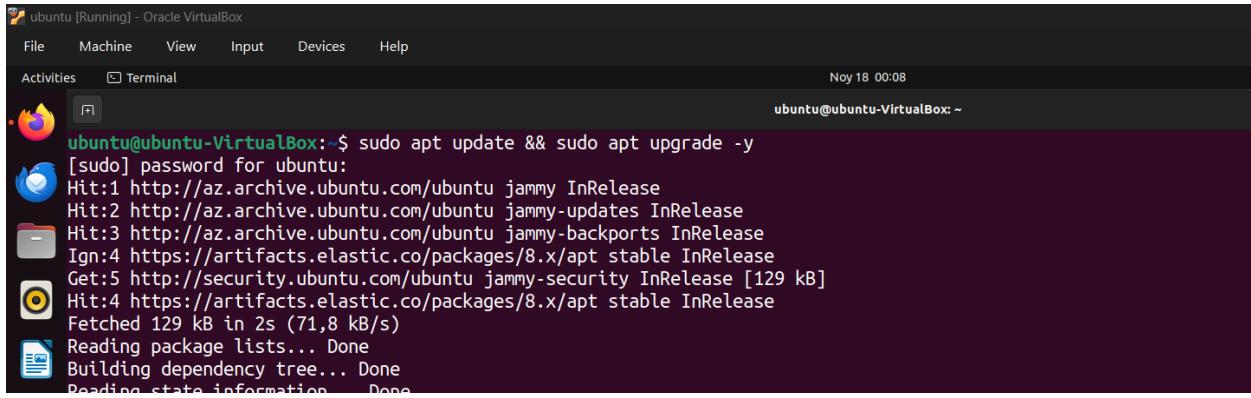


## ELK Deploy step by step

### 1) Update and Upgrade system

1) Let's update and upgrade our system

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



```
ubuntu@ubuntu-VirtualBox:~$ sudo apt update && sudo apt full-upgrade -y
[sudo] password for ubuntu:
Hit:1 http://az.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://az.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://az.archive.ubuntu.com/ubuntu jammy-backports InRelease
Ign:4 https://artifacts.elastic.co/packages/8.x/apt stable InRelease
Get:5 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Hit:6 https://artifacts.elastic.co/packages/8.x/apt stable InRelease
Fetched 129 kB in 2s (71,8 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

### 2) Installing 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/elasticsearch-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

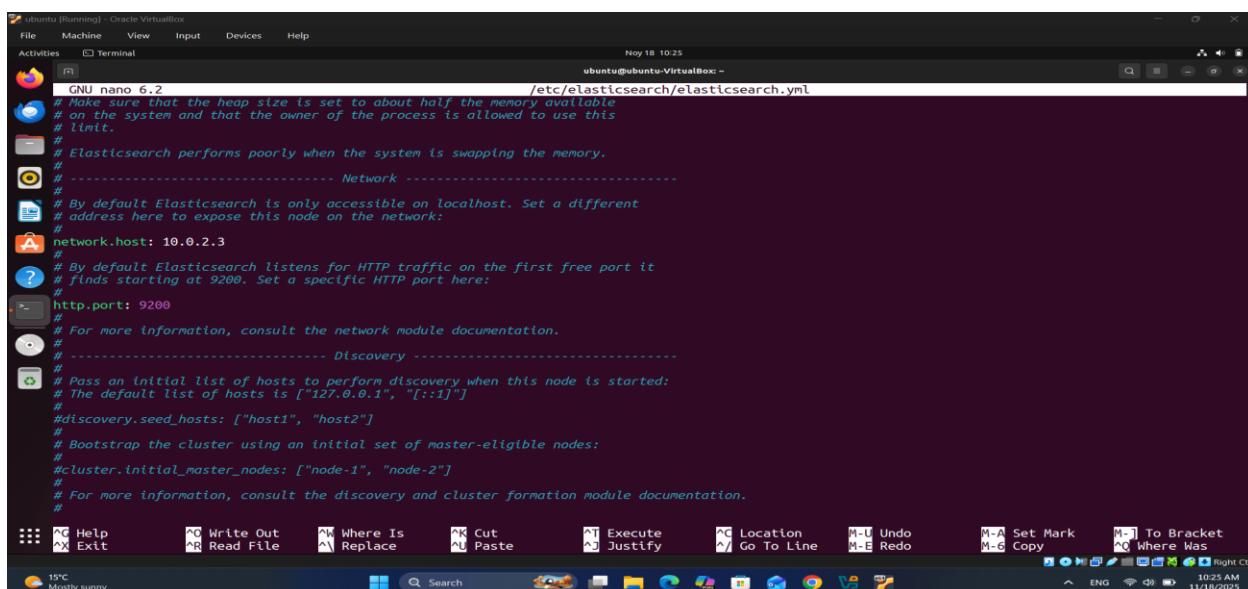
```
sudo nano /etc/elasticsearch/elasticsearch.yml
```

Configure these>

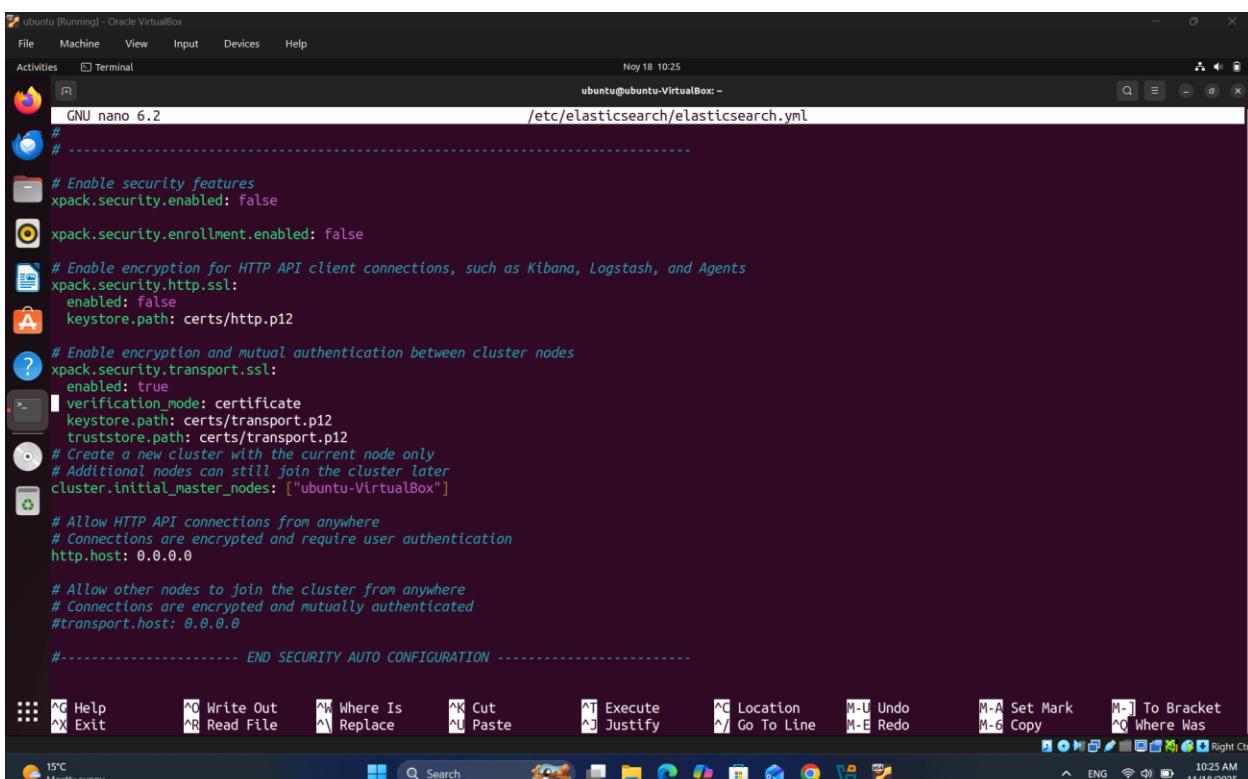
*network.host: 10.0.2.3*

*http.port: 9200*

*xpack.security.enabled: false*



```
ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Nov 18 10:25
ubuntug@ubuntu-VirtualBox: ~
GNU nano 6.2 /etc/elasticsearch/elasticsearch.yml
# Make sure that the heap size is set to about half the memory available
# on the system and that the owner of the process is allowed to use this
# limit.
#
# Elasticsearch performs poorly when the system is swapping the memory.
# -----
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
network.host: 10.0.2.3
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
http.port: 9200
#
# For more information, consult the network module documentation.
# -----
# Discovery -----
#
# Pass an initial list of hosts to perform discovery when this node is started:
# The default list of hosts is ["127.0.0.1", "[::1]"]
#
#discovery.seed_hosts: ["host1", "host2"]
#
# Bootstrap the cluster using an initial set of master-eligible nodes:
#
#cluster.initial_master_nodes: ["node-1", "node-2"]
#
# For more information, consult the discovery and cluster formation module documentation.
#
^G Help ^X Exit ^W Write Out ^R Read File ^W Where Is ^K Cut ^U Paste ^T Execute ^C Location ^G Go To Line M-U Undo M-E Redo M-A Set Mark M-G Copy M-J To Bracket M-Q Where Was
15°C Mostly sunny
ENG 10:25 AM 11/18/2025
```



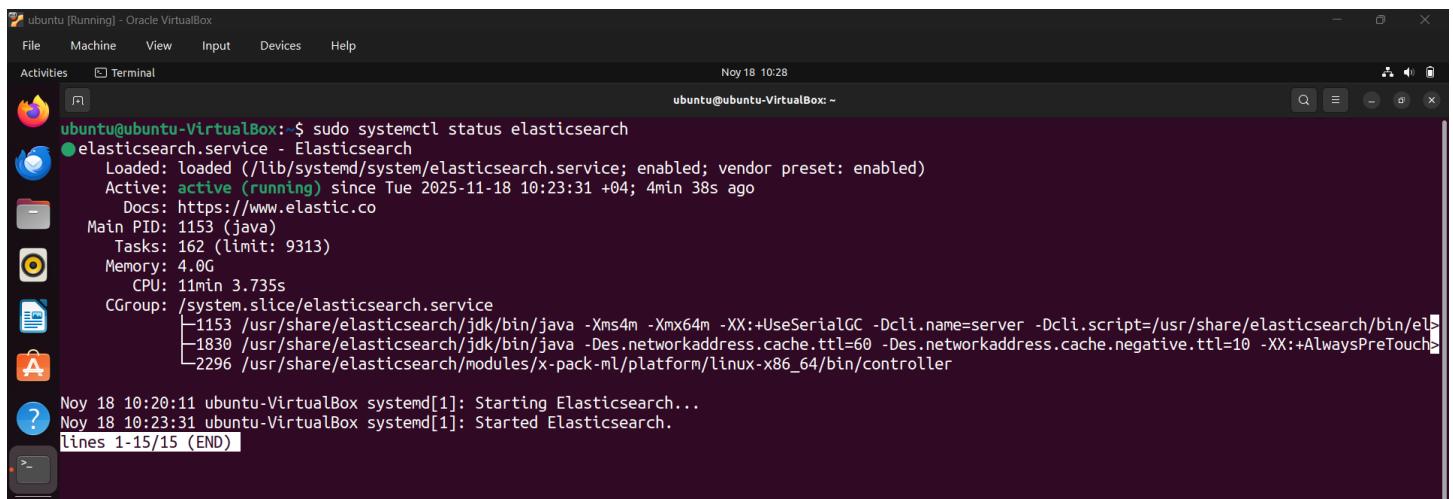
```
ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Nov 18 10:25
ubuntug@ubuntu-VirtualBox: ~
GNU nano 6.2 /etc/elasticsearch/elasticsearch.yml
#
#
# Enable security features
xpack.security.enabled: false
#
# Enable encryption for HTTP API client connections, such as Kibana, Logstash, and Agents
xpack.security.http.ssl:
  enabled: false
  keystore.path: certs/http.p12
#
# Enable encryption and mutual authentication between cluster nodes
xpack.security.transport.ssl:
  enabled: true
  verification_mode: certificate
  keystore.path: certs/transport.p12
  truststore.path: certs/transport.p12
#
# Create a new cluster with the current node only
# Additional nodes can still join the cluster later
cluster.initial_master_nodes: ["ubuntu-VirtualBox"]
#
# Allow HTTP API connections from anywhere
# Connections are encrypted and require user authentication
http.host: 0.0.0.0
#
# Allow other nodes to join the cluster from anywhere
# Connections are encrypted and mutually authenticated
#transport.host: 0.0.0.0
#
#----- END SECURITY AUTO CONFIGURATION -----
```

6) Enable and start the service.

```
sudo systemctl enable elasticsearch && sudo systemctl start elasticsearch
```

7) Check the status

```
sudo systemctl status elasticsearch
```

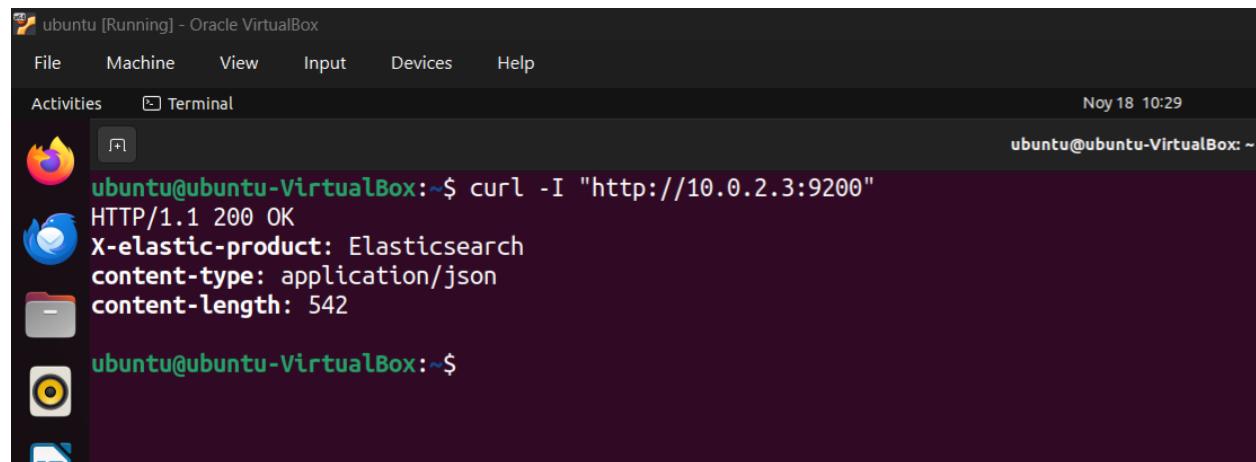


```
ubuntu@ubuntu-VirtualBox:~$ sudo systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2025-11-18 10:23:31 +04; 4min 38s ago
     Docs: https://www.elastic.co
 Main PID: 1153 (java)
   Tasks: 162 (limit: 9313)
   Memory: 4.0G
      CPU: 11min 3.735s
      CGroup: /system.slice/elasticsearch.service
              ├─1153 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+UseSerialGC -Dcli.name=server -Dcli.script=/usr/share/elasticsearch/bin/elasticsearch
              ├─1830 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.negative.ttl=10 -XX:+AlwaysPreTouch
              └─2296 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller

Nov 18 10:20:11 ubuntu-VirtualBox systemd[1]: Starting Elasticsearch...
Nov 18 10:23:31 ubuntu-VirtualBox systemd[1]: Started Elasticsearch.
lines 1-15/15 (END)
```

8) Verify the server is responding to queries

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



```
ubuntu@ubuntu-VirtualBox:~$ curl -I "http://10.0.2.3:9200"
HTTP/1.1 200 OK
X-elastic-product: Elasticsearch
content-type: application/json
content-length: 542

ubuntu@ubuntu-VirtualBox:~$
```

### 3) Install Logstash and configure file

1) Install 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>*

```
input {
```

```
  beats {
```

```
    port => 5044
```

```
}
```

```
}
```

```
output {
```

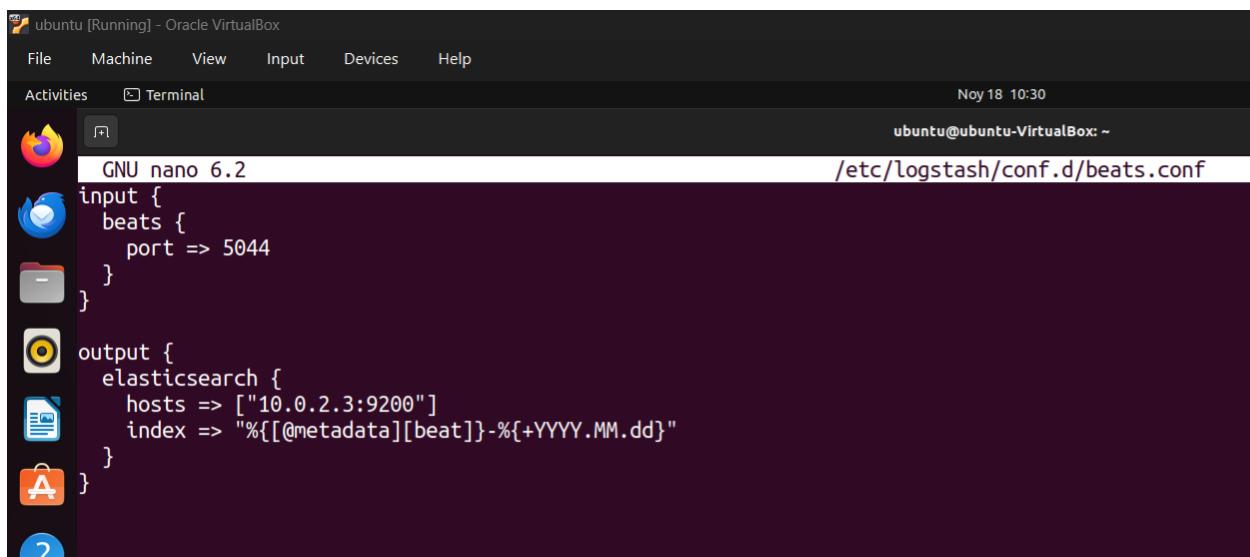
```
  elasticsearch {
```

```
    hosts => ["10.0.2.3:9200"]
```

```
    index => "%{@metadata}[beat]-%{+YYYY.MM.dd}"
```

```
}
```

```
}
```



The screenshot shows a terminal window titled 'ubuntu [Running] - Oracle VirtualBox'. The window displays the contents of the file '/etc/logstash/conf.d/beats.conf' using the 'nano' editor. The configuration file contains the following code:

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

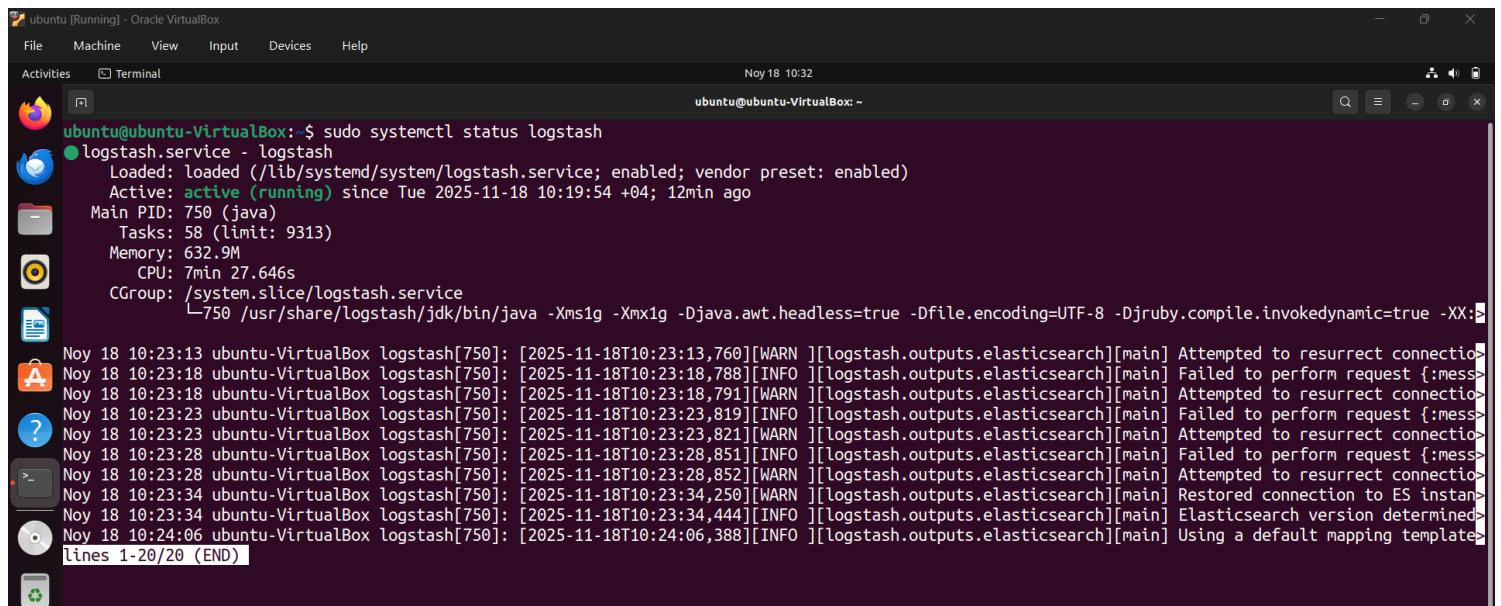
output {
  elasticsearch {
    hosts => ["10.0.2.3:9200"]
    index => "%{@metadata}[beat]-%{+YYYY.MM.dd}"
  }
}
```

### 3) Enable and start Logstash.

```
sudo systemctl enable logstash && sudo systemctl start logstash
```

### 4) Logstash's status

```
sudo systemctl status logstash
```



The screenshot shows a terminal window titled "ubuntu [Running] - Oracle VirtualBox" running on an Ubuntu desktop. The terminal output is as follows:

```
ubuntu@ubuntu-VirtualBox:~$ sudo systemctl status logstash
● logstash.service - logstash
   Loaded: loaded (/lib/systemd/system/logstash.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2025-11-18 10:19:54 +04; 12min ago
     Main PID: 750 (java)
        Tasks: 58 (limit: 9313)
       Memory: 632.9M
          CPU: 7min 27.646s
        CGroup: /system.slice/logstash.service
               └─ 750 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -Djava.awt.headless=true -Dfile.encoding=UTF-8 -Djruby.compile.invokedynamic=true -XX:+
Noy 18 10:23:13 ubuntu-VirtualBox logstash[750]: [2025-11-18T10:23:13,760][WARN ][logstash.outputs.elasticsearch][main] Attempted to resurrect connection<
Noy 18 10:23:18 ubuntu-VirtualBox logstash[750]: [2025-11-18T10:23:18,788][INFO ][logstash.outputs.elasticsearch][main] Failed to perform request {:mess<
Noy 18 10:23:18 ubuntu-VirtualBox logstash[750]: [2025-11-18T10:23:18,791][WARN ][logstash.outputs.elasticsearch][main] Attempted to resurrect connection<
Noy 18 10:23:23 ubuntu-VirtualBox logstash[750]: [2025-11-18T10:23:23,819][INFO ][logstash.outputs.elasticsearch][main] Failed to perform request {:mess<
Noy 18 10:23:23 ubuntu-VirtualBox logstash[750]: [2025-11-18T10:23:23,821][WARN ][logstash.outputs.elasticsearch][main] Attempted to resurrect connection<
Noy 18 10:23:28 ubuntu-VirtualBox logstash[750]: [2025-11-18T10:23:28,851][INFO ][logstash.outputs.elasticsearch][main] Failed to perform request {:mess<
Noy 18 10:23:28 ubuntu-VirtualBox logstash[750]: [2025-11-18T10:23:28,852][WARN ][logstash.outputs.elasticsearch][main] Attempted to resurrect connection<
Noy 18 10:23:34 ubuntu-VirtualBox logstash[750]: [2025-11-18T10:23:34,250][WARN ][logstash.outputs.elasticsearch][main] Restored connection to ES instan<
Noy 18 10:23:34 ubuntu-VirtualBox logstash[750]: [2025-11-18T10:23:34,444][INFO ][logstash.outputs.elasticsearch][main] Elasticsearch version determined<
Noy 18 10:24:06 ubuntu-VirtualBox logstash[750]: [2025-11-18T10:24:06,388][INFO ][logstash.outputs.elasticsearch][main] Using a default mapping template<
lines 1-20/20 (END)
```

## 4) Install Kibana and configure file

### 1) Install Kibana

```
sudo apt install kibana
```

### 2) Kibana file configuration

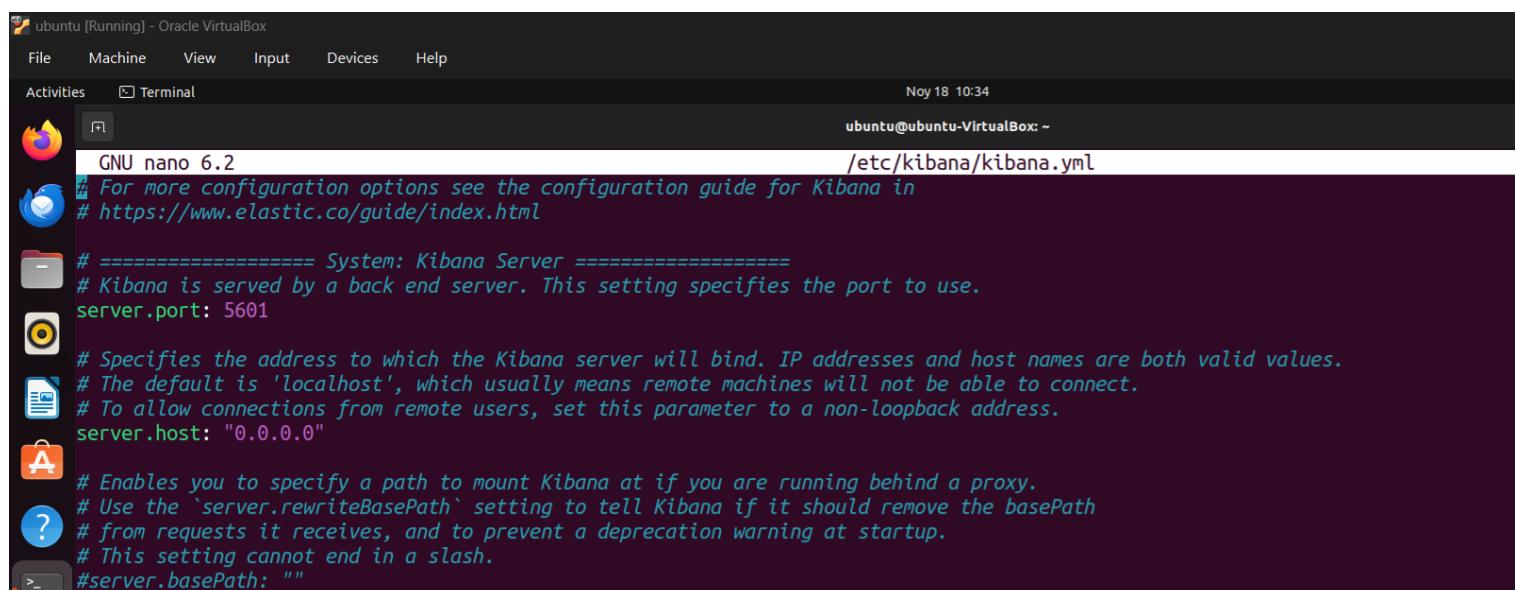
```
sudo nano /etc/kibana/kibana.yml
```

Configure file>

```
server.port: 5601
```

```
server.host: "0.0.0.0"
```

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

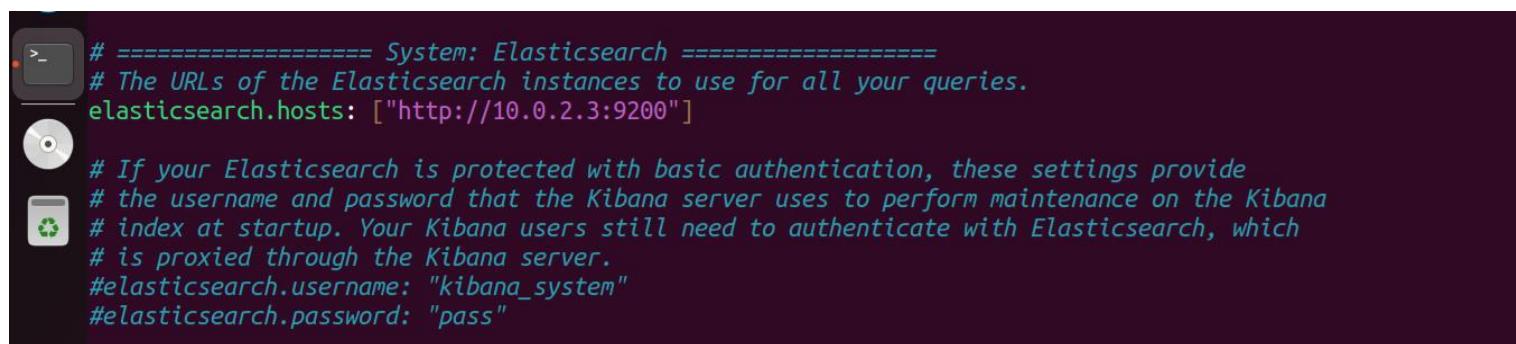


```
ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Noy 18 10:34
ubuntu@ubuntu-VirtualBox: ~
GNU nano 6.2 /etc/kibana/kibana.yml
# For more configuration options see the configuration guide for Kibana in
# https://www.elastic.co/guide/index.html

# ===== System: Kibana Server =====
# Kibana is served by a back end server. This setting specifies the port to use.
server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid values.
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: "0.0.0.0"

# Enables you to specify a path to mount Kibana at if you are running behind a proxy.
# Use the `server.rewriteBasePath` setting to tell Kibana if it should remove the basePath
# from requests it receives, and to prevent a deprecation warning at startup.
# This setting cannot end in a slash.
#server.basePath: ""
```



```
# ===== System: Elasticsearch =====
# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: ["http://10.0.2.3:9200"]

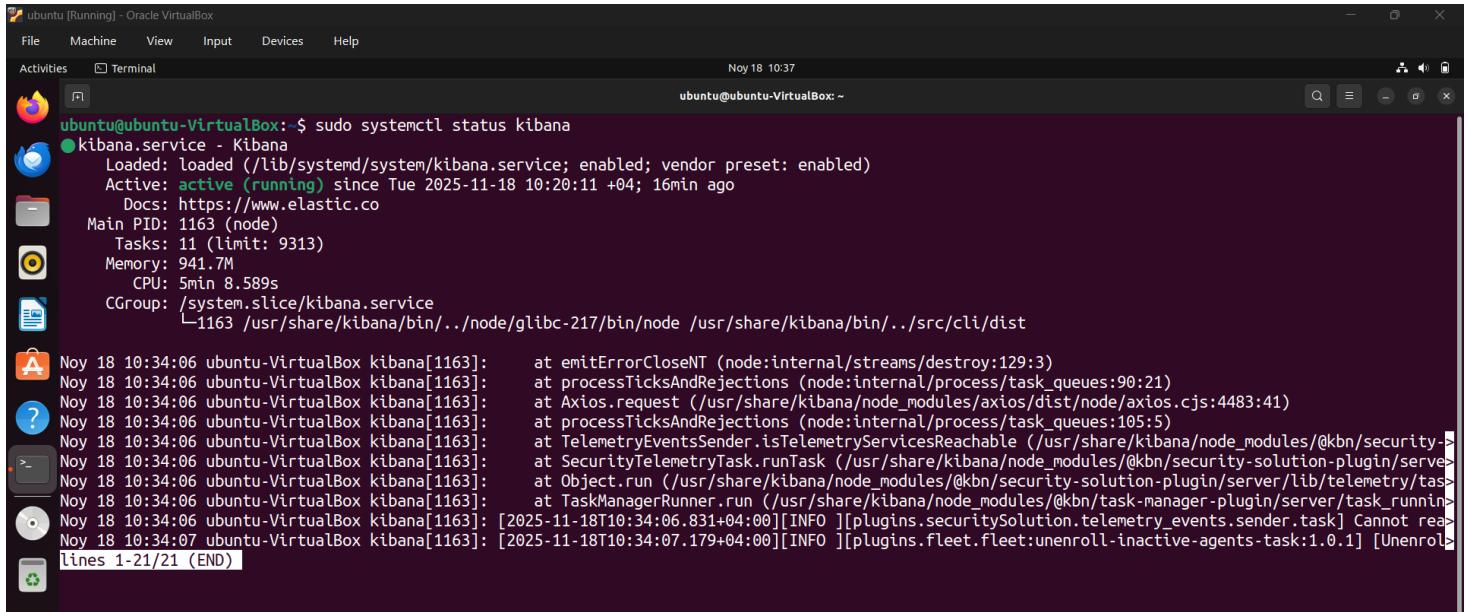
# If your Elasticsearch is protected with basic authentication, these settings provide
# the username and password that the Kibana server uses to perform maintenance on the Kibana
# index at startup. Your Kibana users still need to authenticate with Elasticsearch, which
# is proxied through the Kibana server.
#elasticsearch.username: "kibana_system"
#elasticsearch.password: "pass"
```

### 3) Enable and start Kibana

```
sudo systemctl enable kibana && sudo systemctl start kibana
```

### 4) Kibana's status

```
sudo systemctl status kibana
```

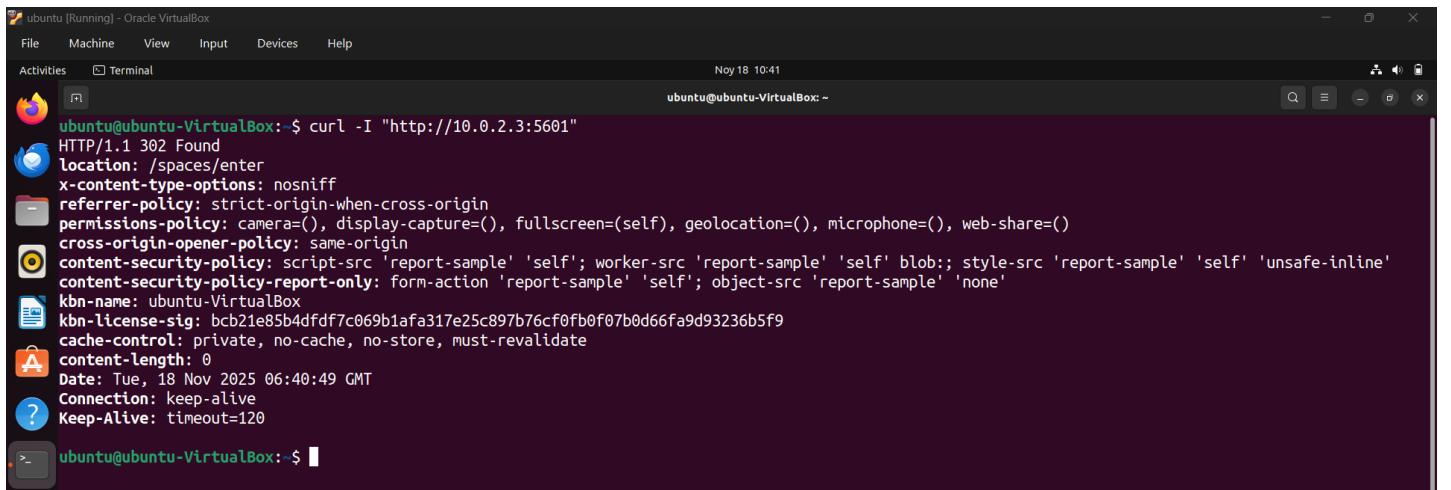


```
ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Nov 18 10:37
ubuntu@ubuntu-VirtualBox:~$ sudo systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/lib/systemd/system/kibana.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2025-11-18 10:20:11 +04; 16min ago
     Docs: https://www.elastic.co
     Main PID: 1163 (node)
        Tasks: 11 (limit: 9313)
       Memory: 941.7M
          CPU: 5min 8.589s
        CGroup: /system.slice/kibana.service
                └─1163 /usr/share/kibana/bin/../node/glibc-217/bin/node /usr/share/kibana/bin/../src/cli/dist

A Noy 18 10:34:06 ubuntu-VirtualBox kibana[1163]:      at emitErrorCloseNT (node:internalstreams/destroy:129:3)
Noy 18 10:34:06 ubuntu-VirtualBox kibana[1163]:      at processTicksAndRejections (node:internal/process/task_queues:90:21)
Noy 18 10:34:06 ubuntu-VirtualBox kibana[1163]:      at Axios.request (/usr/share/kibana/node_modules/axios/dist/node/axios.cjs:4483:41)
Noy 18 10:34:06 ubuntu-VirtualBox kibana[1163]:      at processTicksAndRejections (node:internal/process/task_queues:105:5)
Noy 18 10:34:06 ubuntu-VirtualBox kibana[1163]:      at TelemetryEventsSender.isTelemetryServicesReachable (/usr/share/kibana/node_modules/@kbn/security-solution-plugin/src/services/telemetry/events/send
Noy 18 10:34:06 ubuntu-VirtualBox kibana[1163]:      at SecurityTelemetryTask.runTask (/usr/share/kibana/node_modules/@kbn/security-solution-plugin/server/lib/telemetry/tasks/security-telemetry-task.js:11:13)
Noy 18 10:34:06 ubuntu-VirtualBox kibana[1163]:      at Object.run (/usr/share/kibana/node_modules/@kbn/security-solution-plugin/server/lib/telemetry/tasks/security-telemetry-task.js:11:13)
Noy 18 10:34:06 ubuntu-VirtualBox kibana[1163]:      at TaskManagerRunner.run (/usr/share/kibana/node_modules/@kbn/task-manager-plugin/server/task_manager_runner.js:10:13)
Noy 18 10:34:06 ubuntu-VirtualBox kibana[1163]:      at [2025-11-18T10:34:06.831+04:00][INFO ][plugins.securitysolution.telemetry_events.sender.task] Cannot read property 'run' of undefined
Noy 18 10:34:07 ubuntu-VirtualBox kibana[1163]:      at [2025-11-18T10:34:07.179+04:00][INFO ][plugins.fleet.fleet:unenroll-inactive-agents-task:1.0.1] [Unenroll inactive agents task] failed to run
lines 1-21/21 (END)
```

