**Make Analysis**

Using

**Kibana Dashboard**

ELK stack helps us in different ways. Once we dump the data into elasticsearch engine from different sources, we will use kibana to visualize the logs/data

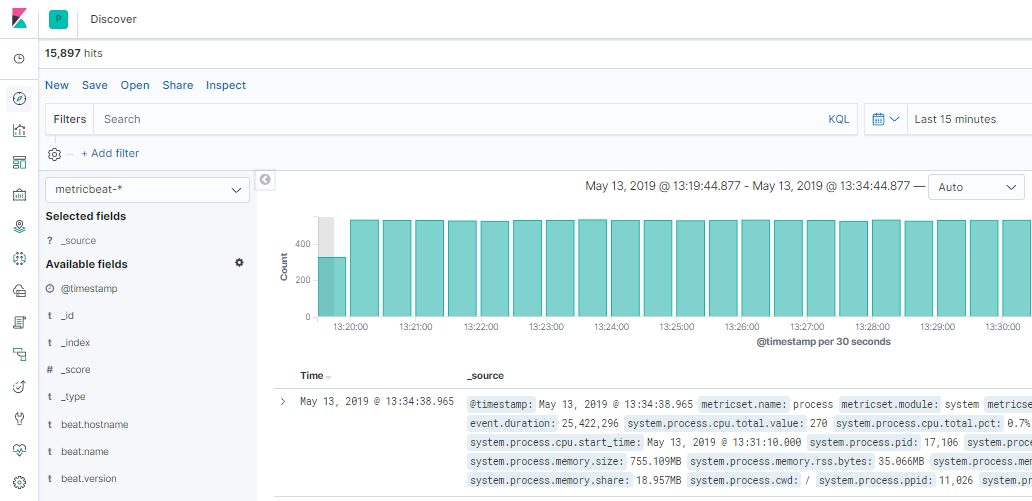
We have kibana up and running in the production environment. In order to use it access the below URL.

[http://Kibana.balluun.com](http://kibana.balluun.com)

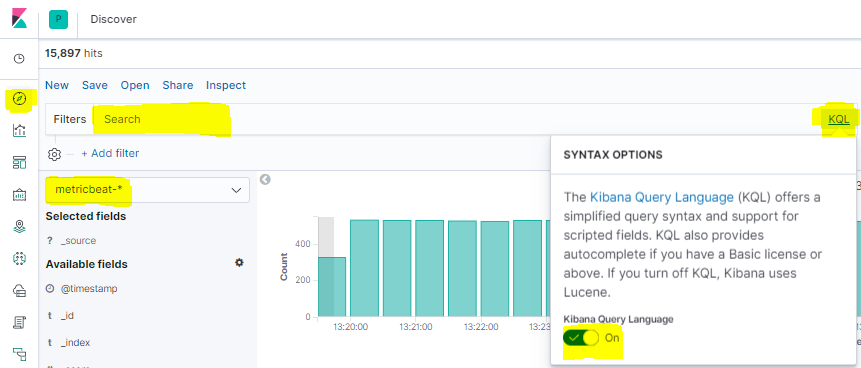
Above URL prompts for basic authentication enter the required credentials and login into kibana dashboard.

**Analyzing the logs:**

This screenshot refers to how normal kibana dashboard appears on the home page.

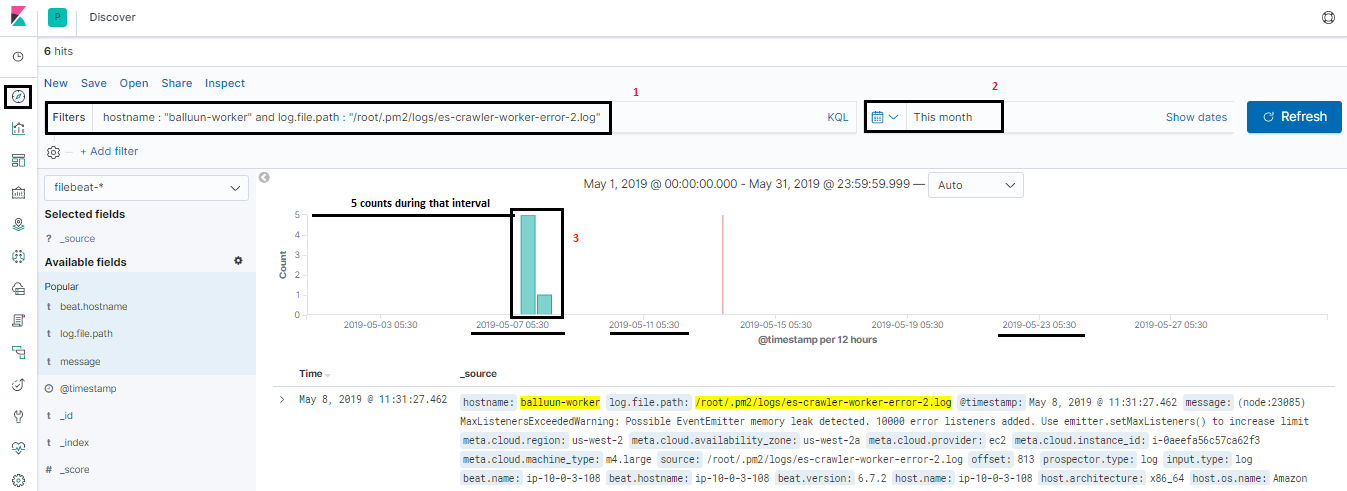
****

Let’s have a deep look into all fields and available options.



