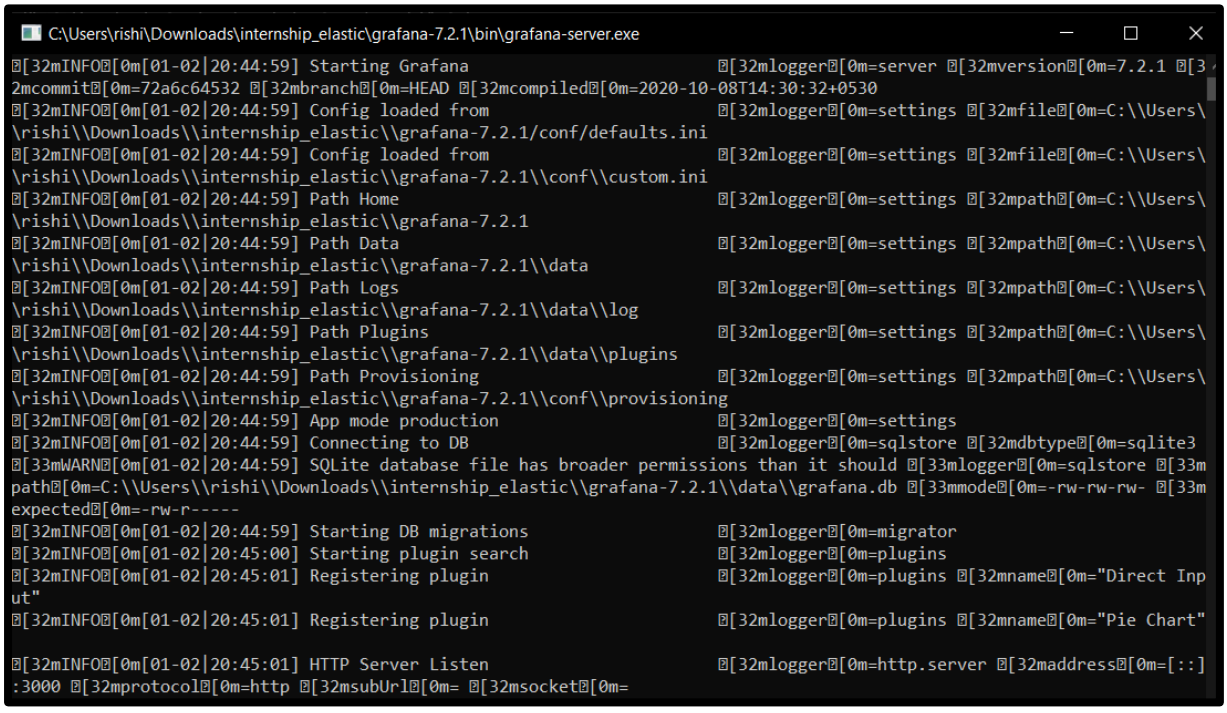
Secondary Software used:

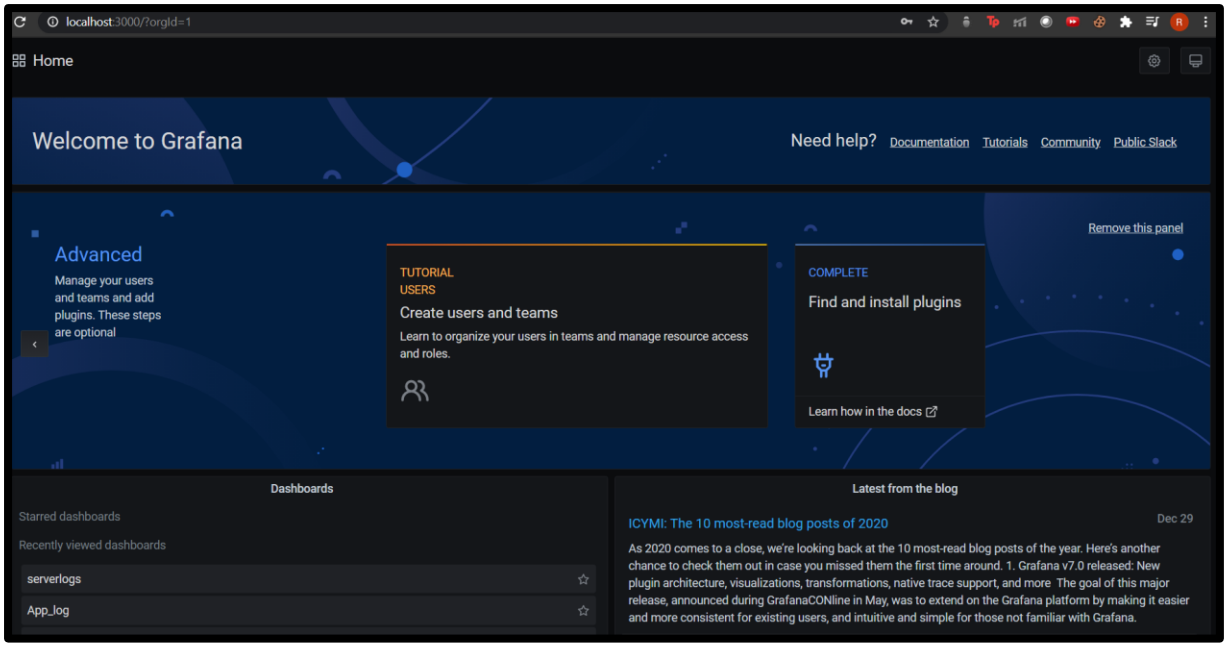
Grafana

1.4. Installing Grafana

Grafana has become the world's most popular technology used to compose observability dashboards with everything from Prometheus & Graphite metrics, to logs and application data to power plants and beehives.

- Go to the official site on Grafana, and download the Grafana installer.
- Unzip the folder, and go to the bin folder.
- Run the Grafana server application file in this folder.
- Run the local host 3000 to get Grafana interface.
- https://grafana.com/docs/grafana/latest/installation/windows/
- https://www.youtube.com/watch?v=grppSMHLueA

