**ELK STACK**

# **Introduction**



The ELK Stack is a collection of three open-source products — Elasticsearch, Logstash, and Kibana.For the purpose of identifying issues with servers or applications, the ELK stack offers centralized logging. It enables comprehensive log searches in one location. By connecting logs from many servers over a certain period of time, problems on multiple servers can also be found.

Elasticsearch is an open source, full-text search and analysis engine, based on the Apache Lucene search engine. Logstash is a log aggregator that collects data from various input sources, executes different transformations and enhancements and then ships the data to various supported output destinations. Kibana is a visualization layer that works on top of Elasticsearch, providing users with the ability to analyze and visualize the data. And last but not least — Beats are lightweight agents that are installed on edge hosts to collect different types of data for forwarding into the stack.

Together, these different components are most commonly used for monitoring, troubleshooting and securing IT environments (though there are many more use cases for the ELK Stack such as business intelligence and web analytics). Beats and Logstash take care of data collection and processing, Elasticsearch indexes and stores the data, and Kibana provides a user interface for querying the data and visualizing it.

# **Project Summary**

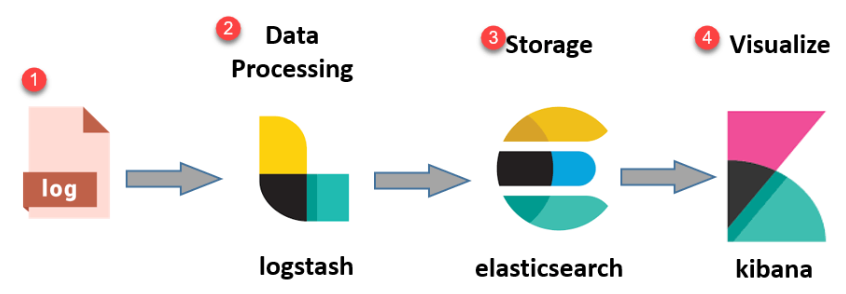
|  |  |
| --- | --- |
| Website | https://www.elastic.co/ |
| Organization/Foundation Name | Elastic N.V. |
| License | Elastic License, Server Side Public License (SSPL) |
| Open/Proprietary | Open |
| Source Path(if open source) | <https://github.com/elastic/elasticsearch>  <https://github.com/elastic/logstash>  <https://github.com/elastic/kibana> |
| Brief Description | ELK Stack is designed to allow users to take data from any source, in any format, and to search, analyze, and visualize that data in real time.  **E** stands for ElasticSearch: used for storing logs  **L** stands for LogStash : used for both shipping as well as processing and storing logs  **K** stands for Kibana: is a visualization tool (a web interface) which is hosted through Nginx or Apache |

# **Project Details**

## **Key Features**

* Used to index any kind of heterogeneous data
* Has REST API web-interface with JSON output
* Near Real Time (NRT) search
* Sharded, replicated searchable, JSON document store
* Schema-free, REST & JSON based distributed document store
* Multi-language & Geolocation support

## **Architecture**



* **Logs:** Server logs that need to be analyzed are identified
* **Logstash:** Collect logs and events data. It even parses and transforms data
* **ElasticSearch:** The transformed data from Logstash isStore, Search, and indexed.
* **Kibana:** Kibana uses Elasticsearch DB to Explore, Visualize, and Share

However, one more component is needed for Data collection called Beats. This led Elastic to rename ELK as the Elastic Stack. While dealing with very large amounts of data, you may need Kafka, RabbitMQ for buffering and resilience. For security, nginx can be used.

**Current Usage**

* **Uber**

Uber uses ELK to monitor and analyze data from its mobile app and website as well as data from its ride-sharing platform. The stack aids the business in problem identification, performance enhancement, and improved user experience.

### **Humanz**

Humanz delivers real-time data returns using Elastic Enterprise Search to match influencer content and demographics with companies and contributes to a 70% improvement in the effectiveness of social media marketing initiatives.

### **Adobe**

ELK is used by Adobe to monitor its cloud-based services and apps. The stack enables the business to analyze data to gain insights, swiftly detect and fix problems, and enhance customer experience.

### **Cisco**

Cisco makes use of ELK to monitor and analyze data from many sources for its network architecture. The stack gives the business the ability to spot possible security issues, enhance network performance, and enhance customer satisfaction.

* **BMW**

BMW dealership and partner after-sales service are kept functioning smoothly throughout Europe by elastic Applications for spare parts, workshop systems, appointment scheduling, data sharing across apps to enhance fault diagnostics, and combining the logging service are just a few examples.

## 

## 

## **Technical Details**

A group of open-source technologies called the ELK stack are used for logging and analyzing huge amounts of data. There are three main parts of the stack:

Large amounts of data are indexed, searched for, and analyzed using the distributed search engine elasticsearch. It can be used to store and search for a range of data kinds, including logs, metrics, and structured data, and is intended to offer real-time search and analytics capabilities.

Before data is indexed in Elasticsearch, it is ingested, processed, and transformed using the Logstash data processing pipeline. It allows for a variety of input sources, such as metrics, events, and logs, and it may be used to filter, aggregate, and enrich data.

Kibana is a web-based user interface for Elasticsearch data visualization and analysis. It offers a variety of visualizations, such as heat maps, line charts, and histograms, and may be used to design unique dashboards and reports.

The ELK stack can also be expanded with a variety of plugins and integrations, such as Beats, which are lightweight data shippers used to gather data from many sources, and X-Pack, which offers extra security, monitoring, and alerting features, in addition to the basic components.

The ELK stack can be used for a broad variety of different use cases, such as security analytics, business intelligence, and machine learning, in addition to log analysis and monitoring, which are two of the most common uses for it. It is a popular option for businesses of all sizes because to its high scalability and ability to be installed on-premises or in the cloud.

### 

### 

### 

### **Project comparison**

* **SigNoz**

A full-stack open source APM called SigNoz offers log analytics and collection. ClickHouse is a columnar database that is particularly effective at consuming and storing log data, and SigNoz utilizes it to store logs. Log data may be stored and made available for analysis relatively efficiently with the help of columnar databases like ClickHouse.

* **Logz.io**

Cloud-hosted services powered by the ELK stack are offered by Logz.io. It is built on Elasticsearch and Kibana's respective open source alternatives, OpenSearch and OpenSearch dashboards. With dashboards and visualizations, you can keep an eye on your logs while setting alarms to inform your team.

* **Graylog**

Graylog is a platform for centralized log management that offers the log management and Security Information Event Management solutions (SIEM). The Graylog Open is an open-source variation of Graylog. Graylog Open provides the fundamental centralized log management features required to gather, store, and analyze log data.

* **Logtail**

Based on the OLAP database ClickHouse, LogTail offers organized log management that is SQL-compatible. By creating unique SQL queries, you may analyze your logs in Logtail. Moreover, you may easily link Logtail to any BI application. It offers hosted Grafana dashboards for visualization, which you may use to make your own charts and dashboards.Your audit logs can also be archived into an S3 glacier or another well-liked data repository. Starting at $0.25 per GB, Logtail is reasonably priced.

* **Logic Sumo**

A SaaS analytics platform called Sumo Logic offers log management as one of its capabilities. A selection of pre-built dashboards from Sumo Logic are available for a variety of technologies, including NGINX, Kubernetes, Docker, etc.

**References**

|  |  |
| --- | --- |
| Website Links | Description |
| https://www.elastic.co/ | Official Site of Elastic Co. |
| https://github.com/elastic/elasticsearch  <https://github.com/elastic/logstash>  <https://github.com/elastic/kibana> | Open Source Repository of Elasticsearch, Logstash and Kibana which constitutes ELK Stack |
| <https://www.guru99.com/elk-stack-tutorial.html> | E-Learning website about ELK Stack made by Elastic Co. |
| <https://signoz.io/blog/elk-alternatives/> | Blog on alternatives of ELK Stack |

**-------------------------------------------------------------------------------------------------------------------------------**