1. Discover option used to search the logs
2. We need to select the source. Here we have 2 sources metricbeat and filebeat
   1. **Metricbeat:** This will store all prod server metrics (CPU, Memory, Disk utilization, N/W In&Out)
   2. **Filebeat:** This will store application logs like Web, API, Worker, Rabbit-MQ and Redis server logs.
3. Once you selected the log source, click on KQL to get the suggestions before forming queries. If we enable this feature it will provide syntax on searching any kind of log.
4. **SEARCH BAR:** This is the area we will enter our query.

Below is the example to do some basic analysis on worker server logs.



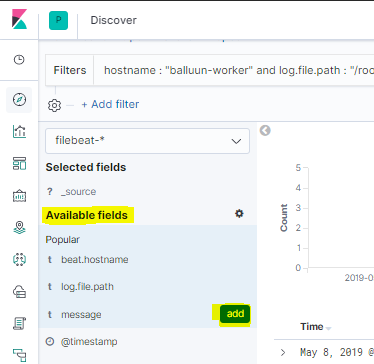
1. Form a query
2. Select time range

When clicking on search it will get the logs by making a query to elasticsearch engine with that time period.

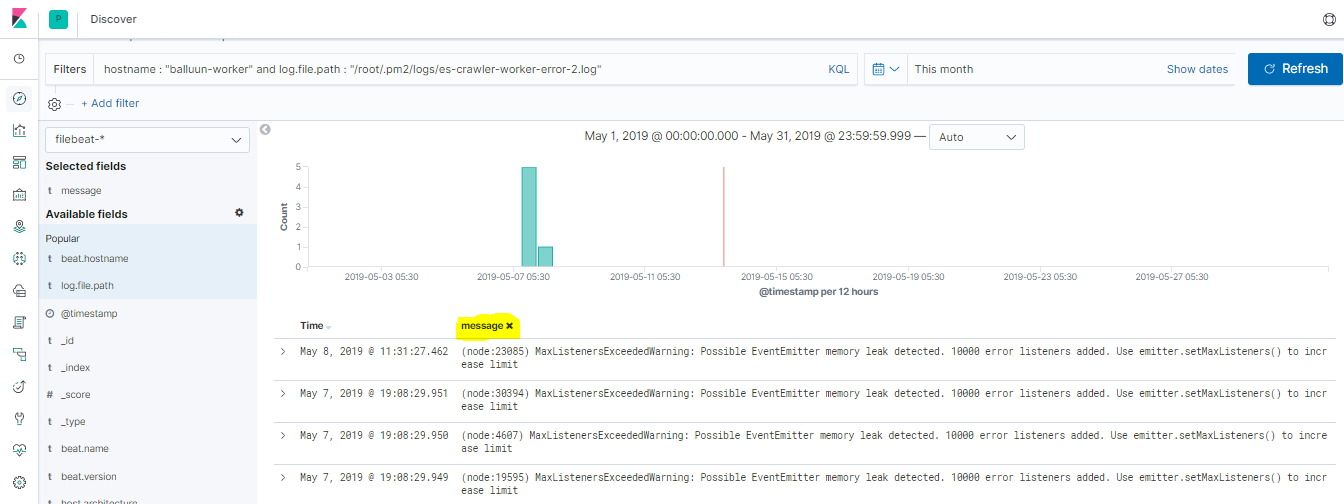
1. Bars indicate no. of times that query matched and count. Counts, we can see the left side and timing we can see the below to bars.

**Adding custom fields to view:**

If we see above dashboards we will be having all unnecessary fields. We may get confused while making some analysis. If you just wanted to see the message you customize the view.



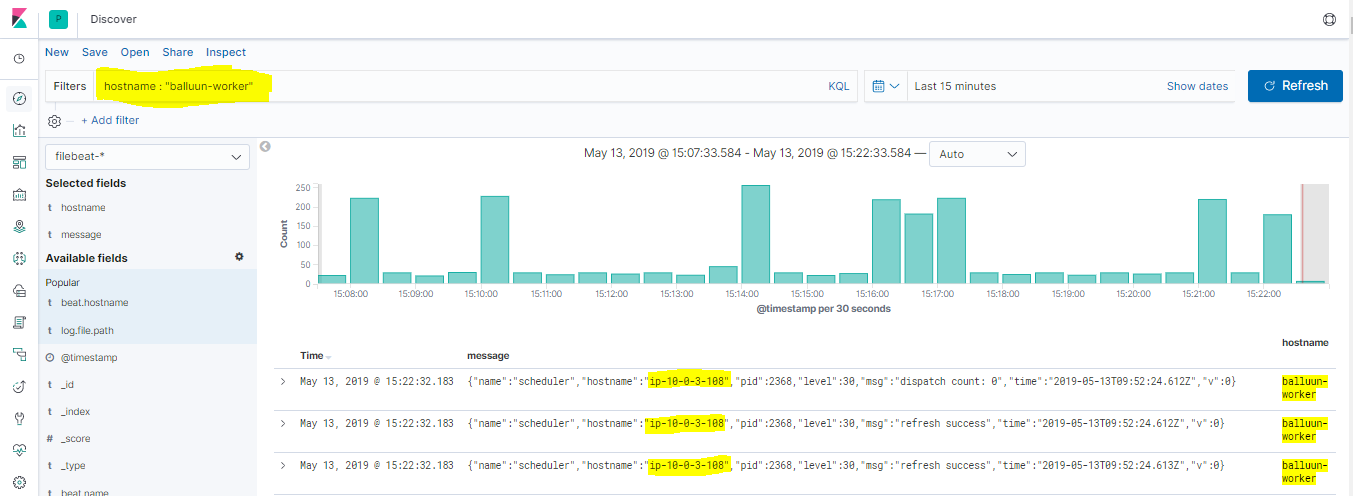
In the available fields, search your custom field and when you place the mouse over there it will show add button and just click on it. After clicking on it Kibana view will be changed to like below.



