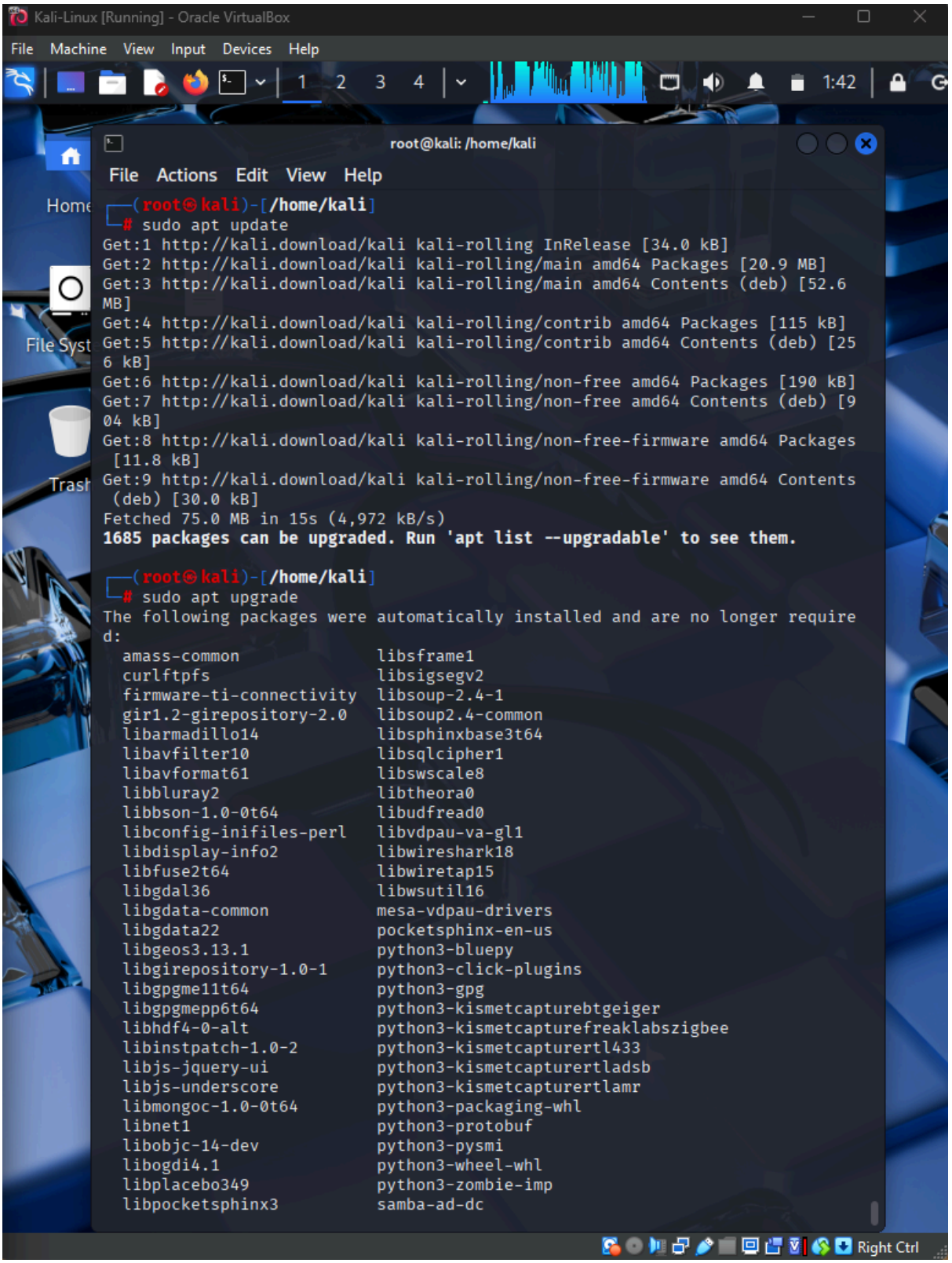
Installations Tasks Section

1. Making sure Linux OS is up to date before starting any new software installation
Commands used:

sudo apt update

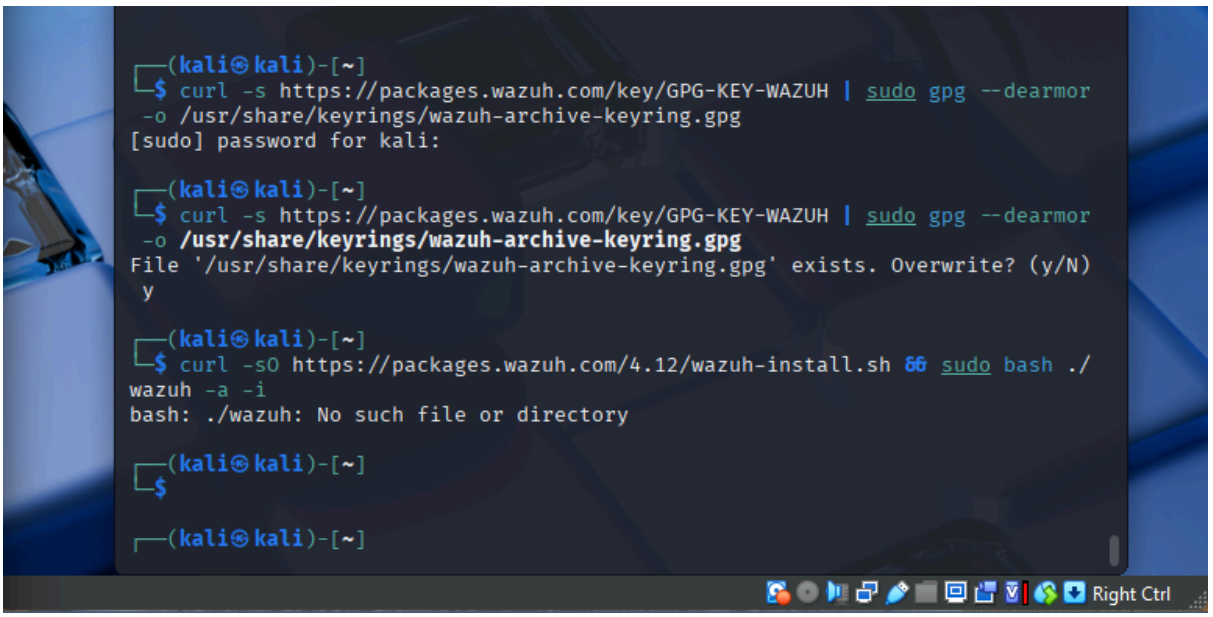
sudo apt upgrade



2. Installing the Wazuh Manager (Linux)

2.1 Add Wazuh GPG Key
Command used:

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



This adds the GPG key to verify Wazuh packages.

2.2 Download and Execute Wazuh Installation Script
Commands used:

curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh && sudo bash ./wazuh-install.sh -a -i

- -a: Installs all components (manager, indexer, etc..)
- -i: Runs in interactive mode

The script installs all required services and configures them automatically.

Kali-Linux [Running] - Oracle VirtualBox

File Machine View Input Devices Help

root@kali: /home/kali

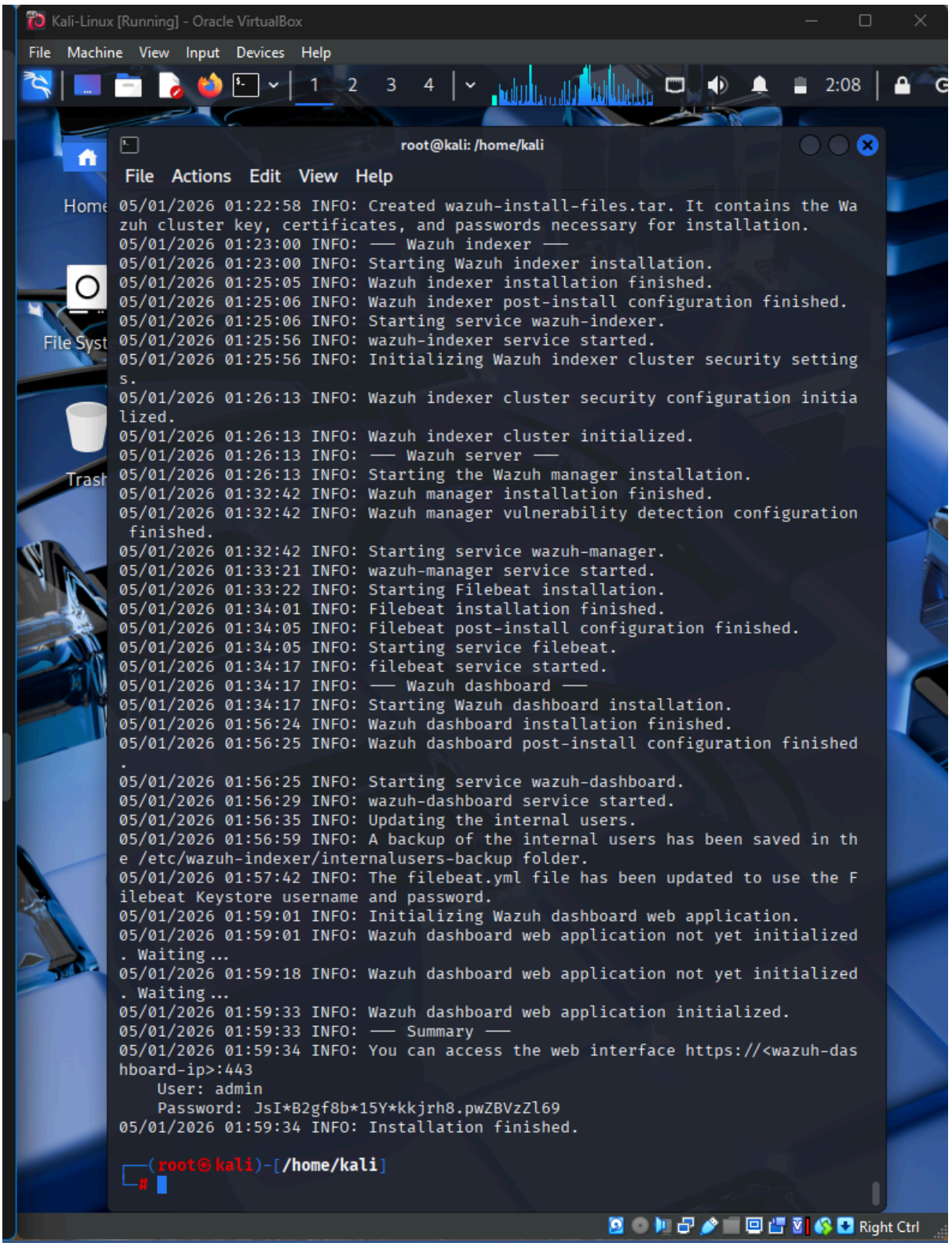
File Actions Edit View Help

```
└─# curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh && sudo bash
./wazuh-install.sh -a -i
bash: ./wazuh-install.sh: Permission denied

┌──(root㉿kali)-[/home/kali]
└─# curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh && sudo bash ./
wazuh-install.sh -a -i

┌──(root㉿kali)-[/home/kali]
└─# curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh && sudo bash ./
wazuh-install.sh -a -i
05/01/2026 01:20:25 INFO: Starting Wazuh installation assistant. Wazuh versio
n: 4.12.0
05/01/2026 01:20:25 INFO: Verbose logging redirected to /var/log/wazuh-instal
l.log
05/01/2026 01:20:25 INFO: The recommended systems are: Red Hat Enterprise Lin
ux 7, 8, 9; CentOS 7, 8; Amazon Linux 2; Ubuntu 16.04, 18.04, 20.04, 22.04.
05/01/2026 01:20:25 WARNING: The current system does not match with the list
of recommended systems. The installation may not work properly.
05/01/2026 01:21:11 WARNING: Hardware checks ignored.
05/01/2026 01:21:12 INFO: Wazuh web interface port will be 443.
05/01/2026 01:21:24 INFO: ── Dependencies ──
05/01/2026 01:21:24 INFO: Installing apt-transport-https.
05/01/2026 01:21:32 INFO: Installing debhelper.
05/01/2026 01:22:06 INFO: Installing software-properties-common.
05/01/2026 01:22:52 INFO: Wazuh repository added.
05/01/2026 01:22:52 INFO: ── Configuration files ──
05/01/2026 01:22:52 INFO: Generating configuration files.
05/01/2026 01:22:55 INFO: Generating the root certificate.
05/01/2026 01:22:55 INFO: Generating Admin certificates.
05/01/2026 01:22:55 INFO: Generating Wazuh indexer certificates.
05/01/2026 01:22:56 INFO: Generating Filebeat certificates.
05/01/2026 01:22:56 INFO: Generating Wazuh dashboard certificates.
05/01/2026 01:22:58 INFO: Created wazuh-install-files.tar. It contains the Wa
zuh cluster key, certificates, and passwords necessary for installation.
05/01/2026 01:23:00 INFO: ── Wazuh indexer ──
05/01/2026 01:23:00 INFO: Starting Wazuh indexer installation.
05/01/2026 01:25:05 INFO: Wazuh indexer installation finished.
05/01/2026 01:25:06 INFO: Wazuh indexer post-install configuration finished.
05/01/2026 01:25:06 INFO: Starting service wazuh-indexer.
05/01/2026 01:25:56 INFO: wazuh-indexer service started.
05/01/2026 01:25:56 INFO: Initializing Wazuh indexer cluster security setting
s.
05/01/2026 01:26:13 INFO: Wazuh indexer cluster security configuration initia
lized.
05/01/2026 01:26:13 INFO: Wazuh indexer cluster initialized.
05/01/2026 01:26:13 INFO: ── Wazuh server ──
05/01/2026 01:26:13 INFO: Starting the Wazuh manager installation.
05/01/2026 01:32:42 INFO: Wazuh manager installation finished.
05/01/2026 01:32:42 INFO: Wazuh manager vulnerability detection configuration
 finished.
05/01/2026 01:32:42 INFO: Starting service wazuh-manager.
```

