ELK Stack:

The **ELK stack** consists of Elasticsearch, Logstash, and Kibana. Although they've all been built to work exceptionally well together, each one is a separate project that is driven by the open-source vendor Elastic—which itself began as an enterprise search platform vendor

**Elastic Stack** is a group of open source products from **Elastic** designed to help users take data from any type of source and in any format and search, analyze, and visualize that data in real time.

**Logstash** is an open source tool for collecting, parsing, and storing logs for future use. Kibana 3 is a web interface that can be used to search and view the logs that**Logstash** has indexed. Both of these tools are based on Elasticsearch. Elasticsearch, **Logstash**, and Kibana, when used together is known as an ELK stack.

**Kibana** is an open source data visualization plugin for Elasticsearch. It provides visualization capabilities on top of the content indexed on an Elasticsearch cluster. Users can create bar, line and scatter plots, or pie charts and maps on top of large volumes of data.

**ELK** Installation:-

 the ELK Stack is most commonly used in log analysis

Elasticsearch is a NoSQL database. That means it stores data in an unstructured way and that you cannot use SQL to query it. Unlike most NoSQL databases, though, Elasticsearch has a strong focus on search capabilities and features — so much so, in fact, that the easiest way to get data from Elasticsearch is to search for it using the REST API

sudo apt-get update

2 sudo add-apt-repository ppa:webupd8team/java

3 sudo apt-get install software-properties-common

4 sudo apt-get install python3-software-properties

5 sudo apt-get install python-software-properties

6 sudo apt-get update

7 sudo apt-get install oracle-java8-installer

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

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

10 sudo wget -qo -https://packages.elastic.co/GPG-KEY-elasticsearch|sudo apt-key add-

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

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

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

14 sudo wget -qO - https://packages.elastic.co/GPG-KEY-elasticsearch | sudo apt-keyadd -

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

16 sudo wget -O - https://packages.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add –

17 echo "deb https://packages.elastic.co/elasticsearch/2.x/debian stable main" | sudo tee -a /etc/apt/sources.list.d/elasticsearch-2.x.list

18 sudo apt-get update

19 sudo apt-get install elasticsearch

20 sudo service elasticsearch restart

21 sudo update-rc.d elasticsearch defaults 95 10

22 curl -X GET <http://localhost:9200>

23 echo "deb https://packages.elastic.co/logstash/2.3/debian stable main" | sudo tee -a /etc/apt/sources.list

24 sudo apt-get update

25 sudo apt-get install logstack

26 sudo apt-get install logstash

27 sudo service logstash restart

28 sudo service logstash status

29 sudo service logstash start

30 sudo update-re.d logstash defaults 96 9

31 sudo update-rc.d logstash defaults 96 9

32 sudo apt-get install apache2 -y

33 sudo service apache2 restart

34 sudo apt-get update

35 sudo wget <https://download.elastic.co/kibana/kibana/kibana-4.5.0-linux-x64.tar.gz>

36 sudo apt-get update

37 ls

38 sudo tar -xvzf kibana-4.5.0-linux-x64.tar.gz

39 sudo mkdir -p /var/www/kibana

40 ls

41 sudo cp -R ~/kibana-4.5.0-linux-x64/\* /var/www/kibana/

42 cd /var/www/kibana/

43 ls

44 sudo nano /etc/apache2/conf-enabled/kibana.conf

45 sudo service apache2 restart

46 sudo service kibana start

47 sudo service kibana stop

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

49 history

50 echo "deb http://packages.elastic.co/kibana /4.5/debian stable main" | sudo tee -a /etc/apt/sources.list

51 sudo apt-get update

52 echo "deb https://packages.elastic.co/kibana /4.5/debian stable main" | sudo tee -a /etc/apt/sources.list

53 apt-get update

54 sudo apt-get update

55 echo "deb https://packages.elastic.co/kibana/4.5/debian stable main" | sudo tee -a /etc/apt/sources.list

