WAZUH – SIEM and File Integrity Monitoring

Step-by-Step Installation and Configuration Guide

Contents

Wazuh – SIEM and File Integrity Monitoring

Wazuh is a free and open-source security platform that unifies XDR and SIEM capabilities. It protects workloads across on-premises, virtualized, containerized, and cloud environments.

This document provides a step-by-step guide to install and configure Wazuh File Integrity Monitoring.

Step 1: Installing Prerequisite Packages

Install the required packages.

sudo apt update && sudo apt install curl apt-transport-https unzip wget gnupg -y

```
root@wazhu-s:/home/kboopathi# apt-get install gnupg apt-transport-https
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
gnupg is already the newest version (2.4.4-2ubuntu17.3).
gnupg set to manually installed.
The following NEW packages will be installed:
  apt-transport-https
0 upgraded, 1 newly installed, 0 to remove and 18 not upgraded.
Need to get 3970 B of archives.
After this operation, 36.9 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu noble-updates/universe amd64 apt-transport-https all 2.8.3
Fetched 3970 B in 1s (3081 B/s)
debconf: delaying package configuration, since apt-utils is not installed
Selecting previously unselected package apt-transport-https.
(Reading database ... 73190 files and directories currently installed.)
Preparing to unpack .../apt-transport-https_2.8.3_all.deb ...
Unpacking apt-transport-https (2.8.3) ...
Setting up apt-transport-https (2.8.3) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.
```

Figure 1: Package installation

Step 2: Installing GPG Key on Ubuntu Server

Ensure that packages from the Wazuh repository are trusted by the server.

curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --dearmor -o /usr/share/keyrings/wazuh.gpg

Figure 2: Installing GPG key

Step 3: Add Wazuh Repository

Add the Wazuh repository to your server.

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

Step 4: Update Package Information

sudo apt update

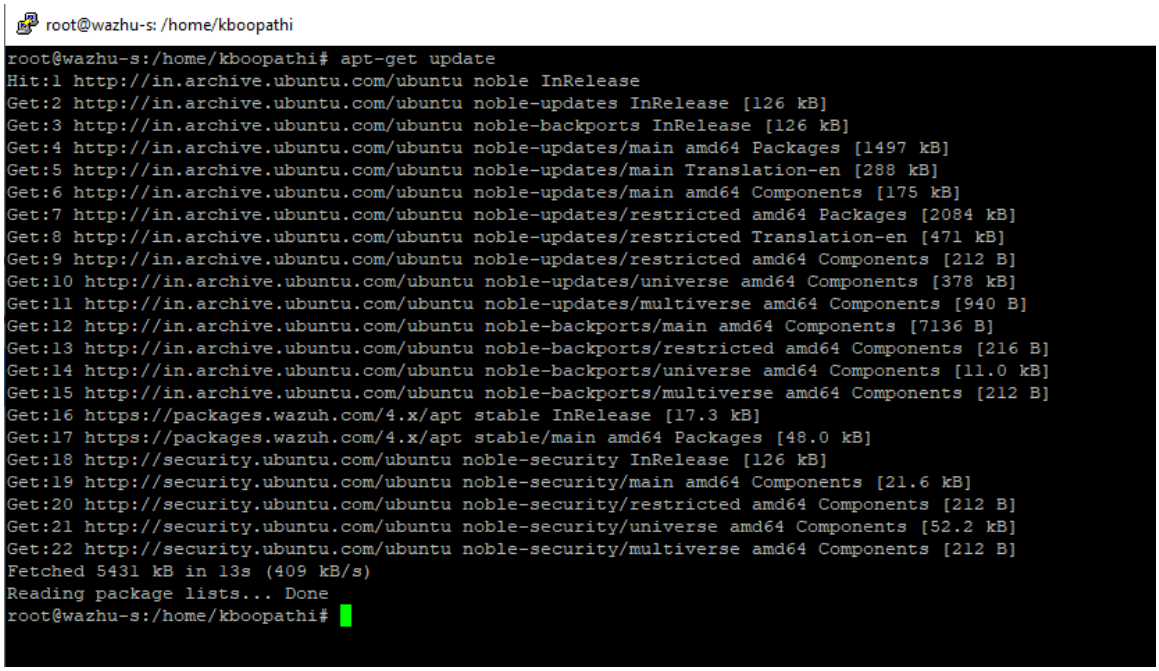

Figure 3: Update packages

Step 5: Execute Installation Script

Download and execute the Wazuh installation script.