### 5) Verify the server is responding to queries

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



```
ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Nov 18 10:41
ubuntu@ubuntu-VirtualBox:~$ curl -I "http://10.0.2.3:5601"
HTTP/1.1 302 Found
location: /spaces/enter
x-content-type-options: nosniff
referrer-policy: strict-origin-when-cross-origin
permissions-policy: camera=(), display-capture=(), fullscreen=(self), geolocation=(), microphone=(), web-share=()
cross-origin-opener-policy: same-origin
content-security-policy: script-src 'report-sample' 'self'; worker-src 'report-sample' 'self' blob; style-src 'report-sample' 'self' 'unsafe-inline'
content-security-policy-report-only: form-action 'report-sample' 'self'; object-src 'report-sample' 'none'
kbn-name: ubuntu-VirtualBox
kbn-license-sig: bcb21e85b4dfdf7c069b1afa317e25c897b76cf0fb0f07b0d66fa9d93236b5f9
cache-control: private, no-cache, no-store, must-revalidate
content-length: 0
Date: Tue, 18 Nov 2025 06:40:49 GMT
Connection: keep-alive
Keep-Alive: timeout=120
ubuntu@ubuntu-VirtualBox:~$
```

## 5) Install 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

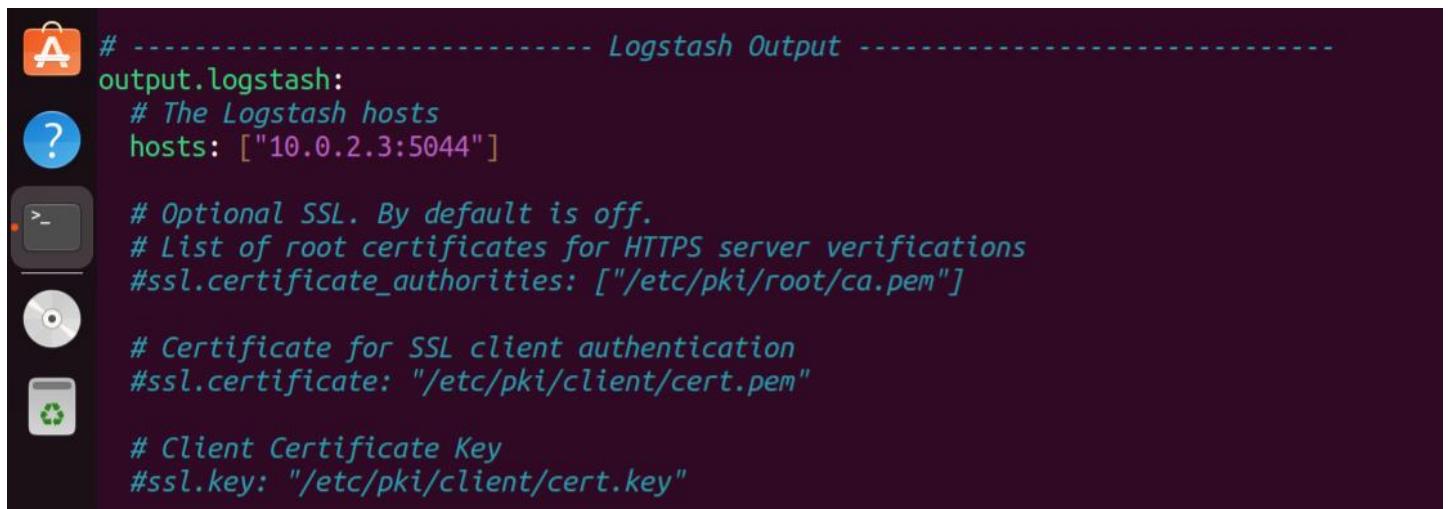
```
sudo nano /etc/filebeat/filebeat.yml
```

Configure file>

*output.logstash:*

*# The Logstash hosts*

*hosts: ["10.0.2.3:5044"]*



```
# ----- 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.certificateAuthorities: ["/etc/pki/root/ca.pem"]

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

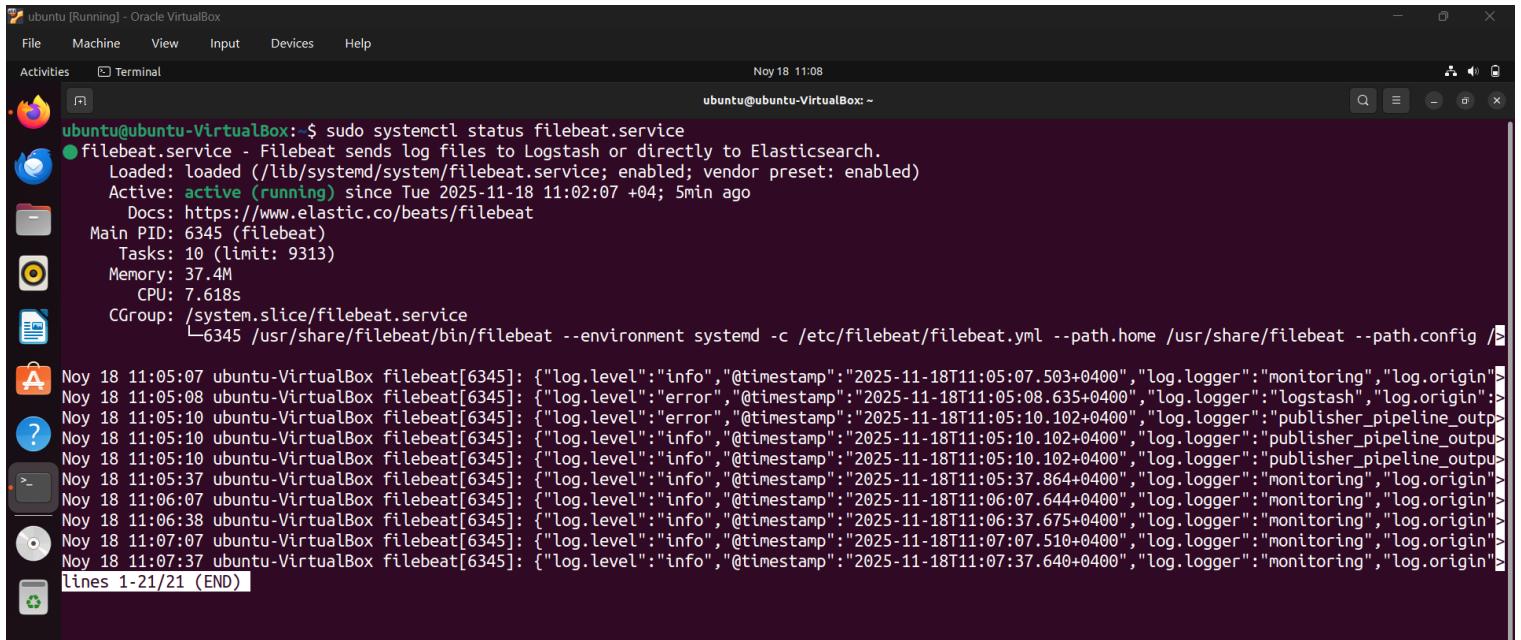
  # Client Certificate Key
  #ssl.key: "/etc/pki/client/cert.key"
```

### 3) Enable and start filebeat

```
sudo systemctl enable filebeat && sudo systemctl start filebeat
```

#### 4) Check the status

```
sudo systemctl status filebeat
```

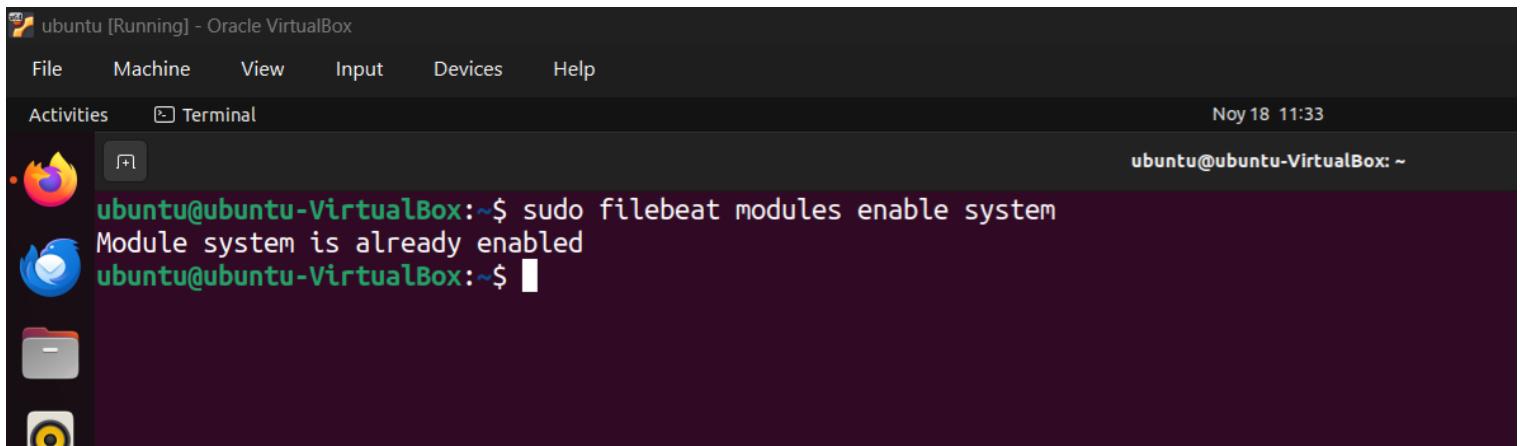


```
ubuntu@ubuntu-VirtualBox:~$ sudo systemctl status filebeat.service
● filebeat.service - Filebeat sends log files to Logstash or directly to Elasticsearch.
   Loaded: loaded (/lib/systemd/system/filebeat.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2025-11-18 11:02:07 +04; 5min ago
       Docs: https://www.elastic.co/beans/filebeat
   Main PID: 6345 (filebeat)
     Tasks: 10 (limit: 9313)
    Memory: 37.4M
      CPU: 7.618s
     CGroup: /system.slice/filebeat.service
             └─6345 /usr/share/filebeat/bin/filebeat --environment systemd -c /etc/filebeat/filebeat.yml --path.home /usr/share/filebeat --path.config /etc/filebeat/filebeat.yml --path.data /var/lib/filebeat --path.logs /var/log/filebeat

Noy 18 11:05:07 ubuntu-VirtualBox filebeat[6345]: {"log.level":"info", "@timestamp":"2025-11-18T11:05:07.503+0400", "log.logger":"monitoring", "log.origin":>
Noy 18 11:05:08 ubuntu-VirtualBox filebeat[6345]: {"log.level":"error", "@timestamp":"2025-11-18T11:05:08.635+0400", "log.logger":"logstash", "log.origin":>
Noy 18 11:05:10 ubuntu-VirtualBox filebeat[6345]: {"log.level":"error", "@timestamp":"2025-11-18T11:05:10.102+0400", "log.logger":"publisher_pipeline_outpu>
Noy 18 11:05:10 ubuntu-VirtualBox filebeat[6345]: {"log.level":"info", "@timestamp":"2025-11-18T11:05:10.102+0400", "log.logger":"publisher_pipeline_outpu>
Noy 18 11:05:37 ubuntu-VirtualBox filebeat[6345]: {"log.level":"info", "@timestamp":"2025-11-18T11:05:37.864+0400", "log.logger":"monitoring", "log.origin">
Noy 18 11:06:07 ubuntu-VirtualBox filebeat[6345]: {"log.level":"info", "@timestamp":"2025-11-18T11:06:07.644+0400", "log.logger":"monitoring", "log.origin">
Noy 18 11:06:38 ubuntu-VirtualBox filebeat[6345]: {"log.level":"info", "@timestamp":"2025-11-18T11:06:37.675+0400", "log.logger":"monitoring", "log.origin">
Noy 18 11:07:07 ubuntu-VirtualBox filebeat[6345]: {"log.level":"info", "@timestamp":"2025-11-18T11:07:07.510+0400", "log.logger":"monitoring", "log.origin">
Noy 18 11:07:37 ubuntu-VirtualBox filebeat[6345]: {"log.level":"info", "@timestamp":"2025-11-18T11:07:37.640+0400", "log.logger":"monitoring", "log.origin">
Lines 1-21/21 (END)
```

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

```
sudo filebeat modules enable system
```

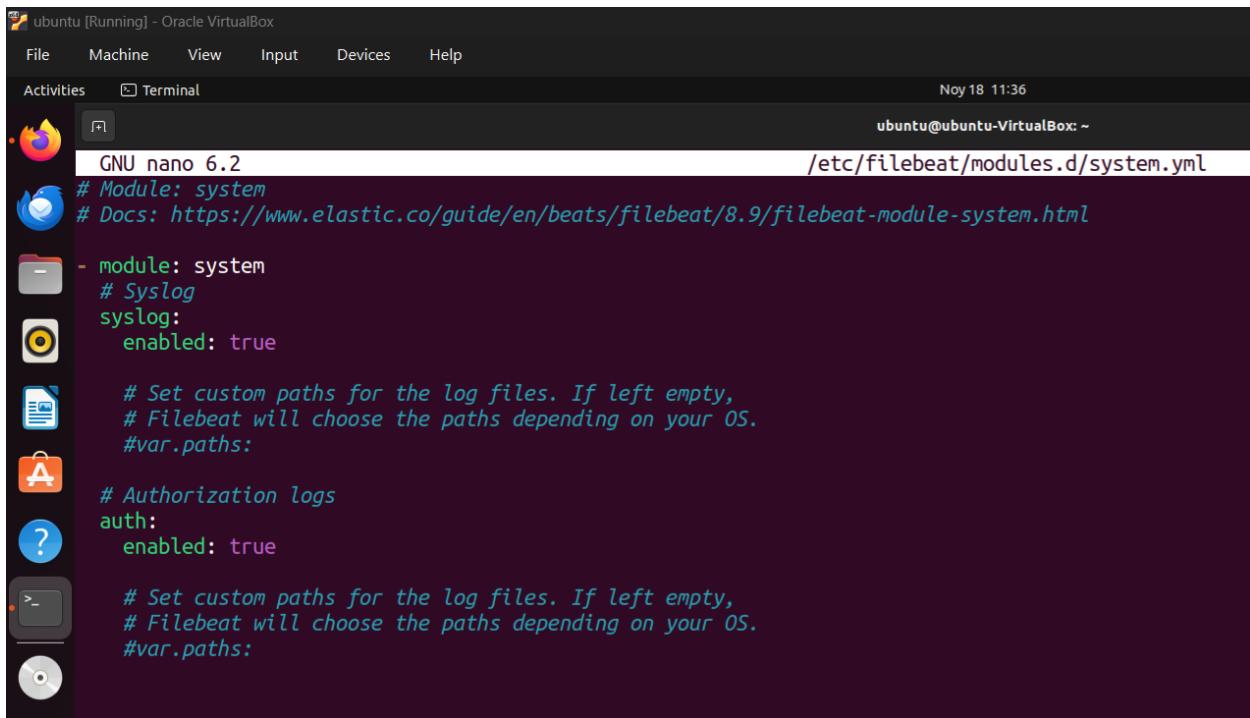


```
ubuntu@ubuntu-VirtualBox:~$ sudo filebeat modules enable system
Module system is already enabled
ubuntu@ubuntu-VirtualBox:~$
```

