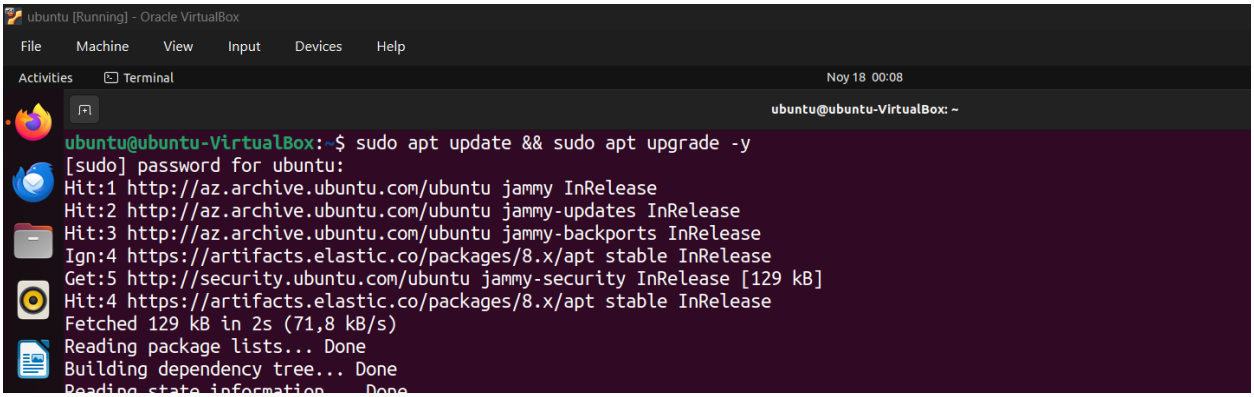
ELK Deploy step by step

1) Update and Upgrade system

1) Let’s update and upgrade our system

sudo apt update && sudo apt full-upgrade –y



2) İnstalling Elastic Search and configure file

1) Install the public key for elastic search

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg

2) Install the apt package that allows https package downloads

sudo apt-get install apt-transport-https

3) Save the repo in the elastic sources list

echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list

4) Then update apt again and install Elastic Search

sudo apt-get update && sudo apt-get install elasticsearch

5) Open the Elastic configuration file

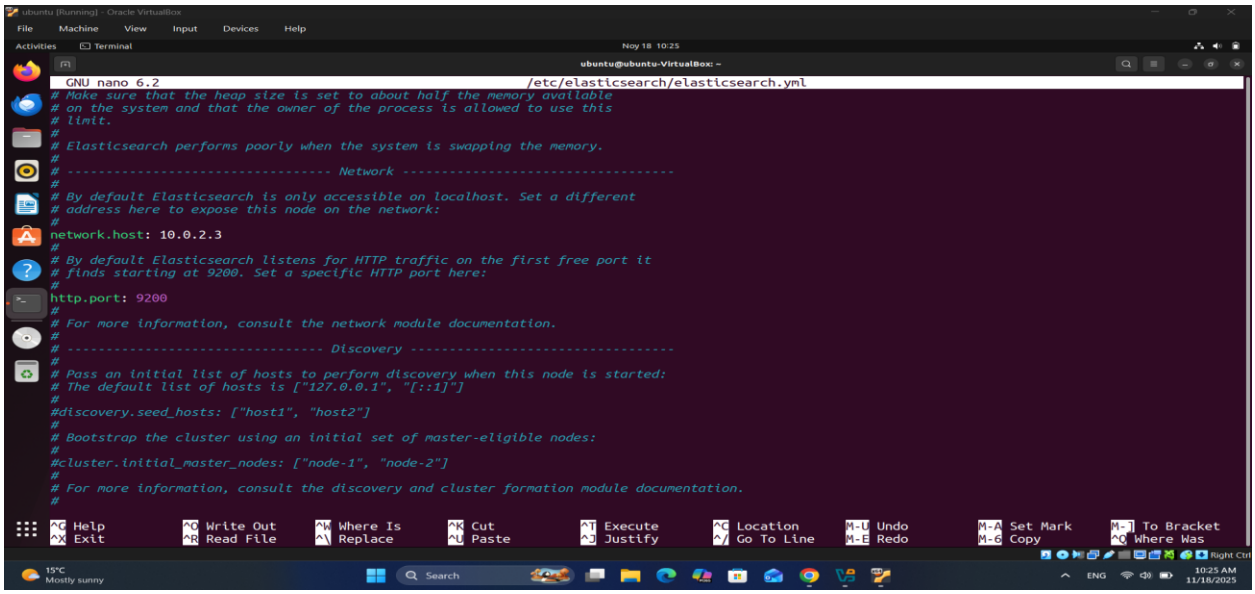
sudo nano /etc/elasticsearch/elasticsearch.yml