curl -sO https://packages.wazuh.com/4.13/wazuh-install.sh
chmod +x wazuh-install.sh
sudo ./wazuh-install.sh

It takes 5–10 minutes to complete. The username and password appear in the logs.

```
-rwxr-xr-x 1 root root 199376 Oct 13 21:11 wazuh-install.sh
root@wazhu-s:/home/kboopathi# ./wazuh-install.sh -a -i
13/10/2025 21:12:19 INFO: Starting Wazuh installation assistant. Wazuh version: 4.13.1
13/10/2025 21:12:19 INFO: Verbose logging redirected to /var/log/wazuh-install.log
13/10/2025 21:12:35 WARNING: Hardware checks ignored.
13/10/2025 21:12:35 INFO: Wazuh web interface port will be 443.
13/10/2025 21:12:52 INFO: --- Dependencies ----
13/10/2025 21:12:52 INFO: Installing debhelper.
13/10/2025 21:13:25 INFO: Wazuh repository added.
13/10/2025 21:13:25 INFO: --- Configuration files ---
13/10/2025 21:13:25 INFO: Generating configuration files.
13/10/2025 21:13:26 INFO: Generating the root certificate.
13/10/2025 21:13:26 INFO: Generating Admin certificates.
13/10/2025 21:13:26 INFO: Generating Wazuh indexer certificates.
13/10/2025 21:13:27 INFO: Generating Filebeat certificates.
13/10/2025 21:13:27 INFO: Generating Wazuh dashboard certificates.
13/10/2025 21:13:28 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation
13/10/2025 21:13:28 INFO: --- Wazuh indexer ---
13/10/2025 21:13:28 INFO: Starting Wazuh indexer installation.
13/10/2025 21:16:47 INFO: Wazuh indexer installation finished.
13/10/2025 21:16:47 INFO: Wazuh indexer post-install configuration finished.
13/10/2025 21:16:47 INFO: Starting service wazuh-indexer.
13/10/2025 21:17:02 INFO: wazuh-indexer service started.
13/10/2025 21:17:02 INFO: Initializing Wazuh indexer cluster security settings.
13/10/2025 21:17:06 INFO: Wazuh indexer cluster security configuration initialized.
13/10/2025 21:17:06 INFO: Wazuh indexer cluster initialized.
13/10/2025 21:17:06 INFO: --- Wazuh server ---
13/10/2025 21:17:06 INFO: Starting the Wazuh manager installation.
13/10/2025 21:19:57 INFO: Wazuh manager installation finished.
13/10/2025 21:19:57 INFO: Wazuh manager vulnerability detection configuration finished.
13/10/2025 21:19:57 INFO: Starting service wazuh-manager.
13/10/2025 21:20:13 INFO: wazuh-manager service started.
13/10/2025 21:20:13 INFO: Starting Filebeat installation.
13/10/2025 21:21:16 INFO: Filebeat installation finished.
13/10/2025 21:21:22 INFO: Filebeat post-install configuration finished.
13/10/2025 21:21:22 INFO: Starting service filebeat.
13/10/2025 21:21:23 INFO: filebeat service started.
13/10/2025 21:21:23 INFO: --- Wazuh dashboard ---
13/10/2025 21:21:23 INFO: Starting Wazuh dashboard installation.
13/10/2025 21:26:50 INFO: Wazuh dashboard installation finished.
13/10/2025 21:26:50 INFO: Wazuh dashboard post-install configuration finished.
13/10/2025 21:26:50 INFO: Starting service wazuh-dashboard.
13/10/2025 21:26:50 INFO: wazuh-dashboard service started.
13/10/2025 21:26:52 INFO: Updating the internal users.
13/10/2025 21:26:55 INFO: A backup of the internal users has been saved in the /etc/wazuh-indexer/internalusers-backup folder.
13/10/2025 21:27:05 INFO: The filebeat.yml file has been updated to use the Filebeat Keystore username and password.
13/10/2025 21:27:36 INFO: Initializing Wazuh dashboard web application.
13/10/2025 21:27:38 INFO: Wazuh dashboard web application initialized.
13/10/2025 21:27:38 INFO: --- Summary ---
13/10/2025 21:27:38 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
    User: admin
    Password: wMHa+FTY7rx?tYD*qN7FBLxzQC53iXGp
13/10/2025 21:27:38 INFO: Installation finished.
root@wazhu-s:/home/kboopathi#
```

4: Installation process

Step 6: Wazuh Console

This is how the Wazuh console looks after a fresh installation.

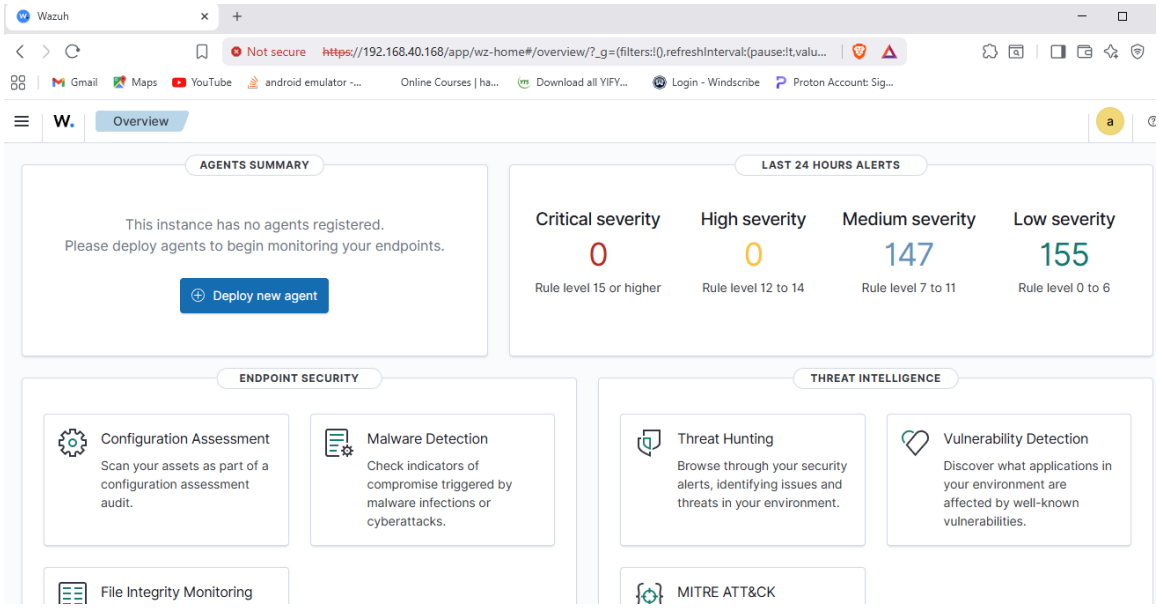

Figure5: Wazuh console

Step 7: Agent Deployment

Download the Wazuh agent from the Deploy New Agent section or from the official site. Install it on Windows.

