2024

Wazuh

INSTALLATION, CONFIGURATION & AGENT MANAGEMENT

MAHAREEB FATIMA

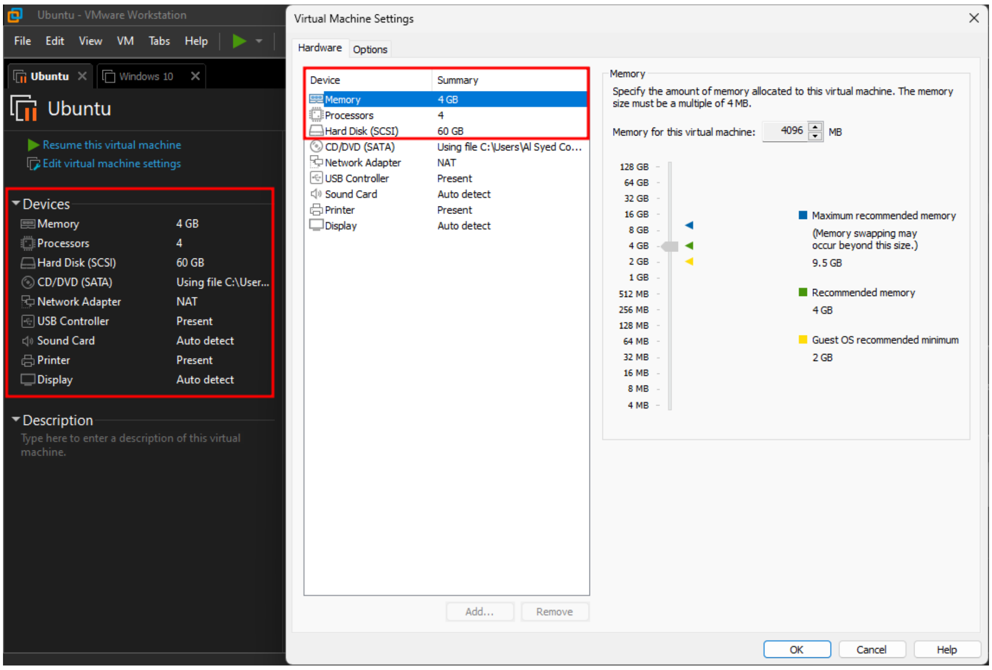
Table of Contents

Introduction

This report details the deployment and configuration of Wazuh, an open-source security monitoring platform, on Ubuntu and Windows systems. It covers key aspects such as installing Wazuh Manager, deploying agents, setting up file integrity monitoring, and integrating Suricata for network intrusion detection. The report also explores advanced features like vulnerability detection, malicious command monitoring, and active response mechanisms, demonstrating Wazuh's comprehensive capabilities in enhancing cybersecurity defenses.

Pre-requisites

1. Ubuntu 20.04 VM → For Wazuh manager installation.


Ubuntu - VMware Workstation
File Edit View VM Tabs Help
Ubuntu
Windows 10
Resume this virtual machine
Edit virtual machine settings
Description
Type here to enter a description of this virtual machine.
Virtual Machine Settings
Hardware Options
Add... Remove
OK Cancel Help

Devices

Device	Summary
Memory	4 GB
Processors	4
Hard Disk (SCSI)	60 GB
CD/DVD (SATA)	Using file C:\Users\Al Syed Co...
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

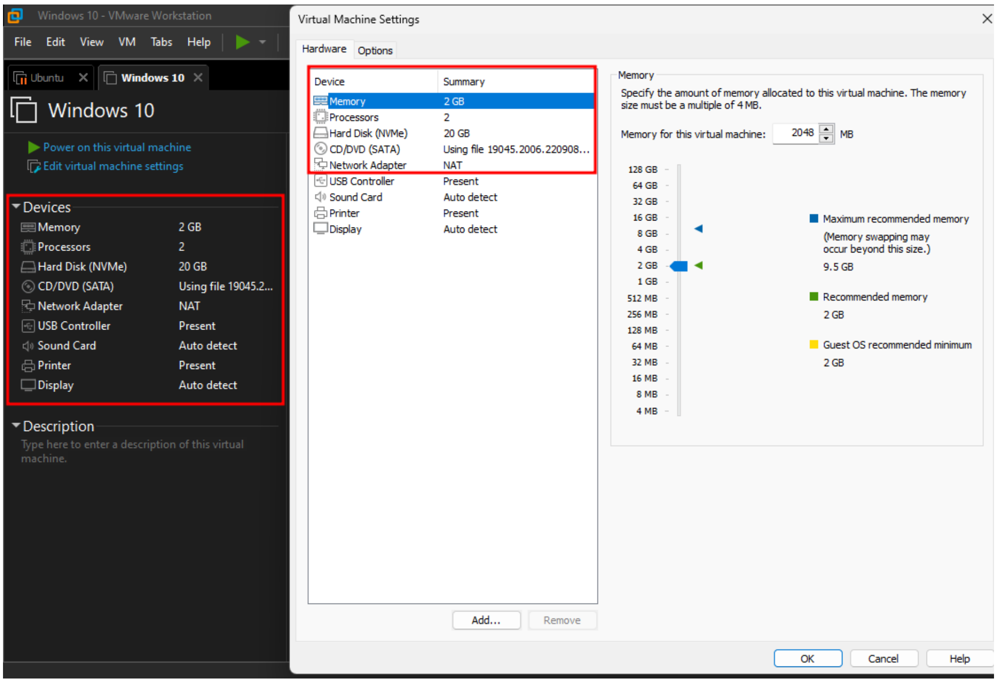
Memory for this virtual machine: 4096 MB

Maximum recommended memory (Memory swapping may occur beyond this size.) 9.5 GB

Recommended memory 4 GB

Guest OS recommended minimum 2 GB

2. Windows VM → For Wazuh agent installation


Windows 10 - VMware Workstation
File Edit View VM Tabs Help
Ubuntu
Windows 10
Power on this virtual machine
Edit virtual machine settings
Description
Type here to enter a description of this virtual machine.
Virtual Machine Settings
Hardware Options
Add... Remove
OK Cancel Help

Devices

Device	Summary
Memory	2 GB
Processors	2
Hard Disk (NVMe)	20 GB
CD/DVD (SATA)	Using file 19045.2006.220908...
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

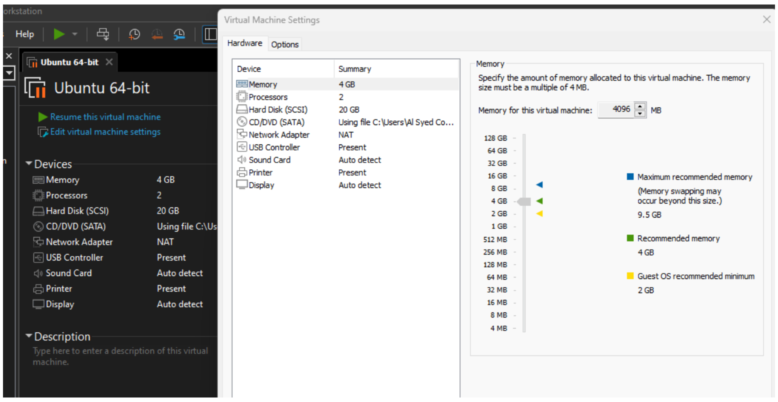
Memory for this virtual machine: 2048 MB

Maximum recommended memory (Memory swapping may occur beyond this size.) 9.5 GB

Recommended memory 2 GB

Guest OS recommended minimum 2 GB

3. Another Ubuntu VM → For Wazuh Agent Installation.



orkstation
Help
Ubuntu 64-bit
Ubuntu 64-bit
Resume this virtual machine
Edit virtual machine settings
Description
Type here to enter a description of this virtual machine.
Virtual Machine Settings
Hardware
Options

Devices

Memory	4 GB
Processors	2
Hard Disk (SCSI)	20 GB
CD/DVD (SATA)	Using file C:\Us
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device	Summary
Memory	4 GB
Processors	2
Hard Disk (SCSI)	20 GB
CD/DVD (SATA)	Using file C:\Users\Al Syed Co...
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 4096 MB

🟦 Maximum recommended memory
(Memory swapping may occur beyond this size.)
9.5 GB

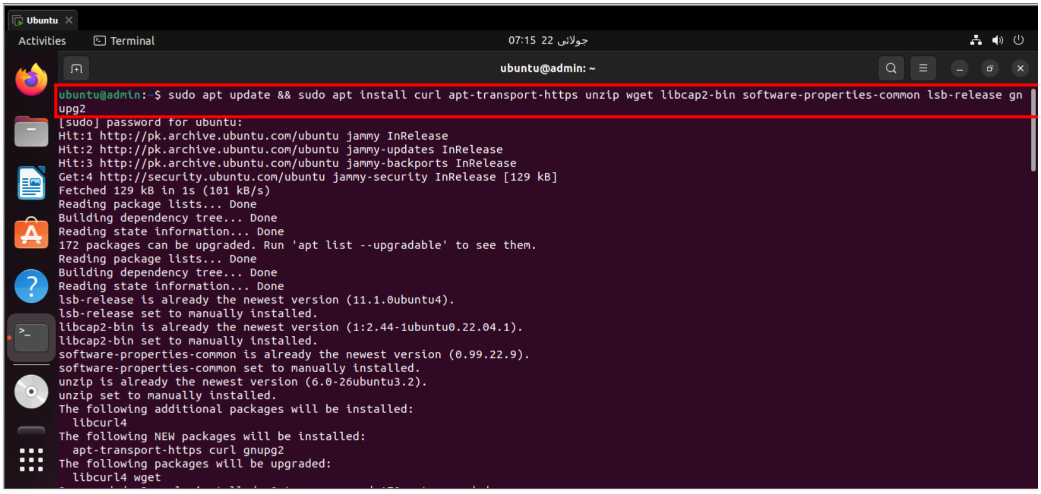
🟩 Recommended memory
4 GB

🟨 Guest OS recommended minimum
2 GB

Wazuh Manager Instalaltion on Ubuntu 22.04

1. Run the follwing command to update your ubuntu VM and install some additional tools needed for Wazuh manager instalation.

