Guru99

ELK Stack Tutorial: What is Kibana, Logstash & Elasticsearch?

By David Taylor Updated February 22, 2022

What is the ELK Stack?

The **ELK Stack** is a collection of three open-source products — Elasticsearch, Logstash, and Kibana. ELK stack provides centralized logging in order to identify problems with servers or applications. It allows you to search all the logs in a single place. It also helps to find issues in multiple servers by connecting logs during a specific time frame.

- **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

ElasticSearch, LogStash and Kibana are all developed, managed ,and maintained by the company named Elastic.

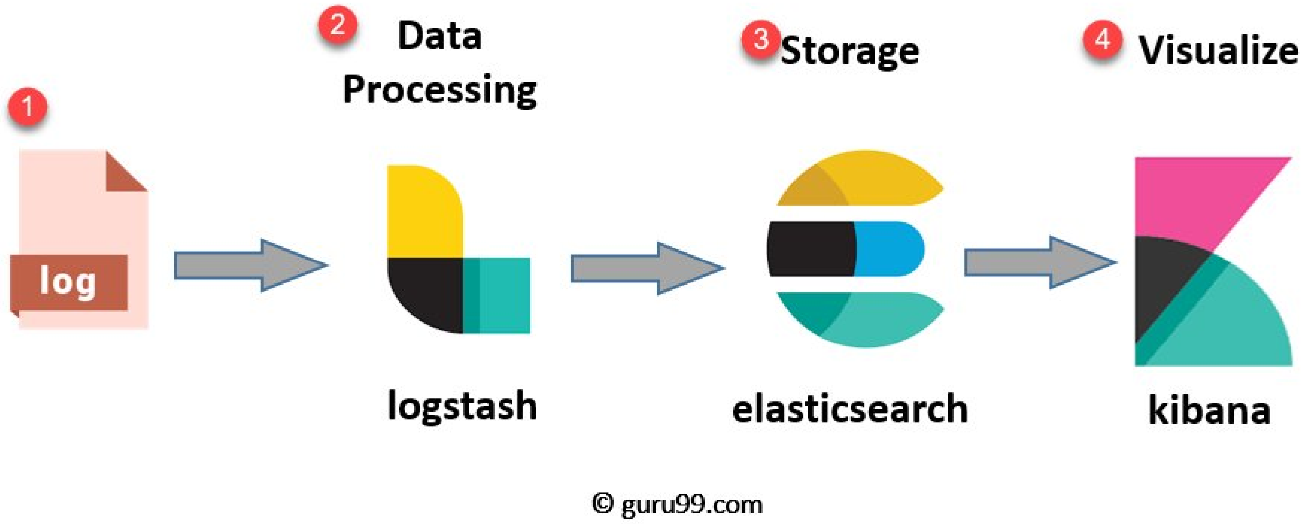
ELK Stack is designed to allow users to take data from any source, in any format, and to search, analyze, and visualize that data in real time.

In this ELK stack tutorial, you will learn

ELK Stack Architecture

Now in this ELK stack tutorial, we will learn about ELK architecture:

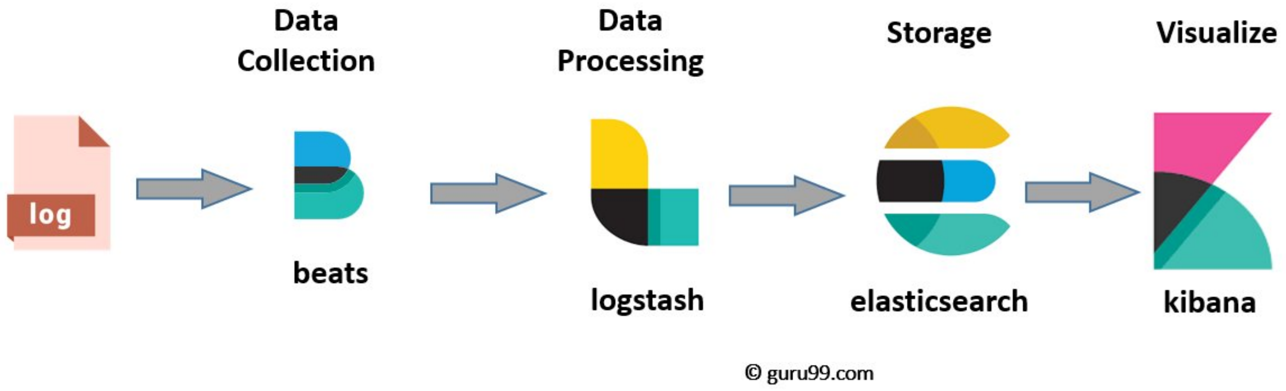
Here is the simple architecture of ELK stack



