ELK and X-Pack

Course Summary

Description

ElasticSearch is one of the leading search platforms. With LogStash, added for log collection, and Kibana for the dashboard, it becomes ELK, a popular log collection and analysis tool. The (licensed) X-pack brings together security, monitoring, and machine learning. All together, these components provide a platform for industrial search applications, and all of them are covered in this course.

This course is intended for architects, developers, and administrators who are want to build versatile search solutions. It gives them practical level of experience, achieved through a combination of 50% lecture and 50% lab work.

Topics

- Elasticsearch
- Logstash
- Kibana
- X-Pack

Audience

This course was designed for architects, developers, and administrators.

Prerequisites

Before taking this course, students must be able to navigate Linux command lines and have basic knowledge of command line Linux editors (VI / nano).

Duration

Four days

ELK and X-Pack

Course Outline

I. Elasticsearch
- A. Elasticsearch functionality
- B. Indexing, updating, and deleting data
- C. Searching your data
- D. Analyzing your data
- E. Searching with relevancy
- F. Exploring your data with aggregations
- G. Relations among documents
- H. Scaling out
- I. Improving performance
- J. Cluster administration

II. Logstash
- A. Shipping, Filtering, and Parsing Events with Logstash
- B. Extending Logstash
- C. Creating, Indexing, and Deleting Data
- D. Searching Data
- E. Mapping and Analysis
- F. Data Exploration with Aggregates

III. Kibana
- A. Data Visualization
- B. The Kibana Dashboard
- C. Designing for Scale
- D. The ELK Stack in Production
- E. Use cases

IV. X-Pack
- A. What's in X-Pack
- B. Security
- C. Monitoring
- D. Alerting and Notification
- E. Reporting
- F. Graph
- G. Machine Learning