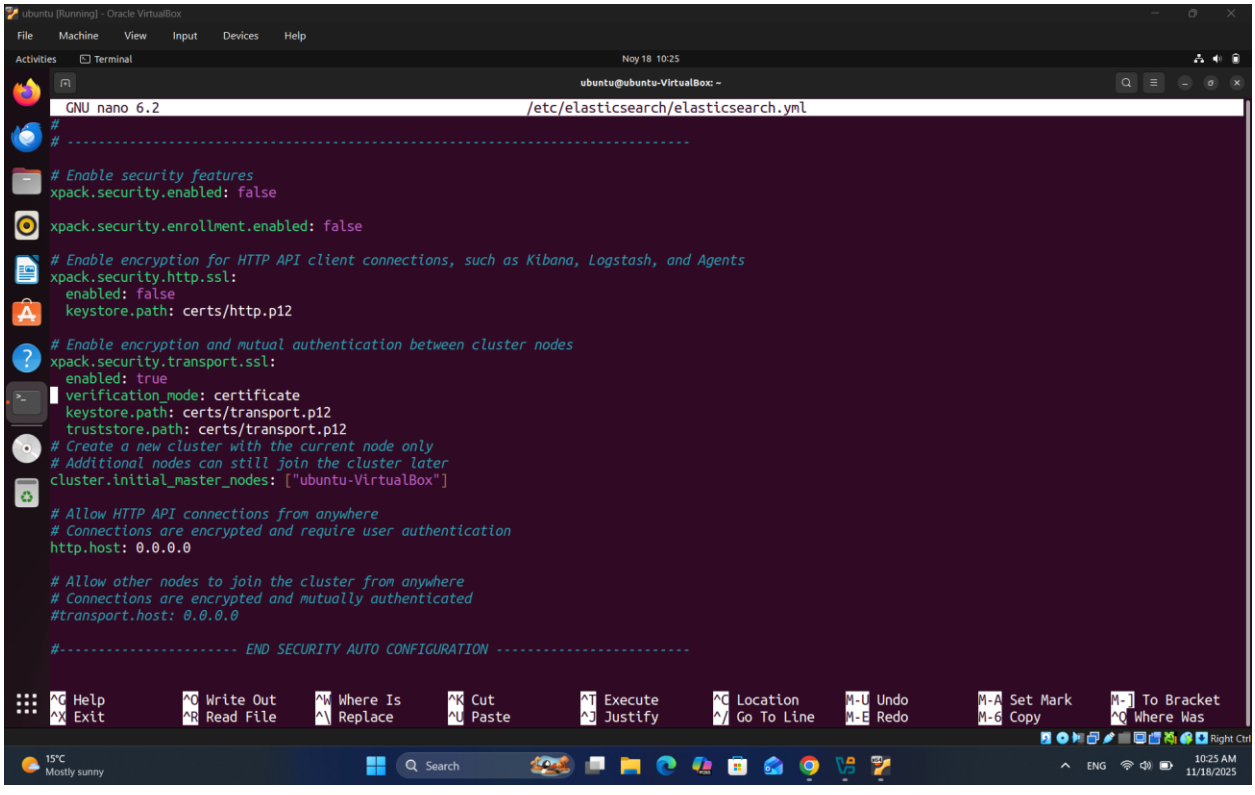
Configure these>

network.host: 10.0.2.3

http.port: 9200

xpack.security.enabled: false



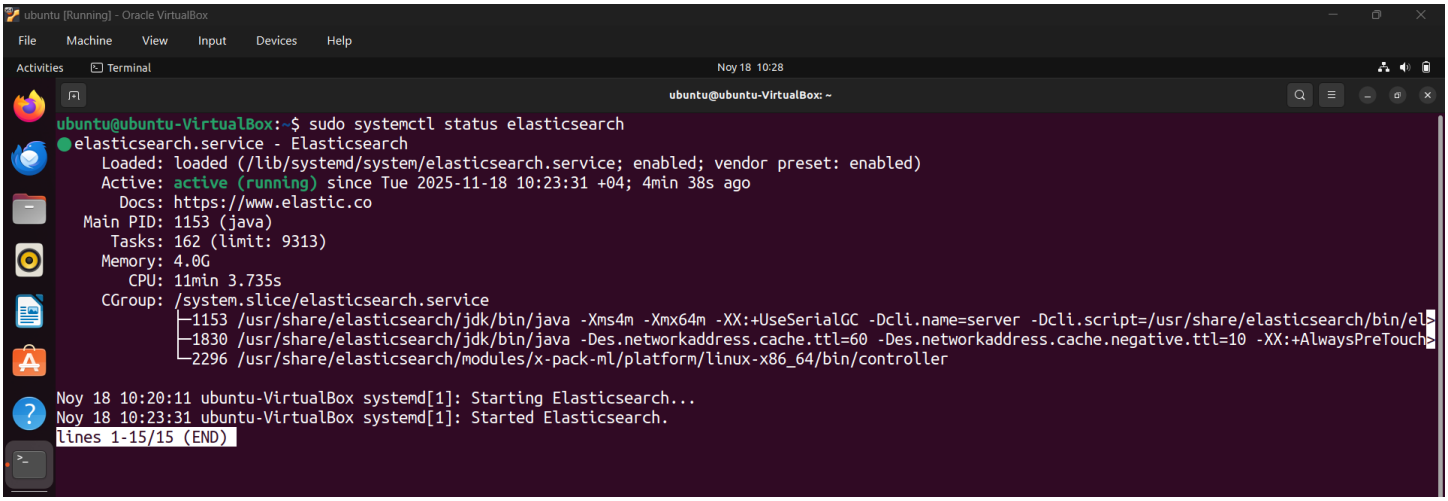


6) Enable and start the service.

sudo systemctl enable elasticsearch && sudo systemctl start elasticsearch

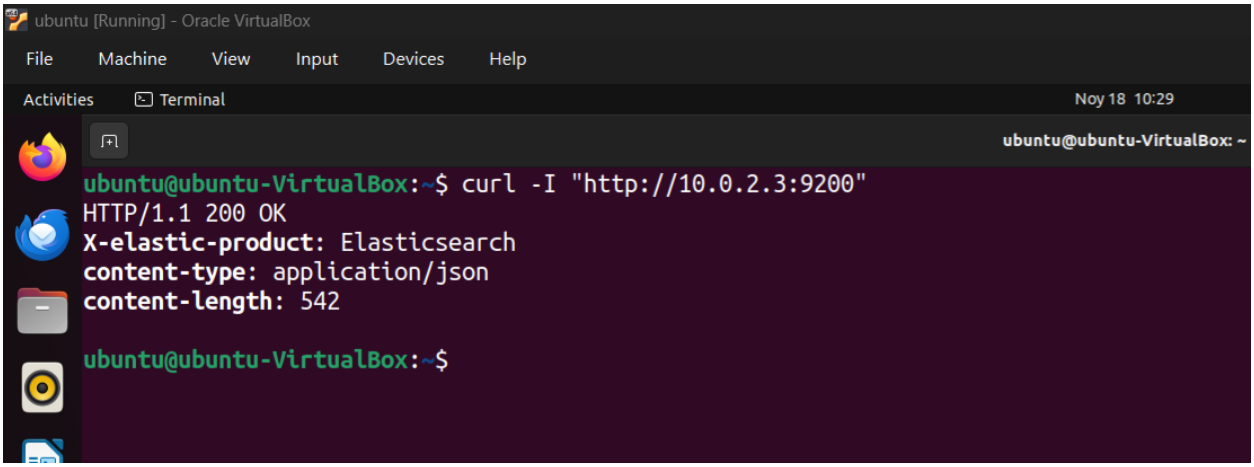
7) Check the status

sudo systemctl status elasticsearch



8) Verify the server is responding to queries

curl -I "http://10.0.2.3:9200"



3) İnstall Logstash and configure file

1) İnstall Logstash

sudo apt install logstash

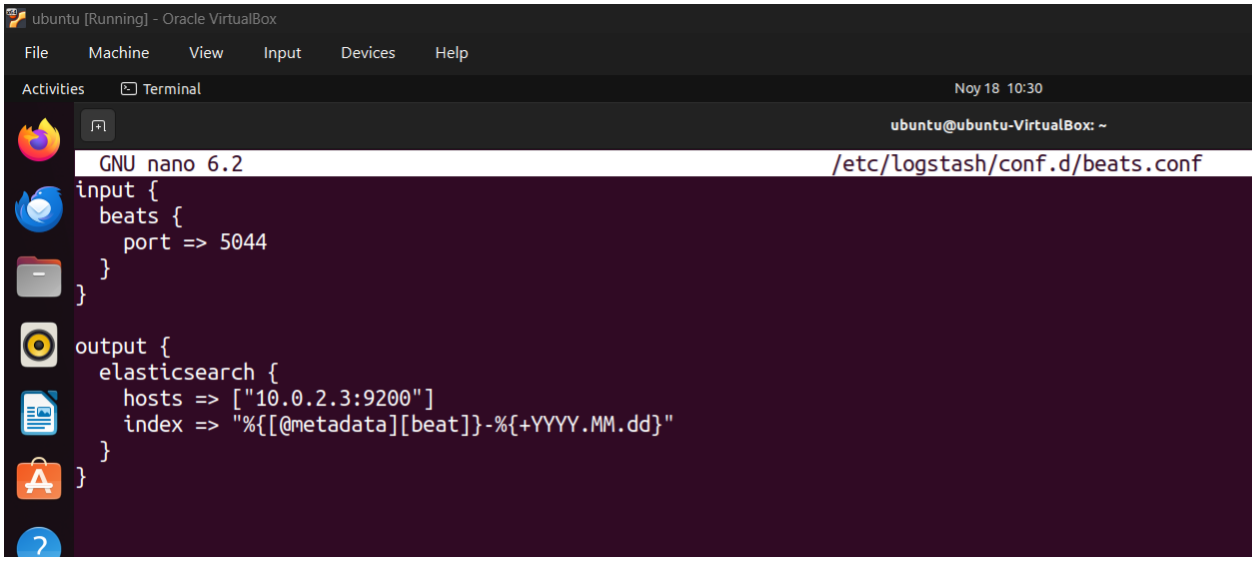
2) Create a filter in Logstash for the Filebeat data we're sending.

