1. Setting Up Wazuh OVA in VMware

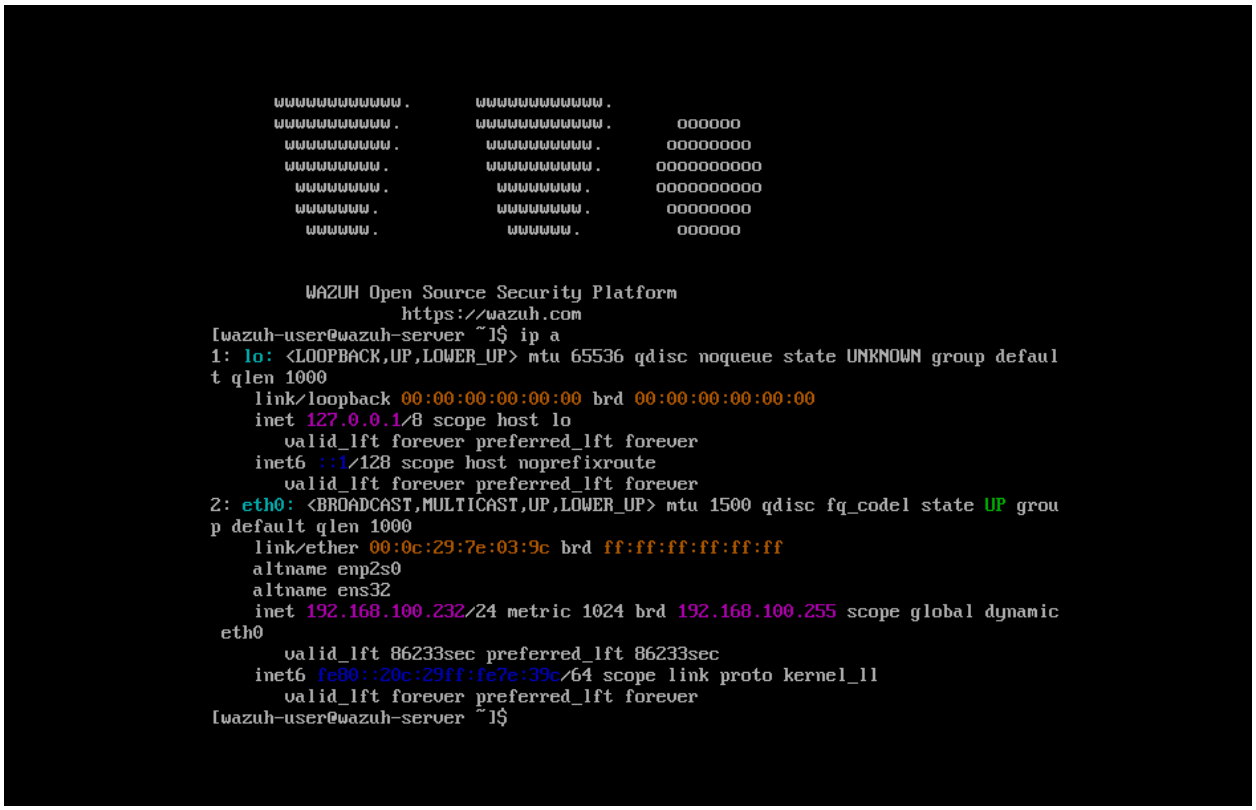
To begin the process, I downloaded the Wazuh OVA (Open Virtual Appliance) from the official Wazuh website. This OVA contains a pre-configured virtual machine with Wazuh manager, Elasticsearch, and the web interface all bundled together.

