**Report ELK**

Elastic Stack, trước đây được gọi là ELK, bao gồm bốn thành phần tích hợp:

• Elasticsearch, công cụ tìm kiếm và nền tảng phân tích

• Logstash, kênh xử lý dữ liệu

• Kibana, công cụ trực quan hóa dữ liệu

• Beats, một tích hợp gần đây

**1-Elasticsearch**

1. What is Elasticsearch?

- Elasticsearch là công cụ tìm kiếm và phân tích phân tán nằm ở trung tâm của Elastic Stack.

- Elasticsearch là nơi diễn ra phép thuật lập chỉ mục, tìm kiếm và phân tích.

- Elasticsearch cung cấp tìm kiếm và phân tích gần như theo thời gian thực cho mọi loại dữ liệu.

2. Install and config

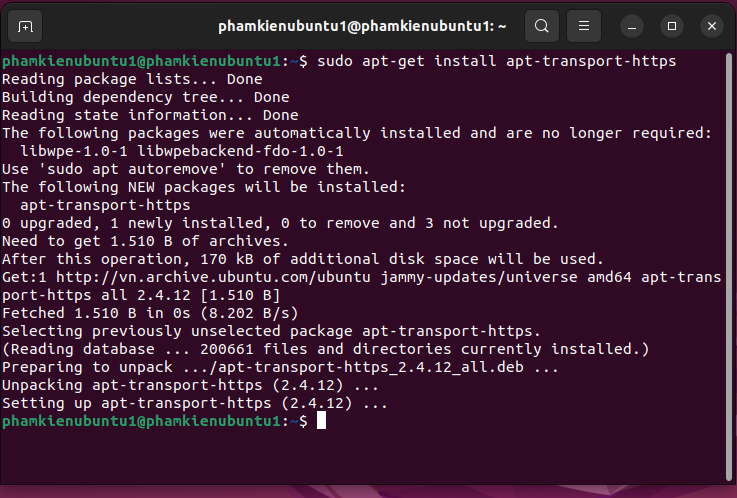
-Import the Elasticsearch PGP Key

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

-From APT repository

* install the apt-transport-https package on Debian before proceeding:

**sudo apt-get install apt-transport-https**

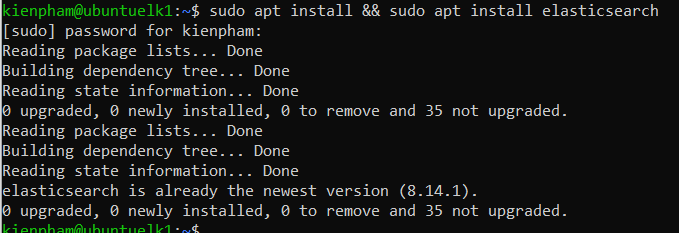


* Save the repository definition to /etc/apt/sources.list.d/elastic-8.x.list:

**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**

* Install ElasticSearch

**sudo apt install && sudo apt install elasticsearch**

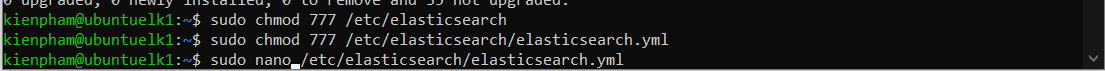


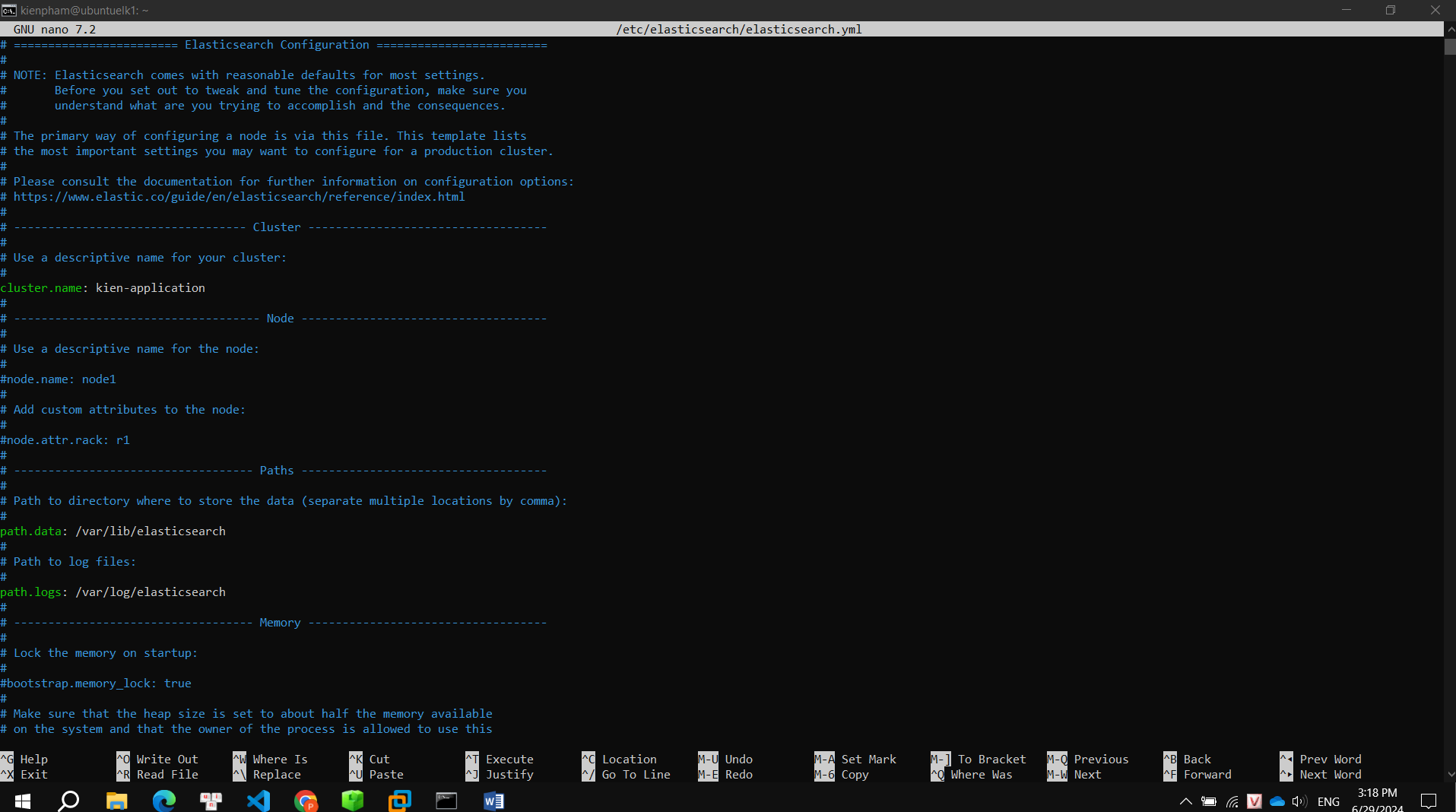
