Elasticsearch Setup on Static IP in Debian/Ubuntu (VMware Lab)

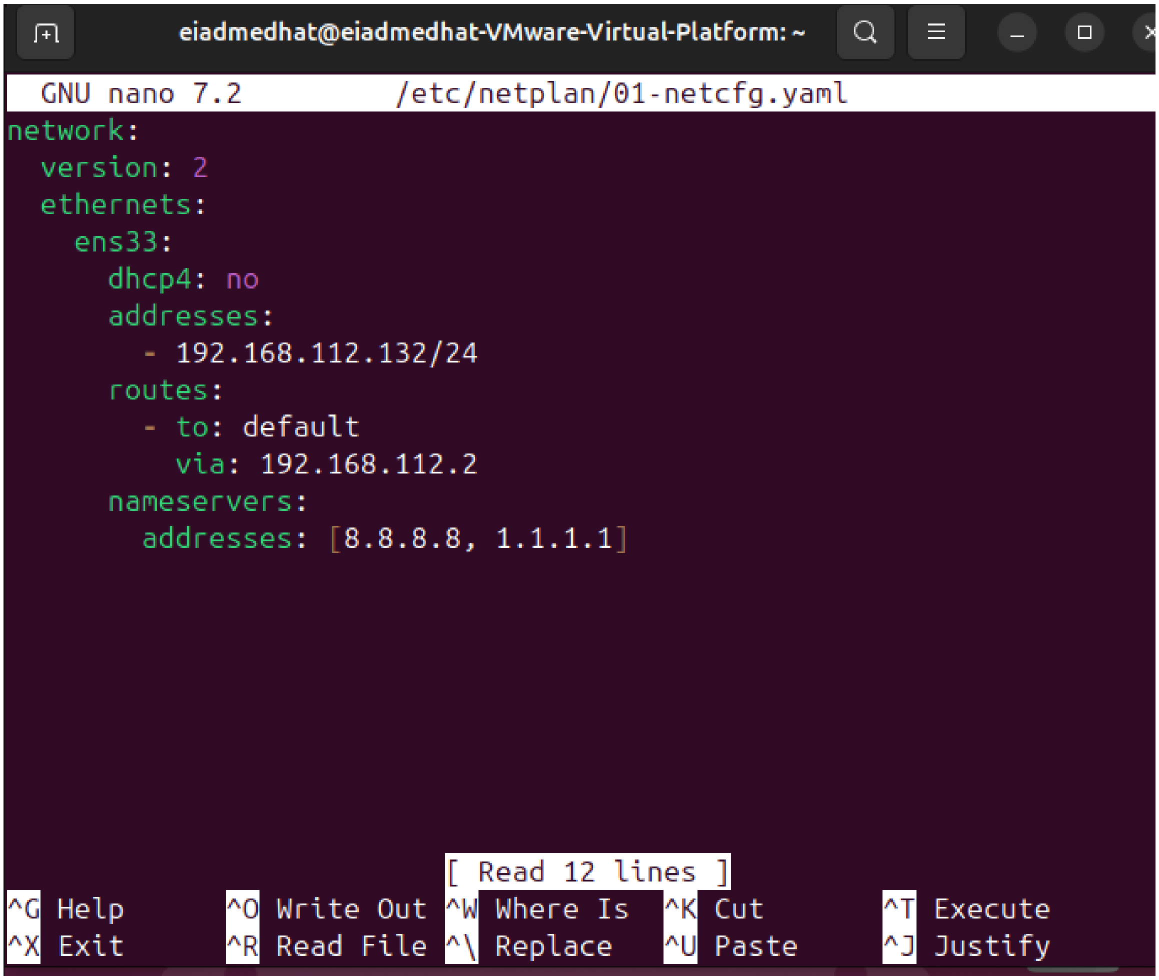
Step 1: Assign a Static IP Address

1. Open the Netplan configuration file:

```
sudo nano /etc/netplan/00-installer-config.yaml
```

2. Edit it to set a static IP, e.g.:

```
network:
 version: 2
 ethernets:
  ens33:
   addresses: [192.168.112.132/24]
   gateway4: 192.168.112.2
   nameservers:
    addresses: [8.8.8.8, 8.8.4.4]
```



```
  GNU nano 7.2          /etc/netplan/01-netcfg.yaml
network:
  version: 2
  ethernets:
    ens33:
      dhcp4: no
      addresses:
        - 192.168.112.132/24
      routes:
        - to: default
          via: 192.168.112.2
      nameservers:
        addresses: [8.8.8.8, 1.1.1.1]

                          [ Read 12 lines ]
^G Help        ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit        ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

3. Apply the configuration:

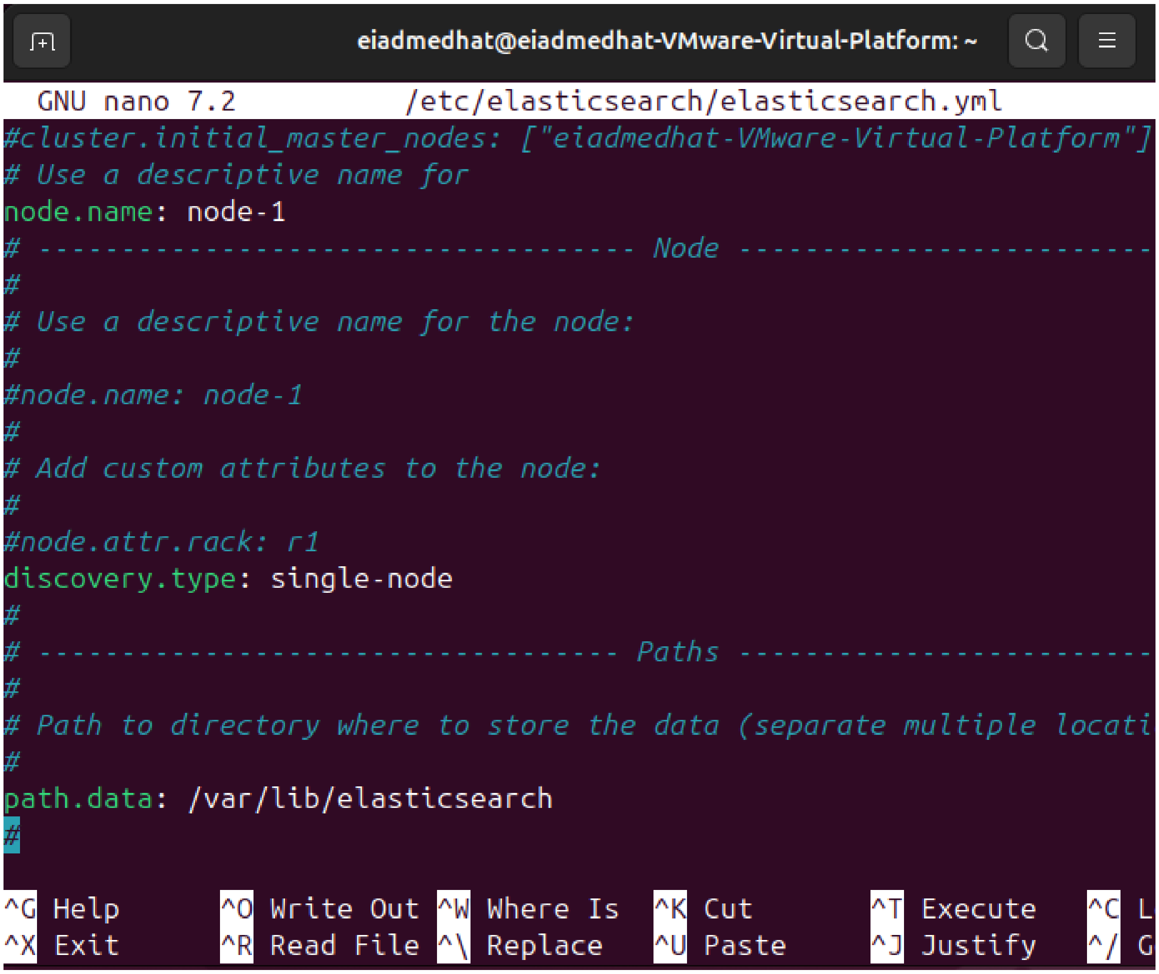
```
sudo netplan apply
```

Step 2: Install Elasticsearch

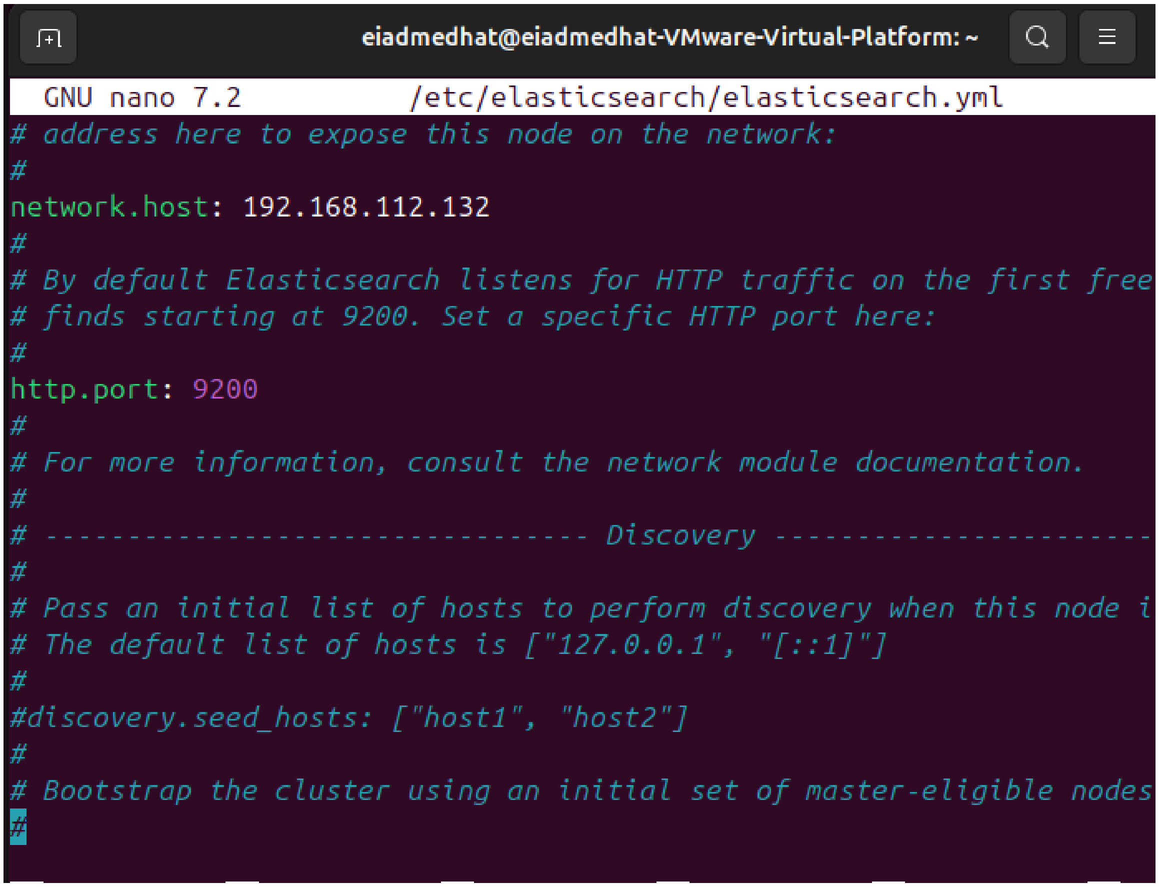
- wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg
- sudo apt-get install apt-transport-https
- echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/9.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-9.x.list
- sudo apt-get update && sudo apt-get install elasticsearch

Step 3: Configure Elasticsearch for Static IP Access

1. Open the config file:
  sudo nano /etc/elasticsearch/elasticsearch.yml
2. Set the following:
  network.host: 192.168.112.132
  http.port: 9200
  cluster.initial_master_nodes: ["node-1"]

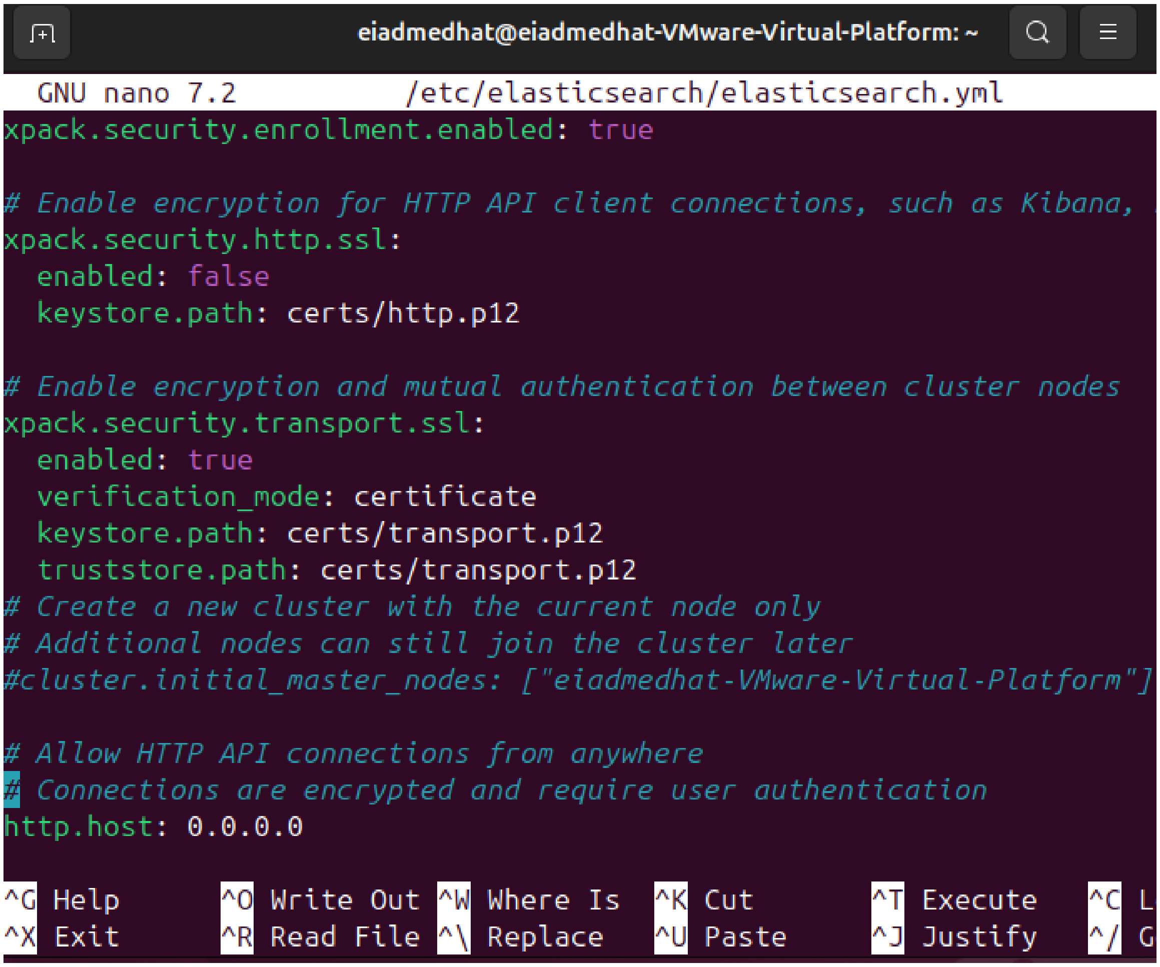


```
#cluster.initial_master_nodes: ["eiadmedhat-VMware-Virtual-Platform"]
# Use a descriptive name for
node.name: node-1
# ----------------------------------- Node -------------------------
#
# Use a descriptive name for the node:
#
#node.name: node-1
#
# Add custom attributes to the node:
#
#node.attr.rack: r1
discovery.type: single-node
#
# ---------------------------------- Paths -------------------------
#
# Path to directory where to store the data (separate multiple locati
#
path.data: /var/lib/elasticsearch
#
```



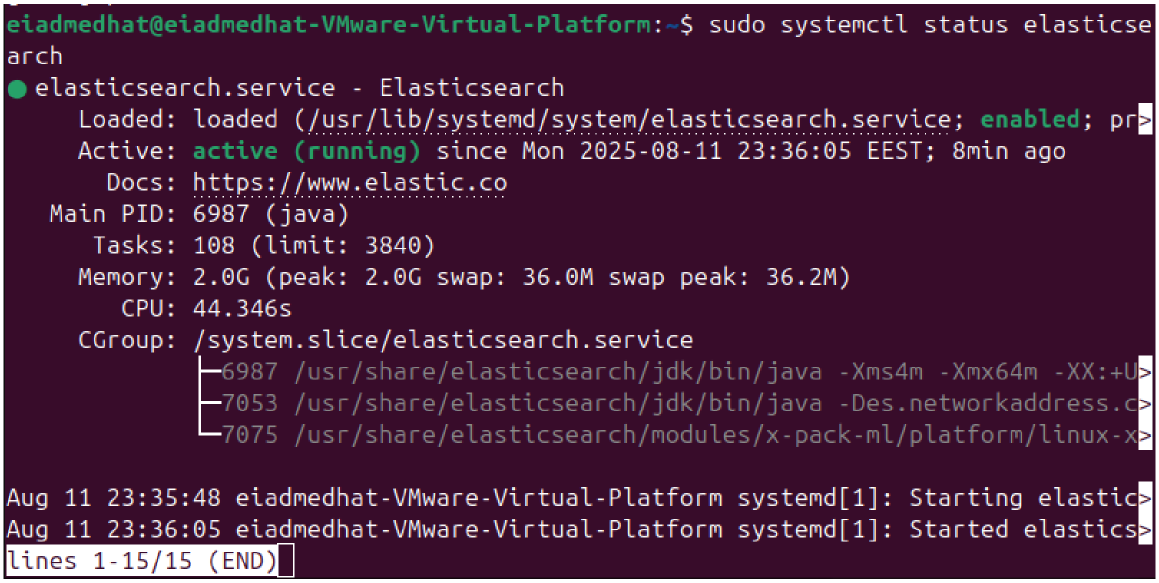
eiadmedhat@eiadmedhat-VMware-Virtual-Platform: ~

