**DỰ ÁN CÁ NHÂN**

**Xây dựng hệ thống giám sát mạng sử dụng mã nguồn mở Wazuh**

1. **Kế hoạch và cài đặt Wazuh**

**Người thực hiện**

***Nguyễn Ngọc Anh***

***Email:*** [***ngocanhnguyen99.xyz@gmail.com***](mailto:ngocanhnguyen99.xyz@gmail.com)

***Phone: 0865448485***

Mục lục

[**I)** **Kế hoạch dự án** 4](#_Toc177132210)

[**Mục Tiêu:** 4](#_Toc177132211)

[**Yêu cầu hệ thống:** 4](#_Toc177132212)

[**Thiết Kế:** 4](#_Toc177132213)

[**1.1** **Mô tả** 5](#_Toc177132214)

[**1.2** **Chuẩn bị** 6](#_Toc177132215)

[**II)** **Set up và cấu hình Wazuh** 6](#_Toc177132216)

[**2.1 Cài đặt Wazuh Server trên Ubuntu Sever** 6](#_Toc177132217)

[**2.2** **Triển khai giám sát các Agent** 18](#_Toc177132218)

[**2.2.1 Đầu tiên, đối với Ubuntu Agent:** 18](#_Toc177132219)

[**2.2.2 Tiếp theo, với máy Agent Windows Server 2012:** 19](#_Toc177132220)

1. **Kế hoạch dự án**

## Mục Tiêu:

Xây dựng hệ thống giám sát bảo đảm an toàn hệ thống mạng cho công ty, doanh nghiệp, trường học,… với mã nguồn mở Wazuh với các chức năng chính như sau:

Giám sát và phát hiện sự cố

Ngăn chặn IP độc hại

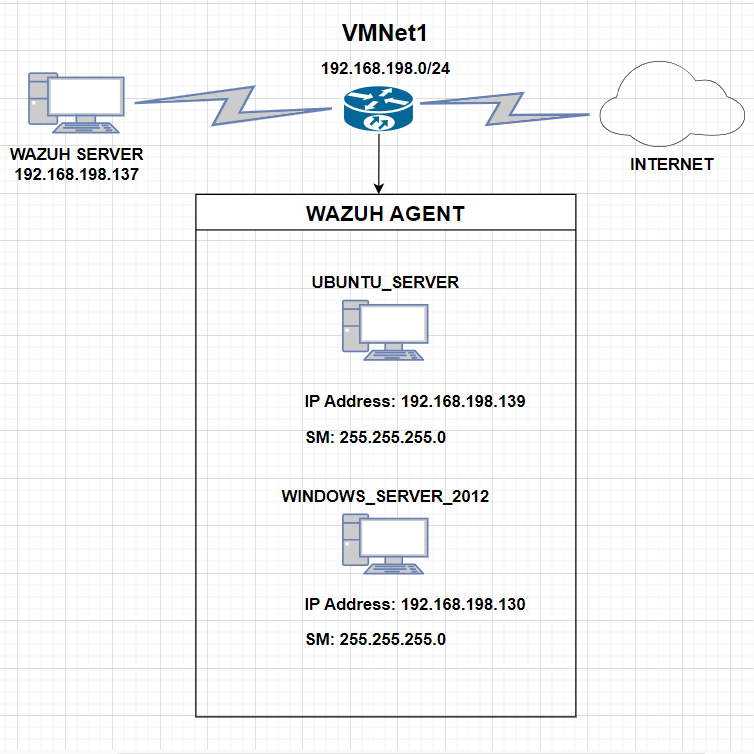
Quản lý tập tin và tích hợp

**Yêu cầu hệ thống:**

* + Cấu hình chặn địa chỉ IP độc hại truy cập đến Web Server
  + Giám sát tính toàn vẹn file(FIM) trên Wazuh
  + Phát hiện cuộc tấn công Brute-force trên Wazuh
  + Giám sát các sự kiên Docker
  + Phát hiện các tiến trình không được ủy quyền
  + Phát hiện các cuộc tấn công SQL Injection
  + Phát hiện các tệp nhị phân đáng ngờ trên Endpoint
  + Tích hợp VirusTotal và Wazuh để phát hiện và xóa các phần mềm độc hại
  + Tích hợp Yara và Wazuh để phát hiện phần mềm độc hại
  + Phát hiện lỗ hổng
  + Phát hiện tiến trình ẩn trên Ubuntu endpoint
  + Giám sát việc thực thi các lệnh độc hại trên Wazuh
  + Phát hiện tấn công Shellshock

