SPRING BOOT + ELK

=================

E L K

E L K Is product of elstic.co https://www.elastic.co/

❖ E - ELASTICSEARCH [JSON]

==================

- Elasticsearch is a tool that allows us to store, search, and analyze large amounts of data, especially logs.
- In microservices, each service creates logs, and Elasticsearch is used to save and organize these logs so they can be searched quickly.
- It makes it easier to find specific logs from different services and allows us to filter, search, and group the logs to understand how the system is working.

❖ L - LOGSTASH

=============

- Logstash is a tool that acts as a pipeline between Spring Boot Application and ELK.
- It will collect, process, and transform log data from different sources.
- In a microservices setup, each service generates logs in different formats.
- Logstash takes these logs, processes them, and converts them into a standard format that can be stored in Elasticsearch.
- It acts as a middleman to clean, filter, and structure the log data before sending it to Elasticsearch for storage and analysis.

❖ K - KIBANA

===========

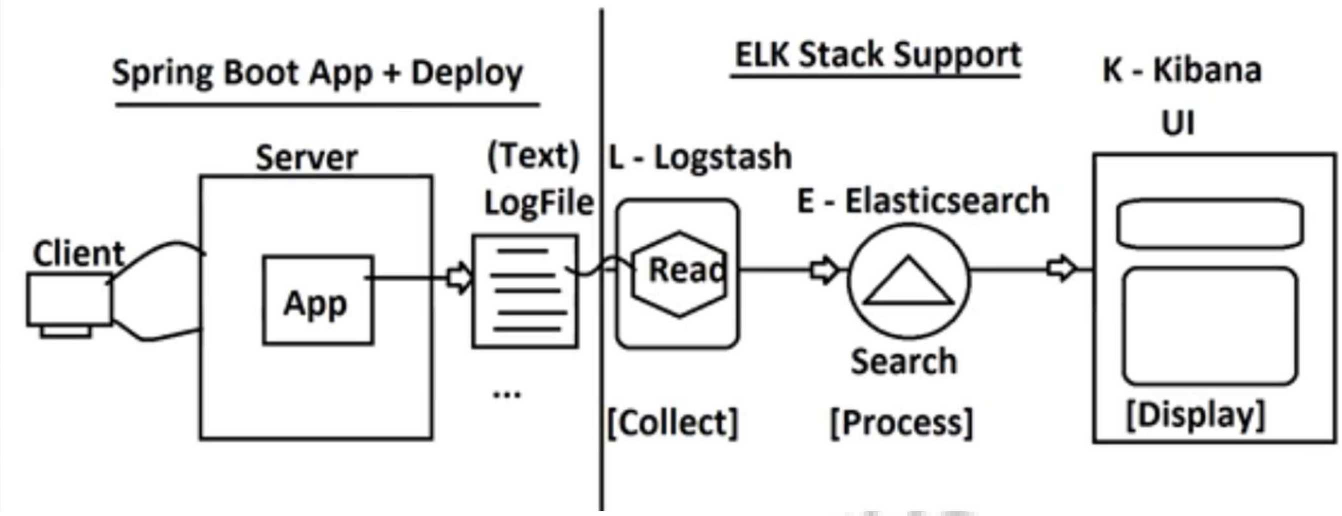
- Kibana is a tool that helps us to visualize and explore log data stored in Elasticsearch.
- It provides a user-friendly interface where we can create charts, graphs, and dashboards to view and analyze the logs.
- In a microservices environment, Kibana allows us to easily search and filter logs from different services, helping us to monitor system performance, identify issues, and understand how everything is working.

WHY ELK :

We have different Spring Boot applications and when we deploy applications in production environment then all success, failure, warning, user activity and other log level messages are stored in a log file.
If I want to analyze the log file then I need to open that log file, need to perform search operation for required contents manually.

But ELK allows us to visualize the logfile content in UI and provides some functionalities.

Spring Boot + ELK :



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

1. Extract the ZIP file
2. Go to Bin folder
3. Run the elasticsearch.bat file
   (Note: Elasticsearch will run on 9200)

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

1. Extract the ZIP file
2. Link kibana with elasticseach
3. Go to config folder and open kibana.yml file
   elasticsearch.hosts : [http://localhost:9200]
   (if not present then add this statement, otherwise just uncomment that statement)
4. Run this command
   bin/kibana.bat
   (kibana will run on 5601)

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

1. Extract the ZIP file
2. Create one configuration file with name ‘logstash.conf’
   It contains information like Input, Filter, Output configuration details.
3. Run this command
   bin/logstash -f logstash.conf

Kibana Index Pattern Creation

- When we, first set up Kibana and connect it to Elasticsearch, you need to create an index pattern.
- This allows Kibana to understand the structure of the data it is pulling from Elasticsearch.
- In Kibana, navigate to Management > Index Patterns.

- Click Create Index Pattern and enter the name of the index (e.g., spring-boot-logs-*).
- Choose the timestamp field (e.g., @timestamp or timestamp depending on your log format).
- After creating the index pattern, you’ll be able to explore your logs in the Discover tab, create visualizations in the Visualize tab, and build dashboards in the Dashboard tab.