```
  GNU nano 7.2            /etc/elasticsearch/elasticsearch.yml
# address here to expose this node on the network:
#
network.host: 192.168.112.132
#
# By default Elasticsearch listens for HTTP traffic on the first free
# 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 i
# 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
#
```



eiadmedhat@eiadmedhat-VMware-Virtual-Platform: ~

```
  GNU nano 7.2            /etc/elasticsearch/elasticsearch.yml
xpack.security.enrollment.enabled: true

# Enable encryption for HTTP API client connections, such as Kibana,
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: ["eiadmedhat-VMware-Virtual-Platform"]

# Allow HTTP API connections from anywhere
# Connections are encrypted and require user authentication
http.host: 0.0.0.0

^G Help        ^O Write Out ^W Where Is  ^K Cut        ^T Execute   ^C L
^X Exit        ^R Read File ^\ Replace   ^U Paste      ^J Justify   ^/ G
```



```
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ sudo systemctl status elasticse
arch
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; pr>
     Active: active (running) since Mon 2025-08-11 23:36:05 EEST; 8min ago
       Docs: https://www.elastic.co
   Main PID: 6987 (java)
      Tasks: 108 (limit: 3840)
     Memory: 2.0G (peak: 2.0G swap: 36.0M swap peak: 36.2M)
        CPU: 44.346s
     CGroup: /system.slice/elasticsearch.service
             ├─6987 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+U>
             ├─7053 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.c>
             └─7075 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x>

Aug 11 23:35:48 eiadmedhat-VMware-Virtual-Platform systemd[1]: Starting elastic>
Aug 11 23:36:05 eiadmedhat-VMware-Virtual-Platform systemd[1]: Started elastics>
lines 1-15/15 (END)
```

3. Save and exit.

Step 4: Enable Security (Built-in User Authentication)

1. In /etc/elasticsearch/elasticsearch.yml, add:

```
xpack.security.enabled: true
xpack.security.http.ssl.enabled: false
```

2. Save and restart Elasticsearch:

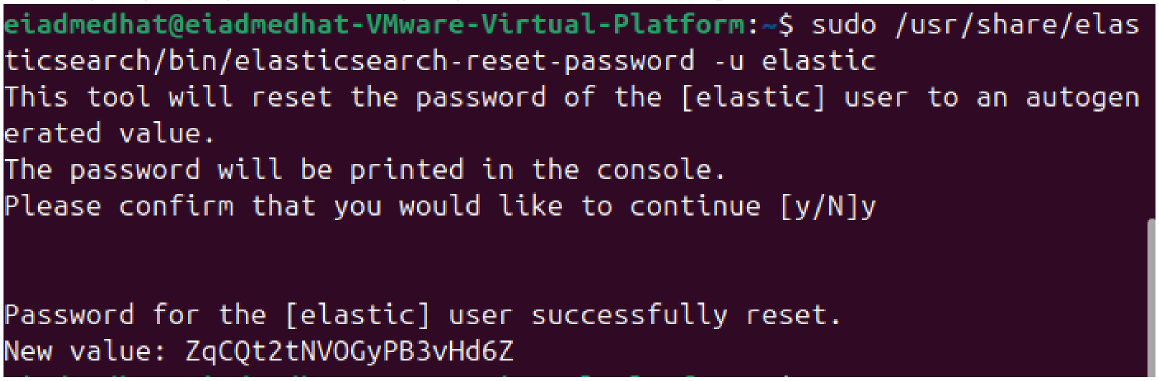
```
sudo systemctl restart elasticsearch
```

Step 5: Enable and Start Elasticsearch Service

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

Step 6: Set Password for elastic User

```
sudo /usr/share/elasticsearch/bin/elasticsearch-reset-password -u elastic
```

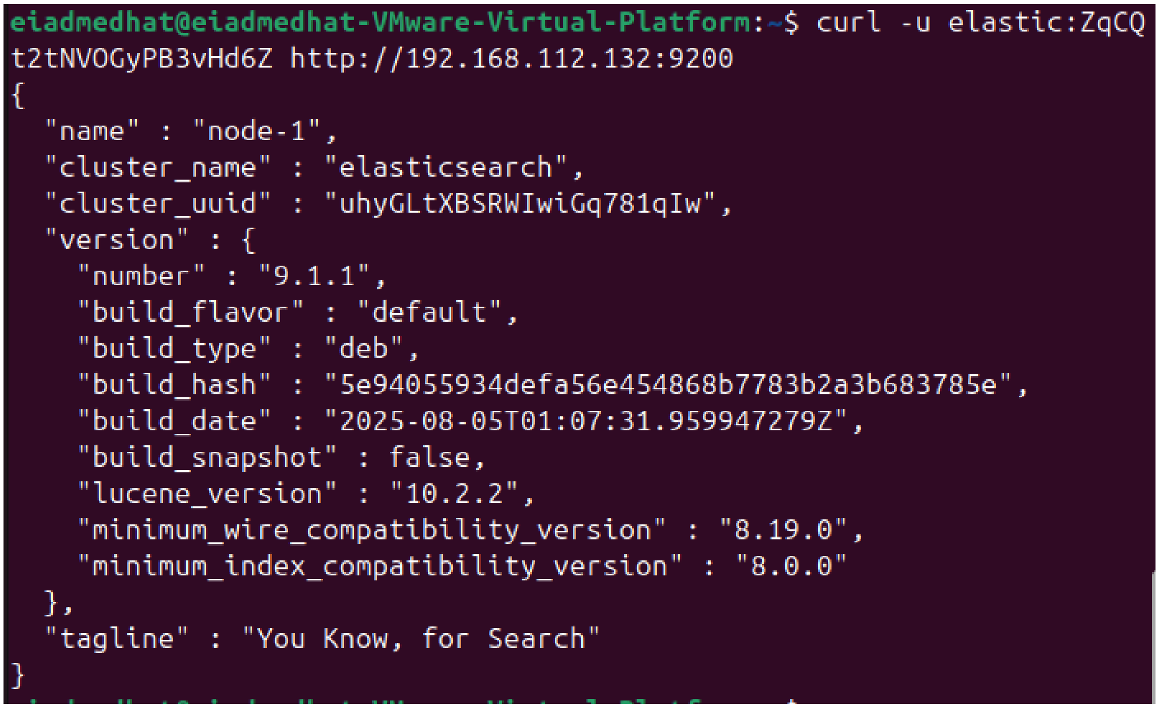


```
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ sudo /usr/share/elas
ticsearch/bin/elasticsearch-reset-password -u elastic
This tool will reset the password of the [elastic] user to an autogen
erated value.
The password will be printed in the console.
Please confirm that you would like to continue [y/N]y


Password for the [elastic] user successfully reset.
New value: ZqCQt2tNVOGyPB3vHd6Z
```

I Changed The Pass After That Because I forgot it So the new pass =” g5E5JsuKDYY4jSYh_h8_” and it will be changed in Filebeat configuration

Step 7: Test the Connection

curl -u elastic:< ZqCQt2tNVOGyPB3vHd6Z > http://192.168.112.132:9200



```
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ curl -u elastic:ZqCQ
t2tNVOGyPB3vHd6Z http://192.168.112.132:9200
{
  "name" : "node-1",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "uhyGLtXBSRWIwiGq781qIw",
  "version" : {
    "number" : "9.1.1",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "5e94055934defa56e454868b7783b2a3b683785e",
    "build_date" : "2025-08-05T01:07:31.959947279Z",
    "build_snapshot" : false,
    "lucene_version" : "10.2.2",
    "minimum_wire_compatibility_version" : "8.19.0",
    "minimum_index_compatibility_version" : "8.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

Then

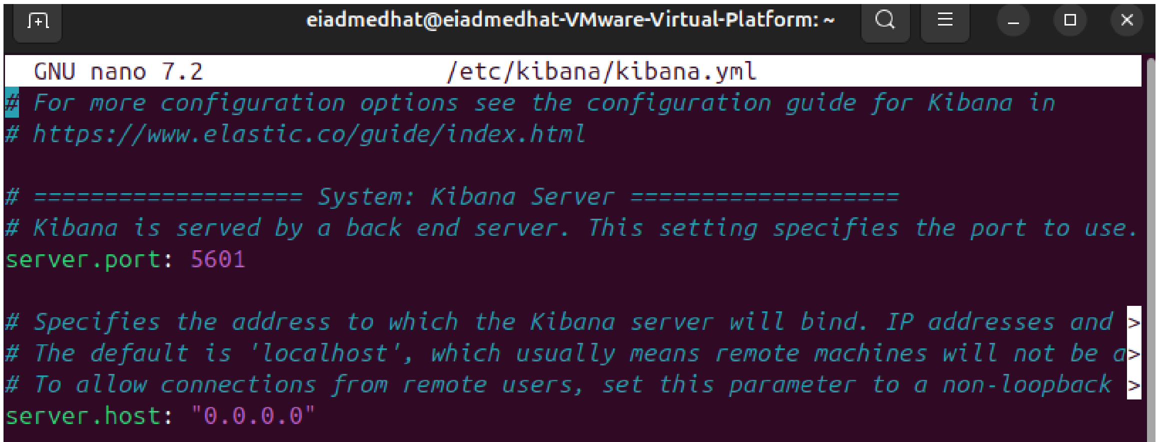
Kibana Installation and Configuration

- wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg
- sudo apt-get install apt-transport-https
- echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/9.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-9.x.list
- sudo apt-get update && sudo apt-get install kibana

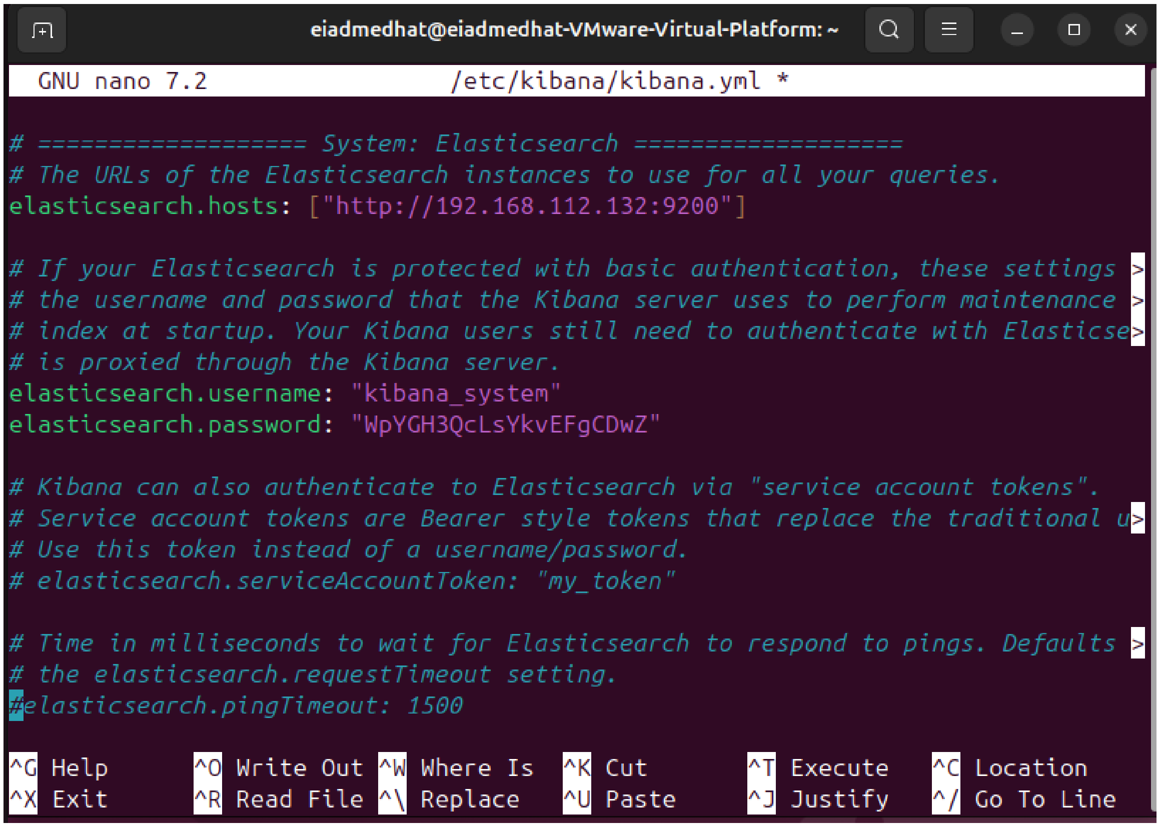
Then

Configure Kibana

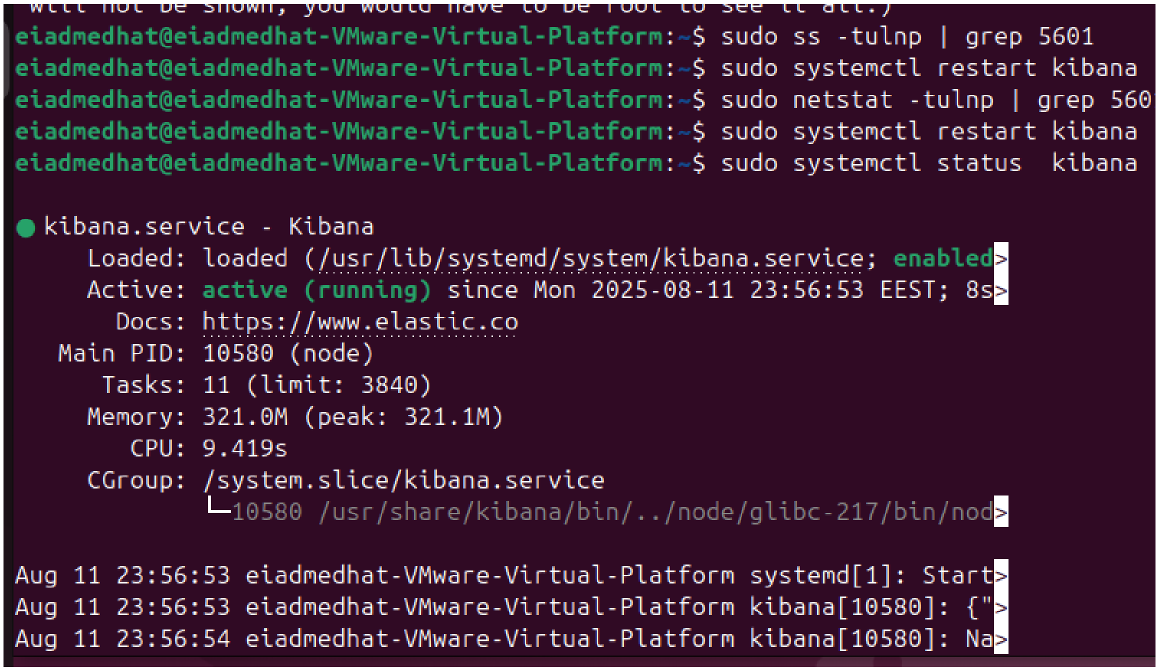
sudo nano /etc/kibana/kibana.yml



```
  GNU nano 7.2                /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 >
# The default is 'localhost', which usually means remote machines will not be a>
# To allow connections from remote users, set this parameter to a non-loopback >
server.host: "0.0.0.0"
```

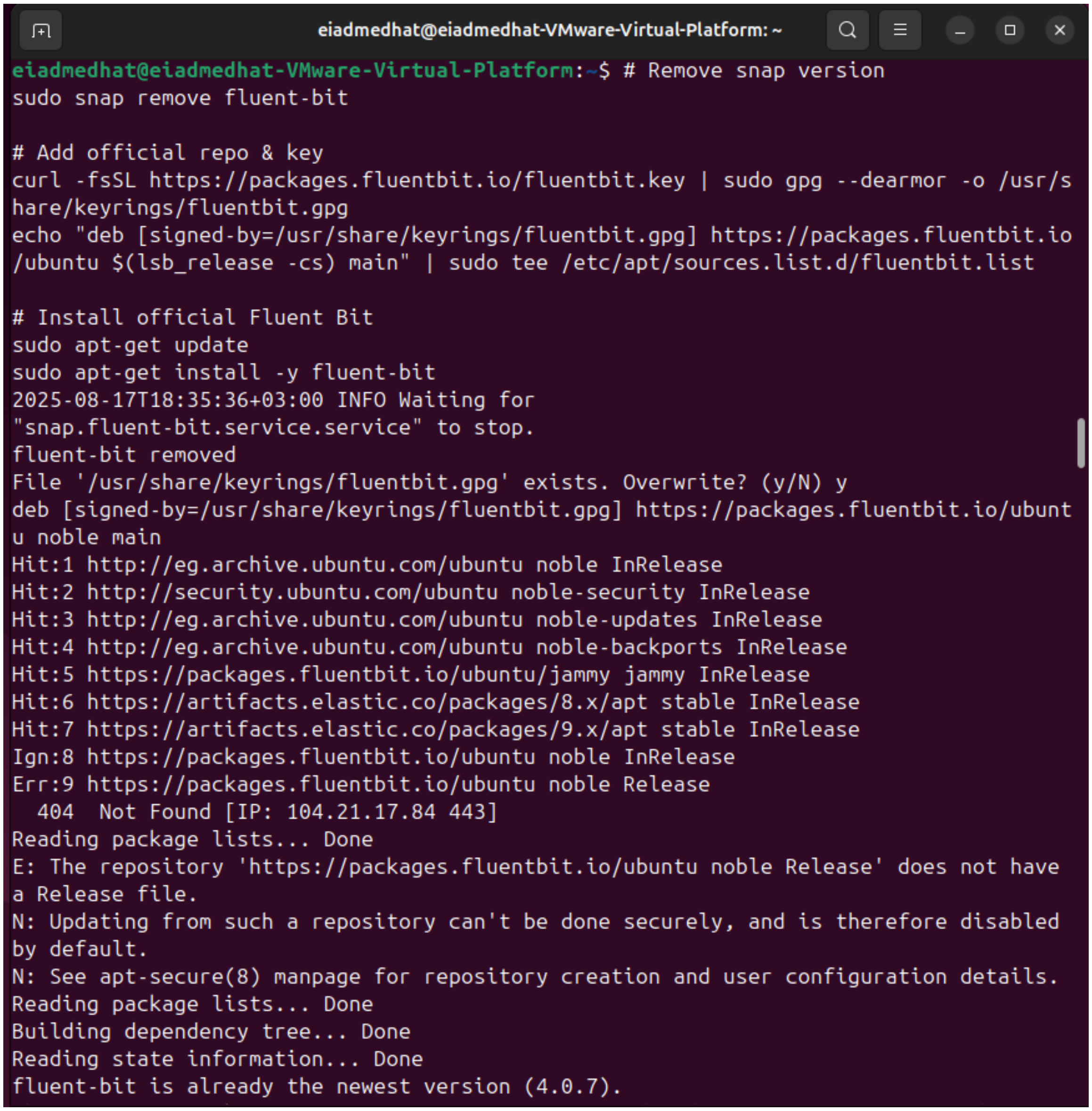


```
  GNU nano 7.2                 /etc/kibana/kibana.yml *

# =================== System: Elasticsearch ===================
# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: ["http://192.168.112.132:9200"]

# If your Elasticsearch is protected with basic authentication, these settings >
# the username and password that the Kibana server uses to perform maintenance >
# index at startup. Your Kibana users still need to authenticate with Elasticse>
# is proxied through the Kibana server.
elasticsearch.username: "kibana_system"
elasticsearch.password: "WpYGH3QcLsYkvEFgCDwZ"

# Kibana can also authenticate to Elasticsearch via "service account tokens".
# Service account tokens are Bearer style tokens that replace the traditional u>
# Use this token instead of a username/password.
# elasticsearch.serviceAccountToken: "my_token"

# Time in milliseconds to wait for Elasticsearch to respond to pings. Defaults >
# the elasticsearch.requestTimeout setting.
#elasticsearch.pingTimeout: 1500

^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line
```

