In this demo tutorial we will learn how to run multiple filebeat instances in the linux system.

Filebeat is one of the Elastic beats and is a lightweight shipper for collecting, forwarding and centralising event log data. It can forward the logs it is collecting to either Elasticsearch or logstash for direct indexing or for further processing before being sent to Elasticsearch for indexing.

**Install & configure filebeat on ubuntu 20.04**

To install filebeat from Elastic repos;

apt install filebeat

Once the installation is done. Configure the endpoints for sending the logs.

Edit the configuration file, **/etc/filebeat/filebeat.yml**

You can set output as per your requirement.

#================================ Outputs =====================================

# Configure what output to use when sending the data collected by the beat.

#-------------------------- Elasticsearch output ------------------------------

**# output.elasticsearch:**

**# Array of hosts to connect to.**

**# hosts: ["localhost:9200"]**

# Optional protocol and basic auth credentials.

#protocol: "https"

#username: "elastic"

#password: "changeme"

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

**output.logstash:**

**# The Logstash hosts**

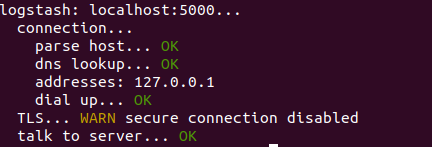
**hosts: ["127.0.0.1:5044"]**

For testing filebeat output connection:

Write this commands

systemctl stop filebeat

Filebeat -e test output



Testing the config for any errors

filebeat -e test config

**Run multiple instance in linux:**

**What is systemd:**

It provides an array of system components for linux. Primary component is “system and service manager” .

It also provides replacement for various darmons and utilities including event logging.

As in our example, we want to collect various logs and send them to various outputs.

Copy the default systemd service unit renaming it accordingly.

cp /lib/systemd/system/filebeat.service /etc/systemd/system/filebeat-elasticsearch.service

Edit the configuration file for the custom service unit and set the appropriate directory.

nano /etc/systemd/system/filebeat-elasticsearch.service

[Unit]

Description=Filebeat sends log files directly to Elasticsearch.

Documentation=https://www.elastic.co/products/beats/filebeat

Wants=network-online.target

After=network-online.target

[Service]

Environment="BEAT\_LOG\_OPTS="

Environment="BEAT\_CONFIG\_OPTS=-c **/etc/filebeat-elasticsearch/filebeat.yml**"

Environment="BEAT\_PATH\_OPTS=--path.home /usr/share/filebeat --path.config **/etc/filebeat-elasticsearch** --path.data **/var/lib/filebeat-elasticsearch** --path.logs **/var/log/filebeat-elasticsearch**"

ExecStart=/usr/share/filebeat/bin/filebeat --environment systemd $BEAT\_LOG\_OPTS $BEAT\_CONFIG\_OPTS $BEAT\_PATH\_OPTS

Restart=always

[Install]

WantedBy=multi-user.target

**Reload Systemd configurations:**

systemctl daemon-reload

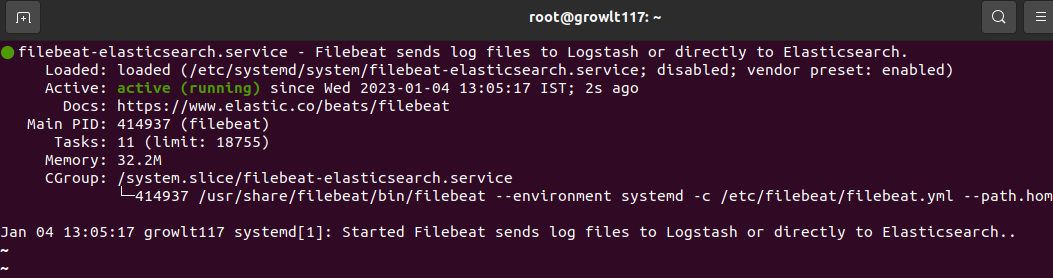
**Start the service:**

systemctl start filebeat-elasticsearch

**Check the status:**

systemctl status filebeat-elasticsearch

If everything is good you will see the following:



That means, we have 2 filebeat instances running.

Now we need to set up filebeat as per our requirements.

Edit filebeat.yml file, /etc/filebeat-elasticsearch/filebeat.yml

output.logstash:

# The Logstash hosts

hosts: ["localhost:2324"]

Now what we need to do is just set up a logstash pipeline for 2nd service.

Here i am open a port 2324 using ufw allow 2324

2nd pipeline code:

input {

tcp{

port => 2324

type => syslog

}

}

output {

elasticsearch {

hosts => ["localhost:9200"]

index => "second\_filebeat"

}

}

So, after that just restart the service using:

systemctl restart filebeat-elasticsearch

As per process, when I request on port localhost:2324 log will be generated and a second\_filebeat index will be generated.

Request on browser: [localhost:2324](https://docs.google.com/document/u/0/d/1tOQC0MrdmDBFWXmaZc3pI4E91zrgi5sZelM_UhDzcX0/edit)

You will see the following:

