ELK Stack

Overview and monitoring

About Me

Software Developer

nectarcrm.com.br

World Wide Web

@gustavomtborges

ElasticSearch

Logstash

Kibana

ElasticSearch

"Elasticsearch is a distributed, RESTful search and analytics engine capable of solving a growing number of use cases. As the heart of the Elastic Stack, it centrally stores your data so you can discover the expected and uncover the unexpected."

https://www.elastic.co/products/elasticsearch

ElasticSearch

- Cluster
- Node
- Index
- Document
- Shards and Replicas

https://www.elastic.co/guide/en/elasticsearch/reference/current/_basic_concepts.html

Logstash

> "Logstash is an open source, server-side data processing pipeline that ingests data from a multitude of sources simultaneously, transforms it, and then sends it to your favorite “stash.” (Ours is Elasticsearch, naturally.)"

https://www.elastic.co/products/logstash

Logstash

Input

- Syslog
- TCP/UDP
- File
- Beats

Filters

- Grok
- Geoip
- mutate
- ...

Output

- Elasticsearch
- S3
- Nagios
- Email

https://www.elastic.co/guide/en/logstash/current/introduction.html

Kibana

> "Kibana lets you visualize your Elasticsearch data and navigate the Elastic Stack, so you can do anything from learning why you're getting paged at 2:00 a.m. to understanding the impact rain might have on your quarterly numbers."

https://www.elastic.co/products/kibana

Kibana

"Kibana lets you visualize your Elasticsearch data and navigate the Elastic Stack, so you can do anything from learning why you're getting paged at 2:00 a.m. to understanding the impact rain might have on your quarterly numbers."

https://www.elastic.co/products/kibana

Kibana

- Discover
- Analyse
- Share
- Maintenance
- Maps, charts, histograms.

https://www.elastic.co/products/kibana

Demo

https://github.com/gustavomtborges/elk-monitor

Questions?

Thanks

Software Developer

nectarcrm.com.br

World Wide Web

@gustavomtborges