## Thiết Kế:

Sơ đồ kiến trúc hệ thống mạng



* 1. **Mô tả**

**Wazuh** là một nền tảng giám sát bảo mật mã nguồn mở, cung cấp các tính năng như phát hiện mối đe dọa, giám sát tính toàn vẹn, phản ứng sự cố và quản lý tuân thủ. Nó thường được sử dụng để theo dõi các sự kiện bảo mật trong mạng, phát hiện xâm nhập và duy trì tính toàn vẹn của hệ thống bằng cách theo dõi liên tục các thay đổi trong cơ sở hạ tầng. Dưới đây là một số tính năng chính của Wazuh:

1. Quản lý thông tin và sự kiện bảo mật (SIEM): Wazuh tích hợp với hệ thống SIEM để thu thập, phân tích và cảnh

2. Phát hiện mối đe dọa: Giúp phát hiện các cuộc tấn công và hoạt động đáng ngờ trong hệ thống của bạn.

3. Giám sát tính toàn vẹn: Theo dõi các thay đổi trong tập tin và thư mục, phát hiện các thay đổi trái phép.

4. Quản lý tuân thủ: Wazuh cung cấp các công cụ để đảm bảo hệ thống của bạn tuân thủ các tiêu chuẩn bảo mật và quy định như PCI DSS, HIPAA, GDPR,...

5. Phản ứng sự cố: Khi phát hiện sự cố bảo mật, Wazuh cung cấp các cảnh báo và có khả năng kích hoạt các hành động tự động để khắc phục hoặc giảm thiểu rủi ro.

Wazuh có thể được triển khai trên nhiều hệ thống khác nhau, từ các máy chủ vật lý, máy ảo đến các nền tảng đám mây.

* 1. **Chuẩn bị**
  + 01 máy ảo hệ điều hành Windows Server 2012:

[**https://www.microsoft.com/en-us/evalcenter/download-windows-server-2012-r2**](https://www.microsoft.com/en-us/evalcenter/download-windows-server-2012-r2)

* + 02 máy ảo hệ điều hành Ubuntu Server 20.04.6 : 1 máy Ubuntu Server chạy Wazuh Agent (có nghĩa là máy chủ này được giám sát bởi 1 máy chủ có Wazuh Server), 1 máy Ubuntu Server chạy Wazuh Sever (là máy giám sát máy chủ Ubuntu Server có Wazuh Agent)

[**https://releases.ubuntu.com/focal/**](https://releases.ubuntu.com/focal/)

hoặc tải bản mới nhất nếu máy bạn mạnh [**https://ubuntu.com/download/server**](https://ubuntu.com/download/server)

* + 3 máy đều chung card mạng NAT

1. **Set up và cấu hình Wazuh**

Để cài đặt Wazuh trên Ubuntu, cần làm theo các bước dưới đây. Quá trình này sẽ bao gồm việc cài đặt thành phần Wazuh Server và Wazuh Agent. Dưới đây là hướng dẫn từng bước để cài đặt Wazuh trên Ubuntu.

## 2.1 Cài đặt Wazuh Server trên Ubuntu Sever

**Bước 1: Cập nhật hệ thống**

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

sudo apt update

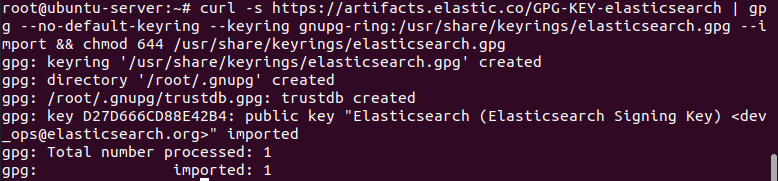
sudo apt upgrade –y

**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 Ubuntu Server và Agent)*

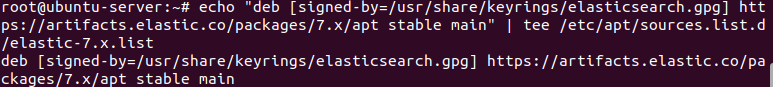
**Bước 3: Cài đặt khóa GPG** (GNU Privacy Guard: là một loại khóa mã hóa được sử dụng trong hệ thống mã hóa **GPG**, một phần mềm mã nguồn mở dùng để mã hóa và xác thực dữ liệu. GPG hỗ trợ cả mã hóa **symmetric** (mã hóa đối xứng) và **asymmetric** (mã hóa bất đối xứng), trong đó mã hóa bất đối xứng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

**

**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

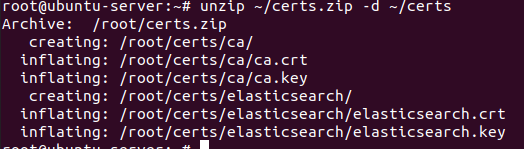
Bước 7: Tạo các chứng chỉ (cert)

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

**

**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

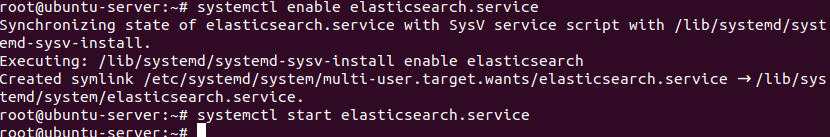
**Bước 10: Kích hoạt và bắt đầu dịch vụ Elasticsearch**

systemctl daemon-reload

systemctl enable elasticsearch.service

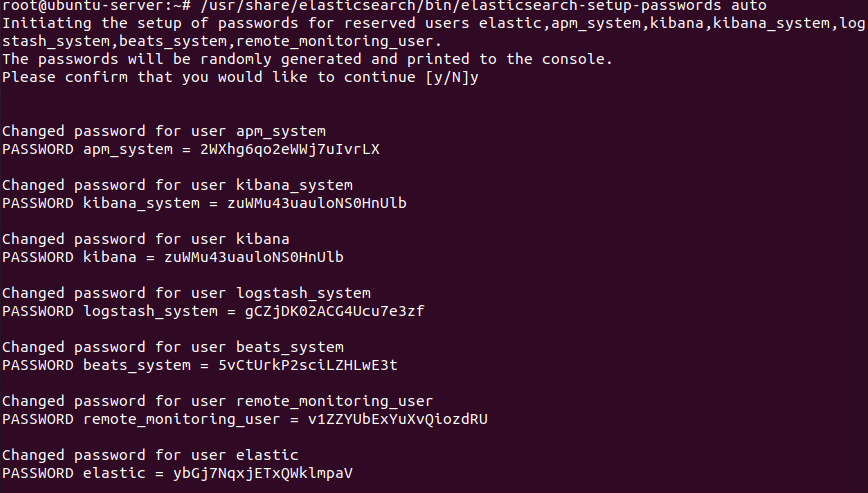
systemctl start elasticsearch.service

**

**

**Bước 11: Tạo thông tin xác thực**

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

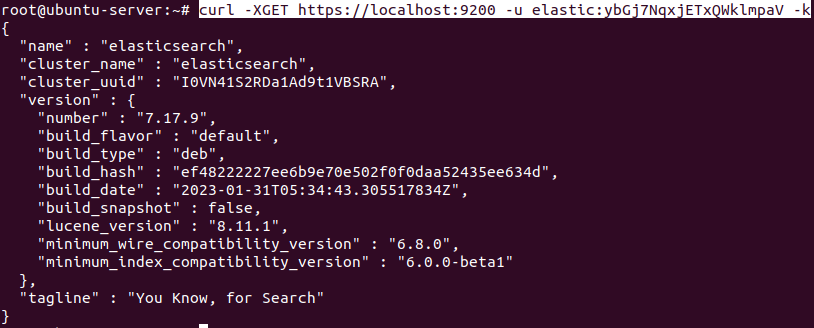
****

**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*

****

**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**

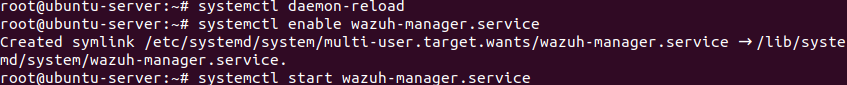
apt install wazuh-manager

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

systemctl daemon-reload

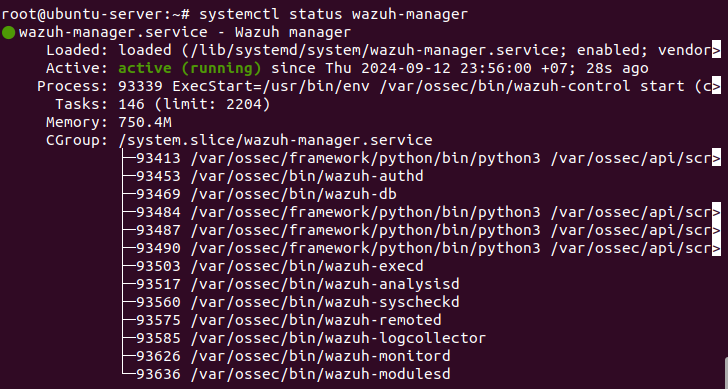
systemctl enable wazuh-manager.service

systemctl start wazuh-manager.service

**

**Bước 18: Kiểm tra trạng thái của Wazuh**

systemctl status wazuh-manager

**

**Bước 19: Cài đặt gói Filebeat**

apt install filebeat=7.17.9

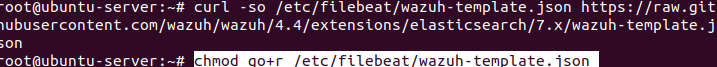
**Bước 20: Tải cấu hình Filebeat**

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**

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

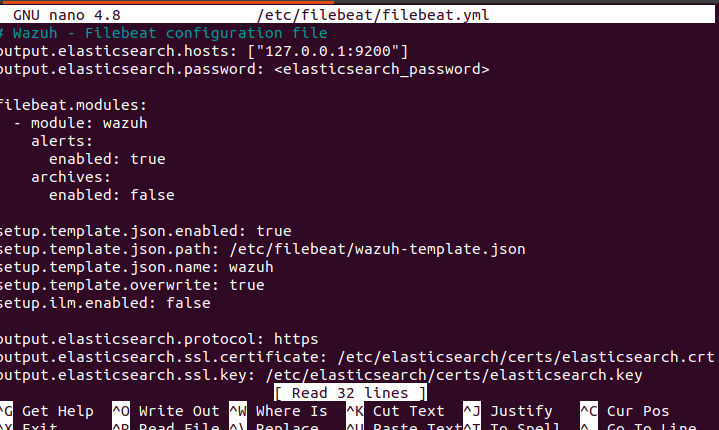


**Bước 22: Tải modun Wazuh cho filebeat**

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 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**

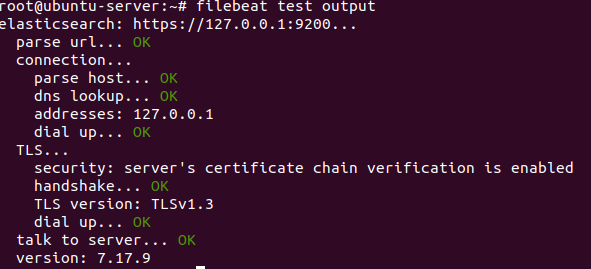
systemctl daemon-reload

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



**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/

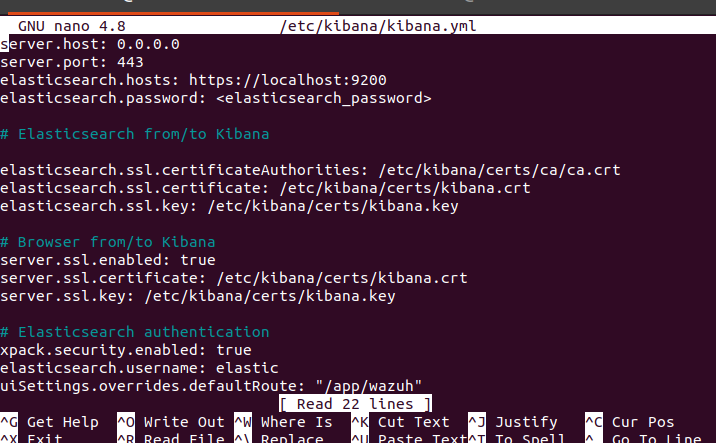
chmod 440 /etc/kibana/certs/ca/ca.\* /etc/kibana/certs/kibana.\*

**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 elastic đã tạo ngẫu nhiên và lưu trước đó**

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

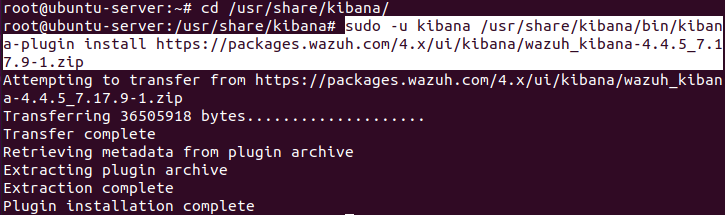
mkdir /usr/share/kibana/data

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



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

setcap 'cap\_net\_bind\_service=+ep' /usr/share/kibana/node/bin/node



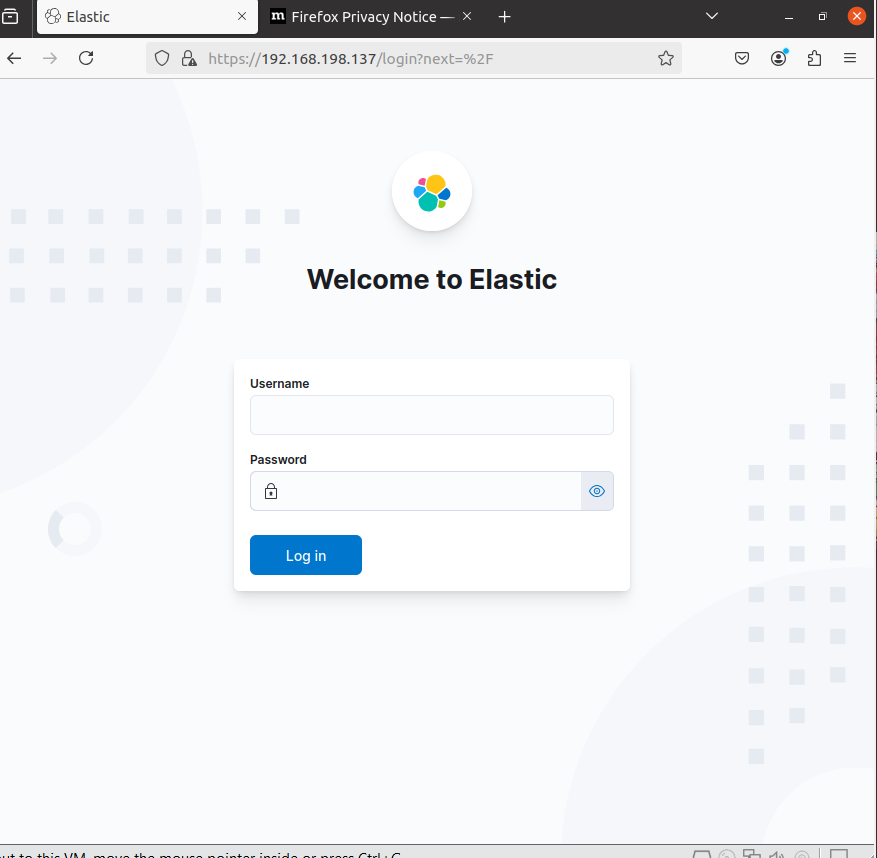
**Bước 33: Kích hoạt và bắt đầu dịch vụ kibana**

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*

* 1. **Triển khai giám sát các Agent**

### 2.2.1 Đầu tiên, đối với Ubuntu Agent:

**Bước 1: Import 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 2: Thêm kho lưu trữ**

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 3: Cập nhật các thông tin gói**

apt update

**Bước 4: Triển khai wazuh agent**

WAZUH\_MANAGER=192.168.198.137 apt install wazuh-agent

192.168.198.137: Địa chỉ của ubuntu server

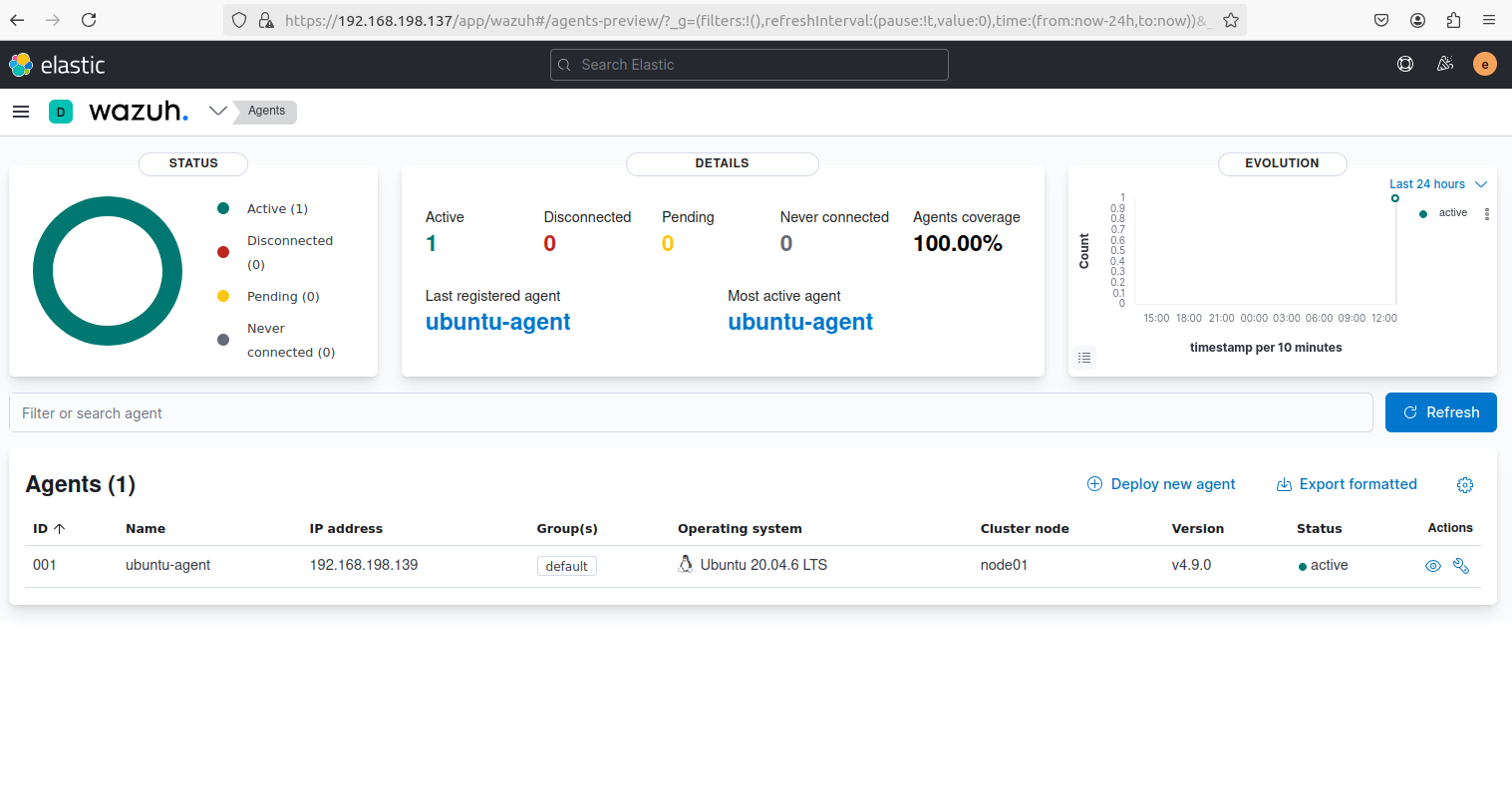
**Bước 5: Kích hoạt và bắt đầu dịch vụ wazuh agent**

systemctl daemon-reload

systemctl enable wazuh-agent.service

systemctl start wazuh-agent.service

Kiểm tra: Ta đã thành công kết nối giám sát với máy ubuntu-agent

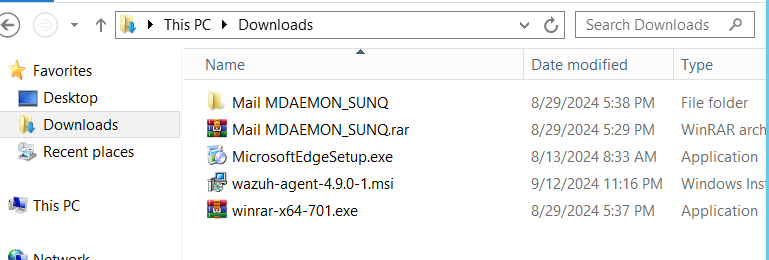


**2.2.2 Tiếp theo, với máy Agent Windows Server 2012:**

Ta sẽ vào trang chủ của Wazuh để tải về phần mềm quản lý Wazuh Agent

Link: <https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-windows.html>

**Bước 1: Download Wazuh Agent lưu ở thư mục download**



**Bước 2: Triển khai Wazuh Agent**

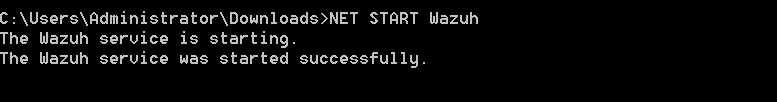
cd Downloads

wazuh-agent-4.9.0-1.msi /q WAZUH\_MANAGER=192.168.198.137

192.168.198.137: Địa chỉ của ubuntu server

**Bước 3: Bắt đầu chạy Wazuh Agent**

NET START Wazuh



Kiểm tra: thành công kết nối giám sát máy Windows Server Agent

