File Integrity Monitoring (FIM) Using Wazuh

Report Task # 01 (Team IOTA)

SUBMITTED TO :-

Mr. Zain

SUBMITTED BY :-

Nasir Sharif

National University of Modern Languages H-9 Islamabad

31 July 2025

Contents

File Integrity Monitoring (FIM)

Task Overview

Set up Wazuh in your environment, start collecting real-time logs. This task will serve as the foundation for advanced monitoring and traffic analysis in the upcoming phases. As part of this task, you will also configure File Integrity Monitoring (FIM) — a crucial security capability that detects changes to critical system files and directories in real-time. FIM helps identify unauthorized modifications, additions, or deletions, which can be early indicators of compromise or malicious activity. You will monitor specific paths, generate alerts based on file changes, and tune the system to reduce false positives while maintaining visibility.

Objective:

To deploy the Wazuh Security Information and Event Management (SIEM) platform using a virtual appliance (OVA), install and configure agents on Windows and Linux systems, and enable File Integrity Monitoring (FIM) for real-time tracking of file modifications, additions, and deletions. This lab is intended to establish a foundation for security monitoring and traffic analysis in a SOC (Security Operations Center) environment.

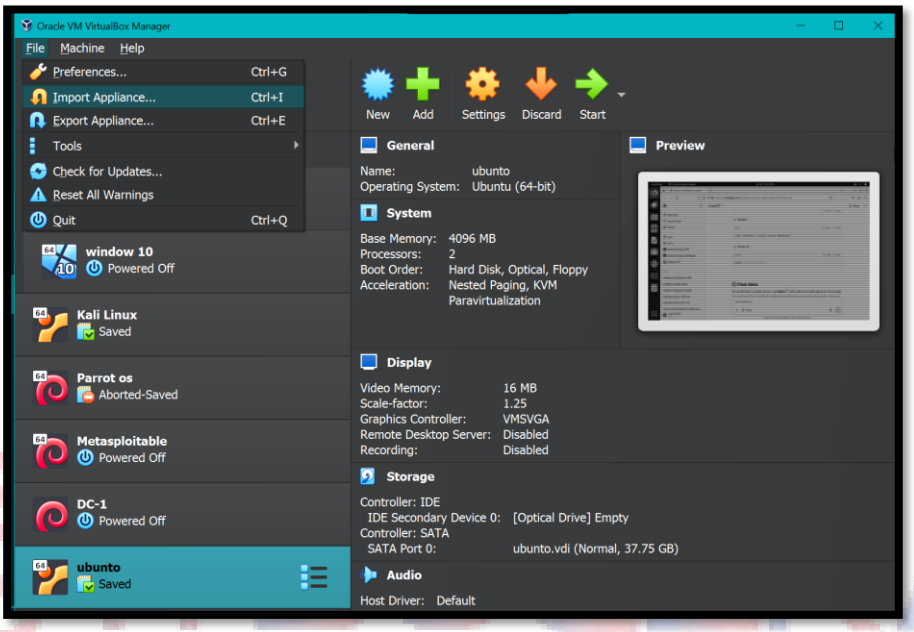
This guide provides **detailed step-by-step instructions** along with **troubleshooting solutions** for potential issues.

