

**What Is ELK Stack? – ELK Stack Tutorial**

Popularly known as ELK Stack has been recently re-branded as Elastic Stack. It is a powerful collection of three open source tools: Elasticsearch, Log stash, and Kibana.

These three different products are most commonly used together for log analysis in different IT environments. Using  ELK Stack you can perform centralized logging which helps in identifying the problems with the web servers or applications. It lets you search through all the logs at a single place and identify the issues spanning through multiple servers by correlating their logs within a specific time frame.

**Logstash:**

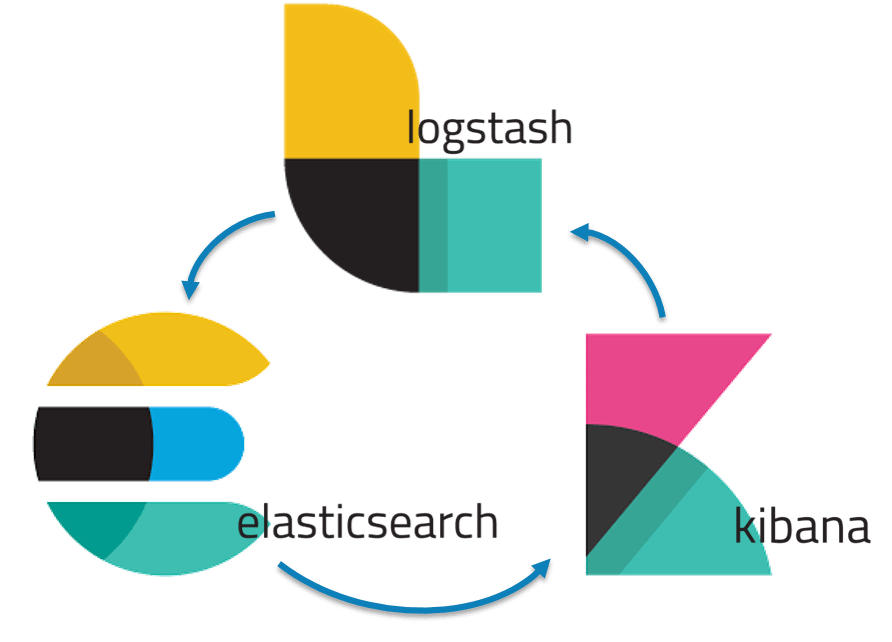
Logstash is the data collection pipeline tool. It the first component of ELK Stack which collects data inputs and feeds it to the Elasticsearch. It collects various types of data from different sources, all at once and makes it available immediately for further use.

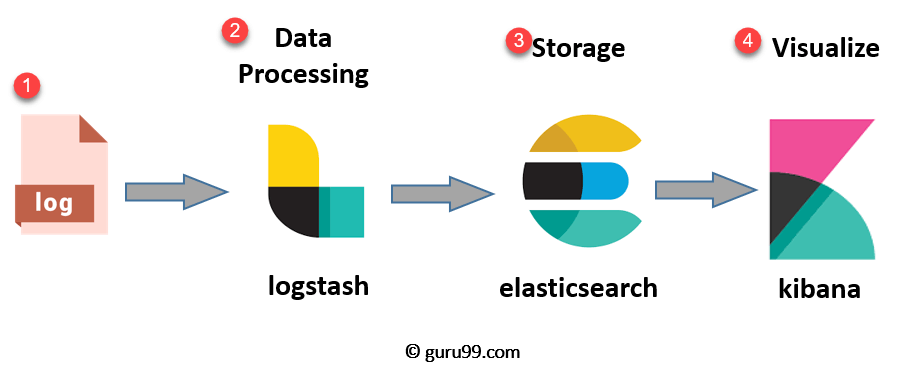
**Elasticsearch:**

Elasticsearch is a NoSQL database which is based on Lucene search engine and is built with RESTful APIs. It is a highly flexible and distributed search and analytics engine. Also, it provides simple deployment, maximum reliability, and easy management through horizontal scalability. It provides advanced queries to perform detailed analysis and stores all the data centrally for quick search of the documents.

