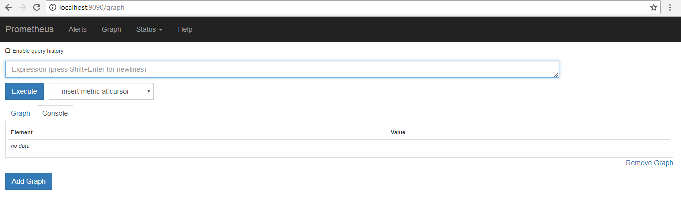
Documentation – Summer Internship 2018

Prometheus

Open source monitoring system with a time series database.

Installation:

Prometheus (and alertmanager) can be downloaded from https://prometheus.io/download/ and then unzipped into any folder. After running the prometheus.bat server, Prometheus should be accessible from <http://localhost:9090>



Configuration:

All configurations of Prometheus must be done in prometheus.yml file.

Scraping ports are configured under “scrape\_configs” section

job\_name: the label added in the time series

metric\_path: path from where metrics will be scraped (default ‘/metrics’)

targets: [hostname: port] for that path

Health status of the targets can be seen in the Prometheus UI under status/targets. Guide for querying through Prometheus metrics can be found here: <https://prometheus.io/docs/prometheus/latest/querying/basics/>

Alertmanager configuration:

Configuration of alertmanager for sending alerts is done under “alerting” section. Rules for alerts are configured in separate yml (ex. rules.yml) files under the “rules” section:

-alert: Name of the Alert

-expr: The expression that must be true for firing the alarm

-for: Duration of how long the expression needs to remain true for firing the alarm

Files where rules are written are specified under the “rule\_files” section of prometheus.yml. Receivers of the alerts (email/slack etc.), repeat interval etc. are configured inside alertmanager.yml file.

References:

<https://prometheus.io/docs/prometheus/latest/getting_started/>

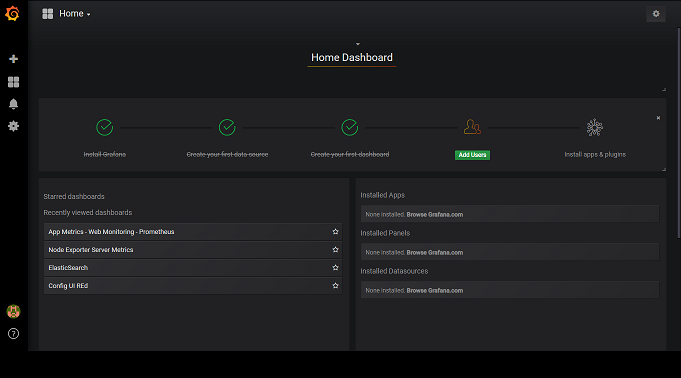
<https://prometheus.io/docs/alerting/alertmanager/>

Grafana

Grafana is an open source software for time series analytics and monitoring.

Installation:

Grafana can be downloaded from <https://grafana.com> and extracted to any folder. After running the bin/grafana.bat server, Grafana should be accessible from <http://localhost:3000/> (Username: admin Password: admin)



Configuration:

Default configuration of Grafana can be changed by creating a custom.ini file inside conf folder, copying everything from sample.ini into custom.ini and then changing desired attributes (ex: http\_port, domain).

Grafana Dashboards can be created or exported from <https://grafana.com/dashboards>.

Different types of panels are available in a Grafana dashboard for facilitating the visualization. Descriptions of the panels and dashboard features can be found here: <http://docs.grafana.org/>

Grafana supports querying Prometheus. Guide for using Prometheus data source in Grafana can be found here: <http://docs.grafana.org/features/datasources/prometheus/>

References:

<http://docs.grafana.org/guides/getting_started/>

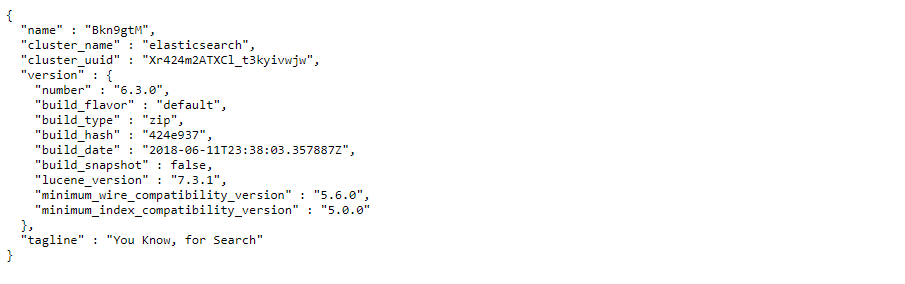
<https://prometheus.io/docs/visualization/grafana/>

Elasticsearch

Open source search engine and analytics

Installation:

Elasticsearch can be downloaded from <https://www.elastic.co/> and then unzipped into any folder. After running bin/elasticsearch.bat server, can be checked if it is running successfully from <http://localhost:9200>



Configuration:

Configuration of elasticsearch can be done in config/elasticsearch.yml file. Plugins like Xpack / Search Guard needs to be configured in the same file.