**Custom fields from filebeats:**

As we are dumping each server log files into elasticsearch we need a way to filter the server level. So we have added one custom field in each server and we can customize like this.

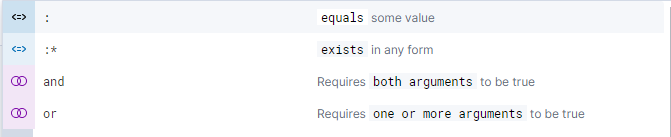
Query: hostname: “balluun-worker” / hostname: “balluun-mq”



It will apply the filter it will get the data for those specific fields only.

**Kibana filters:**

We have the basic filters in kibana to form the query and get the required data.



When you want to match field value exactly we will “:” or if it is similar “:\*”

Example:

* hostname : “balluun-worker”
* hostname :\* “balluun-worker”
* hostname : “balluun-worker” and log.file.path : “/var/log/rabbitmq/\*.log”
* hostname and log.file.path : "balluun-worker"

Note: AND can be used only when both perfectly match. OR can be used when any one of its matches.

It’s better to enable KQL to get the suggestions.

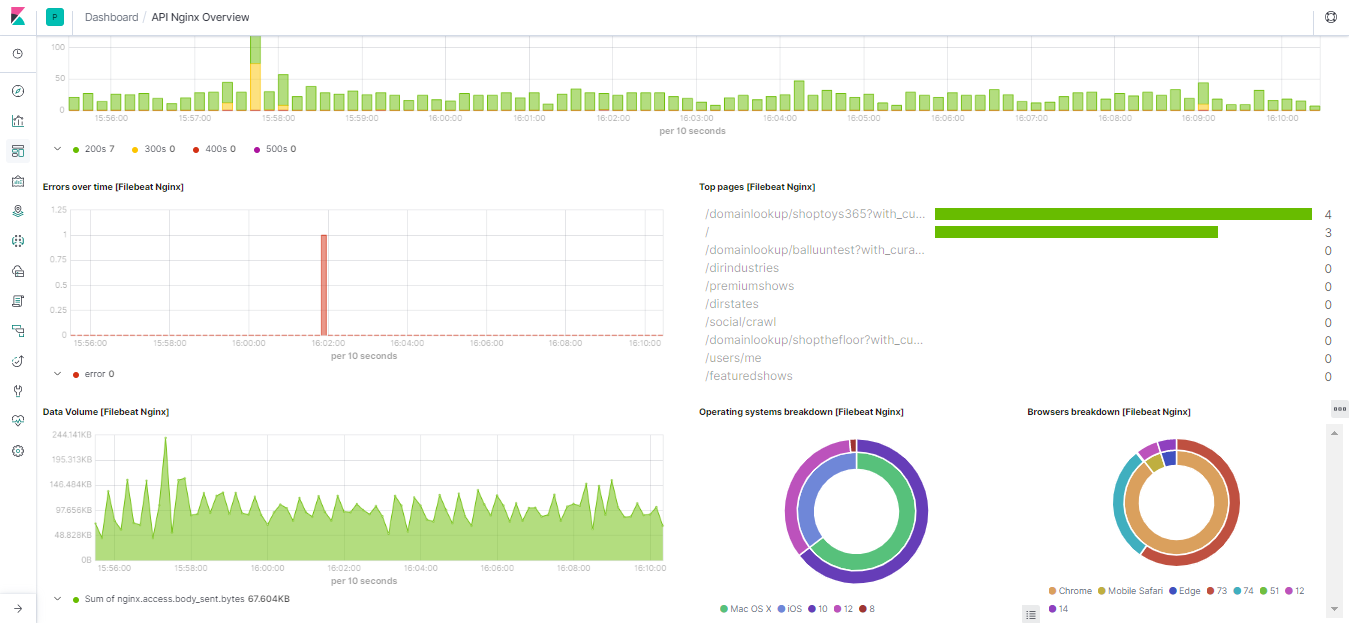
**Kibana Dashboards for Log analysis**

Currently we have 9 different dashboards for production environment.

1. [API Nginx Overview](http://kibana.balluun.com/app/kibana#/dashboard/55a9e6e0-a29e-11e7-928f-5dbe6f6f5519)
2. [API-Nginx Access and error logs](http://kibana.balluun.com/app/kibana#/dashboard/046212a0-a2a1-11e7-928f-5dbe6f6f5519)
3. [API-Nginx URL Explorer](http://kibana.balluun.com/app/kibana#/dashboard/ML-Nginx-Remote-IP-URL-Explorer)
4. [Balluun Web Dashboard](http://kibana.balluun.com/app/kibana#/dashboard/Filebeat-Apache2-Dashboard)
5. [Production Servers Overview](http://kibana.balluun.com/app/kibana#/dashboard/79ffd6e0-faa0-11e6-947f-177f697178b8)
6. [Rabbit-MQ Overview](http://kibana.balluun.com/app/kibana#/dashboard/38fa6940-7261-11e9-abc9-e353fafaff8f)
7. [Redis Logs Dashboard](http://kibana.balluun.com/app/kibana#/dashboard/7fea2930-478e-11e7-b1f0-cb29bac6bf8b)
8. [Redis Overview Dashboard](http://kibana.balluun.com/app/kibana#/dashboard/AV4YjZ5pux-M-tCAunxK)
9. [Whole Production Servers](http://kibana.balluun.com/app/kibana#/dashboard/Metricbeat-system-overview)

**1. API Nginx Overview:**

This Dashboard gives us an overview on current API behavior. Like What is the IP source, access URL’s, response codes, and browsers information.



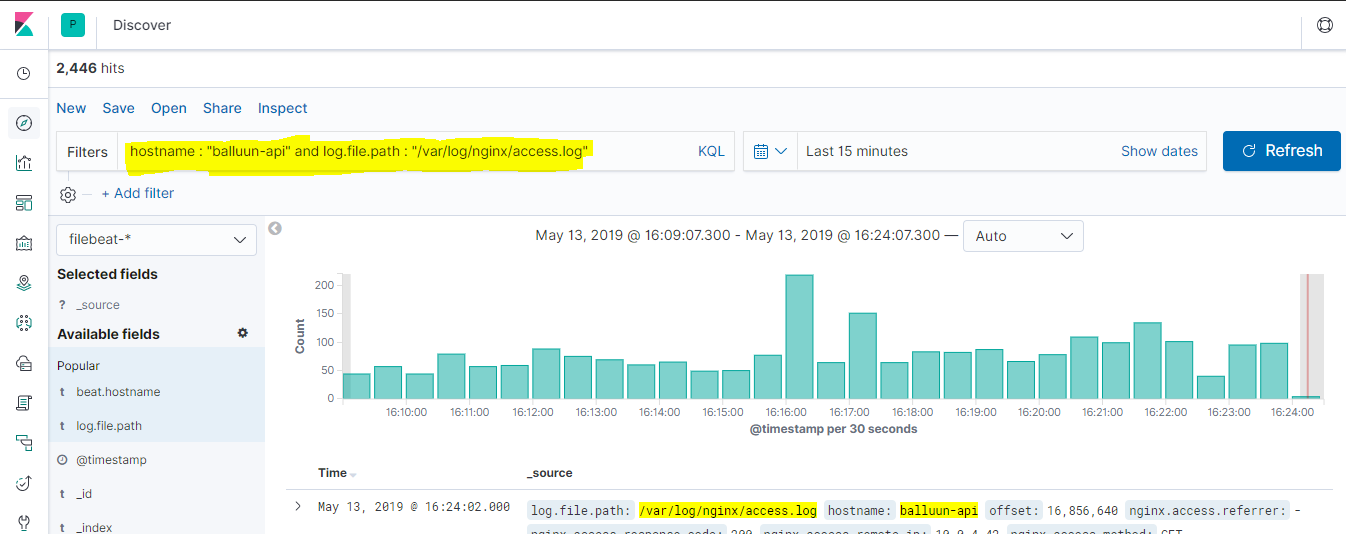
If we go through each dashboard it has so much information

1. Access maps (As our API internal use we do not have much access locations)
2. Response codes (200, 300, 400, 500)
3. Errors (Nginx error logs)
4. Top pages being used
5. Data volume (amount of data from request body)
6. Operating system information and browsers information.