* Config file elasticsearch.yml

**sudo chmod 777 /etc/elasticsearch/**

**sudo chmod 777 /etc/elasticsearch/elasticsearch.yml**

**sudo nano /etc/elasticsearch/elasticsearch.yml**

****

****

Config: network.host:0.0.0.0

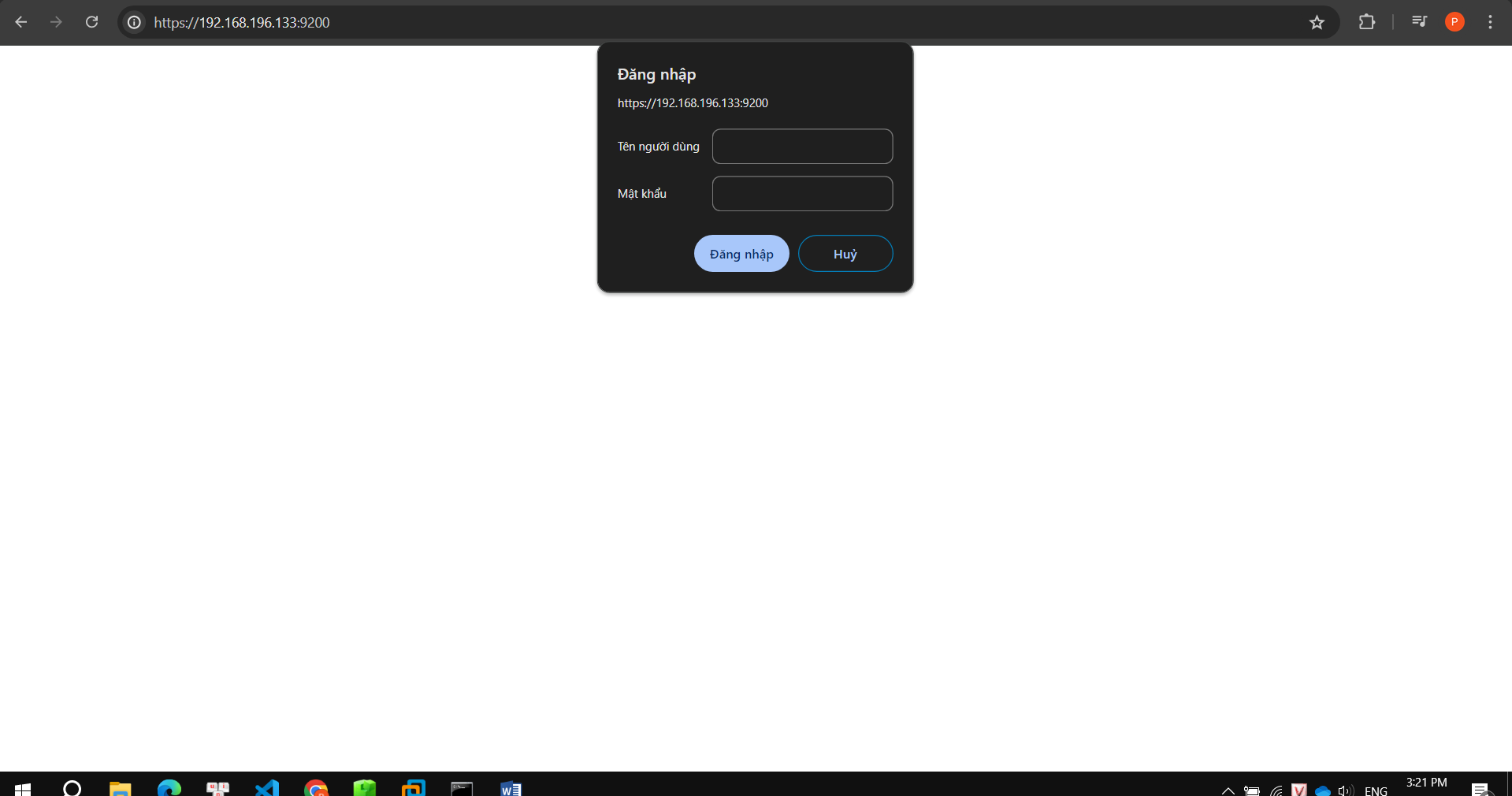