Right Ctrl

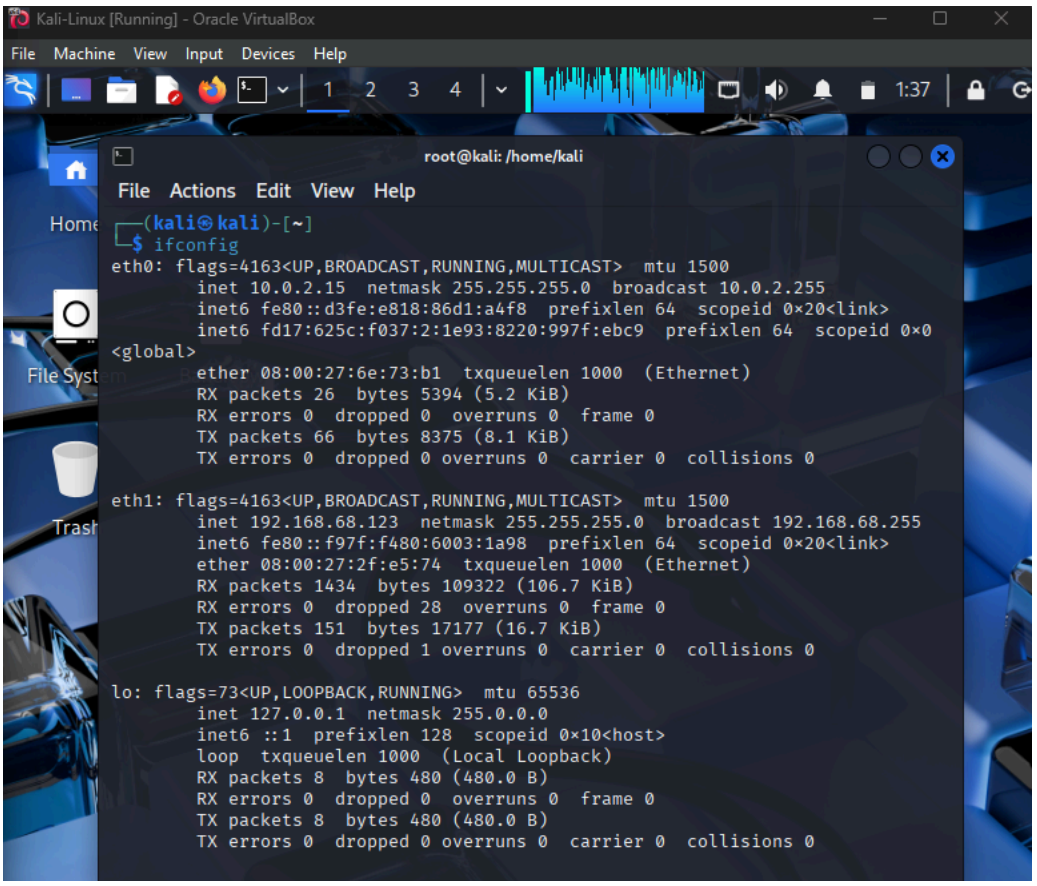


3. Accessing the Wazuh Dashboard

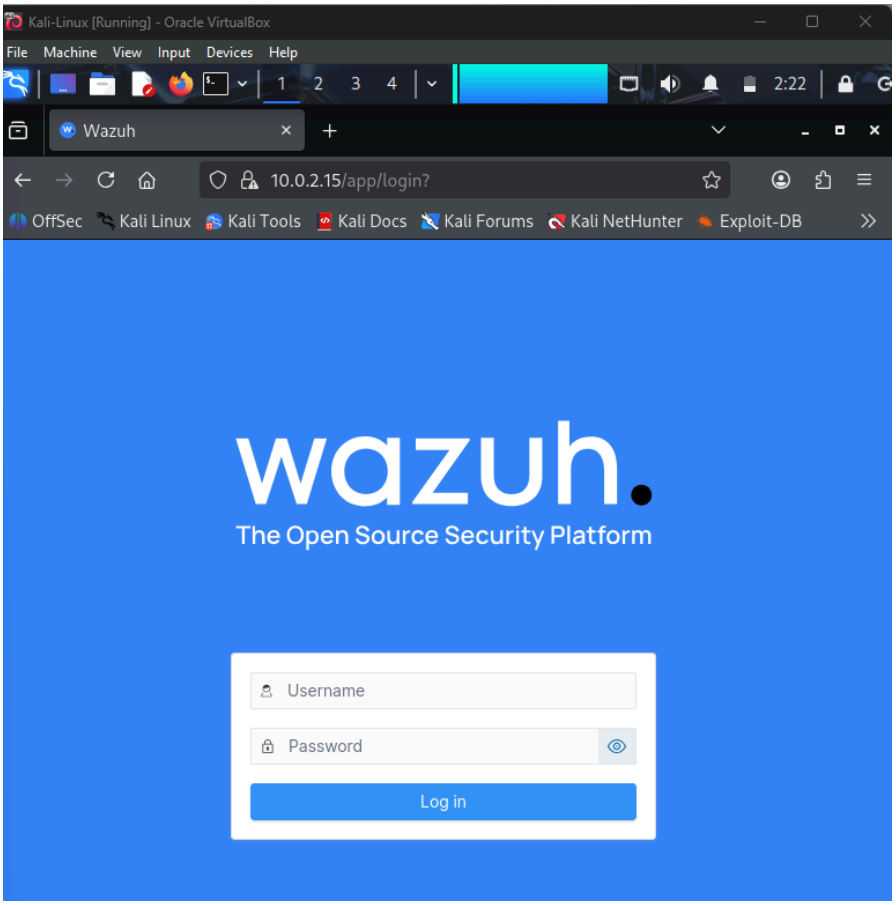
After installation:

3.1 - Check my Linux VM's IP address:
Commands used:

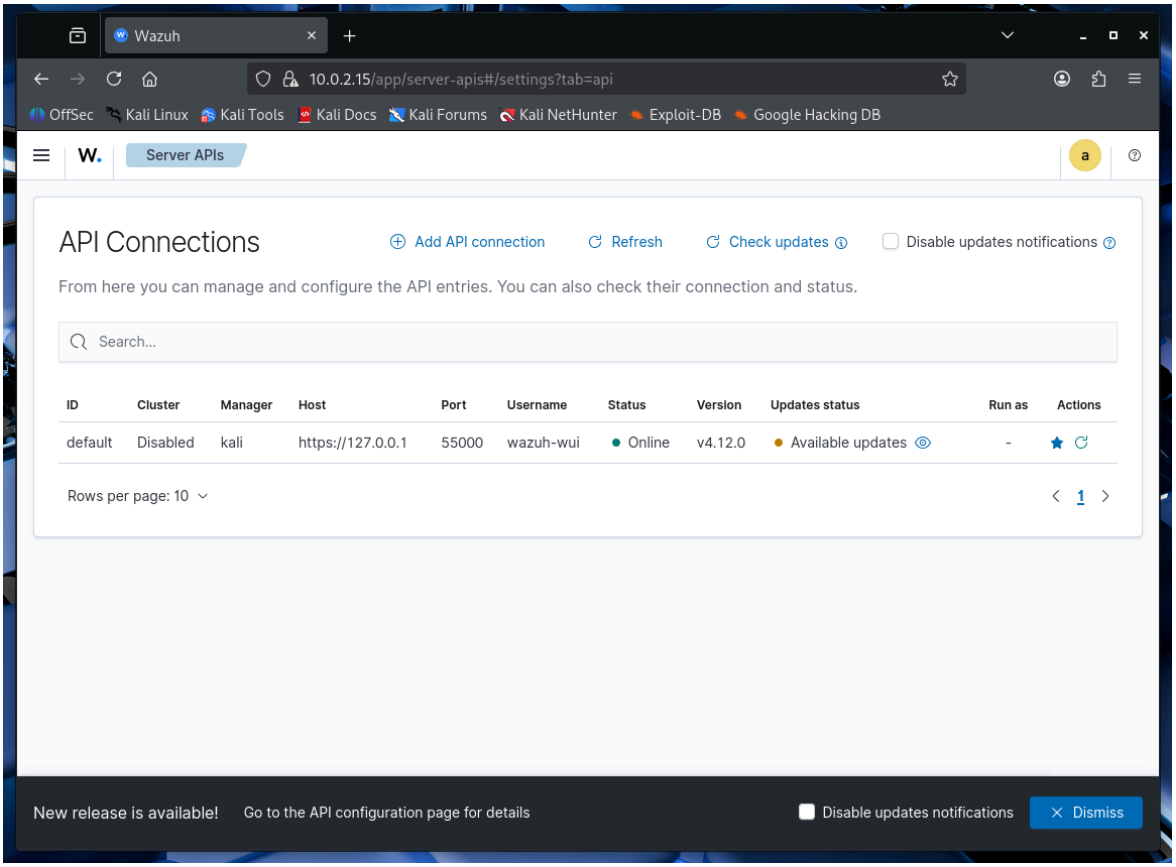
Ifconfig



3.2 - On my Linux server, open a browser and go to:
https://<kali-ip> (on this part, I should put the IP that is configured as Bridged Adapter (eth1), on the screenshot I tried using NAT network(eth0), but it will have API Connection issues with the agent)



3.3 - Logging in using the credentials displayed at the end of the installation script.

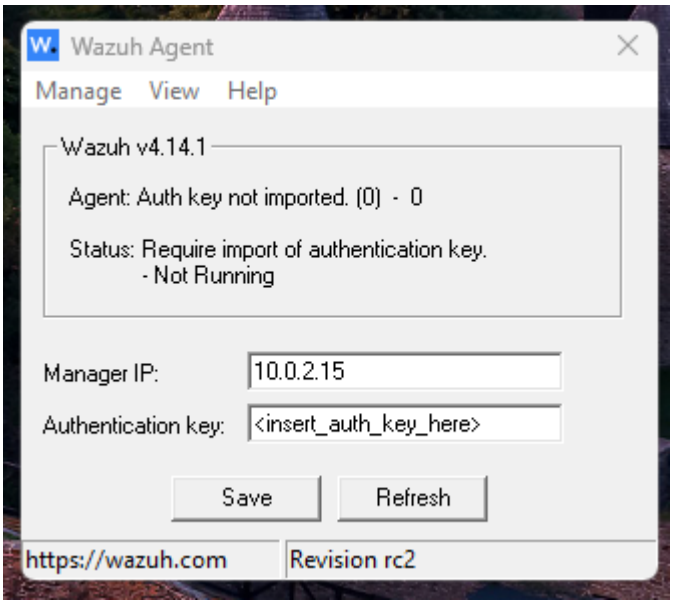


Wazuh Dashboard is prepared with these steps.