**Analysis in Discover:**

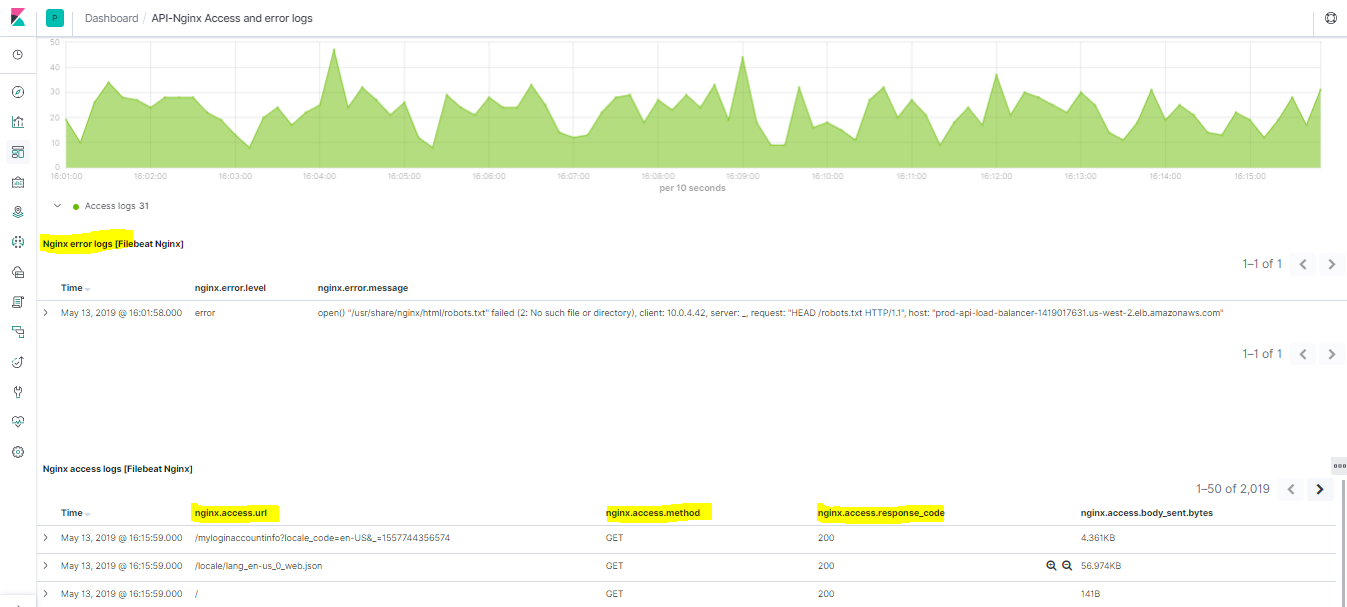
Use the below query to see access logs or error logs in Discover section.

**Query:** hostname : "balluun-api" and log.file.path : "/var/log/nginx/access.log"



**2. API-Nginx Access and Error Logs**

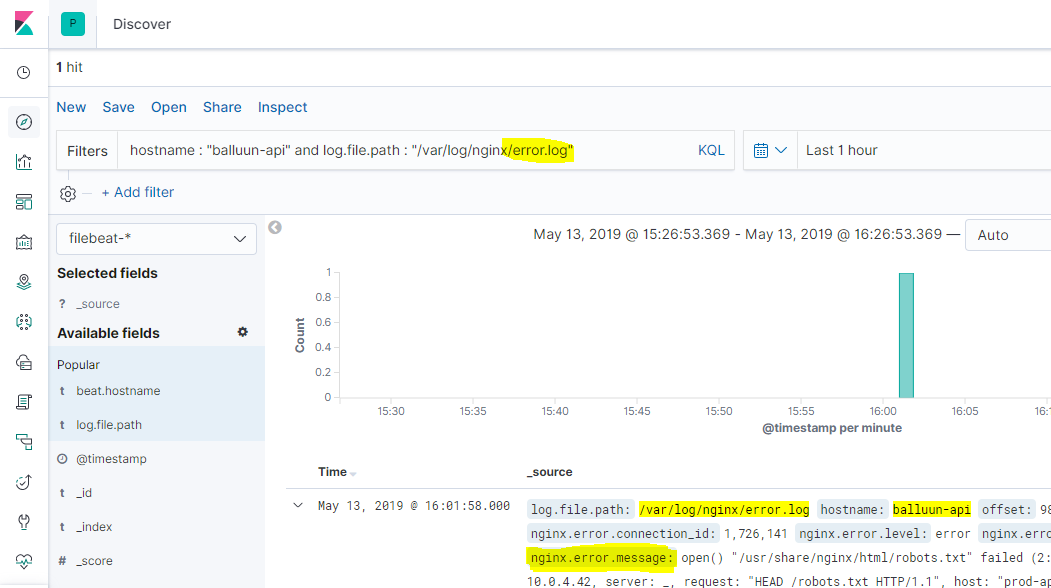
This dashboard brief about the API access and error logs information. In addition to that we could see what kind of pages API talking to, what is the response code and methods it is getting.



**Analysis in Discover:**

Use the below query to see error logs in Discover section.

**Query:** hostname : "balluun-api" and log.file.path : "/var/log/nginx/error.log"

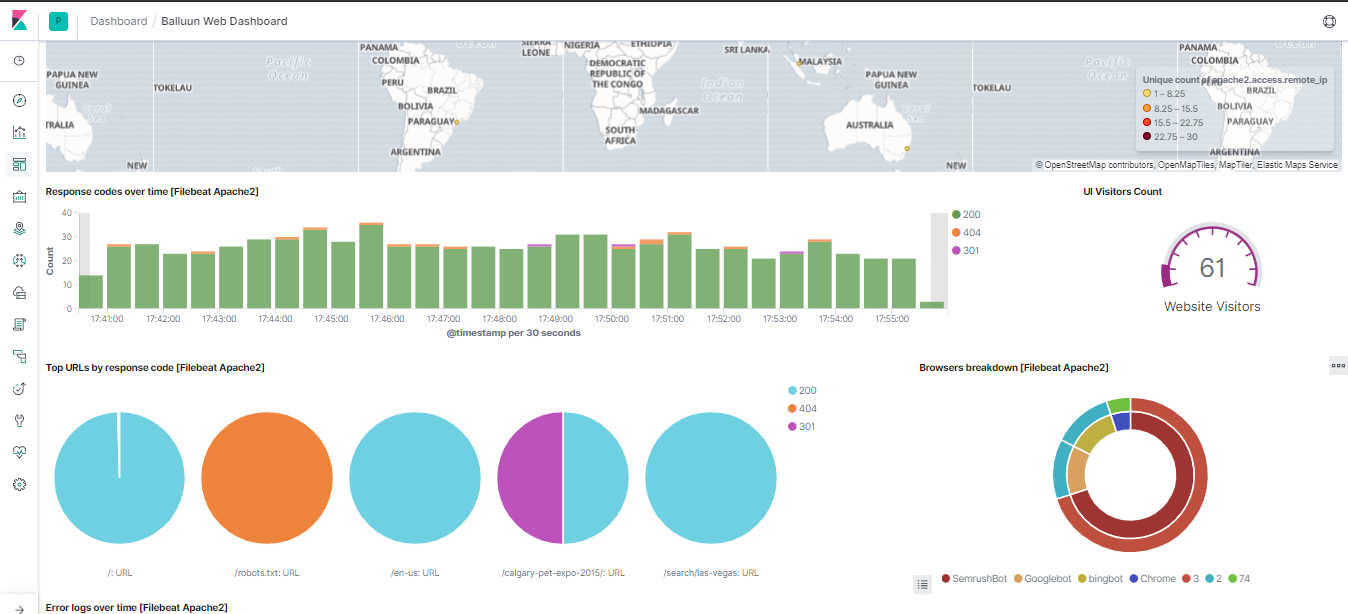


**3. API-Nginx URL Explorer:**

This dashboard was very similar to the above dashboards but additionally, it provides some information like how many times this page is calling in each API call.



**4. Balluun Web Dashboard:**

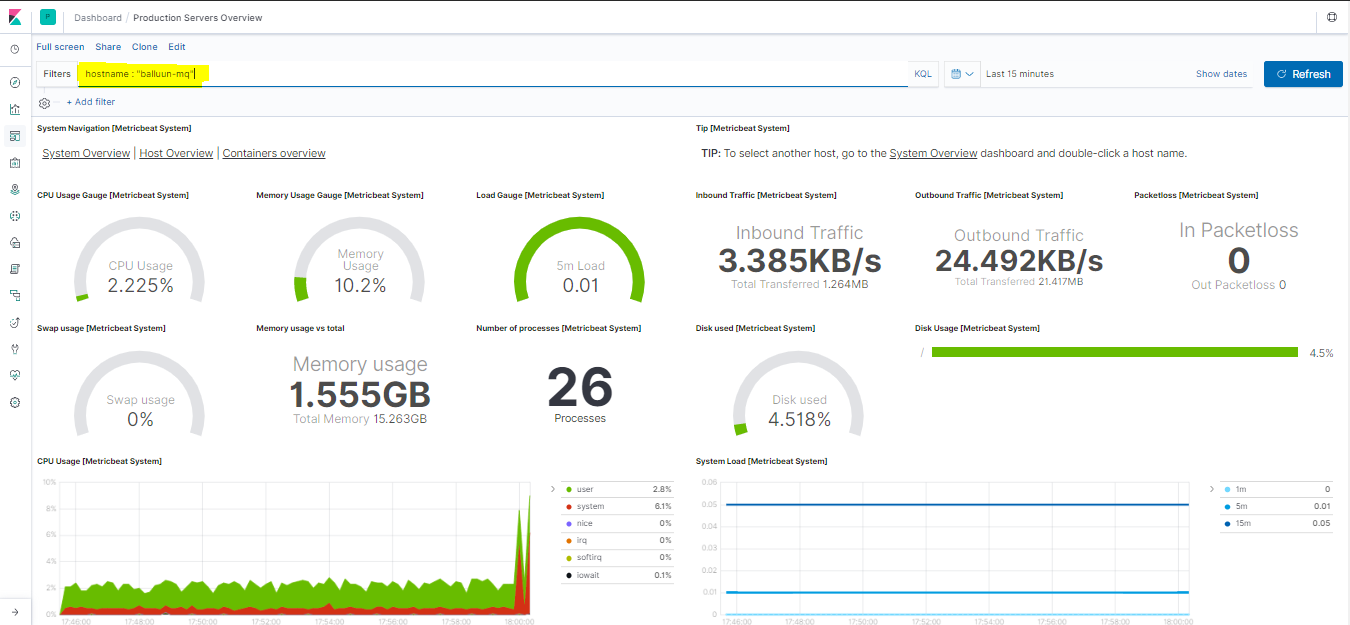


Balluun Web Dashboard describes the following things in production environment.

1. Access location of application End-Users
2. Response codes over the calls
3. Website visitors count
4. Top pages accessing by the users
5. What kind of browsers they are using
6. Is the application has any errors while serving the requests.