http.port:9200

sudo systemctl start elasticsearch

sudo systemctl enable elasticsearch

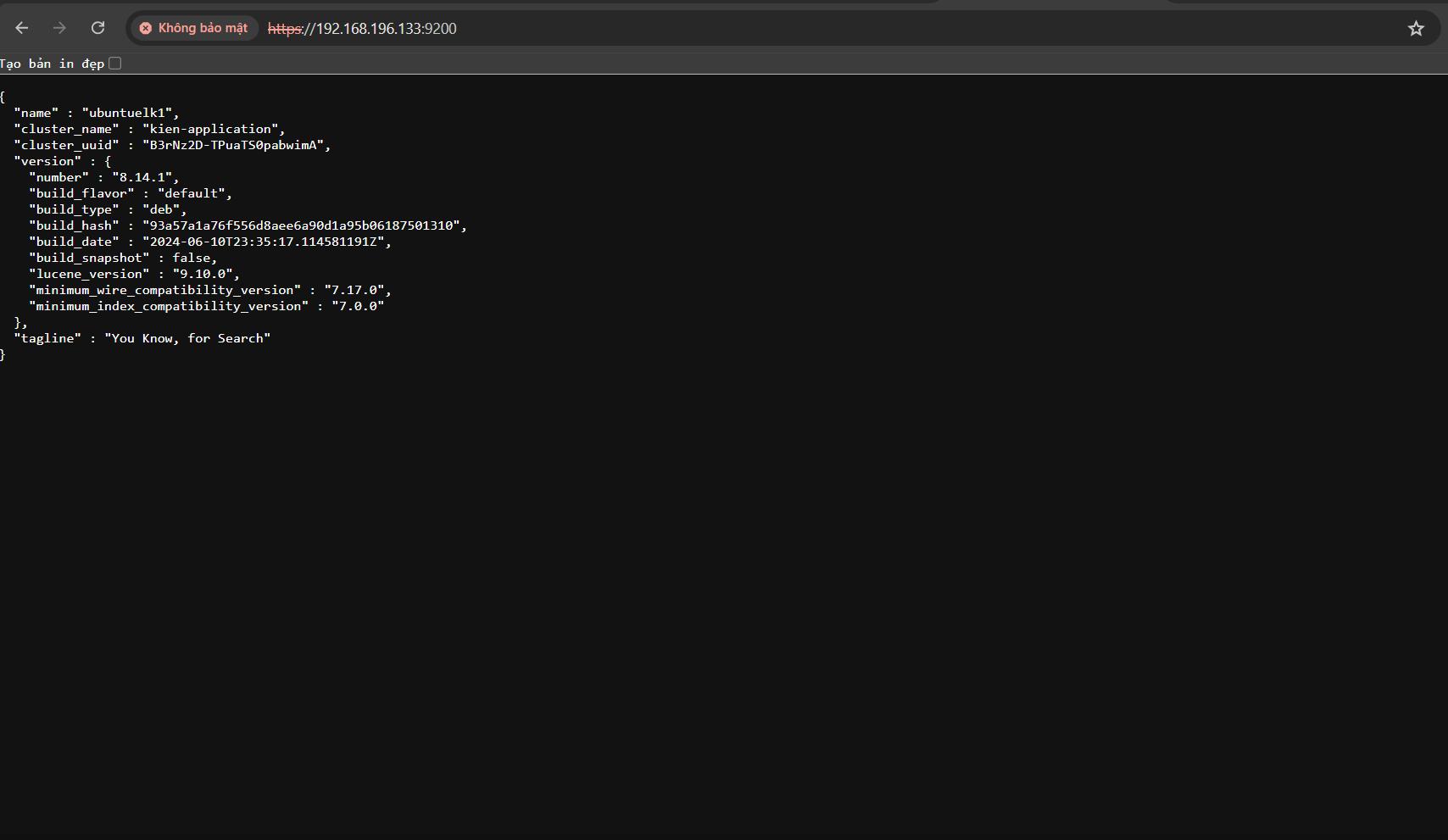
sudo systemctl status elasticsearch ( kiểm tra dịch vụ elasticsearch đã chạy chưa)

