Bước 1: Cập nhật hệ thống

Trước khi bắt đầu, hãy đảm bảo rằng hệ thống được cập nhật với các bản vá và phần mềm mới nhất.

sudo apt update

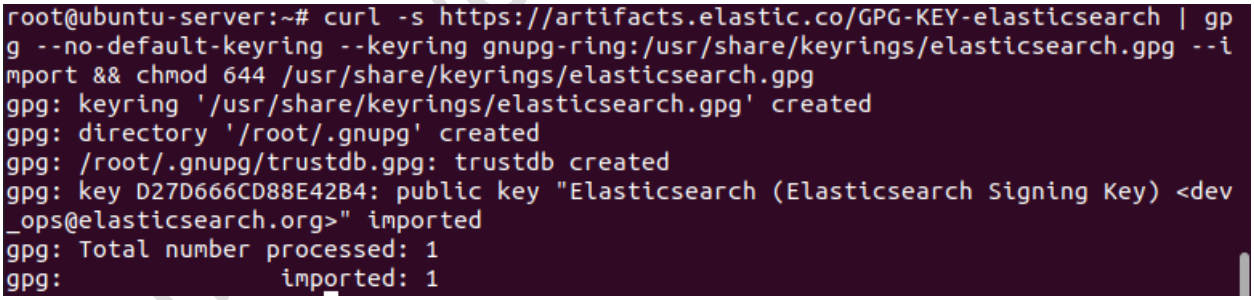
sudo apt upgrade –y

Bước 2: Tải các gói cần thiết cho máy

apt install apt-transport-https zip unzip lsb-release curl gnupg net-tools *(cả 2 máy Wazuh Server và Agent Ubuntu)*

Bước 3: Cài đặt khóa GPG (GNU Privacy Guard: là một loại khóa mã hóa được sử dụng trong hệ thống mã hóa **GPG**, một phần mềm mã nguồn mở dùng để mã hóa và xác thực dữ liệu. GPG hỗ trợ cả mã hóa **symmetric** (mã hóa đối xứng) và **asymmetric** (mã hóa bất đối xứng), trong đó mã hóa bất đối xứng là cơ chế thường dùng cho các khóa GPG.)

curl -s https://artifacts.elastic.co/GPG-KEY-elasticsearch | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/elasticsearch.gpg --import && chmod 644 /usr/share/keyrings/elasticsearch.gpg



Bước 4: Thêm kho lưu trữ Wazuh

echo "deb [signed-by=/usr/share/keyrings/elasticsearch.gpg] https://artifacts.elastic.co/packages/7.x/apt stable main" | tee /etc/apt/sources.list.d/elastic-7.x.list

```
root@ubuntu-server:~# echo "deb [signed-by=/usr/share/keyrings/elasticsearch.gpg] htt
ps://artifacts.elastic.co/packages/7.x/apt stable main" | tee /etc/apt/sources.list.d
/elastic-7.x.list
deb [signed-by=/usr/share/keyrings/elasticsearch.gpg] https://artifacts.elastic.co/pa
ckages/7.x/apt stable main
```

Bước 5: Cài đặt gói ElasticSearch

Cập nhật lại danh sách gói và cài đặt gói **ElasticSearch**:

sudo apt update

sudo apt install elasticsearch=7.17.9

Bước 6: Download file cấu hình /etc/elasticsearch/elasticsearch.yml

curl -so /etc/elasticsearch/elasticsearch.yml https://packages.wazuh.com/4.4/tpl/elastic-basic/elasticsearch_all_in_one.yml

Bước 7: Tạo các chứng chỉ (cert)

curl -so /usr/share/elasticsearch/instances.yml https://packages.wazuh.com/4.4/tpl/elastic-basic/instances_aio.yml

/usr/share/elasticsearch/bin/elasticsearch-certutil cert ca --pem --in instances.yml --keep-ca-key --out ~/certs.zip

Bước 8: Giải nén tệp *certs.zip*

unzip ~/certs.zip -d ~/certs

```
root@ubuntu-server:~# unzip ~/certs.zip -d ~/certs
Archive:  /root/certs.zip
   creating: /root/certs/ca/
  inflating: /root/certs/ca/ca.crt
  inflating: /root/certs/ca/ca.key
   creating: /root/certs/elasticsearch/
  inflating: /root/certs/elasticsearch/elasticsearch.crt
  inflating: /root/certs/elasticsearch/elasticsearch.key
```