6. Installing the Wazuh Agent (Windows Host)

6.1 - Download the Wazuh agent MSI installer from the official documentation
(On this part, I made a mistake on installing the latest version, but it needs to be the same version with the Wazuh Manager in order for the API connection to function well.)

6.2- Install the MSI package on my Windows system using the default settings.



7. Registering the Agent with the Manager

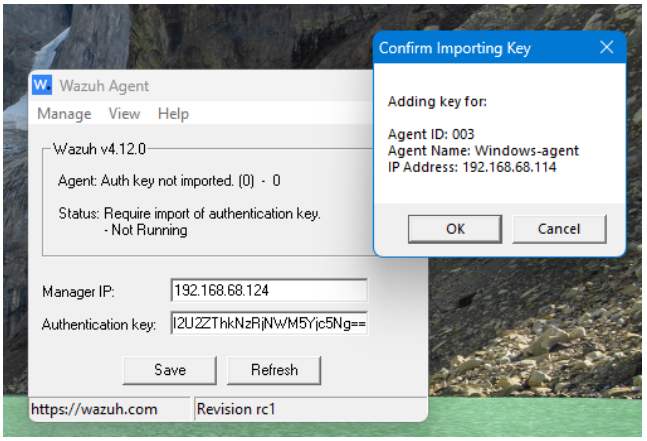
7.1 Generate Agent Key on Wazuh Manager (Linux)
Commands used:

sudo /var/ossec/bin/manage_agents

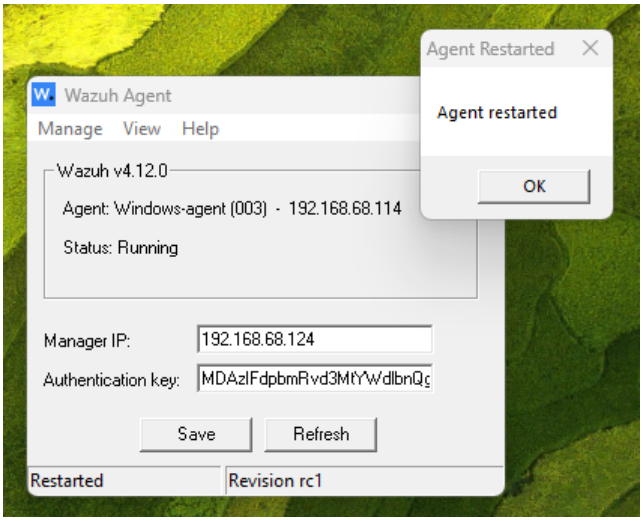
- Select A to add an agent.
- Assign a name (e.g., WindowsHost).
- After creation, select E to extract the key.
- Copy the key output.

7.2 Apply Key in the Windows Agent

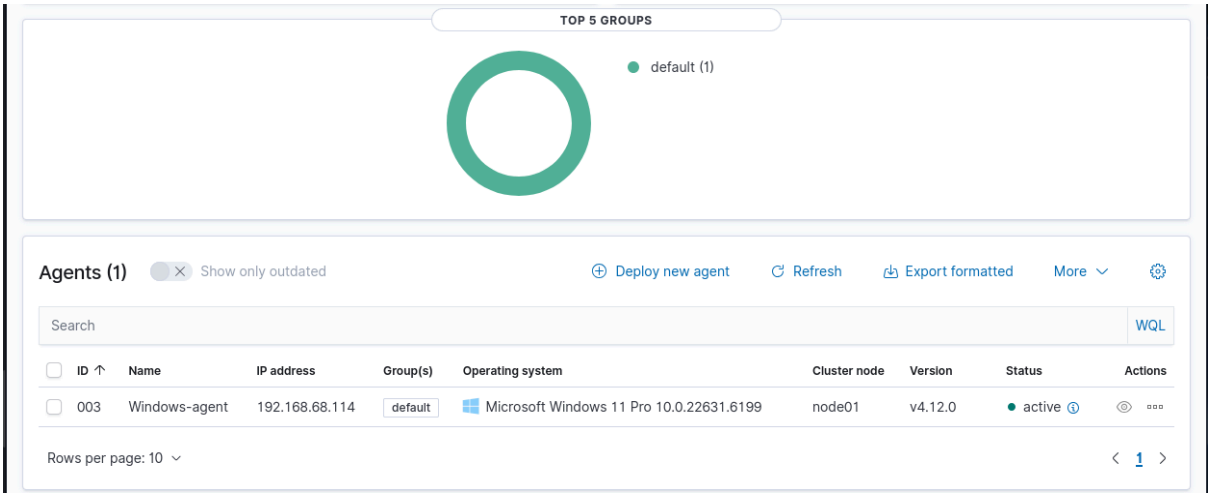
1. Open Wazuh Agent Manager GUI from the Start Menu.
2. Paste the copied key into the appropriate field.
3. Save and apply the key.
4. Add the manager's IP address (IP address of your Linux manager, make sure it is IP that configured as Bridged Adapter)



