ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

NT132 - QUẢN TRỊ MẠNG VÀ HỆ THỐNG

TÊN ĐỀ TÀI: WAZUH MONITORING

NGUYỄN TẤN GIA QUỐC - 23521308
NGUYỄN NHẤT DƯƠNG - 23520353

TP. HỒ CHÍ MINH, NĂM 2025

Mục lục

Danh sách hình ảnh

Tổng quan

1.1 Định nghĩa / Giới thiệu

Wazuh là một nền tảng *mã nguồn mở (open-source)* dùng để **giám sát an ninh, phát hiện xâm nhập (IDS/IPS)** và **quản lý thông tin – sự kiện an ninh (SIEM – Security Information and Event Management)**.

Nó giúp quản trị viên mạng **phát hiện, phân tích và phản ứng kịp thời** với các hành vi bất thường trong hệ thống, đồng thời hỗ trợ **kiểm tra tuân thủ (compliance)** theo các tiêu chuẩn bảo mật như PCI DSS, GDPR, HIPAA hay CIS.

Wazuh được phát triển dựa trên dự án **OSSEC**, nhưng được mở rộng với nhiều cải tiến mạnh mẽ hơn về khả năng trực quan hóa dữ liệu, mở rộng quy mô và quản lý tập trung. Nền tảng này thường được tích hợp với **Elastic Stack (Elasticsearch, Logstash, Kibana)** để cung cấp **giao diện giám sát trực quan và phân tích sâu dữ liệu an ninh**.

Mục tiêu của Wazuh

- Phát hiện tấn công và hành vi bất thường trong hệ thống.
- Giám sát tính toàn vẹn của tệp tin, phát hiện thay đổi trái phép.
- Cung cấp báo cáo tuân thủ an toàn thông tin theo các chuẩn quốc tế.
- Phản ứng tự động với sự kiện an ninh (ví dụ: chặn IP, dừng tiến trình, gửi cảnh báo).

Nhờ khả năng hoạt động linh hoạt trên nhiều nền tảng như **Windows, Linux, macOS, container (Docker, Kubernetes)**, Wazuh được sử dụng rộng rãi trong doanh nghiệp, tổ chức chính phủ và môi trường học thuật.

1.2 Thành phần

Một hệ thống Wazuh hoàn chỉnh gồm ba thành phần chính: **Wazuh Manager**, **Wazuh Agent**, và **Wazuh Dashboard (UI)**.

1.2.1 Wazuh Manager

Đây là **trung tâm xử lý dữ liệu** của toàn hệ thống. Manager nhận log từ các agent, giải mã – phân tích – đối chiếu quy tắc (*rules*) và tạo cảnh báo khi phát hiện bất thường.

Các chức năng chính:

- Xử lý và lưu trữ dữ liệu log gửi từ agent.
- So khớp các sự kiện với tập quy tắc (ruleset) tích hợp sẵn hoặc do người quản trị tùy chỉnh.
- Quản lý danh sách agent, gửi cấu hình và lệnh điều khiển.
- Tích hợp với **Elasticsearch** để lưu trữ dữ liệu và truy vấn nhanh.

1.2.2 Wazuh Agent

Agent là **thành phần được cài trên các máy bị giám sát** (endpoint). Nó thu thập dữ liệu về:

- Nhật ký hệ thống (system logs).
- Tình trạng tiến trình, registry, hoạt động mạng.
- Thay đổi tệp tin quan trọng (file integrity monitoring).
- Cấu hình bảo mật của hệ điều hành.

Dữ liệu sau đó được mã hóa và gửi về Wazuh Manager thông qua giao thức TCP/UDP an toàn.

1.2.3 Wazuh Dashboard

Dashboard cung cấp **giao diện trực quan** giúp người quản trị theo dõi tình hình an ninh của toàn hệ thống.

Các tính năng nổi bật:

- Biểu đồ thống kê và hiển thị log theo thời gian thực.

- Xem chi tiết từng cảnh báo, mức độ rủi ro (low – medium – high – critical).
- Quản lý agent, người dùng, rule và cấu hình hệ thống.
- Hỗ trợ tìm kiếm và lọc dữ liệu bằng câu lệnh Elasticsearch Query DSL.

Ngoài ra, hệ thống có thể tích hợp thêm:

- **Filebeat / Logstash** để truyền dữ liệu log đến Elasticsearch.
- **Elasticsearch** để lưu trữ, phân tích log và cảnh báo.
- **Alerting module** để gửi cảnh báo qua email, Slack, webhook, v.v.

1.3 Hoạt động

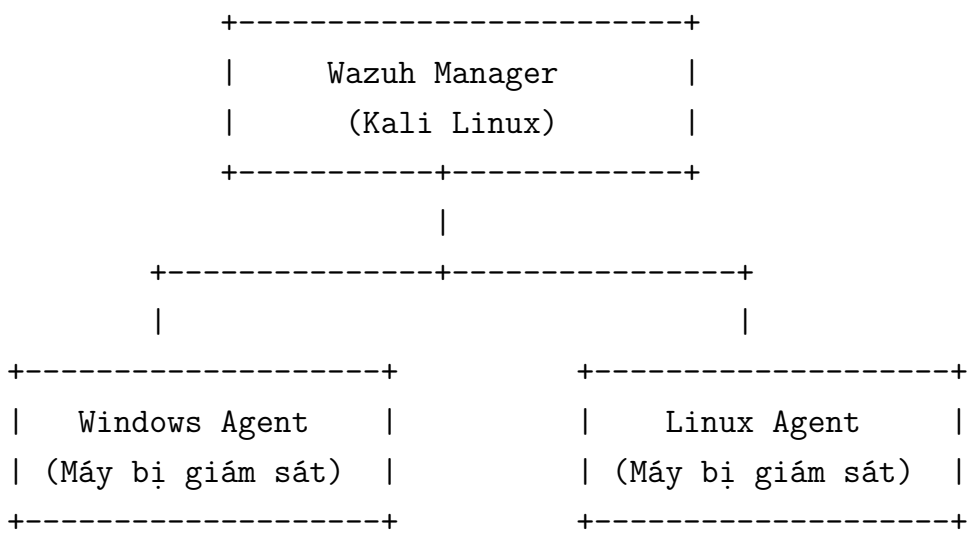
Cơ chế hoạt động của Wazuh có thể mô tả theo chu trình sau:

1. **Thu thập dữ liệu (Data Collection):** Wazuh Agent thu thập log, trạng thái hệ thống, thay đổi file, tiến trình đang chạy, v.v.
2. **Gửi dữ liệu (Data Transmission):** Dữ liệu được mã hóa và gửi về Wazuh Manager thông qua cổng 1514 (TCP hoặc UDP).
3. **Phân tích dữ liệu (Data Analysis):** Manager phân tích log dựa trên tập quy tắc (ruleset). Nếu phát hiện hành vi đáng ngờ như brute-force, thay đổi file hệ thống, kết nối trái phép,… thì tạo ra cảnh báo.
4. **Lưu trữ và hiển thị (Storage & Visualization):** Dữ liệu và cảnh báo được lưu vào Elasticsearch. Dashboard hiển thị kết quả trực quan giúp người quản trị dễ dàng nhận biết tình trạng an ninh hiện tại.
5. **Phản ứng (Response):** Hệ thống có thể thực hiện hành động tự động như khóa tài khoản, chặn IP, hoặc gửi thông báo khi phát hiện sự cố.

Triển khai

2.1 Mô hình

Mô hình triển khai Wazuh trong đồ án môn học được minh họa như sau:



Giải thích mô hình:

- **Máy chủ (Wazuh Manager):** Cài đặt Wazuh Manager, Elasticsearch và Dashboard. Dùng để quản lý và phân tích log.
- **Máy bị giám sát (Agents):** Hai máy ảo Windows và Linux, có cài đặt Wazuh Agent để gửi dữ liệu log về server.
- Các máy ảo kết nối qua cùng mạng **VMnet (NAT)** để đảm bảo liên lạc nội bộ.

2.2 Cài đặt

2.2.1 Bước 1. Chuẩn bị

- Một máy chủ (**Ubuntu** hoặc **Kali Linux**) có thể truy cập mạng nội bộ với các máy ảo.
- Hai máy ảo: **Windows** và **Linux**, dùng để cài đặt Wazuh Agent.

2.2.2 Bước 2. Cài đặt Wazuh Manager và Dashboard

Trên máy chủ, thực hiện lệnh sau:

```
curl -sO https://packages.wazuh.com/4.14/wazuh-install.sh
sudo bash wazuh-install.sh -a
```

Script này tự động cài đặt:

- **Wazuh Manager**
- **Wazuh Indexer**
- **Wazuh Dashboard**

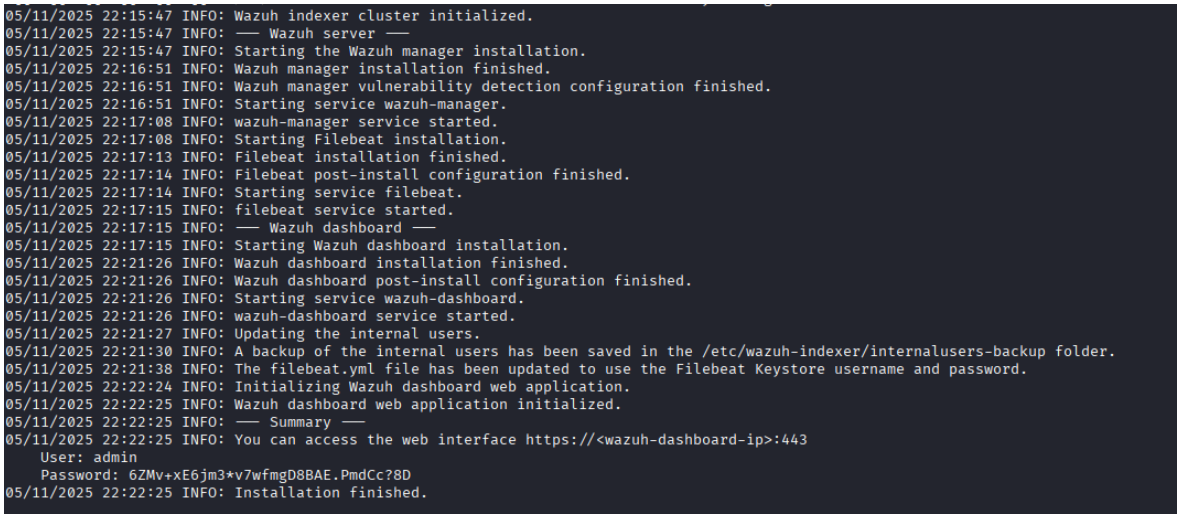


Figure 2.1: Quá trình tải và cài đặt trên máy chủ

Sau khi cài đặt hoàn tất, truy cập trang đăng nhập qua địa chỉ:
http://localhost/app/login

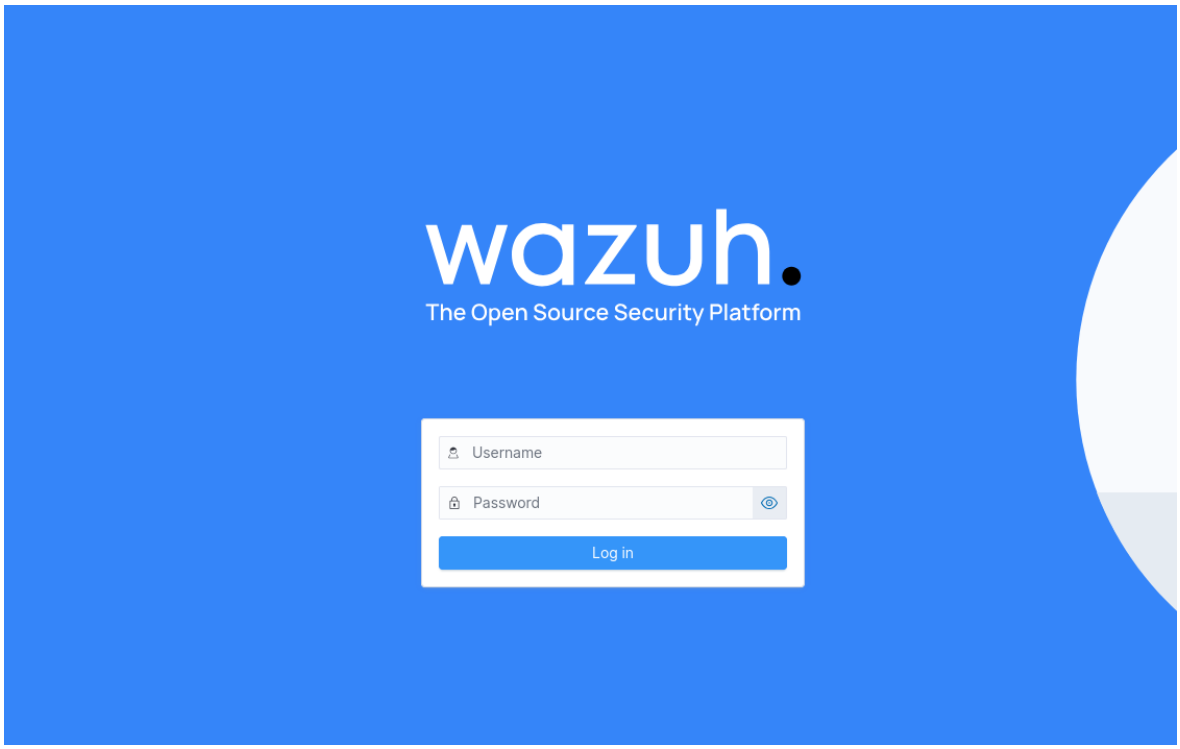


Figure 2.2: Giao diện đăng nhập Wazuh Dashboard

Nhập thông tin được cung cấp trong quá trình cài đặt để truy cập vào Dashboard.

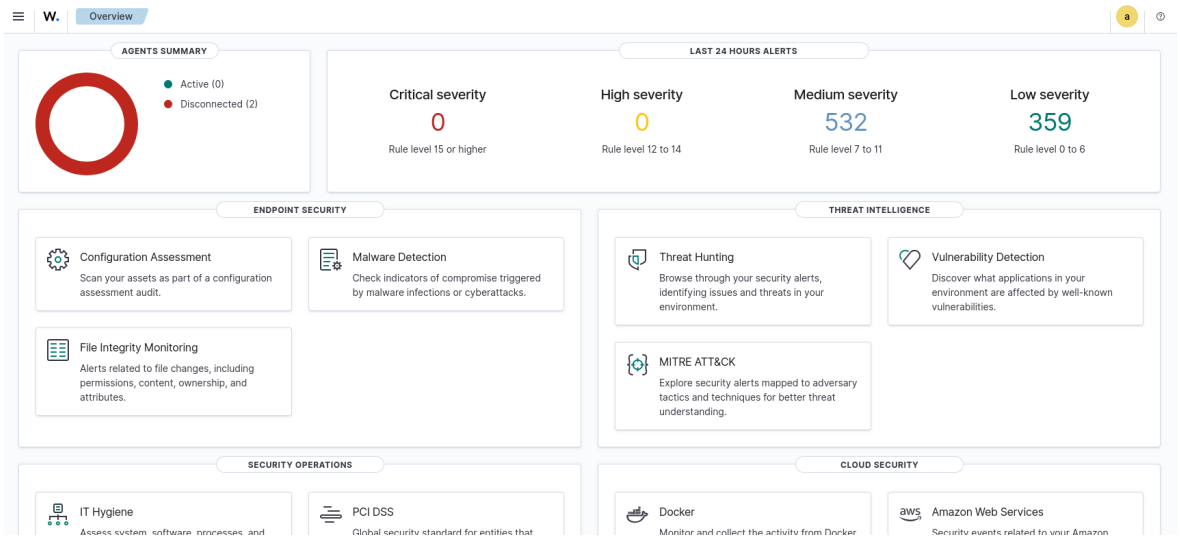


Figure 2.3: Giao diện Dashboard của Wazuh

2.2.3 Bước 3. Cài đặt Wazuh Agent

Trên Windows

Bước 1: Chọn hệ điều hành, kiến trúc và địa chỉ IP của server.

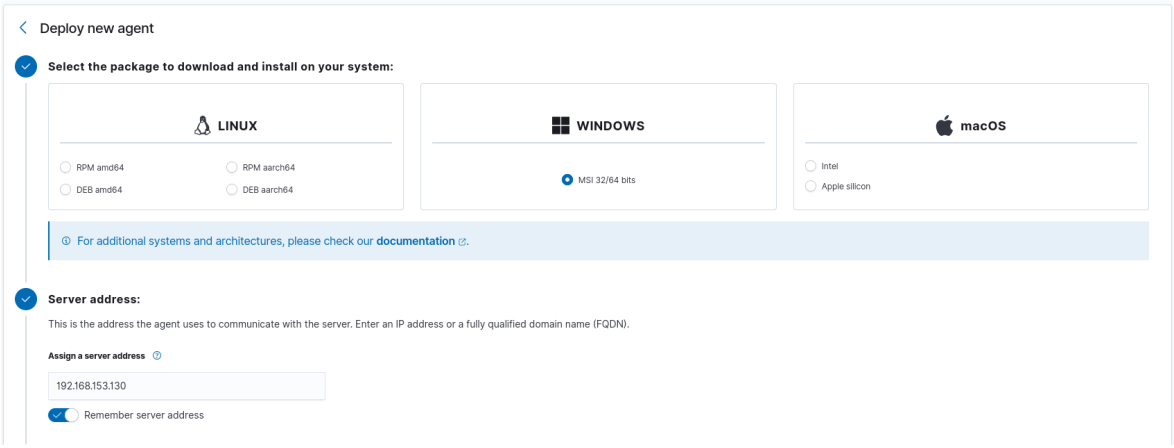


Figure 2.4: Chọn hệ điều hành, kiến trúc và địa chỉ server IP

Bước 2: Đặt tên Agent và phân phối nhóm.

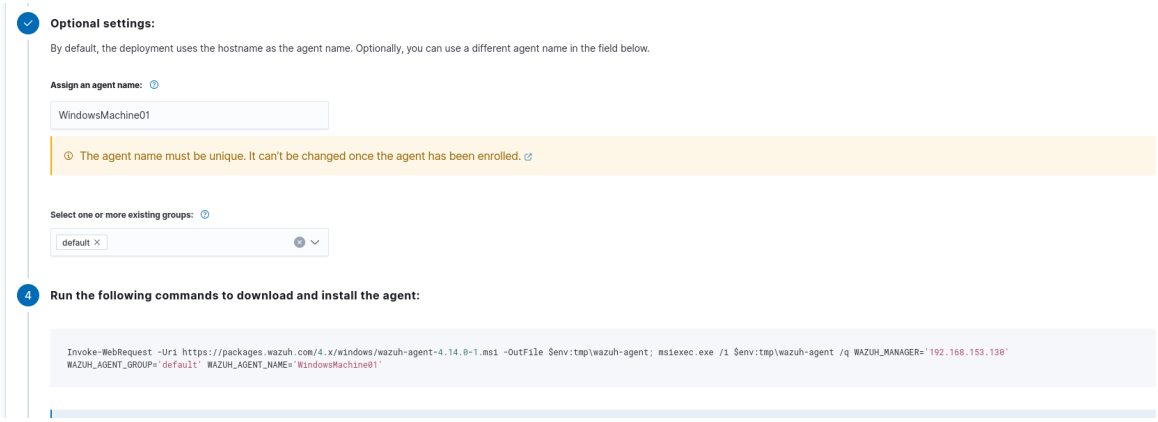


Figure 2.5: Đặt tên Agent và phân phối nhóm

Bước 3: Cấu hình phía Agent.

```
PS C:\Windows\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.14.0-1.msi -OutFile
$env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.153.130' WAZUH_AGENT_GROUP='default'
 WAZUH_AGENT_NAME='WindowsMachine01'
PS C:\Windows\system32> NET START Wazuh
The Wazuh service is starting.
The Wazuh service was started successfully.

PS C:\Windows\system32>
```

Figure 2.6: Cấu hình phía Agent Windows

Trong một số trường hợp, service `wazuh-agent` không khởi động được. Khi đó cần chỉnh sửa file **ossec.conf** tại: `C:\Program Files (x86)\ossec-agent`

ossec.conf - Notepad

File Edit Format View Help

```
<!--
  Wazuh - Agent - Default configuration for Windows
  More info at: https://documentation.wazuh.com
  Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>

  <client>
    <server>
      <address>192.168.153.130</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>windows, windows2016, windows-server, windows-serv
    <crypto_method>aes</crypto_method>
    <notify_time>20</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
  </client>

  <!-- Agent buffer options -->
  <client_buffer>
    <disabled>no</disabled>
```

Figure 2.7: Chỉnh sửa file `ossec.conf` để khắc phục lỗi service

Trên Linux

Thực hiện tương tự: chọn hệ điều hành, kiến trúc, server IP, đặt tên, phân phối nhóm, và sao chép command line để chạy trong shell bash:

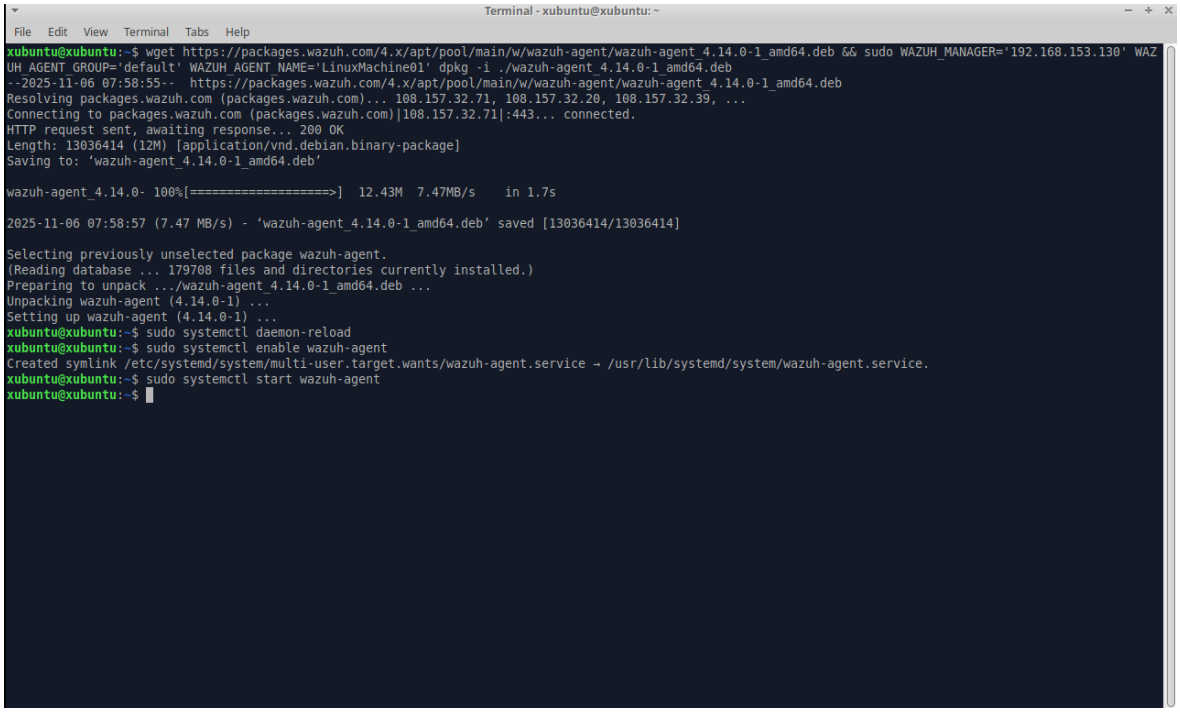


Figure 2.8: Cài đặt Wazuh Agent trên Linux

Sau khi hoàn tất, kết quả hiển thị như sau:

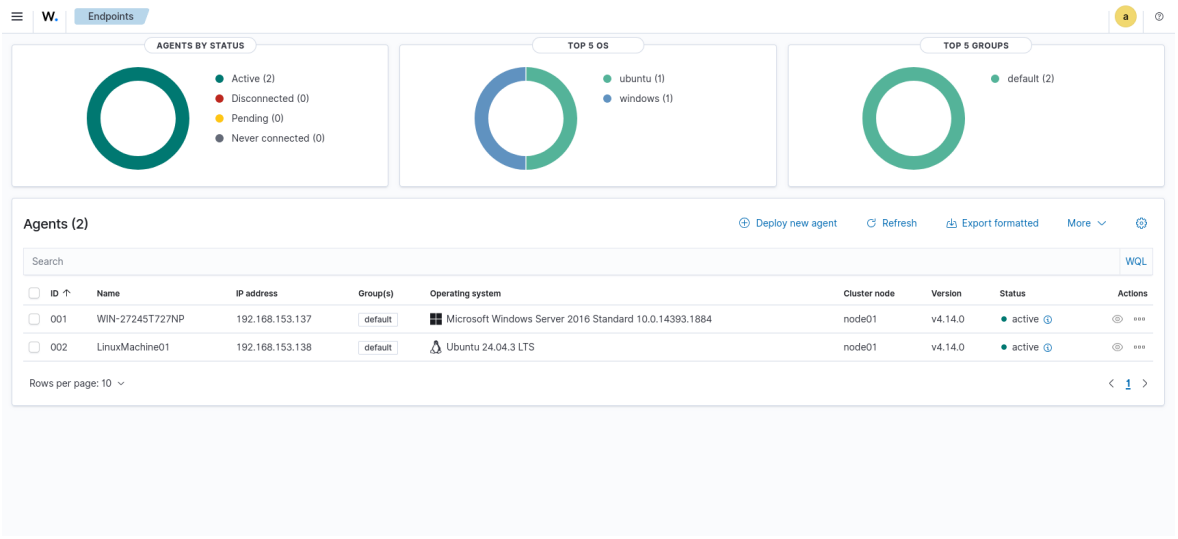


Figure 2.9: Kết quả cài đặt thành công Wazuh Agent

2.3 Cấu hình

Trong phần này, tiến hành cấu hình hệ thống Wazuh nhằm thiết lập quá trình giám sát cho các máy agent chạy Windows và Linux. Toàn bộ cấu hình được thực hiện trực tiếp trên **Wazuh Dashboard** nhằm đảm bảo tính trực quan và dễ quản lý. Việc tạo nhóm giúp quản lý và áp dụng cấu hình đồng bộ cho nhiều máy agent cùng lúc, tránh việc chỉnh sửa thủ công từng agent riêng lẻ.

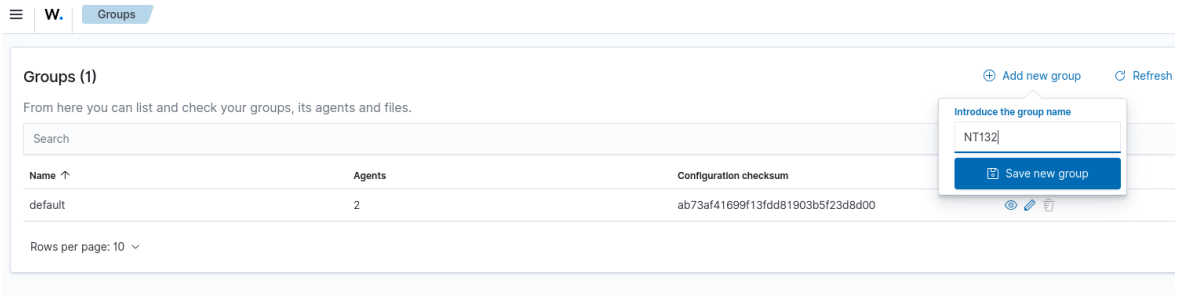


Figure 2.10: Tạo nhóm Wazuh

Đầu tiên, nhóm mới được tạo trong giao diện Wazuh Dashboard để gom các agent có cùng mục đích giám sát.

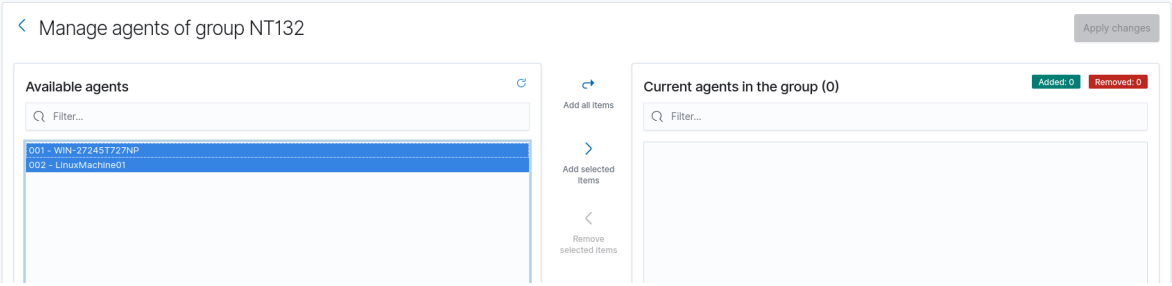


Figure 2.11: Thêm Agent vào nhóm Wazuh

Sau đó, các máy agent (Windows và Linux) được thêm vào nhóm để áp dụng cùng một cấu hình.

```
<agent_config os="all">
  <!-- ==================== FILE INTEGRITY MONITORING ==================== -->
  <syscheck>
    <frequency>3600</frequency>
    <!-- Kiểm tra mỗi 1 giờ -->
    <directories check_all="yes">/etc,/usr/bin,/usr/sbin,/bin,/sbin,C:\Windows\System32</directories>
    <ignore>/var/log,/tmp,C:\Windows\Temp</ignore>
  </syscheck>
  <!-- ==================== ROOTCHECK ==================== -->
  <rootcheck>
    <disabled>no</disabled>
  </rootcheck>
```

Figure 2.12: Cấu hình Group kiểm tra thư mục hệ thống

```
<!-- ==================== LINUX LOGS ==================== -->
<localfile os="linux">
  <log_format>syslog</log_format>
  <location>/var/log/auth.log</location>
</localfile>

<localfile os="linux">
  <log_format>syslog</log_format>
  <location>/var/log/syslog</location>
</localfile>
```

Figure 2.13: Cấu hình Group cho máy Linux

```
<!-- ==================== WINDOWS LOGS ==================== -->
<localfile os="windows">
  <log_format>eventchannel</log_format>
  <location>Security</location>
</localfile>

<localfile os="windows">
  <log_format>eventchannel</log_format>
  <location>System</location>
</localfile>

<localfile os="windows">
  <log_format>eventchannel</log_format>
  <location>Application</location>
</localfile>
```

Figure 2.14: Cấu hình Group cho máy Windows

Giải thích cấu hình

- **File Integrity Monitoring (Syscheck):** Phần này cho phép Wazuh theo dõi sự thay đổi của các tệp hệ thống quan trọng. Cấu hình đặt tần suất kiểm tra là mỗi 3600 giây (1 giờ). Các thư mục như `/etc`, `/usr/bin`, `/usr/sbin`, `/bin`, `/sbin` trên Linux và `C:\Windows\System32` trên Windows được giám sát chặt chẽ. Các thư mục `/var/log`, `/tmp`, và `C:\Windows\Temp` được bỏ qua để tránh báo động giả do thay đổi thường xuyên.
- **Rootcheck:** Tính năng này được bật (`<disabled>no</disabled>`) nhằm phát hiện rootkit, malware hoặc các cấu hình hệ thống đáng ngờ trên máy agent.
- **Giám sát log hệ thống Linux:** Hai tệp log chính được thu thập là:
  - `/var/log/auth.log`: chứa thông tin xác thực và đăng nhập.
  - `/var/log/syslog`: chứa thông tin hệ thống và các sự kiện dịch vụ.
- **Giám sát log hệ thống Windows:** Các kênh log `Security`, `System`, và `Application` được Wazuh thu thập thông qua Event Channel, giúp phát hiện các sự kiện bảo mật, lỗi hệ thống và hoạt động của ứng dụng.

Tệp cấu hình trên đảm bảo rằng cả hai loại hệ điều hành (Windows và Linux) đều được giám sát một cách toàn diện, từ tính toàn vẹn tệp cho đến nhật ký sự kiện bảo mật.

Kết quả

Tài liệu tham khảo

- Template Overleaf: Overleaf