

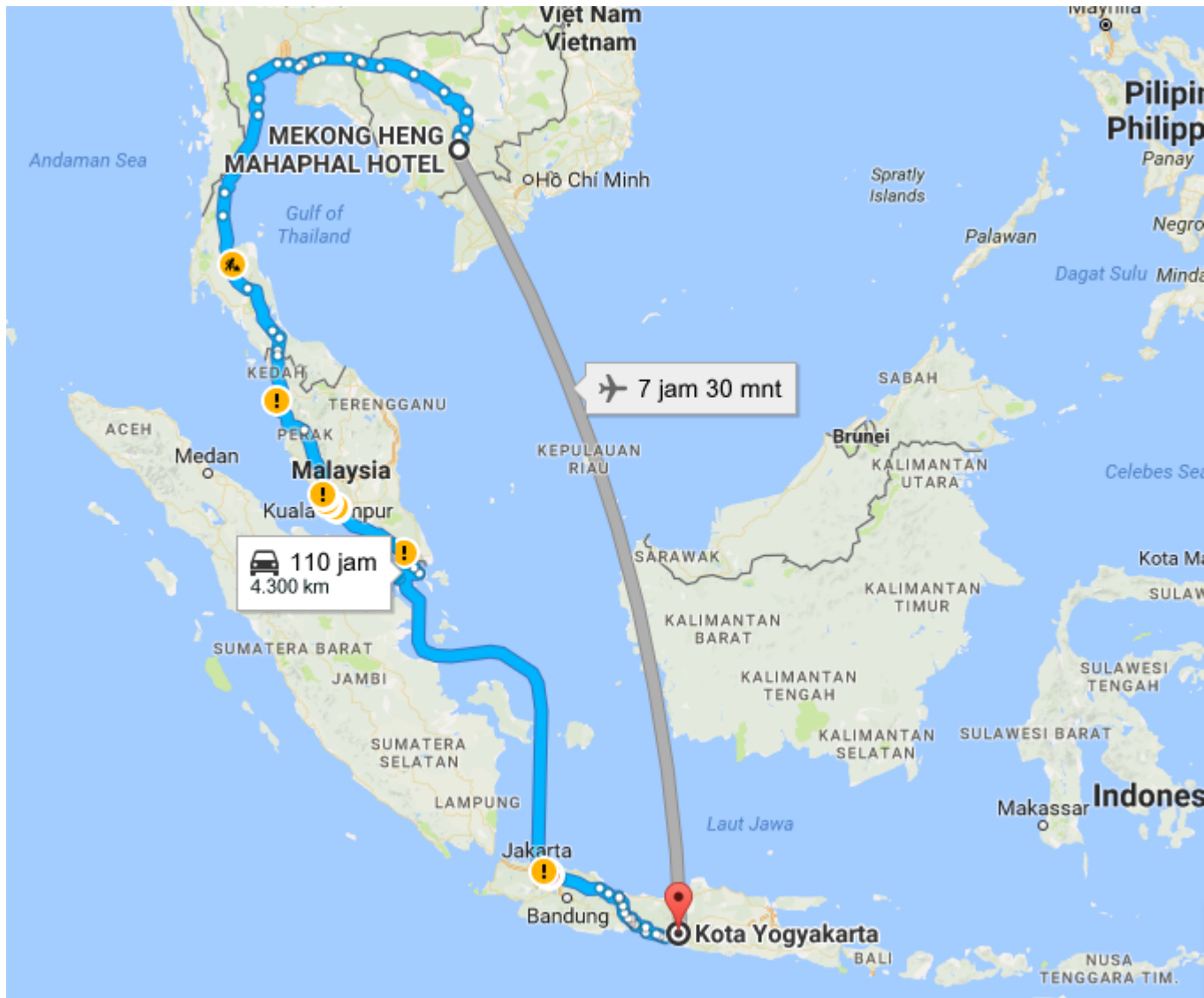
Centralized Logs using ELK Stack

FUDCon APAC, Phnom Penh
6 November 2016

About Me

- Estu Fardani | @tuanpembual
- I am from Yogyakarta, Indonesia

Where is it?