Once downloaded, I imported the OVA into VMware Workstation. The setup process was straightforward:
-> Open VMware Workstation
- >Click on 'Open a Virtual Machine'
- >Select the downloaded .ova file
- >Follow the prompts to import the virtual appliance

After the import, I powered on the virtual machine. It booted into a preconfigured Linux environment with Wazuh running. Once the system finished loading,
Then i entered the command

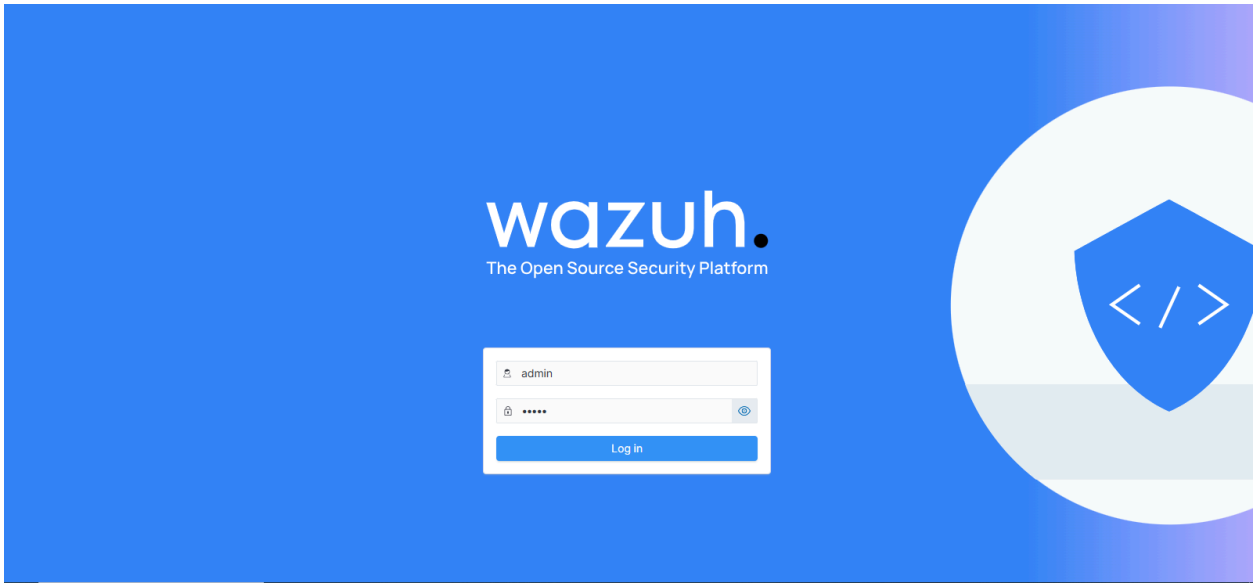
Ip a

This command gave me the the ip
I noted the assigned IP address (e.g., 192.168.100.232), which I used later to access the Wazuh dashboard from my host machine.



2. Accessing the Wazuh Dashboard

To begin, I accessed the Wazuh dashboard hosted on the IP address 192.168.100.232. This was done via a browser by navigating to: https://192.168.100.232. Once I entered the login credentials, I successfully reached the Wazuh web interface.

