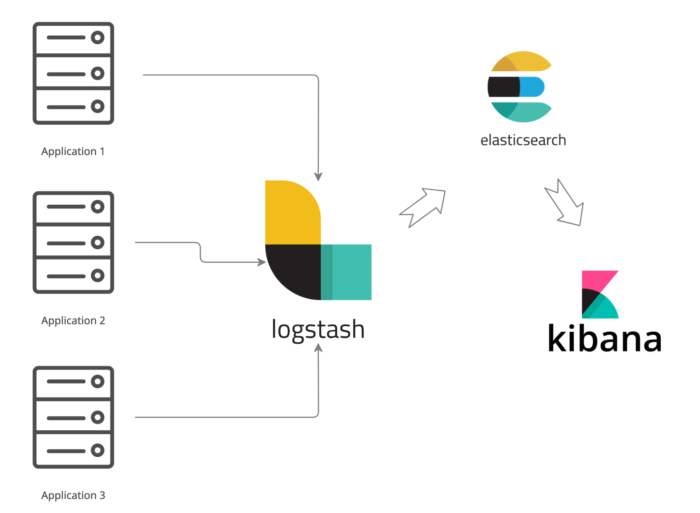
Day 25 Spring Boot with ELK Stack Demo.

ELK – ElasticSearch, Logstash, Kibana (ELK Stack) – This stack is used for Centralized logging and visualizing it.

The ELK Stack is a suite of three popular open-source tools—Elasticsearch, Logstash, and Kibana—used for real-time data analysis, particularly with large volumes of log data. It's used for [log management](https://www.google.com/search?cs=0&sca_esv=4f58605518abfa49&sxsrf=AE3TifO6jvA-f7DdHaWfTKKWer3I8Fq8jg%3A1759746541108&q=log+management&sa=X&ved=2ahUKEwjt3ubbro-QAxV38DgGHXDZLmIQxccNegQIBBAB&mstk=AUtExfBd9nHJmoZumsQKVLZBmVGKL-gnuHAP8s1yI_QIb7cPoNY8v_92wAcvl8jUPKEdGVtlJk97XjtaiPIwq2uWVwpF5qhhjZgcx2_dwze1D7jUTepTbeUUu5FmlGUzuePBa-kK4U-RoMpIX3Dy7mNvyqDoWhX7FoZqobcY_OeVApwoLLE&csui=3), [application and infrastructure monitoring](https://www.google.com/search?cs=0&sca_esv=4f58605518abfa49&sxsrf=AE3TifO6jvA-f7DdHaWfTKKWer3I8Fq8jg%3A1759746541108&q=application+and+infrastructure+monitoring&sa=X&ved=2ahUKEwjt3ubbro-QAxV38DgGHXDZLmIQxccNegQIBBAC&mstk=AUtExfBd9nHJmoZumsQKVLZBmVGKL-gnuHAP8s1yI_QIb7cPoNY8v_92wAcvl8jUPKEdGVtlJk97XjtaiPIwq2uWVwpF5qhhjZgcx2_dwze1D7jUTepTbeUUu5FmlGUzuePBa-kK4U-RoMpIX3Dy7mNvyqDoWhX7FoZqobcY_OeVApwoLLE&csui=3), troubleshooting, [security analysis](https://www.google.com/search?cs=0&sca_esv=4f58605518abfa49&sxsrf=AE3TifO6jvA-f7DdHaWfTKKWer3I8Fq8jg%3A1759746541108&q=security+analysis&sa=X&ved=2ahUKEwjt3ubbro-QAxV38DgGHXDZLmIQxccNegQIBBAD&mstk=AUtExfBd9nHJmoZumsQKVLZBmVGKL-gnuHAP8s1yI_QIb7cPoNY8v_92wAcvl8jUPKEdGVtlJk97XjtaiPIwq2uWVwpF5qhhjZgcx2_dwze1D7jUTepTbeUUu5FmlGUzuePBa-kK4U-RoMpIX3Dy7mNvyqDoWhX7FoZqobcY_OeVApwoLLE&csui=3), and business intelligence by collecting, processing, storing, and visualizing data from various sources.

The Elastic Stack (ELK) includes Elasticsearch, Kibana, Beats, and Logstash. It helps **search, analyze, and visualize data** from any source.





Logstash – Collect, Parse, Transform Logs (Stashing)

XML & JSON – Universal Data Exchange Format. (Platform, Language & Architecture Neutral)

XML is both case and space sensitive.

