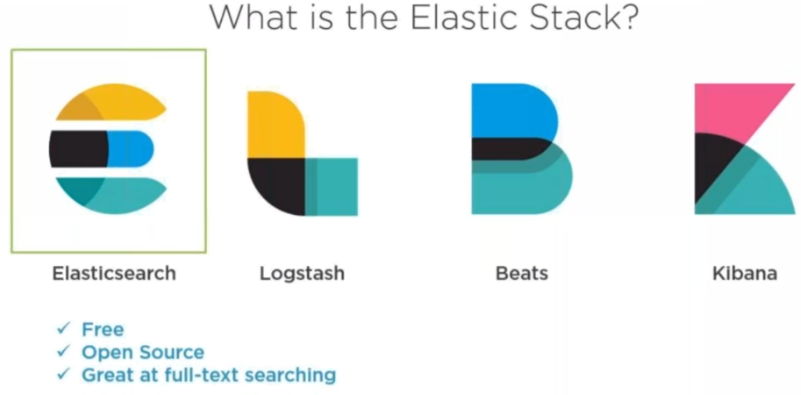
**Elastic Stack:**

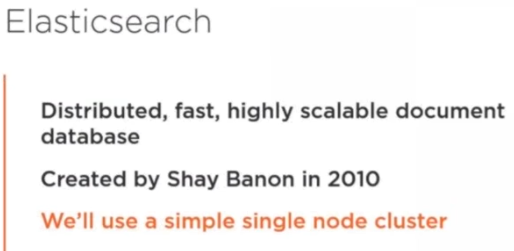
* ELK has 4 components
* Elastic search
* Logstash
* Kibana
* Beats
* ES is like database, we can pull logs from any machine and store in ES
* Kibana UI
* Logstash used to convert into other formats. It reads and sends to some other destination (ES)
* Beats are personalisation. We can ask to send only some related logs

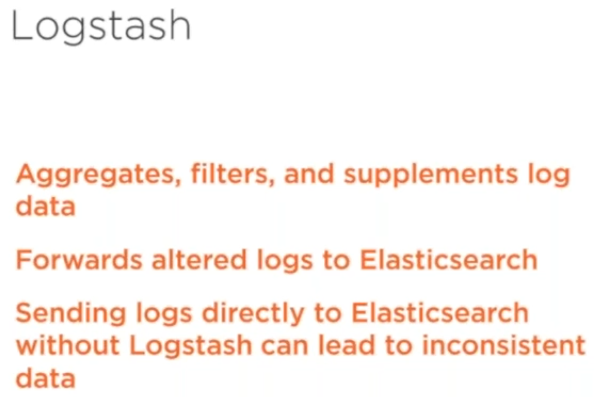


* Text search is very good in elastic search

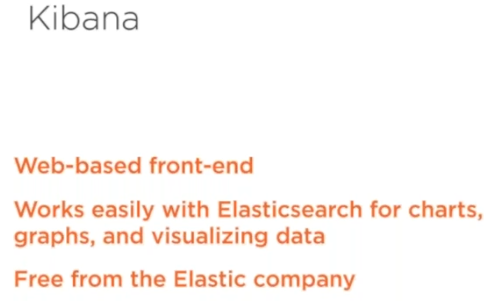


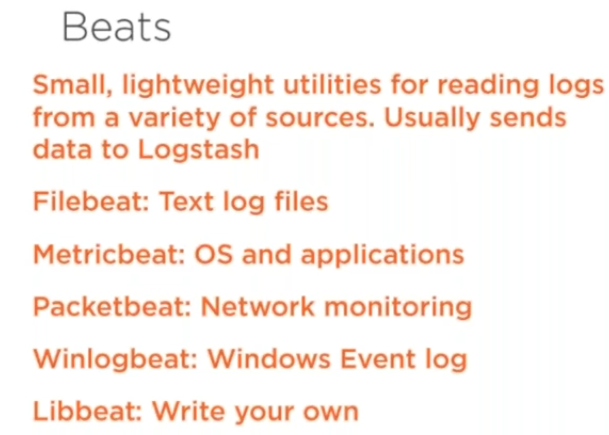
* There might many servers like db, web etc
* Our responsibility is to build a monitoring solution for this



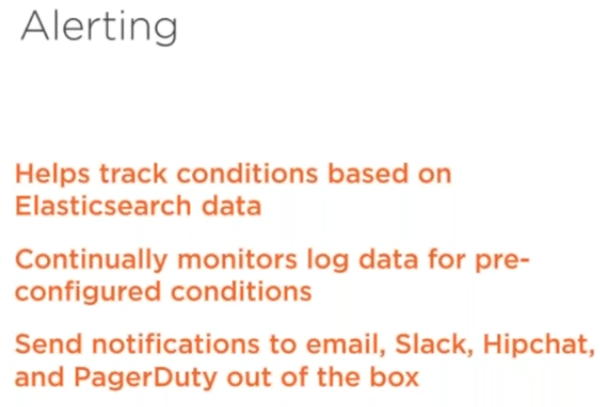


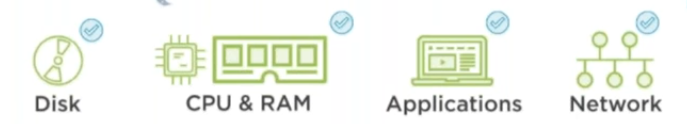
* Logstash is mainly used to convert the logs in the way which we want

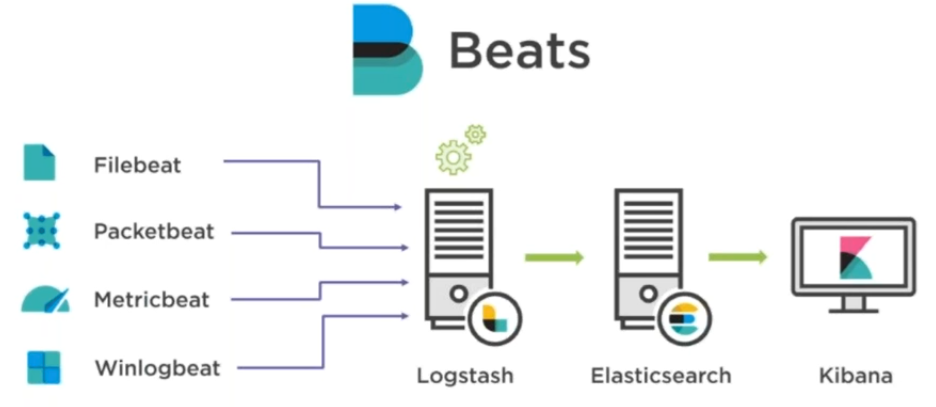




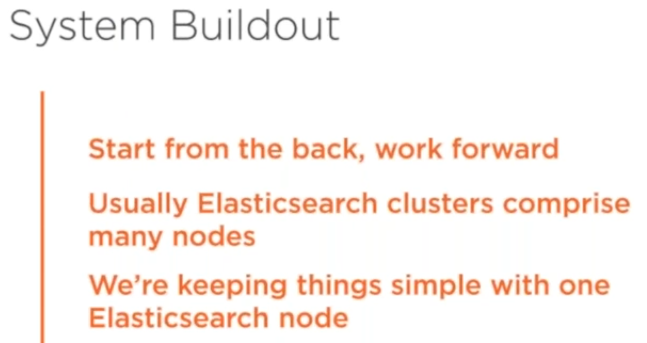
* It can send the logs directly to the elastic search also. But there might be some inconsistency if we do like that







* We have different beats components, they talk with logstash and it speaks with elastic search and the same we can view in kibana



* We can use either Linux or windows