#07 practical class

ELK stack

COMPUTING SYSTEMS AND INFRASTRUCTURES

(SISTEMAS E INFRAESTRUTURAS DE COMPUTAÇÃO)

Overview

- ELK stack
- Elasticsearch
- Logstash
- Kibana

ELK stack

- The ELK stack is an acronym used to describe a collection of three open-source projects – Elasticsearch, Logstash, and Kibana. Elasticsearch is a full-text search and analytics engine
- ELK stack consists of:
  - Elasticsearch
  - Logstash
  - Kibana

Elasticsearch

- Server environment for storing and querying large-scale structured index entries
  - Document-oriented (structured) index entries
  - Combines “full text”-oriented search options- (for text fields) with more precise search options for other types of fields, like date + time fields, geolocation fields, etc.
  - Near real-time search and analysis capabilities
- Provides Restful API as JSON over HTTP

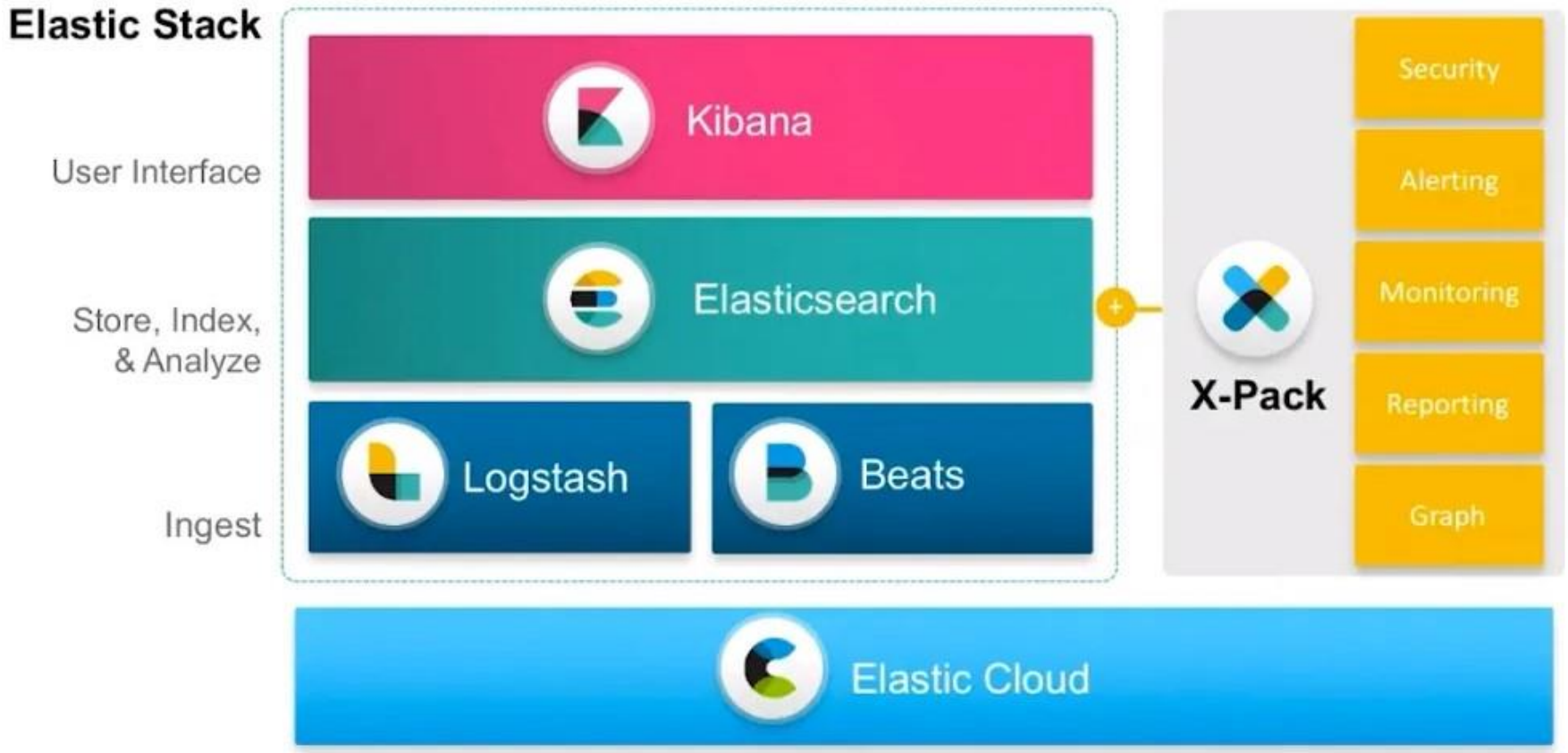
Logstash

- Collect, transform, filter and forward data (e.g., log data) from input sources to output sources (e.g., Elasticsearch)
- Implemented in JRuby
- Runs on a JVM (Java Virtual Machine)
- Simple message-based architecture
- Extendable by plugins (input, output, and filter plugins)

Kibana

- Web-based application for exploring and visualizing data
- Modern browser-based interface (HTML5 + JavaScript)
- Ships with its own web server for easier setup
- Seamless integration with Elasticsearch

Elastic Stack, X-Pack, Cloud



Deploy ELK stack

- Focus on the resources file provided
- Discuss and analyze all the files provided
  - How-to
  - *.yml
  - *.conf
  - .env
  - etc