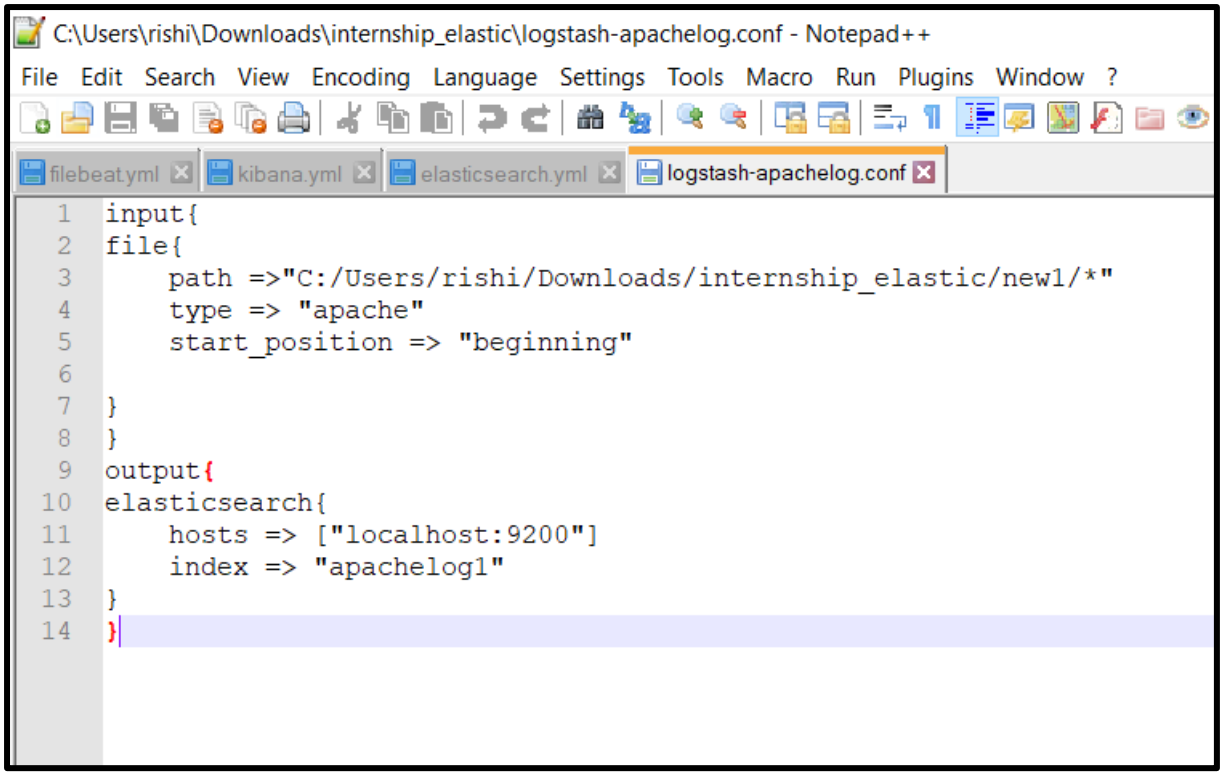


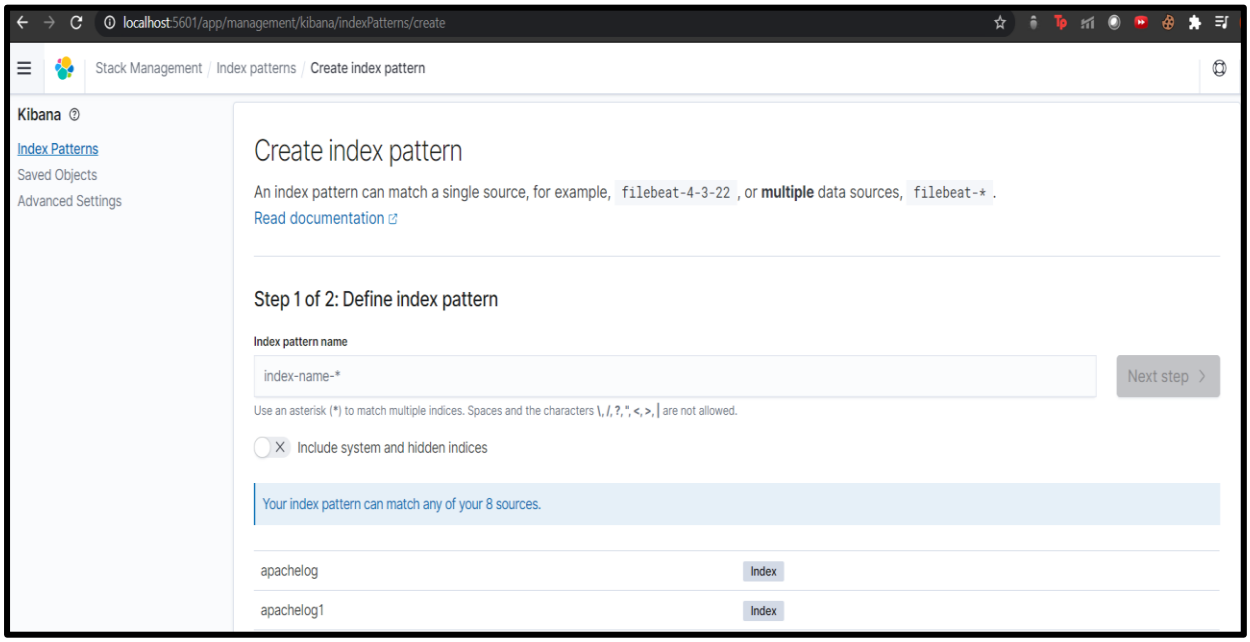


2. Uploading the data onto Elastic Search

   The next task is to load the log files on to the search engine.

   - In Kibana, in the stack management tab, there is an option to create index pattern.
   - We need to create this index pattern, in order to load the data into Kibana which would be connected to elastic search.
   - To load the data, we first need to make a config file.
   - In the file we need to give two fields, input and output.
     •The input contains, the file path, file type and the start position.
     •The output contains the host and index name.
   - We will save this file in the same folder with our other software.
   - Then we would run this file using the command prompt, detailed instructions are given in video link below.
   - After this, we refresh our index pattern page and select the required index name and the data would get loaded on Kibana.
   - https://www.youtube.com/watch?v=5UsFBqoQ_90

