DevOps Platform - Integrated Analytics Framework (ELK Stack/ Prometheus Kafka)

Analytics – Plugin-collectors for selected DevOps tool chain to collect activity elements and store into ELK / Prometheus to be rendered to UI dashboard

Elasticsearch **L**ogstash **K**ibana **Framework**

Elasticsearch - It provides a distributed, multitenant-capable full-text search engine with an HTTP web interface and schema-free JSON documents. Elasticsearch is developed in Java and is released as open source under the terms of the Apache License.

Key features

- Real-Time Analysis- By integrating rapid, high-powered search mechanism with strong analytics features, users are able to have a much better grasp of the nature of data. By finding out more about data, we can build a better business.
- Scalability- Elasticsearch is built to be always available, and to scale with your needs. Scale can come from buying bigger servers (vertical scale, or scaling up) or from buying more servers (horizontal scale, or scaling out).
- Resiliency- If any node in Elasticsearch becomes non functional due to any reason, there will not be any issue since there are backup nodes.
- Documents- Users can store sophisticated business information as a structured JSON document within Elasticsearch. Everything automatically gets integrated into the index. User can check all indices with one request, so that you can quickly answer complicated questions.
- No Schema- Getting started with Elasticsearch is very easy. The indexing of JSON document is very easy as program knows to identify the structure and format of the data.
- RESTful API- This API is very important part of Elasticsearch. Any task can be done making use of REST API.
- Open Source License- Elasticsearch uses the open source Apache 2 license, which allows users to install it, work with it, and customize it completely for free. Apache 2 is one of the most user-friendly licenses available for open source apps.
- Apache Lucene- Elasticsearch is built on top of Apache Lucene. Apache Lucene is a high-performance, full-featured text search engine library written entirely in Java.

Multiple stacks creation can be done for ELK stacks

1. Container ELK stack

- Individual ELK containers and use docker compose to build ELK stack.
- One container have all three components
- Logstash consumes a lot of resources so it is not an optimum solution to have Logstash installed on all fileservers. Instead we can use Beats in such scenarios.

2. AWS Elasticsearch managed service

3. VM provisioning and install induvial ELK modules

How to check indices in Elasticsearch

http://localhost:9200/_cat/indices?v