**What is an ELK stack?**ELK is a software stack used in data pipelines for logging data and turning it into visualisations  
In our case, this data will be coming from EC2 instances

E - ElasticSearch (Analytics engine For transforming raw data in order to run complex  
queries and recieve complex summaries)  
L - Logstash (For collecting and transforming data. In our case, this data will be taken from  
logs sent from EC2 instances via Filebeats)  
K - Kibana (Used for turning the transformed & analysed data into visualisations eg   
historams, line graphs, pie charts and maps. )

**How it works (with diagram):**  
You attach filebeats to each server you want to monitor and manage. File beats is a lightweight shipper which is used for forwarding and centralizing log data. Once attached, Filebeat will monitor the log files/locations that are specified. This data is then either sent to Elasticsearch or Logstash where it will be indexed. In this project, the data will be sent to Logstash. Logstash will then dynamically ingest the data, then transform it regardless of the data’s complexity or format. When logstash receives data, it filters prase each event. It will then identify the named fields to build structure after which it transforms them to converge on a format more common which allows for more powerful analysis and increases business value. This is then sent over to Elasticsearch. Elasticsearch allows you to accomplish and combine a variety of different searches; whether it be structured, unstructured, geo metric. Elasticsearch aggregation allow you to zoom out to then discover patterns and trends within the data. The transformed data is then sent to Kibana which visualizes the data in a much more aesthetically.

**Networking:**

All three services communicate using different ports. Elasticsearch communicates using port using 9200, Logstash uses port 5044 where is Kibana uses port 5601.

For them to communicate Logstash will need to send a certificate to the client,

Logstash 5044 which talks to file beast . go thru filter into elasticsearch -> elasticsearch talks to kibana using 9200 then kibana sends it to a url

**Prerequisites:**  
Oracle VirtualBox  
Vagrant  
Chef

**To run the ELK stack:**  
As this vagrant set up has two VMs, the ELK Stack and the client, they need to be spun up separately (i.e. vagrant up ELK in one gitbash and vagrant up client in another). These machines will become suspended and access to the Kibana Dashboard will be available with IP 192.168.10.120.

Click on the left side where it says “filebeat.\*” and click on the start to make this the default index, you can now view the Kibana stats under the “Discover” tab at the top of the Dashboard.

What the finished result should look like:

Problems encountered during development:

In an ideal world where you manage multiple servers, you'd like a way to monitor their performance easily.  
The easiest to monitor things is with.