JSON is very Simple. Both Human and Machine can understand it easily.

Kibana -- Kibana is an open-source data visualization and exploration tool from Elastic, used to interact with [Elasticsearch data](https://www.google.com/search?sca_esv=4f58605518abfa49&sxsrf=AE3TifNu6w01ERs5wENTylB0HXj5q3XIJQ%3A1759747539039&q=Elasticsearch+data&sa=X&ved=2ahUKEwi8itW3so-QAxVp96ACHTZAMakQxccNegQIHRAC&mstk=AUtExfB6rcEIJzQiUBVjXEU0Z-EjU4klOZcfPptb29MOVZ0CJd9pK1HsckYBb9LuPh22itTm6VwS11crjbWIzuyE2Q-coM0yEqlKwh3zH_Ai5Q1Cn4UBbdclaNqGNosRzS5j3LJ5jnBk5GOhXQiTBd6Yr2fdhYxnvltLAYT-dFFFh3VdWPiIvTljx12niMC6EJESRXKL_PrG8ettAkp_b574SkyS8vlFjaQng_J4KHdABdIw7tFrenWL6u4XwolibnVN6aX64R5yNEZTXdizJmcpLOLH&csui=3) to create dashboards, charts, and reports. It is the visual interface of the [Elastic Stack](https://www.google.com/search?sca_esv=4f58605518abfa49&sxsrf=AE3TifNu6w01ERs5wENTylB0HXj5q3XIJQ%3A1759747539039&q=Elastic+Stack&sa=X&ved=2ahUKEwi8itW3so-QAxVp96ACHTZAMakQxccNegQIGRAB&mstk=AUtExfB6rcEIJzQiUBVjXEU0Z-EjU4klOZcfPptb29MOVZ0CJd9pK1HsckYBb9LuPh22itTm6VwS11crjbWIzuyE2Q-coM0yEqlKwh3zH_Ai5Q1Cn4UBbdclaNqGNosRzS5j3LJ5jnBk5GOhXQiTBd6Yr2fdhYxnvltLAYT-dFFFh3VdWPiIvTljx12niMC6EJESRXKL_PrG8ettAkp_b574SkyS8vlFjaQng_J4KHdABdIw7tFrenWL6u4XwolibnVN6aX64R5yNEZTXdizJmcpLOLH&csui=3) (also known as the ELK Stack), working alongside [Logstash](https://www.google.com/search?sca_esv=4f58605518abfa49&sxsrf=AE3TifNu6w01ERs5wENTylB0HXj5q3XIJQ%3A1759747539039&q=Logstash&sa=X&ved=2ahUKEwi8itW3so-QAxVp96ACHTZAMakQxccNegQIGRAC&mstk=AUtExfB6rcEIJzQiUBVjXEU0Z-EjU4klOZcfPptb29MOVZ0CJd9pK1HsckYBb9LuPh22itTm6VwS11crjbWIzuyE2Q-coM0yEqlKwh3zH_Ai5Q1Cn4UBbdclaNqGNosRzS5j3LJ5jnBk5GOhXQiTBd6Yr2fdhYxnvltLAYT-dFFFh3VdWPiIvTljx12niMC6EJESRXKL_PrG8ettAkp_b574SkyS8vlFjaQng_J4KHdABdIw7tFrenWL6u4XwolibnVN6aX64R5yNEZTXdizJmcpLOLH&csui=3) (data collection) and Elasticsearch (data storage and search). Kibana helps users discover, visualize, and analyze data for various use cases, such as log analysis, [application monitoring](https://www.google.com/search?sca_esv=4f58605518abfa49&sxsrf=AE3TifNu6w01ERs5wENTylB0HXj5q3XIJQ%3A1759747539039&q=application+monitoring&sa=X&ved=2ahUKEwi8itW3so-QAxVp96ACHTZAMakQxccNegQIGhAB&mstk=AUtExfB6rcEIJzQiUBVjXEU0Z-EjU4klOZcfPptb29MOVZ0CJd9pK1HsckYBb9LuPh22itTm6VwS11crjbWIzuyE2Q-coM0yEqlKwh3zH_Ai5Q1Cn4UBbdclaNqGNosRzS5j3LJ5jnBk5GOhXQiTBd6Yr2fdhYxnvltLAYT-dFFFh3VdWPiIvTljx12niMC6EJESRXKL_PrG8ettAkp_b574SkyS8vlFjaQng_J4KHdABdIw7tFrenWL6u4XwolibnVN6aX64R5yNEZTXdizJmcpLOLH&csui=3), and [operational intelligence](https://www.google.com/search?sca_esv=4f58605518abfa49&sxsrf=AE3TifNu6w01ERs5wENTylB0HXj5q3XIJQ%3A1759747539039&q=operational+intelligence&sa=X&ved=2ahUKEwi8itW3so-QAxVp96ACHTZAMakQxccNegQIGhAC&mstk=AUtExfB6rcEIJzQiUBVjXEU0Z-EjU4klOZcfPptb29MOVZ0CJd9pK1HsckYBb9LuPh22itTm6VwS11crjbWIzuyE2Q-coM0yEqlKwh3zH_Ai5Q1Cn4UBbdclaNqGNosRzS5j3LJ5jnBk5GOhXQiTBd6Yr2fdhYxnvltLAYT-dFFFh3VdWPiIvTljx12niMC6EJESRXKL_PrG8ettAkp_b574SkyS8vlFjaQng_J4KHdABdIw7tFrenWL6u4XwolibnVN6aX64R5yNEZTXdizJmcpLOLH&csui=3)

<https://dev.to/devaaai/achieving-comprehensive-observability-in-spring-boot-microservices-with-the-elk-stack-and-2hg2>

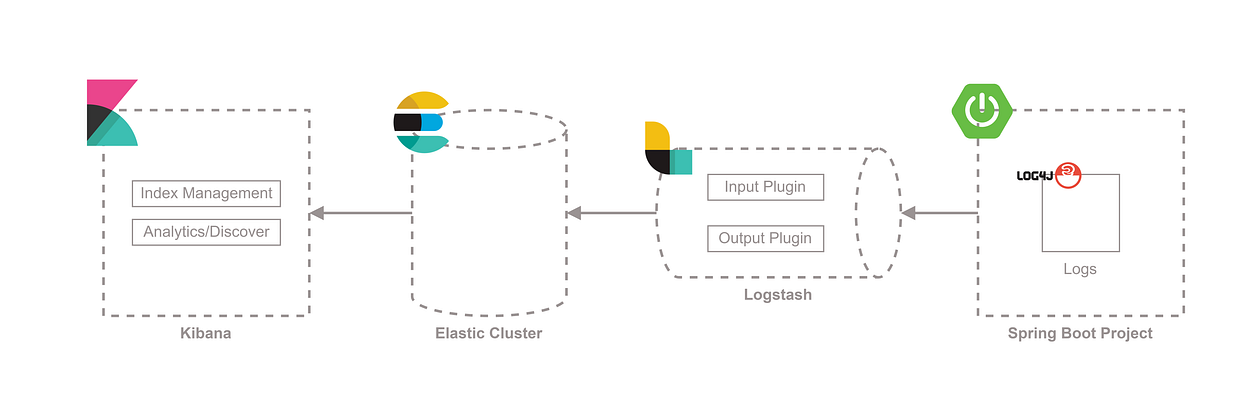
<https://www.geeksforgeeks.org/advance-java/set-up-elk-stack-with-spring-boot-for-centralized-logging-purposes/>

ELK is an acronym that stands for Elasticsearch, Logstash, and Kibana. It is a powerful open-source software stack used for centralized logging, log analysis, and visualization. Each component of ELK serves a specific purpose:

* **Elasticsearch:** *It is a distributed search and analytics engine that stores and indexes data. Elasticsearch allows for fast and efficient searching, aggregating, and analyzing of large volumes of data.*
* **Logstash:** *It is a data processing pipeline that ingests, filters, and transforms data from various sources before sending it to Elasticsearch for indexing. Logstash can handle different types of data, such as logs, metrics, and other event data.*
* **Kibana:** *It is a web-based data visualization and exploration tool that works in conjunction with Elasticsearch. Kibana provides a user-friendly interface for searching, analyzing, and visualizing data stored in Elasticsearch. It offers various visualizations, dashboards, and tools to help gain insights from the data.*

Together, these three components form the ELK stack, which is widely used for log management, monitoring, and troubleshooting in various applications and systems.

The following high-level architecture diagram illustrates the placement of components within a system.



<https://medium.com/cloud-native-daily/elk-spring-boot-a-guide-to-local-configuration-b6d9fa7790f6>

APM – Application Performance Monitoring (Prometheus & Grafana )