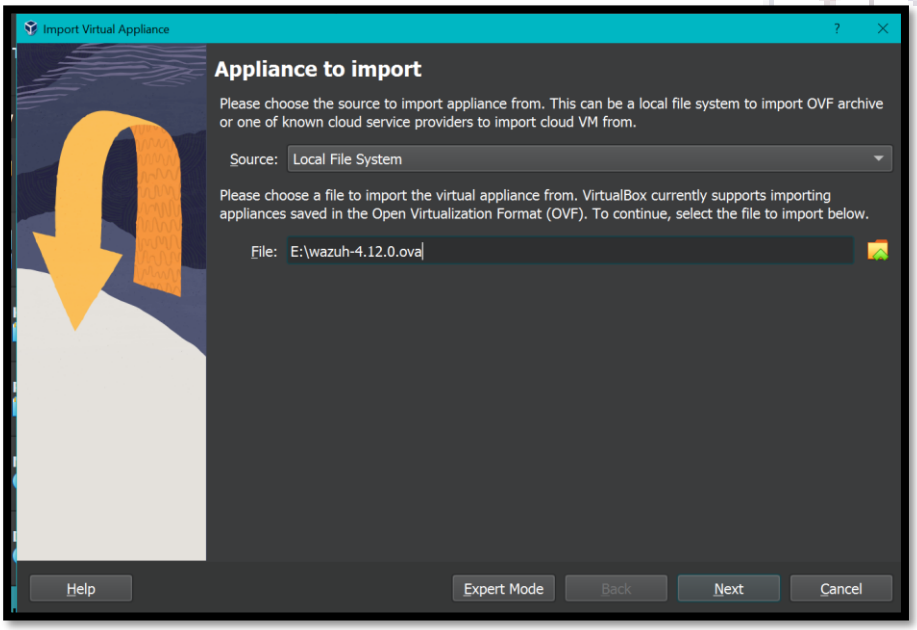
1. Environment Setup

- **Virtualization Software:** Oracle VirtualBox
- **Host OS:** [Insert Host OS e.g., Windows 11]
- **Wazuh Version:** 4.11.2 (OVA)
- **Guest VMs:**
    - Wazuh Server (OVA)
    - Windows 10 VM
    - Ubuntu/Kali Linux VM

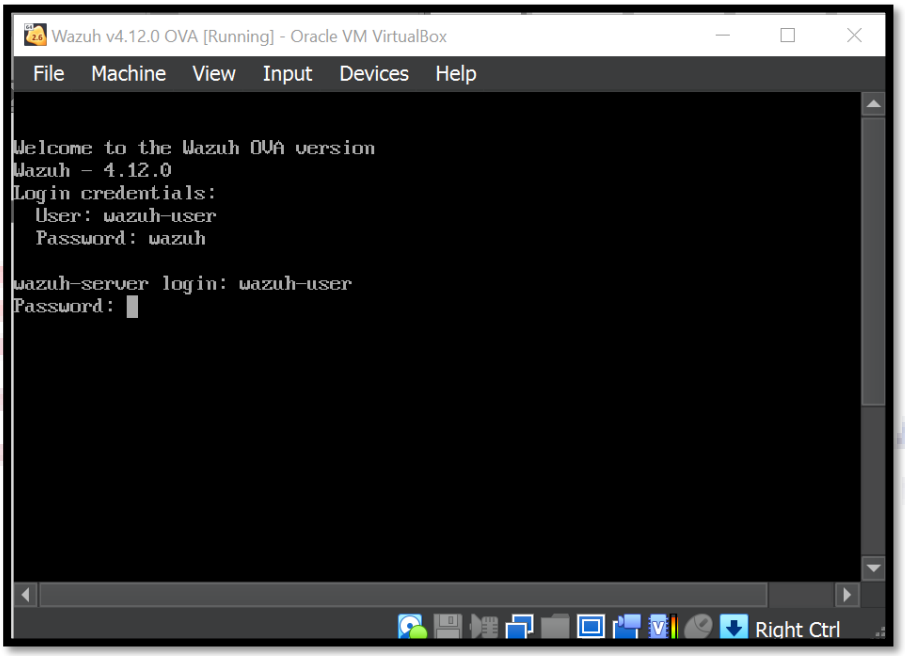
1.1. Wazuh Server Deployment (OVA)

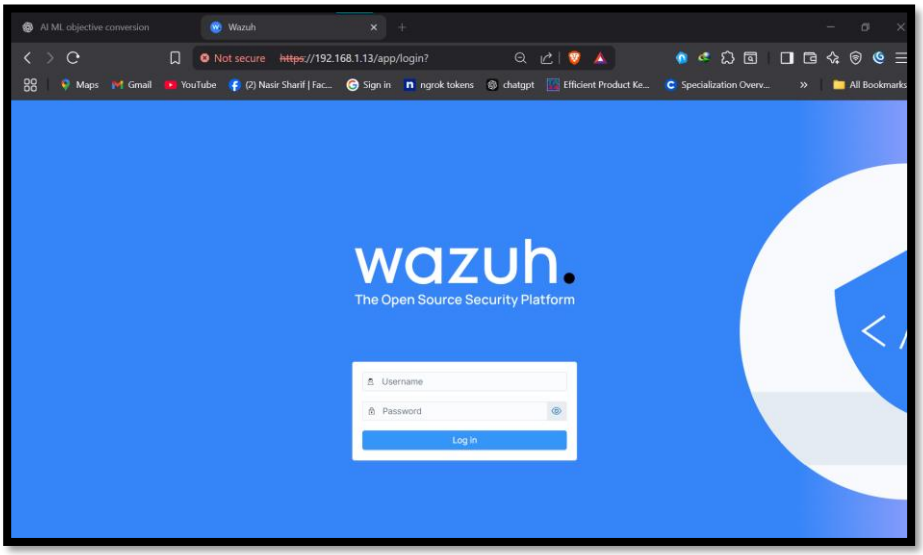
1. Download Wazuh OVA file from: https://documentation.wazuh.com/current/deployment-options/virtual-machine/virtual-machine.html
2. Import the OVA into VirtualBox:
    - File → Import Appliance → Select OVA → Import






