**Installtion steps for Logstash:**

step 1: Download and install the Public Signing Key:

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

step 2: You may need to install the apt-transport-https package on Debian before proceeding:

**sudo apt-get install apt-transport-https**

step 3: Save the repository definition to /etc/apt/sources.list.d/elastic-5.x.list:

**echo "deb https://artifacts.elastic.co/packages/5.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-5.x.list**

step 4: Run sudo apt-get update and the repository is ready for use. You can install it with:

sudo apt-get update

**sudo apt-get update && sudo apt-get install logstash**

**To start logstash:**

**sudo systemctl start logstash.service**

**Directory Layout of Debain Packages:**

The Debian package and the RPM package each place config files, logs, and the settings files in the appropriate locations for the system:

| Type | Description | Default Location | Setting |
| --- | --- | --- | --- |
| home | Home directory of the Logstash installation. | /usr/share/logstash |  |
| bin | Binary scripts including logstash to start Logstash and logstash-plugin to install plugins | /usr/share/logstash/bin |  |
| settings | Configuration files, including logstash.yml, jvm.options, and startup.options | /etc/logstash | path.settings |
| conf | Logstash pipeline configuration files | /etc/logstash/conf.d | path.config |
| logs | Log files | /var/log/logstash | path.logs |
| plugins | Local, non Ruby-Gem plugin files. Each plugin is contained in a subdirectory. Recommended for development only. | /usr/share/logstash/plugins | path.plugins |
| data | Data files used by logstash and its plugins for any persistent needs. | /var/lib/logstash | path.data |

**Filebeats Installation process**

step 1: Download and install the Public Signing Key:

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

step 2: You may need to install the apt-transport-https package on Debian before proceeding:

**sudo apt-get install apt-transport-https**

step3: Save the repository definition to /etc/apt/sources.list.d/elastic-5.x.list:

**echo "deb https://artifacts.elastic.co/packages/5.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-5.x.list**

step 4: Run apt-get update, and the repository is ready for use. For example, you can install Filebeat by running:

**sudo apt-get update && sudo apt-get install filebeat**

step 5: To configure the Beat to start automatically during boot, run:

**sudo update-rc.d filebeat defaults 95 10**

**Directory layout for Filebeat**

Filebeat uses the following default paths unless you explicitly change them.

| Type | Description | Location |
| --- | --- | --- |
| home | Home of the Filebeat installation. | /usr/share/filebeat |
| bin | The location for the binary files. | /usr/share/filebeat/bin |
| config | The location for configuration files. | /etc/filebeat |
| data | The location for persistent data files. | /var/lib/filebeat |
| logs | The location for the logs created by Filebeat. | /var/log/filebeat |

**Elastic Search:**

Download tar file from  **https://www.elastic.co/downloads/elasticsearch**

unpack the file and run **bin/elastisearch**

**Installing Kibana**

**sudo apt-get update && sudo apt-get install kibana**

**If any problem:**

**Check with your** kibana.yml **file, whether correct configuration is present or not**

uncomment below line at /etc/kibaba/kibana.yml

#The Elasticsearch instance to use for all your queries.

elasticsearch\_url: "http://localhost:9200"

### **Running Kibana with systemd**

To configure Kibana to start automatically when the system boots up, run the following commands:

**sudo /bin/systemctl daemon-reload**

**sudo /bin/systemctl enable kibana.service**

Kibana can be started and stopped as follows:

**sudo systemctl start kibana.service**

**sudo systemctl stop kibana.service**

**to check --> sudo service kibana/apache status**

open browser and enter 127.0.0.1:5601/status and check for the elastic search confguration

**Configuring ELK stack**

**step 1.) configuring logstash with filebeats:**

Go to **/etc/filebeat** and open filebeat.yml file as a root user(with sudo permission)

1 add path for your logfiles

2. comment the Elastcsearch output part

# output.elasticsearch:

# Array of hosts to connect to.

# hosts: ["localhost:9200"]

3. Uncomment the logstash output part

output.logstash:

# The Logstash hosts

hosts: ["localhost:5044"]

save the file

**step 2**

go to /usr/share/logstash/bin and create logstash configguration file

for example:

/usr/share/logstash/bin/first-pipeline.conf ##for logstash

**# The # character at the beginning of a line indicates a comment. Use**

**# comments to describe your configuration.**

**input {**

**beats{**

**port => "5044"**

**}**

**}**

**# The filter part of this file is commented out to indicate that it is**

**# optional.**

**# filter {**

**# }**

**output {**

**stdout { codec => rubydebug }**

**elasticsearch {**

**hosts => ["127.0.0.1:9200"]**

**}**

**}**

set the path using below command

**sudo -Hu logstash /usr/share/logstash/bin/logstash --path.settings=/etc/logstash -t**

To verify your configuration, run the following command:

Go to **/usr/share/logstash/bin**

**sudo ./logstash -f first-pipeline.conf --config.test\_and\_exit**

The --config.test\_and\_exit option parses your configuration file and reports any errors.

If the configuration file passes the configuration test, start Logstash with the following command:

**before running logstash, run elastic search otherwise we will get error**

**for ruuning elastic search go the extracted path of elastic search and run bin/elasticsearch**

**then run logstash**

**sudo ./logstash -f first-pipeline.conf --config.reload.automatic**

**after that run filebeat:**

**Go to /usr/share/filebeat/bin and run**

**sudo ./filebeat -e -c /etc/filebeat/filebeat.yml -d "publish"**

**Open browser and enter 127.0.0.1:5601 ## kibana**

**You will find indexes and events if ElK works as expected**

**Elastic search commands**

list all indexes:

[**http://localhost:9200/\_cat/indices?v&pretty**](http://localhost:9200/_cat/indices?v&pretty)

**curl -XGET 'localhost:9200/\_cat/indices?v&pretty'**

**delete index**

**curl -XDELETE 'localhost:9200/logstash-2017.11.14?pretty'**

**overview:**

**(precaution--> first run elastic serach--> logstash-->filebeat-->kibana(browser))**

1988 sudo ./elasticsearch

1989 ./elasticsearch

1990 cd

1991 cd /usr/share/logstash/bin/

1992 ls

1993 sudo ./logstash -f first-pipeline.conf --config.test\_and\_exit

1994 sudo ./logstash -f first-pipeline.conf --config.reload.automatic