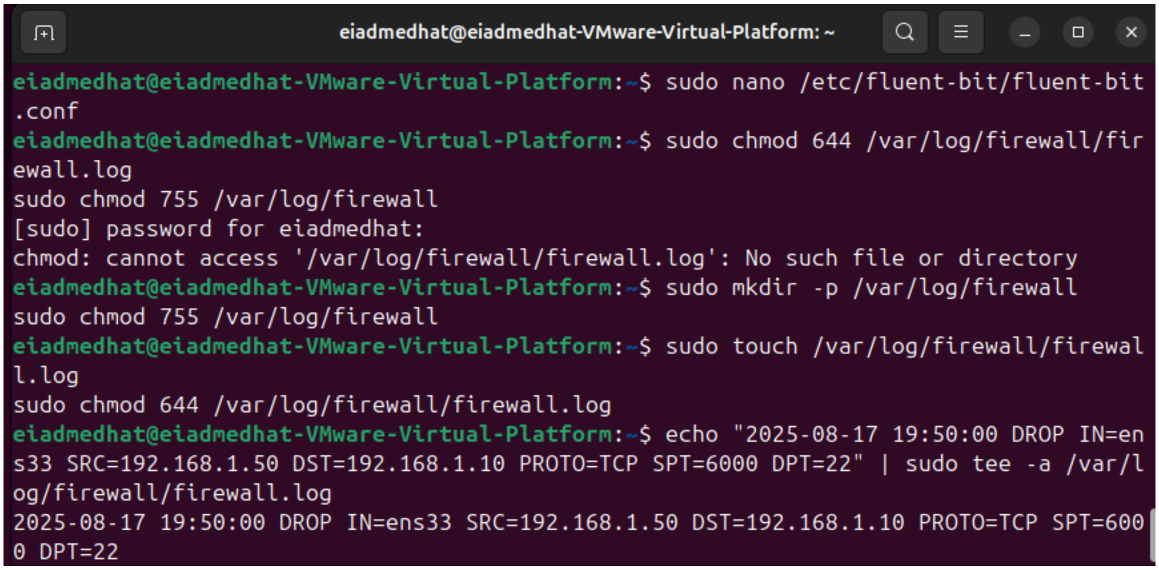


```
 will not be shown, you would have to be root to see it all.)
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ sudo ss -tulnp | grep 5601
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ sudo systemctl restart kibana
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ sudo netstat -tulnp | grep 560
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ sudo systemctl restart kibana
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ sudo systemctl status  kibana

● kibana.service - Kibana
     Loaded: loaded (/usr/lib/systemd/system/kibana.service; enabled>
     Active: active (running) since Mon 2025-08-11 23:56:53 EEST; 8s>
       Docs: https://www.elastic.co
   Main PID: 10580 (node)
      Tasks: 11 (limit: 3840)
     Memory: 321.0M (peak: 321.1M)
        CPU: 9.419s
     CGroup: /system.slice/kibana.service
             └─10580 /usr/share/kibana/bin/../node/glibc-217/bin/nod>

Aug 11 23:56:53 eiadmedhat-VMware-Virtual-Platform systemd[1]: Start>
Aug 11 23:56:53 eiadmedhat-VMware-Virtual-Platform kibana[10580]: {">
Aug 11 23:56:54 eiadmedhat-VMware-Virtual-Platform kibana[10580]: Na>
```

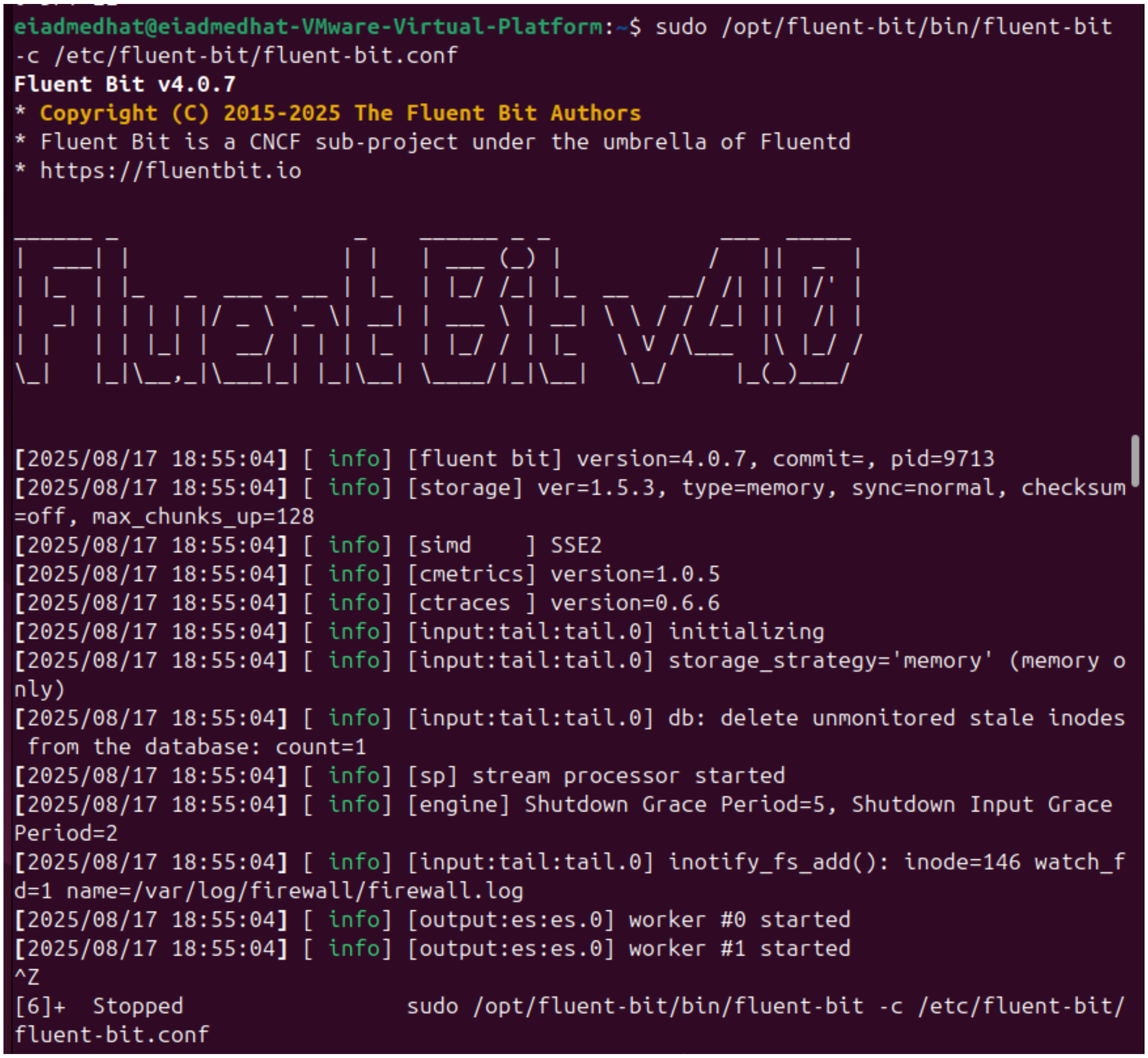
Filebeat Configuration:



```
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ # Remove snap version
sudo snap remove fluent-bit

# Add official repo & key
curl -fsSL https://packages.fluentbit.io/fluentbit.key | sudo gpg --dearmor -o /usr/s
hare/keyrings/fluentbit.gpg
echo "deb [signed-by=/usr/share/keyrings/fluentbit.gpg] https://packages.fluentbit.io
/ubuntu $(lsb_release -cs) main" | sudo tee /etc/apt/sources.list.d/fluentbit.list

# Install official Fluent Bit
sudo apt-get update
sudo apt-get install -y fluent-bit
2025-08-17T18:35:36+03:00 INFO Waiting for
"snap.fluent-bit.service.service" to stop.
fluent-bit removed
File '/usr/share/keyrings/fluentbit.gpg' exists. Overwrite? (y/N) y
deb [signed-by=/usr/share/keyrings/fluentbit.gpg] https://packages.fluentbit.io/ubunt
u noble main
Hit:1 http://eg.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:3 http://eg.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:4 http://eg.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:5 https://packages.fluentbit.io/ubuntu/jammy jammy InRelease
Hit:6 https://artifacts.elastic.co/packages/8.x/apt stable InRelease
Hit:7 https://artifacts.elastic.co/packages/9.x/apt stable InRelease
Ign:8 https://packages.fluentbit.io/ubuntu noble InRelease
Err:9 https://packages.fluentbit.io/ubuntu noble Release
  404  Not Found [IP: 104.21.17.84 443]
Reading package lists... Done
E: The repository 'https://packages.fluentbit.io/ubuntu noble Release' does not have
a Release file.
N: Updating from such a repository can't be done securely, and is therefore disabled
by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
fluent-bit is already the newest version (4.0.7).
```