Truy cập https://<địa chỉ máy cài elk>:9200



Cài đặt lại user và password

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

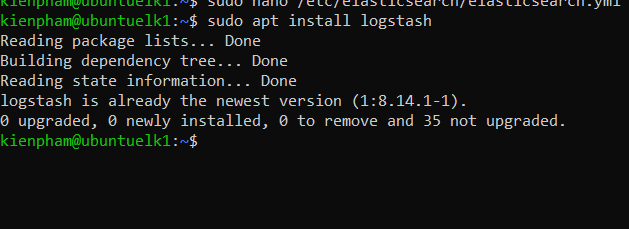


**Done config Elasticsearch**

**2-Logstash**

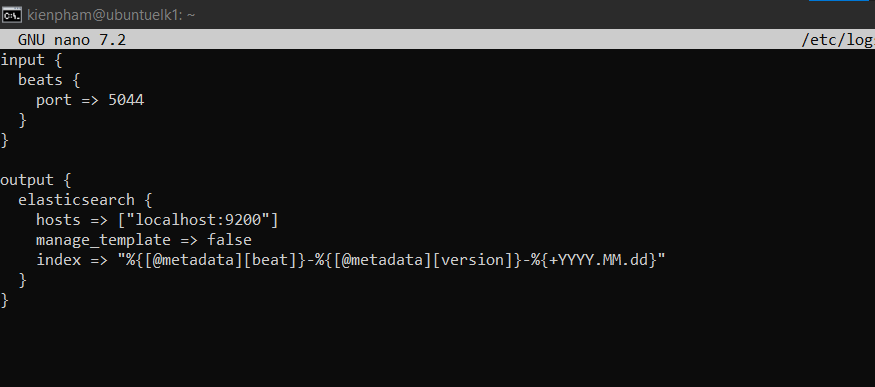
* Install Logstash

**sudo apt install logstash**

****

* Create file config for Logstash

**nano /etc/logstash/conf.d/01-logstash.conf**

****

* Khởi động và kiểm tra dịch vụ

sudo systemctl enable logstash

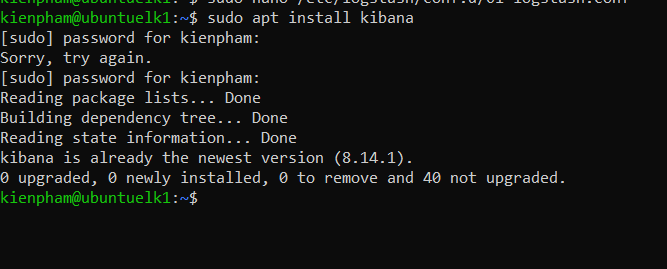
sudo systemctl start logstash

sudo systemctl status logstash

**Done config Logstash**

**3-Kibana**

* Install Kibana

****

* Config file kiban.yml

**sudo chmod 777 /etc/kibana**

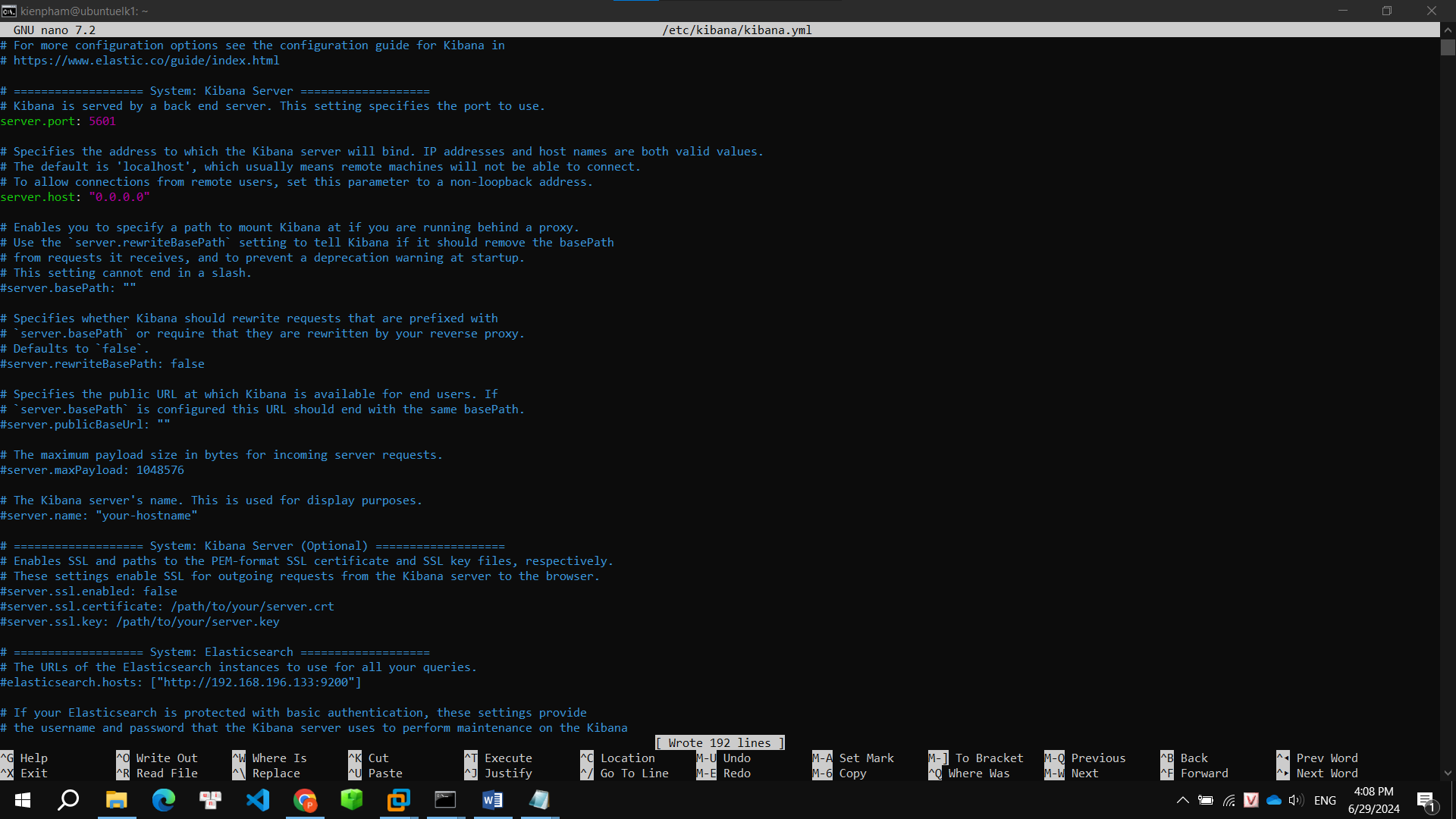
**sudo chmod 777 /etc/kibana/kibana.yml**