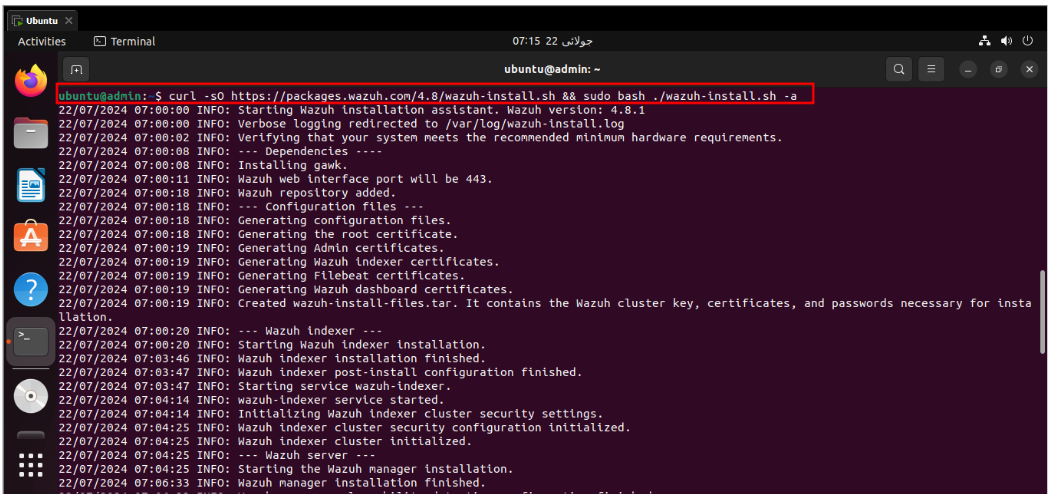
sudo apt update && sudo apt install curl apt-transport-https unzip wget libcap2-bin software-properties-common lsb-release gnupg2



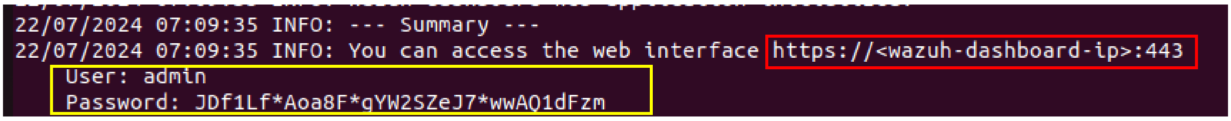
```
ubuntu@admin:~$ sudo apt update && sudo apt install curl apt-transport-https unzip wget libcap2-bin software-properties-common lsb-release gn
upg2
[sudo] password for ubuntu:
Hit:1 http://pk.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://pk.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://pk.archive.ubuntu.com/ubuntu jammy-backports InRelease
Get:4 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Fetched 129 kB in 1s (101 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
172 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
lsb-release is already the newest version (11.1.0ubuntu4).
lsb-release set to manually installed.
libcap2-bin is already the newest version (1:2.44-1ubuntu0.22.04.1).
libcap2-bin set to manually installed.
software-properties-common is already the newest version (0.99.22.9).
software-properties-common set to manually installed.
unzip is already the newest version (6.0-26ubuntu3.2).
unzip set to manually installed.
The following additional packages will be installed:
  libcurl4
The following NEW packages will be installed:
  apt-transport-https curl gnupg2
The following packages will be upgraded:
  libcurl4 wget
```

2. Run the following command to install wazuh manager.

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



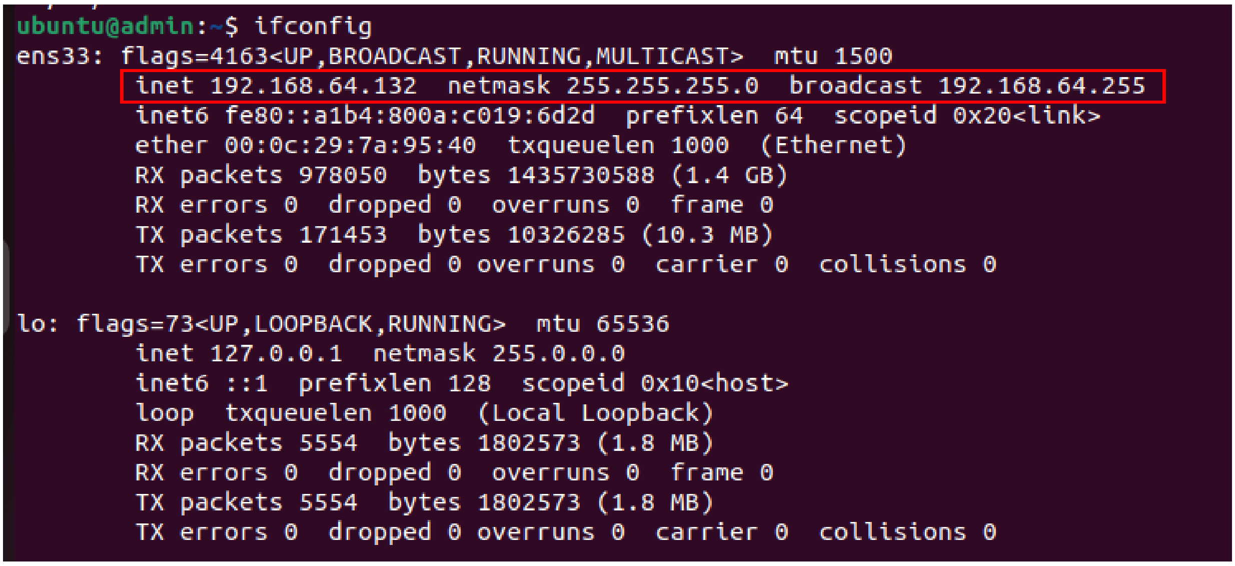
```
ubuntu@admin:~$ curl -sO https://packages.wazuh.com/4.8/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
22/07/2024 07:00:00 INFO: Starting Wazuh installation assistant. Wazuh version: 4.8.1
22/07/2024 07:00:00 INFO: Verbose logging redirected to /var/log/wazuh-install.log
22/07/2024 07:00:02 INFO: Verifying that your system meets the recommended minimum hardware requirements.
22/07/2024 07:00:08 INFO: --- Dependencies ----
22/07/2024 07:00:08 INFO: Installing gawk.
22/07/2024 07:00:11 INFO: Wazuh web interface port will be 443.
22/07/2024 07:00:18 INFO: Wazuh repository added.
22/07/2024 07:00:18 INFO: --- Configuration files ---
22/07/2024 07:00:18 INFO: Generating configuration files.
22/07/2024 07:00:18 INFO: Generating the root certificate.
22/07/2024 07:00:19 INFO: Generating Admin certificates.
22/07/2024 07:00:19 INFO: Generating Wazuh indexer certificates.
22/07/2024 07:00:19 INFO: Generating Filebeat certificates.
22/07/2024 07:00:19 INFO: Generating Wazuh dashboard certificates.
22/07/2024 07:00:19 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for insta
llation.
22/07/2024 07:00:20 INFO: --- Wazuh indexer ---
22/07/2024 07:00:20 INFO: Starting Wazuh indexer installation.
22/07/2024 07:03:46 INFO: Wazuh indexer installation finished.
22/07/2024 07:03:47 INFO: Wazuh indexer post-install configuration finished.
22/07/2024 07:03:47 INFO: Starting service wazuh-indexer.
22/07/2024 07:04:14 INFO: wazuh-indexer service started.
22/07/2024 07:04:14 INFO: Initializing Wazuh indexer cluster security settings.
22/07/2024 07:04:25 INFO: Wazuh indexer cluster security configuration initialized.
22/07/2024 07:04:25 INFO: Wazuh indexer cluster initialized.
22/07/2024 07:04:25 INFO: --- Wazuh server ---
22/07/2024 07:04:25 INFO: Starting the Wazuh manager installation.
22/07/2024 07:06:33 INFO: Wazuh manager installation finished.
```



```
22/07/2024 07:09:35 INFO: --- Summary ---
22/07/2024 07:09:35 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
    User: admin
    Password: JDf1Lf*Aoa8F*gYW2SZeJ7*wwAQ1dFzm
```

User: admin

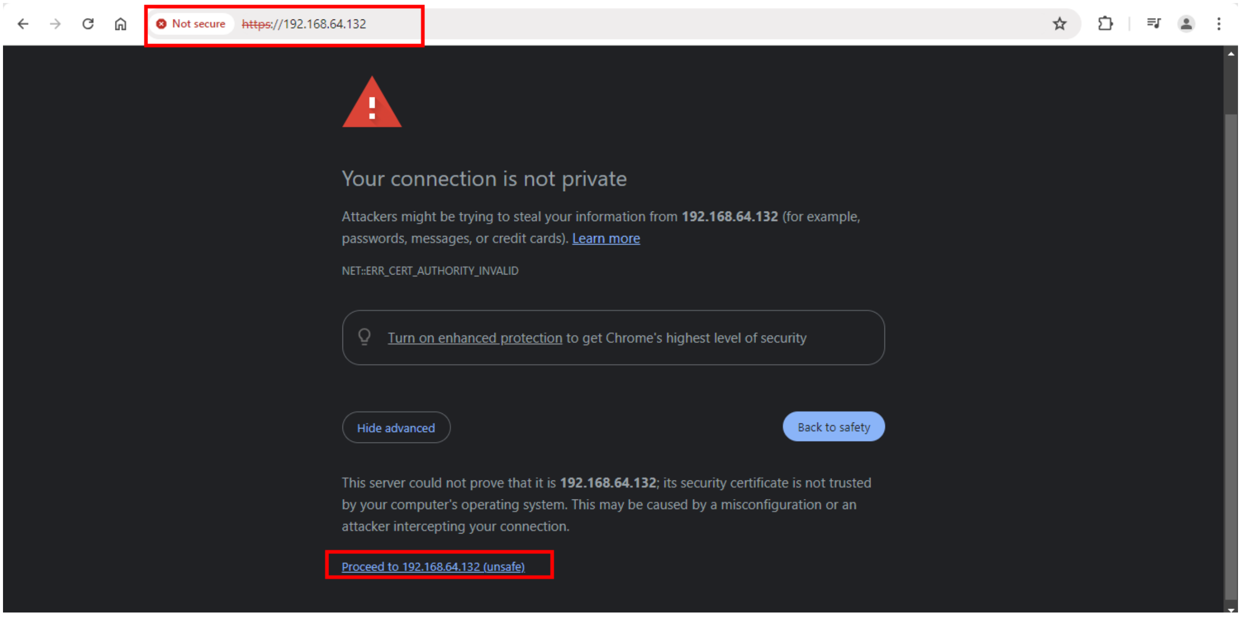
Password: JDf1Lf*Aoa8F*gYW2SZeJ7*wwAQ1dFzm



```
ubuntu@admin:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.64.132  netmask 255.255.255.0  broadcast 192.168.64.255
        inet6 fe80::a1b4:800a:c019:6d2d  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:7a:95:40  txqueuelen 1000  (Ethernet)
        RX packets 978050  bytes 1435730588 (1.4 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 171453  bytes 10326285 (10.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 5554  bytes 1802573 (1.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5554  bytes 1802573 (1.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Wazuh

1. Use your Ubuntu's IP to access Wazuh.



Your connection is not private

Attackers might be trying to steal your information from **192.168.64.132** (for example, passwords, messages, or credit cards). Learn more

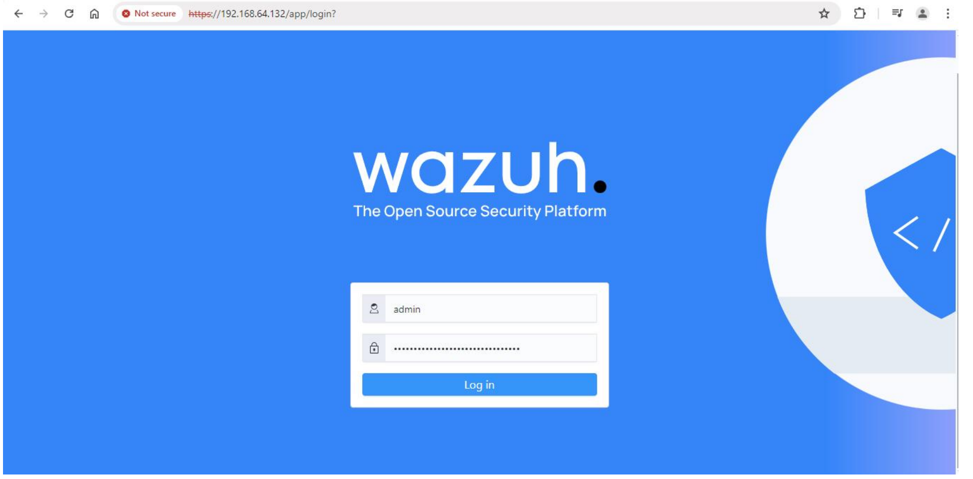
NET::ERR_CERT_AUTHORITY_INVALID

Turn on enhanced protection to get Chrome's highest level of security

This server could not prove that it is **192.168.64.132**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 192.168.64.132 (unsafe)

2. Login with the provided credentials.



Not secure ~~https~~://192.168.64.132/app/login?

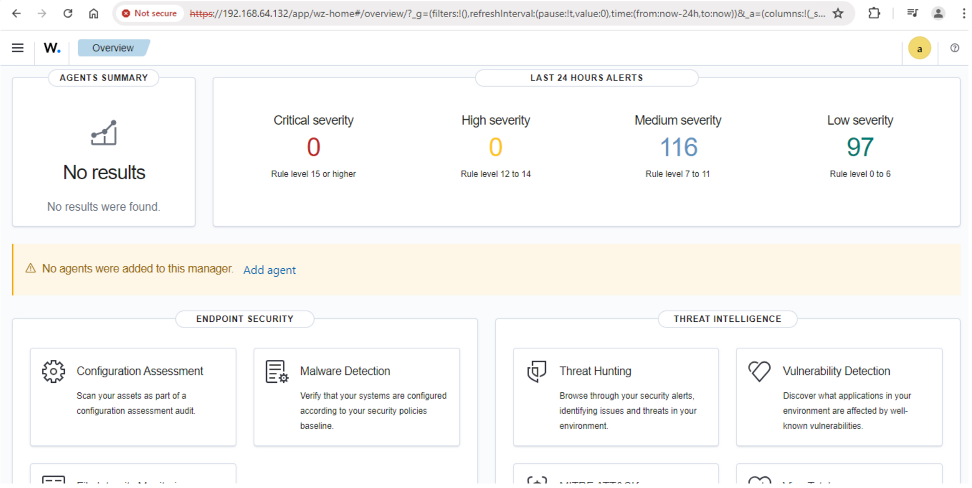
wazuh.

The Open Source Security Platform

admin

••••••••••••••••••••••••••••••••

Log in



Not secure ~~https~~://192.168.64.132/app/wz-home#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_s...

Overview

AGENTS SUMMARY

No results

No results were found.

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	0	116	97
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	Rule level 0 to 6

⚠ No agents were added to this manager. Add agent

ENDPOINT SECURITY

Configuration Assessment
Scan your assets as part of a configuration assessment audit.

Malware Detection
Verify that your systems are configured according to your security policies baseline.

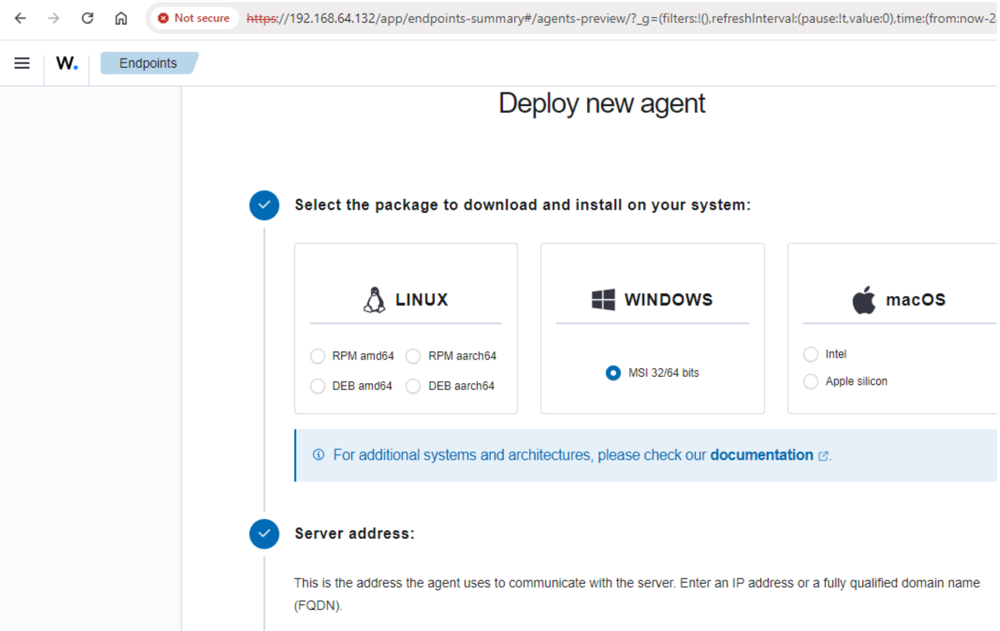
THREAT INTELLIGENCE

Threat Hunting
Browse through your security alerts, identifying issues and threats in your environment.

Vulnerability Detection
Discover what applications in your environment are affected by well-known vulnerabilities.

1. Deploying a Windows Agent

We are going to deploy two wazuh agents. Window-10 & Linux Ubuntu agent.



Not secure ~~https~~://192.168.64.132/app/endpoints-summary#/agents-preview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-2

Endpoints

Deploy new agent

Select the package to download and install on your system:

LINUX
○ RPM amd64 ○ RPM aarch64
○ DEB amd64 ○ DEB aarch64

WINDOWS
● MSI 32/64 bits

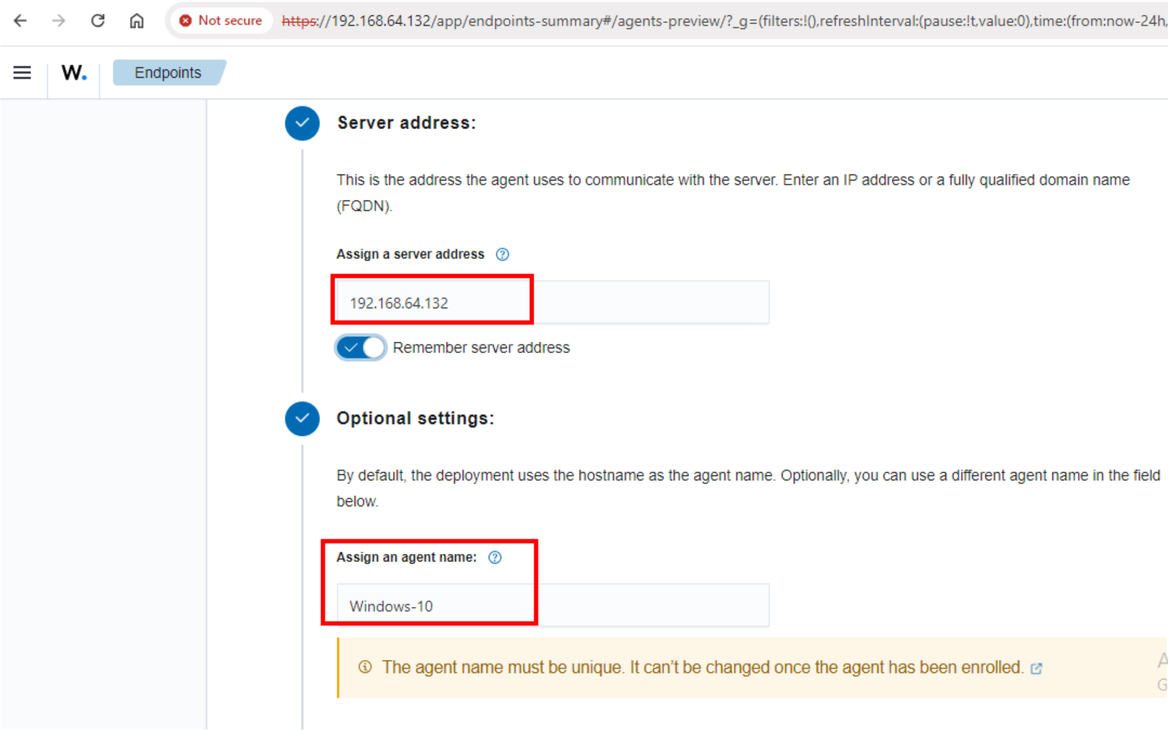
macOS
○ Intel
○ Apple silicon

ⓘ For additional systems and architectures, please check our **documentation**

Server address:

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).

Assign Server address, agent name, and assign agent group. Since I'm only going to deploy 1 window-10 agent, so I've assigned it to default agent group.



Not secure
https://192.168.64.132/app/endpoints-summary#/agents-preview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,
W.
Endpoints

Server address:

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).

Assign a server address

192.168.64.132

Remember server address

Optional settings:

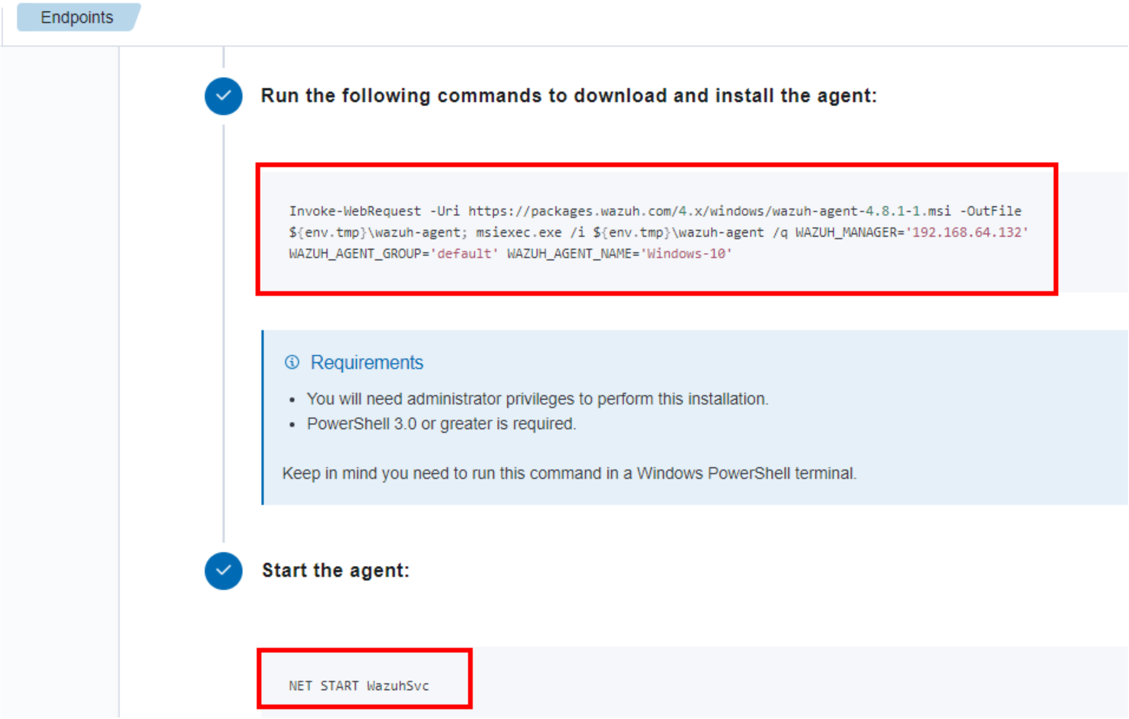
By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

Assign an agent name:

Windows-10

The agent name must be unique. It can't be changed once the agent has been enrolled.

Run the given commands to install wazuh agent on the respective machine and start the agent.



Run the following commands to download and install the agent:

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.8.1-1.msi -OutFile
${env.tmp}\wazuh-agent; msiexec.exe /i ${env.tmp}\wazuh-agent /q WAZUH_MANAGER='192.168.64.132'
WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='Windows-10'
```