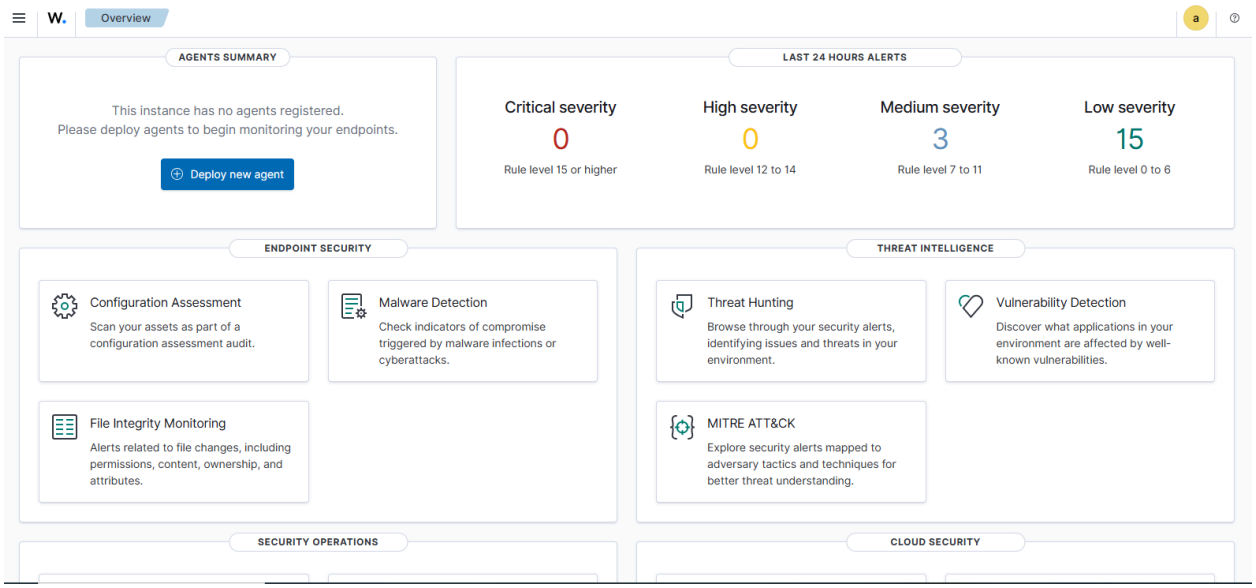


After entering the credentials:

Username: admin

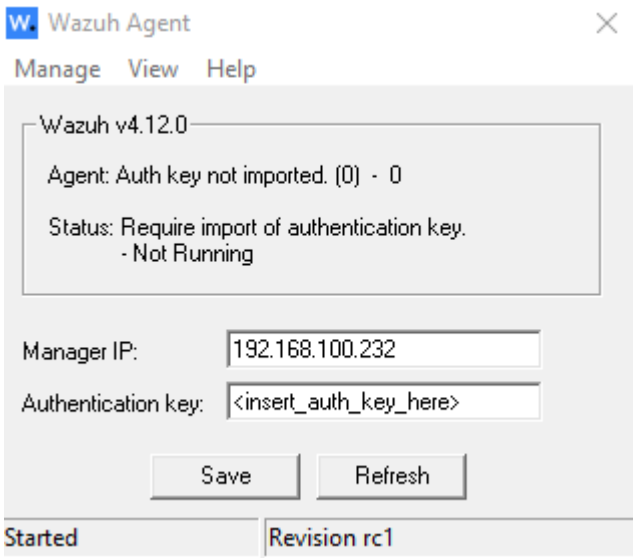
Password: admin

I accessed the wazuh dashboard



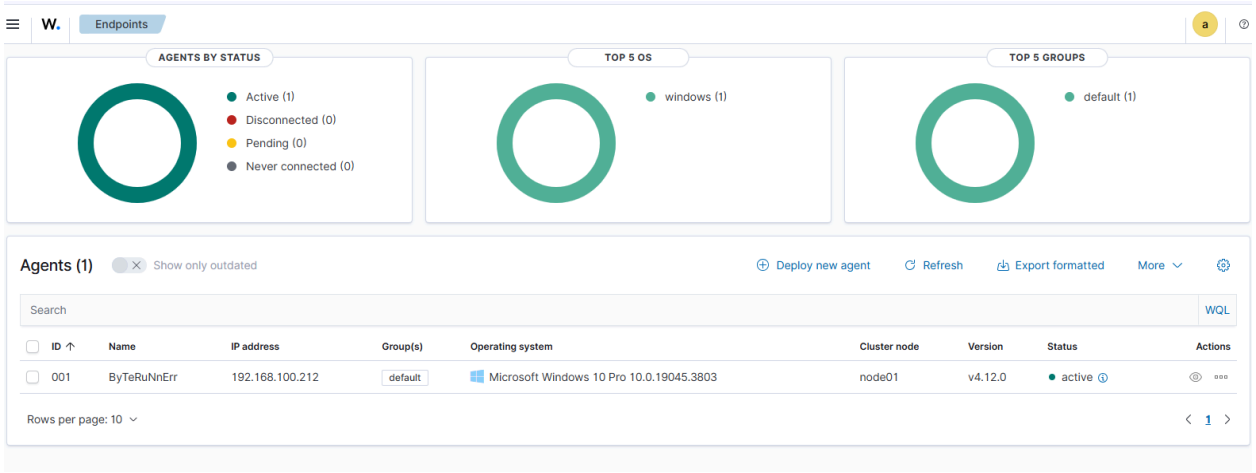
3. Installing the Wazuh Agent (Windows)