References:

<https://www.elastic.co/guide/en/elasticsearch/reference/current/getting-started.html>

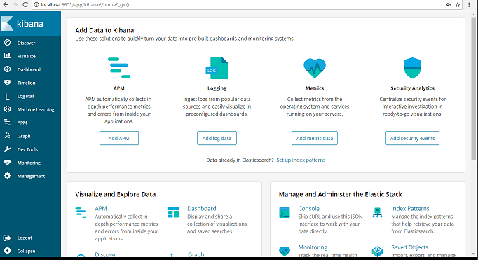
<https://www.edureka.co/blog/elk-stack-tutorial/>

Kibana

Kibana is an open source data visualization plugin for Elasticsearch.

Installation:

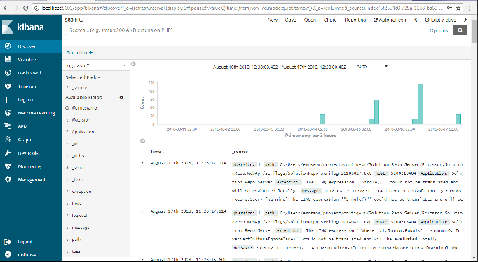
Kibana can be downloaded from <https://www.elastic.co/products/kibana> and unzipped in any folder. After running the server, kibana can be accessed from <http://localhost:5601>



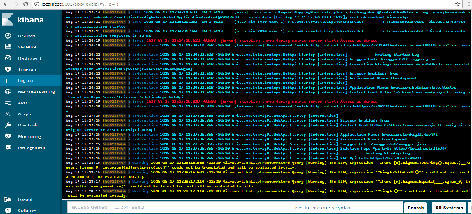
Configuration:

Configuration of kibana (ex. server port, elasticsearch url) can be done inside config/kibana.yml file. Configuration of plugins like x-pack, Searchguard also needs to be done here.

The discover menu in Kibana allows to set time filter, search data, filter by field, view document data/context and view field data statistics. Kibana dashboard displays a collection of visualizations and searches.



LogTrail is a Kibana plugin to view, search and tail logs in developer/sysadmin friendly interface. Full installation and configuration guide for logtrail can be found here: <https://github.com/sivasamyk/logtrail>



References:

<https://www.elastic.co/guide/en/elasticsearch/reference/current/getting-started.html>

<https://www.edureka.co/blog/elk-stack-tutorial/>

Logstash

Logstash is an open source, server-side data processing pipeline that ingest logs from multiple sources simultaneously and feed to elasticsearch.

Installation:

Logstash can be downloaded from <https://www.elastic.co/products/logstash> and unzipped into any folder.

Configuration:

Logstash needs to be configured with in configuration file (ex. config/logstash.conf) and then initialized with that configuration file.

In the configuration file, the sources of the logs need to be specified inside the input section:

path => path to the log files from multiple sources

codec => multiline {

pattern =>

negate =>

what =>

}

start\_position => ""

sincedb\_path => ""

Also, inside the output section a section for elasticsearch must be configured so that logstash can stash the logs to elasticsearch. If any security control is enabled on Elasticsearch, then the access credentials also need to be specified here.

References:

<https://www.elastic.co/guide/en/elasticsearch/reference/current/getting-started.html>

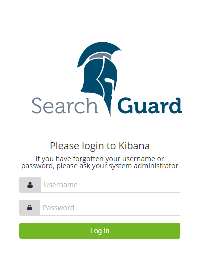
Search Guard

Search Guard enables security control over ELK stack (Elasticsearch, Logstash, Kibana). Search Guard plugin can be downloaded from <https://github.com/floragunncom/search-guard> .

Full installation and configuration guide for implementing Search Guard in Elasticsearch (windows platform) can be found here: <https://docs.search-guard.com/latest/installation-windows>.

Full installation and configuration guide for implementing Search Guard in Kibana can be found here: <https://docs.search-guard.com/latest/kibana-plugin-installation>.

Full installation and configuration guide for implementing Search Guard in Logstash can be found here: https://docs.search-guard.com/latest/logstash



Elasticsearch username: admin; Password: admin

Kibana username: admin; Password: admin

References:

https://sematext.com/blog/elasticsearch-kibana-security-search-guard/