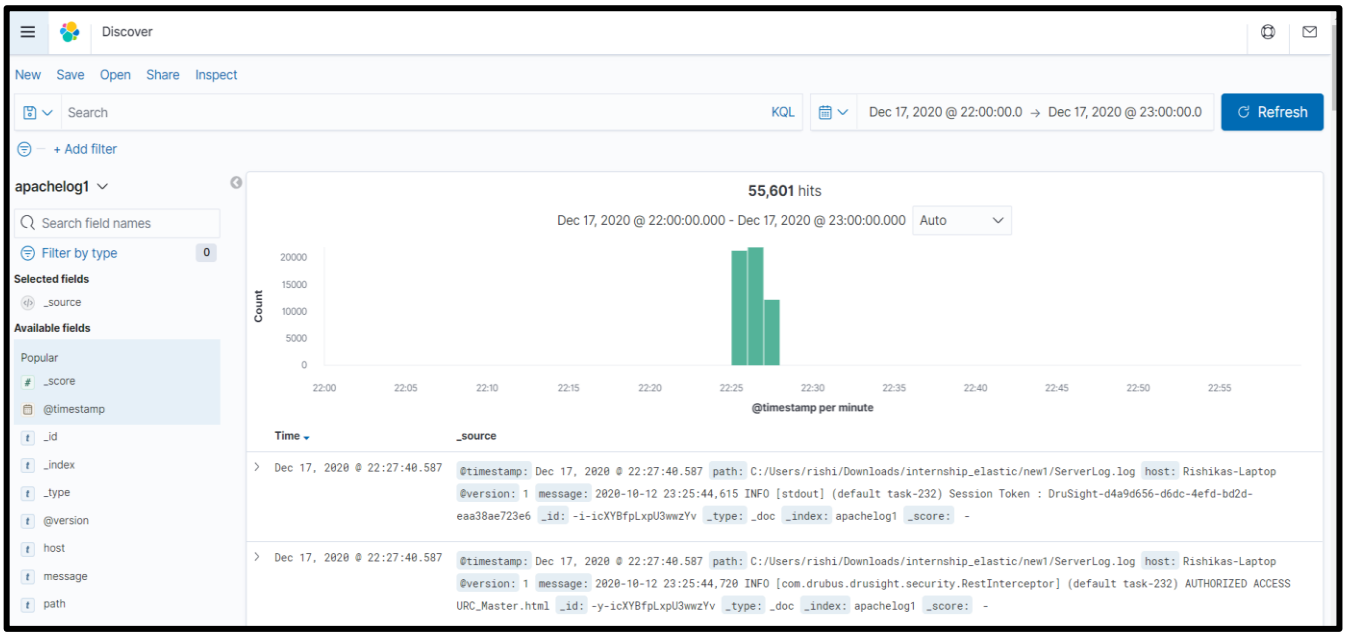

C:\Users\rishi\Downloads\internship_elastic\logstash-apachelog.conf - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
filebeat.yml
kibana.yml
elasticsearch.yml
logstash-apachelog.conf
input{
file{
path =>"C:/Users/rishi/Downloads/internship_elastic/new1/*"
type => "apache"
start_position => "beginning"
}
}
output{
elasticsearch{
hosts => ["localhost:9200"]
index => "apachelog1"
}
}


localhost:5601/app/management/kibana/indexPatterns/create
Stack Management / Index patterns / Create index pattern
Kibana
Index Patterns
Saved Objects
Advanced Settings
Create index pattern
An index pattern can match a single source, for example, filebeat-4-3-22 , or multiple data sources, filebeat-* .
Read documentation
Step 1 of 2: Define index pattern
Index pattern name
index-name-*
Next step
Use an asterisk (*) to match multiple indices. Spaces and the characters \, /, ?, ", <, >, | are not allowed.
Include system and hidden indices
Your index pattern can match any of your 8 sources.
apachelog
Index
apachelog1
Index