6) Edit the system module configuration file

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

7) Configure file



```
GNU nano 6.2
/etc/filebeat/modules.d/system.yml
# Module: system
# Docs: https://www.elastic.co/guide/en/beats/filebeat/8.9/filebeat-module-system.html

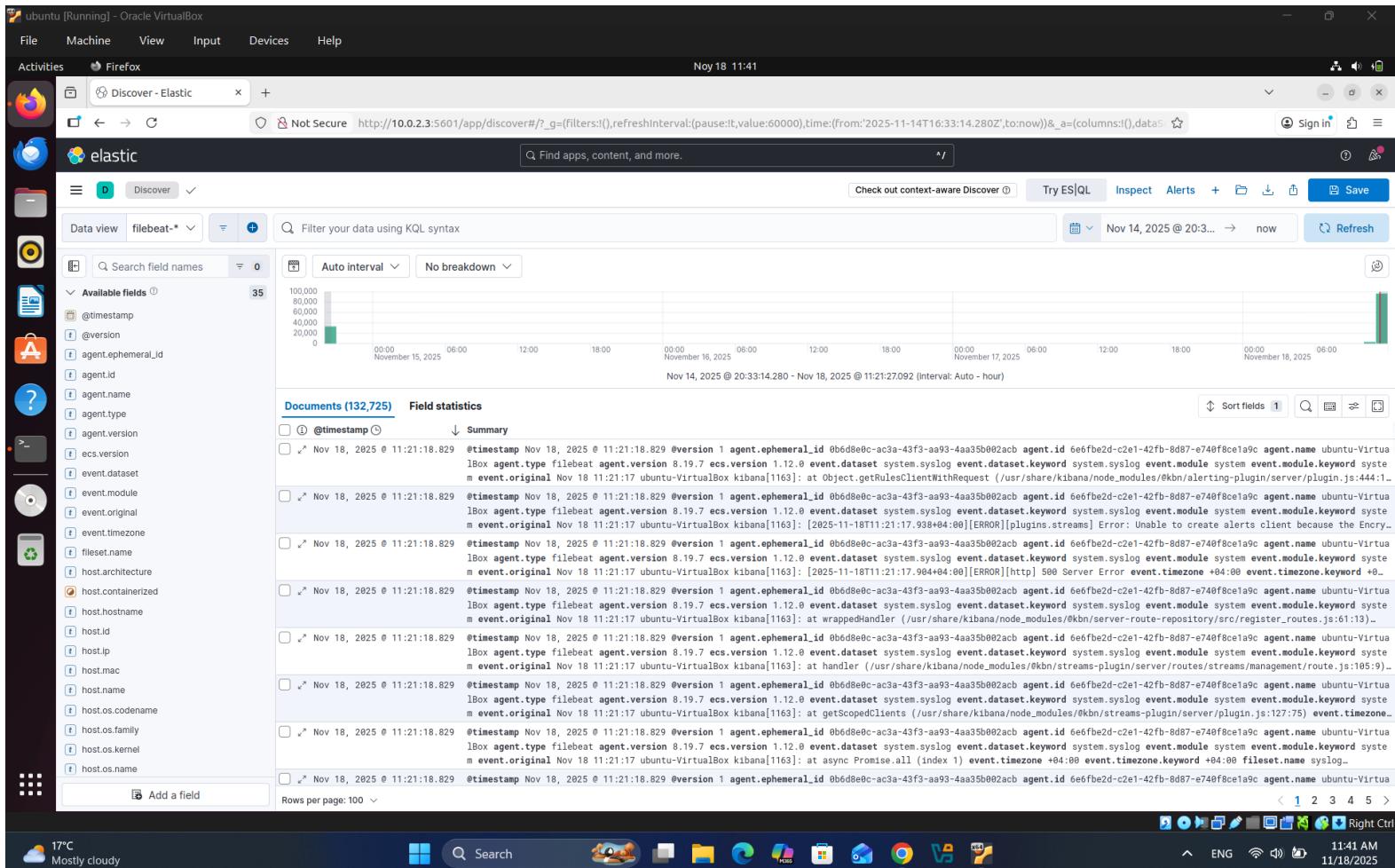
- module: system
  # Syslog
  syslog:
    enabled: true

  # Set custom paths for the log files. If left empty,
  # Filebeat will choose the paths depending on your OS.
  #var.paths:

  # Authorization logs
  auth:
    enabled: true

  # Set custom paths for the log files. If left empty,
  # Filebeat will choose the paths depending on your OS.
  #var.paths:
```

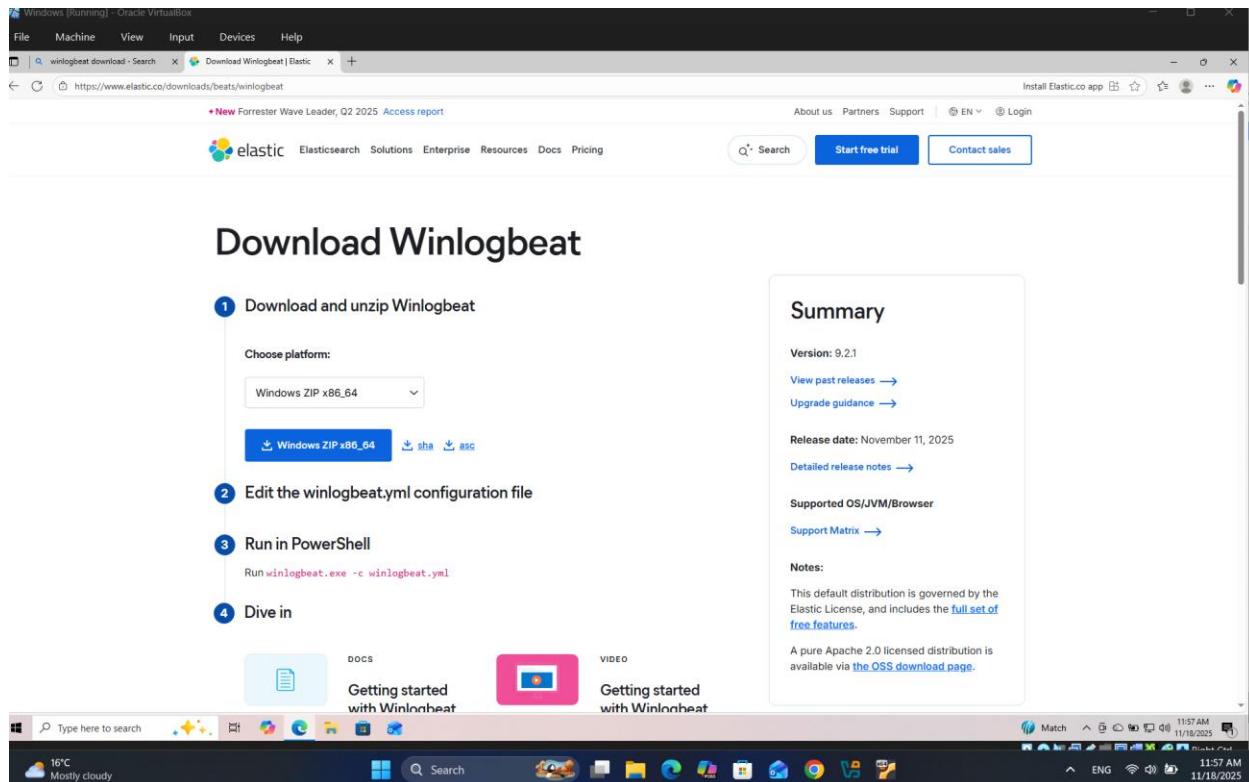
## 6) Kibana visualization result for filebeat



## 7) Install winlogbeat and configure file

### 1) Install winlogbeat

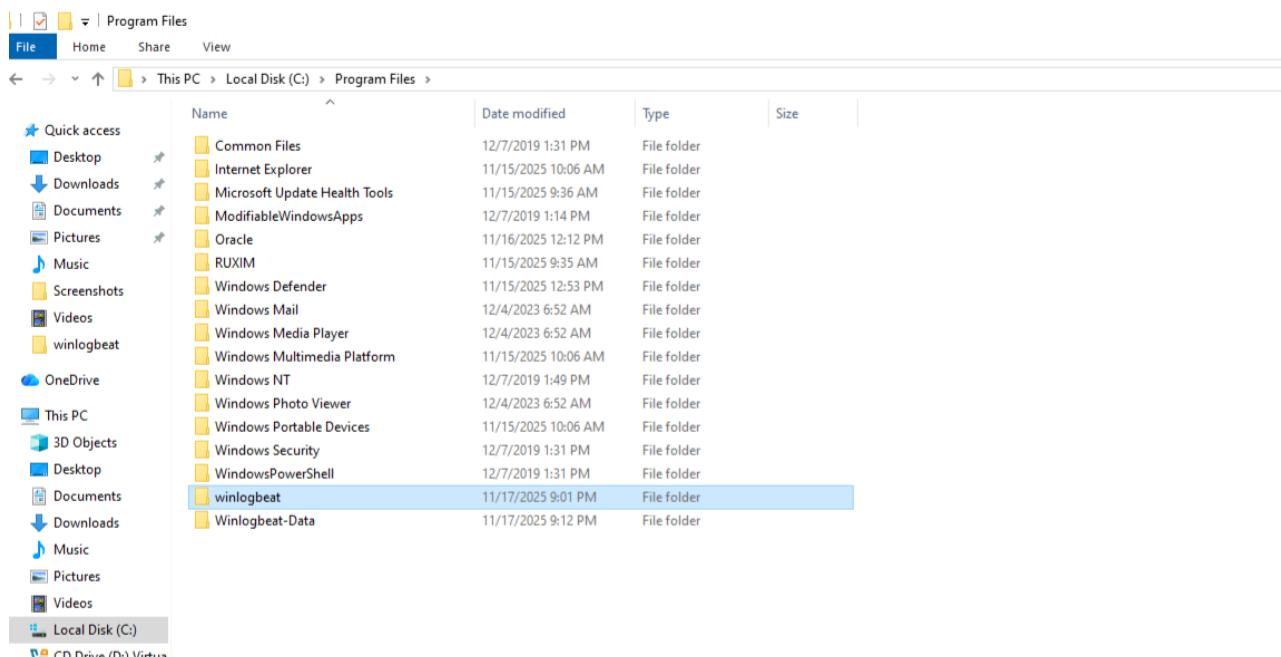
<https://www.elastic.co/downloads/beats/winlogbeat>



The screenshot shows a Windows 10 desktop environment. A browser window is open to the elastic.co website, specifically the Winlogbeat download page. The page displays the following information:

- Summary:** Version 9.2.1, Release date November 11, 2025.
- Download and unzip Winlogbeat:** Platform selection dropdown set to "Windows ZIP x86\_64". Buttons for "Windows ZIP x86\_64", "sha", and "asc".
- Get started:** Links to "docs" (Getting started with Winlogbeat), "VIDEO" (Getting started with Winlogbeat), and "Support Matrix".
- Notes:** Default distribution governed by the Elastic License, includes the full set of free features.