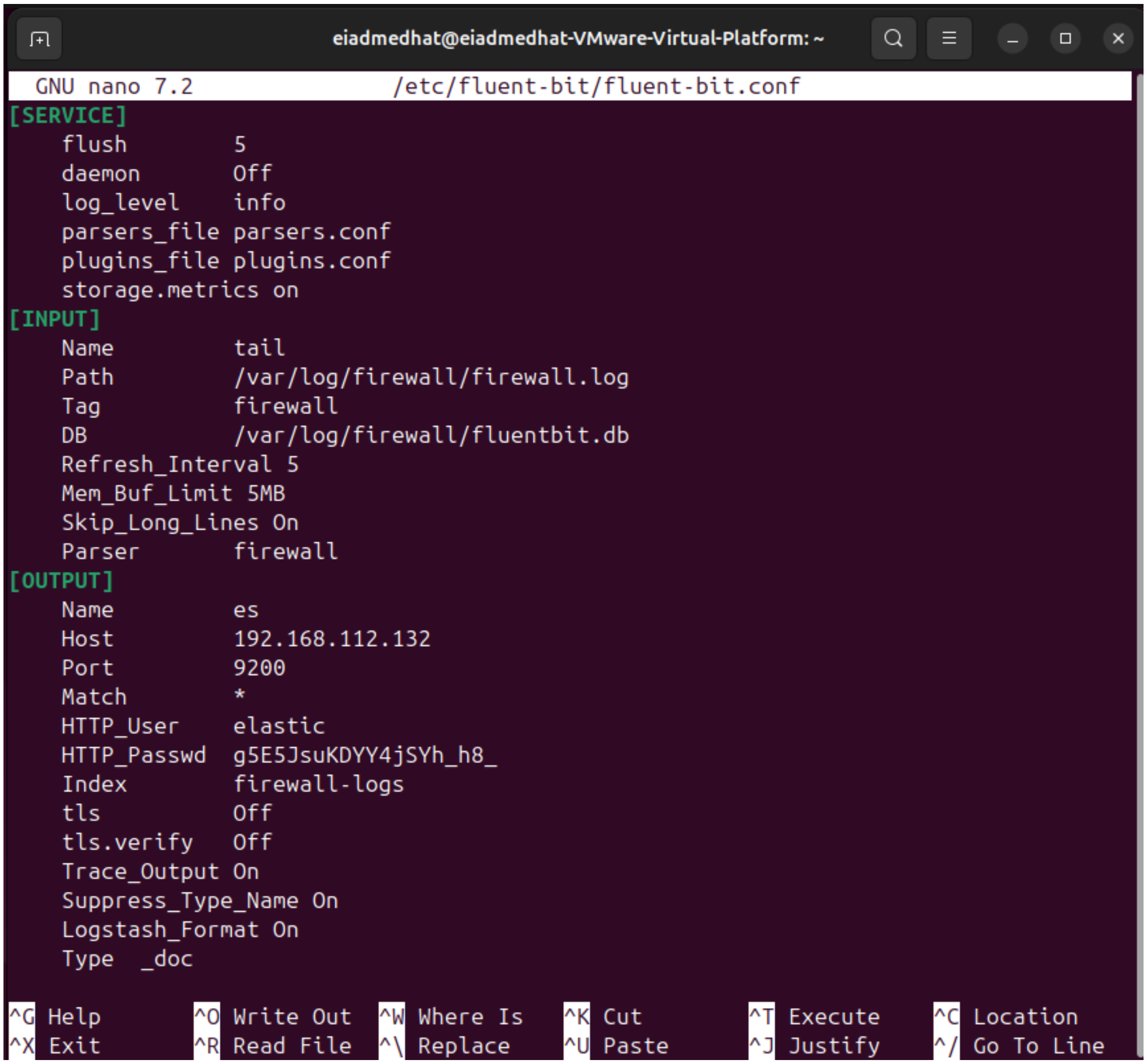


```
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ sudo nano /etc/fluent-bit/fluent-bit
.conf
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ sudo chmod 644 /var/log/firewall/fir
ewall.log
sudo chmod 755 /var/log/firewall
[sudo] password for eiadmedhat:
chmod: cannot access '/var/log/firewall/firewall.log': No such file or directory
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ sudo mkdir -p /var/log/firewall
sudo chmod 755 /var/log/firewall
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ sudo touch /var/log/firewall/firewal
l.log
sudo chmod 644 /var/log/firewall/firewall.log
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ echo "2025-08-17 19:50:00 DROP IN=en
s33 SRC=192.168.1.50 DST=192.168.1.10 PROTO=TCP SPT=6000 DPT=22" | sudo tee -a /var/l
og/firewall/firewall.log
2025-08-17 19:50:00 DROP IN=ens33 SRC=192.168.1.50 DST=192.168.1.10 PROTO=TCP SPT=600
0 DPT=22
```



```
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ sudo /opt/fluent-bit/bin/fluent-bit
-c /etc/fluent-bit/fluent-bit.conf
Fluent Bit v4.0.7
* Copyright (C) 2015-2025 The Fluent Bit Authors
* Fluent Bit is a CNCF sub-project under the umbrella of Fluentd
* https://fluentbit.io

______ _                  _    ______ _ _             ___  _____
|  ___| |                | |   | ___ (_) |           /   ||  _  |
| |_  | |_   _  ___ _ __ | |_  | |_/ /_| |_  __   __/ /| || |/' |
|  _| | | | | |/ _ \ '_ \| __| | ___ \ | __| \ \ / / /_| ||  /| |
| |   | | |_| |  __/ | | | |_  | |_/ / | |_   \ V /\___  |\ |_/ /
\_|   |_|\__,_|\___|_| |_|\__| \____/|_|\__|   \_/     |_(_)___/


[2025/08/17 18:55:04] [ info] [fluent bit] version=4.0.7, commit=, pid=9713
[2025/08/17 18:55:04] [ info] [storage] ver=1.5.3, type=memory, sync=normal, checksum
=off, max_chunks_up=128
[2025/08/17 18:55:04] [ info] [simd    ] SSE2
[2025/08/17 18:55:04] [ info] [cmetrics] version=1.0.5
[2025/08/17 18:55:04] [ info] [ctraces ] version=0.6.6
[2025/08/17 18:55:04] [ info] [input:tail:tail.0] initializing
[2025/08/17 18:55:04] [ info] [input:tail:tail.0] storage_strategy='memory' (memory o
nly)
[2025/08/17 18:55:04] [ info] [input:tail:tail.0] db: delete unmonitored stale inodes
 from the database: count=1
[2025/08/17 18:55:04] [ info] [sp] stream processor started
[2025/08/17 18:55:04] [ info] [engine] Shutdown Grace Period=5, Shutdown Input Grace
Period=2
[2025/08/17 18:55:04] [ info] [input:tail:tail.0] inotify_fs_add(): inode=146 watch_f
d=1 name=/var/log/firewall/firewall.log
[2025/08/17 18:55:04] [ info] [output:es:es.0] worker #0 started
[2025/08/17 18:55:04] [ info] [output:es:es.0] worker #1 started
^Z
[6]+  Stopped                 sudo /opt/fluent-bit/bin/fluent-bit -c /etc/fluent-bit/
fluent-bit.conf
```

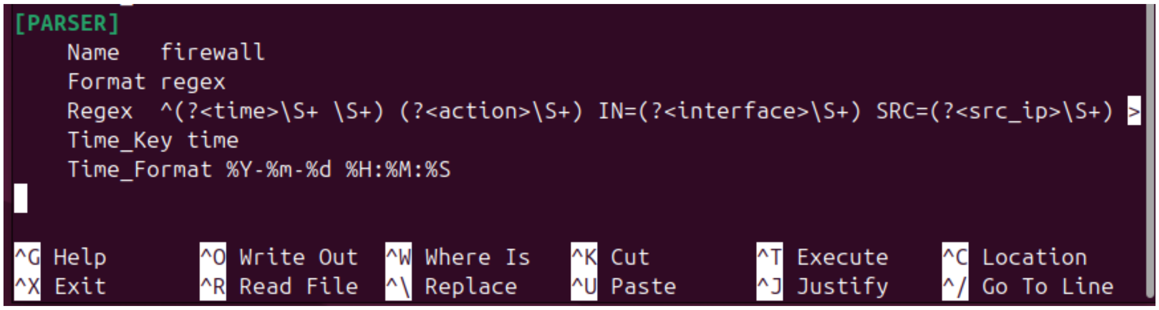
Then: sudo nano /etc/fluent-bit/fluent-bit.conf



