## ELK Stack

Intro to ELK stack

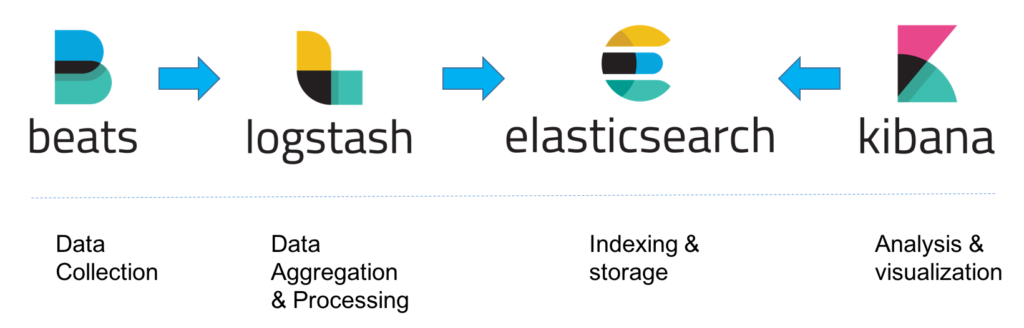
The ELK Stack is a collection of three open-source products Elastic Search, Logstash, Kibana -all developed, managed and maintained by Elastic. Elasticsearch is a NoSQL database that is based on the Lucene search engine. Logstash is a log pipeline tool that accepts inputs from various sources, executes different transformations, and exports the data to various targets. Kibana is a visualization layer that works on top of Elasticsearch.

The stack also includes a family of log shippers called Beats, which led Elastic to rename ELK as the Elastic Stack.

Together, these different open source products are most commonly used for centralized logging in IT environments (though there are many more use cases for the ELK Stack including business intelligence, security and compliance, and web analytics). Logstash collects and parses logs, and then Elasticsearch indexes and stores the information. Kibana then presents the data in visualizations that provide actionable insights into one’s environment.

ELK Stack Architecture

The various components in the ELK Stack were designed to interact and play nicely with each other without too much extra configuration. However, how you end up constructing the stack greatly depends on the environment and specific use case in question. For a small-sized development environment, the classic architecture will look as follows:



However, for handling more complex pipelines built for handling large amounts of data in production, additional components are likely to be added into your logging architecture, for resiliency (Kafka, RabbitMQ, Redis) and security (nginx):



Installation:

ELK can be installed locally, on the cloud, using Docker and configuration management systems like Ansible, Puppet, and Chef. The stack can be installed using tarball or .zip packages or from repositories.

Steps to install all components of the stack on Linux:

**Java**:

ELK requires the installation of Java 8 and higher. The first thing to do is check what Java version you are running and update accordingly.

**ElasticSearch**:

Execute the following commands in the order mentioned,

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

echo "deb https://artifacts.elastic.co/packages/6.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-6.x.list

sudo apt-get update

sudo apt-get install elasticsearch

Elasticsearch configurations are done using a configuration file that allows you to configure general settings. Open the elasticsearch.yml located under ***/etc/elasticsearch/elasticsearch.yml***to bind Elasticsearch to either a private IP or localhost as:

network.host : “localhost”

http.port : 9200

To run elastic search,

sudo service elasticsearch start

Point curl or browser to <http://localhost:9200> to check if everything is working fine

**Logstash**:

sudo apt-get install logstash

**Kibana**:

sudo apt-get install kibana

Open up the Kibana configuration file at: /etc/kibana/kibana.yml, and make sure to have the following configurations defined:

Server.port: 5601

Elasticsearch.url: “http://localhost:9200”

These specific configurations tell Kibana which Elasticsearch to connect to and which port to use.

Now, start kibana:

sudo service kibana start

In the browser, go to <http://localhost:5601> you will be presented with the Kibana home page.

References:

https://logz.io/learn/complete-guide-elk-stack/#installing-elk