sudo nano /etc/logstash/conf.d/beats.conf

Configure file>

```
nput {
  beats {
    port => 5044
  }
}

output {
  elasticsearch {
    hosts => ["10.0.2.3:9200"]
    index => "%{[@metadata][beat]}-%{+YYYY.MM.dd}"
  }
}
```

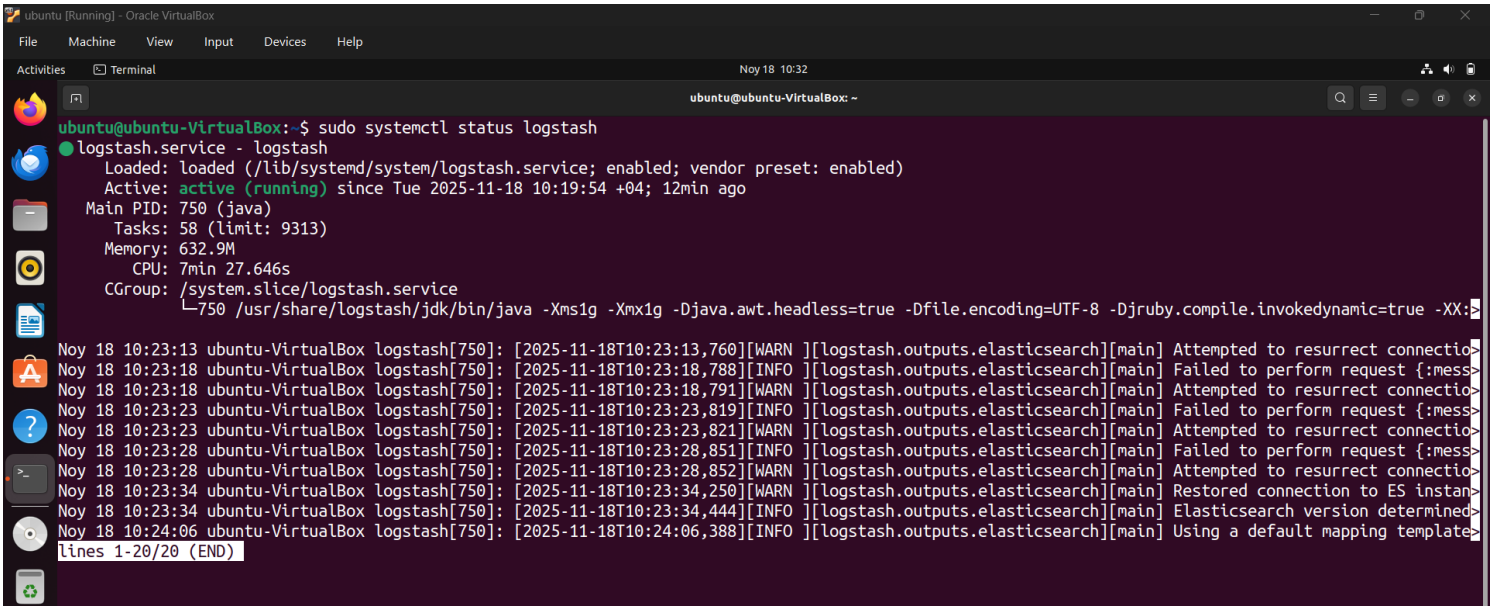


3) Enable and start Logstash.

sudo systemctl enable logstash && sudo systemctl start logstash

4) Logstash's status

sudo systemctl status logstash



4)İnstall Kibana and configure file

1) Install Kibana

sudo apt install kibana

2) Kibana file configuration

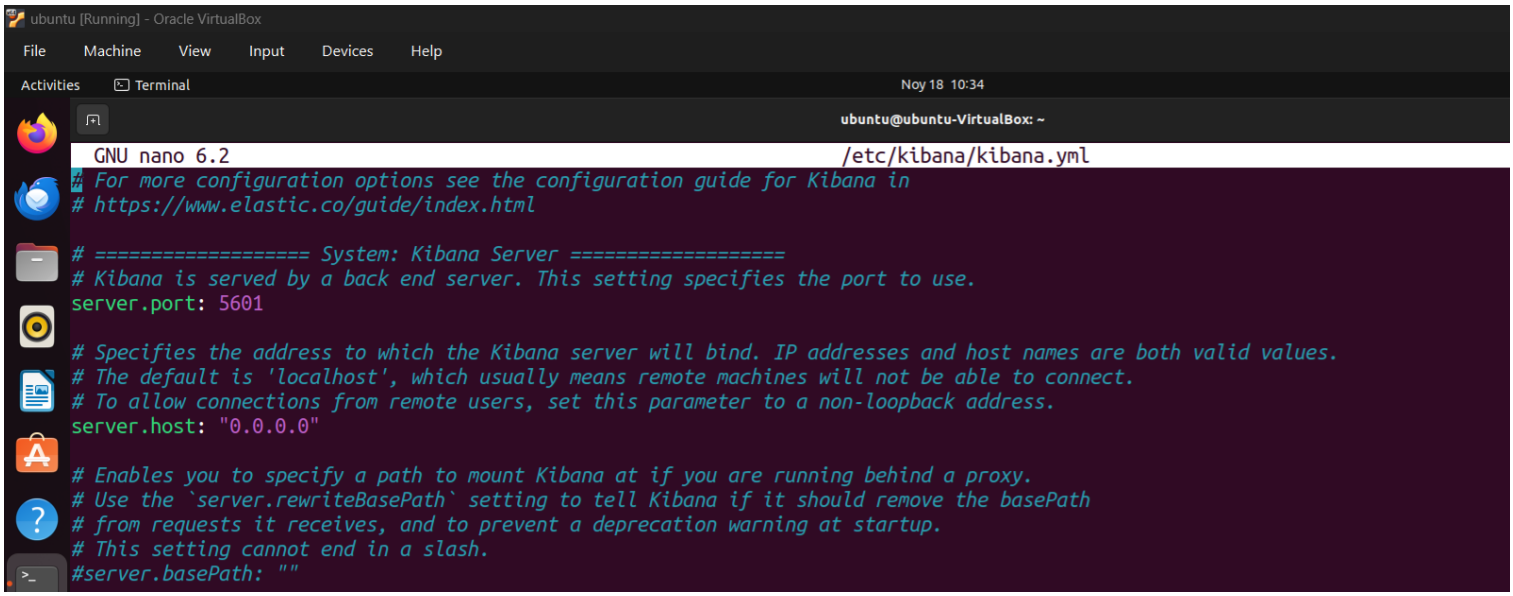
sudo nano /etc/kibana/kibana.yml

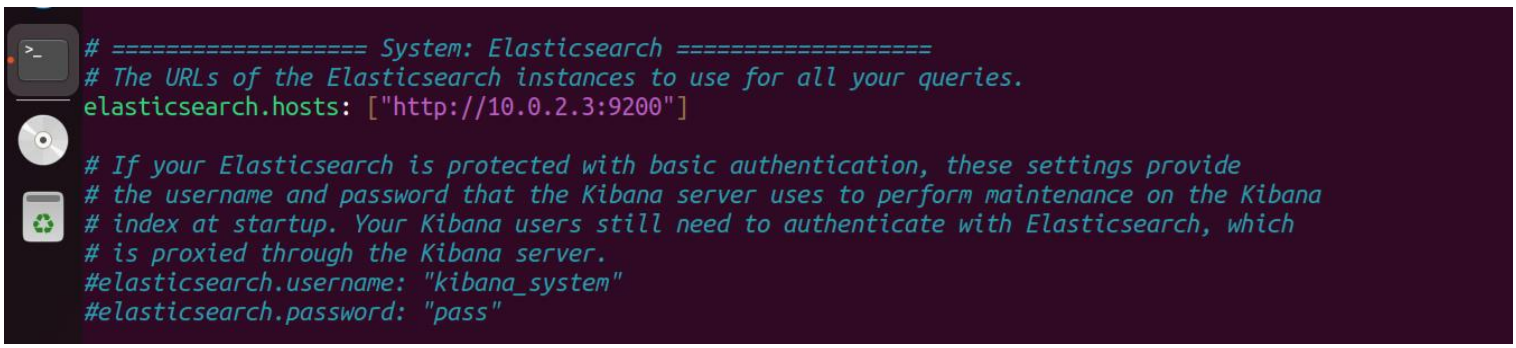
Configure file>

server.port: 5601

server.host: "0.0.0.0"

elasticsearch.hosts: [http://10.0.2.3:9200]