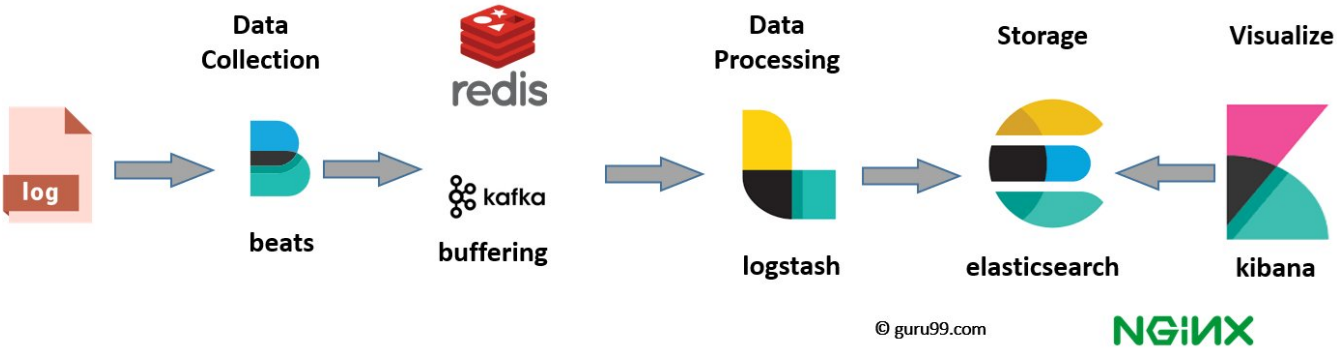
ELK Stack Architecture

- **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 is Store, Search, and indexed.
- **Kibana:** Kibana uses Elasticsearch DB to Explore, Visualize, and Share

However, one more component is needed or 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.



Now in this Elastic stack tutorial, **Let's deep dive all of these open source products:**

What is Elasticsearch?

Elasticsearch is a NoSQL database. It is based on Lucene search engine, and it is built with RESTful APIS. It offers simple deployment, maximum reliability, and easy management. It also offers advanced queries to perform detail analysis and stores all the data centrally. It is helpful for executing a quick search of the documents.

Elasticsearch also allows you to store, search and analyze big volume of data. It is mostly used as the underlying engine to powers applications that completed search requirements. It has been adopted in search engine platforms for modern web and mobile applications. Apart from a quick search, the tool also offers complex analytics and many advanced features.

Features of Elastic search:

- Open source search server is written using Java
- Used to index any kind of heterogeneous data
- Has REST API web-interface with JSON output
- Full-Text Search
- Near Real Time (NRT) search
- Sharded, replicated searchable, JSON document store
- Schema-free, REST & JSON based distributed document store
- Multi-language & Geolocation support

Advantages of Elasticsearch

- Store schema-less data and also creates a schema for your data
- Manipulate your data record by record with the help of Multi-document APIs
- Perform filtering and querying your data for insights
- Based on Apache Lucene and provides RESTful API
- Provides horizontal scalability, reliability, and multitenant capability for real time use of indexing to make it faster search
- Helps you to scale vertically and horizontally

Important Terms used in Elastic Search

Now in this ELK tutorial, let's learn about key terms used in ElasticSearch:

Term	Usage
Cluster	A cluster is a collection of nodes which together holds data and provides joined indexing and search capabilities.
Node	A node is an elasticsearch Instance. It is created when an elasticsearch instance begins.
Index	An index is a collection of documents which has similar characteristics. e.g., customer data, product catalog. It is very useful while performing indexing, search, update, and delete operations. It allows you to define as

	many indexes in one single cluster.
Document	It is the basic unit of information which can be indexed. It is expressed in JSON (key: value) pair. ‘{“user”: “nullcon”}’. Every single Document is associated with a type and a unique id.
Shard	Every index can be split into several shards to be able to distribute data. The shard is the atomic part of an index, which can be distributed over the cluster if you want to add more nodes.

What is Logstash?

Logstash is the data collection pipeline tool. It collects data inputs and feeds into the Elasticsearch. It gathers all types of data from the different source and makes it available for further use.

Logstash can unify data from disparate sources and normalize the data into your desired destinations. It allows you to cleanse and democratize all your data for analytics and visualization of use cases.

It consists of three components:

- **Input**: passing logs to process them into machine understandable format
- **Filters**: It is a set of conditions to perform a particular action or event
- **Output**: Decision maker for processed event or log

Features of Logstash

Now in this LogStash tutorial, let’s learn about features of LogStash:

- Events are passed through each phase using internal queues
- Allows different inputs for your logs
- Filtering/parsing for your logs

Advantage of Logstash

- Offers centralize the data processing
- It analyzes a large variety of structured/unstructured data and events
- ELK LogStash offers plugins to connect with various types of input sources and

platforms

What is Kibana?

Kibana is a data visualization which completes the ELK stack. This tool is used for visualizing the Elasticsearch documents and helps developers to have a quick insight into it. Kibana dashboard offers various interactive diagrams, geospatial data, and graphs to visualize complex quires.

It can be used for search, view, and interact with data stored in Elasticsearch directories. Kibana helps you to perform advanced data analysis and visualize your data in a variety of tables, charts, and maps.

In Kibana there are different methods for performing searches on your data.

Here are the most common search types:

Search Type	Usage
Free text searches	It is used for searching a specific string
Field-level searches	It is used for searching for a string within a specific field
Logical statements	It is used to combine searches into a logical statement.
Proximity searches	It is used for searching terms within specific character proximity.

