



Spring Boot Microservices

Beginner to Guru

Consolidated Logging with ELK Stack



Consolidated Logging with ELK Stack

- **E** - Elasticsearch
- **L** - Logstash
- **K** - Kibana
- All products open source, supported company called **elastic**
- Elasticsearch - JSON based search engine based on Lucine
 - Highly scalable - 100s of nodes (cloud scale)





Logstash

- Data processing pipeline for log data
- Allows to:
 - Collect from multiple sources
 - Transform
 - Send



Kibana

- Data visualization tool for Elasticsearch
- Can query data and act as a dashboard
- Can also create charts, graphs, and alerts
 - Many many more features



Filebeat

- Filebeat is a log shipper
- Moves log data to a destination
- Often destination is a logstash server
 - Logstash is used for further transformation before sending to Elasticsearch



ELK without Logstash

- Filebeat has ability to do some transformations
- Thus, possible to skip Logstash and write directly to Elasticsearch
- Previously we setup JSON log output
- Filebeat can convert JSON logs to JSON objects for Elasticsearch



Docker Logs



Beer Service

Overview



Order Service



Inventory Service



Filebeat



Elasticsearch



Kibana



desktop



2020