From the official Wazuh documentation site, I downloaded the Windows agent installer. After completing the installation wizard, I configured the agent by entering the IP address of my Wazuh manager (192.168.100.232) to enable communication between the agent and the manager.



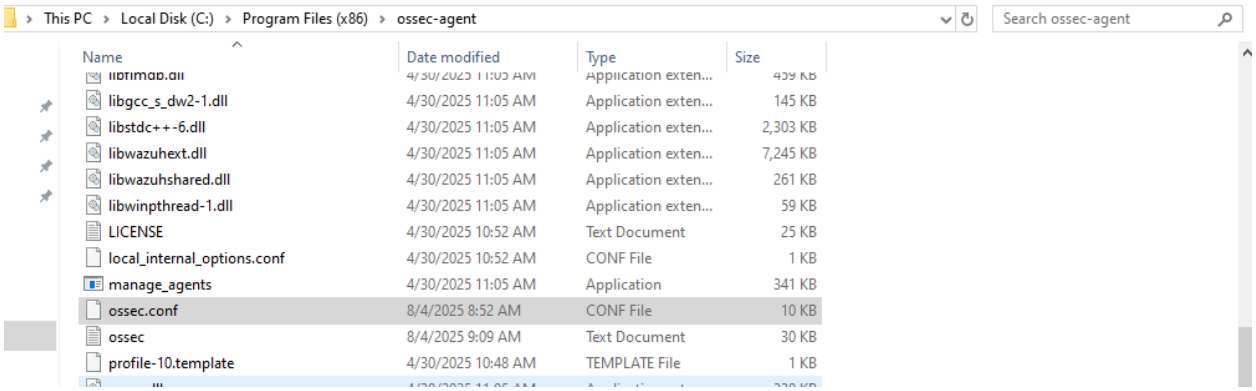
4. Connecting the Agent to the Manager

After installation, I launched the agent service. Shortly afterward, I could see my Windows agent appearing on the Wazuh dashboard under the Agents section. The agent status changed from 'Never connected' to 'Active', confirming successful registration.



5. Configuring File Integrity Monitoring

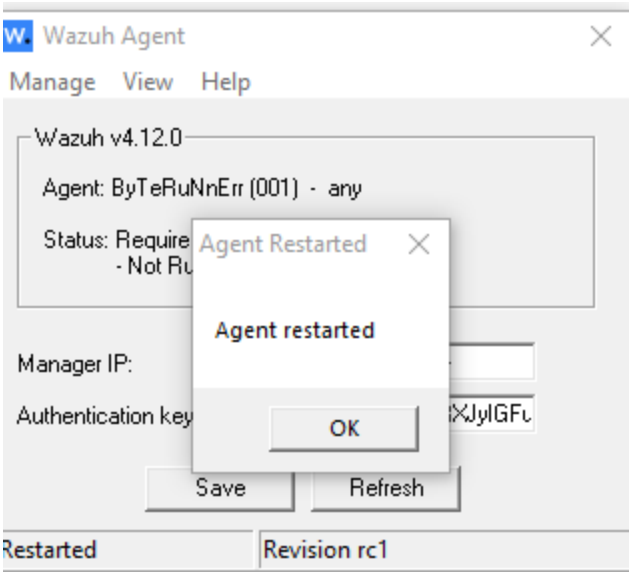
Next, I configured the agent to monitor a specific directory on my Windows machine. To do this, I located the configuration file at: C:\Program Files (x86)\ossec-agent\ossec.conf.