5. Restart the agent service.

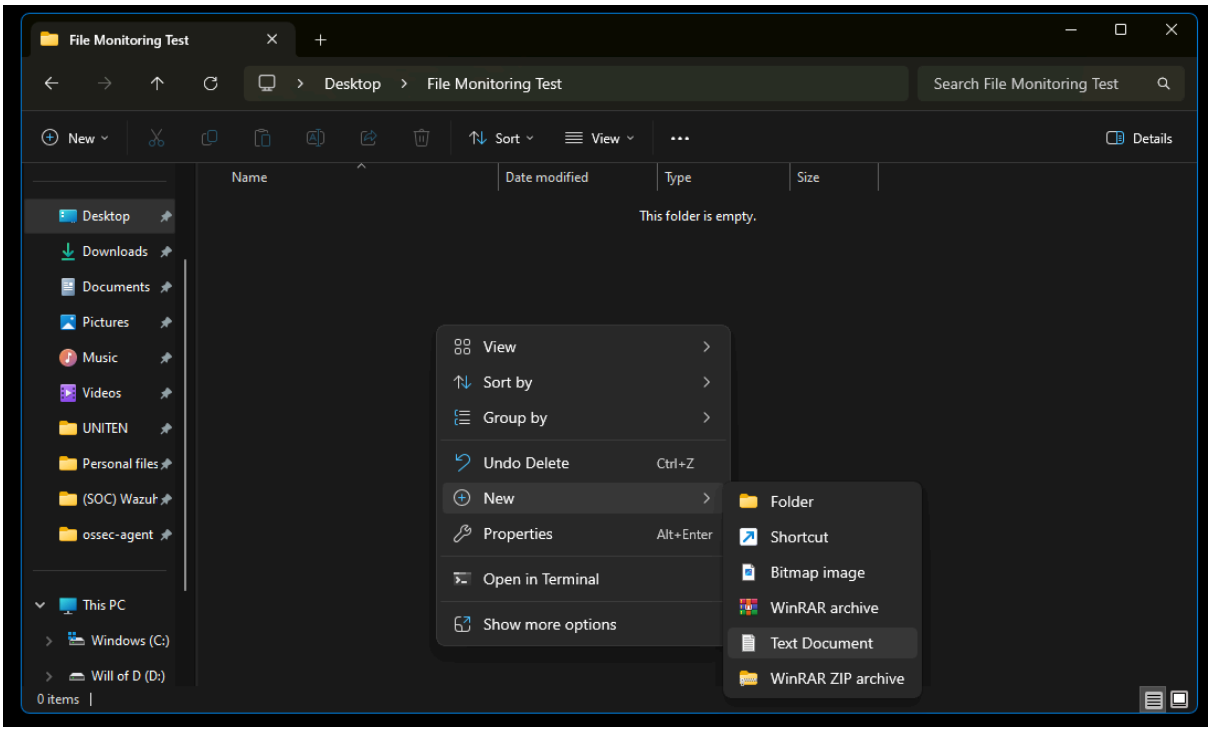


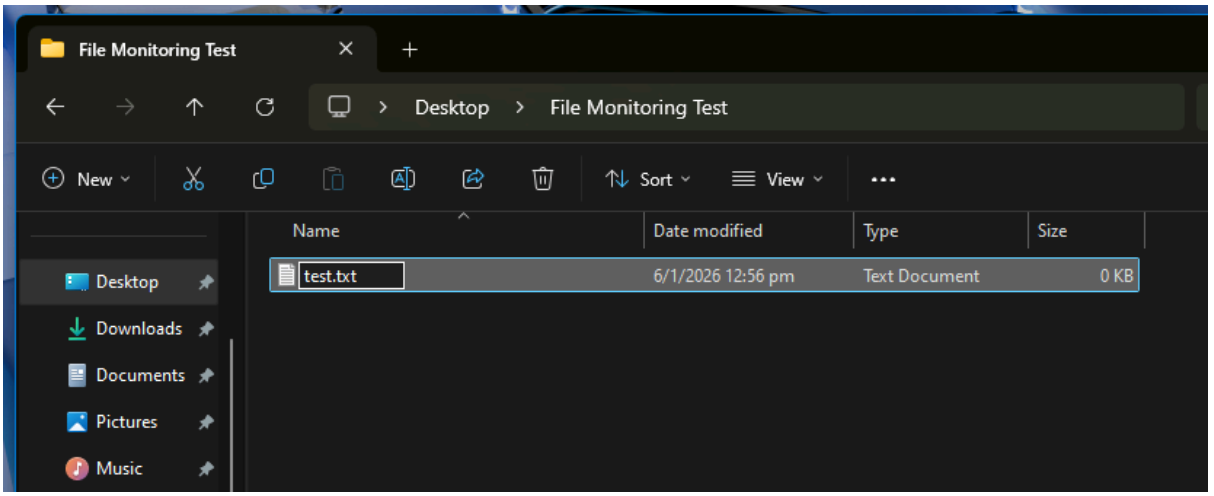
Go to the WAZUH dashboard and see the agent onboarded.