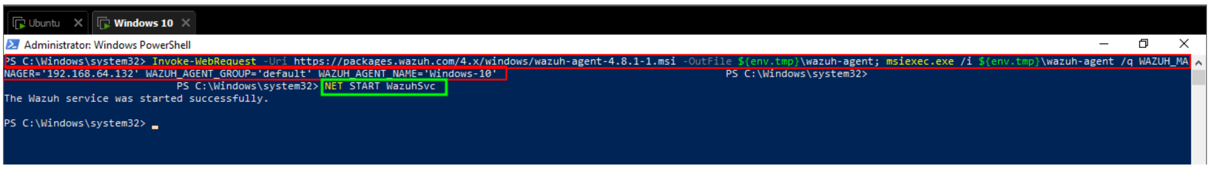
Requirements

- You will need administrator privileges to perform this installation.
- PowerShell 3.0 or greater is required.

Keep in mind you need to run this command in a Windows PowerShell terminal.

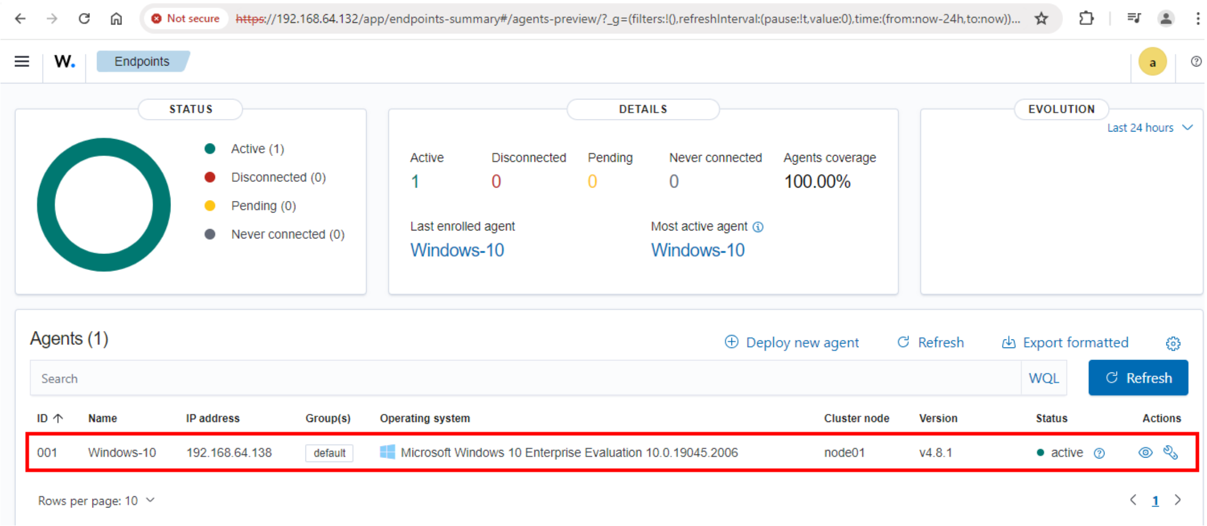
Start the agent:

```
NET START WazuhSvc
```



```
PS C:\Windows\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.8.1-1.msi -OutFile ${env.tmp}\wazuh-agent; msiexec.exe /i ${env.tmp}\wazuh-agent /q WAZUH_MA
NAGER='192.168.64.132' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='Windows-10'                                PS C:\Windows\system32>
                         PS C:\Windows\system32> NET START WazuhSvc
The Wazuh service was started successfully.

PS C:\Windows\system32> _
```

Now, our agent is visible and fully covered by Wazuh.



Not secure
https://192.168.64.132/app/endpoints-summary#/agents-preview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))...
W.
Endpoints
a
STATUS
DETAILS
EVOLUTION
Last 24 hours

STATUS:

- ● Active (1)
- ● Disconnected (0)
- ● Pending (0)
- ● Never connected (0)

DETAILS:

Active	Disconnected	Pending	Never connected	Agents coverage
1	0	0	0	100.00%

Last enrolled agent: Windows-10

Most active agent: Windows-10

Agents (1)

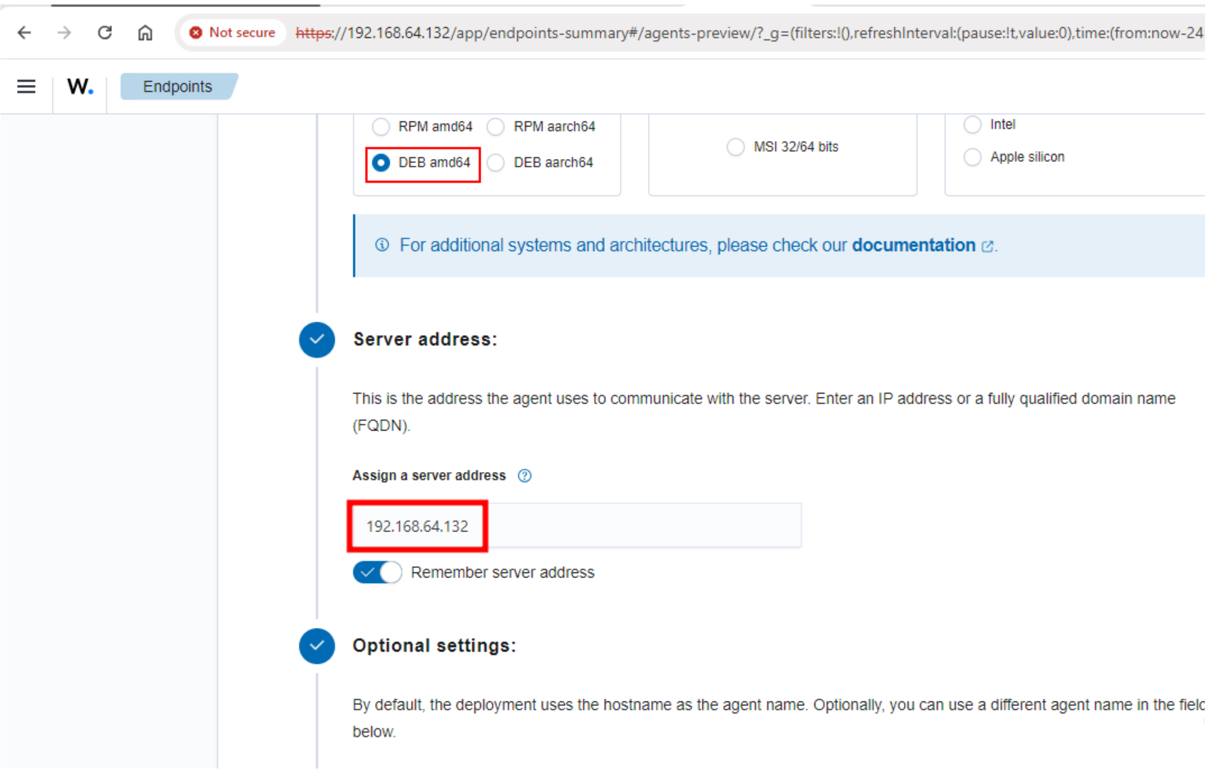
Deploy new agent
Refresh
Export formatted
Search
WQL
Refresh