**5. Production server overview:**

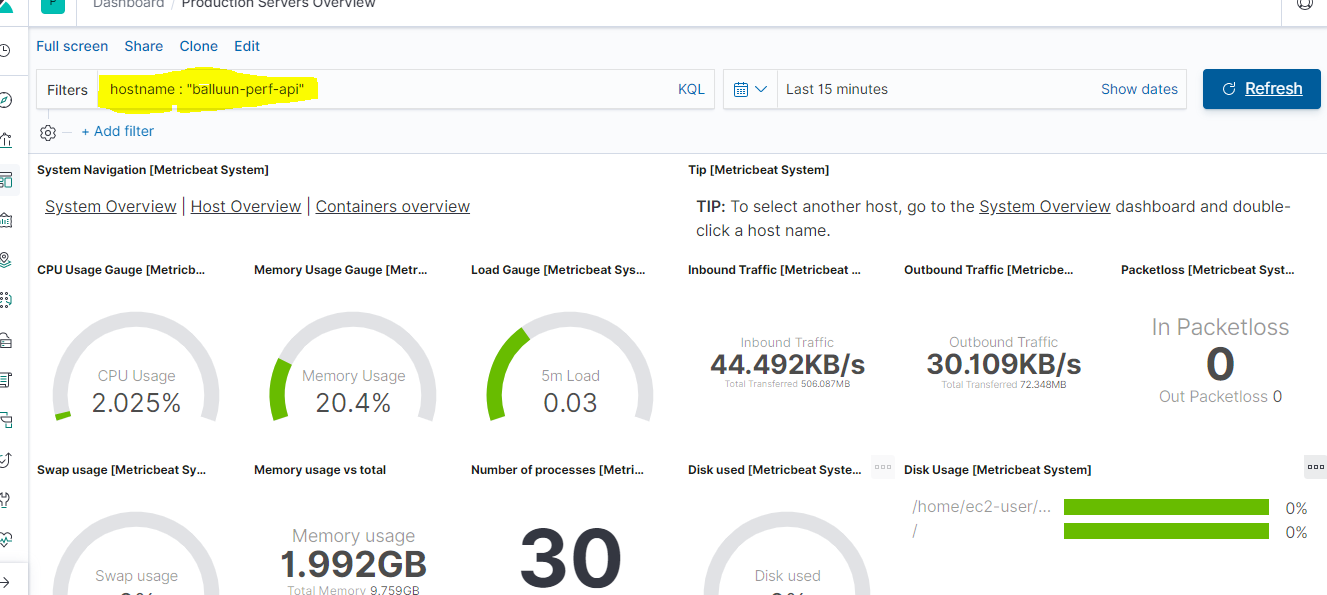
This Dashboard has a complete view of each server running in the production.



When we open, it will show metrics for any one of the servers (**balluun-mq** server in the above dashboard) health with the below metrics in a certain period.

1. CPU Avg Utilization
2. RAM Utilization
3. Load of the current server
4. Inbound traffic
5. Outbound traffic
6. Is there any Packet loss
7. Swap usage
8. RAM utilized / Total Ram
9. How many processes running
10. How much disk it is utilizaed
11. In-depth usage of CPU
12. In-depth usage of RAm
13. Network Traffic In & Out flow
14. Top processes CPU and RAM usage
15. Network utilization.

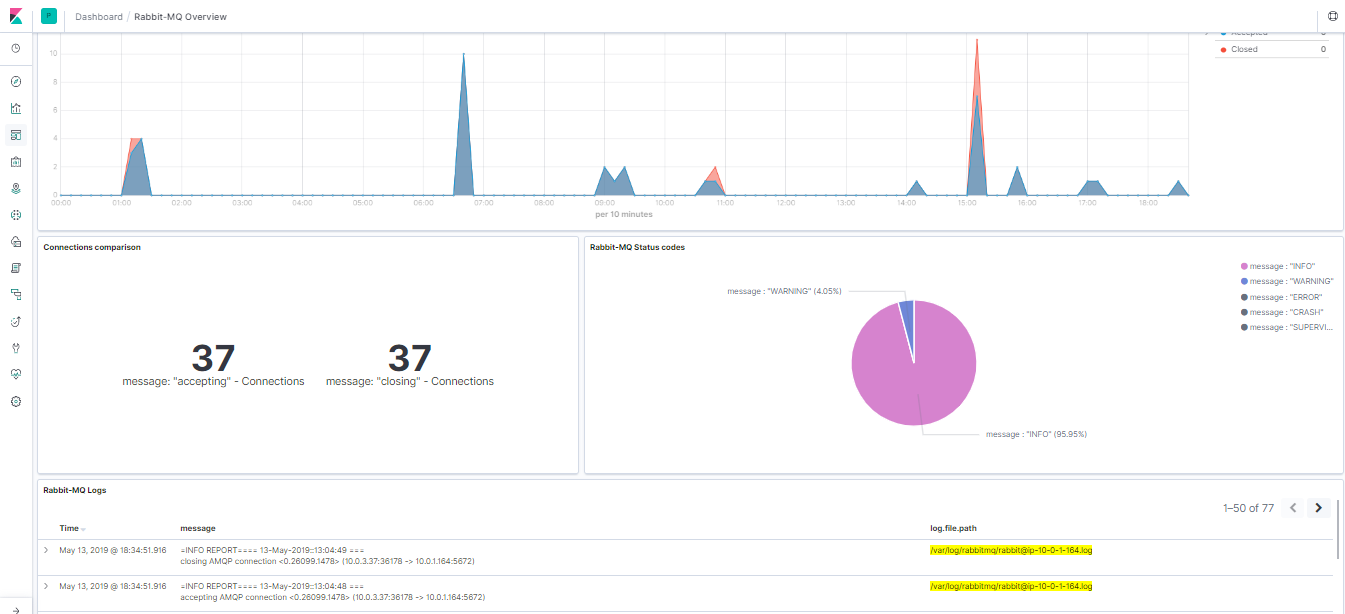
This Dashboard was designed in a very generic way if you want to see any other server metrics, just change hostname in the filter.



