CODING SHUTTLE

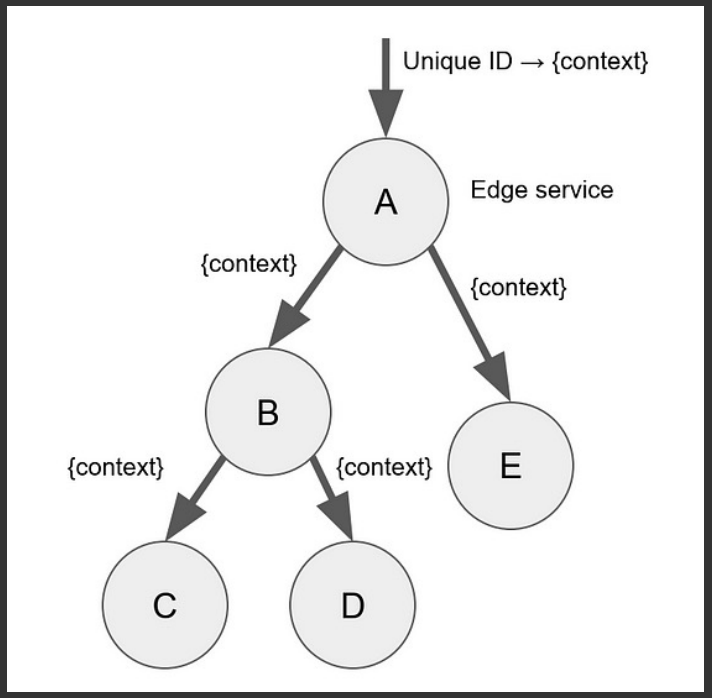
Microservice

Centralized Logging with the ELK Stack

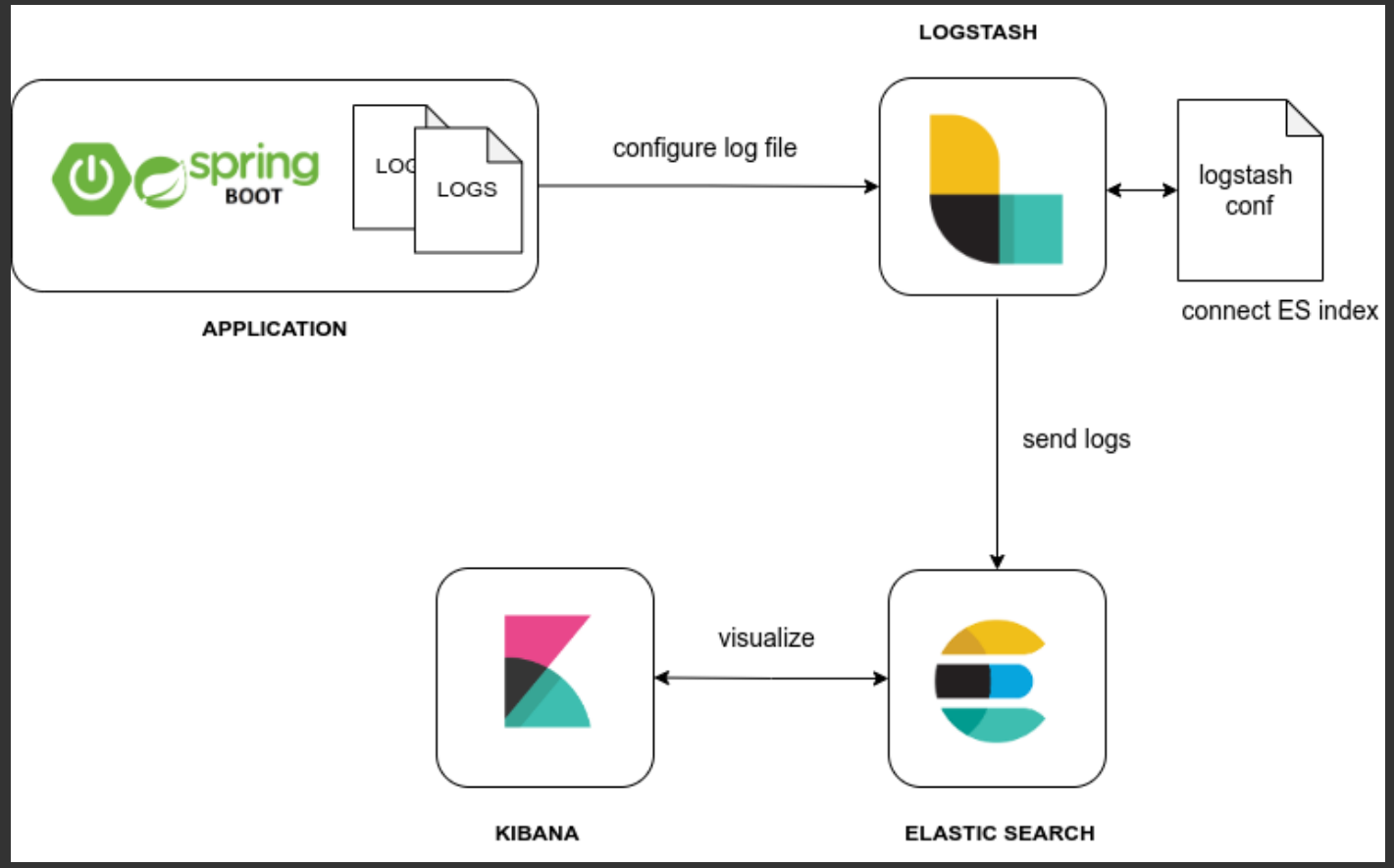
Why Centralized Logging?