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	Windows-10	192.168.64.138	default	Microsoft Windows 10 Enterprise Evaluation 10.0.19045.2006	node01	v4.8.1	● active	

Rows per page: 10

2. Deploying Ubuntu Agent

Deploying the second agent.



Not secure
https://192.168.64.132/app/endpoints-summary#/agents-preview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24
W.
Endpoints

○ RPM amd64 ○ RPM aarch64
● DEB amd64 ○ DEB aarch64

○ MSI 32/64 bits

○ Intel
○ Apple silicon

For additional systems and architectures, please check our **documentation**.

Server address:

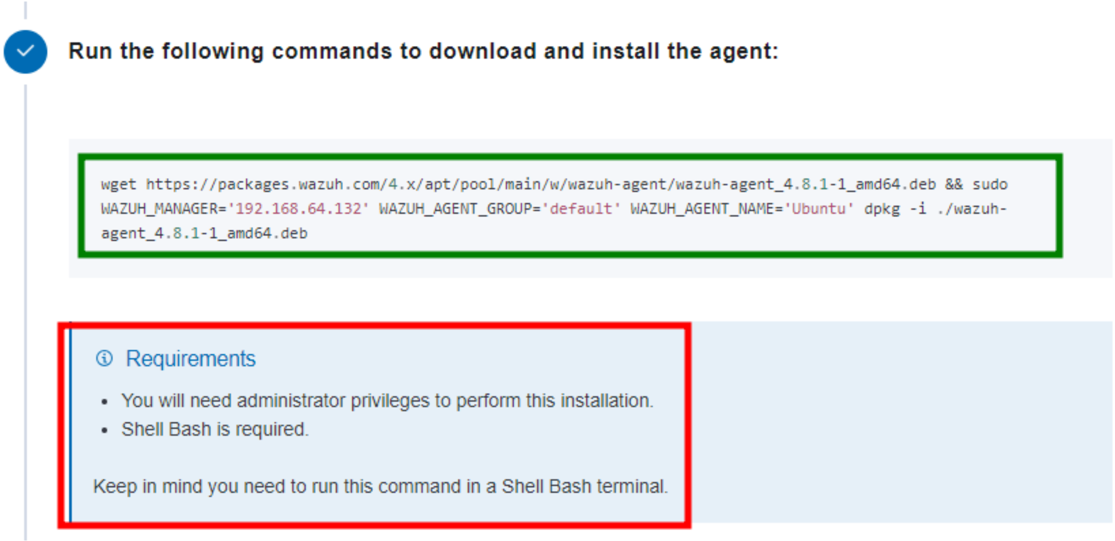
This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).

Assign a server address: 192.168.64.132

☑ Remember server address

Optional settings:

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the fielc below.



Run the following commands to download and install the agent:

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.8.1-1_amd64.deb && sudo
WAZUH_MANAGER='192.168.64.132' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='Ubuntu' dpkg -i ./wazuh-
agent_4.8.1-1_amd64.deb
```

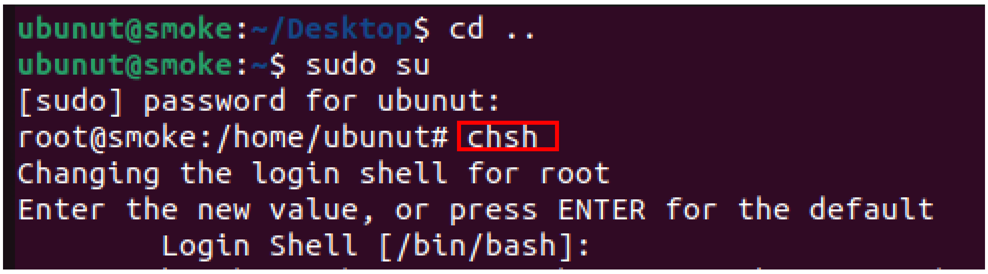
ⓘ Requirements

- You will need administrator privileges to perform this installation.
- Shell Bash is required.

Keep in mind you need to run this command in a Shell Bash terminal.

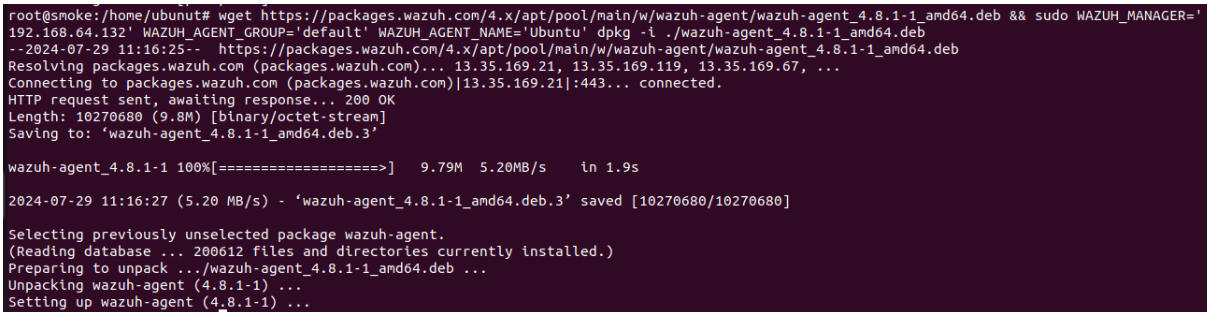
The requirements state that the given command should be run in bash script with super user privileges.

- **sudo su** → for super user privileges.
- Use the **chsh** command to change the shell to bash.



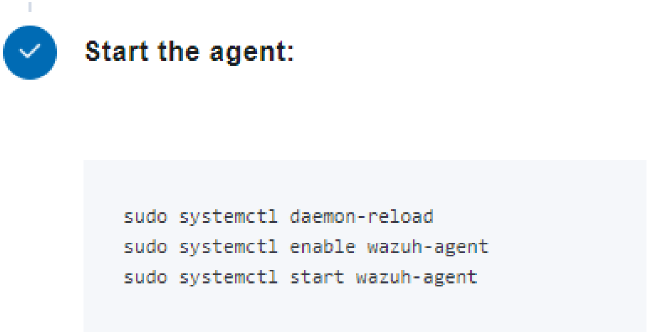
```
ubunut@smoke:~/Desktop$ cd ..
ubunut@smoke:~$ sudo su
[sudo] password for ubunut:
root@smoke:/home/ubunut# chsh
Changing the login shell for root
Enter the new value, or press ENTER for the default
        Login Shell [/bin/bash]:
```

Now, that the requirements for running the command are fulfilled, run the command.



```
root@smoke:/home/ubunut# wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.8.1-1_amd64.deb && sudo WAZUH_MANAGER='
192.168.64.132' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='Ubuntu' dpkg -i ./wazuh-agent_4.8.1-1_amd64.deb
--2024-07-29 11:16:25--  https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.8.1-1_amd64.deb
Resolving packages.wazuh.com (packages.wazuh.com)... 13.35.169.21, 13.35.169.119, 13.35.169.67, ...
Connecting to packages.wazuh.com (packages.wazuh.com)|13.35.169.21|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10270680 (9.8M) [binary/octet-stream]
Saving to: ‘wazuh-agent_4.8.1-1_amd64.deb.3’

wazuh-agent_4.8.1-1 100%[===================>]   9.79M  5.20MB/s    in 1.9s

2024-07-29 11:16:27 (5.20 MB/s) - ‘wazuh-agent_4.8.1-1_amd64.deb.3’ saved [10270680/10270680]