About Me

- Working as Product Engineer in GO-JEK, online booking transportation, using motorcycle
- Documentation Team at BlankOn Linux
- Local Committee of
 - openSUSE.Asia Summit 2016
 - GNOME.Asia Summit 2015
- Fedora User

ELK Stack

- I am not an Elastic Sales Marketing :D

How to monitor lot of servers?

- Log, Status, Networks
- There are many tools to do that. I believe.

Where is the starting point?

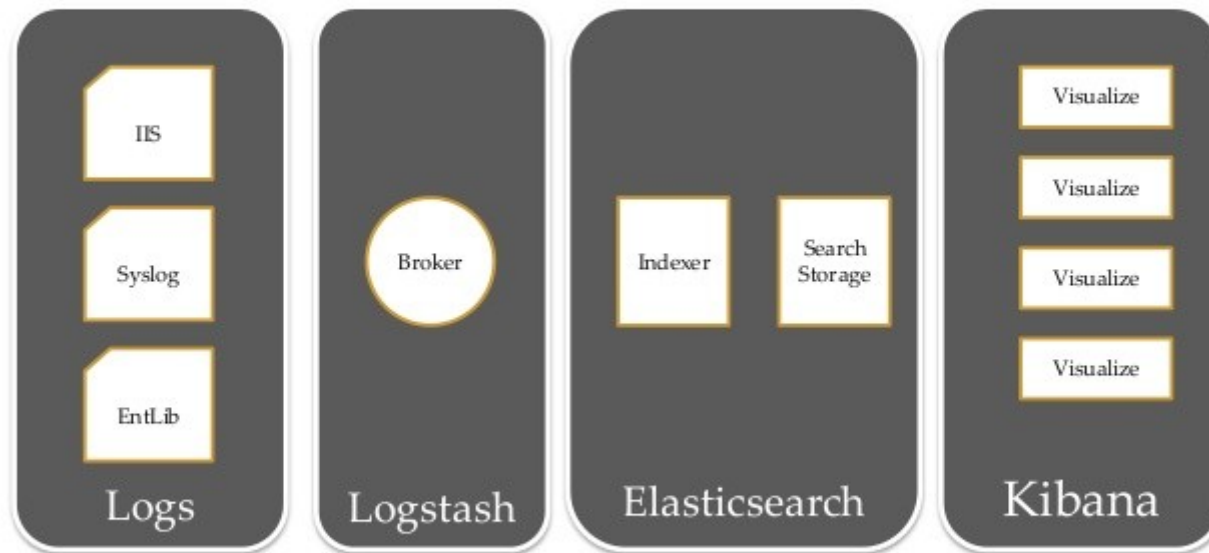
- Last March 2016, starting move to DevOps
 - Working with Ruby, chef DK, Vagrant, Jenkins.
- My Project have 3 Env with 28 Box
- 3 service run in six box (each Env)
- How to monitoring its logs?