3. Analysing the data and start with Visualisation in Kibana

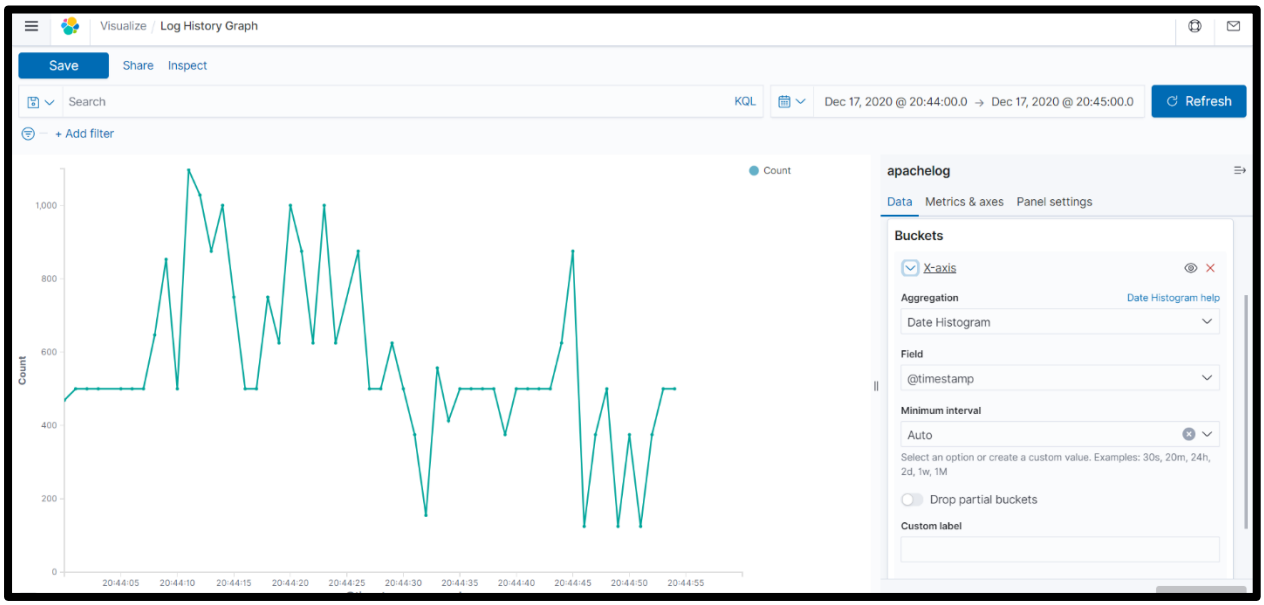
3.1. Analysing the log file

- Now that we have added our index into Kibana, we are ready to analyse it.
- Go to discover tab, which would be on the left side of the interface where we can select which data we want to visualise.
- After selecting the file, it may show a message ‘Expand your data range, no data available’. This would mean that for the default time range, our data is not present.
- On the upper right side, we can change the data-time range and then observe our data.
- After selecting the correct time range, we would get a total number of hits in that time range and al the fields of the data.
- We can start visualising it, log data would contain fields like ip, host, message, timestamp, path, etc.
- We have a filter tab on the top, from which we choose which data we want to display and then we can keep a record of the total number of hits with that filter.
- The most important field is the message field, we can filter the message keyword for words like error, server shutdown, authorise access and get their time series graph.
- All the messages in the log file were new to me, so I searched them on the internet to derive meaning from them.