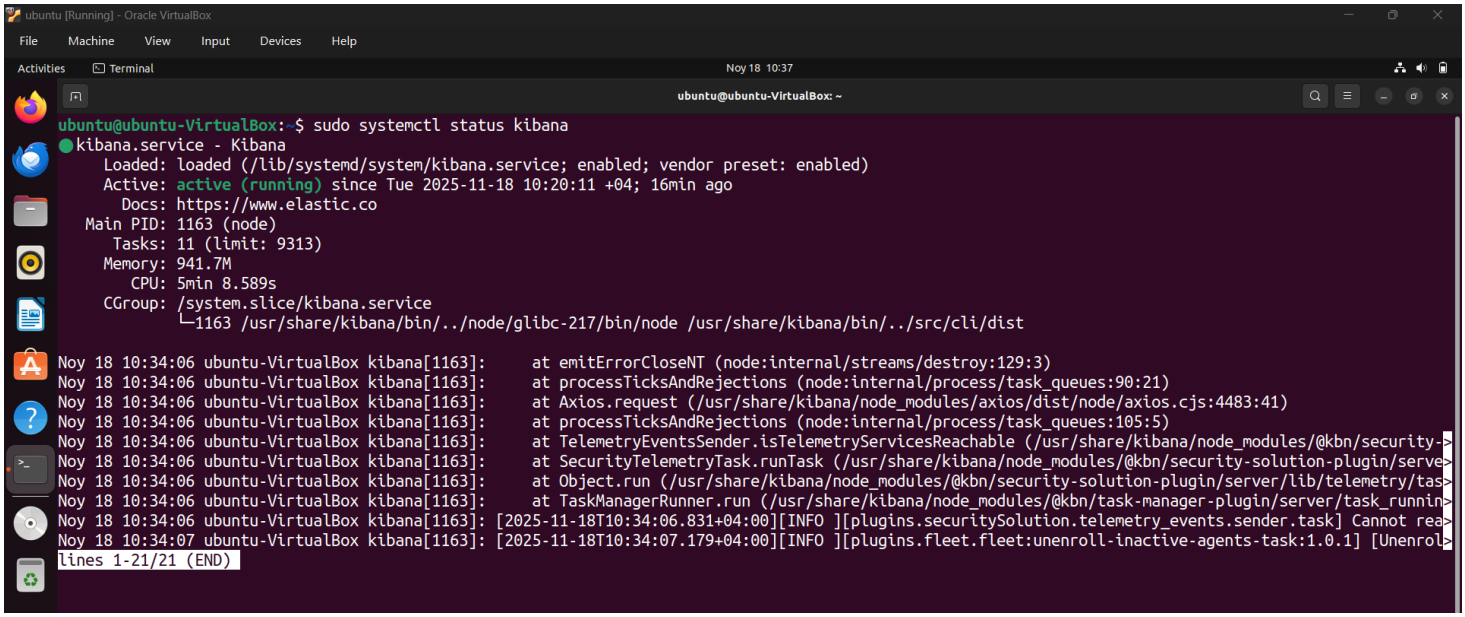


3) Enable and start Kibana

sudo systemctl enable kibana && sudo systemctl start kibana

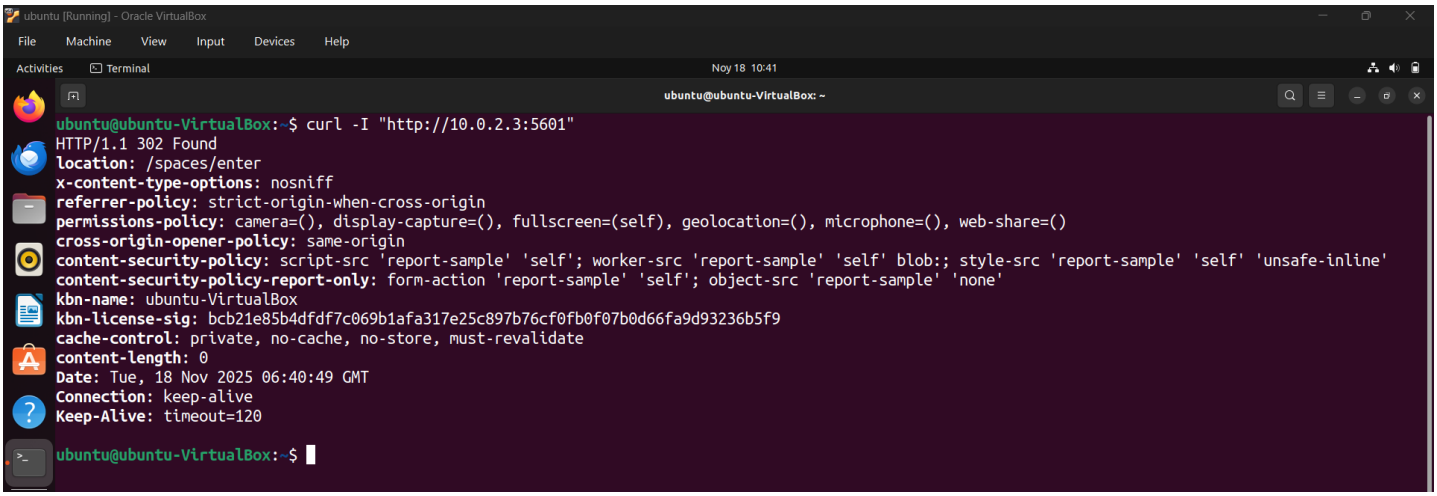
4) Kibana's status

sudo systemctl status kibana



5) Verify the server is responding to queries

curl -I "http://10.0.2.3:5601"