56 sudo apt-get update

57 sudo service kibana start

58 cd

59 wget -qO - https://packages.elastic.co/GPG-KEY-elasticsearch | sudo apt-get add –

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

61 echo "deb http://packages.elastic.co/kibana/4.5/debian stable main" | sudo tee -a /etc/apt/sources.list

62 sudo apt-get update

63 sudo service kibana status

64 ls

65 sudo apt-get install kibana

66 echo "deb http://packages.elastic.co/kibana/4.5/debian stable main" | sudo tee -a /etc/apt/sources.listsudo apt-get update

67 sudo apt-get update

68 sudo apt-get install kibana

69\* Duplicate sources.list entry http://packages.elastic.co/kibana/4.5/debian/ stable/main amd64 Packages (/var/lib/apt/lists/packages.elastic.co\_kibana\_4.5\_debi

70 Duplicate sources.list entry http://packages.elastic.co/kibana/4.5/debian/ stable/main amd64 Packages (/var/lib/apt/lists/packages.elastic.co\_kibana\_4.5\_debian\_dists\_stable\_main\_binary-amd64\_Packages)

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

72 echo "deb http://packages.elastic.co/kibana/4.5/debian stable main" | sudo tee -a /etc/apt/sources.list

73 sudo apt-get update

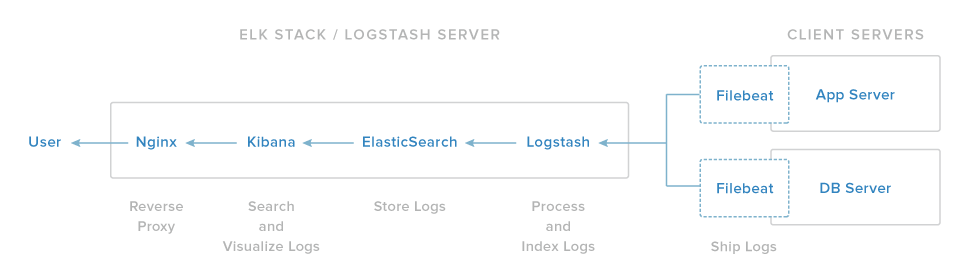
74 cd /etc/apt/sources.list.d/

75 ls

76 echo "deb http://packages.elastic.co/kibana/4.4/debian stable main" | sudo tee -a /etc/apt/sources.list.d/kibana-4.4.x.list

77 sudo apt-get update

sudo apt-get -y install kibana

79 history

Why we need to use ELK stack?

**Problem statement:**

You have different applications feeding into each other. Debugging an issue requires logging into each individual box to look at the logs. With small number of apps/boxes it's not an issue, but it quickly becomes tedious as the number of apps/boxes increase!

**Solution:**

It would be awesome to have all of your logs aggregated into one place so you can see the process flow and perform queries against the logs from all applications from one place.

Enter ELK stack. It will also improve your heart health because no need to log into 100 different boxes to follow the logs!

**What is ELK stack?**

ELK stands for Elasticsearch, Logstash and Kibana.

Brief definitions:

**Logstash:** It is a tool for managing events and logs. You can use it to collect logs, parse them, and store them for later use (like, for searching). Speaking of searching, logstash comes with a web interface for searching and drilling into all of your logs. It is fully free and fully open source.

**Elasticsearch**: Elasticsearch is a search server based on Lucene. It provides a distributed, multitenant-capable full-text search engine with a RESTful web interface and schema-free JSON documents.

**Kibana**: A nifty tool to visualize logs and timestamped data.

**How do we use it?**

Here's one possible (and recommended) architecture diagram that helps visualize the flow of log information: 

As shown in the diagram: App 1...App n are generating logs. Logstash shipper\* is reading the logs from a log file and sending the logs to a redis database. Logstash in the *ELK stack* is reading off of the redis database, feeding that information on to *elasticsearch*. *Kibana* is a configrable web dashboard that is querying elastic search for log information and presenting it to the user. Logstash of course can be configured to read logs/register events from a myriad of sources and send log events to multiple different sources. We will cover *Logstash* in more depth in a different post.