Start with ELK

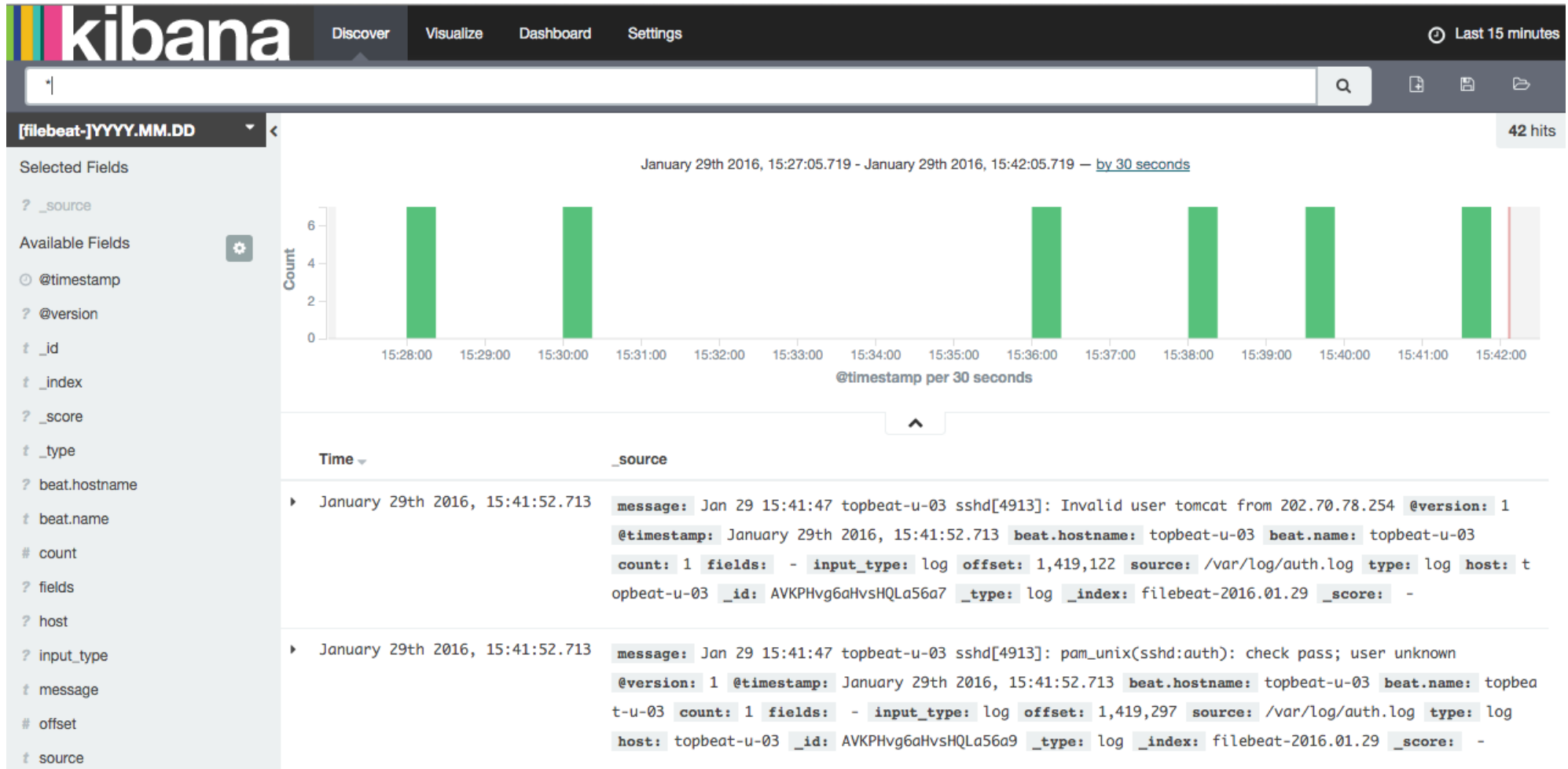
- Log sender in client
 - Beat, Filebeat and Topbeat
 - Using certificate to verify sender
- Log collector in server
 - Logstash
- Search engine in server
 - Elasticsearch
- Dashboard for visualization
 - Kibana