5) İnstall Filebeat and configure file

1) Install Filebeat

curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-8.9.2-amd64.deb

sudo dpkg -i filebeat-8.9.2-amd64.deb

2) Filebeat's configuration file

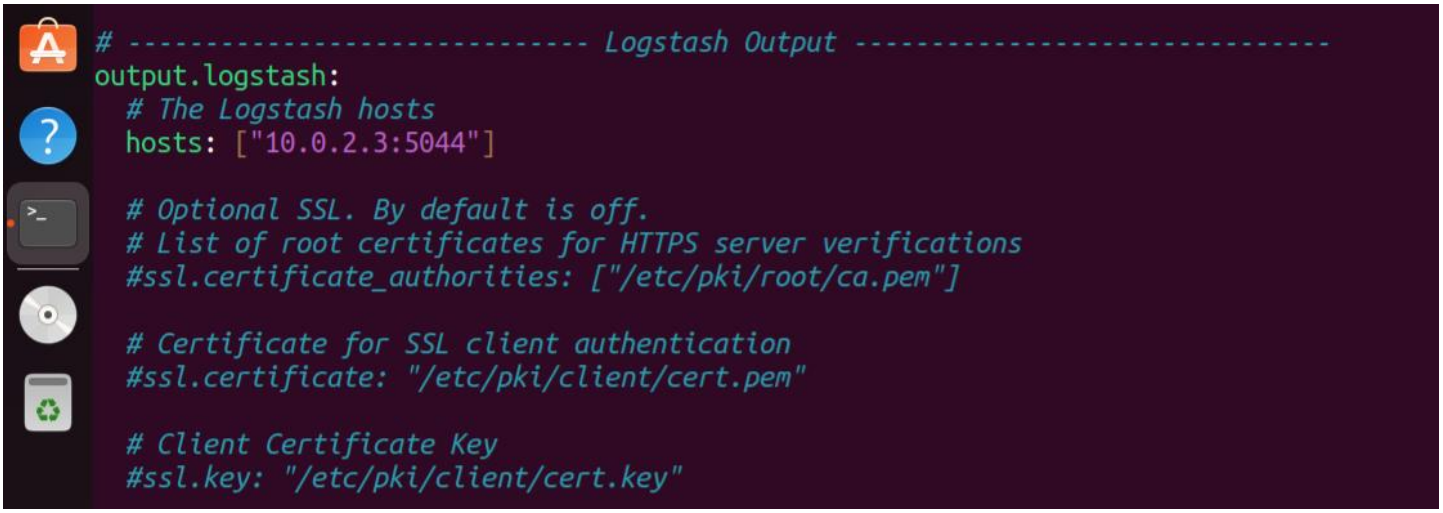
sudo nano /etc/filebeat/filebeat.yml

Configure file>

output.logstash:

 # The Logstash hosts

hosts: ["10.0.2.3:5044"]