Oracle VM VirtualBox Manager
File Machine Help
New group
kali linux
Powered Off
window 10
Powered Off
Kali Linux
Saved
Parrot os
Aborted-Saved
Metasploitable
Powered Off
DC-1
Powered Off
ubunto
New Add Settings Discard Start
Start
General
Name: Wazuh v4.12.0 OVA
Operating System: Linux 2.6 / 3.x / 4.x / 5.x (64-bit)
Preview
Wazuh v4.12.0 OVA
System
Base Memory: 8192 MB
Processors: 4
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization
Display
Video Memory: 16 MB
Graphics Controller: VBoxVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Secondary Device 0: wazuh-4.12.0-disk-1.vdi (Normal, 25.00 GB)
Controller: Floppy
Floppy Device 0: Empty


Wazuh v4.12.0 OVA [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Welcome to the Wazuh OVA version
Wazuh - 4.12.0
Login credentials:
User: wazuh-user
Password: wazuh
wazuh-server login: wazuh-user
Password:
Right Ctrl

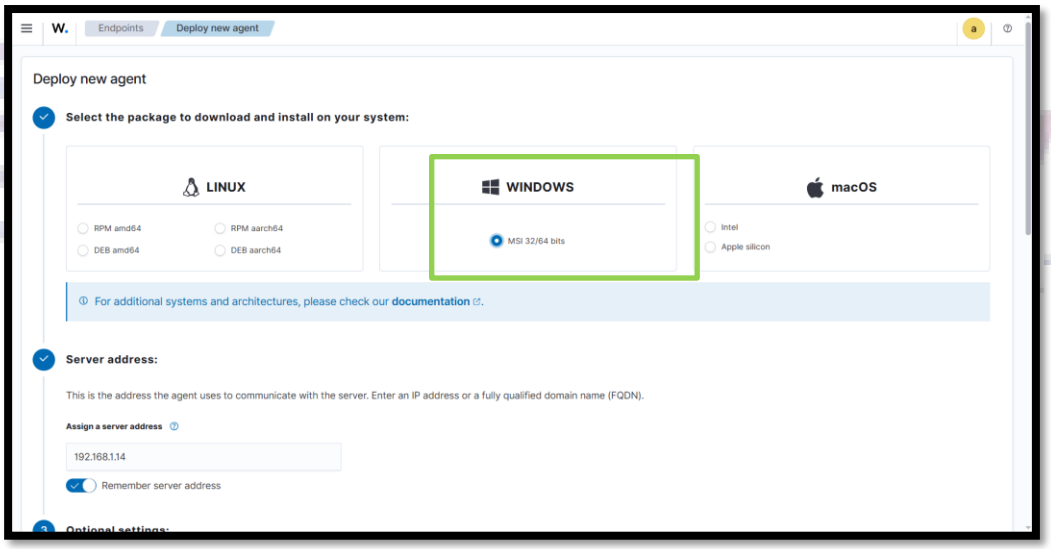

Wazuh
Not secure https://192.168.1.13/app/login?
wazuh.
The Open Source Security Platform
Username
Password
Log in

3. Start the Wazuh VM.
4. Default login credentials:
    - **Username:** wazuh-user
    - **Password:** wazuh
5. Retrieve the Wazuh server IP using ip a inside the VM.
6. Access Wazuh Dashboard from browser: https://<wazuh_server_ip>
    - Login: **admin** / **admin**

1.2. Wazuh Agent Installation

Windows Agent

- Download and install agent via "Deploy New Agent" wizard on Wazuh Dashboard.
- Input Wazuh Manager IP during setup.
- Start the agent using net start wazuh.



Linux Agent (Kali/Ubuntu)

- Deploy agent using Linux package (DEB amd64).
- Run installation commands with sudo rights.
- Register agent to Wazuh Manager.