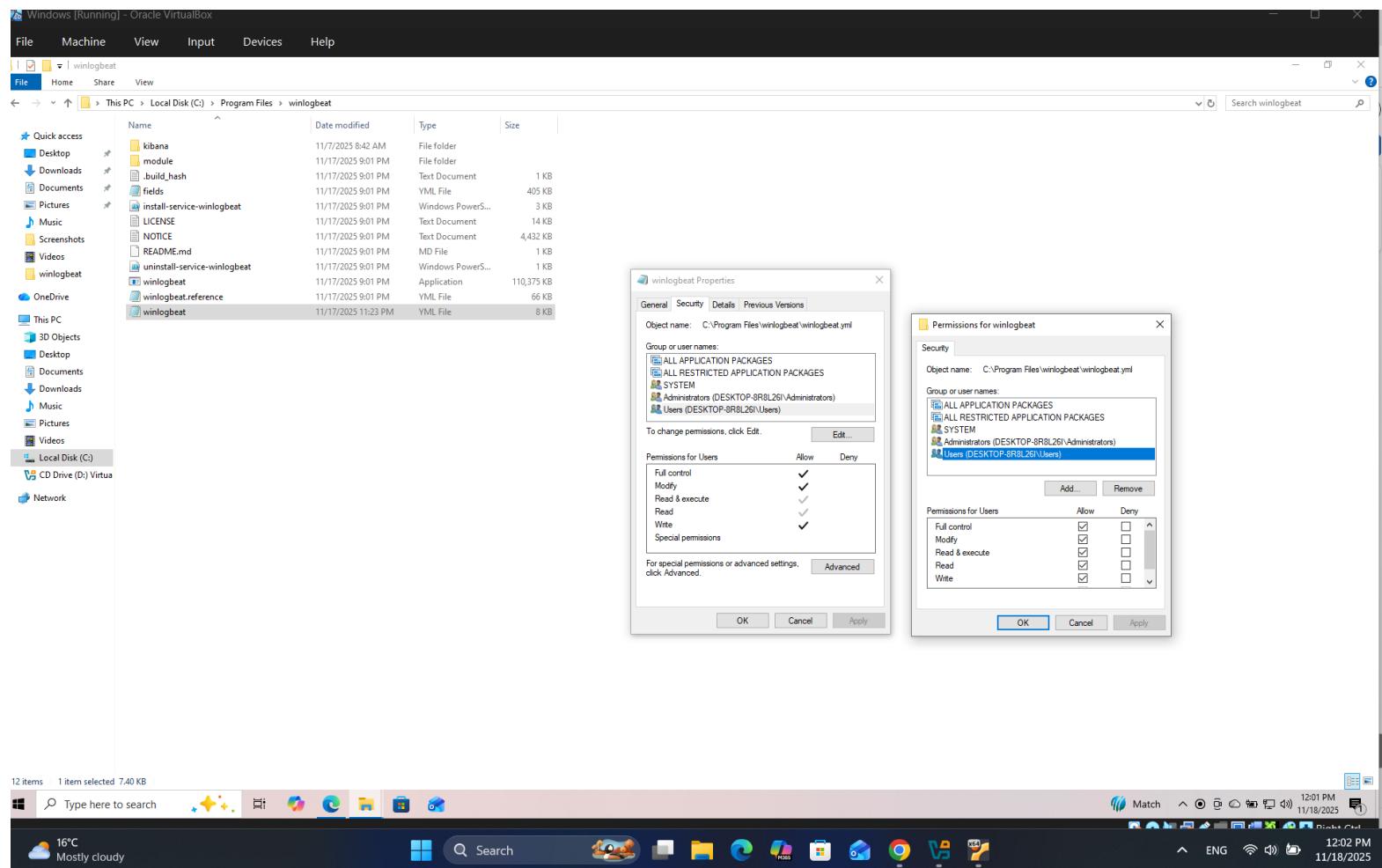
### 2) Extract all files to C:/Program files



The screenshot shows a Windows File Explorer window displaying the contents of the "Program Files" folder located on the Local Disk (C:). The "winlogbeat" folder is selected and highlighted with a blue selection bar. The file list includes:

Name	Date modified	Type	Size
Common Files	12/7/2019 1:31 PM	File folder	
Internet Explorer	11/15/2025 10:06 AM	File folder	
Microsoft Update Health Tools	11/15/2025 9:36 AM	File folder	
ModifiableWindowsApps	12/7/2019 1:14 PM	File folder	
Oracle	11/16/2025 12:12 PM	File folder	
RUXIM	11/15/2025 9:35 AM	File folder	
Windows Defender	11/15/2025 12:53 PM	File folder	
Windows Mail	12/4/2023 6:52 AM	File folder	
Windows Media Player	12/4/2023 6:52 AM	File folder	
Windows Multimedia Platform	11/15/2025 10:06 AM	File folder	
Windows NT	12/7/2019 1:49 PM	File folder	
Windows Photo Viewer	12/4/2023 6:52 AM	File folder	
Windows Portable Devices	11/15/2025 10:06 AM	File folder	
Windows Security	12/7/2019 1:31 PM	File folder	
WindowsPowerShell	12/7/2019 1:31 PM	File folder	
winlogbeat	11/17/2025 9:01 PM	File folder	
Winlogbeat-Data	11/17/2025 9:12 PM	File folder	

### 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 an 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.certificateAuthorities: ["/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"
```

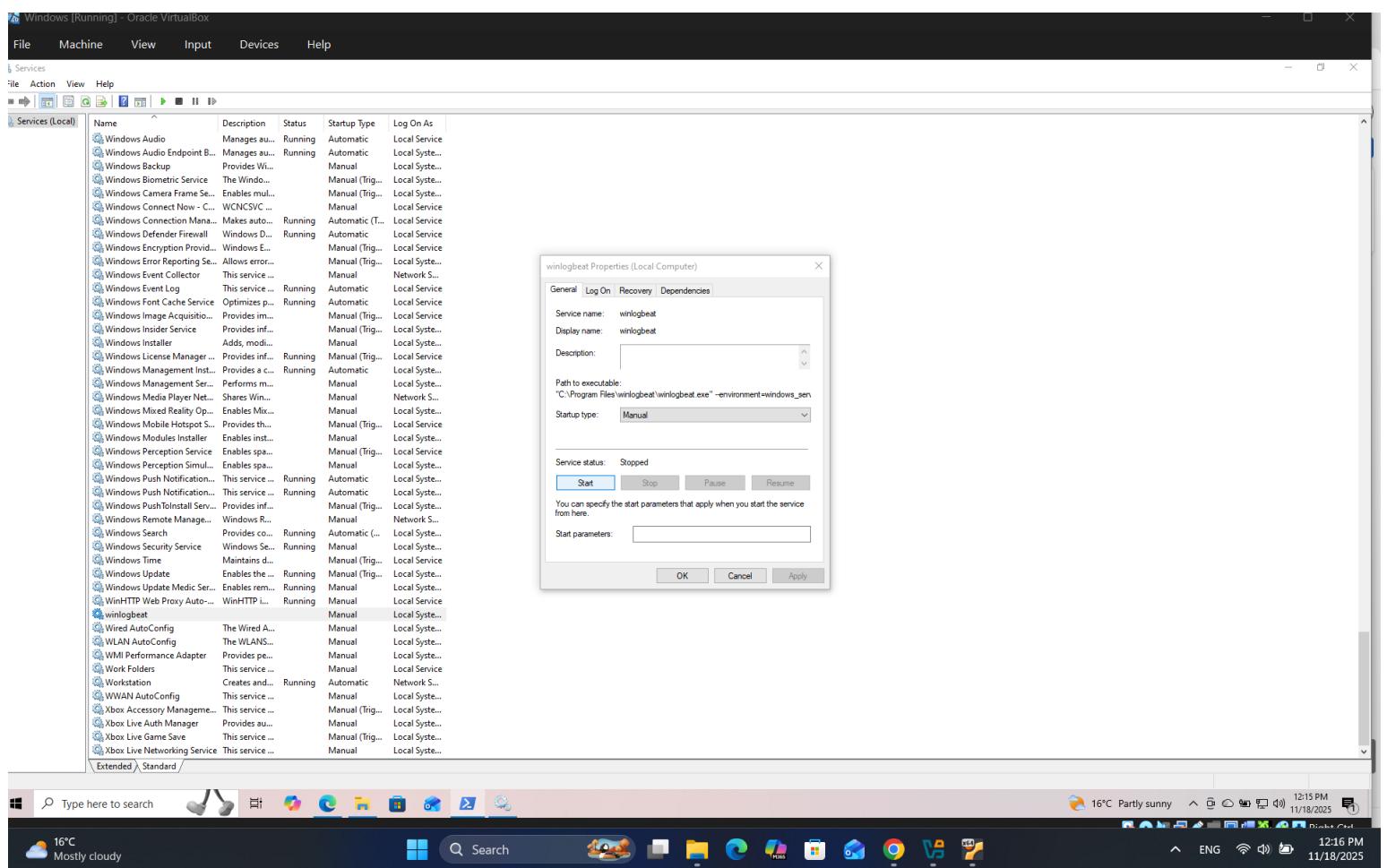
## 5) Powershell install winlogbeat service

- 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