Bước 9: Tạo thư mục /etc/elasticsearch/certs

mkdir /etc/elasticsearch/certs/ca –p

cp -R ~/certs/ca/ ~/certs/elasticsearch/* /etc/elasticsearch/certs/

chown -R elasticsearch: /etc/elasticsearch/certs

chmod -R 500 /etc/elasticsearch/certs

chmod 400 /etc/elasticsearch/certs/ca/ca.* /etc/elasticsearch/certs/elasticsearch.*

rm -rf ~/certs/ ~/certs.zip

Bước 10: Kích hoạt và bắt đầu dịch vụ Elasticsearch

systemctl daemon-reload

systemctl enable elasticsearch.service

systemctl start elasticsearch.service

```
root@ubuntu-server:~# systemctl daemon-reload
```

```
root@ubuntu-server:~# systemctl enable elasticsearch.service
Synchronizing state of elasticsearch.service with SysV service script with /lib/systemd/syst
emd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /lib/sys
temd/system/elasticsearch.service.
root@ubuntu-server:~# systemctl start elasticsearch.service
root@ubuntu-server:~#
```

Bước 11: Tạo thông tin xác thực ngẫu nhiên

/usr/share/elasticsearch/bin/elasticsearch-setup-passwords auto

```
root@ubuntu-server:~# /usr/share/elasticsearch/bin/elasticsearch-setup-passwords auto
Initiating the setup of passwords for reserved users elastic,apm_system,kibana,kibana_system,log
stash_system,beats_system,remote_monitoring_user.
The passwords will be randomly generated and printed to the console.
Please confirm that you would like to continue [y/N]y


Changed password for user apm_system
PASSWORD apm_system = 2WXhg6qo2eWWj7uIvrLX

Changed password for user kibana_system
PASSWORD kibana_system = zuWMu43uauloNS0HnUlb

Changed password for user kibana
PASSWORD kibana = zuWMu43uauloNS0HnUlb

Changed password for user logstash_system
PASSWORD logstash_system = gCZjDK02ACG4Ucu7e3zf

Changed password for user beats_system
PASSWORD beats_system = 5vCtUrkP2sciLZHLwE3t

Changed password for user remote_monitoring_user
PASSWORD remote_monitoring_user = v1ZZYUbExYuXvQiozdRU

Changed password for user elastic
PASSWORD elastic = ybGj7NqxjETxQWklmpaV
```

Lưu lại password đã được tạo ngẫu nhiên ở trên

Bước 12: Kiểm tra quá trình cài đặt

curl -XGET https://localhost:9200 -u elastic:ybGj7NqxjETxQWklmpaV –k

ybGj7NqxjETxQWklmpaV*: đây là mật khẩu của elastic*

```
root@ubuntu-server:~# curl -XGET https://localhost:9200 -u elastic:ybGj7NqxjETxQWklmpaV -k
{
  "name" : "elasticsearch",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "I0VN41S2RDa1Ad9t1VBSRA",
  "version" : {
    "number" : "7.17.9",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "ef48222227ee6b9e70e502f0f0daa52435ee634d",
    "build_date" : "2023-01-31T05:34:43.305517834Z",
    "build_snapshot" : false,
    "lucene_version" : "8.11.1",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

Bước 13: Cài đặt khóa GPG

curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg

Bước 14: Thêm kho lưu trữ Wazuh

echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list

Bước 15: Cập nhật thông tin gói

sudo apt update

Bước 16: Cài đặt gói quản lý Wazuh

apt install wazuh-manager

Bước 17: Kích hoạt và bắt đầu dịch vụ quản lý Wazuh

systemctl daemon-reload

systemctl enable wazuh-manager.service

systemctl start wazuh-manager.service

```
root@ubuntu-server:~# systemctl daemon-reload
root@ubuntu-server:~# systemctl enable wazuh-manager.service
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-manager.service → /lib/syste
md/system/wazuh-manager.service.
root@ubuntu-server:~# systemctl start wazuh-manager.service
```

Bước 18: Kiểm tra trạng thái của Wazuh

systemctl status wazuh-manager

