***Elasticsearch Installation***

**Distribution:** Elastic

**Version:** 5.6.2

1. Copy the **ELK** directory from pendrive to home directory (/home/jpasolutions)
2. Open the terminal (Ctrl+Alt+t)
3. Change the directory to ELK

~$ cd ~/ELK

1. Extract the Elasticsearch(ES) tar file under home directory (/home/jpasolutions)

~$ tar -xzvf elasticsearch-5.6.2.tar.gz -C $HOME

1. Set up the environment variables in ~/.bashrc file

export ES\_HOME=/home/jpasolutions/elasticsearch-5.6.2

export PATH=$PATH:$ES\_HOME/bin

1. Environment variables to reflect on the current shell, source the file.

~$ source ~/.bashrc

1. Check the changes applied properly

~$ echo $ES\_HOME

~$ which elasticsearch

1. Start Elasticsearch service

~$ elasticsearch -d

**Note:** This will start the elasticsearch in background.

1. Check if Elasticsearch is up and running

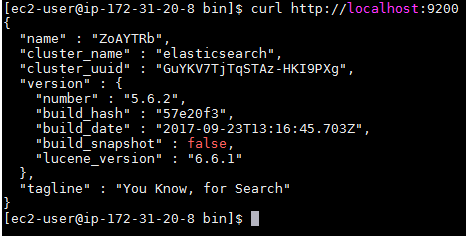
~$ jps

**Note:** You should be able to see Elasticsearch

1. Verify the ES installation

~$ curl <http://localhost:9200>

Sample screenshot is given below



***Logstash Installation***

**Distribution:** Elastic

**Version:** 5.6.2

1. Copy the **ELK** directory from pendrive to home directory (/home/jpasolutions)

**Note:** Ignore this step if you are already done this on Elasticsearch installation

1. Open the terminal (Ctrl+Alt+t)
2. Change the directory to ELK

~$ cd ~/ELK

1. Extract the Logstash(LS) tar file under home directory (/home/jpasolutions)

~$ tar -xzvf logstash-5.6.2.tar.gz -C $HOME

1. Set up the environment variables in ~/.bashrc file

export LS\_HOME=/home/jpasolutions/logstash-5.6.2

export PATH=$PATH:$LS\_HOME/bin

1. Environment variables to reflect on the current shell, source the file.

~$ source ~/.bashrc

1. Check the changes applied properly

~$ echo $LS\_HOME

~$ which logstash

1. Start Logstash service

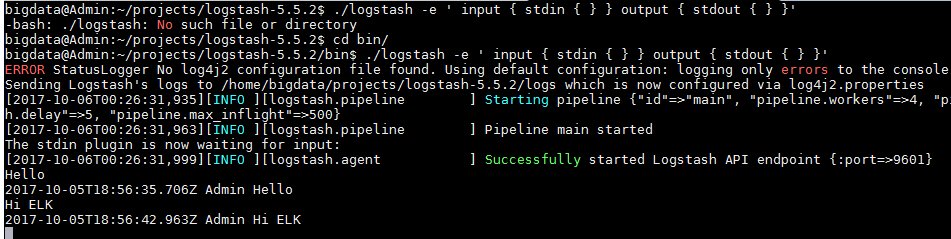
There is no service required to start.

1. Verify the LS installation

~$ logstash -e ' input { stdin { } } output { stdout { } }'

**Note:**

* Wait for the line “Successfully started Logstash API endpoint {:port=>9601}”
* This will start the logstash service which will accept the input from console and output the same on the console with Date, Time and Hostname
* Sample Screenshot is given below



***Kibana Installation***

**Distribution:** Elastic

**Version:** 5.6.2

1. Copy the **ELK** directory from pendrive to home directory (/home/jpasolutions)
2. Open the terminal (Ctrl+Alt+t)
3. Change the directory to ELK

~$ cd ~/ELK

1. Extract the Kibana tar file under home directory (/home/jpasolutions)

~$ tar -xzvf kibana-5.6.2.tar.gz -C $HOME

1. Set up the environment variables in ~/.bashrc file

export KIBANA\_HOME=/home/jpasolutions/kibana-5.6.2

export PATH=$PATH:$KIBANA\_HOME/bin

1. Environment variables to reflect on the current shell, source the file.

~$ source ~/.bashrc

1. Check the changes applied properly

~$ echo $KIBANA\_HOME

~$ which kibana

1. Start Kibana Service

~$ kibana

**Note:** This will start the kibana in foreground. Open new window for other tasks

1. Verify the Kibana installation

Open the browser and hit the URL “http://localhost:5601”