**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

Running logstash:

**Goto: /usr/share/logstash/bin**

and run below command:

**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. | {extract.path}- Directory created by unpacking the archive |  |
| bin | Binary scripts, including logstash to start Logstash and logstash-plugin to install plugins | {extract.path}/bin |  |
| settings | Configuration files, including logstash.yml and jvm.options | {extract.path}/config | path.settings |
| logs | Log files | {extract.path}/logs | path.logs |
| plugins | Local, non Ruby-Gem plugin files. Each plugin is contained in a subdirectory. Recommended for development only. | {extract.path}/plugins+ | path.plugins |
| data | Data files used by logstash and its plugins for any persistent needs. | {extract.path}/data | 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 |

**configuring logstash with filebeats:**

**filebeat.yml**

**open the file with sudo ====> /etc/filebeat/filebeat.yml -- for filebeat**

**then modify the file using below lines**

filebeat.prospectors:

# Each - is a prospector. Most options can be set at the prospector level, so

# you can use different prospectors for various configurations.

# Below are the prospector specific configurations.

- input\_type: log

# Paths that should be crawled and fetched. Glob based paths.

paths:

#- /var/log/\*.log

- /opt/ltp/results/\*.log

#- c:\programdata\elasticsearch\logs\\*

#comment out the elastic search output part

and uncomment the logstash output part

**#----------------------------- Logstash output --------------------------------**

**output.logstash:**

**# The Logstash hosts**

**hosts: ["localhost:5044"]**

**/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:

Goto : /usr/share/logstash/bin

execute below command

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

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

Goto: **/usr/share/logstash/bin**

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

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

**runninng filebeat:**

**goto : /usr/share/filebeat/bin**

and run below command

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

**Elastic Search:**

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

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

**Kibana Installation process:**

**https://www.elastic.co/guide/en/kibana/current/deb.html**

**--------------------------------------**

Download and install the public signing key:

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

sudo apt-get install apt-transport-https

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

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

### Running Kibana with systemd[edit](https://github.com/elastic/kibana/edit/5.6/docs/setup/install/systemd.asciidoc)

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

|  |  |  |
| --- | --- | --- |
|  |  |  |

### Directory Layout of Debian and RPM Packages[edit](https://github.com/elastic/logstash/edit/6.0/docs/static/setting-up-logstash.asciidoc)

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 |

### Directory Layout of Docker Images[edit](https://github.com/elastic/logstash/edit/6.0/docs/static/setting-up-logstash.asciidoc)

The Docker images are created from the .tar.gz packages, and follow a similar directory layout.

| 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 and jvm.options | /usr/share/logstash/config | path.settings |
| conf | Logstash pipeline configuration files | /usr/share/logstash/pipeline | path.config |
| plugins | Local, non Ruby-Gem plugin files. Each plugin is contained in a subdirectory. Recommended for development only. | /usr/share/logstash/plugins | path.plugins |



Logstash Docker containers do not create log files by default. They log to standard output.