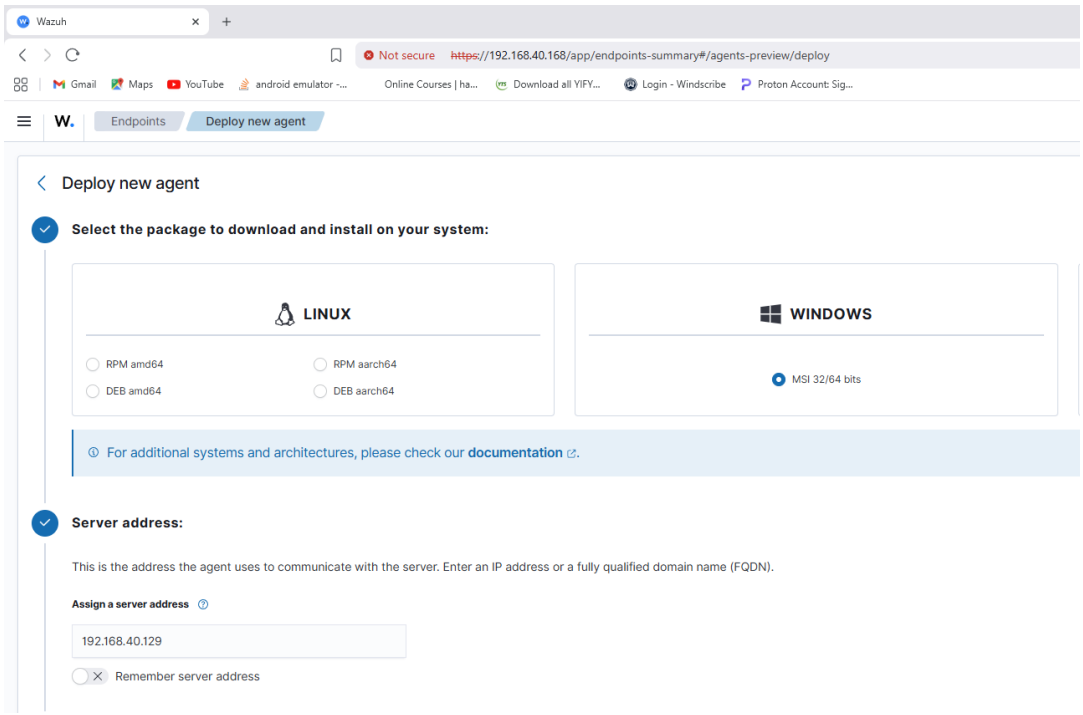

Figure 6a: Wazuh agent deployment

Run the agent configuration interface and provide the Wazuh server IP address and authentication key.