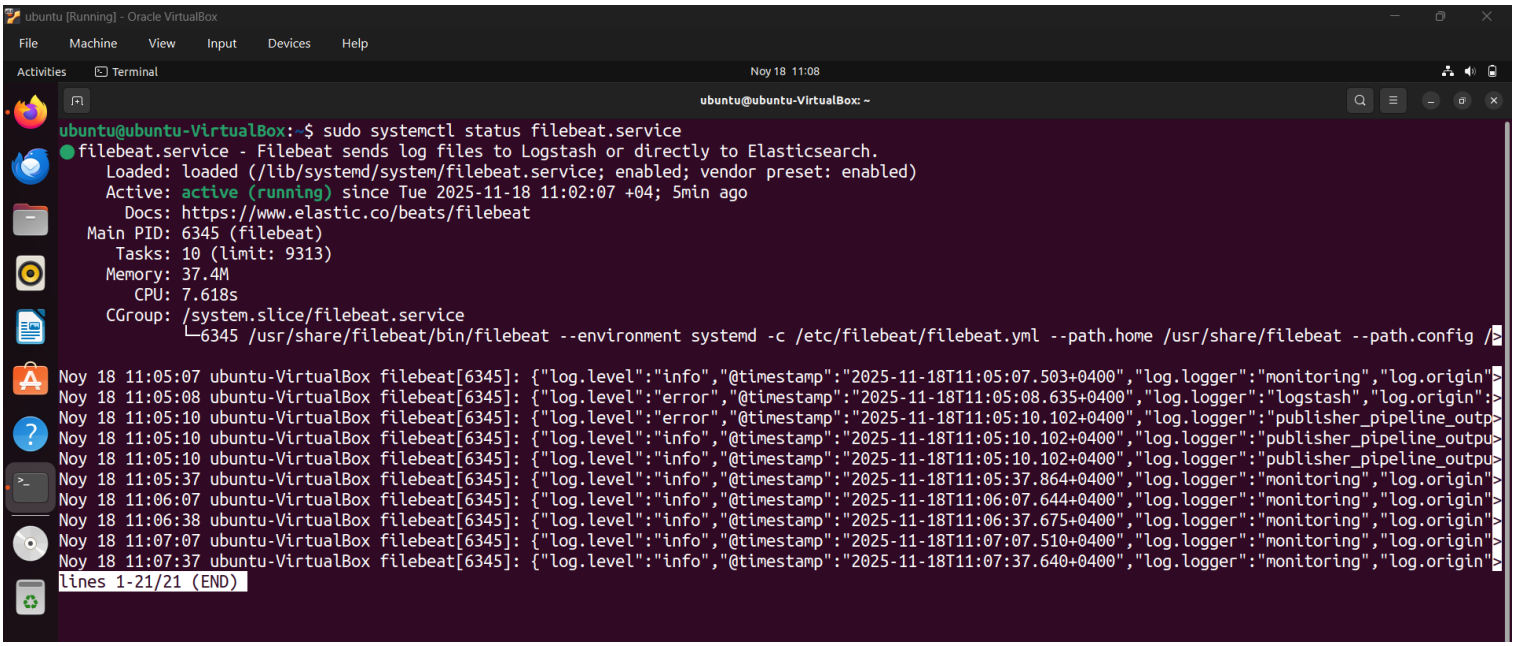


3) Enable and start filebeat

sudo systemctl enable filebeat && sudo systemctl start filebeat

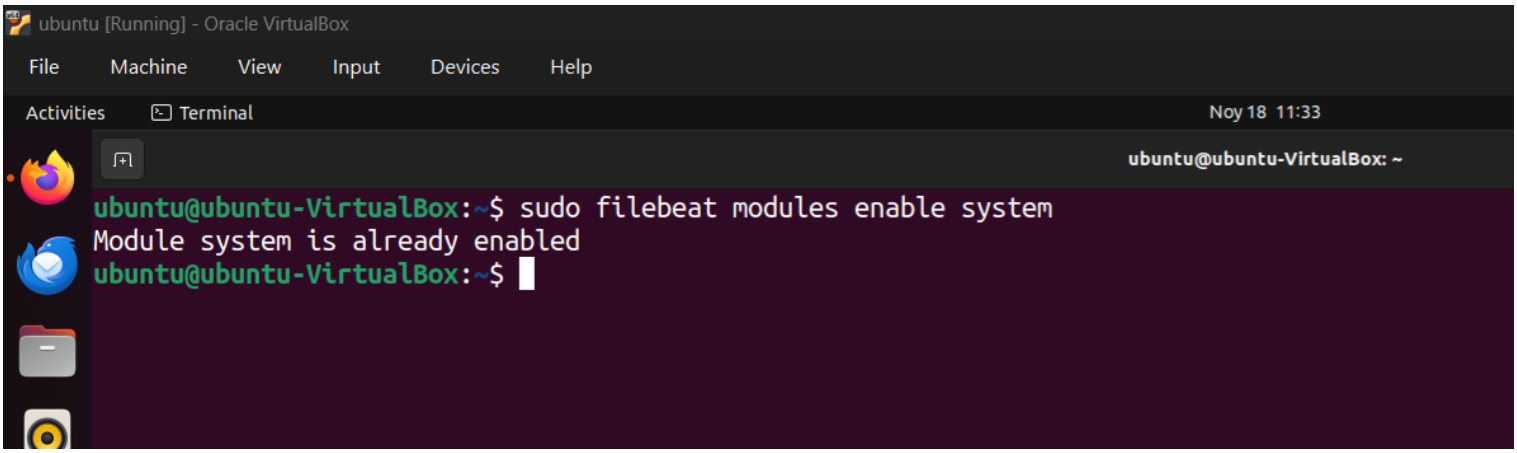
4) Check the status

sudo systemctl status filebeat



5) We're only interested in system module for collecting audit logs

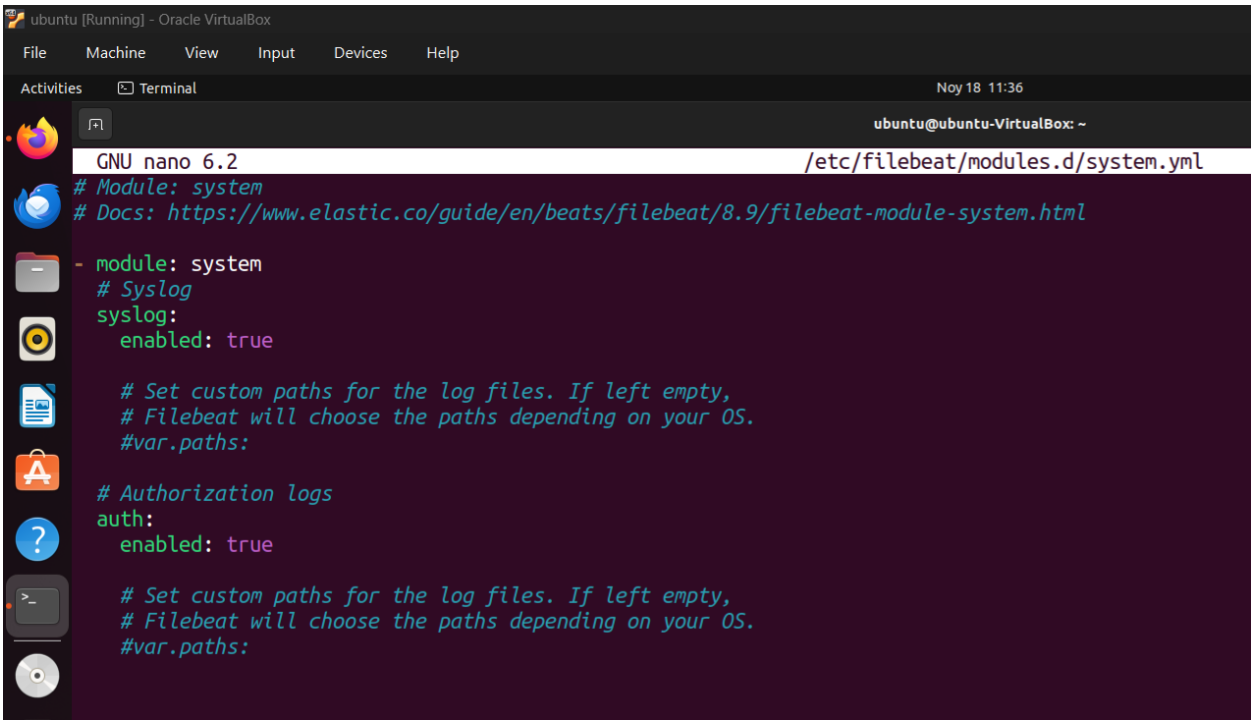
sudo filebeat modules enable system



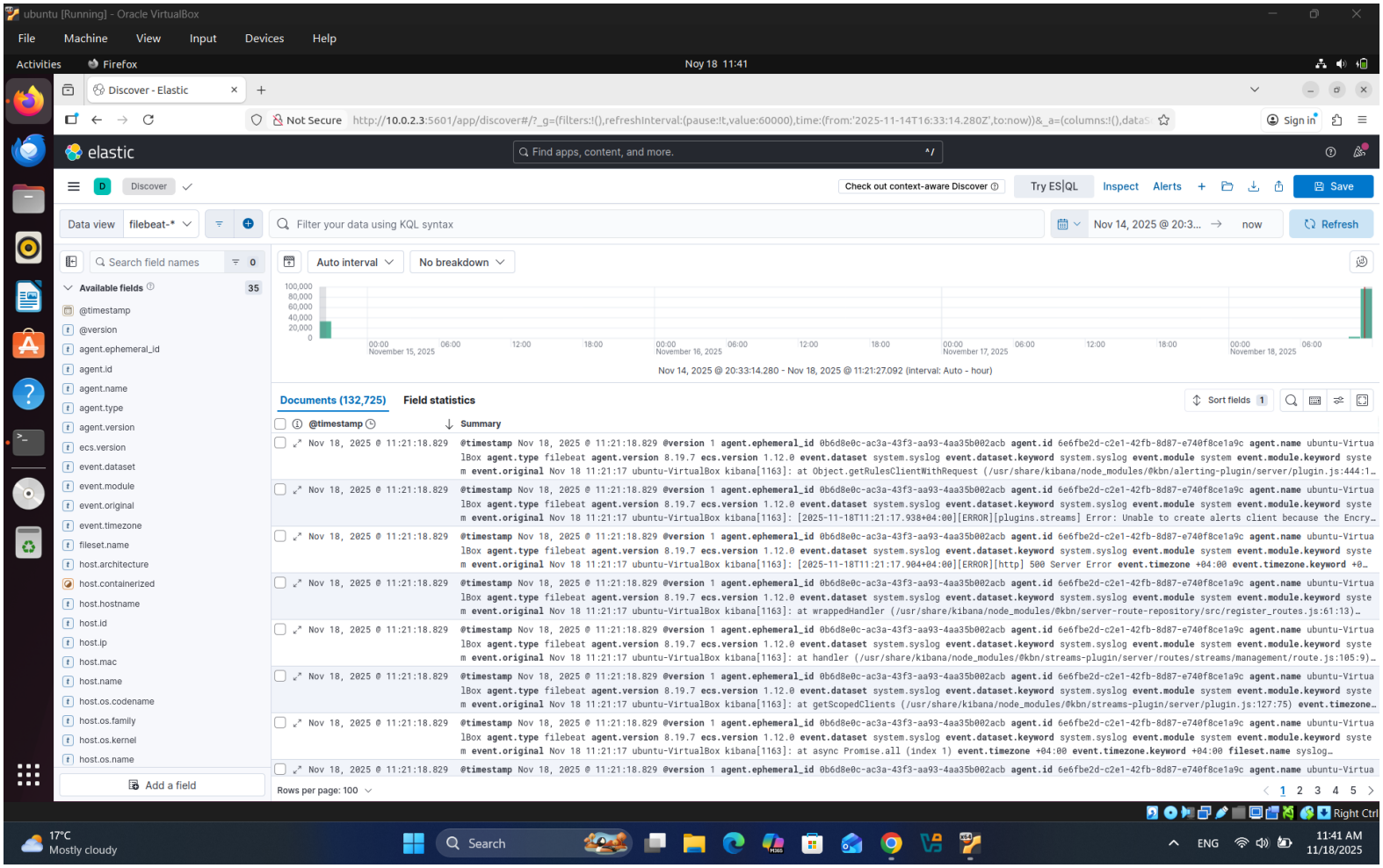
6) Edit the system module configuration file

