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.

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

Open source software for time series analytics.

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>.

\*Dashboard description here\*

References:

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

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. If plugins are installed ( xpack / searchguard ) then those needs to be configured in the same file.

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

Elasticsearch username: admin; Password: admin

References:

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

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

Kibana

Open source data visualization plugin for Elasticsearch

Installation:

Kibana can be downloaded from <https://www.elastic.co/products/kibana> and unzipped in any folder. The executable to run the server is provided inside. 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 etc also needs to be done here.

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

Kibana username: admin; Password: admin

\*kibana dashboard goes here\*

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

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.

References:

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