Selecting previously unselected package wazuh-agent.
(Reading database ... 200612 files and directories currently installed.)
Preparing to unpack .../wazuh-agent_4.8.1-1_amd64.deb ...
Unpacking wazuh-agent (4.8.1-1) ...
Setting up wazuh-agent (4.8.1-1) ...
```

To start the agent run the following commands:

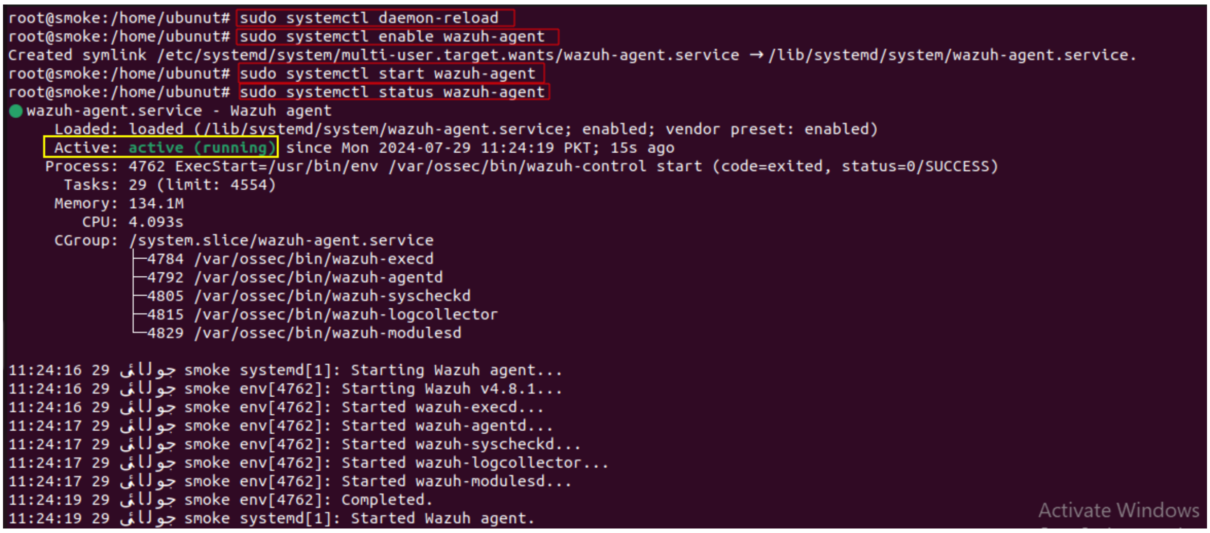


Start the agent:

```
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```

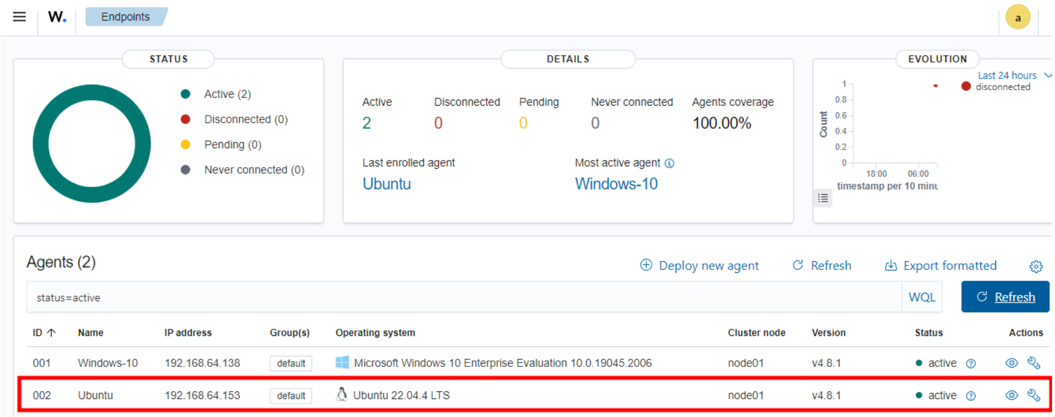
After wazuh starts, check if the wazuh service is up and running by using the following command.

sudo systemctl status wazuh-agent



```
root@smoke:/home/ubunut# sudo systemctl daemon-reload
root@smoke:/home/ubunut# sudo systemctl enable wazuh-agent
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service → /lib/systemd/system/wazuh-agent.service.
root@smoke:/home/ubunut# sudo systemctl start wazuh-agent
root@smoke:/home/ubunut# sudo systemctl status wazuh-agent
● wazuh-agent.service - Wazuh agent
     Loaded: loaded (/lib/systemd/system/wazuh-agent.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2024-07-29 11:24:19 PKT; 15s ago
    Process: 4762 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
      Tasks: 29 (limit: 4554)
     Memory: 134.1M
        CPU: 4.093s
     CGroup: /system.slice/wazuh-agent.service
             ├─4784 /var/ossec/bin/wazuh-execd
             ├─4792 /var/ossec/bin/wazuh-agentd
             ├─4805 /var/ossec/bin/wazuh-syscheckd
             ├─4815 /var/ossec/bin/wazuh-logcollector
             └─4829 /var/ossec/bin/wazuh-modulesd

11:24:16 29 جولائی smoke systemd[1]: Starting Wazuh agent...
11:24:16 29 جولائی smoke env[4762]: Starting Wazuh v4.8.1...
11:24:16 29 جولائی smoke env[4762]: Started wazuh-execd...
11:24:17 29 جولائی smoke env[4762]: Started wazuh-agentd...
11:24:17 29 جولائی smoke env[4762]: Started wazuh-syscheckd...
11:24:17 29 جولائی smoke env[4762]: Started wazuh-logcollector...
11:24:17 29 جولائی smoke env[4762]: Started wazuh-modulesd...
11:24:19 29 جولائی smoke env[4762]: Completed.
11:24:19 29 جولائی smoke systemd[1]: Started Wazuh agent.
```

And our Ubuntu Agent is up and active.



● Active (2)
● Disconnected (0)
● Pending (0)
● Never connected (0)

DETAILS

Active	Disconnected	Pending	Never connected	Agents coverage
2	0	0	0	100.00%

Last enrolled agent: Ubuntu

Most active agent: Windows-10

Agents (2)

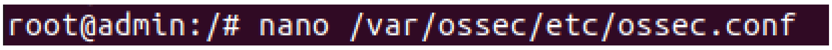
status=active

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	Windows-10	192.168.64.138	default	Microsoft Windows 10 Enterprise Evaluation 10.0.19045.2006	node01	v4.8.1	● active	
002	Ubuntu	192.168.64.153	default	Ubuntu 22.04.4 LTS	node01	v4.8.1	● active	

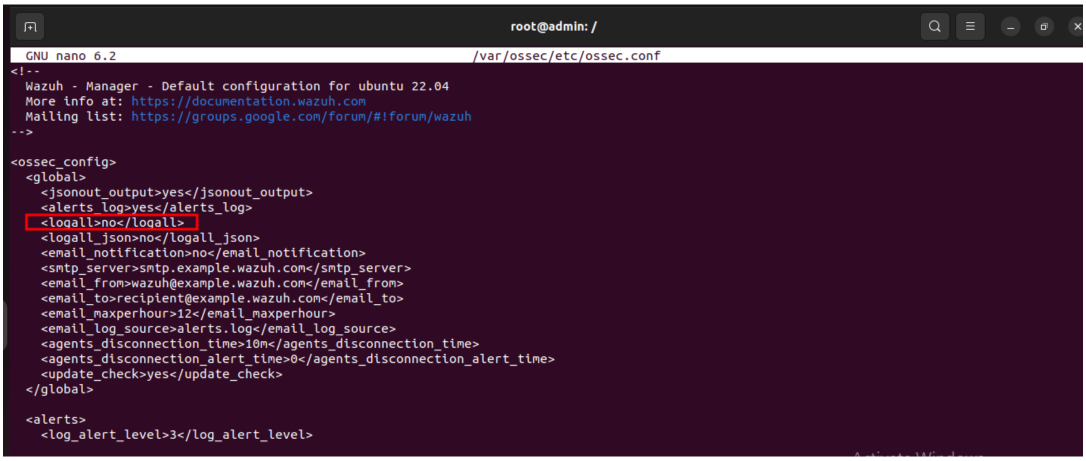
3. File Integrity Monitoring

3.1 Wazuh Ubuntu manager ossec.conf file configuration

Change the configuration of the **ossec.conf** file using the following command

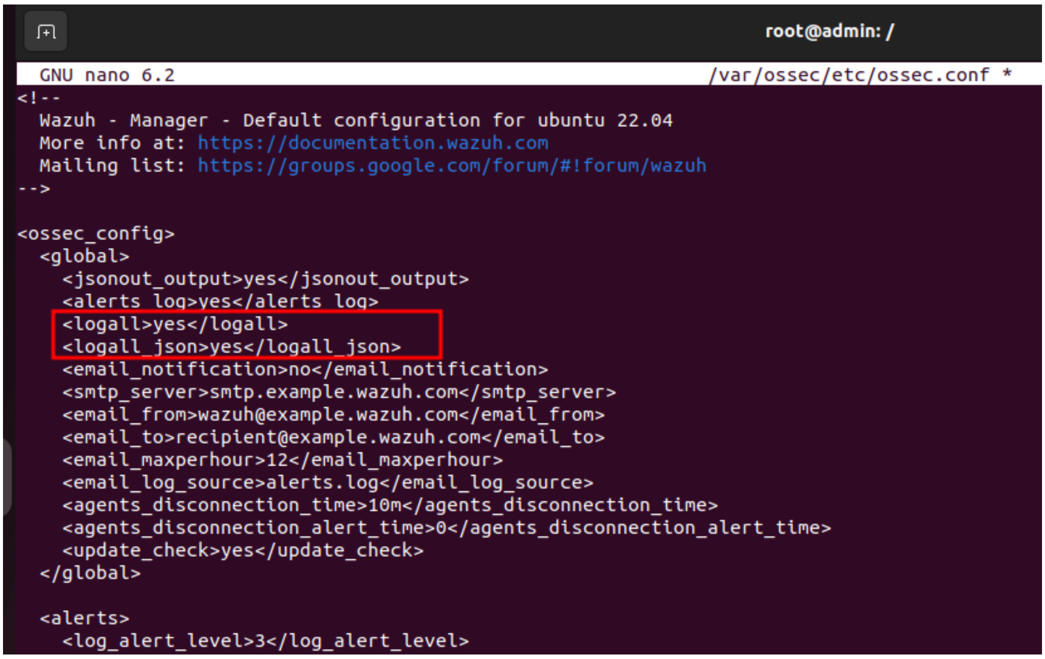


```
root@admin:/# nano /var/ossec/etc/ossec.conf
```