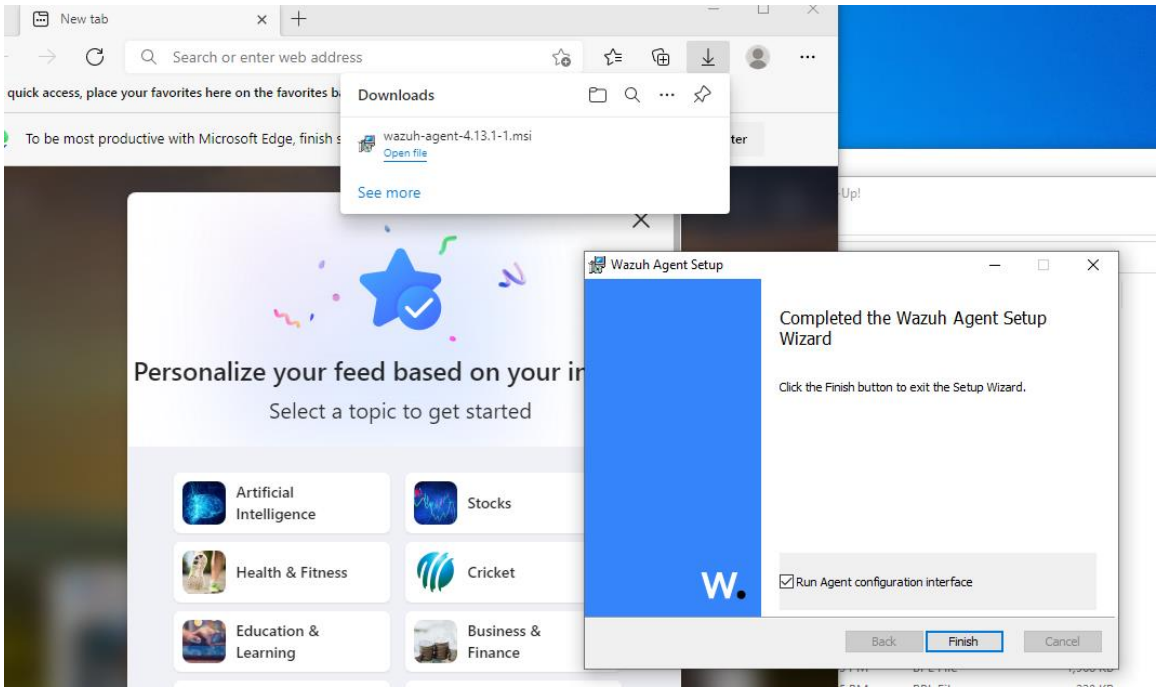

Figure 6b: Wazuh agent deployment

To retrieve the key:

/var/ossec/bin/manage_agents

Use the E option to extract the key by entering the agent name and IP.

```
root@wazhu-s:/home/kboopathi# /var/ossec/bin/manage_agents


****************************************
* Wazuh v4.13.1 Agent manager.         *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: E

Available agents:
   ID: 001, Name: THEPUNISHER, IP: 192.168.10.129
   ID: 002, Name: SPIDERMAN, IP: 192.168.10.130
   ID: 003, Name: HYDRA-DC, IP: 192.168.10.128
Provide the ID of the agent to extract the key (or '\q' to quit):
```

Figure 6c: Wazuh agent deployment

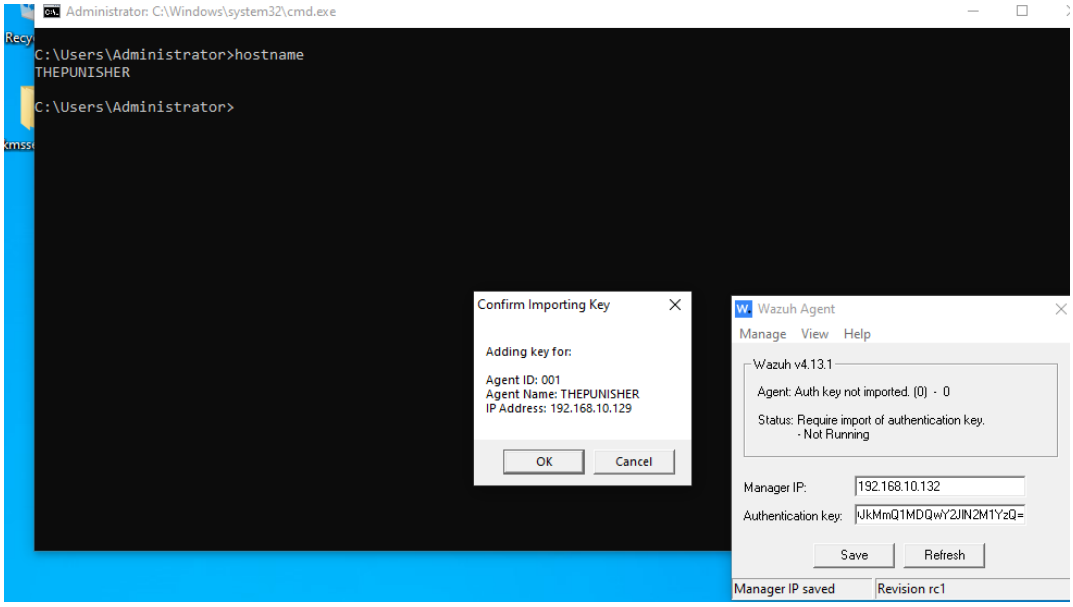

Figure 6d: Wazuh agent deployment

Step 8: Setting up File Integrity Monitoring

Wazuh supports real-time monitoring of file and folder changes using Syscheck.

Edit ossec.conf on the client machine:

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

Add:

```
<syscheck>
 <directories realtime="yes">C:\Users\Administrator\Desktop\wazuh-FIM</directories>
</syscheck>
```

Save and restart the Wazuh agent.