```
root@ubuntu-server:~# systemctl status wazuh-manager
● wazuh-manager.service - Wazuh manager
     Loaded: loaded (/lib/systemd/system/wazuh-manager.service; enabled; vendor>
     Active: active (running) since Thu 2024-09-12 23:56:00 +07; 28s ago
    Process: 93339 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (c>
      Tasks: 146 (limit: 2204)
     Memory: 750.4M
     CGroup: /system.slice/wazuh-manager.service
             ├─93413 /var/ossec/framework/python/bin/python3 /var/ossec/api/scr>
             ├─93453 /var/ossec/bin/wazuh-authd
             ├─93469 /var/ossec/bin/wazuh-db
             ├─93484 /var/ossec/framework/python/bin/python3 /var/ossec/api/scr>
             ├─93487 /var/ossec/framework/python/bin/python3 /var/ossec/api/scr>
             ├─93490 /var/ossec/framework/python/bin/python3 /var/ossec/api/scr>
             ├─93503 /var/ossec/bin/wazuh-execd
             ├─93517 /var/ossec/bin/wazuh-analysisd
             ├─93560 /var/ossec/bin/wazuh-syscheckd
             ├─93575 /var/ossec/bin/wazuh-remoted
             ├─93585 /var/ossec/bin/wazuh-logcollector
             ├─93626 /var/ossec/bin/wazuh-monitord
             └─93636 /var/ossec/bin/wazuh-modulesd
```

Bước 19: Cài đặt gói Filebeat

apt install filebeat=7.17.9

Bước 20: Tải cấu hình Filebeat

curl –so /etc/filebeat/filebeat.yml https://packages.wazuh.com/4.4/tpl/elastic-basic/filebeat_all_in_one.yml

Bước 21: Tải mẫu cảnh báo cho Elasticsearch và cấp quyền go+r cho /etc/filebeat/wazuh-template.json

curl -so /etc/filebeat/wazuh-template.json https://raw.githubusercontent.com/wazuh/wazuh/4.4/extensions/elasticsearch/7.x/wazuh-template.json

chmod go+r /etc/filebeat/wazuh-template.json

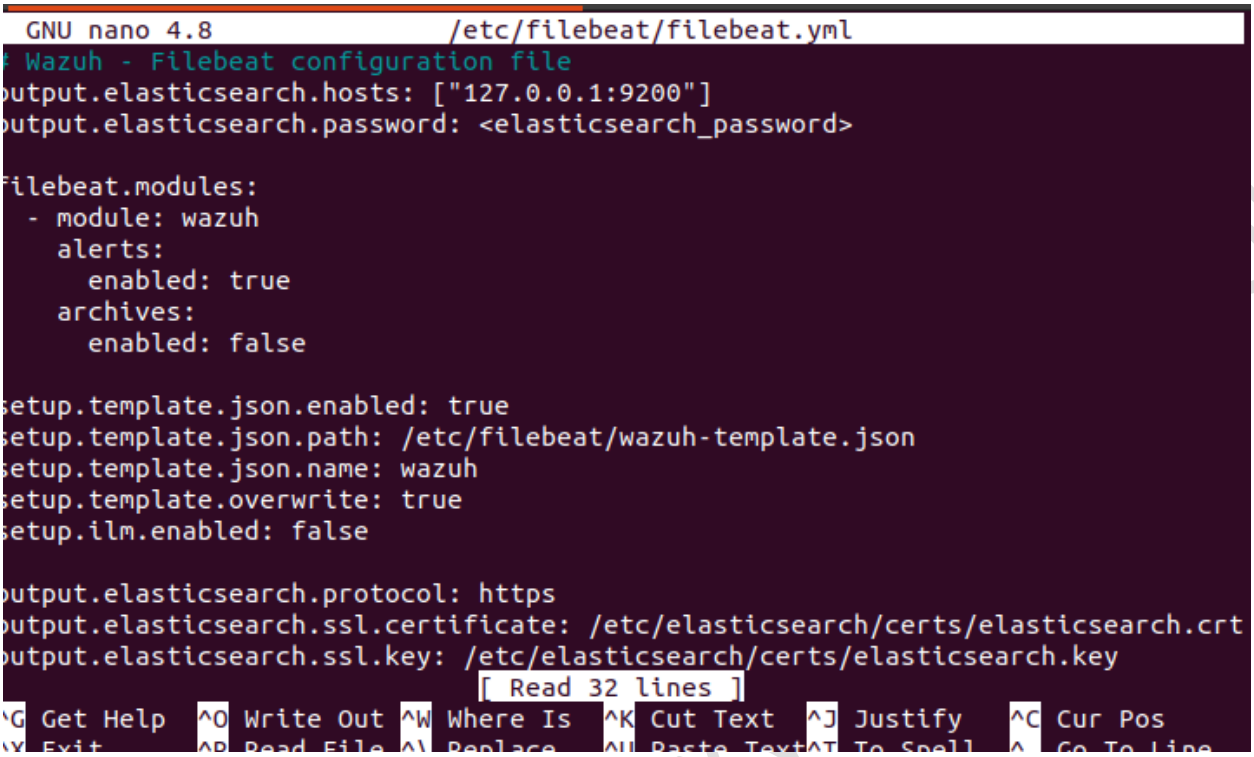
```
root@ubuntu-server:~# curl -so /etc/filebeat/wazuh-template.json https://raw.git
hubusercontent.com/wazuh/wazuh/4.4/extensions/elasticsearch/7.x/wazuh-template.j
son
root@ubuntu-server:~# chmod go+r /etc/filebeat/wazuh-template.json
```

Bước 22: Tải modun Wazuh cho filebeat

curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat-0.2.tar.gz | tar -xvz -C /usr/share/filebeat/module

Bước 23: Chỉnh sửa tệp /etc/filebeat/filebeat.yml

nano /etc/filebeat/filebeat.yml



Thay thế <elasticsearch_password> bằng mật khẩu của elastic đã tạo và lưu trước đó

Bước 24: Sao chép các chứng chỉ vào /etc/filebeat/certs/

cp -r /etc/elasticsearch/certs/ca/ /etc/filebeat/certs/

cp /etc/elasticsearch/certs/elasticsearch.crt /etc/filebeat/certs/filebeat.crt

cp /etc/elasticsearch/certs/elasticsearch.key /etc/filebeat/certs/filebeat.key

Bước 25: Kích hoạt và bắt đầu dịch vụ filebeat

systemctl daemon-reload

systemctl enable filebeat.service

systemctl start filebeat.service

Để đảm bảo dịch vụ filebeat đã được cài đặt thành công chúng ta chạy lệnh sau:

filebeat test output

```
root@ubuntu-server:~# filebeat test output
elasticsearch: https://127.0.0.1:9200...
  parse url... OK
  connection...
    parse host... OK
    dns lookup... OK
    addresses: 127.0.0.1
    dial up... OK
  TLS...
    security: server's certificate chain verification is enabled
    handshake... OK
    TLS version: TLSv1.3
    dial up... OK
  talk to server... OK
  version: 7.17.9
```

Bước 26: Cài đặt gói Kibana

apt install kibana=7.17.9

Bước 27: Sao chép các chứng chỉ Elasticsearch vào thư mục cấu hình kibana

mkdir /etc/kibana/certs/ca –p

cp -R /etc/elasticsearch/certs/ca/ /etc/kibana/certs/

cp /etc/elasticsearch/certs/elasticsearch.key /etc/kibana/certs/kibana.key

cp /etc/elasticsearch/certs/elasticsearch.crt /etc/kibana/certs/kibana.crt

chown -R kibana:kibana /etc/kibana/

chmod -R 500 /etc/kibana/certs/

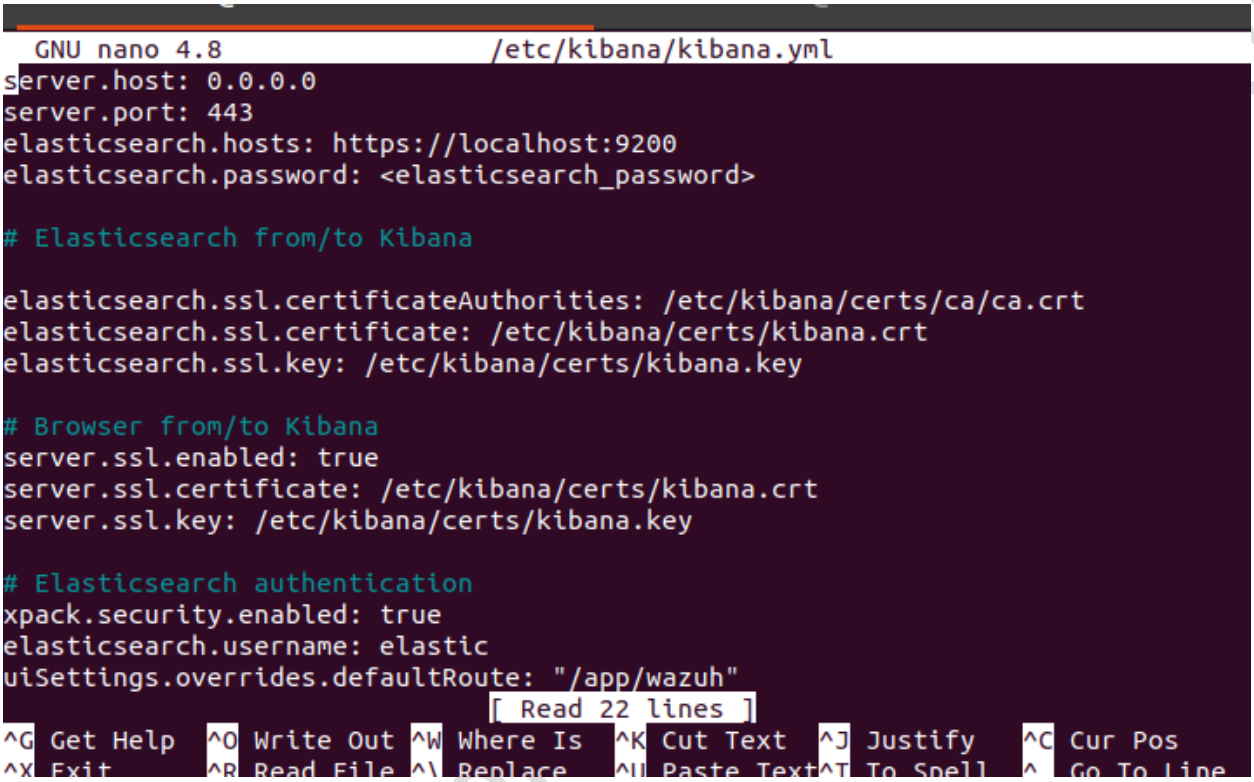
chmod 440 /etc/kibana/certs/ca/ca.* /etc/kibana/certs/kibana.*

Bước 28: Tải tệp cấu hình kibana

curl -so /etc/kibana/kibana.yml https://packages.wazuh.com/4.4/tpl/elastic-basic/kibana_all_in_one.yml

Bước 29: Chỉnh sửa tệp /etc/kibana/kibana.yml

nano /etc/kibana/kibana.yml



Tương tự, thay thế <elasticsearch_password> bằng mật khẩu của elastic đã tạo ngẫu nhiên và lưu trước đó

Bước 30: Tạo thư mục /usr/share/kibana/data

mkdir /usr/share/kibana/data

chown -R kibana:kibana /usr/share/kibana/

Bước 31: Cài đặt plugin Wazuh kibana

cd /usr/share/kibana/

sudo -u kibana /usr/share/kibana/bin/kibana-plugin install https://packages.wazuh.com/4.x/ui/kibana/wazuh_kibana-4.4.5_7.17.9-1.zip