While Zipkin is an excellent tool for distributed tracing and observing request paths through microservices, it doesn't offer deep log analysis. ELK Stack complements tracing tools like Zipkin by offering:

- Deep log analysis and insights across microservices.
- Long-term storage and powerful search capabilities.
- Real-time monitoring and alerting.
- Centralized view of logs for easier debugging and troubleshooting.

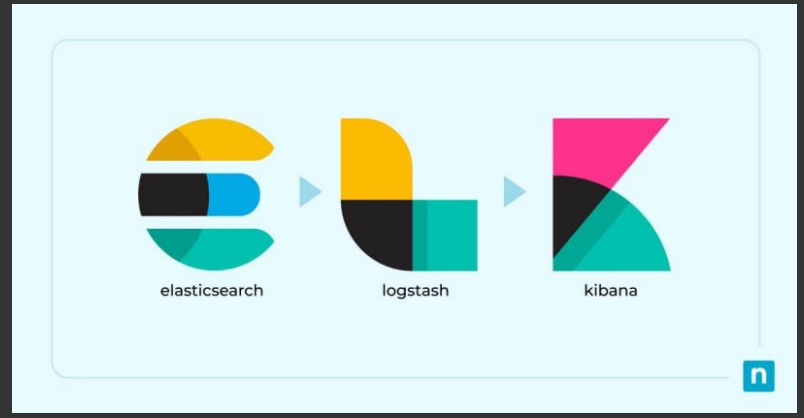


The ELK Stack



The ELK Stack

ELK is a collection of three open-source applications - Elasticsearch, Logstash, and Kibana from Elastic that accepts data from any source or format, on which you can then perform *search, analysis, and visualize* that data.



1. **Elasticsearch** – Elasticsearch stores and indexes the data. It is a NoSQL database based on Lucene's open-source search engine. Since Elasticsearch is developed using Java, therefore, it can run on different platforms. One particular aspect where it excels is indexing streams of data such as logs.

The ELK Stack

2. **Logstash** – Logstash is a tool that integrates with a variety of deployments. It is used to collect, parse, transform, and buffer data from a variety of sources. The data collected by Logstash can be shipped to one or more targets like Elasticsearch.

3. **Kibana** – Kibana acts as an analytics and visualization layer on top of Elasticsearch. Kibana can be used to search, view, and interpret the data stored in Elasticsearch.

Installing the ELK Stack

Download:

ElasticSearch: https://www.elastic.co/downloads/elasticsearch

Logstash: https://www.elastic.co/downloads/logstash

Kibana: https://www.elastic.co/downloads/kibana

Installation:

ElasticSearch

Logstash

Kibana

Or follow this for windows and this for MacOS

Configure Logstash

1. Configure Applications to send their logs to log file. Create a logback-spring.xml to generate logs.
2. Create a configuration file for Logstash – logstash.conf and save this file in the logstash installation folder.
3. Edit this file to include the input and output locations. Here the input will be the location of the logs, and the output will be the ElasticSearch index.
4. Save this file and run bin/logstash –f logstash.conf

How does Logstash work?

1. When new log entries are added to the specified files, Logstash reads these entries and converts them into structured events. Each line or entry in the log file is treated as a separate event.
2. Once the events are processed, Logstash sends them to the configured outputs. In this case, it sends the events to both the console (for debugging) and to Elasticsearch. The logs are sent in near real-time, allowing for timely analysis and visualization.
3. Elasticsearch receives the log events and indexes them according to the specified index pattern. This makes the logs searchable and allows for data analysis using tools like Kibana.