Ondrej Sika DevOps

Course

Elastic Stack Log Management

Course Outline

- Introduction
    - Introduction to Log Management
    - Introduction to Elastic Stack (former ELK)
    - Elastic Stack Alternatives (Loki Stack)
    - Best log output / format (in own applications)
- ELK Setup
    - VMs (without Docker)
    - VMs + Docker
    - Kubernetes with ECK (Elastic Cloud on Kubernetes, preferred)
    - Node Types
- Logs in ElasticSearch (Indices & Data Streams)
    - Indices
    - Data Streams
    - Stages (hot, warm, cold)
    - Retention policies
    - Sharding
- Beats (log sources)
    - What are Beats
    - Installation of Beats
    - Filebeat, MetricBeat
    - Beats in Kubernetes
- Working with Logs in Beats
    - Filters
    - Processors
    - Parsing
    - Outputs
- Working with logs in Elastic Search (ingest pipelines)
- Kibana
    - Intro into Kibana
    - Log Stram
    - KQL (Kibana Query Language)
    - Spaces & Discover
    - Dashboards
- Backups
- Cross cluster replication