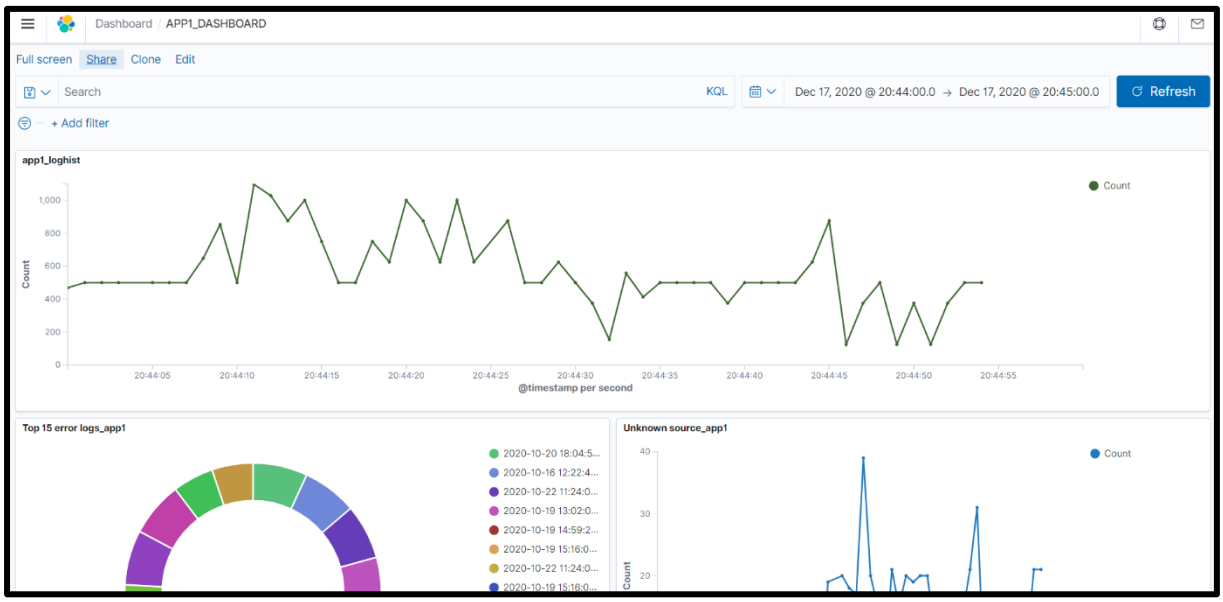
3.2. Visualising the Data

- After spending some time on analysing the data and deciding on what graphs to plot, we can now visualise it.
- To implement this, we head over to the visualise tab, there click on create visualisation.
- Then we would get a bunch options to choose from, we can choose any graph that we want to. As an example, let us first choose the line graph option.
    - After selecting the line graph, it presents an option for us to choose the data.
    - Having choosing the data we get our graph.
    - To get the pattern of the time series total log count hits, we select the appropriate time range we need.
    - For this graph we need time stamp as our x axis, so on the right under the buckets tab, we select the x axis aggregation to be date histogram, which would automatically choose the field as the timestamp and we can get our graphs.
    - Similarly, we can get other graphs by adding filters, which can be chosen on the upper left side.



4. Dashboarding in Kibana

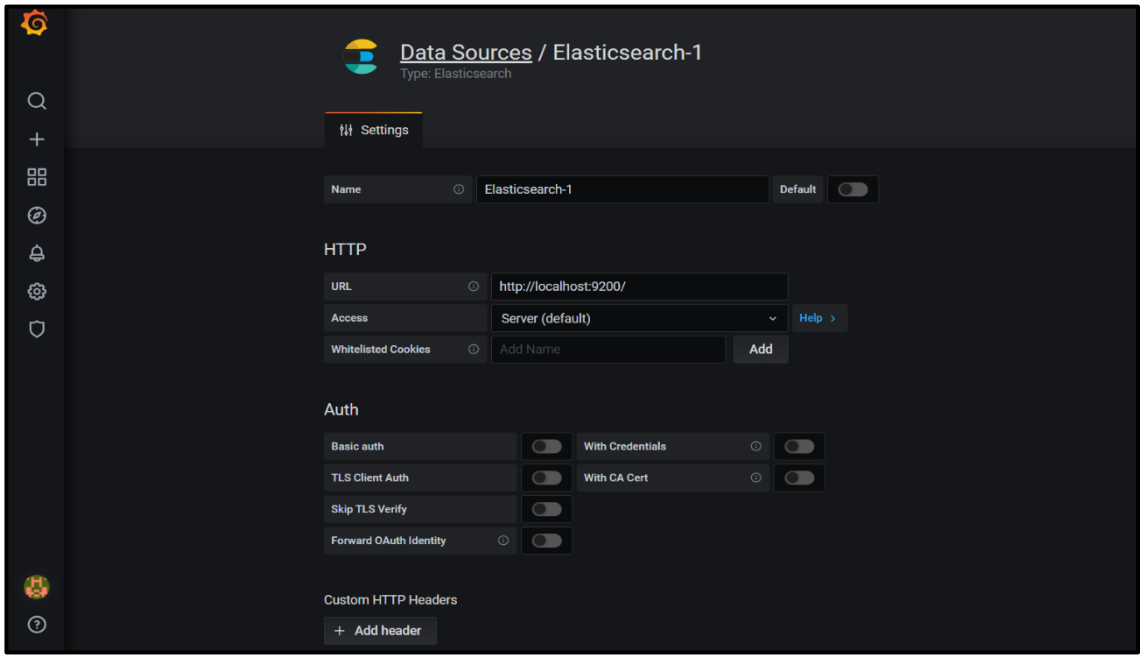
- After having made the required visualisations, we need to display them on the dashboard.
- Choose the dashboard tab on the left, select create new dashboard and we get an empty dashboard.
- Then we have an add option on the top, we can add our visualisations which are already made.
- The whole dashboard is set on a single time range, if we change the time range of the dashboard all the graphs would change accordingly, therefore sometimes for a specific time range, we can have certain graphs which do not have any values.
- We can change the size of each graph and choose to display it, how we want it.

