elastic stack

Agenda

01 What is ELK?

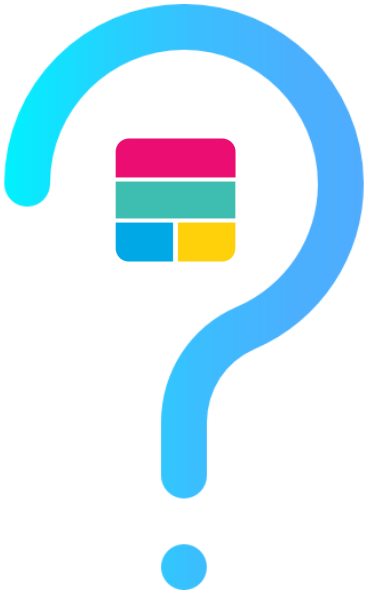
02 What are the components of ELK?

03 ELK Flow

04 Features of ELK

05 ELK Installation

06 ELK Hands-on



What is ELK?

What is ELK?

Elastic Stack (ELK) refers to a set of open-source products developed by Elastic to help its users collect data from different types of sources, analyze the collected data, and represent the analysis in an easy-to-understand and aesthetic visualization so that meaningful observations can be made

Learning how to use all components of Elastic Stack takes some time, but the payoff is great and grants a deeper understanding of the software's underlying structure

What are the components of ELK?

What are the components of ELK?

Elasticsearch	Logstash	Kibana	Beats
			
For storing and searching collected data	For collecting and filtering the input data	Provides a graphical user interface	Offers multiple light-weight data collectors

What are the components of ELK?

Elasticsearch

Logstash

Kibana

Beats

Elasticsearch is a NoSQL database that was developed based on Apache Lucene search engine. It can be used to index and store different types of documents and data. It provides a function to search for the data that is stored in real time as it’s being fed

What are the components of ELK?

Elasticsearch

Logstash

Kibana

Beats

Logstash is a collection agent used to collect both heterogenous/non-heterogenous data from various sources. It has the capability to screen, breakdown, and make string alterations in the data it collects. After collecting and filtering the data, it then sends it to Elasticsearch for storage

What are the components of ELK?

Elasticsearch

Logstash

Kibana

Beats

Kibana is a graphical user interface used to display the data that is collected and stored in Elasticsearch. It displays the data with appealing visuals so that the data could be easily understood and analyzed; it does so by using multiple types of visuals like bar chart, pie chart, world map, heat map, co-ordinate map, etc.

What are the components of ELK?

Elasticsearch

Logstash

Kibana

Beats

Features of Kibana

- Discover your data by exploring it
- Analyze your data by applying different metrics
- Visualize the data by creating different types of charts
- Apply Machine Learning on the data to get data anomaly
- Manage users and roles
- Offer a console to run Elasticsearch expressions
- Play with time-series data using Timeline
- Monitor your Elastic Stack using monitoring

What are the components of ELK?

Elasticsearch

Logstash

Kibana

Beats

Beats is similar to Logstash in the fact that they both collect data that will be later stored and analyzed, but Beats differs in the method of collection. Beats is a set of multiple small software installed on different servers from where they collect the data and send it to Elasticsearch

ELK Flow

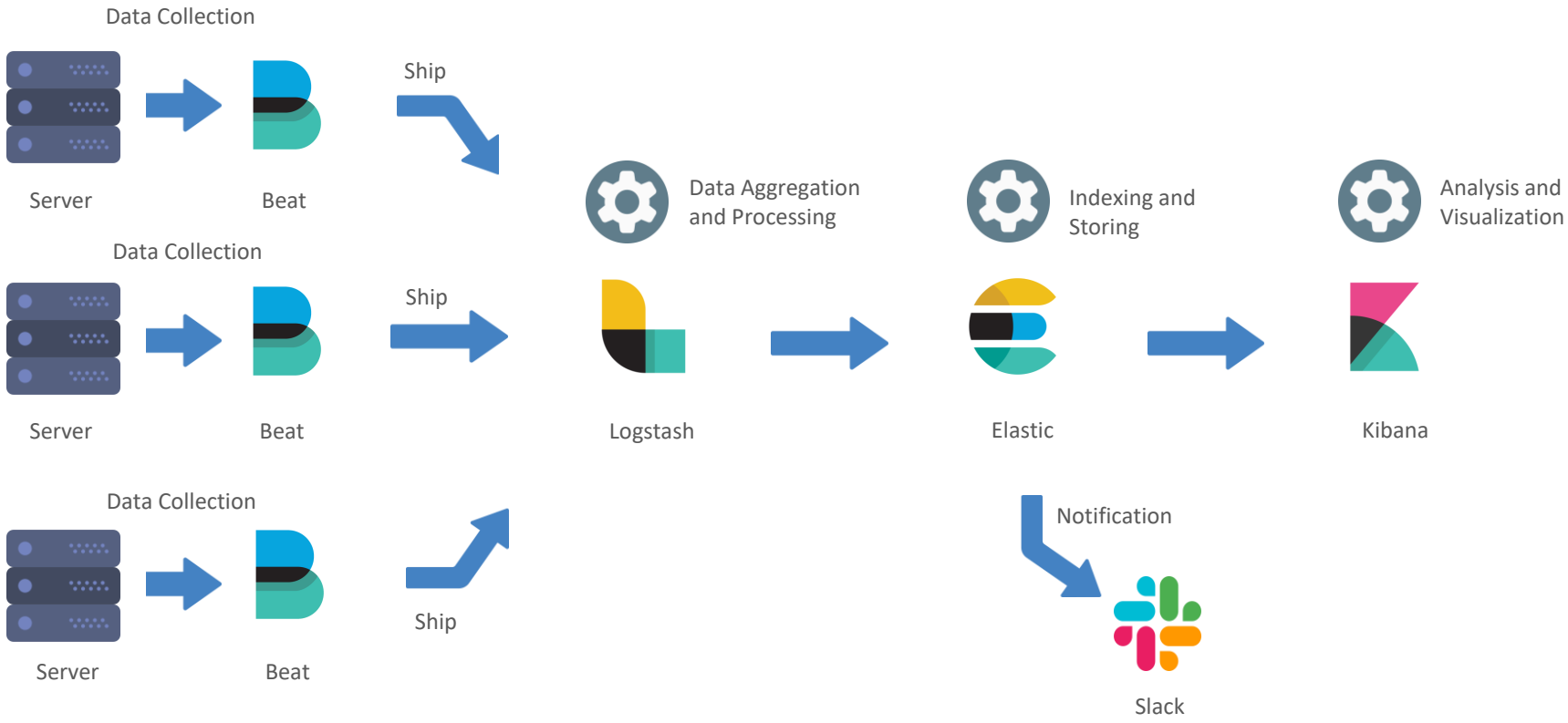
ELK Flow

First, Beats are attached to remote servers from where these Beats collect information from various sources

After collecting all the data needed, they either ship the data to Logstash for filtration or directly send it to Elasticsearch

The data is then stored in Elasticsearch. From here, it will not be directly sent to Kibana. Kibana first needs to find where Elastic is and then go and get the data by itself

ELK Flow


Data Collection
Server
Beat
Ship
Data Collection
Server
Beat
Ship
Data Collection
Server
Beat
Ship
Data Aggregation and Processing
Logstash
Indexing and Storing
Elastic
Analysis and Visualization
Kibana
Notification
Slack

Features of ELK

Features of ELK

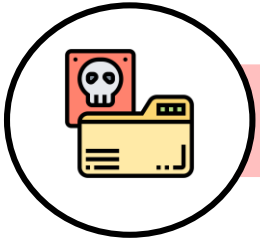
System Performance Monitoring

Log Management

Application Performance Monitoring

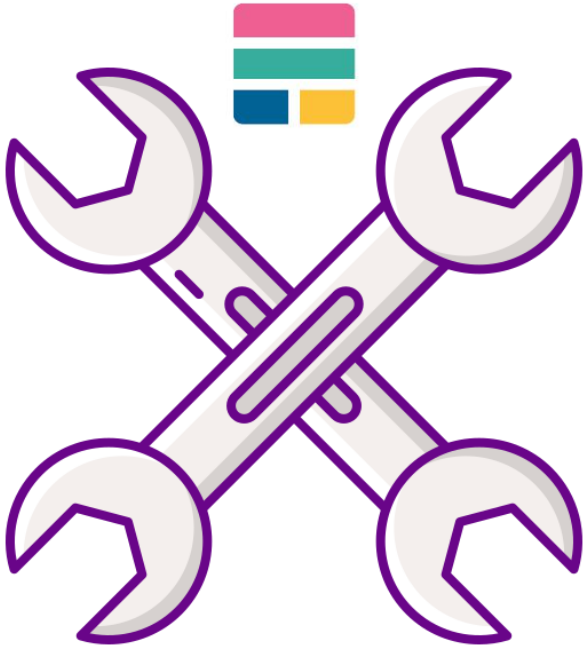
Features of ELK

Application Data Analysis



Security Monitoring and Alerting

Data Visualization

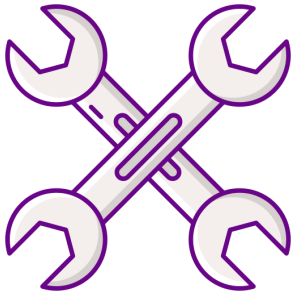


ELK Installation

ELK Installation

Prerequisites:

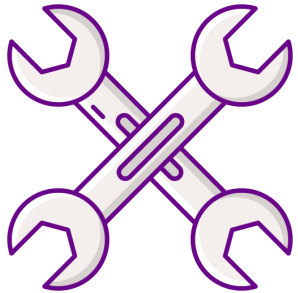
- At least 2 GB of RAM
- At least 20 GB storage
- JAVA



ELK Installation

Installing JAVA on the instance:

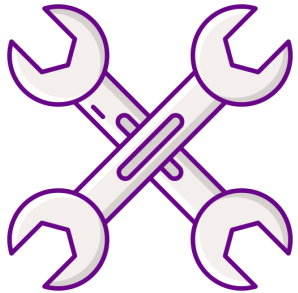
$ sudo apt-get update
$ sudo apt-get install -y openjdk-8-jdk



ELK Installation

Installing nginx on the instance:

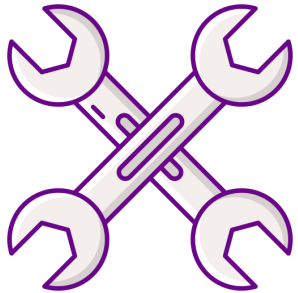
```
$ sudo apt-get update
$ sudo apt-get -y install nginx
$ sudo systemctl enable nginx
```



ELK Installation

Downloading and installing Elasticsearch:

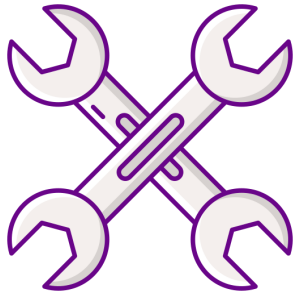
$ wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.2.0-amd64.deb
$ sudo dpkg -i elasticsearch-7.2.0-amd64.deb



ELK Installation

Downloading and installing Kibana:

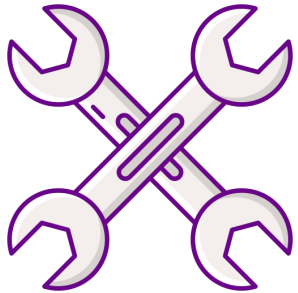
$ wget https://artifacts.elastic.co/downloads/kibana/kibana-7.2.0-amd64.deb
$ sudo dpkg -i kibana-7.2.0-amd64.deb



ELK Installation

Downloading and Installing Logstash:

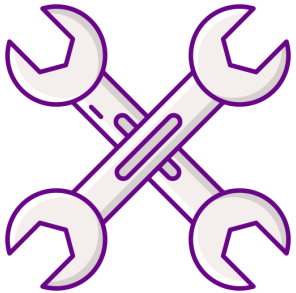
$ wget https://artifacts.elastic.co/downloads/logstash/logstash-7.2.0.deb
$ sudo dpkg -i logstash-7.2.0.deb



ELK Installation

Installing a few dependencies:

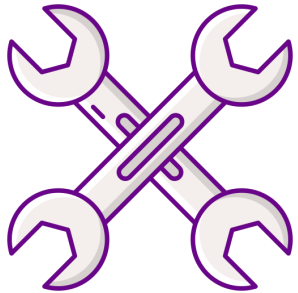
$ sudo apt-get install -y apt-transport-https

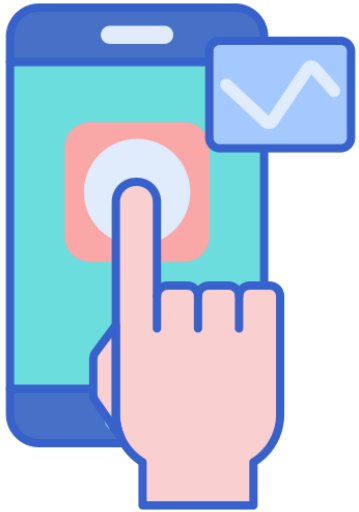


ELK Installation

Downloading and Installing Filebeat:

$ wget https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.2.0-amd64.deb
$ sudo dpkg -i filebeat-7.2.0-amd64.deb





ELK Hands-on

ELK Hands-on

1. Collect static Apache logs using Logstash and analyze them using Kibana

2. Collect static '.CSV' using Logstash and analyze them using Kibana

3. Collect and configure real-time web logs, inject them into Elasticsearch, and analyze them using Kibana