sudo nano /etc/filebeat/modules.d/system.yml

7) Configure file



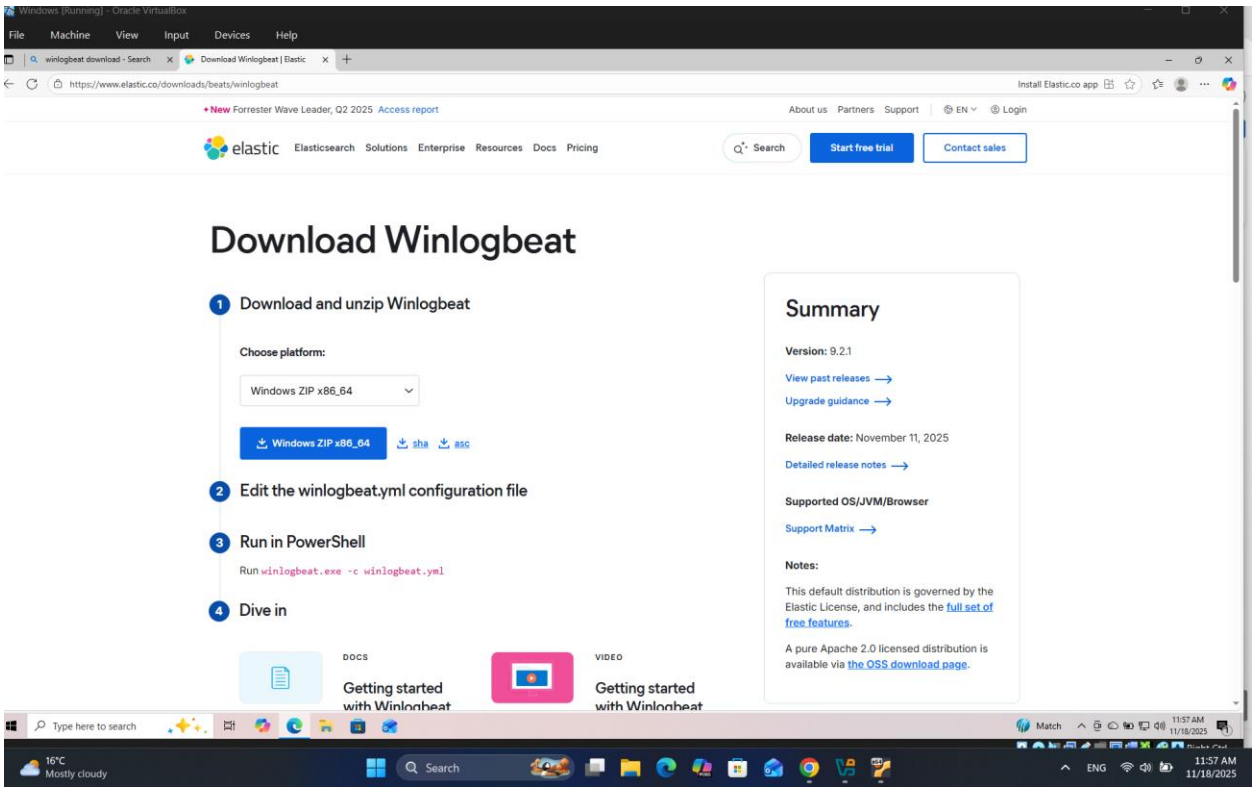
6) Kibana vizualization result for filebeat



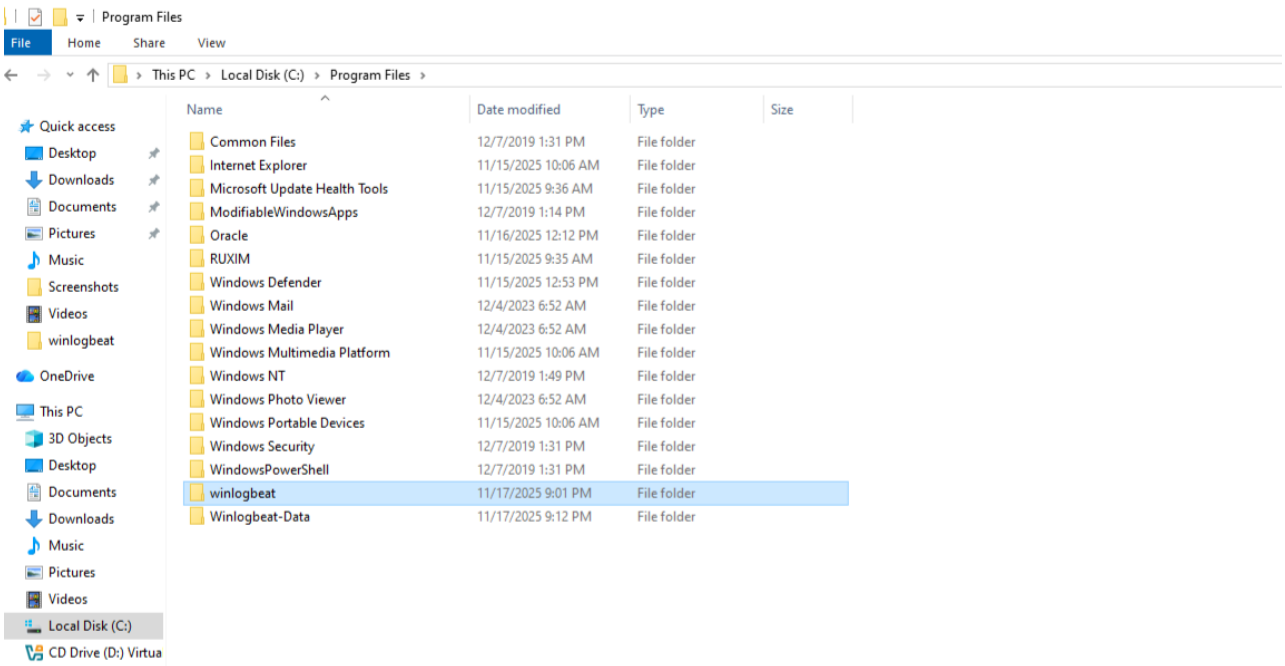
7) Install winlogbeat and configure file

1) Install winlogbeat

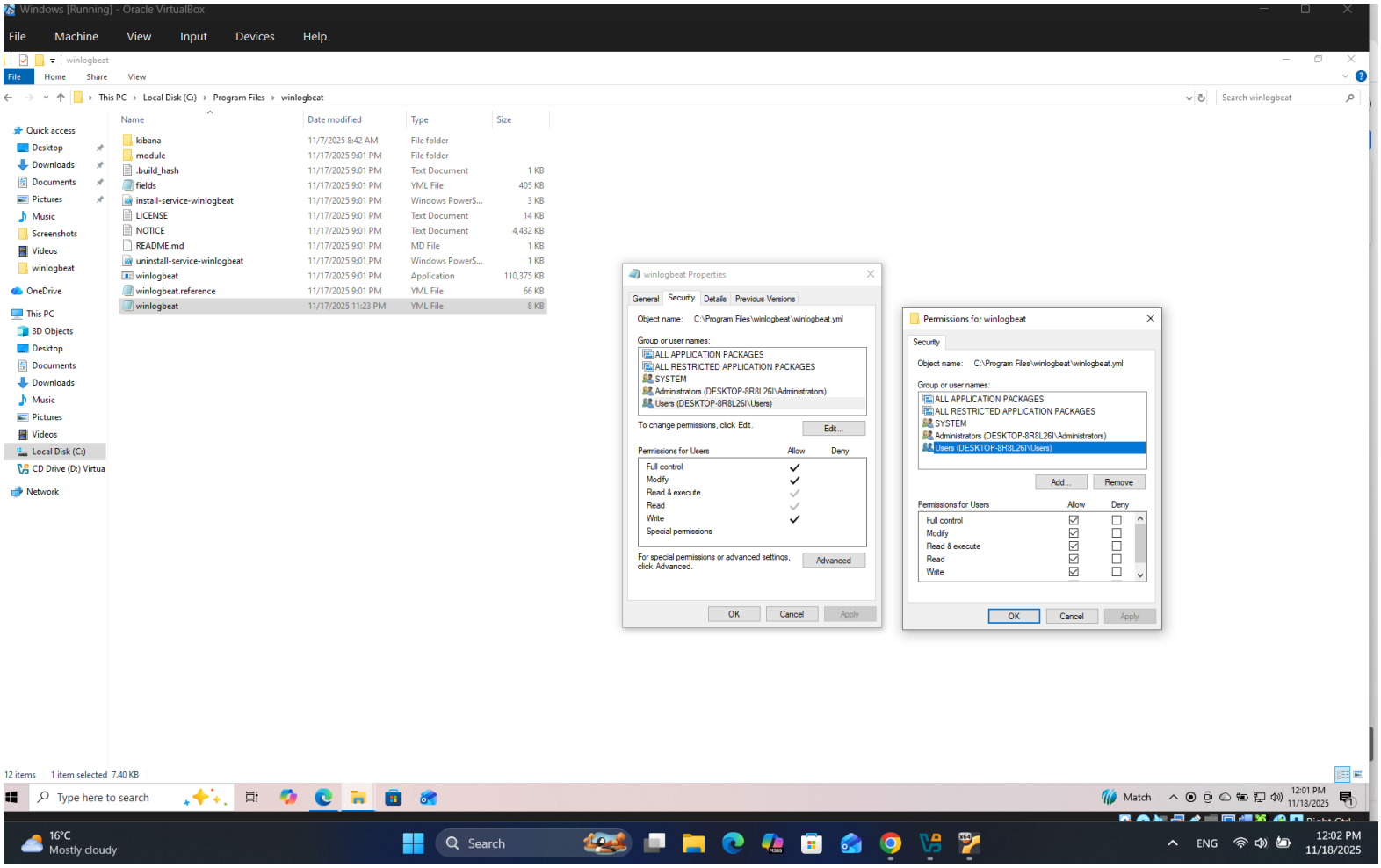
https://www.elastic.co/downloads/beats/winlogbeat