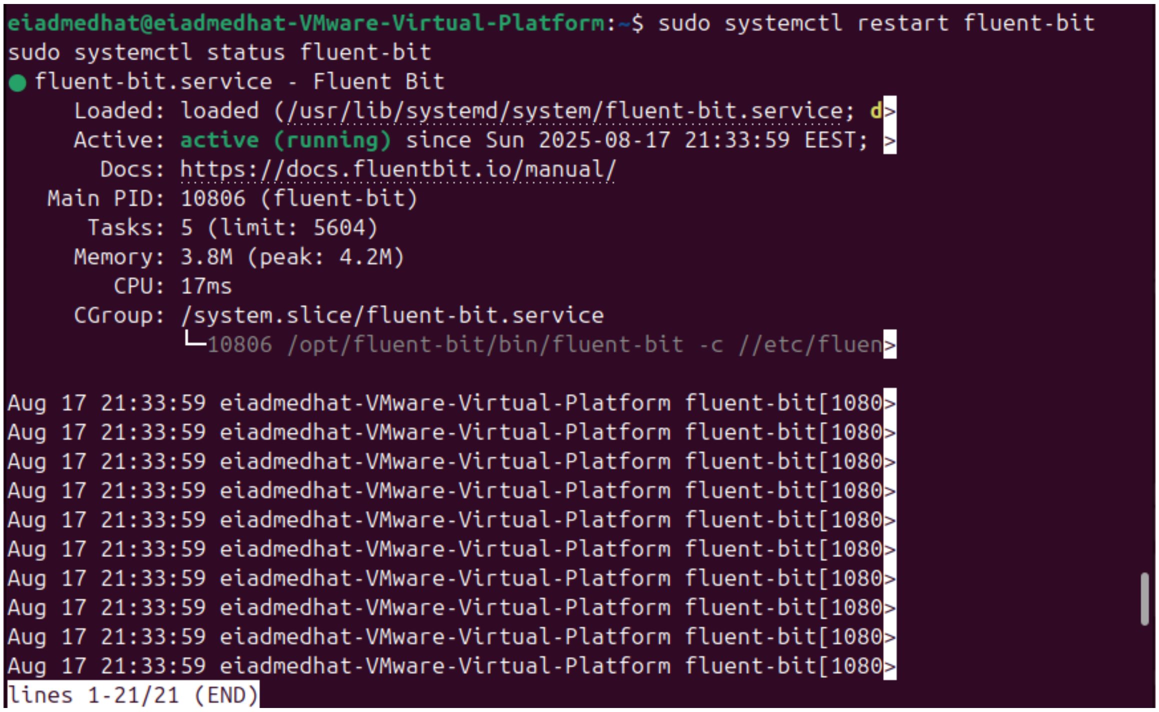
```
 GNU nano 7.2                /etc/fluent-bit/fluent-bit.conf
[SERVICE]
    flush        5
    daemon       Off
    log_level    info
    parsers_file parsers.conf
    plugins_file plugins.conf
    storage.metrics on
[INPUT]
    Name         tail
    Path         /var/log/firewall/firewall.log
    Tag          firewall
    DB           /var/log/firewall/fluentbit.db
    Refresh_Interval 5
    Mem_Buf_Limit 5MB
    Skip_Long_Lines On
    Parser       firewall
[OUTPUT]
    Name         es
    Host         192.168.112.132
    Port         9200
    Match        *
    HTTP_User    elastic
    HTTP_Passwd  g5E5JsuKDYY4jSYh_h8_
    Index        firewall-logs
    tls          Off
    tls.verify   Off
    Trace_Output On
    Suppress_Type_Name On
    Logstash_Format On
    Type   _doc

^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line
```

We Add sudo nano /etc/fluent-bit/parsers.conf

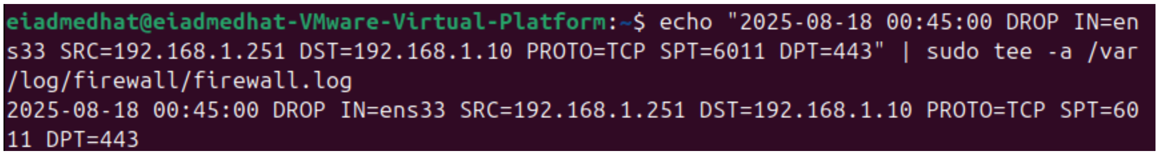
```
[PARSER]

  Name  firewall

  Format regex

  Regex  ^(?<time>\S+ \S+) (?<action>\S+) IN=(?<interface>\S+) SRC=(?<src_ip>\S+) >

  Time_Key time

  Time_Format %Y-%m-%d %H:%M:%S
```



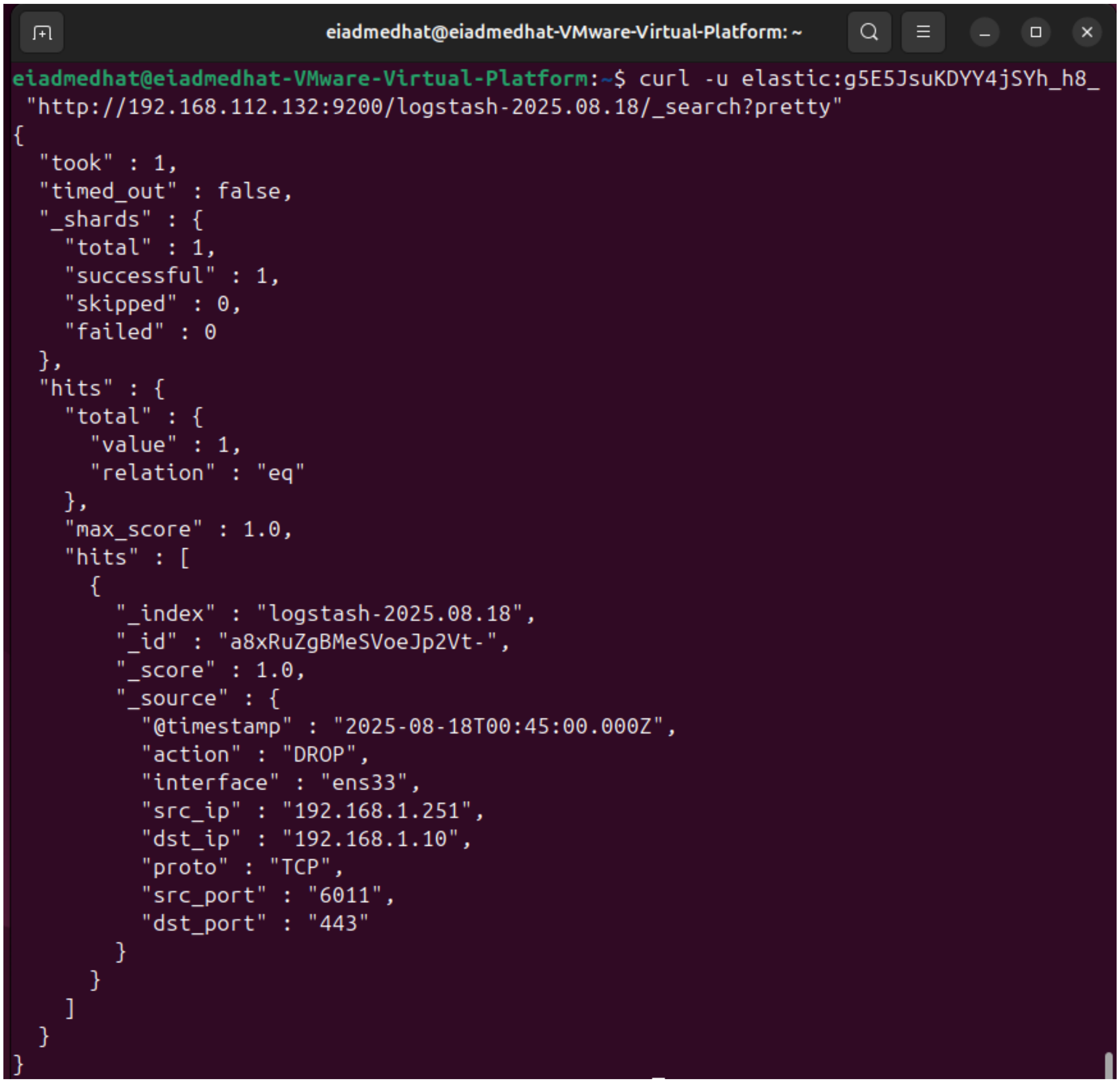
```
[PARSER]
    Name   firewall
    Format regex
    Regex  ^(?<time>\S+ \S+) (?<action>\S+) IN=(?<interface>\S+) SRC=(?<src_ip>\S+) >
    Time_Key time
    Time_Format %Y-%m-%d %H:%M:%S

^G Help         ^O Write Out    ^W Where Is     ^K Cut          ^T Execute      ^C Location
^X Exit         ^R Read File    ^\ Replace      ^U Paste        ^J Justify      ^/ Go To Line
```



```
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ sudo systemctl restart fluent-bit
sudo systemctl status fluent-bit
● fluent-bit.service - Fluent Bit
     Loaded: loaded (/usr/lib/systemd/system/fluent-bit.service; d>
     Active: active (running) since Sun 2025-08-17 21:33:59 EEST; >
       Docs: https://docs.fluentbit.io/manual/
   Main PID: 10806 (fluent-bit)
      Tasks: 5 (limit: 5604)
     Memory: 3.8M (peak: 4.2M)
        CPU: 17ms
     CGroup: /system.slice/fluent-bit.service
             └─10806 /opt/fluent-bit/bin/fluent-bit -c //etc/fluen>

Aug 17 21:33:59 eiadmedhat-VMware-Virtual-Platform fluent-bit[1080>
Aug 17 21:33:59 eiadmedhat-VMware-Virtual-Platform fluent-bit[1080>
Aug 17 21:33:59 eiadmedhat-VMware-Virtual-Platform fluent-bit[1080>
Aug 17 21:33:59 eiadmedhat-VMware-Virtual-Platform fluent-bit[1080>
Aug 17 21:33:59 eiadmedhat-VMware-Virtual-Platform fluent-bit[1080>
Aug 17 21:33:59 eiadmedhat-VMware-Virtual-Platform fluent-bit[1080>
Aug 17 21:33:59 eiadmedhat-VMware-Virtual-Platform fluent-bit[1080>
Aug 17 21:33:59 eiadmedhat-VMware-Virtual-Platform fluent-bit[1080>
Aug 17 21:33:59 eiadmedhat-VMware-Virtual-Platform fluent-bit[1080>
Aug 17 21:33:59 eiadmedhat-VMware-Virtual-Platform fluent-bit[1080>
lines 1-21/21 (END)
```



```
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ echo "2025-08-18 00:45:00 DROP IN=en
s33 SRC=192.168.1.251 DST=192.168.1.10 PROTO=TCP SPT=6011 DPT=443" | sudo tee -a /var
/log/firewall/firewall.log
2025-08-18 00:45:00 DROP IN=ens33 SRC=192.168.1.251 DST=192.168.1.10 PROTO=TCP SPT=60
11 DPT=443
```