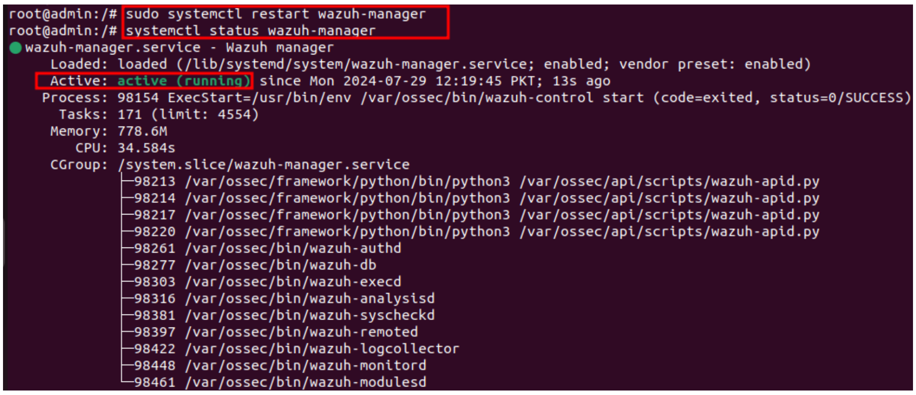
```
  GNU nano 6.2                                  /var/ossec/etc/ossec.conf
<!--
  Wazuh - Manager - Default configuration for ubuntu 22.04
  More info at: https://documentation.wazuh.com
  Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>no</logall>
    <logall_json>no</logall_json>
    <email_notification>no</email_notification>
    <smtp_server>smtp.example.wazuh.com</smtp_server>
    <email_from>wazuh@example.wazuh.com</email_from>
    <email_to>recipient@example.wazuh.com</email_to>
    <email_maxperhour>12</email_maxperhour>
    <email_log_source>alerts.log</email_log_source>
    <agents_disconnection_time>10m</agents_disconnection_time>
    <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
    <update_check>yes</update_check>
  </global>

  <alerts>
    <log_alert_level>3</log_alert_level>
```

Change the **logall** tag to **yes** to log all the alerts.



```
root@admin: /
GNU nano 6.2                                          /var/ossec/etc/ossec.conf *
<!--
  Wazuh - Manager - Default configuration for ubuntu 22.04
  More info at: https://documentation.wazuh.com
  Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>yes</logall>
    <logall_json>yes</logall_json>
    <email_notification>no</email_notification>
    <smtp_server>smtp.example.wazuh.com</smtp_server>
    <email_from>wazuh@example.wazuh.com</email_from>
    <email_to>recipient@example.wazuh.com</email_to>
    <email_maxperhour>12</email_maxperhour>
    <email_log_source>alerts.log</email_log_source>
    <agents_disconnection_time>10m</agents_disconnection_time>
    <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
    <update_check>yes</update_check>
  </global>

  <alerts>
    <log_alert_level>3</log_alert_level>
```

Restart the service and check its status.

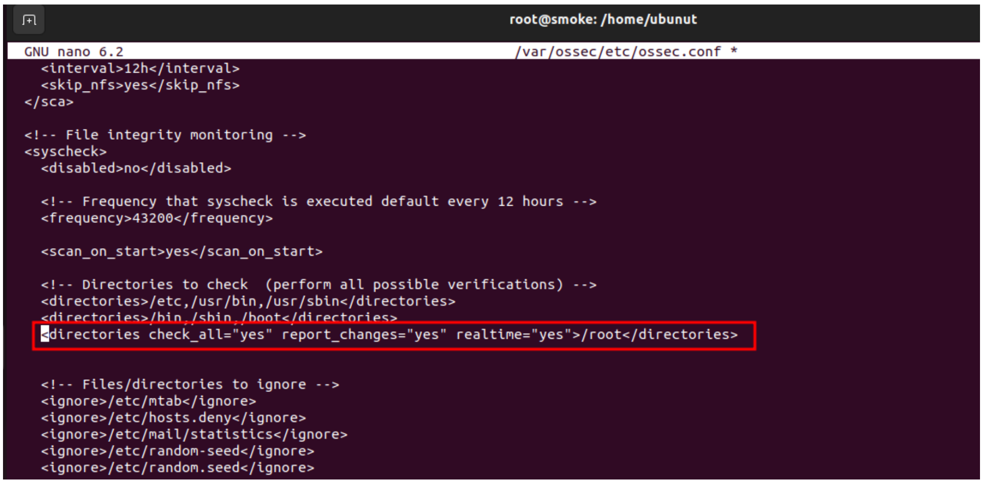


```
root@admin:/# sudo systemctl restart wazuh-manager
root@admin:/# systemctl status wazuh-manager
● wazuh-manager.service - Wazuh manager
     Loaded: loaded (/lib/systemd/system/wazuh-manager.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2024-07-29 12:19:45 PKT; 13s ago
    Process: 98154 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
      Tasks: 171 (limit: 4554)
     Memory: 778.6M
        CPU: 34.584s
     CGroup: /system.slice/wazuh-manager.service
             ├─98213 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             ├─98214 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             ├─98217 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             ├─98220 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             ├─98261 /var/ossec/bin/wazuh-authd
             ├─98277 /var/ossec/bin/wazuh-db
             ├─98303 /var/ossec/bin/wazuh-execd
             ├─98316 /var/ossec/bin/wazuh-analysisd
             ├─98381 /var/ossec/bin/wazuh-syscheckd
             ├─98397 /var/ossec/bin/wazuh-remoted
             ├─98422 /var/ossec/bin/wazuh-logcollector
             ├─98448 /var/ossec/bin/wazuh-monitord
             └─98461 /var/ossec/bin/wazuh-modulesd
```

3.2 Wazuh Ubuntu Agent ossec.conf file configuration

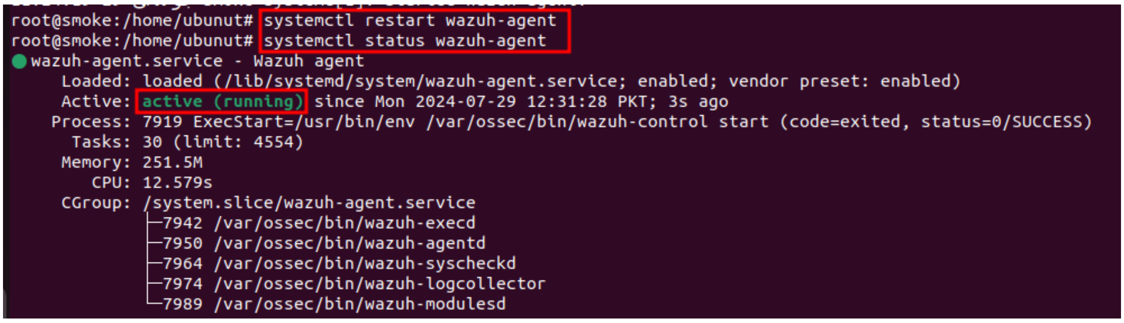
Added a new clause to check all the directories in real time and report all the changes.

Save the final configurations and exit the file.



```
root@smoke: /home/ubunut
GNU nano 6.2                                   /var/ossec/etc/ossec.conf *
    <interval>12h</interval>
    <skip_nfs>yes</skip_nfs>
  </sca>

  <!-- File integrity monitoring -->
  <syscheck>
    <disabled>no</disabled>

    <!-- Frequency that syscheck is executed default every 12 hours -->
    <frequency>43200</frequency>

    <scan_on_start>yes</scan_on_start>

    <!-- Directories to check  (perform all possible verifications) -->
    <directories>/etc,/usr/bin,/usr/sbin</directories>
    <directories>/bin,/sbin,/boot</directories>
    <directories check_all="yes" report_changes="yes" realtime="yes">/root</directories>


    <!-- Files/directories to ignore -->
    <ignore>/etc/mtab</ignore>
    <ignore>/etc/hosts.deny</ignore>
    <ignore>/etc/mail/statistics</ignore>
    <ignore>/etc/random-seed</ignore>
    <ignore>/etc/random.seed</ignore>
```

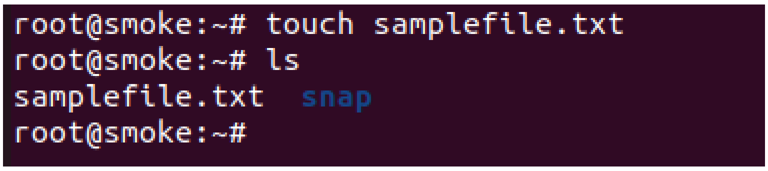
Restart the wazuh agent and check the status.



```
root@smoke:/home/ubunut# systemctl restart wazuh-agent
root@smoke:/home/ubunut# systemctl status wazuh-agent
● wazuh-agent.service - Wazuh agent
     Loaded: loaded (/lib/systemd/system/wazuh-agent.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2024-07-29 12:31:28 PKT; 3s ago
    Process: 7919 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
      Tasks: 30 (limit: 4554)
     Memory: 251.5M
        CPU: 12.579s
     CGroup: /system.slice/wazuh-agent.service
             ├─7942 /var/ossec/bin/wazuh-execd
             ├─7950 /var/ossec/bin/wazuh-agentd
             ├─7964 /var/ossec/bin/wazuh-syscheckd
             ├─7974 /var/ossec/bin/wazuh-logcollector
             └─7989 /var/ossec/bin/wazuh-modulesd
```