Now in this Kibana tutorial, let's learn about important features of Kibana:

Features of Kinbana:

- Powerful front-end dashboard which is capable of visualizing indexed information from the elastic cluster
- Enables real-time search of indexed information
- You can search, View, and interact with data stored in Elasticsearch
- Execute queries on data & visualize results in charts, tables, and maps
- Configurable dashboard to slice and dice logstash logs in elasticsearch
- Capable of providing historical data in the form of graphs, charts, etc.
- Real-time dashboards which is easily configurable

- Kibana ElasticSearch enables real-time search of indexed information

Advantages and Disadvantages of Kinbana

- Easy visualizing
- Fully integrated with Elasticsearch
- Visualization tool
- Offers real-time analysis, charting, summarization, and debugging capabilities
- Provides instinctive and user-friendly interface
- Allows sharing of snapshots of the logs searched through
- Permits saving the dashboard and managing multiple dashboards

Why Log Analysis?

In cloud-based environment infrastructures, performance, and isolation is very important. The performance of virtual machines in the cloud may vary based on the specific loads, environments, and number of active users in the system. Therefore, reliability and node failure can become a significant issue.

Log management platform can monitor all above-given issues as well as process operating system logs, NGINX, IIS server log for web traffic analysis, application logs, and logs on AWS (Amazon web services).

Log management helps DevOps engineers, system admin to make better business decisions. Hence, log analysis via Elastic Stack or similar tools is important.

ELK vs. Splunk

Elk	Splunk
Elk is open source tool	Splunk is a commercial tool.
Elk stack does not offer Solaris Portability because of Kibana.	Splunk offers Solaris Portability.
Processing speed is strictly limited.	Offers accurate and speedy processes.
ELK is a technology stack created with the combination Elastic Search-Logstash-Kibana.	Splunk is a proprietary tool. It provides both on-premise and cloud solutions.

In ELK Searching, Analysis & Visualization will be only possible after the ELK stack is setup.	Splunk is a complete data management package at your disposal.
ELK tool does not support integration with other tools.	Splunk is a useful tool for setting up integrations with other tools.

Case Studies

NetFlix

Netflix heavily relies on ELK stack. The company using ELK stack to monitor and analyze customer service operation's security log. It allows them to index, store, and search documents from more than fifteen clusters which comprise almost 800 nodes.

LinkedIn

The famous social media marketing site LinkedIn uses ELK stack to monitor performance and security. The IT team integrated ELK with Kafka to support their load in real time. Their ELK operation includes more than 100 clusters across six different data centers.

Tripwire:

Tripwire is a worldwide Security Information Event Management system. The company uses ELK to support information packet log analysis.

Medium:

Medium is a famous blog-publishing platform. They use ELK stack to debug their production issues. The company also uses ELK to detect DynamoDB hotpots. Moreover, using this stack, the company can support 25 million unique readers as well as thousands of published posts each week.

Advantages and Disadvantages of ELK stack

Advantages

- ELK works best when logs from various Apps of an enterprise converge into a single ELK instance

- It provides amazing insights for this single instance and also eliminates the need to log into hundred different log data sources
- Rapid on-premise installation
- Easy to deploy Scales vertically and horizontally
- Elastic offers a host of language clients which includes Ruby. Python. PHP, Perl, .NET, Java, and JavaScript, and more
- Availability of libraries for different programming and scripting languages

Disadvantages

- Different components In the stack can become difficult to handle when you move on to complex setup
- There's nothing like trial and error. Thus, the more you do, the more you learn along the way

Summary

- Centralized logging can be useful when attempting to identify problems with servers or applications
- ELK server stack is useful to resolve issues related to centralized logging system
- ELK stack is a collection of three open source tools Elasticsearch, Logstash Kibana
- Elasticsearch is a NoSQL database
- Logstash is the data collection pipeline tool
- Kibana is a data visualization which completes the ELK stack
- In cloud-based environment infrastructures, performance and isolation is very important
- In ELK stack processing speed is strictly limited whereas Splunk offers accurate and speedy processes
- Netflix, LinkedIn, Tripware, Medium all are using ELK stack for their business
- ELK Syslog works best when logs from various Apps of an enterprise converge into a single ELK instance
- Different components In the stack can become difficult to handle when you move on to complex setup

Refer our ElasticSearch Interview Questions and Answers for fresher as well as experienced candidates.

You Might Like:

- Splunk Tutorial for Beginners: What is Splunk Tool? How to Use?
- 30 Best New Relic Alternatives (Open-Source & Paid) in 2022
- Best 8 Ansible Alternatives & equivalent in 2022
- 25 Best Remote Desktop Software (Remote Access Software)
- 10+ Best IT Automation Software Tools (Feb 2022)

← Prev

Report a Bug

Next →

About

About Us
Advertise with Us
Write For Us
Contact Us

Career Suggestion

SAP Career Suggestion Tool
Software Testing as a Career

Interesting

eBook
Blog
Quiz
SAP eBook

Execute online

Execute Java Online
Execute Javascript
Execute HTML
Execute Python