Like that, we can change to any server in the prod.

**6. Rabbit-MQ Overview:**

This Dashboard completely describes Rabbit MQ working status like how many connections it is accepting and closing, is there any latency in closing the request, Info / Warning / Error Status.

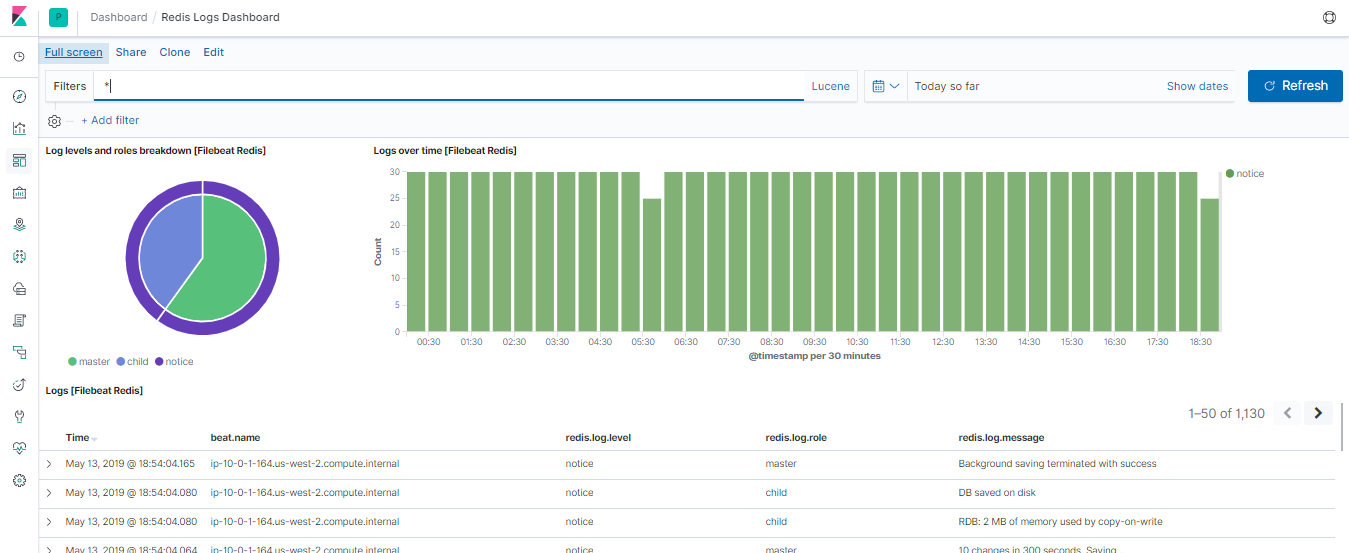


It has the following things

1. Connections accept and closing status (Graphical view for latency)
2. Total connections accepted and closed
3. Info and Warning percentages throughout the day
4. Live logs for Rabbit-MQ server.

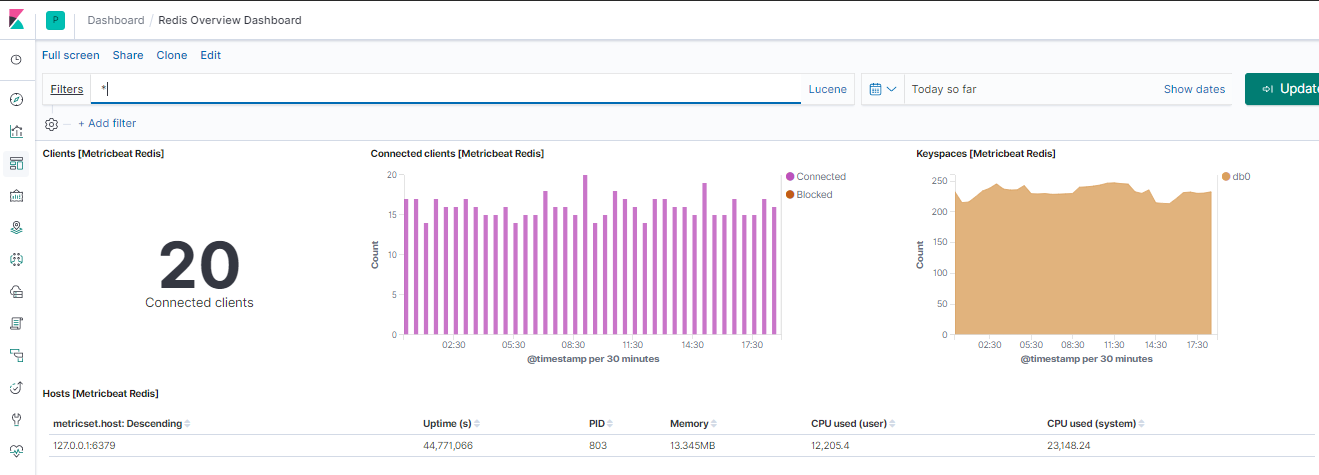
**7. Redis Logs Overview**

This Dashboard is very similar to Rabbit MQ, it will provide complete logs on the Redis server.



**8. Redis Overview**

This is just to see connected clients and some additional info about Redis



**9. Whole Production Servers Overview**

This Dashboard provides an overview of servers overview.

