Elastic Stack: Elasticsearch, Logstash a Kibana

Course code: ELASTICSTACK

The course is focused on obtaining logs, transforming them into something usable for subsequent analysis, storing them in Elasticsearch, and the analysis and visualization of data in Kibana. We will also take a look at Kibana APM (Application Performance Monitoring), and in the end, we will deploy everything on Kubernetes using ECK (Elastic Cloud on Kubernetes).

Required input knowledge

- The course assumes knowledge and experience with Docker at the level of the DOCKER course

Teaching methods

- Expert explanation with practical examples, exercises on computers.

Studying materials

- Printed presentations of the subject matter.

Course syllabus

Fluentd or Filebeat &Logstash

- collection of application logs from files
- log parsing and its transformation into JSON
- Transformation &filtering
- connection with ElasticSearch
- MDC (Mapped Diagnostic Context)

Elasticsearch

- architecture
- cluster
- shards, nodes, indexes
- index operations
- search
- Elasticsearch SQL
- ILM (Index Lifecycle Management)
- hot &warm &cold nodes
- backup &restore
- monitoring
- tuning

Kibana

- Configuration
- Index patterns
- Visualization
- Dashboards
- Search in data
- KQL (Kibana Query Language)

APM

- Kibana APM (Application Performance Monitoring)
- Monitoring of microservice architecture operations

ECK

- Elastic Cloud on Kubernetes (ECK)
- Deploy Elastic to Kubernetes cluster