**ELK Stack**

**Installation guide**

**1.** Install **Java 8**

<http://www.javahelps.com/2015/03/install-oracle-jdk-in-ubuntu.html>

Java and other tools doesn’t need actual installation (just unzip, set env var, add to path)

(set environment variable to java home)

export JAVA\_HOME=/usr/java/jdk1.5.0\_07

**2.** Install **Elasticsearch**

(<https://www.elastic.co/guide/en/elasticsearch/reference/6.0/zip-targz.html> )

wget<https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.0.0.zip>

sha1sum elasticsearch-6.0.0.zip

unzip elasticsearch-6.0.0.zip

cd elasticsearch-6.0.0/

(set environment variable to elastic home)

export ES\_HOME=<elastic\_install\_path>

*run:*

./bin/elasticsearch

**3.** Install **Kibana**

(<https://www.elastic.co/guide/en/kibana/6.0/install.html> )

wget<https://artifacts.elastic.co/downloads/kibana/kibana-6.0.0-linux-x86_64.tar.gz>

sha1sum kibana-6.0.0-linux-x86\_64.tar.gz

tar -xzf kibana-6.0.0-linux-x86\_64.tar.gz

cd kibana-6.0.0-linux-x86\_64/

*run:*

./bin/kibana

**4.** Install **Logstash**

(<https://www.elastic.co/downloads/logstash> )

download and unzip:<https://artifacts.elastic.co/downloads/logstash/logstash-6.0.0.zip>

copy [apache\_logstash.conf file](https://raw.githubusercontent.com/elastic/examples/master/Common%20Data%20Formats/apache_logs/logstash/apache_logstash.conf) to /conf folder

copy [apache\_template.json file](https://raw.githubusercontent.com/elastic/examples/master/Common%20Data%20Formats/apache_logs/logstash/apache_template.json) to /bin folder

*run:*

./bin/logstash -f apache\_logstash.conf

**5.** Open in browser **[http://localhost:5601](http://localhost:5601/)**

select Discover on the left menu (still *no* data)

**6.** Inject some sample **logs** messages:

[open apache\_logs, copy all rows](https://raw.githubusercontent.com/elastic/examples/master/Common%20Data%20Formats/apache_logs/apache_logs)

open logstash command window (4) and just paste it there

**7.** Return to the browser and hit **refresh** (should show the injected logs messages and graph)

(in case you still don’t see data select dates range on the right-up side of Discover)