Elastic Stack: Elasticsearch, Logstash a Kibana

Kód kurzu: ELASTICSTACK

Kurz je zaměřen na získání logů, jejich transformace do něčeho použitelného pro následnou analýzu, uložení do Elasticsearch a samotná analýza a vizualizace dat v Kibaně. Také se podíváme na Kibana APM (Application Performance Monitoring) a nakonec si vše dáme do Kubernetes pomocí ECK (Elastic Cloud on Kubernetes).

Požadované vstupní znalosti

- Kurz předpokládá znalosti a zkušenosti s Dockerem na úrovni kurzu DOCKER

Metody výuky

- Odborný výklad s praktickými ukázkami, cvičení na počítačích.

Studijní materiály

- Tištěné prezentace probírané látky.

Osnova kurzu

Fluentd nebo Filebeat &Logstash

- sběr aplikačních logů ze souborů
- parsování logu a jeho transformace do JSON
- transformace &filtrování
- propojení s ElasticSearch
- MDC (Mapped Diagnostic Context)

Elasticsearch

- architektura
- cluster
- shardy, nody, indexy
- operace nad indexy
- vyhledávání
- Elasticsearch SQL
- ILM (Index Lifecycle Management)
- hot &warm &cold uzly
- backup &restore
- monitoring
- tuning

Kibana

- Konfigurace
- Index patterns
- Vizualizace
- Dashboardy
- Vyhledávání v datech
- KQL (Kibana Query Language)

APM

- Kibana APM (Application Performance Monitoring)
- Monitorování operací microservice architektury

ECK

- Elastic Cloud on Kubernetes (ECK)
- Nasazení Elastic do Kubernetes clusteru

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk