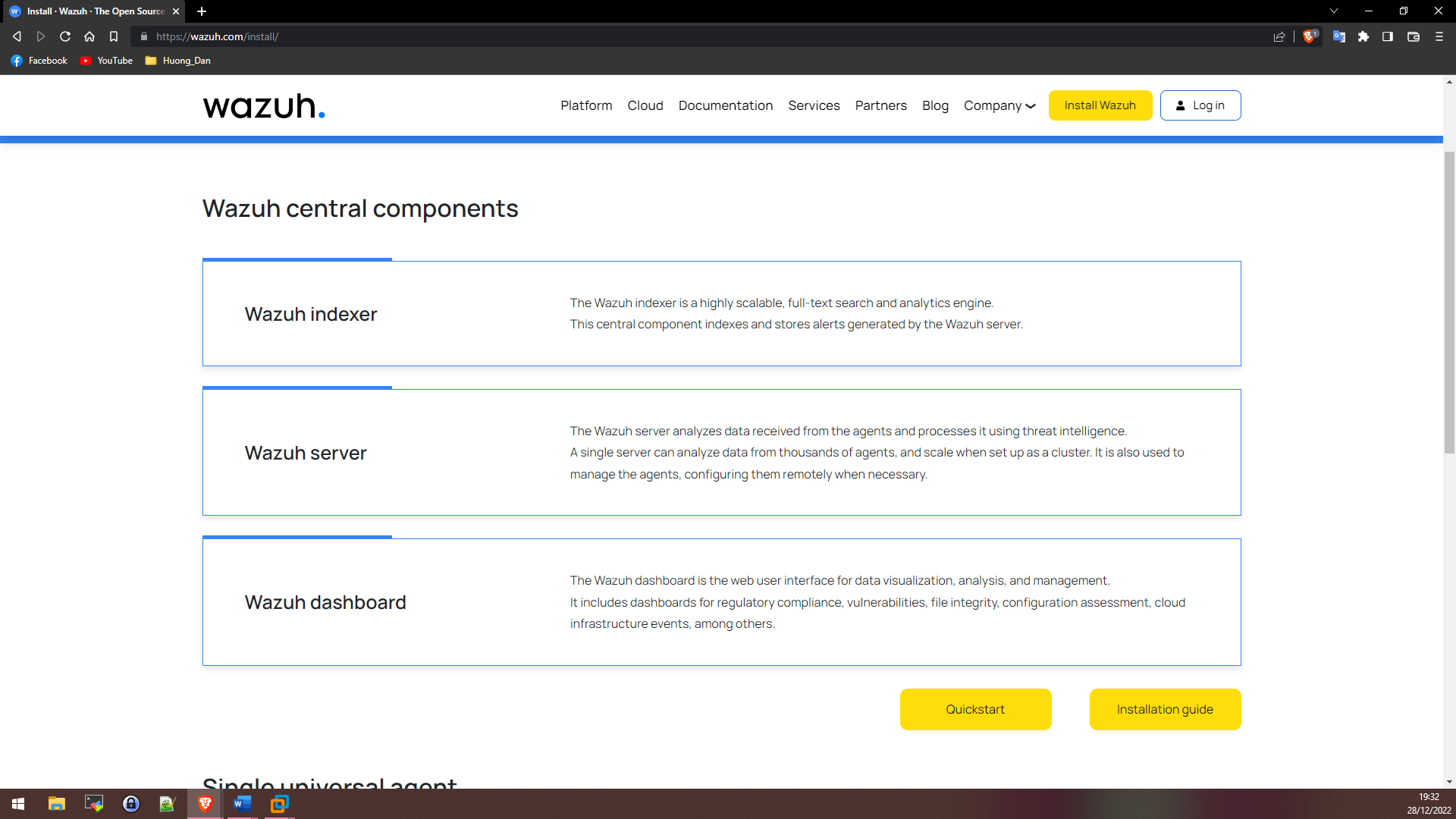
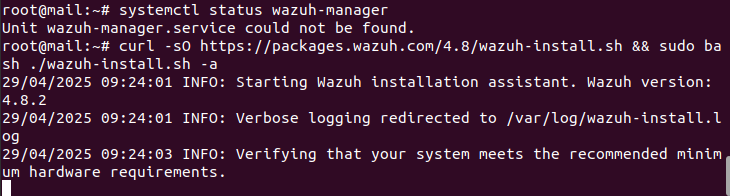
1. **Triển khai**
2. **Install**

Trong quá trình tìm hiểu thay vì phải cài từng phần riêng lẻ cho wazuh ta có thể dùng 1 dòng lệnh để cài tất cả các gói tin, các thành phần để có thể monitoring bằng wazuh

Ở trang install wazuh ta chọn Quickstart



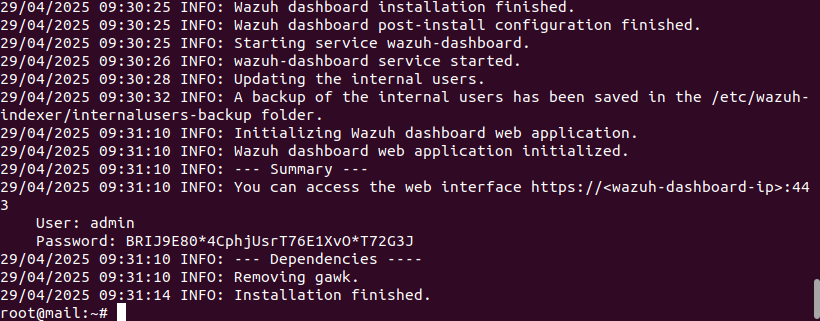
Hình 1: chọn Quickstart



Hình 2: cài đặt wazuh bằng 1 lệnh

Dùng lệnh

curl -sO https://packages.wazuh.com/4.8/wazuh-install.sh && sudo bash ./wazuh-install.sh -a



Hình 3: đã hoàn thành quá trình tải

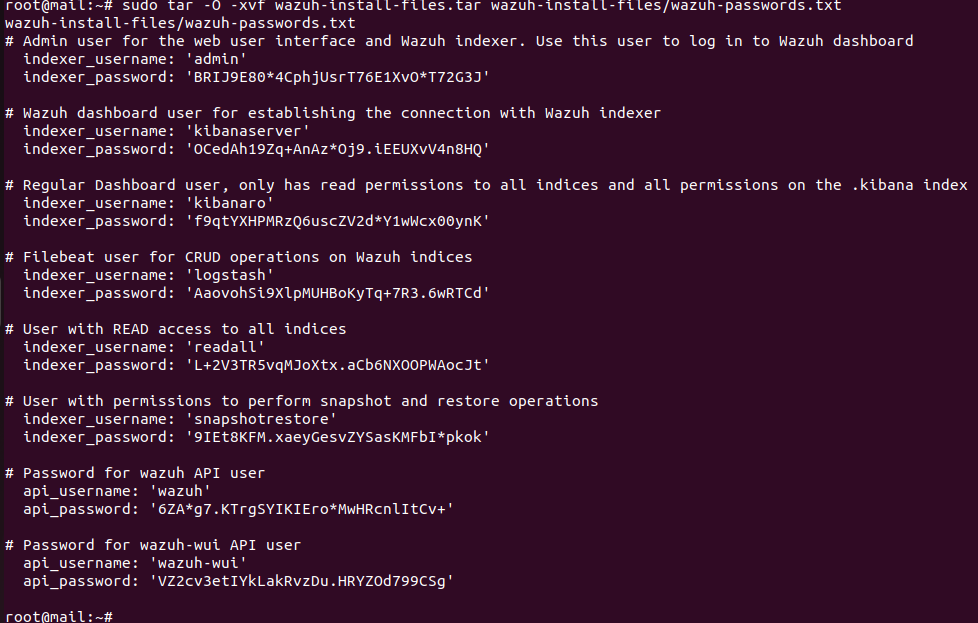
User: admin

Password: BRIJ9E80\*4CphjUsrT76E1XvO\*T72G3J

Khi cài wazuh bằng 1 thì nó sẽ tự cài đặt các thành phần của wazuh như: wazuh index, filebeat ,wazuh server, wazuh dashboard,tự tạo các chứng chỉ cần thiết (từ bản 4.3 sẽ cần phải có các chứng thực từ dịch vụ). Đồng nghĩa với việc nó sẽ tự đặt password cho các dịch vụ trong warzuh. Để lấy được password của các dịch vụ ta tiến hành dùng câu lệnh

sudo tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt

lệnh này dùng để giải nén file wazuh file wazuh-instrall-file.tar và xuất ra thành file theo wazuh-install-files/wazuh-passwords.txt



Hình 4: Passwd của các thành phần wazuh

Như vậy đã xong quá trình cài đặt

Để có thể truy cập vào wazuh gõ theo cú pháp:

https://<IP server wazuh>

Nhưng ta nên thay đổi port để không bị trùng với các dịch vụ có sẵn hoặc cần tích hợp sau này

Thay đổi ở:

nano /etc/wazuh-dashboard/opensearch\_dashboards.yml

Chuyển lại thành:

server.port: 9443

Sau đó Restart dịch vụ:

sudo systemctl restart wazuh-dashboard

Giờ ta có thể truy cập https://<ip-server>:9443/

Tiếp theo ta cần chỉnh lại một xíu nếu thông qua reverse proxy

Tạo thêm file /etc/nginx/sites-enabled/wazuh

Nội dung như sau:

server {

listen 443 ssl;

server\_name wazuh.local;

ssl\_certificate /etc/wazuh-dashboard/certs/wazuh-dashboard.pem;

ssl\_certificate\_key /etc/wazuh-dashboard/certs/wazuh-dashboard-key.pem;

location / {

proxy\_pass https://127.0.0.1:443;

proxy\_ssl\_verify off;

proxy\_set\_header Host $host;

proxy\_set\_header X-Real-IP $remote\_addr;

proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;

}

}

Sửa lại Wazuh Dashboard:

Trong file /etc/wazuh-dashboard/opensearch\_dashboards.yml, đổi:

server.host: 127.0.0.1

(Chỉ listen localhost, để nginx là reverse proxy.)

Restart:

sudo systemctl restart wazuh-dashboard

sudo systemctl reload nginx

Truy cập: https://wazuh.local/

Chú ý: wazuh.local phải được khai báo trong file /etc/hosts hoặc DNS nhé. Ví dụ:

192.168.1.30 wazuh.local

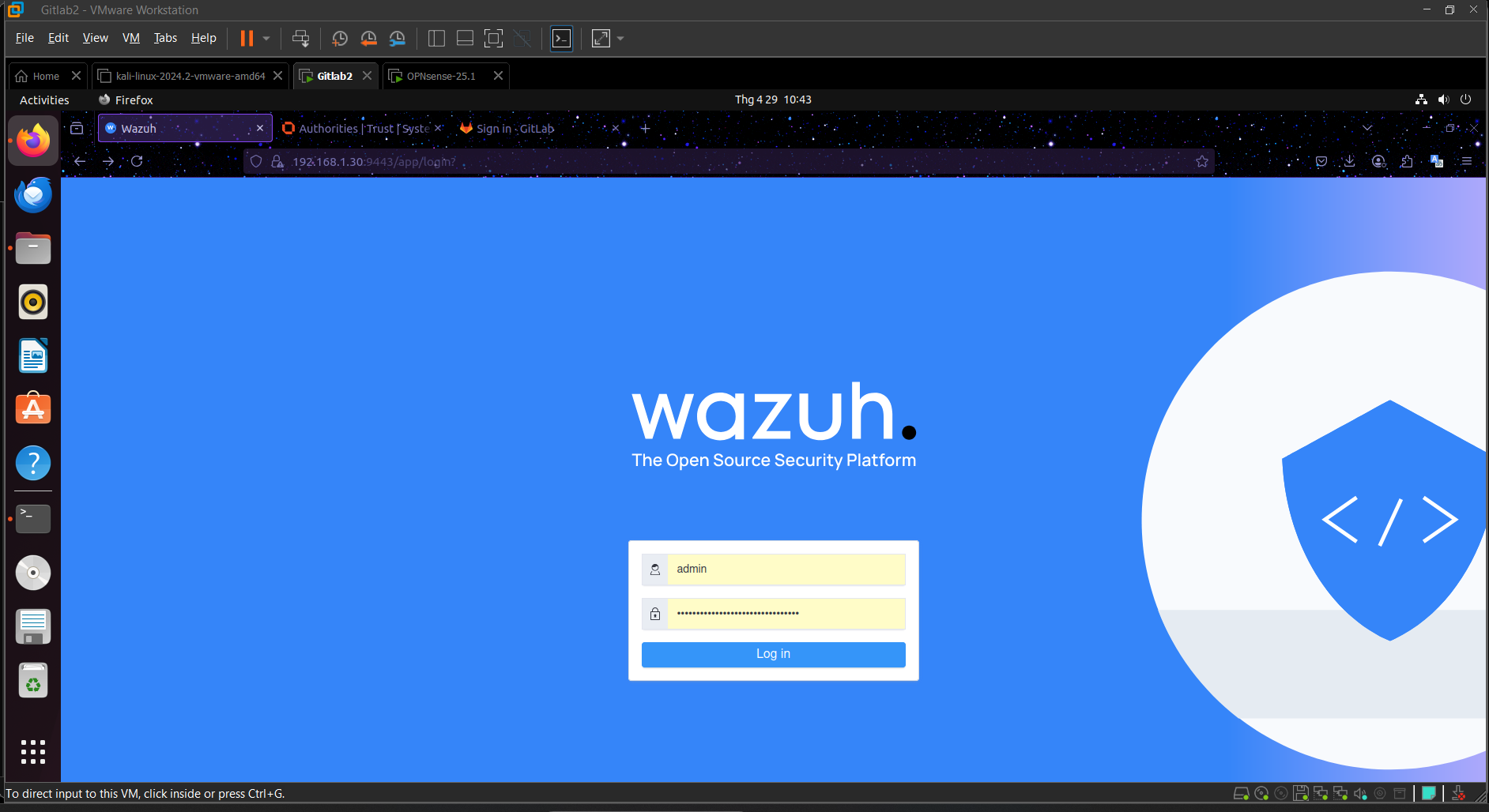
Mặc định username và passwd sẽ là: admin/admin. Do ta cài bằng phương pháp setup nhanh nên đã vô tình kích hoạt tool thay đổi toàn bộ passwd sao cho có tính an toàn của wazuh. Dòng lệnh vô tình đã kích hoạt:

/usr/share/wazuh-indexer/plugins/opensearch-security/tools/wazuh-passwords-tool.sh --change-all --admin-user wazuh --admin-password wazuh

Ở đây ta sẽ đăng nhập bằng username/passwd đã được cấp sẳn:

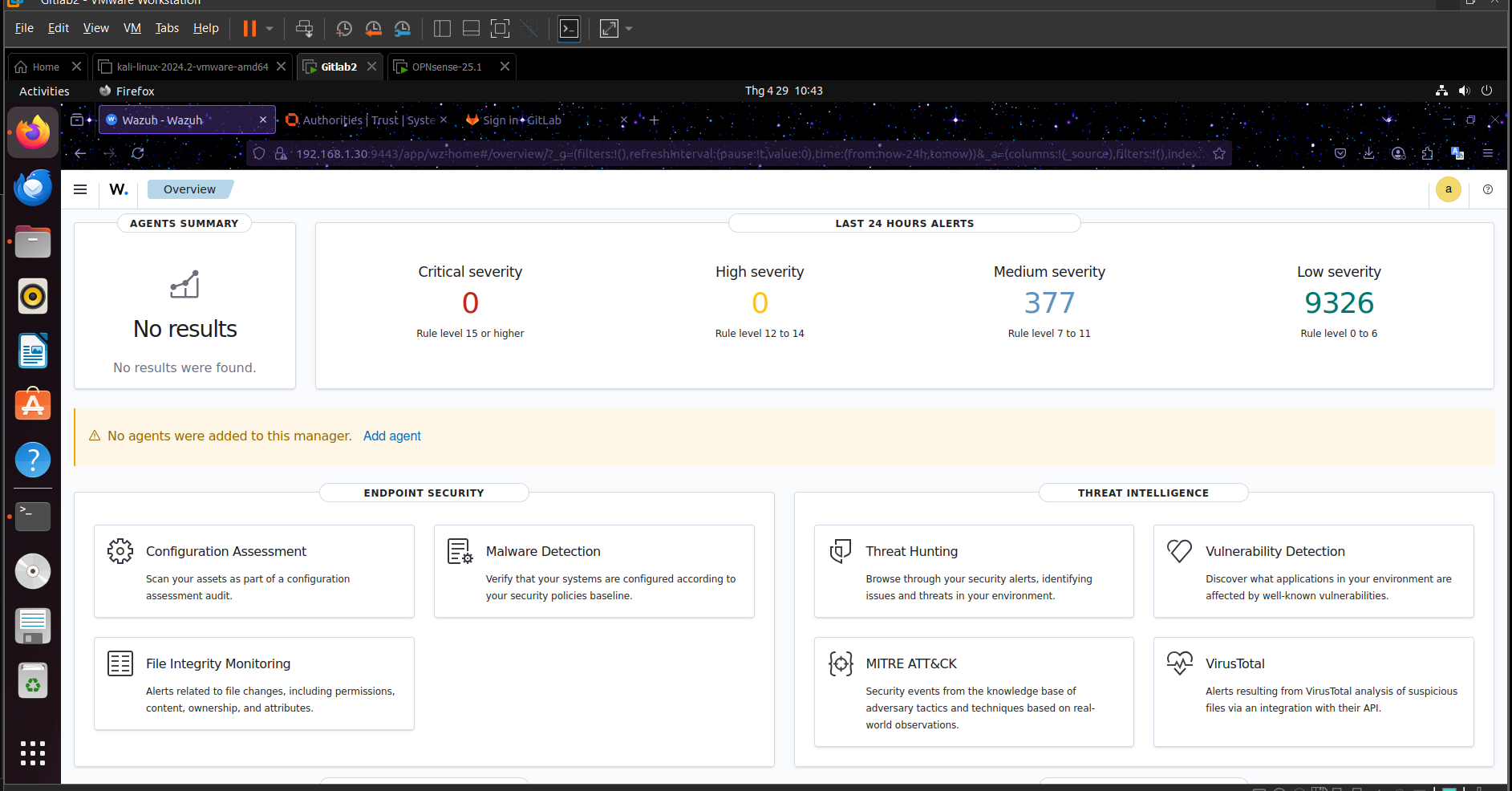
admin

BRIJ9E80\*4CphjUsrT76E1XvO\*T72G3J



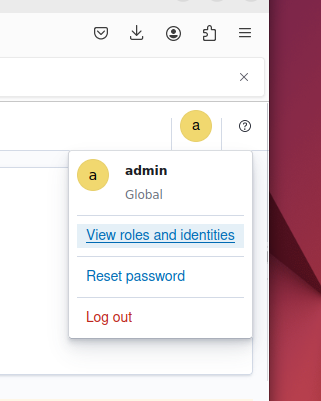
Hình 5: Giao diện chính của wazuh

Như vậy đã vào được wazuh



Hình 6: Trang chủ sau khi đăng nhập

Ta có thể reset password lại

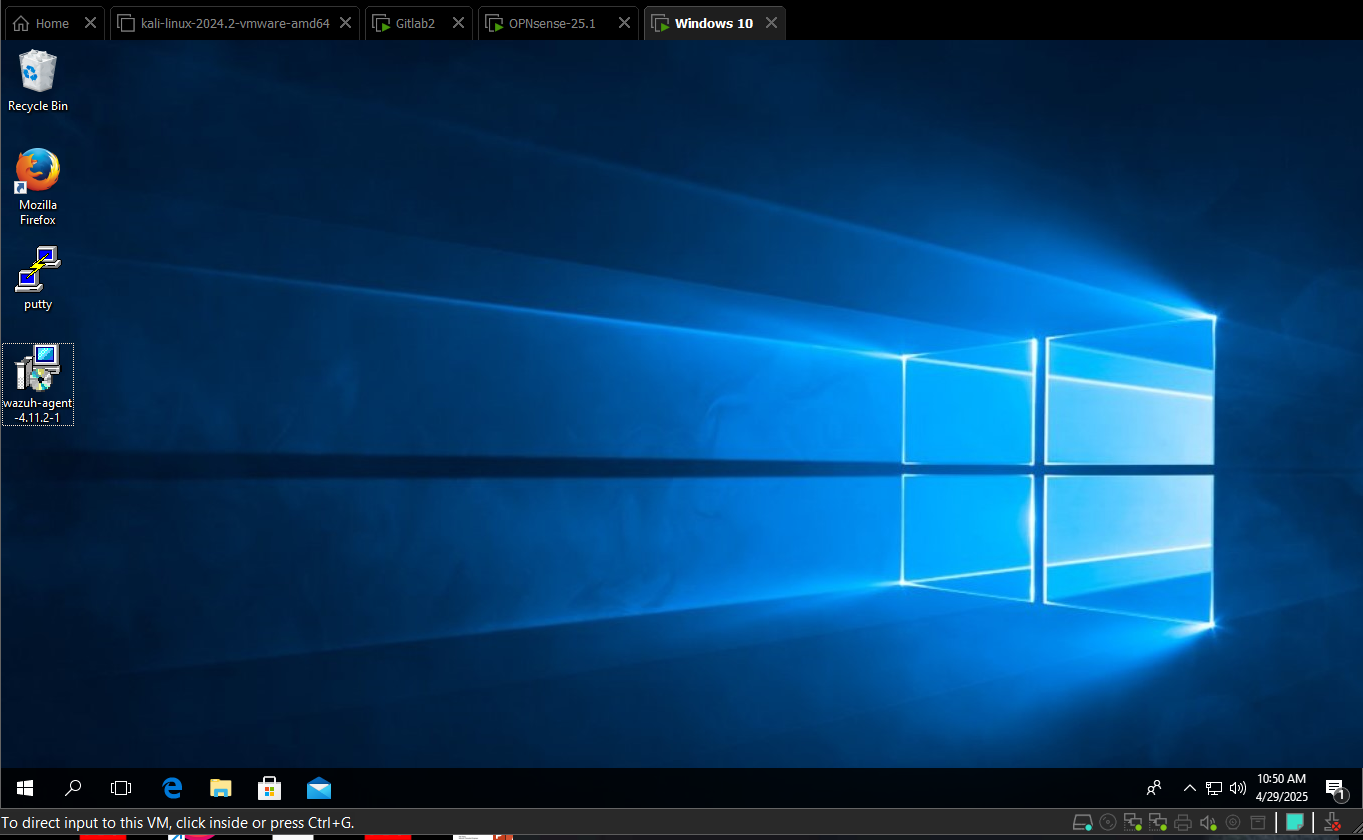


1. **Monitor**

Sau cài cặt thành công tiến hành monitor máy window

Download window agent tại:

<https://packages.wazuh.com/4.x/windows/wazuh-agent-4.8.2-1.msi>



A computer screen with a computer screen

Description automatically generated

Hình 7: biểu tượng sau khi cài

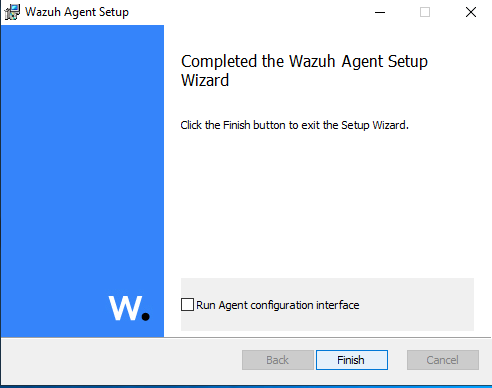
Tiến hành cài đặt

A screenshot of a computer

Description automatically generated

Hình 8: install wazuh agent

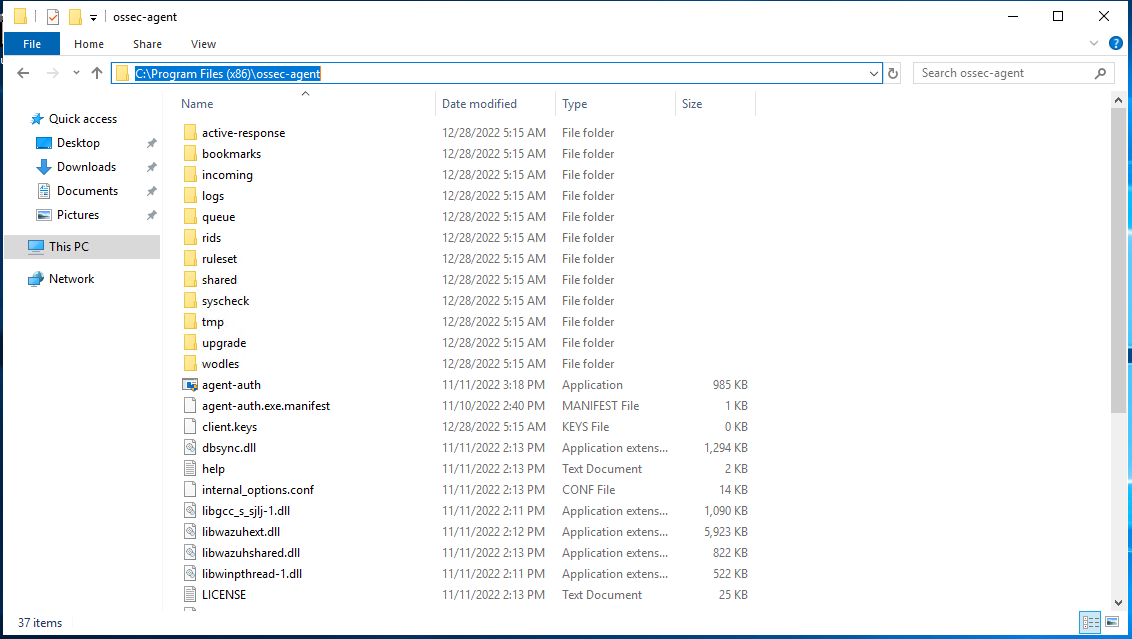
Nhấn Finish



Hình 9: hoàn tất cài đặt

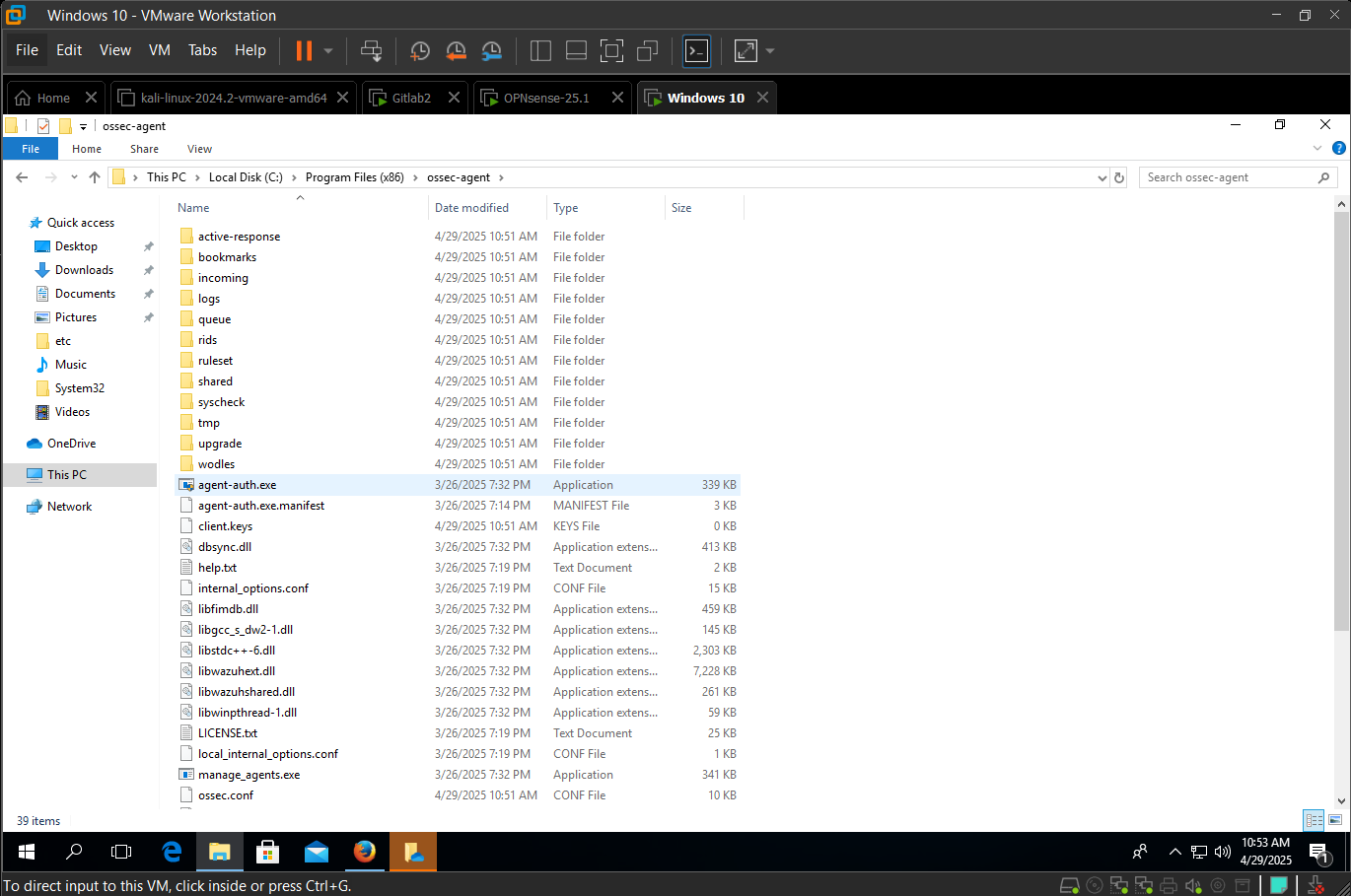
Để kết nối với máy chủ wazuh vào theo đường dẫn

C:\Program Files (x86)\ossec-agent



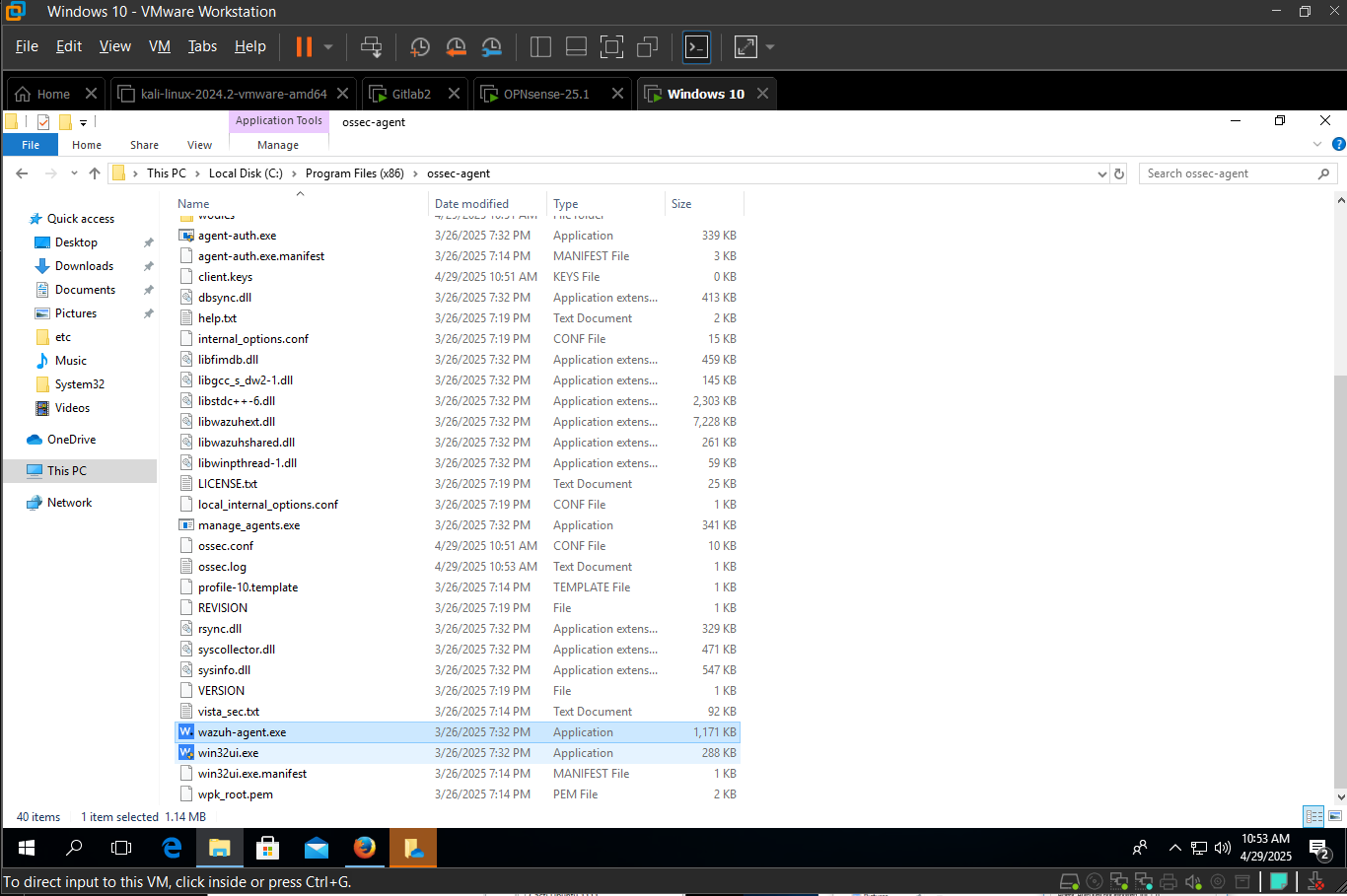
Hình 10: thư mục chứa Agent

Chạy file agent-auth.exe để lấy key xác thực



Hình 11: file agent-auth.exe

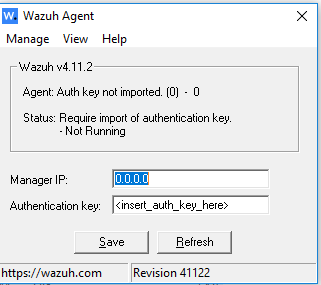
Chạy file win32ui.exe để tiến hành kết nối với wazuh server



Hình 12: file win32ui.exe

Nhập IP của wazuh server vào. Tới đây sẽ có 2 trường hợp:

Trường hợp 1: không nhận được key xác thực



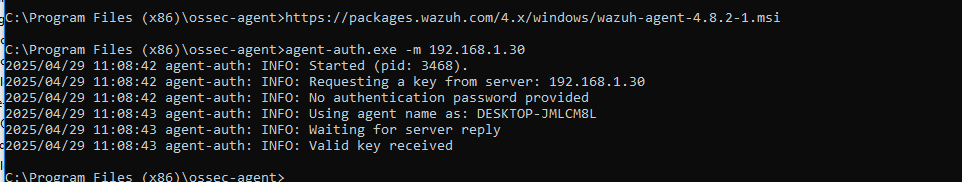
Hình 13: không có key xác thực

Cách giải quyết:

+ bật CMD (mở tại thư mục chưa Agent)

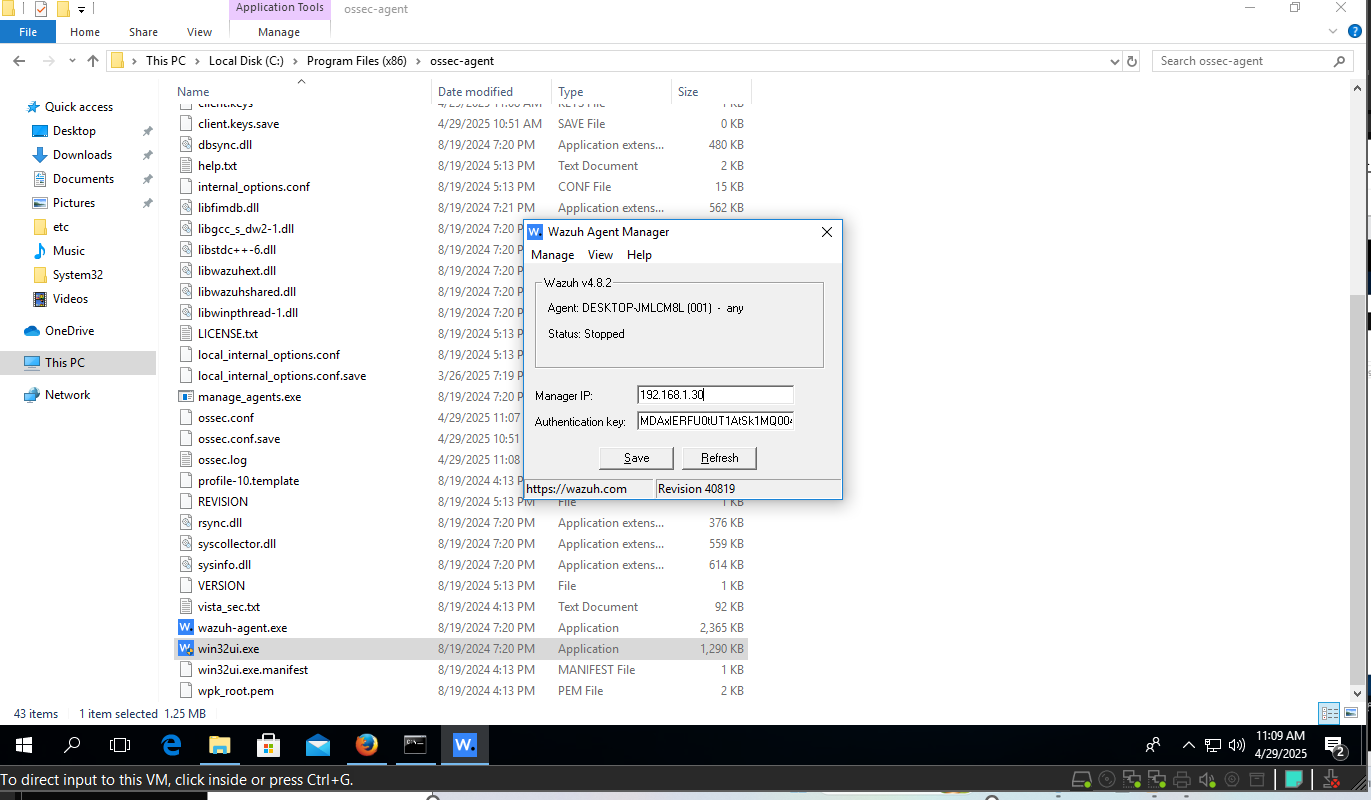
+ chạy lệnh: agent-auth.exe -m 192.168.1.30

Câu lệnh có ý nghĩa: chạy lại file agent-auth.exe. -m là, và trỏ về địa chỉ IP của server



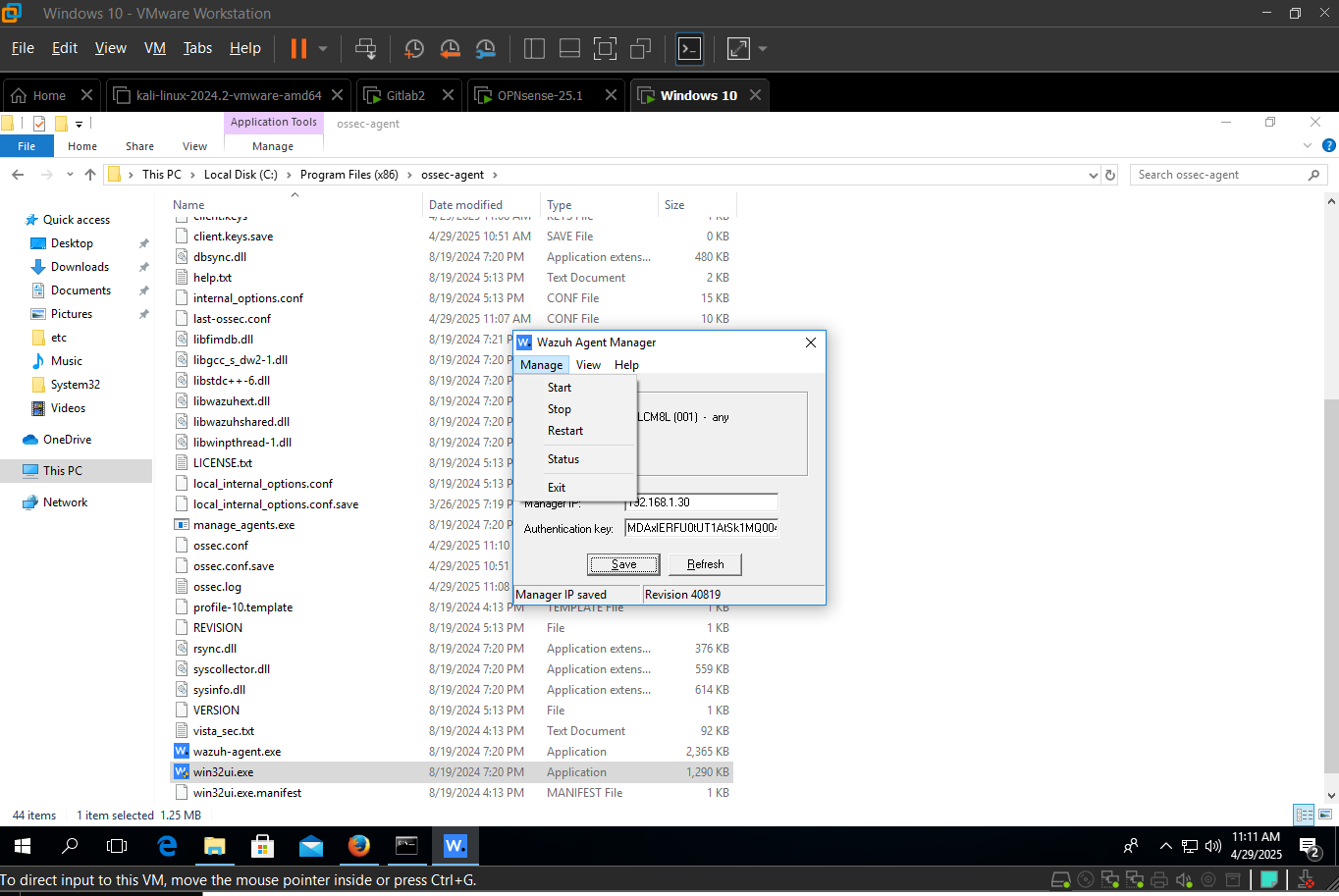
Hình 14: giải quyết vấn đề không nhận được key xác thực

Lúc này chạy lại win32ui.exe đã được cấp key xác thực



Hình 15: đã cấp key xác thực cho agent

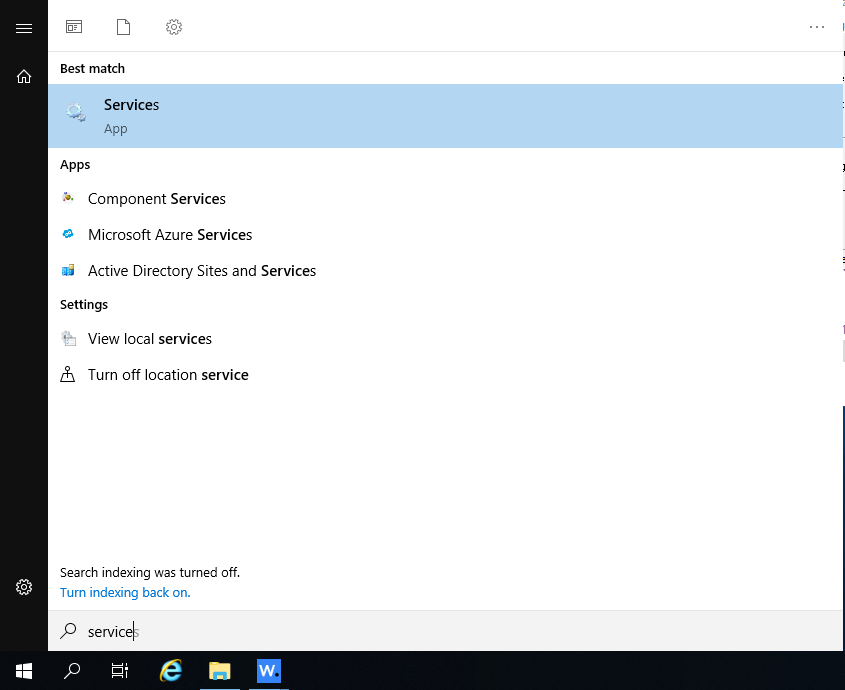
Tiếp theo nhấn save và start agent



Hình 16: start agent

Để chắc chắn agent đã chạy vào services kiểm tra xem wazuh-agent đã start chưa

Để vào services: vào thành tìm kiếm của window gõ services



Hình 17: cách vào services

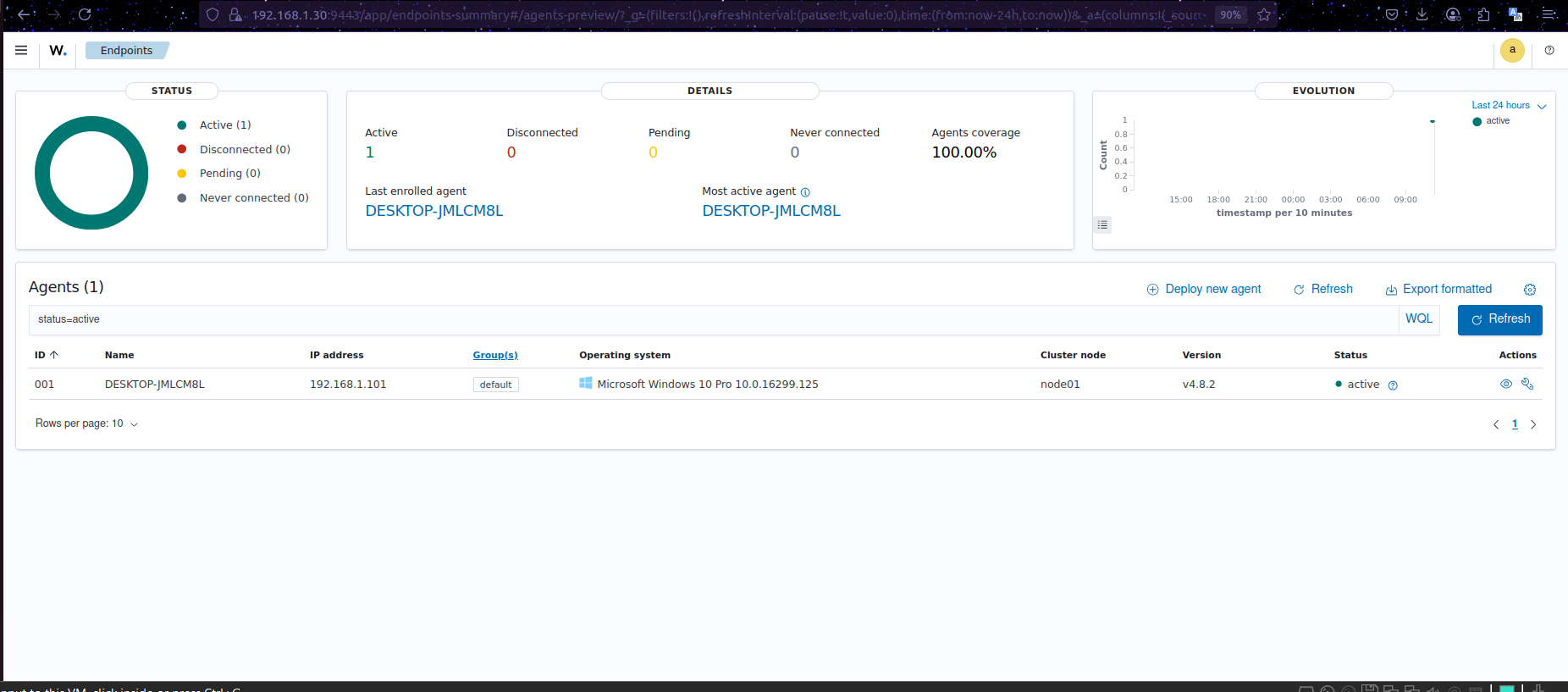
Ban đầu Wazuuh chưa chạy service nhấn vào Start.

A computer screen shot of a computer

Description automatically generated

Hình 18: Nếu service chưa start thì hãy nhấn nút start

Kiểm tra lại trên web wazuh đã thấy agent nhảy lên 1



Hình 20: Đã monitor được window 10

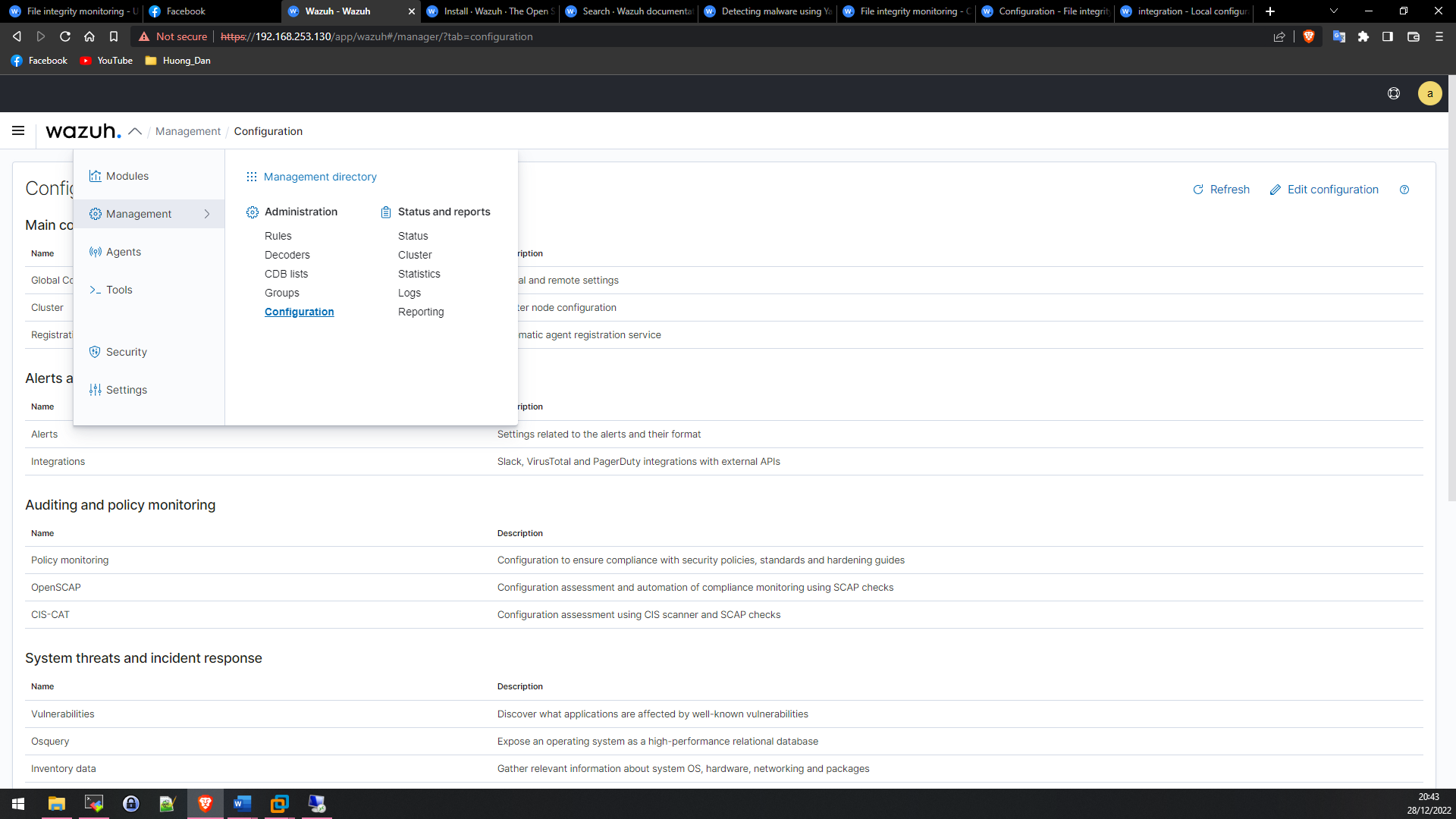
Như vậy đã monitor thành công Agent

1. **Configure**
   1. **File integrity monitoring**

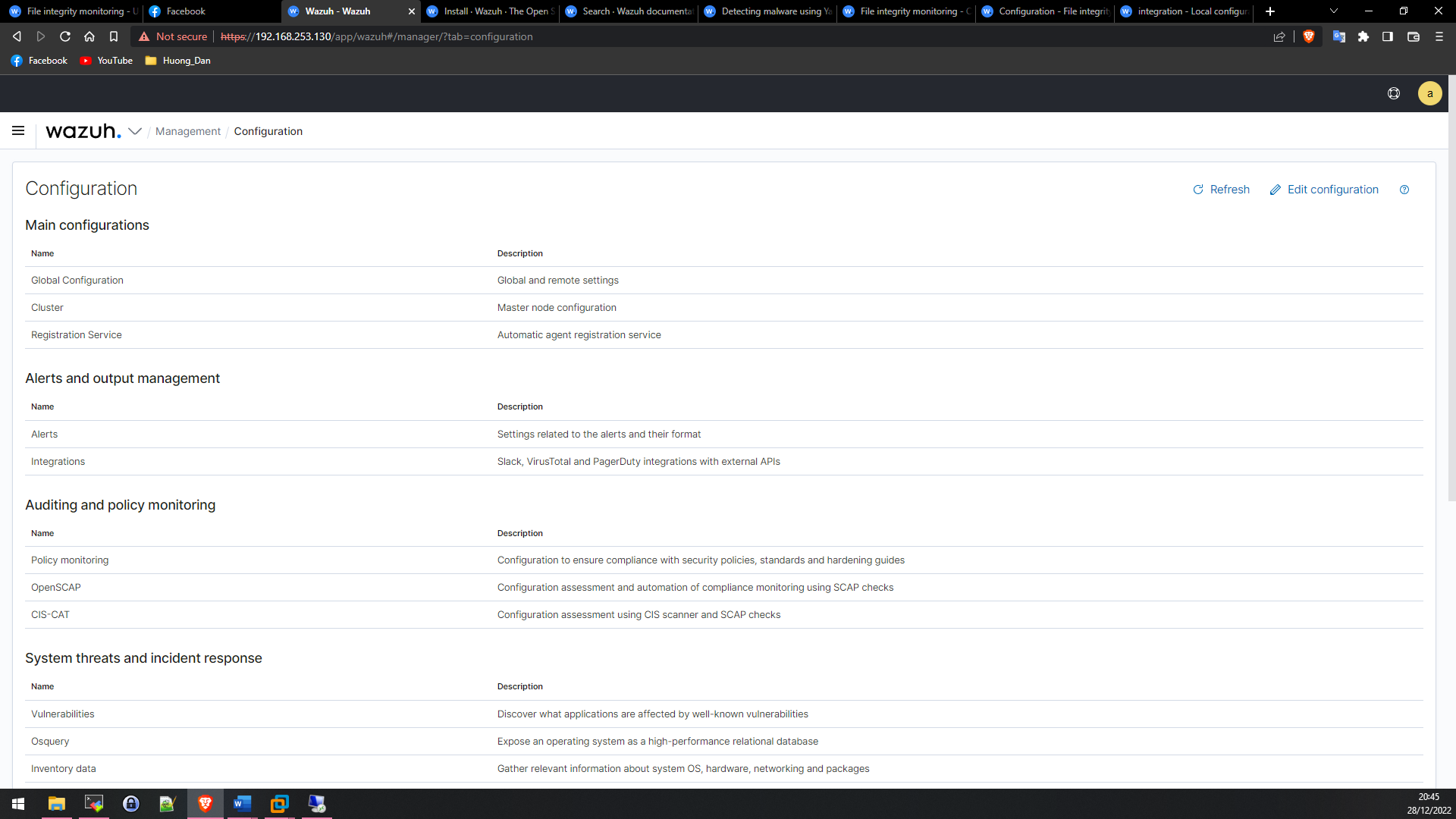
Để có thể monitor 1 cách hiểu quả ta tiến hành configure giám sát file trên window (file integrity monitoring)

Cách làm này sẽ chỉnh file ossec.conf trên riêng con wazuh server. Để config được thì cần phải chỉnh 1 số thử sau:

Vào Management 🡪 Configuration 🡪 edit configuration



Hình 21: vào file ossec.conf



Hình 22: vào file ossec.conf

Chỉnh các rule đang có tag <disabled>no<disabled> 🡪 <disabled>yes<disabled>, nói đơn giản chuyến hết tag đang có <disabled>/<enabled> mà đang có trạng thái no 🡪 yes

A screenshot of a computer

Description automatically generated

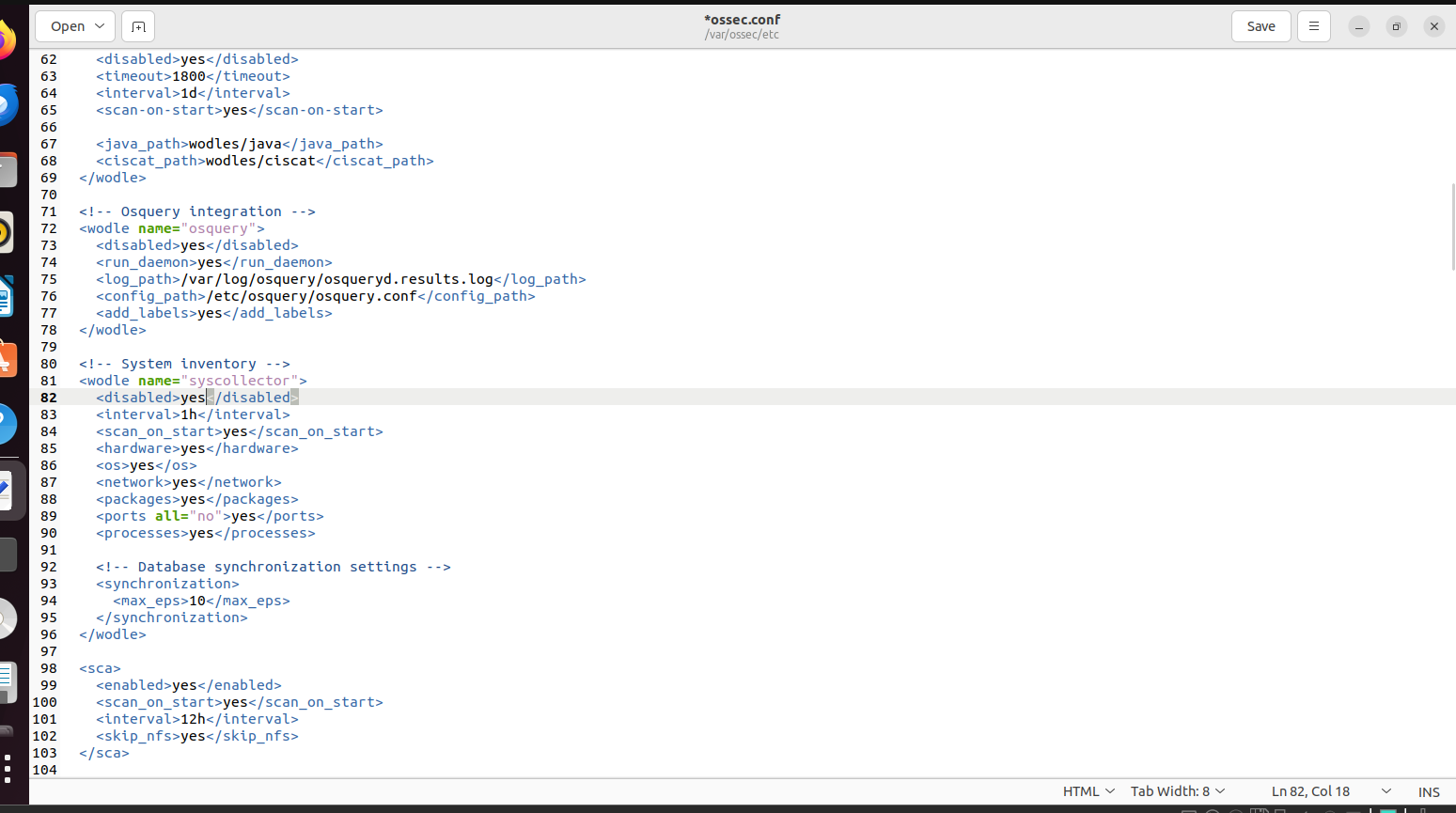
Hình 23: chỉnh các rule đang có trạng thái no 🡪 yes

<logall>yes</logall> bật tính năng ghi log

<logall\_json>yes</logall\_json> ghi log dạng json giúp dễ đọc, phân tích

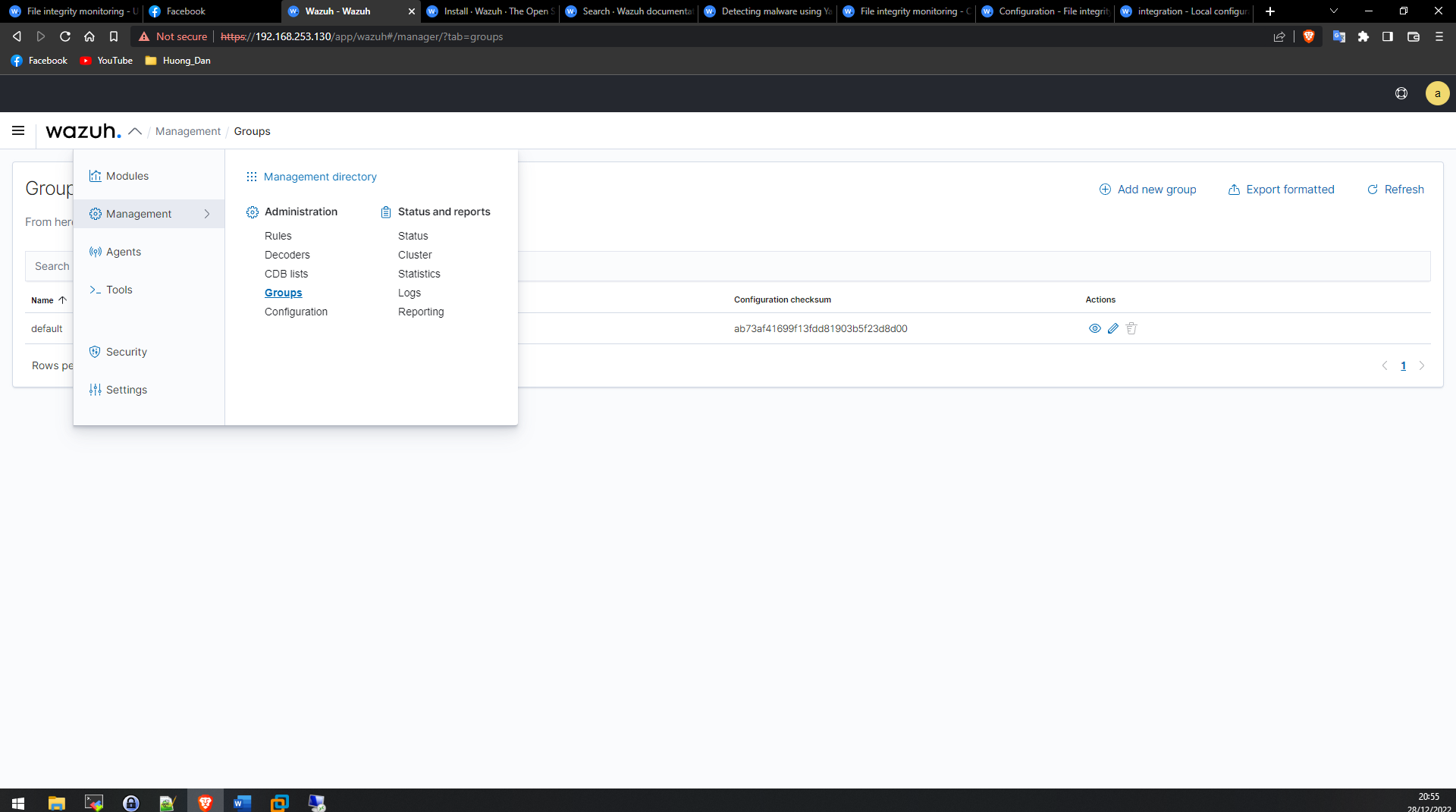
<email\_notification>yes</email\_notification> bật thông báo bằng mai

Hoặc đơn giản là dùng lệnh  
  
sudo gedit /var/ossec/etc/ossec.conf



Sau khi chỉnh file ossec.conf ở máy manager xong thì ta sẽ tiến hành chỉnh file ossec.conf ở các máy agent. Ta sẽ chỉnh trực tiếp từ trên giao diện web luôn. Vì khi các máy agent sẽ được quản lý trên cùng 1 group (nếu config theo mặc định thì group mặc định sẽ là default). Config trên trực tiếp giao diện web sau từ đây sẽ đồng bộ với file ossec.conf trên các máy agent được quản lý chung 1 group với nhau

Management 🡪 Groups



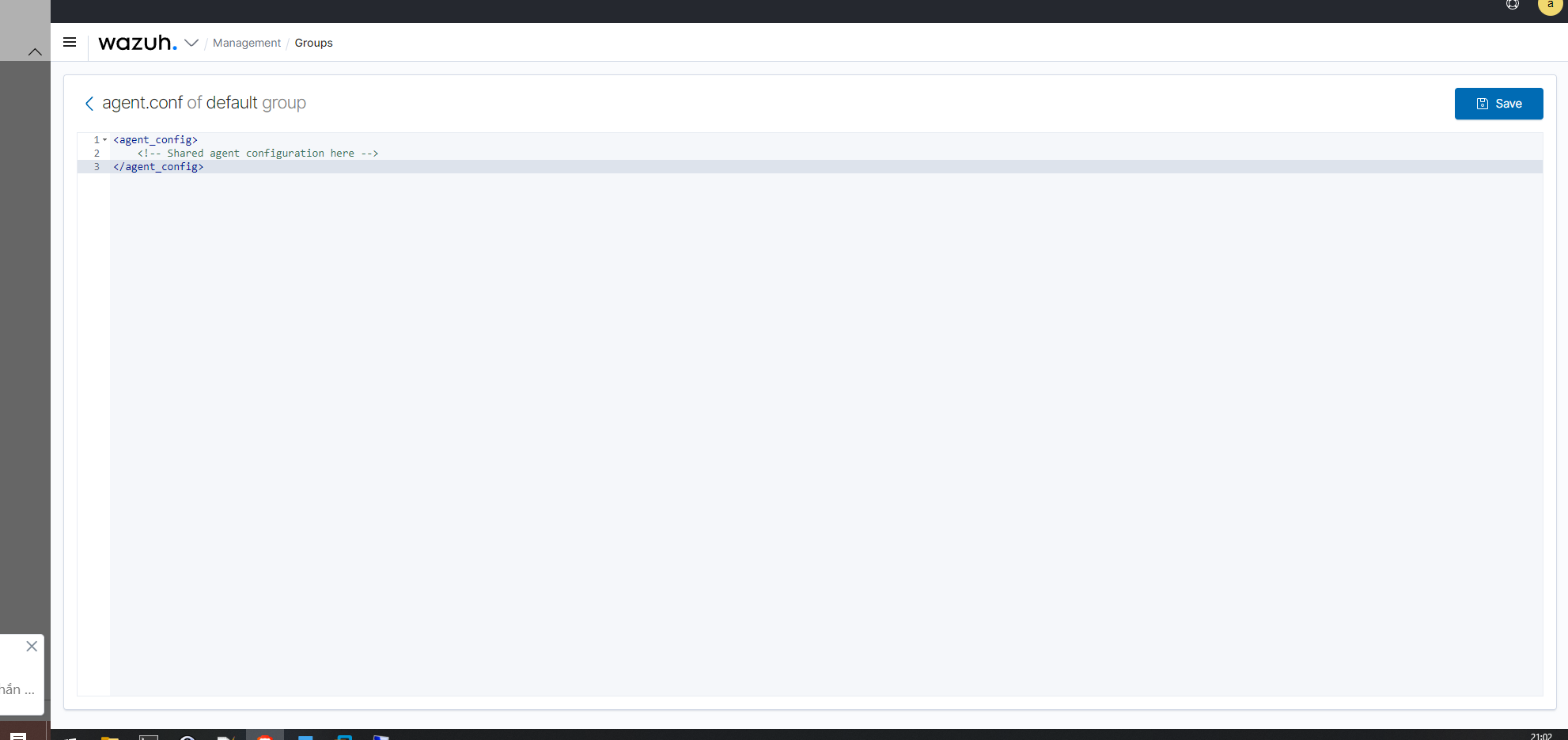
Hình 24: vào file ossec.conf của các máy agent

A screenshot of a computer

Description automatically generated



Hình 25: nhấn vào cây bút chì



Hình 26: mặc định file config

Ta sẽ bỏ vào đó file phần syscheck để có thể thu thập event từ máy agent khi có thêm, sửa, xóa file ở ổ đĩa mình quản lý

Thêm đoạn này vào giữa tag agent\_config:

<syscheck>

<disabled>no</disabled>

<!—Start Custom syscheck Configurations 🡪

<!—Real-Time Monitoring 🡪

<directories check\_all=”yes” realtime=”yes”>C:/Temp//</directories>

<directories check\_all=”yes” realtime=”yes”>C:/Windows/Temp </directories>

<directories check\_all=”yes” realtime=”yes”>C:/Users\*/Downloads/</directories>

<directories check\_all=”yes” realtime=”yes”>C:/Users/\*/Desktop/</directories>

<directories check\_all=”yes” realtime=”yes”>C:/Users/\*/Documents/</directories>

<directories check\_all=”yes” realtime=”yes”>C:/Users/\*/Start Menu/Programs/Startup/</directories>

<!—End Custom syscheck Configurations 🡪

<!—Start Default syscheck Configurations 🡪

<!—Frequency that syscheck is executed default every 12 hours 🡪

<frequency>43200</frequency>

<!—Default files to be monitored. 🡪

<directories recursion\_level=”0” restrict=”regedit.exe$|system.ini$|win.ini$”>%WINDIR%</directories>

<directories recursion\_level=”0” restrict=”at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|net.exe$|net1.exe$|netsh.exe$|reg.exe$|regedt32.exe|regsvr32.exe|runas.exe|sc.exe|schtasks.exe|sethc.exe|subst.exe$”>%WINDIR%\SysNative</directories>

<directories recursion\_level=”0”>%WINDIR%\SysNative\drivers\etc</directories>

<directories recursion\_level=”0” restrict=”WMIC.exe$”>%WINDIR%\SysNative\wbem</directories>

<directories recursion\_level=”0” restrict=”powershell.exe$”>%WINDIR%\SysNative\WindowsPowerShell\v1.0</directories>

<directories recursion\_level=”0” restrict=”winrm.vbs$”>%WINDIR%\SysNative</directories>

<!—32-bit programs. 🡪

<directories recursion\_level=”0” restrict=”at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|net.exe$|net1.exe$|netsh.exe$|reg.exe$|regedit.exe$|regedt32.exe$|regsvr32.exe$|runas.exe$|sc.exe$|schtasks.exe$|sethc.exe$|subst.exe$”>%WINDIR%\System32</directories>

<directories recursion\_level=”0”>%WINDIR%\System32\drivers\etc</directories>

<directories recursion\_level=”0” restrict=”WMIC.exe$”>%WINDIR%\System32\wbem</directories>

<directories recursion\_level=”0” restrict=”powershell.exe$”>%WINDIR%\System32\WindowsPowerShell\v1.0</directories>

<directories recursion\_level=”0” restrict=”winrm.vbs$”>%WINDIR%\System32</directories>

<directories realtime=”yes”>%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup</directories>

<ignore>%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini</ignore>

<ignore type=”sregex”>.log$|.htm$|.jpg$|.png$|.chm$|.pnf$|.evtx$</ignore>

<!—Windows registry entries to monitor. 🡪

<windows\_registry>HKEY\_LOCAL\_MACHINE\Software\Classes\batfile</windows\_registry>

<windows\_registry>HKEY\_LOCAL\_MACHINE\Software\Classes\cmdfile</windows\_registry>

<windows\_registry>HKEY\_LOCAL\_MACHINE\Software\Classes\comfile</windows\_registry>

<windows\_registry>HKEY\_LOCAL\_MACHINE\Software\Classes\exefile</windows\_registry>

<windows\_registry>HKEY\_LOCAL\_MACHINE\Software\Classes\piffile</windows\_registry>

<windows\_registry>HKEY\_LOCAL\_MACHINE\Software\Classes\AllFilesystemObjects</windows\_registry>

<windows\_registry>HKEY\_LOCAL\_MACHINE\Software\Classes\Directory</windows\_registry>

<windows\_registry>HKEY\_LOCAL\_MACHINE\Software\Classes\Folder</windows\_registry>

<windows\_registry arch=”both”>HKEY\_LOCAL\_MACHINE\Software\Classes\Protocols</windows\_registry>

<windows\_registry arch=”both”>HKEY\_LOCAL\_MACHINE\Software\Policies</windows\_registry>

<windows\_registry>HKEY\_LOCAL\_MACHINE\Security</windows\_registry>

<windows\_registry arch=”both”>HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer</windows\_registry>

<windows\_registry>HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services</windows\_registry>

<windows\_registry>HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Session Manager\KnownDLLs</windows\_registry>

<windows\_registry>HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\SecurePipeServers\winreg</windows\_registry>

<windows\_registry arch=”both”>HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run</windows\_registry>

<windows\_registry arch=”both”>HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce</windows\_registry>

<windows\_registry>HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx</windows\_registry>

<windows\_registry arch=”both”>HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\URL</windows\_registry>

<windows\_registry arch=”both”>HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies</windows\_registry>

<windows\_registry arch=”both”>HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows</windows\_registry>

<windows\_registry arch=”both”>HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon</windows\_registry>

<windows\_registry arch=”both”>HKEY\_LOCAL\_MACHINE\Software\Microsoft\Active Setup\Installed Components</windows\_registry>

<!—Windows registry entries to ignore. 🡪

<registry\_ignore>HKEY\_LOCAL\_MACHINE\Security\Policy\Secrets</registry\_ignore>

<registry\_ignore>HKEY\_LOCAL\_MACHINE\Security\SAM\Domains\Account\Users</registry\_ignore>

<registry\_ignore type=”sregex”>\Enum$</registry\_ignore>

<registry\_ignore>HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\MpsSvc\Parameters\AppCs</registry\_ignore>

<registry\_ignore>HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\MpsSvc\Parameters\PortKeywords\DHCP</registry\_ignore>

<registry\_ignore>HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\MpsSvc\Parameters\PortKeywords\IPTLSIn</registry\_ignore>

<registry\_ignore>HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\MpsSvc\Parameters\PortKeywords\IPTLSOut</registry\_ignore>

<registry\_ignore>HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\MpsSvc\Parameters\PortKeywords\RPC-EPMap</registry\_ignore>

<registry\_ignore>HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\MpsSvc\Parameters\PortKeywords\Teredo</registry\_ignore>

<registry\_ignore>HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\PolicyAgent\Parameters\Cache</registry\_ignore>

<registry\_ignore>HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx</registry\_ignore>

<registry\_ignore>HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\ADOVMPPackage\Final</registry\_ignore>

<!—Frequency for ACL checking (seconds) 🡪

<windows\_audit\_interval>60</windows\_audit\_interval>

<!—Nice value for Syscheck module 🡪

<process\_priority>10</process\_priority>

<!—Maximum output throughput 🡪

<max\_eps>100</max\_eps>

<!—Database synchronization settings 🡪

<synchronization>

<enabled>yes</enabled>

<interval>5m</interval>

<max\_interval>1h</max\_interval>

<max\_eps>10</max\_eps>

</synchronization>

<!—End Default syscheck Configurations 🡪

</syscheck>

A screenshot of a computer

Description automatically generated

Hình 27: add syscheck

ở đây mình them vào ở đầu tag <agent\_config os = “window”>, tức là trong group này các hệ điều hành nào là windows sẽ được đỗ các dòng config này vào file ossec.conf. nếu muốn đổ vào các agent chạy os là linux thì làm tương tự.

Thêm Linux vào thì:

<agent\_config>

<syscheck>

<disabled>no</disabled>

<!-- Start Custom syscheck Configurations -->

<!-- Real-Time Monitoring for Windows -->

<directories check\_all="yes" realtime="yes">C:/Temp/</directories>

<directories check\_all="yes" realtime="yes">C:/Windows/Temp</directories>

<directories check\_all="yes" realtime="yes">C:/Users/\*/Downloads/</directories>

<directories check\_all="yes" realtime="yes">C:/Users/\*/Desktop/</directories>

<directories check\_all="yes" realtime="yes">C:/Users/\*/Documents/</directories>

<directories check\_all="yes" realtime="yes">C:/Users/\*/Start Menu/Programs/Startup/</directories>

<!-- Real-Time Monitoring for Linux -->

<directories check\_all="yes" realtime="yes">/etc</directories>

<directories check\_all="yes" realtime="yes">/bin</directories>

<directories check\_all="yes" realtime="yes">/usr/bin</directories>

<directories check\_all="yes" realtime="yes">/sbin</directories>

<directories check\_all="yes" realtime="yes">/usr/sbin</directories>

<directories check\_all="yes" realtime="yes">/home</directories>

<directories check\_all="yes" realtime="yes">/root</directories>

<!-- Start Default syscheck Configurations -->

<!-- Frequency that syscheck is executed (default: every 12 hours) -->

<frequency>43200</frequency>

<!-- Default files to be monitored (Windows) -->

<directories recursion\_level="0" restrict="regedit.exe$|system.ini$|win.ini$">%WINDIR%</directories>

<directories recursion\_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|net.exe$|net1.exe$|netsh.exe$|reg.exe$|regedt32.exe$|regsvr32.exe$|runas.exe$|sc.exe$|schtasks.exe$|sethc.exe$|subst.exe$">%WINDIR%\SysNative</directories>

<directories recursion\_level="0">%WINDIR%\SysNative\drivers\etc</directories>

<directories recursion\_level="0" restrict="WMIC.exe$">%WINDIR%\SysNative\wbem</directories>

<directories recursion\_level="0" restrict="powershell.exe$">%WINDIR%\SysNative\WindowsPowerShell\v1.0</directories>

<directories recursion\_level="0" restrict="winrm.vbs$">%WINDIR%\SysNative</directories>

<!-- 32-bit programs (Windows) -->

<directories recursion\_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|net.exe$|net1.exe$|netsh.exe$|reg.exe$|regedit.exe$|regedt32.exe$|regsvr32.exe$|runas.exe$|sc.exe$|schtasks.exe$|sethc.exe$|subst.exe$">%WINDIR%\System32</directories>

<directories recursion\_level="0">%WINDIR%\System32\drivers\etc</directories>

<directories recursion\_level="0" restrict="WMIC.exe$">%WINDIR%\System32\wbem</directories>

<directories recursion\_level="0" restrict="powershell.exe$">%WINDIR%\System32\WindowsPowerShell\v1.0</directories>

<directories recursion\_level="0" restrict="winrm.vbs$">%WINDIR%\System32</directories>

<directories realtime="yes">%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup</directories>

<ignore>%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini</ignore>

<ignore type="sregex">.log$|.htm$|.jpg$|.png$|.chm$|.pnf$|.evtx$</ignore>

<!-- Windows registry entries to monitor -->

<windows\_registry>HKEY\_LOCAL\_MACHINE\Software\Classes\batfile</windows\_registry>

<windows\_registry>HKEY\_LOCAL\_MACHINE\Software\Classes\cmdfile</windows\_registry>

<windows\_registry>HKEY\_LOCAL\_MACHINE\Software\Classes\comfile</windows\_registry>

<windows\_registry>HKEY\_LOCAL\_MACHINE\Software\Classes\exefile</windows\_registry>

<windows\_registry>HKEY\_LOCAL\_MACHINE\Software\Classes\piffile</windows\_registry>

<windows\_registry>HKEY\_LOCAL\_MACHINE\Software\Classes\AllFilesystemObjects</windows\_registry>

<windows\_registry>HKEY\_LOCAL\_MACHINE\Software\Classes\Directory</windows\_registry>

<windows\_registry>HKEY\_LOCAL\_MACHINE\Software\Classes\Folder</windows\_registry>

<windows\_registry arch="both">HKEY\_LOCAL\_MACHINE\Software\Classes\Protocols</windows\_registry>

<windows\_registry arch="both">HKEY\_LOCAL\_MACHINE\Software\Policies</windows\_registry>

<windows\_registry>HKEY\_LOCAL\_MACHINE\Security</windows\_registry>

<windows\_registry arch="both">HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer</windows\_registry>

<windows\_registry>HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services</windows\_registry>

<windows\_registry>HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Session Manager\KnownDLLs</windows\_registry>

<windows\_registry>HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\SecurePipeServers\winreg</windows\_registry>

<windows\_registry arch="both">HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run</windows\_registry>

<windows\_registry arch="both">HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce</windows\_registry>

<windows\_registry>HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx</windows\_registry>

<windows\_registry arch="both">HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\URL</windows\_registry>

<windows\_registry arch="both">HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies</windows\_registry>

<windows\_registry arch="both">HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows</windows\_registry>

<windows\_registry arch="both">HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon</windows\_registry>

<windows\_registry arch="both">HKEY\_LOCAL\_MACHINE\Software\Microsoft\Active Setup\Installed Components</windows\_registry>

<!-- Windows registry entries to ignore -->

<registry\_ignore>HKEY\_LOCAL\_MACHINE\Security\Policy\Secrets</registry\_ignore>

<registry\_ignore>HKEY\_LOCAL\_MACHINE\Security\SAM\Domains\Account\Users</registry\_ignore>

<registry\_ignore type="sregex">\\Enum$</registry\_ignore>

<registry\_ignore>HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\MpsSvc\Parameters\AppCs</registry\_ignore>

<registry\_ignore>HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\MpsSvc\Parameters\PortKeywords\DHCP</registry\_ignore>

<registry\_ignore>HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\MpsSvc\Parameters\PortKeywords\IPTLSIn</registry\_ignore>

<registry\_ignore>HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\MpsSvc\Parameters\PortKeywords\IPTLSOut</registry\_ignore>

<registry\_ignore>HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\MpsSvc\Parameters\PortKeywords\RPC-EPMap</registry\_ignore>

<registry\_ignore>HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\MpsSvc\Parameters\PortKeywords\Teredo</registry\_ignore>

<registry\_ignore>HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\PolicyAgent\Parameters\Cache</registry\_ignore>

<registry\_ignore>HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx</registry\_ignore>

<registry\_ignore>HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\ADOVMPPackage\Final</registry\_ignore>

<!-- Frequency for ACL checking (seconds) -->

<windows\_audit\_interval>60</windows\_audit\_interval>

<!-- Nice value for Syscheck module -->

<process\_priority>10</process\_priority>

<!-- Maximum output throughput -->

<max\_eps>100</max\_eps>

<!-- Database synchronization settings -->

<synchronization>

<enabled>yes</enabled>

<interval>5m</interval>

<max\_interval>1h</max\_interval>

<max\_eps>10</max\_eps>

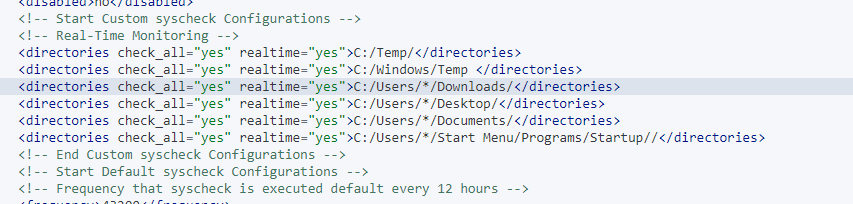
</synchronization>

<!-- End Default syscheck Configurations -->

</syscheck>

</agent\_config>

Các script trong đây được lấy trên Document của wazuh, khi lấy về cần phải sửa lại 1 ít ở phần sau:



Hình 28: chỉnh lại sao cho phù hợp

Ta thêm vào dòng:

<directories check\_all=”yes” realtime=”yes”>C:/Temp/</directories>

Để check các file đã được them, sửa, xóa ở đường dẫn. Trường realtime là để giám sát theo thời gian thực. vì khi trường này không có hoặc để no thì sẽ rất lâu mới nhận được thông báo file bị chỉnh sửa hoặc them, xóa trên server

Để quản lý file trên linux cũng tương tự. Thay C:/…. Thành etc/… các đường dẫn theo cấu trục cây thư mục của linux

Sau khi Save file xong thì restart lại service trên agent

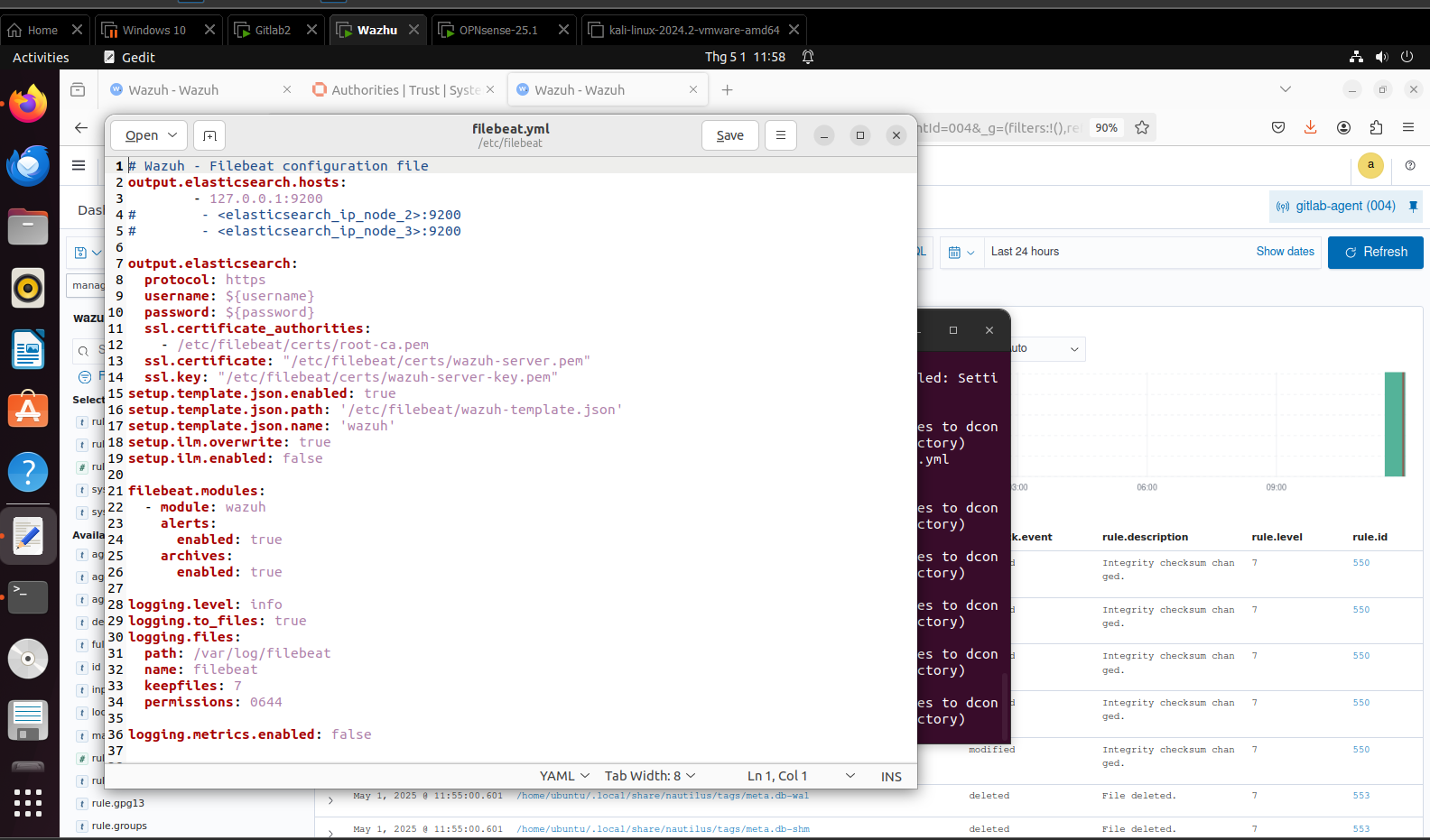
Tạo pattems

A computer screen with a computer screen

Description automatically generated

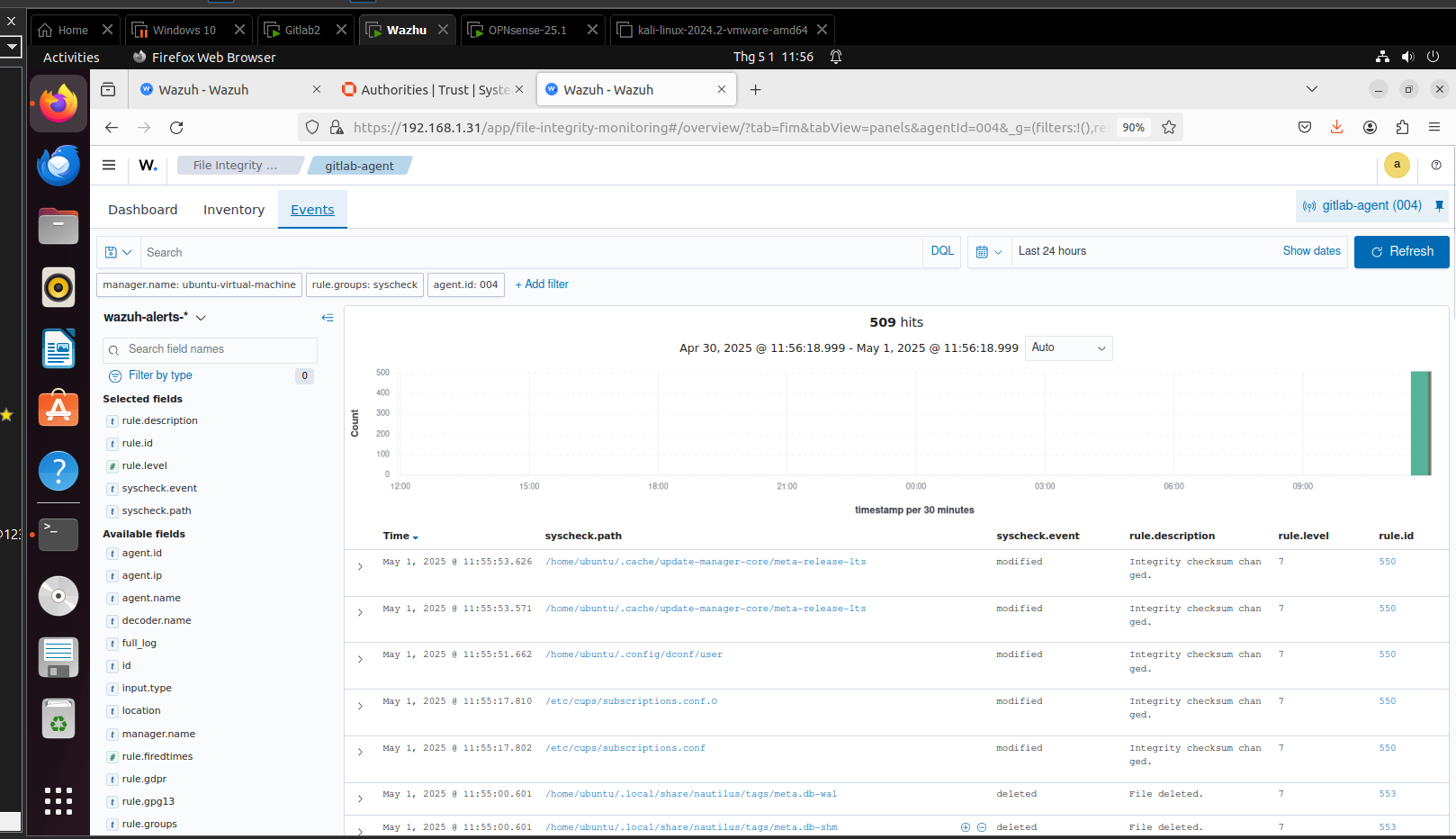
Cấu hình cơ bản trong filebeat.yml

/etc/filebeat/filebeat.yml



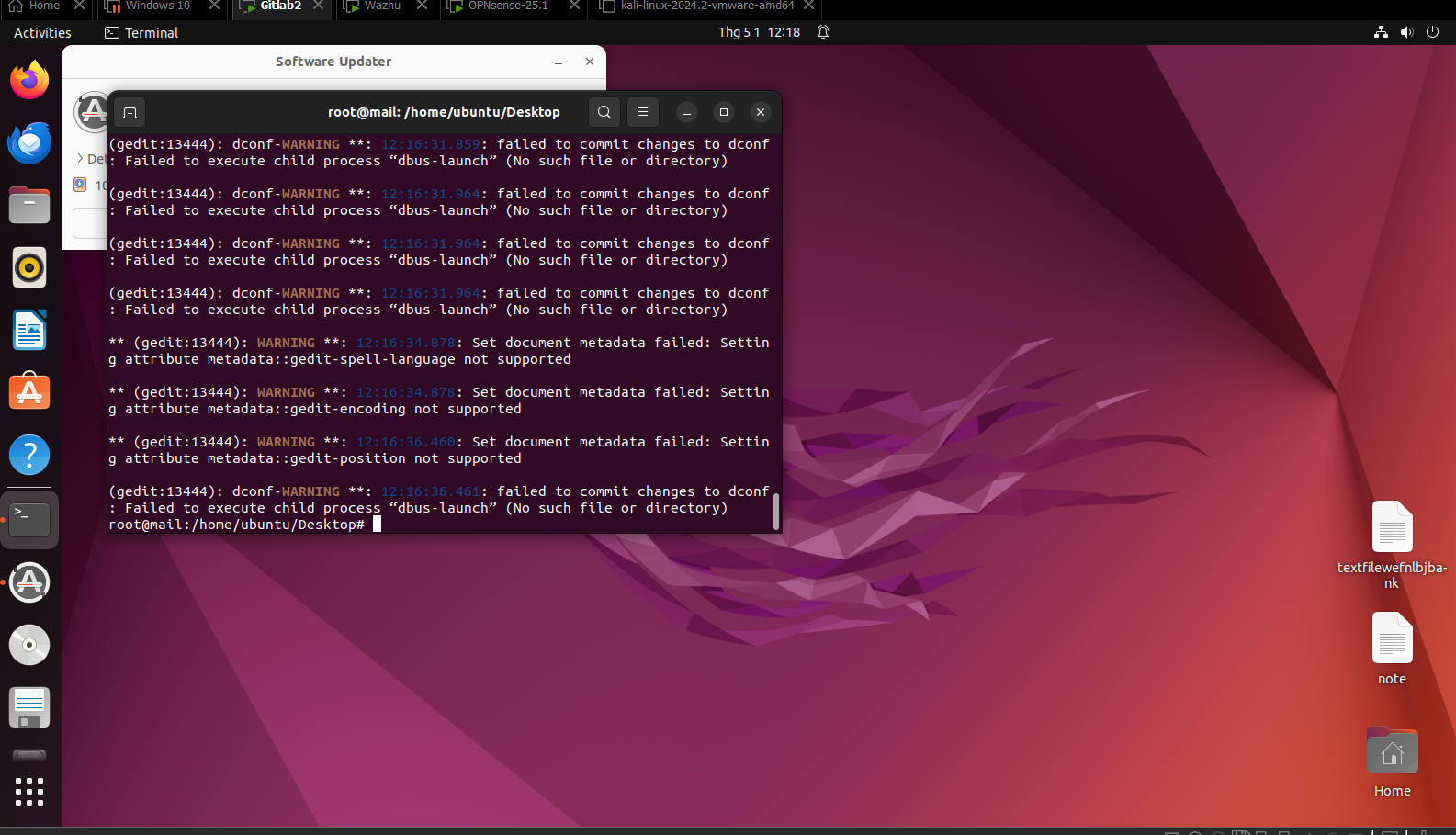
sudo systemctl restart filebeat

Sau khi restart thì agent đã gửi log về server



Hình 29: Cấu hình thành công giám sát file

Thực hiện test thử chức năng



Hình 30: tạo thử 1 thư mục và 1 file text ở ngoài desktop sau đó chỉnh sửa và xóa nó



FIM (File Integrity Monitoring) là một thành phần trong hệ thống giám sát an toàn (như Wazuh, OSSEC) dùng để **phát hiện thay đổi đối với file và thư mục quan trọng trên hệ thống**. Cách hoạt động về nguyên lý như sau:

**Nguyên lý hoạt động của FIM**

1. **Lập danh sách các file cần theo dõi** (từ các thẻ <directories>, <windows\_registry>, v.v.).
2. **Quét ban đầu**:
   * Khi FIM khởi động (hoặc theo chu kỳ cấu hình trong <frequency>, ví dụ 43200s = 12h), nó sẽ:
     + Tính toán **hash (thuật toán SHA1 hoặc SHA256)** cho từng file được theo dõi.
     + Lưu hash này vào **database cục bộ**, gọi là **Syscheck DB** (syscheck là module FIM của Wazuh/OSSEC).

**File hash cũ lưu ở đâu?**

* + Trong Linux: thường ở file **/var/ossec/queue/syscheck/syscheck** (nhị phân).
  + Cấu trúc lưu trữ là một database nội bộ, không thể đọc thủ công dễ dàng mà do Wazuh quản lý.

1. **Giám sát theo thời gian thực (real-time)**:
   * Nếu bạn bật realtime="yes":
     + Wazuh sử dụng các cơ chế hệ điều hành:
       - Trên **Linux**: inotify hoặc auditd.
       - Trên **Windows**: ReadDirectoryChangesW hoặc Windows API tương tự.
     + Khi có sự kiện (file bị thay đổi, thêm, xóa), agent sẽ:
       - Tính lại hash mới của file.
       - So sánh với hash cũ trong database.
       - Nếu khác nhau, **tạo cảnh báo (alert)** gửi về server.
2. **Cảnh báo (Alerting)**:
   * Nếu phát hiện sự khác biệt:
     + Cảnh báo sẽ sinh ra theo mức độ (level) và nội dung chi tiết (tên file, hash cũ, hash mới, quyền file...).
     + Tùy bạn có cấu hình dùng ELK, Splunk, Graylog hay chỉ log đơn thuần thì log sẽ được gửi về đó.

**Các trường hợp sinh cảnh báo**

* Nội dung file thay đổi → hash thay đổi.
* File bị **xóa** hoặc **tạo mới** trong thư mục theo dõi.
* Quyền file (chmod, chown) thay đổi nếu có bật ACL checking.
* Trên Windows, nếu giá trị registry thay đổi.

Hình 31: trên server báo log ngay

* 1. Cài agent ubuntu

<https://documentation.wazuh.com/4.8/installation-guide/packages-list.html>

Chọn bản ubutnu

**Cài đặt gói Wazuh Agent:** Nếu file .deb đã có trong thư mục hiện tại (~/Downloads), bạn có thể cài đặt Wazuh Agent bằng lệnh:

sudo dpkg -i wazuh-agent\_4.8.2-1\_amd64.deb

**Cài đặt các phụ thuộc nếu có lỗi:** Nếu xuất hiện lỗi thiếu phụ thuộc, hãy chạy lệnh sau để cài đặt:

sudo apt-get install -f

**Cấu hình Wazuh Agent:** Sau khi cài đặt xong, bạn cần cấu hình Wazuh Agent để kết nối với Wazuh Manager. Mở file cấu hình ossec.conf và thay đổi thông số server để chỉ định địa chỉ IP của Wazuh Manager.

sudo gedit /var/ossec/etc/ossec.conf

Tìm phần <server> và sửa thành:

<client>

<server>

<address>192.168.1.31</address>

<port>1514</port>

<protocol>tcp</protocol>

</server>

</client>

**Khởi động lại Wazuh Agent:** Sau khi cấu hình xong, bạn khởi động lại dịch vụ Wazuh Agent:

sudo systemctl restart wazuh-agent

sudo systemctl enable wazuh-agent

sudo systemctl start wazuh-agent

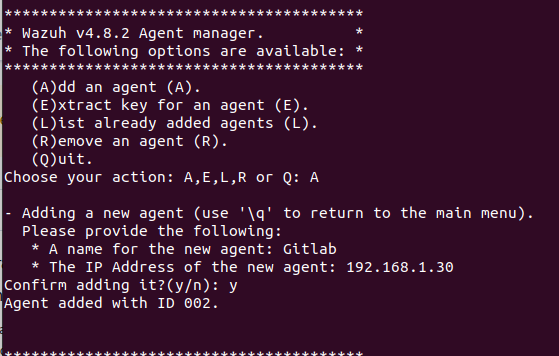
**Trên máy Manager (máy dựng wazuh manager)**:

* Thêm agent vào bằng lệnh:

sudo /var/ossec/bin/manage\_agents

Chọn:

* (A)dd an agent → nhập tên agent → nhập IP → nhận key → copy.



Quay lại máy Agent:

sudo /var/ossec/bin/agent-auth -m <IP\_MAY\_MANAGER> -p 1515 -A <TÊN\_AGENT>

sudo /var/ossec/bin/agent-auth -m 192.168.1.31 -p 1515 -A Gitlab