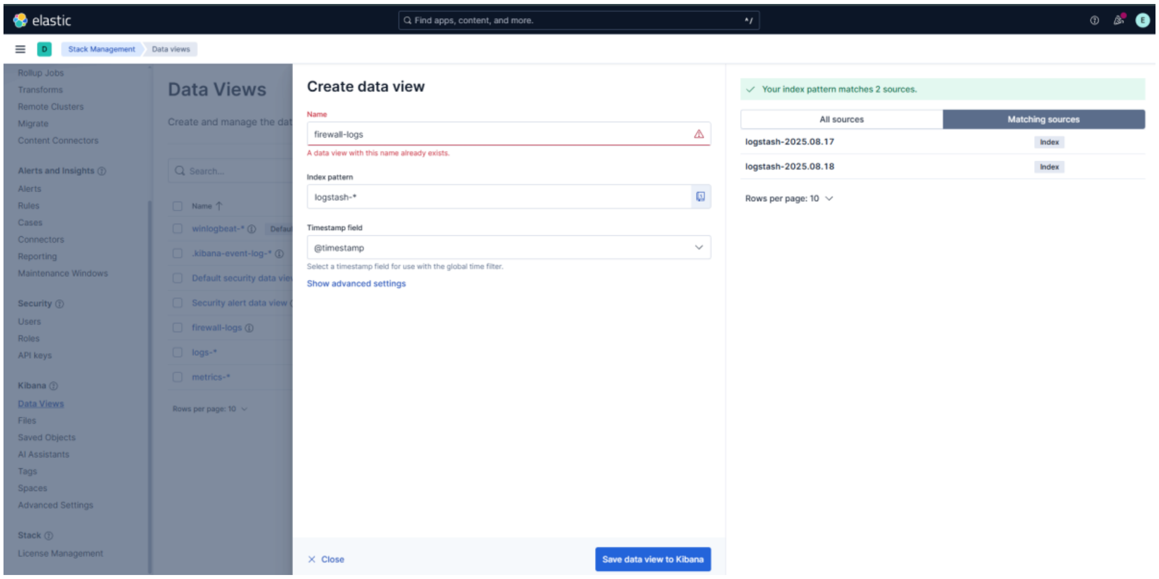


```
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ curl -u elastic:g5E5JsuKDYY4jSYh_h8_
 "http://192.168.112.132:9200/logstash-2025.08.18/_search?pretty"
{
  "took" : 1,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 1,
      "relation" : "eq"
    },
    "max_score" : 1.0,
    "hits" : [
      {
        "_index" : "logstash-2025.08.18",
        "_id" : "a8xRuZgBMeSVoeJp2Vt-",
        "_score" : 1.0,
        "_source" : {
          "@timestamp" : "2025-08-18T00:45:00.000Z",
          "action" : "DROP",
          "interface" : "ens33",
          "src_ip" : "192.168.1.251",
          "dst_ip" : "192.168.1.10",
          "proto" : "TCP",
          "src_port" : "6011",
          "dst_port" : "443"
        }
      }
    ]
  }
}
```

Check the Data View

In Kibana:

1. Go to **Stack Management → Data Views**.
2. Make sure you created a data view with:
    - **Index pattern**: logstash-*
    - **Time field**: @timestamp



Create data view

Name: firewall-logs

A data view with this name already exists.

Index pattern: logstash-*

Timestamp field: @timestamp

Select a timestamp field for use with the global time filter.

Show advanced settings

✓ Your index pattern matches 2 sources.

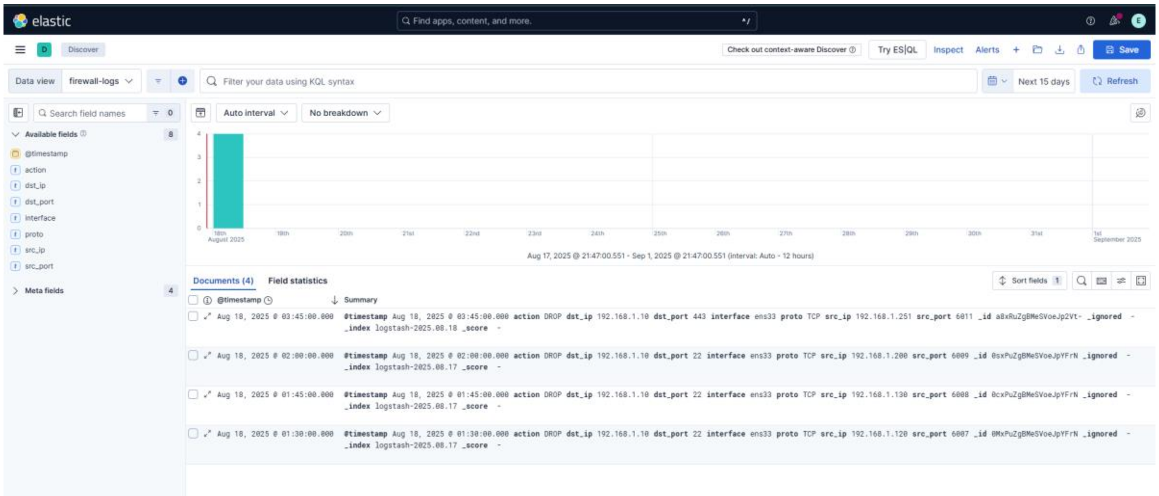
All sources | Matching sources

logstash-2025.08.17	Index
logstash-2025.08.18	Index

Rows per page: 10

Then

- Go to **Discover**
- In the **top-right corner**, change the time filter:



Aug 17, 2025 @ 21:47:00.551 - Sep 1, 2025 @ 21:47:00.551 (interval: Auto - 12 hours)

```
@timestamp                     Summary
Aug 18, 2025 @ 03:45:00.000   @timestamp Aug 18, 2025 @ 03:45:00.000 action DROP dst_ip 192.168.1.10 dst_port 443 interface ens33 proto TCP src_ip 192.168.1.251 src_port 6011 _id a8xRuZgBMeSVoeJp2Vt- _ignored -
                               _index logstash-2025.08.18 _score -
Aug 18, 2025 @ 02:00:00.000   @timestamp Aug 18, 2025 @ 02:00:00.000 action DROP dst_ip 192.168.1.10 dst_port 22 interface ens33 proto TCP src_ip 192.168.1.200 src_port 6009 _id 0sxPuZgBMeSVoeJpYFrN _ignored -
                               _index logstash-2025.08.17 _score -
Aug 18, 2025 @ 01:45:00.000   @timestamp Aug 18, 2025 @ 01:45:00.000 action DROP dst_ip 192.168.1.10 dst_port 22 interface ens33 proto TCP src_ip 192.168.1.130 src_port 6008 _id 0cxPuZgBMeSVoeJpYFrN _ignored -
                               _index logstash-2025.08.17 _score -
Aug 18, 2025 @ 01:30:00.000   @timestamp Aug 18, 2025 @ 01:30:00.000 action DROP dst_ip 192.168.1.10 dst_port 22 interface ens33 proto TCP src_ip 192.168.1.120 src_port 6007 _id 0MxPuZgBMeSVoeJpYFrN _ignored -
                               _index logstash-2025.08.17 _score -
```