**sudo nano /etc/kiban/kibana.yml**

Config:

sever.port:5601

sever.host:0.0.0.0

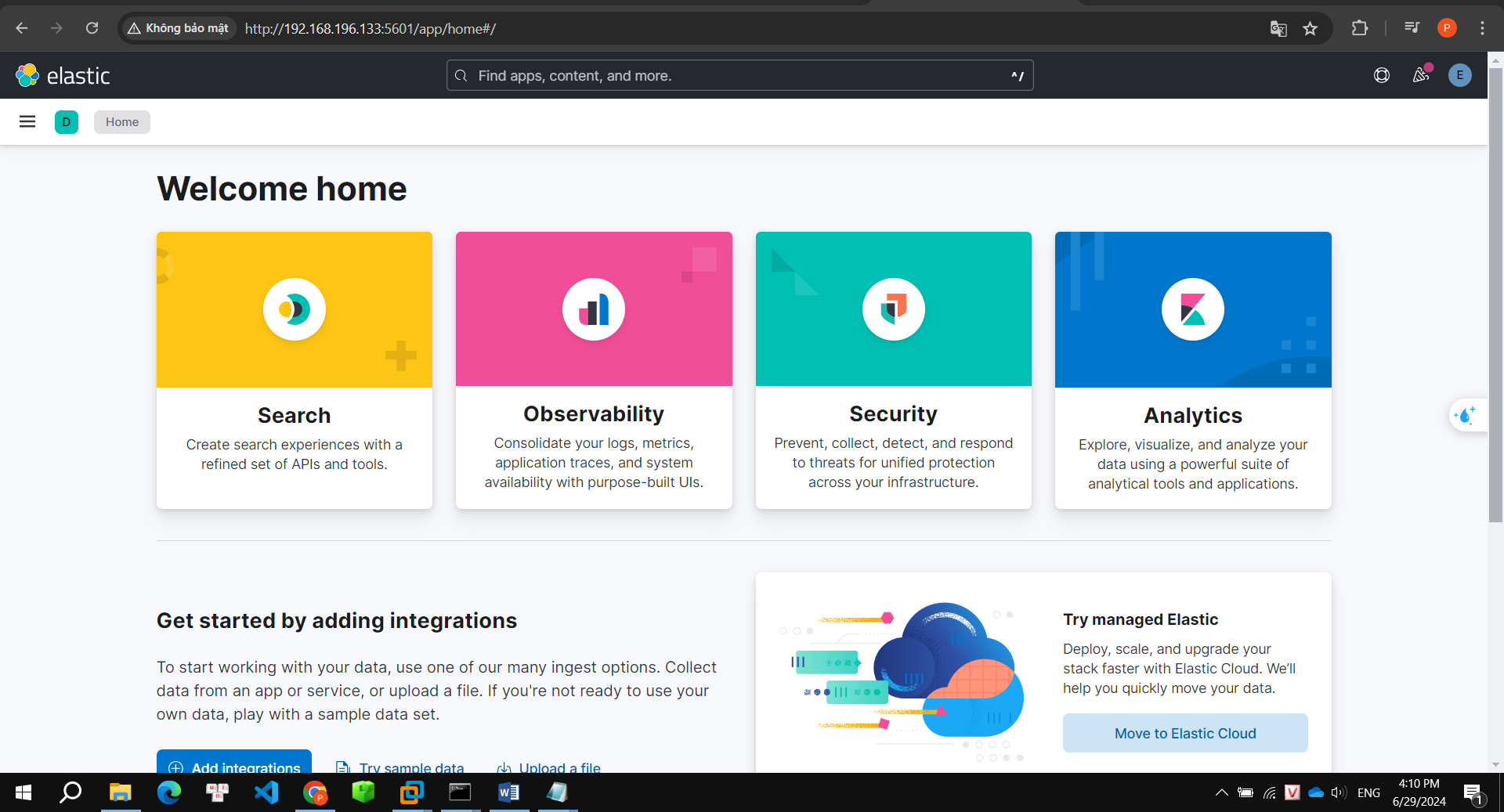


sudo systemctl start kibana

sudo systemctl enable kibana

Truy cập: http://<địa chỉ máy elk>:5601

Sử dụng user và password ở elasticsearch



**4-Filebeat in other Server**

* Install

-Import the Elasticsearch PGP Key

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

-From APT repository

install the apt-transport-https package on Debian before proceeding:

**sudo apt-get install apt-transport-https**

**-**Save the repository definition to /etc/apt/sources.list.d/elastic-8.x.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**

-install

**sudo apt install filebeat**

* Config

sudo nano /etc/filebeat/filebeat.yml

Thay đổi all enable false thành enable true

Output.elasticsearch

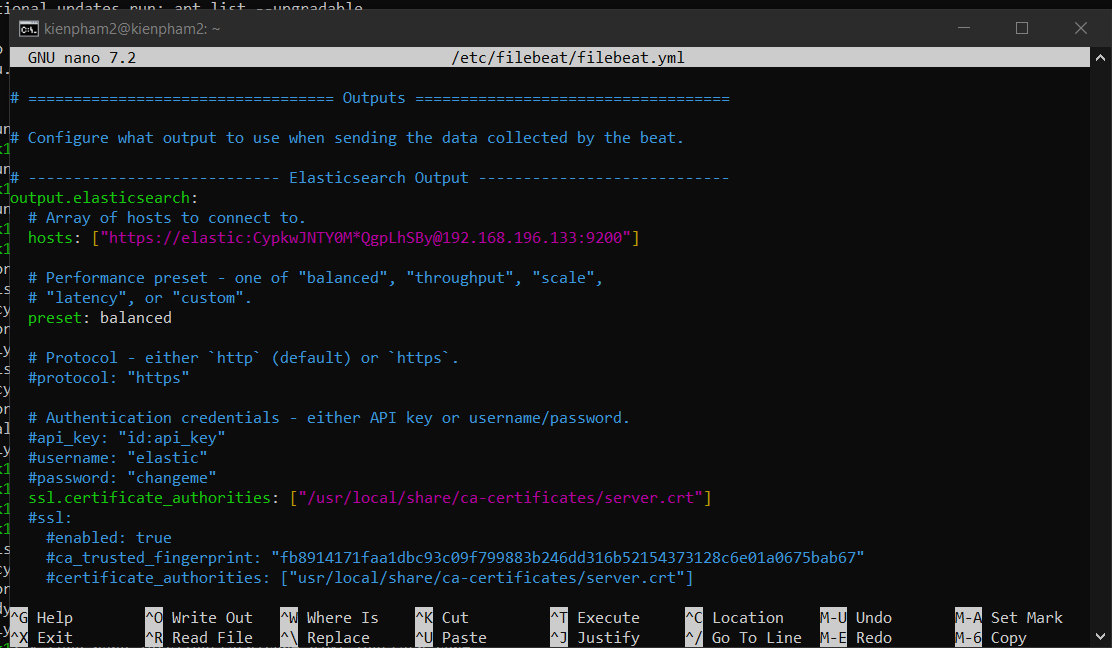
Host:[“https://user:pass@<địa chỉ máy server filebeat>:9200]

ssl.certificate\_authorities: ["/usr/local/share/ca-certificates/server.crt"]

* Lấy cert của filebeat

openssl s\_client -connect 192.168.196.133:9200 -showcerts </dev/null 2>/dev/null | sed -n '/BEGIN CERTIFICATE/,/END CERTIFICATE/p' > server.crt