2) Extract all files to C:/Program files



3)Change permission of winlogbeat configuration file



4) Configure file

setup.dashboards.enabled: true

```
# ================================== Dashboards =====================================
# These settings control loading the sample dashboards to the Kibana index. Loading
# the dashboards is disabled by default and can be enabled either by setting the
# options here or by using the `setup` command.
setup.dashboards.enabled: true

# The URL from where to download the dashboard archive. By default, this URL
# has a value that is computed based on the Beat name and version. For released
# versions, this URL points to the dashboard archive on the artifacts.elastic.co
# website.
#setup.dashboards.url:
```

setup.kibana

host:"10.0.2.3:5601"

```
# ================================== Kibana ===================================

# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:

  # Kibana Host
  # Scheme and port can be left out and will be set to the default (http and 5601)
  # In case you specify and additional path, the scheme is required: http://localhost:5601/path
  # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
  host: "10.0.2.3:5601"

  # Kibana Space ID
  # ID of the Kibana Space into which the dashboards should be loaded. By default,
  # the Default Space will be used.
  #space.id:
```

output.logstash:

hosts: ["10.0.2.3:5044]

```
# ------------------------------ Logstash Output -------------------------------
output.logstash:
  # The Logstash hosts
  hosts: ["10.0.2.3:5044"]

  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]

  # Certificate for SSL client authentication
  #ssl.certificate: "/etc/pki/client/cert.pem"

  # Client Certificate Key
  #ssl.key: "/etc/pki/client/cert.key"
```

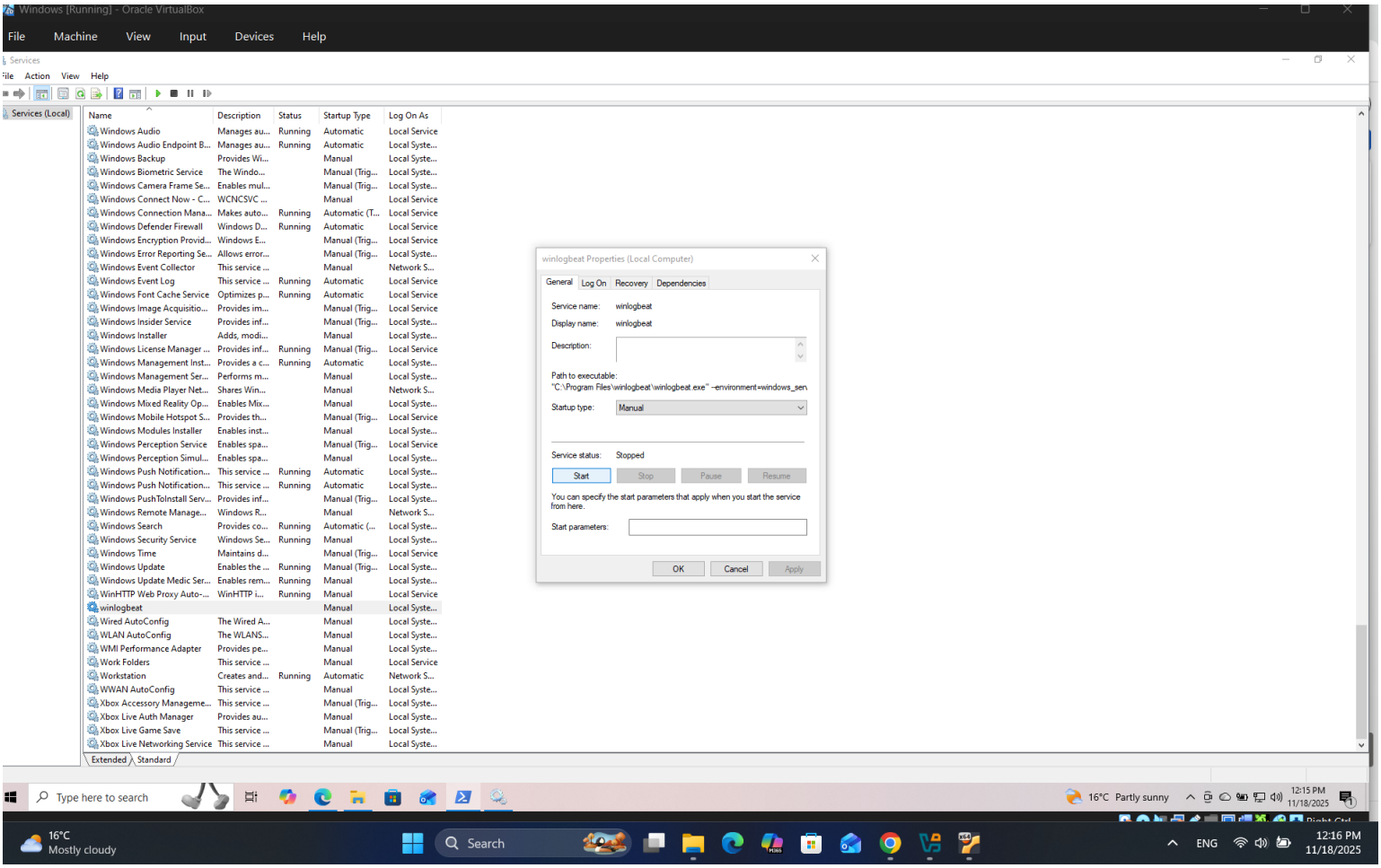
5) Powershell install winlogbeat service

- Powershell run as Administrator
- cd 'C:\Program Files\winlogbeat'
- .\install-service-winlogbeat.ps1

If an error occurs

- Set-ExecutionPolicy -ExecutionPolicy Bypass -Scope Process

6) Start Service



8) Kibana vizualization result for winlogbeat