**Kibana:**

Kibana is a data visualization tool. It is used for visualizing the Elasticsearch documents and helps the developers to have an immediate insight into it. Kibana dashboard provides various interactive diagrams, geospatial data, timelines, and graphs to visualize the complex queries done using Elasticsearch. Using Kibana you can create and save custom graphs according to your specific needs.

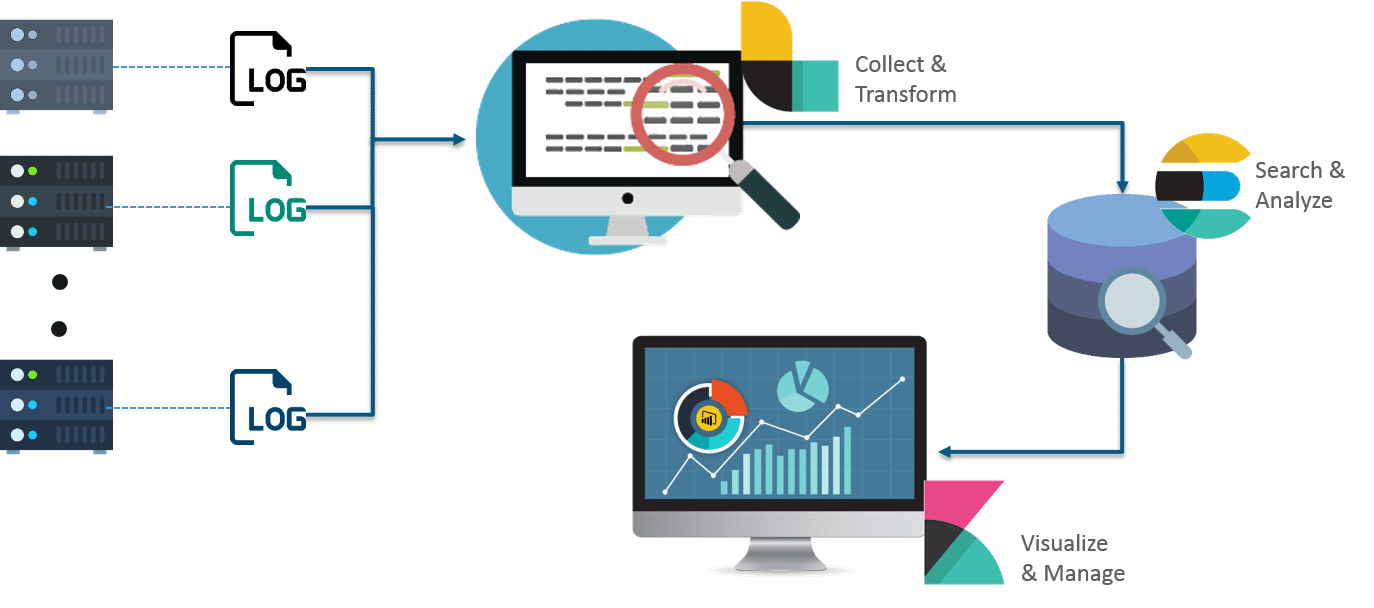
****



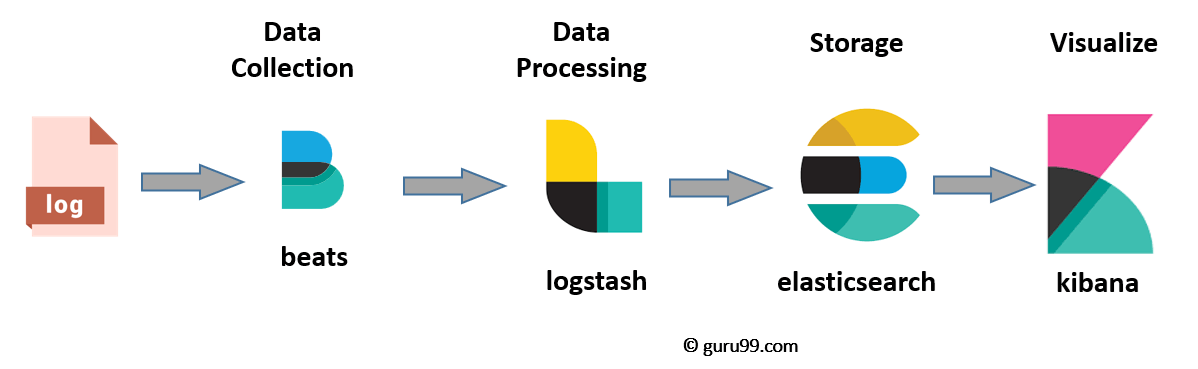
* **Logs:** Server logs that need to be analyzed are identified
* **Logstash:** Collect logs and events data. It even parses and transforms data
* **ElasticSearch:**The transformed data from Logstash is Store, Search, and indexed.
* **Kibana:** Kibana uses Elasticsearch DB to Explore, Visualize, and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

## ****ELK Stack Architecture – ELK Stack Tutorial****

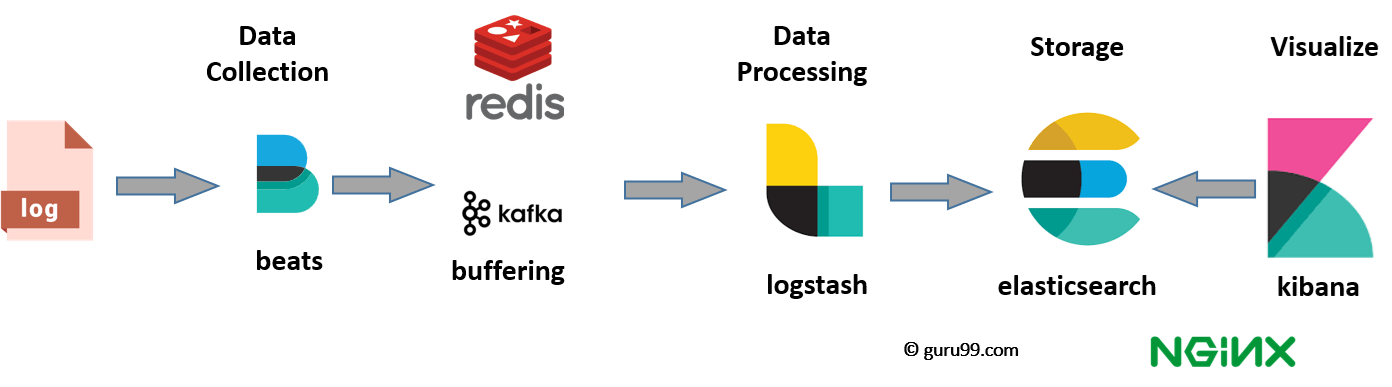
The following is the architecture of ELK Stack which shows the proper order of log flow within ELK. Here, the logs generated from various sources are collected and processed by Logstash, based on the provided filter criteria. Logstash then pipes those logs to Elasticsearch which then analyzes and searches the data. Finally, using Kibana, the logs are visualized and managed as per the requirements.



However, one more component is needed or Data collection called Beats. This led Elastic to rename ELK as the Elastic Stack.

[](https://www.guru99.com/images/tensorflow/082918_1504_ELKStackTut2.png)

While dealing with very large amounts of data, you may need Kafka, RabbitMQ for buffering and resilience. For security, nginx can be used.

[](https://www.guru99.com/images/tensorflow/082918_1504_ELKStackTut3.png)

Read:

<https://www.edureka.co/blog/elk-stack-tutorial/>

<https://www.edureka.co/blog/elasticsearch-tutorial/>