```
root@ubuntu-server:~# cd /usr/share/kibana/
root@ubuntu-server:/usr/share/kibana# sudo -u kibana /usr/share/kibana/bin/kiban
a-plugin install https://packages.wazuh.com/4.x/ui/kibana/wazuh_kibana-4.4.5_7.1
7.9-1.zip
Attempting to transfer from https://packages.wazuh.com/4.x/ui/kibana/wazuh_kiban
a-4.4.5_7.17.9-1.zip
Transferring 36505918 bytes....................
Transfer complete
Retrieving metadata from plugin archive
Extracting plugin archive
Extraction complete
Plugin installation complete
```

Bước 32: Liên kết socket của kibana vào cổng đặc quyền 443

setcap 'cap_net_bind_service=+ep' /usr/share/kibana/node/bin/node

```
root@ubuntu-server:/usr/share/kibana# setcap 'cap_net_bind_service=+ep' /usr/sha
re/kibana/node/bin/node
root@ubuntu-server:/usr/share/kibana#
```

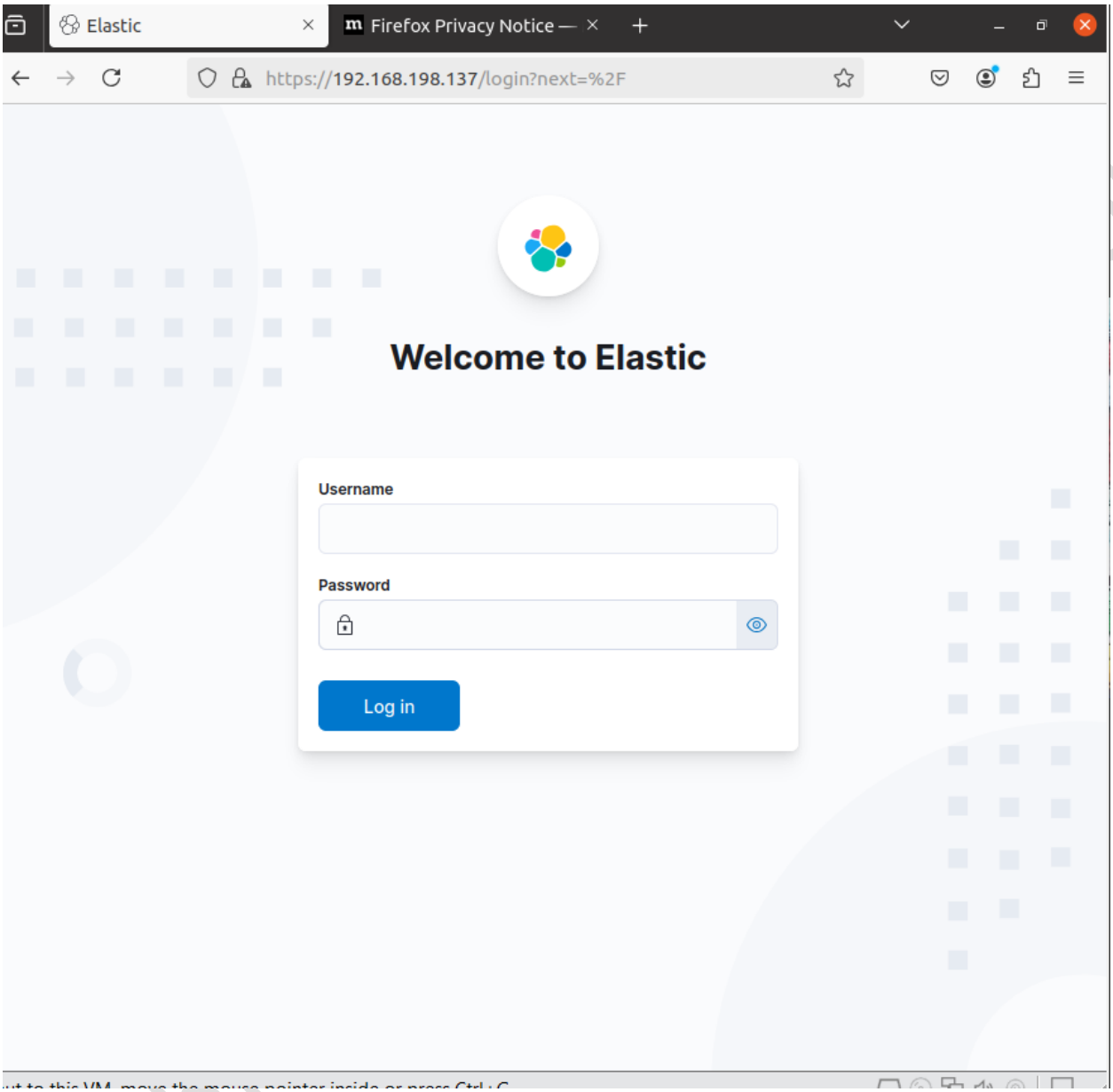
Bước 33: Kích hoạt và bắt đầu dịch vụ kibana

systemctl daemon-reload

systemctl enable kibana.service

systemctl start kibana.service

Bước 34: Truy cập vào giao diện web của Wazuh



Username: elastic

Password: *đã tạo và lưu trước đó*