How ELK Work

The ELK architecture

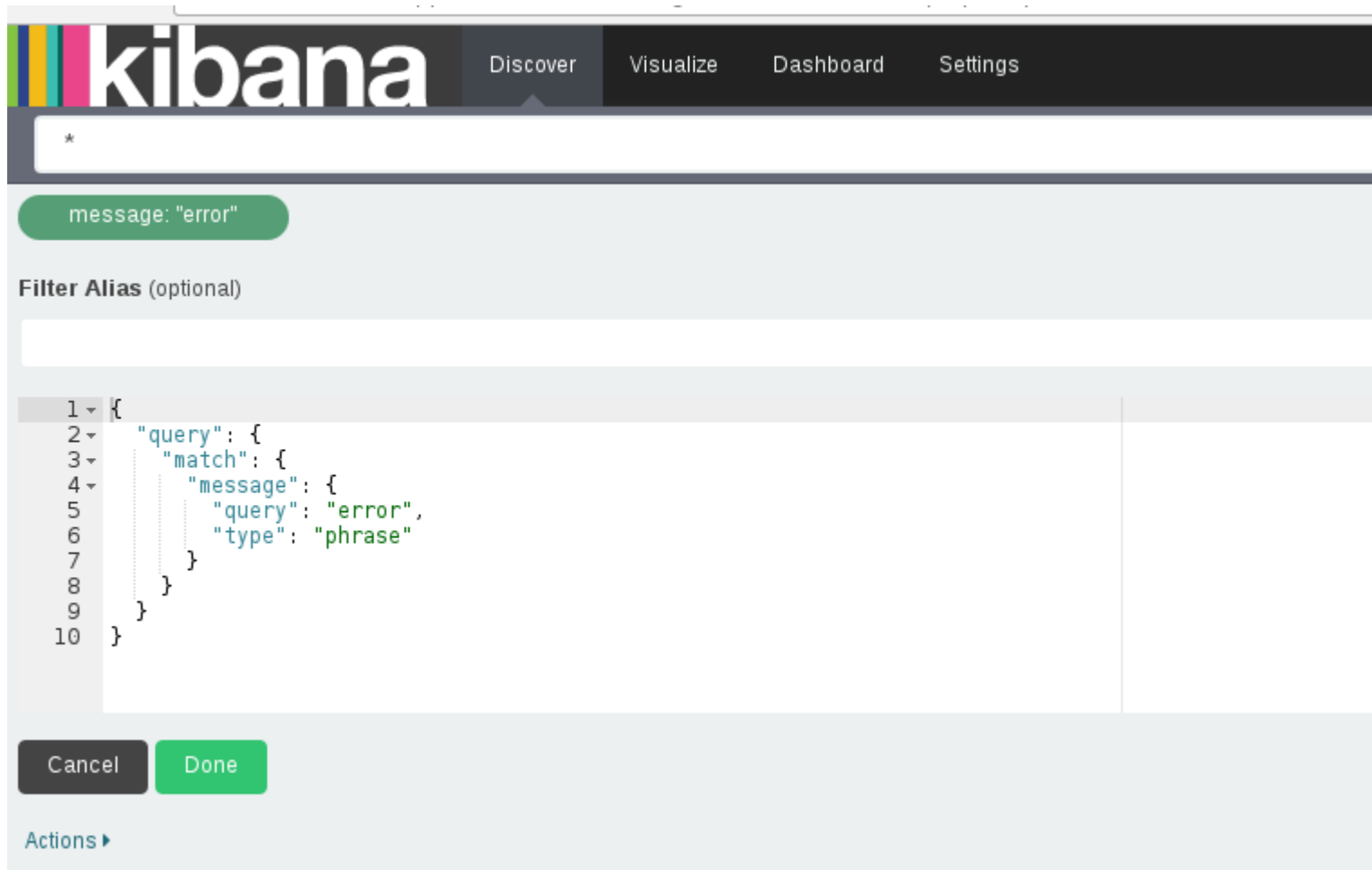


Demo



Search

- Text, Phrase



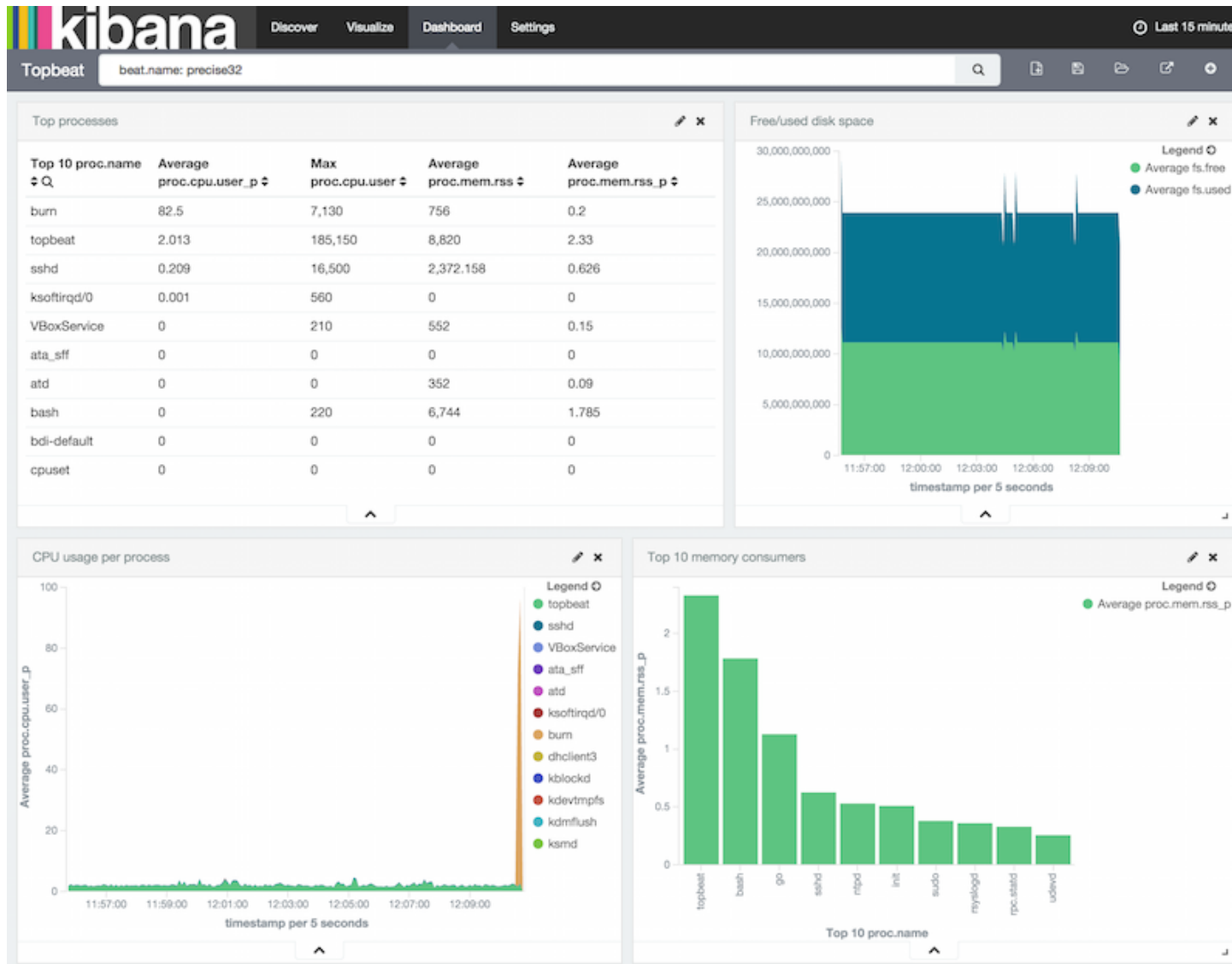
The screenshot shows the Kibana search interface. At the top, the Kibana logo is on the left, and navigation links for 'Discover', 'Visualize', 'Dashboard', and 'Settings' are on the right. Below the navigation bar is a search input field containing an asterisk (*). Underneath the input field is a green pill-shaped button with the text 'message: "error"'. Below this is a section labeled 'Filter Alias (optional)' with an empty input field. The main part of the interface is a query editor with a line-numbered list on the left (1-10) and a JSON query structure on the right. The query is a phrase search for the field 'message'. At the bottom left of the query editor are 'Cancel' and 'Done' buttons. At the bottom right is an 'Actions' link with a right-pointing arrow.

```
1 {  
2   "query": {  
3     "match": {  
4       "message": {  
5         "query": "error",  
6         "type": "phrase"  
7       }  
8     }  
9   }  
10 }
```

Cancel Done

Actions ▶

Status



- Topbeat Dashboard

Questions

Thank you

Contact me:

Estu Fardani | FB

estu@jogja.linux.or.id

@tuanpembual

tuanpembual.wordpress.com

