

- Elastic search is a search engine based on Apache Lucene library.
- Can think of it as a noSql database which can be communicated through via Json requests.
- Used for log analytics, full text search, security intelligence, business analytics and operational intelligence.
- Entirely written in Java.
- Often described as -> Search Engine, Analytics Database, index, big data solution, kind of like google
- distributed noSQL database in the form of JSON Documents
- Elastic as a company has many tools:
  - Kibana
  - LogStash
  - Beats
  - ECE
  - Elastic Cloud
  - Elastic Search
- The most enterprise search engine
- One of the 10 most popular dbms
- At its core, you can think of elasticsearch as a server that can process JSON requests and give you back JSON data in response.
- Way to query data from ElasticSearch is by using REST apis
- ELK Stack:
 

Elastic is a company that has released many components that work together and form a Stack. The core components together are called the ELK stack which refers to Elasticsearch, Logstash, and Kibana.

  - E** - Elasticsearch-> Distributed NoSql Database where you can store messages in the form of JSON. You can expose restful Apis from the elasticsearch instance.
  - L** - Logstash-> Another framework, collector that collects data from different sources and Streams, and it allows the streaming of data in the form of a data processing pipeline.  
**Imagine Elasticsearch as the database, and logstash as the streaming component which pushes the logs into the elasticsearch.**
  - K** - Kibana-> Visualization tool that is deploy dover the elasticsearch instance where you

can customized statistics, reports and dashboards from the data present in Elasticsearch.

**Use Cases:**

- Netflix
- Ebay
- walmart