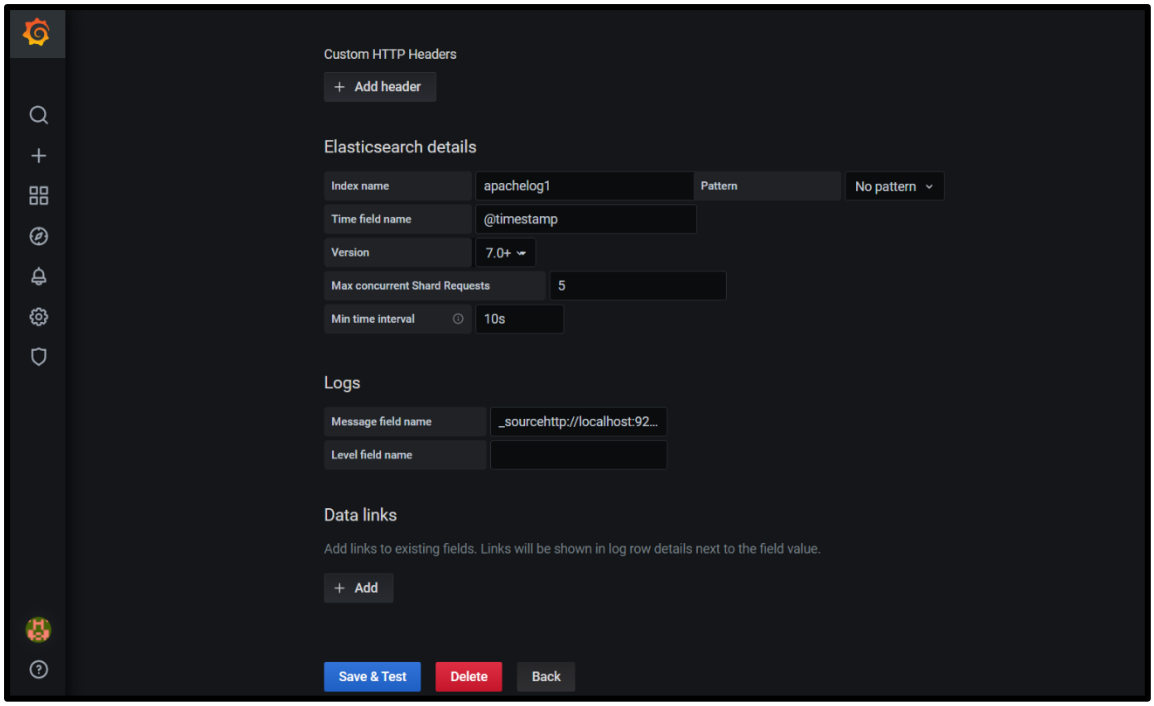


5. Visualising in Grafana

5.1. Loading the Data on Grafana

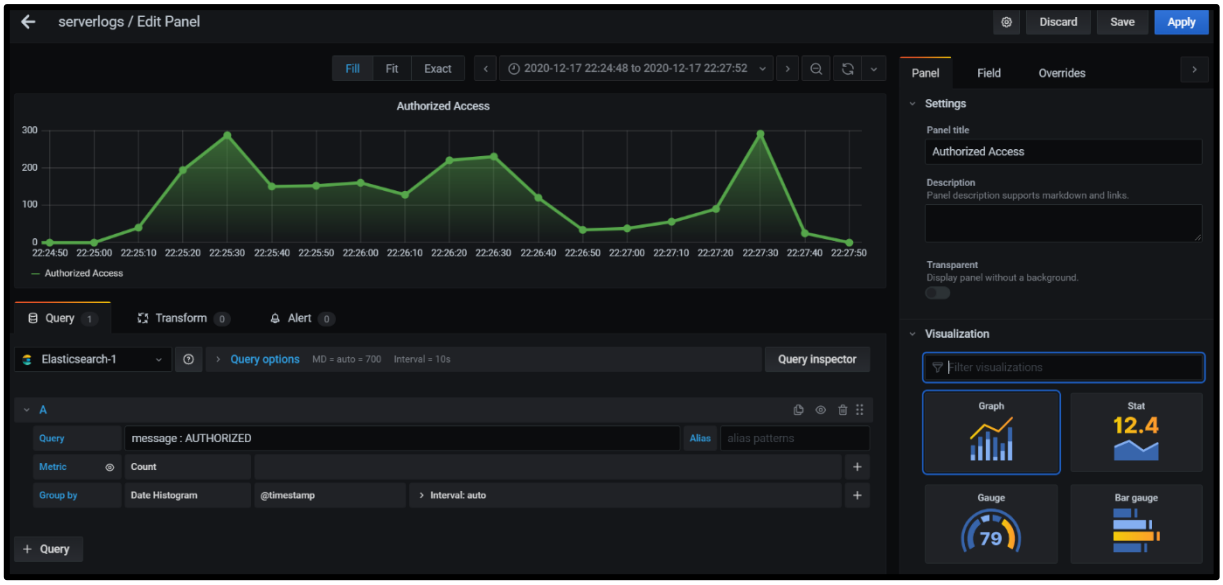
- After installing Grafana, we need to connect the dataset which we uploaded on elastic search.
- In Grafana we have a lot of options from where we connect our data sources like MySQL, Prometheus, elastic search etc.
- We go to the configuration tab, and choose the data source option, then choose add data source.
- Choose elastic search, and fill in the necessary details, like the images below, then click on save and test.



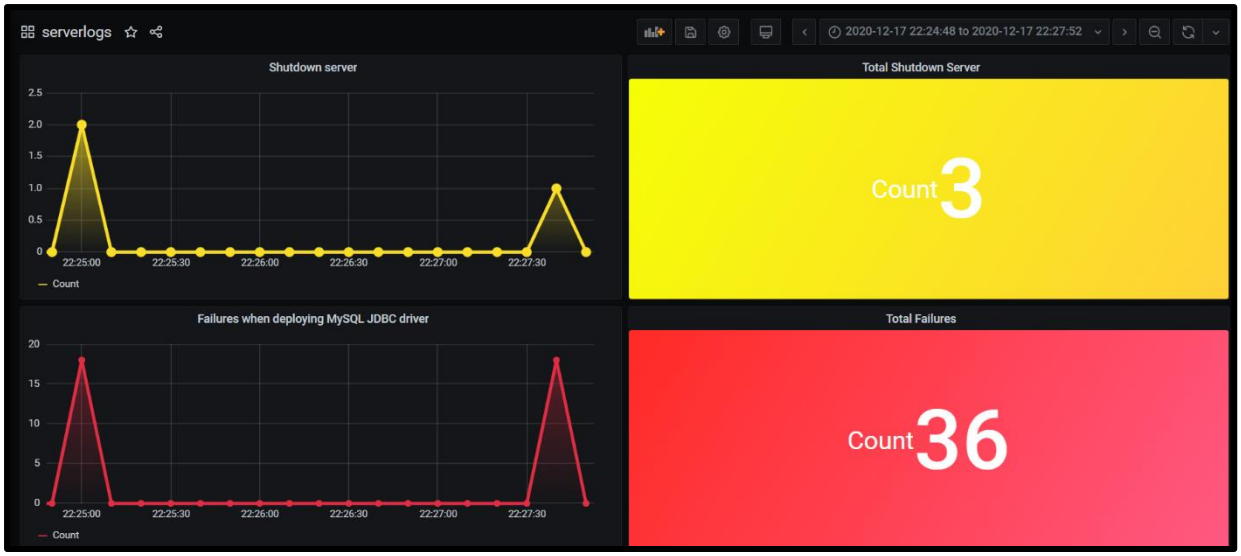


5.2. Graphs and Dashboard

- We will make similar graphs as we did in Kibana, click on the plus sign on the left side column, it is the create tab and select dashboard.
- After that click on add new panel, then an interface with different types of graph options would open up. Choose the data source which you want to visualise, under the query tab and also adjust the time range so we get the data.
- After acquiring the data, we choose the type of graph we want and play around with display options to make it look presentable.
- Like we filtered in Kibana, we query the message field to obtain the desired graphs.
- Save the graphs on the same dashboard, adjust the dimensions of each graph.



SERVER LOGS DASHBOARD



APPLICATION LOGS DASHBOARD