sudo cp server.crt /usr/local/share/ca-certificates/



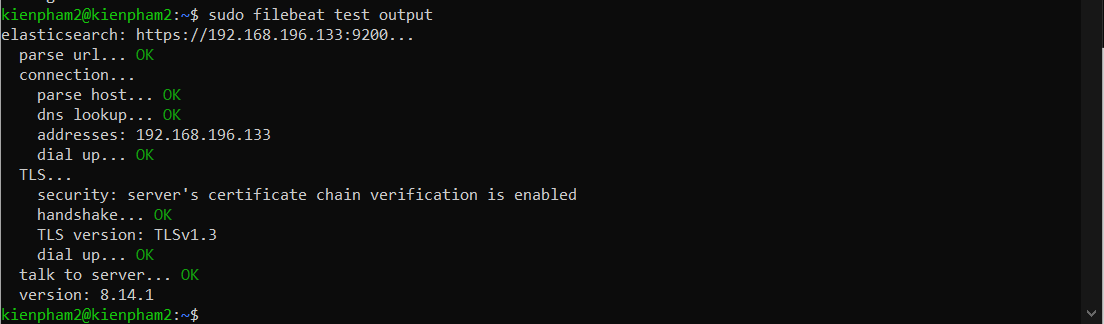
* Test config

sudo filebeat test config



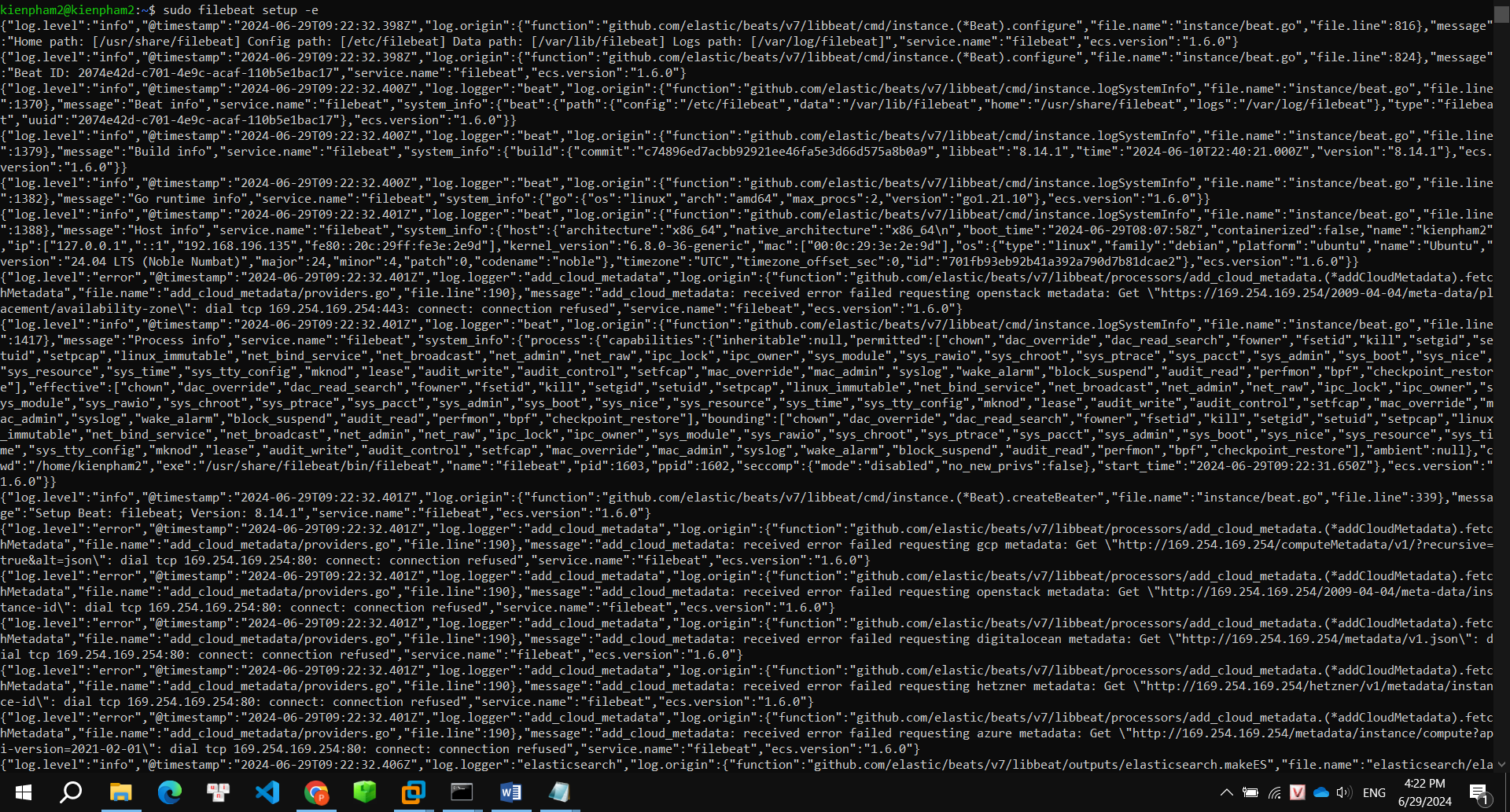
* Test output

sudo filebeat test output



* Đẩy log của sever filebeat lên kibana

sudo filebeat setup –e



Truy cập kibana để xem log