1.3. File Integrity Monitoring (FIM) Windows Agent FIM Setup

Edit **ossec.conf** located in **C:\Program Files\ossec-agent\ossec.conf**

```
  <!-- File integrity monitoring -->
<syscheck>
  <disabled>no</disabled>
  <frequency>5</frequency>

  <!-- Monitor Desktop folder -->
  <directories check_all="yes" report_changes="yes" realtime="yes">C:\Users\4G Traders\Desktop</directories>

  <!-- Monitor Documents -->
  <directories check_all="yes" report_changes="yes" realtime="yes">C:\Users\4G Traders\Documents</directories>

  <!-- Monitor Startup Programs -->
  <directories realtime="yes">%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup</directories>
  <ignore>%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini</ignore>

  <!-- Ignore common extensions -->
  <ignore type="sregex">.log$|.htm$|.jpg$|.png$|.chm$|.pnf$|.evtx$</ignore>
```

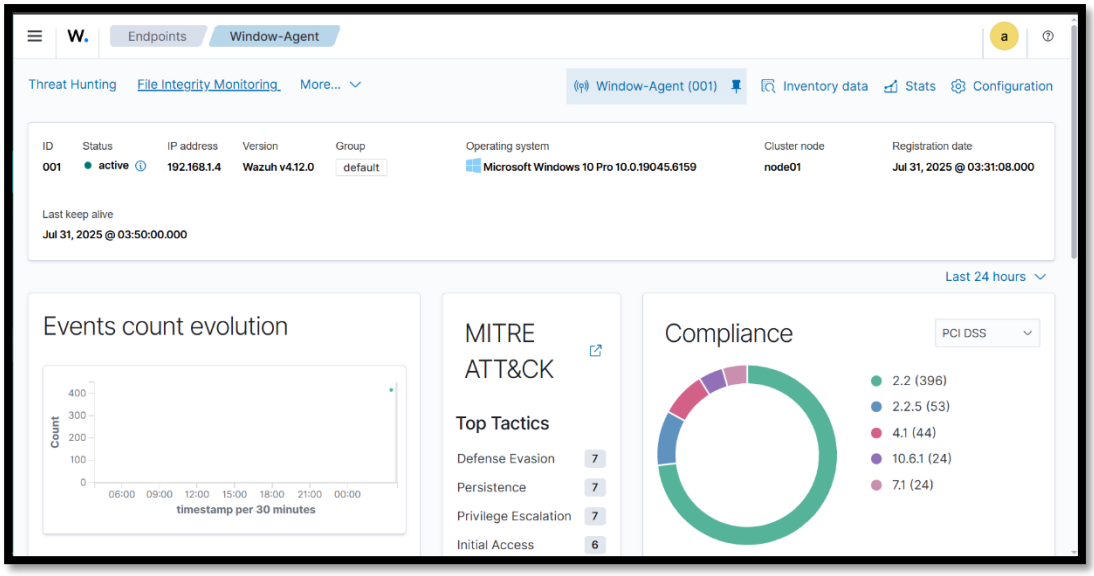
Restart Wazuh Agent:

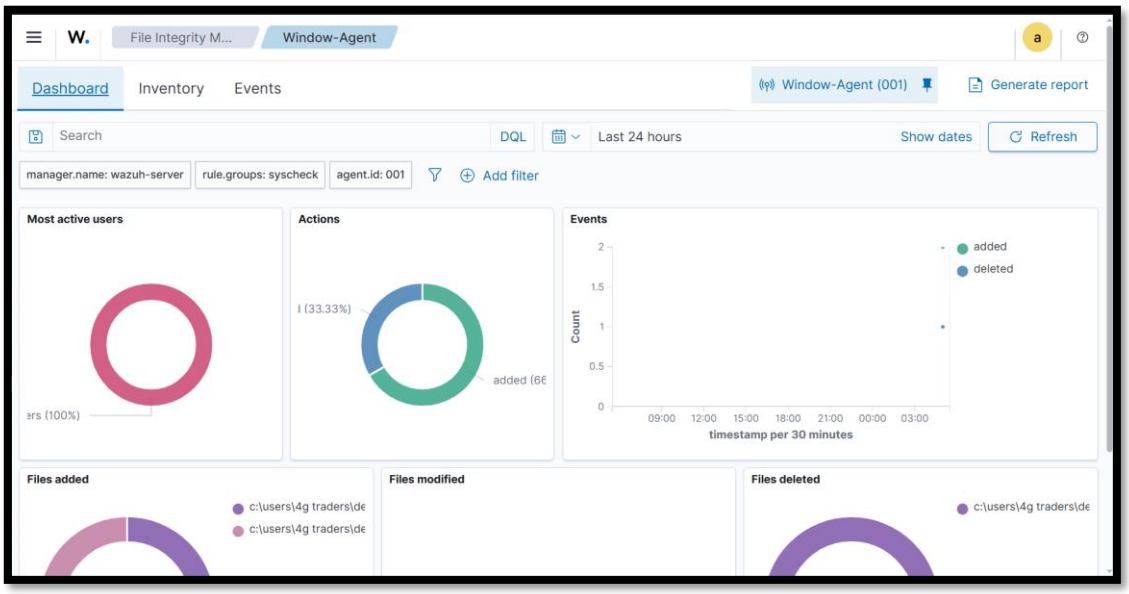
```
net stop wazuh
net start wazuh
```

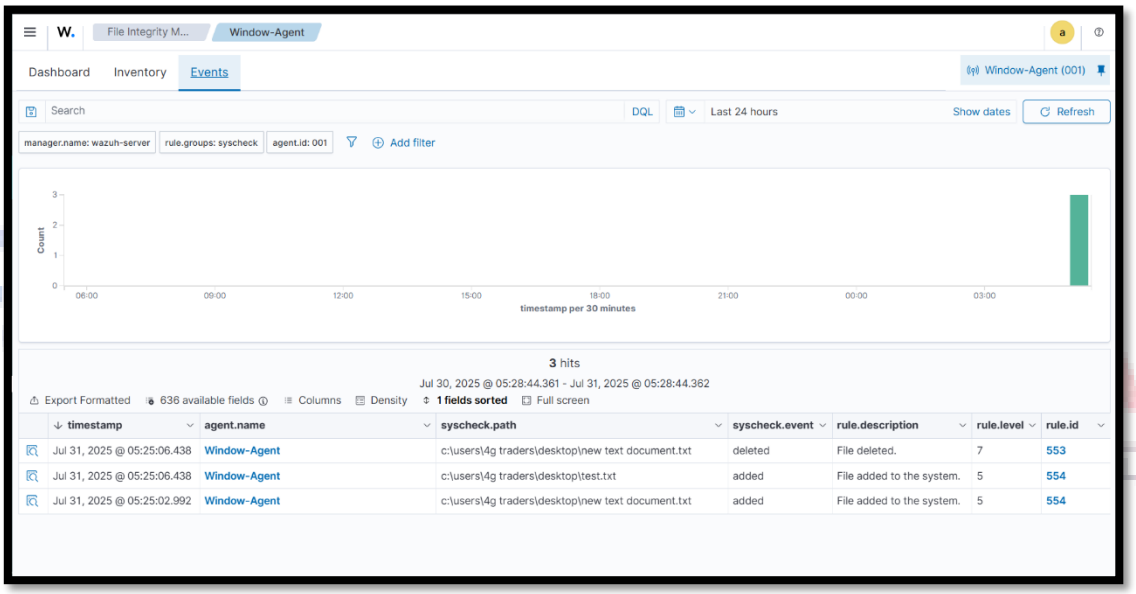
Validation & Monitoring

- Navigate to: Security Events → File Integrity Monitoring
- Apply filter:

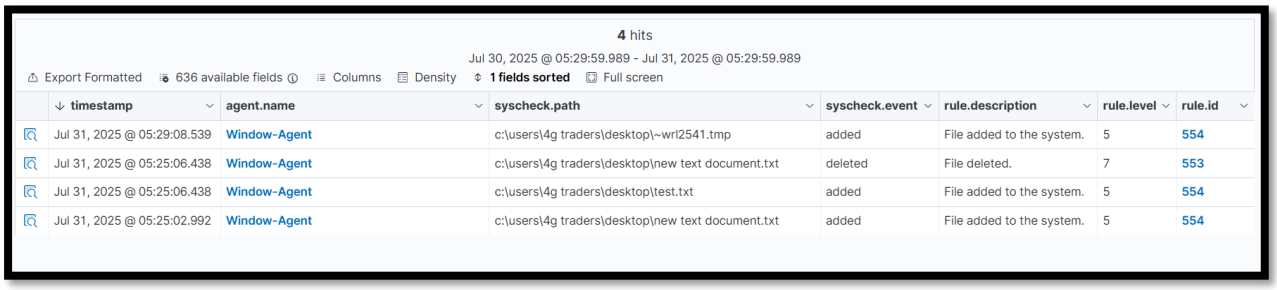
rule.group:FIM
Confirm logs like Created, Modified, Deleted appear.







ALL the changes showing after every 5 Second due to frequency I have set in ossec.conf



Conclusion

- Successfully deployed Wazuh SIEM using pre-built OVA.
- Installed Wazuh agents on Windows and Linux systems.
- Enabled and verified File Integrity Monitoring.
- Captured file activity logs in real-time.
- Dashboard and log data confirmed agent communication and FIM functionality.

The complete the foundational setup for advanced monitoring and threat detection using Wazuh.