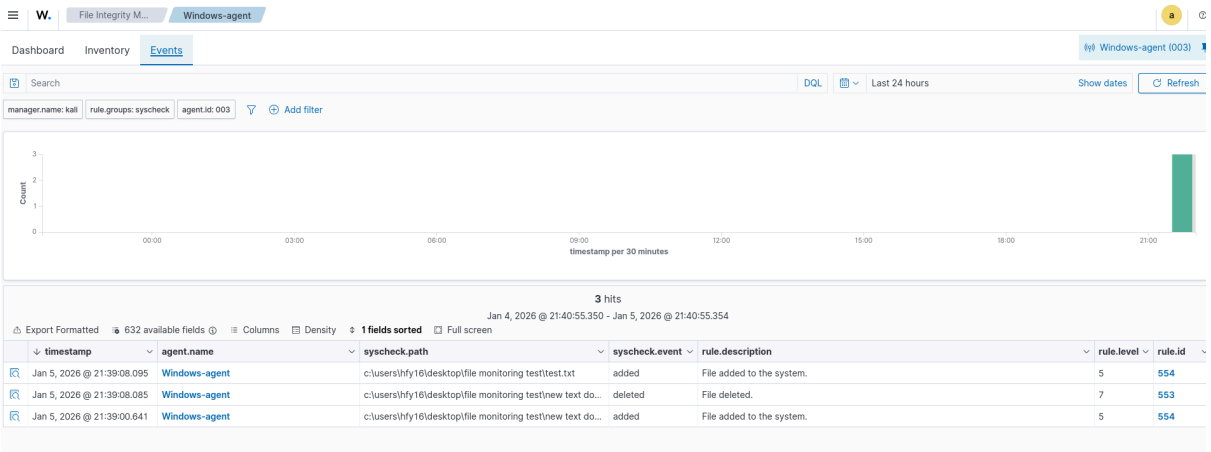
File Integrity Monitoring Section

1. Creating a Test.txt File for log testing

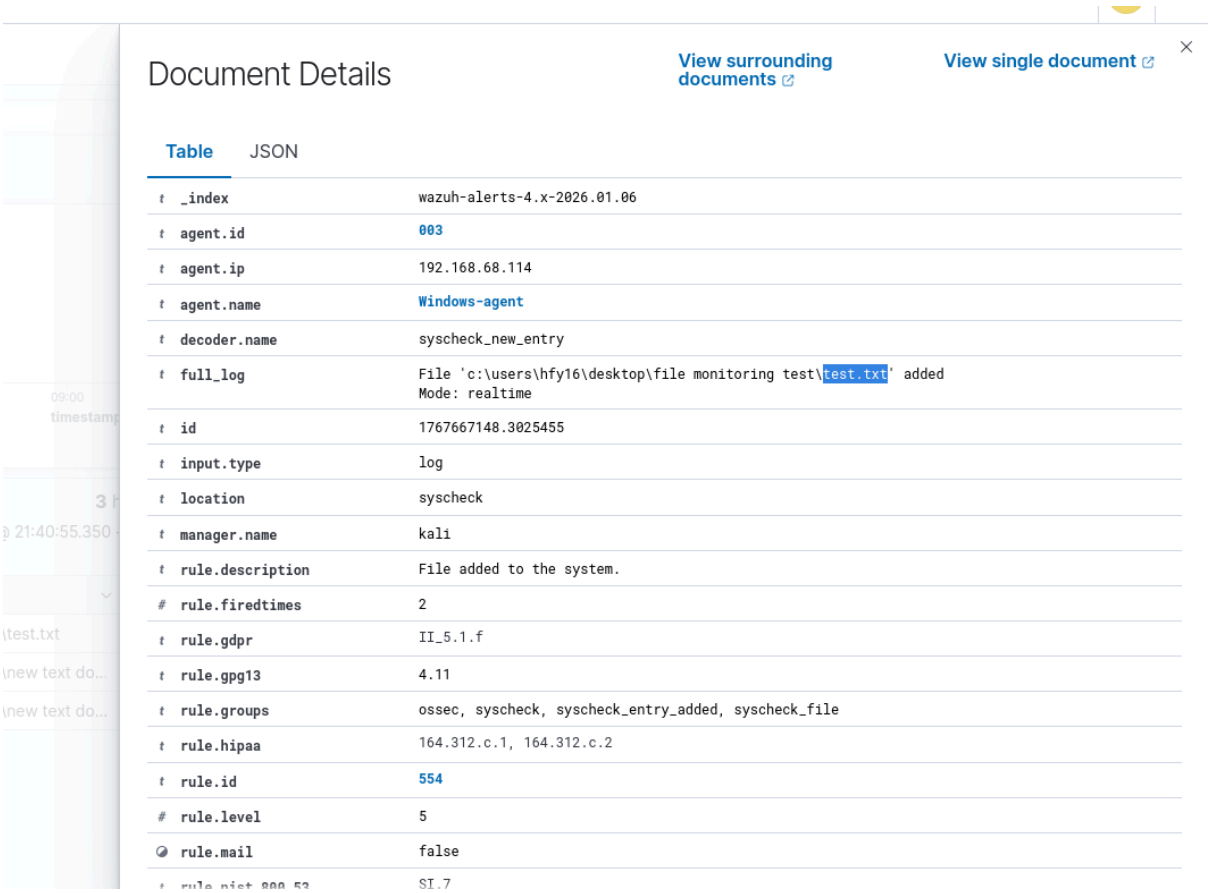




2. Verifying the new file log in Wazuh Endpoint Dashboard



3. **Inspecting the full log for further verification**



Document Details

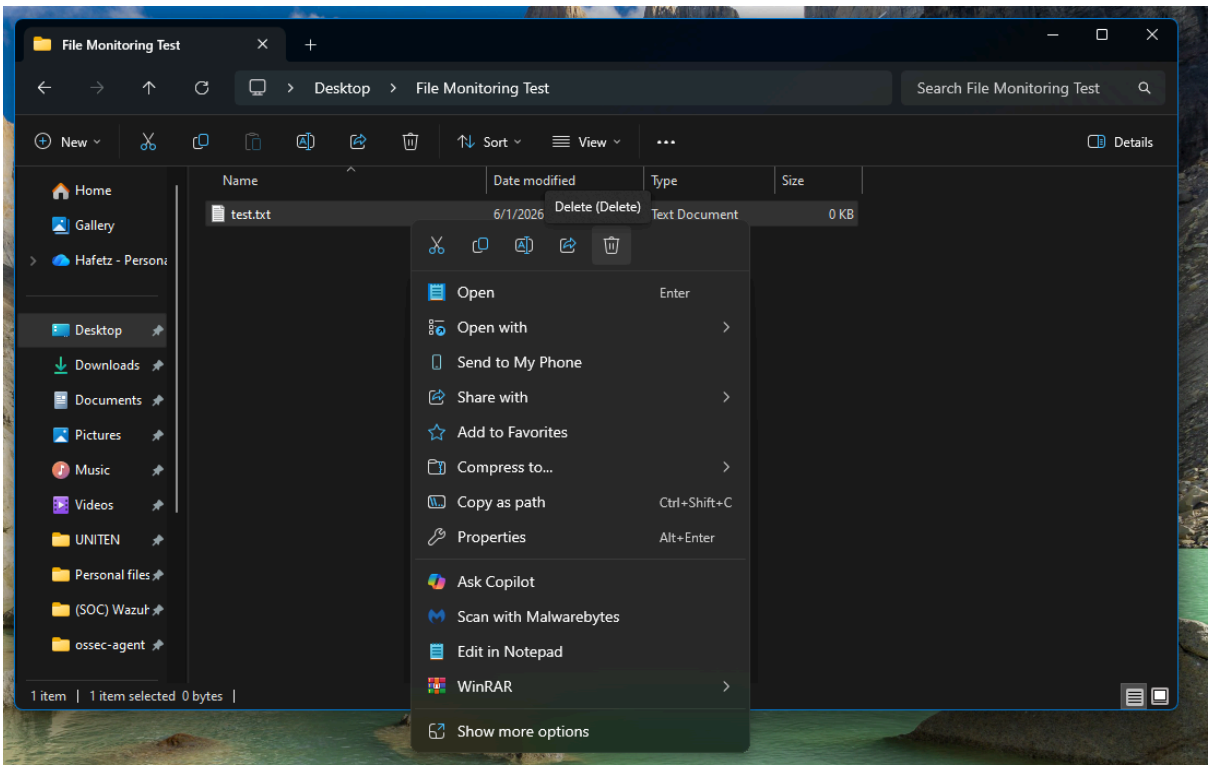
View surrounding documents

View single document

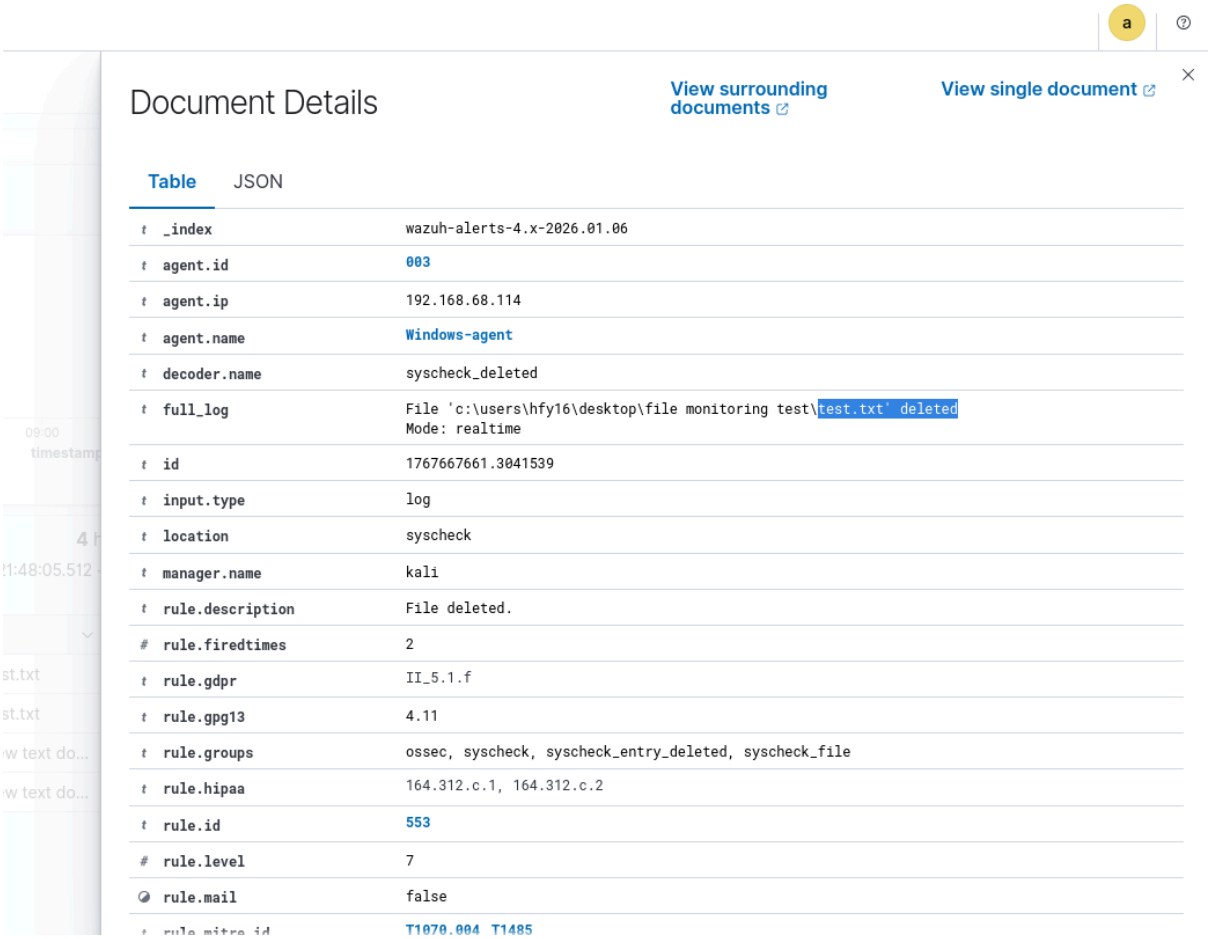
Table JSON

t _index	wazuh-alerts-4.x-2026.01.06
t agent.id	003
t agent.ip	192.168.68.114
t agent.name	Windows-agent
t decoder.name	syscheck_new_entry
t full_log	File 'c:\users\hfy16\desktop\file monitoring test\test.txt' added Mode: realtime
t id	1767667148.3025455
t input.type	log
t location	syscheck
t manager.name	kali
t rule.description	File added to the system.
# rule.firedtimes	2
t rule.gdpr	II_5.1.f
t rule.gpg13	4.11
t rule.groups	ossec, syscheck, syscheck_entry_added, syscheck_file
t rule.hipaa	164.312.c.1, 164.312.c.2
t rule.id	554
# rule.level	5
rule.mail	false
t rule.nist_800_53	SI.7

4. **Deleting the Test.txt file for further log testing**



5. **Verifying the file deletion log by inspecting the new log entry.**



Document Details

View surrounding documents

View single document

Table JSON

_index	wazuh-alerts-4.x-2026.01.06
agent.id	003
agent.ip	192.168.68.114
agent.name	Windows-agent
decoder.name	syscheck_deleted
full_log	File 'c:\users\hfy16\desktop\file monitoring test\test.txt' deleted Mode: realtime
id	1767667661.3041539
input.type	log
location	syscheck
manager.name	kali
rule.description	File deleted.
rule.firedtimes	2
rule.gdpr	II_5.1.f
rule.gpg13	4.11
rule.groups	ossec, syscheck, syscheck_entry_deleted, syscheck_file
rule.hipaa	164.312.c.1, 164.312.c.2
rule.id	553
rule.level	7
rule.mail	false
rule.mitre.id	T1070.004, T1485