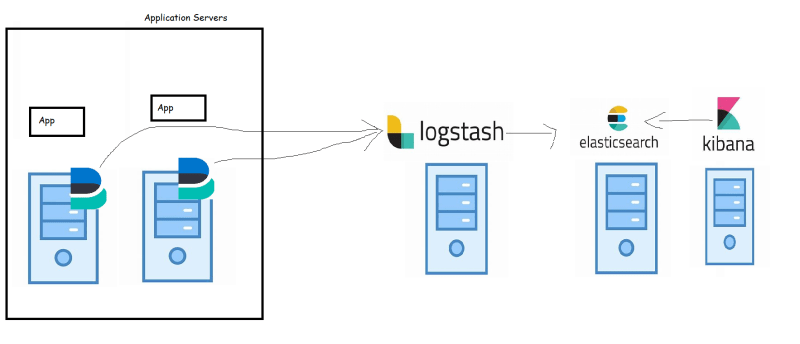
**What are logs**

* A log file records either events that occur in operatings or the software runs
* There are three kinds of logs
  + Event Log
  + Transactional logs
  + Message logs

**Components of Elastic Stack**

* Elastic Search: This store all your data and provides search and analytics capabilities in scalable way
* Logstash:
  + This helps in centralizing event data such as logs, metrics and other data in any format.
  + This can perform transformation
  + This is a server-side component.
  + Logstash enable collection of data from wide number of input sources and transforms and sends the logs to Elastic Search
* Kibana: This helps in providing visual interfaces to search the elastic search and provide analysis
* Beats:
  + This is complementary to Logstash
  + Beats is a client-side component.
  + Beats can read different logs and forward it to the Logstash/elastic search
* X-pack:
  + This pack has features such as
    - Security (Authentication and authorization)
    - monitoring
    - reporting
    - alerting
    - graph
    - machine learning



* Elastic Cloud: Elastic cloud is the hosted and managed setup of Elastic Stack components

**Installing Elastic Stack**

* Let’s take one server an install elastic search and Kibana in it.
* This server needs atleast 2 Vcpus and 4 GB of RAM
* This server will be a linux server with ubuntu distribution or centos distribution
* Installing elastic search on ubuntu <https://www.elastic.co/guide/en/elasticsearch/reference/current/install-elasticsearch.html>

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

sudo apt-get install apt-transport-https

echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list

sudo apt-get update && sudo apt-get install elasticsearch

* post configuration

sudo /bin/systemctl daemon-reload sudo /bin/systemctl enable elasticsearch.service