I opened this file using Notepad with administrator privileges. Inside the <ossec_config> block, I added the path to specify the folder to monitor:

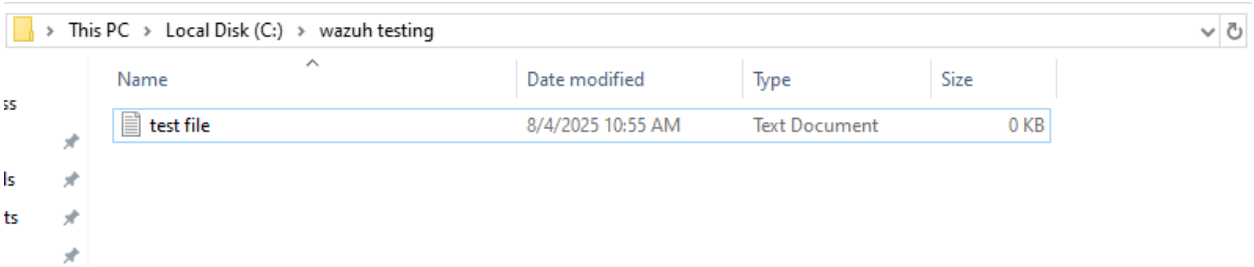
```
<!-- 32-bit programs. -->
<directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|net.exe$|net1.exe$|ne
<directories recursion_level="0">%WINDIR%\System32\drivers\etc</directories>
<directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\System32\wbem</directories>
<directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\System32\WindowsPowerShell\v1.0</directories>
<directories check_all="yes" report_changes="yes" realtime="yes">C:\wazuh testing</directories>
<directories recursion_level="0" restrict="winrm.vbs$">%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>
```

After saving the file, I restarted the agent service to apply the new monitoring configuration.



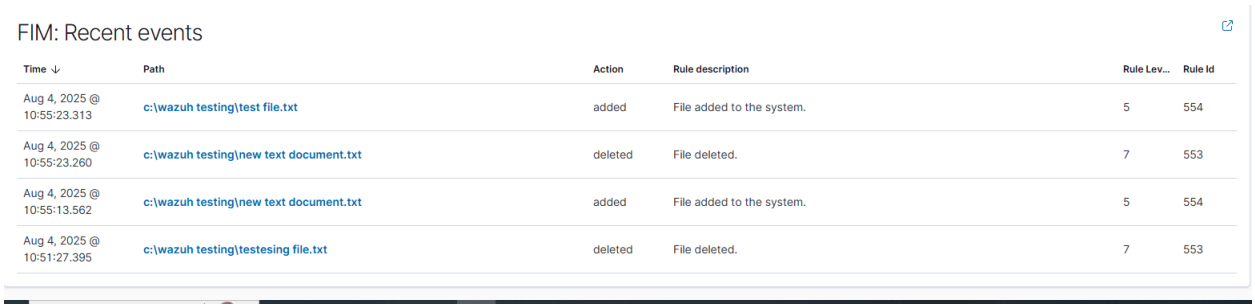
6. Testing File Monitoring

To ensure everything was working as expected, I created a sample file named 'testfile.txt' in the monitored directory. This file creation was intended to trigger a monitoring event.



7. Verifying Logs on the Dashboard

Returning to the Wazuh dashboard, I opened the Security Events section and filtered by my agent. I observed that the new file event had been logged successfully. This confirmed that Wazuh detected the change and recorded it as expected.



8. Conclusion:

Overall, the Wazuh agent was installed and connected to the manager without issues. File integrity monitoring was set up effectively, and changes within the configured directory were successfully detected and logged. This task reinforced my understanding of endpoint monitoring and gave me practical experience with Wazuh’s configuration and capabilities.