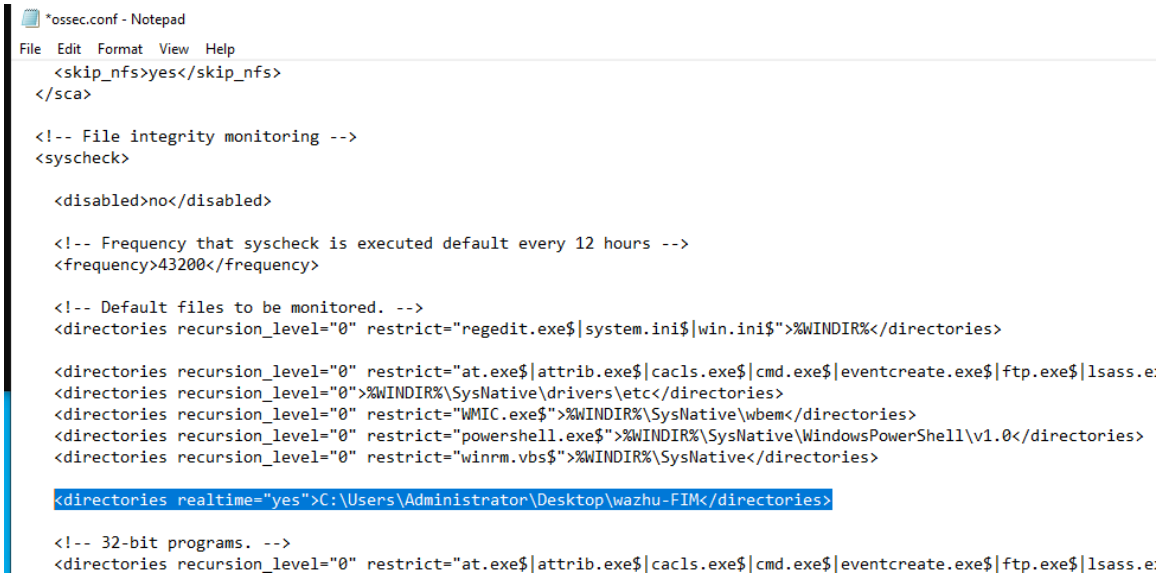

Figure7: FIM setup

Step 9: Creating a Sample File

Create a test file in C:\Users\Administrator\Desktop\wazuh-FIM.

