Elastic stack

1)elk -elastic search log-stach kibana

2)efk – “” fluence “”

Elastic search is search engine for analytics, searching is done through queries.

Elk is used for APm, events, mainly used for analysing data. ElK stores data in the form of documents(fields) like sql. Request to elk will go as restAPI and response also from restAPI. It is written in JAVA and built on lucene(apache tool). It is highly scalable.

In elastic stack we have🡪elatic search, logstach, kibana, beats, x-pack

Kibana -> visualization platform, it pulls data from elastic-search , it can be integrated with elastic-search and logstach.

Kafka is a messaging tool

Logstach->data processing pipeline(.xml,json,csv…)used for filtering.

Data flow------🡪app->kafka->logstach->elastic->kibana

x-pack 🡪 used for security, reporting, altering, monitoring

beats🡪

Example

------------

Client 🡪webapp 🡪db

logstach

es 🡪 kibana(same or diff m/c)

from web app to es connection🡪in es we have elastic seq, jdbc driver..connects using http libraries

web app keeps update both es and db, if someone do full search it will search from es not db.

We can download elk in servers or directly in cloud we can use it.