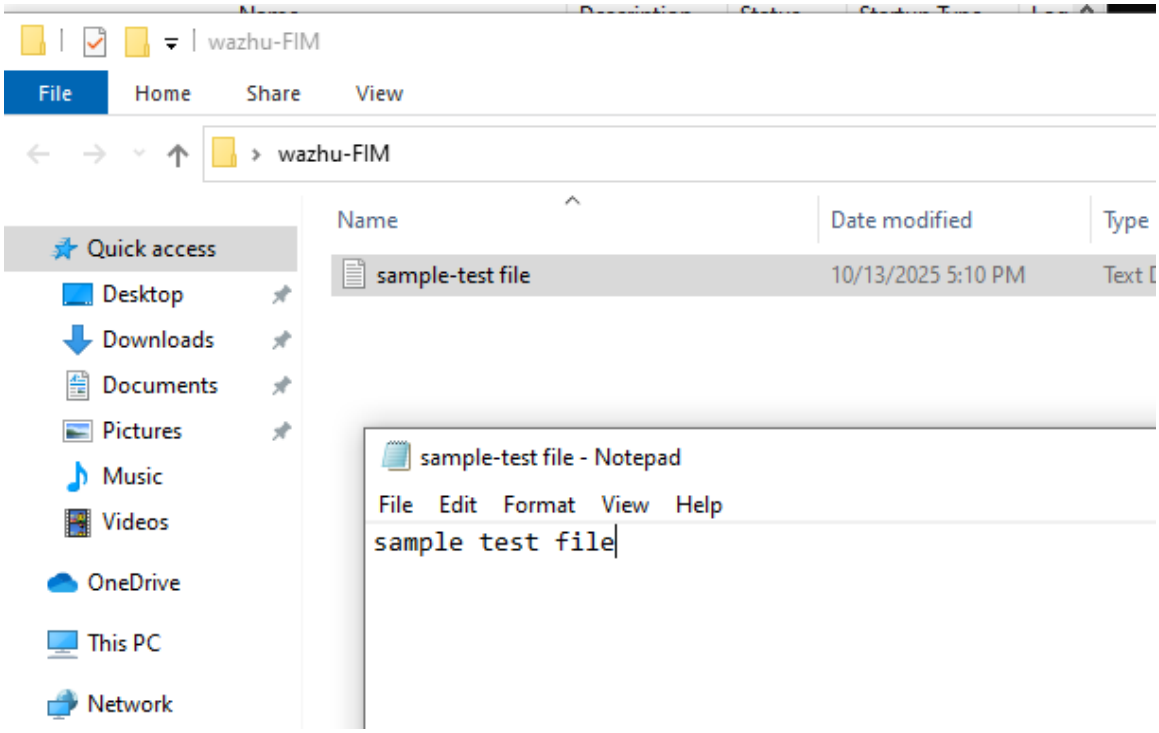

Figure 8: Sample file creation

Step 10: Verifying File Integrity Monitoring Events

When a file is created or modified, alerts appear on the Wazuh dashboard. Directory changes are recorded and reported in real time.

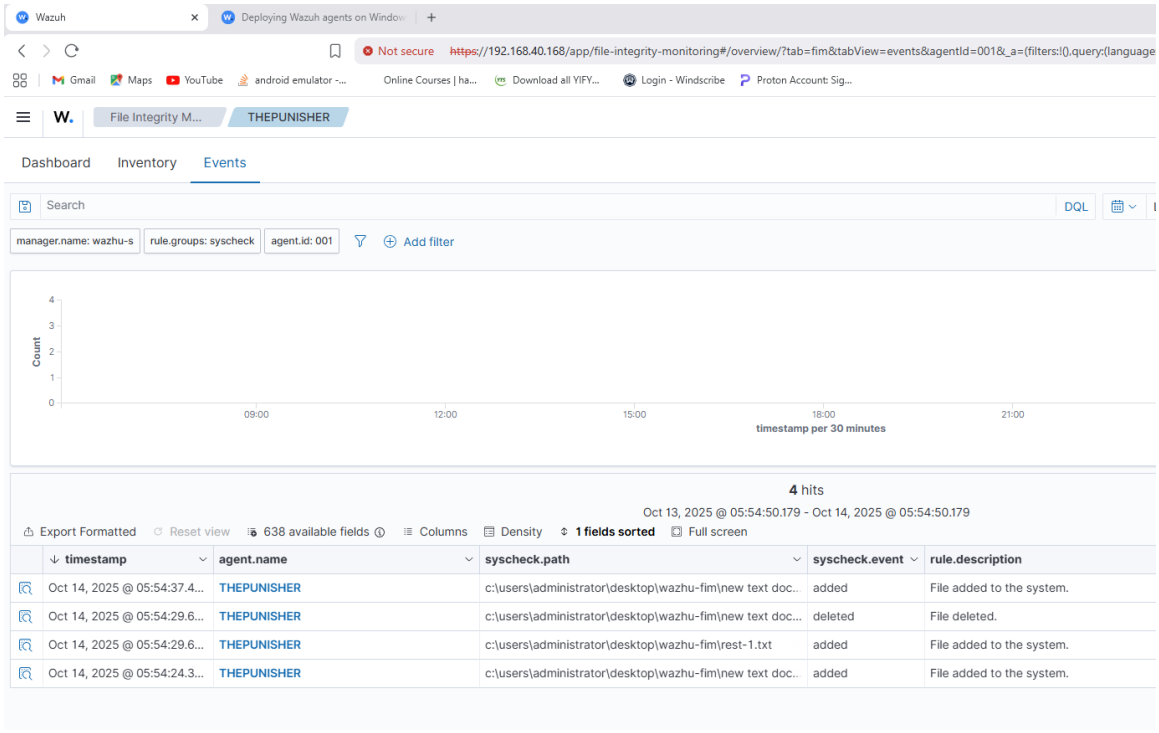

Figure 9: File integrity alert