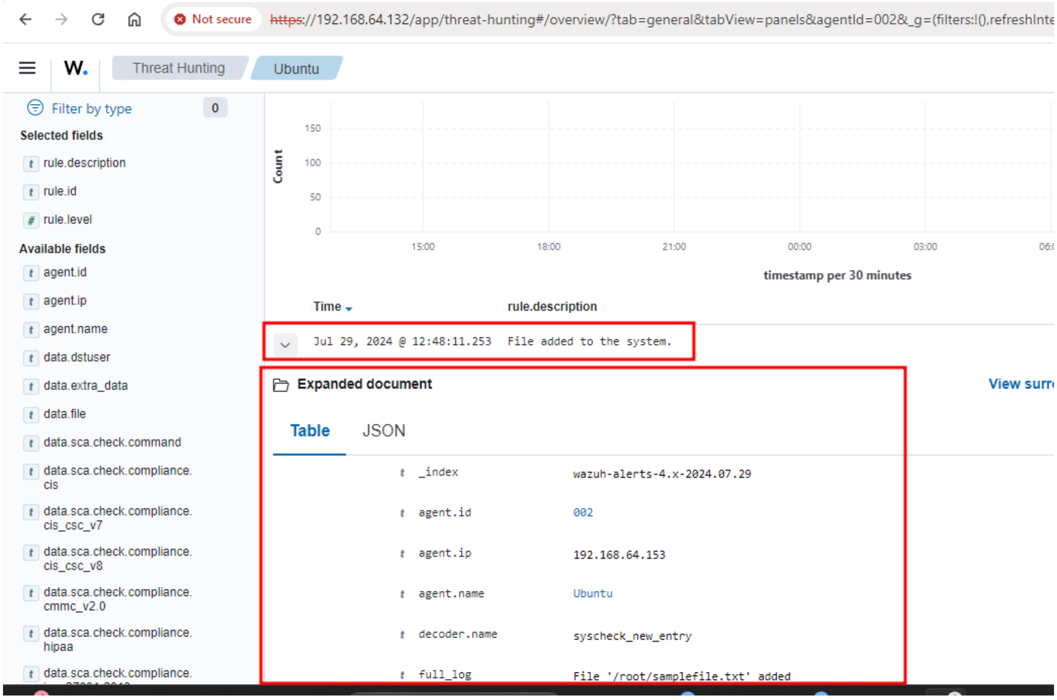
3.3 Testing Wazuh Alerts

Add a file in root directory. In this case I made a new file called **smaplefile.txt**.



```
root@smoke:~# touch samplefile.txt
root@smoke:~# ls
samplefile.txt  snap
root@smoke:~#
```

Now check the logs on wazuh dashboard. Wazuh is detecting and generating an alert for the new file added.



https://192.168.64.132/app/threat-hunting#/overview/?tab=general&tabView=panels&agentId=002&_g=(filters:!(),refreshInte

Time	rule.description
Jul 29, 2024 @ 12:48:11.253	File added to the system.

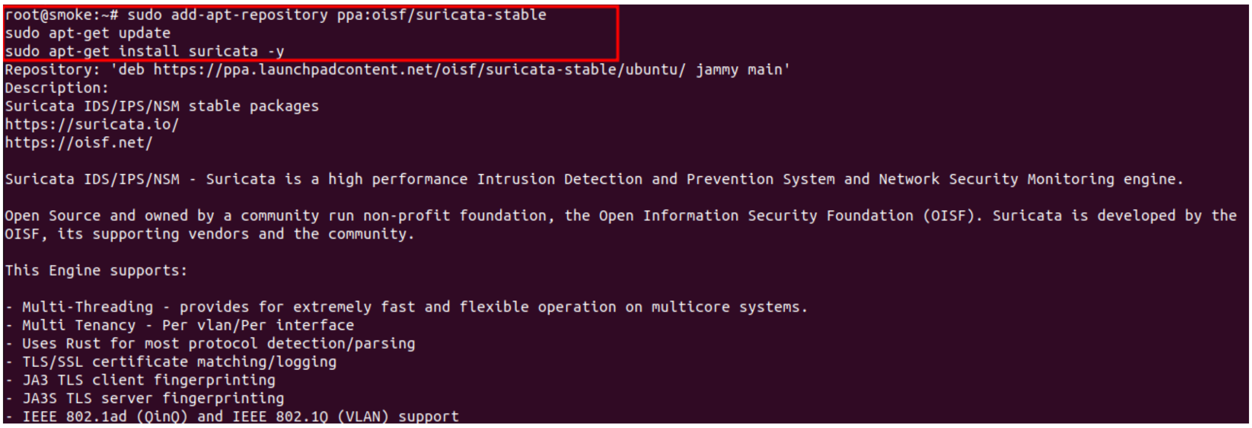
_index	wazuh-alerts-4.x-2024.07.29
agent.id	002
agent.ip	192.168.64.153
agent.name	Ubuntu
decoder.name	syscheck_new_entry
full_log	File '/root/samplefile.txt' added

4. Detecting Network Intrusion using Suricata IDS

4.1 Installing & Configuring Suricata on Ubuntu Agent

1. Install suricata using the following commands.

- **sudo add-apt-repository ppa:oisf/suricata-stable**
- **sudo apt-get update**
- **sudo apt-get install suricata -y**

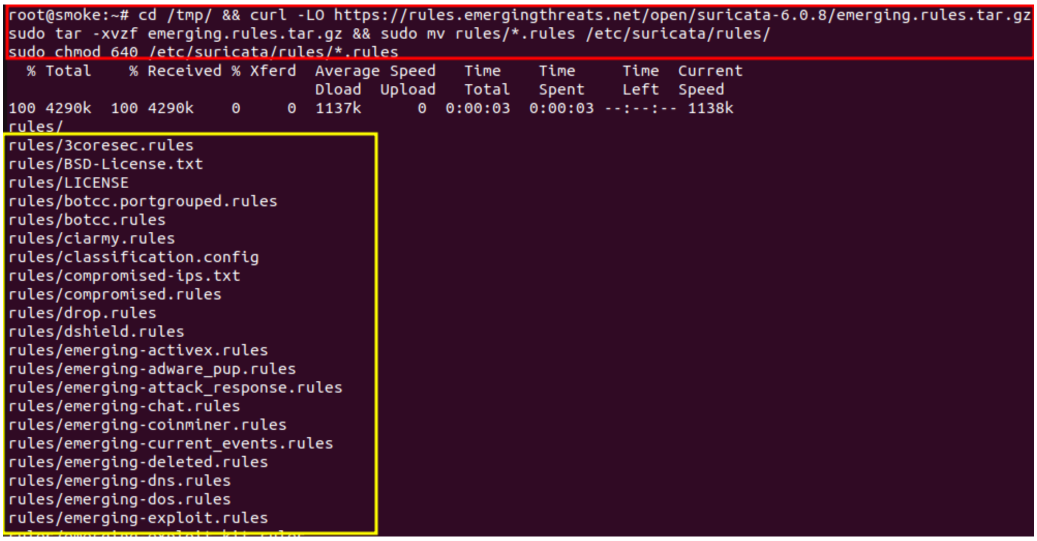


```
root@smoke:~# sudo add-apt-repository ppa:oisf/suricata-stable
sudo apt-get update
sudo apt-get install suricata -y
Repository: 'deb https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu/ jammy main'
Description:
Suricata IDS/IPS/NSM stable packages
https://suricata.io/
https://oisf.net/

Suricata IDS/IPS/NSM - Suricata is a high performance Intrusion Detection and Prevention System and Network Security Monitoring engine.

Open Source and owned by a community run non-profit foundation, the Open Information Security Foundation (OISF). Suricata is developed by the
OISF, its supporting vendors and the community.

This Engine supports:

- Multi-Threading - provides for extremely fast and flexible operation on multicore systems.
- Multi Tenancy - Per vlan/Per interface
- Uses Rust for most protocol detection/parsing
- TLS/SSL certificate matching/logging
- JA3 TLS client fingerprinting
- JA3S TLS server fingerprinting
- IEEE 802.1ad (QinQ) and IEEE 802.1Q (VLAN) support
```

2. Download & Install the Emerging threats Suricata ruleset.

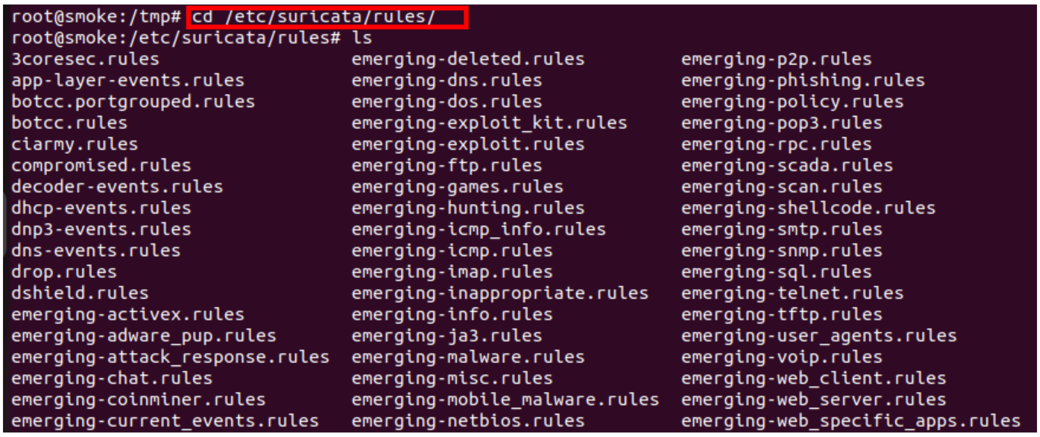
- **cd /tmp/ && curl -LO https://rules.emergingthreats.net/open/suricata-6.0.8/emerging.rules.tar.gz**
- **sudo tar -xvzf emerging.rules.tar.gz && sudo mv rules/*.rules /etc/suricata/rules/**
- **sudo chmod 640 /etc/suricata/rules/*.rules**

Note: Suricata is an IDS, it cannot work unless you have a rule set for it to work on. Emerging threat is a community which builds the rules for IDS like Suricata, which can be used directly by installing on your machine.



```
root@smoke:~# cd /tmp/ && curl -LO https://rules.emergingthreats.net/open/suricata-6.0.8/emerging.rules.tar.gz
sudo tar -xvzf emerging.rules.tar.gz && sudo mv rules/*.rules /etc/suricata/rules/
sudo chmod 640 /etc/suricata/rules/*.rules
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 4290k  100 4290k    0     0  1137k      0  0:00:03  0:00:03 --:--:-- 1138k
rules/
rules/3coresec.rules
rules/BSD-License.txt
rules/LICENSE
rules/botcc.portgrouped.rules
rules/botcc.rules
rules/ciarmy.rules
rules/classification.config
rules/compromised-ips.txt
rules/compromised.rules
rules/drop.rules
rules/dshield.rules
rules/emerging-activex.rules
rules/emerging-adware_pup.rules
rules/emerging-attack_response.rules
rules/emerging-chat.rules
rules/emerging-coinminer.rules
rules/emerging-current_events.rules
rules/emerging-deleted.rules
rules/emerging-dns.rules
rules/emerging-dos.rules
rules/emerging-exploit.rules
```

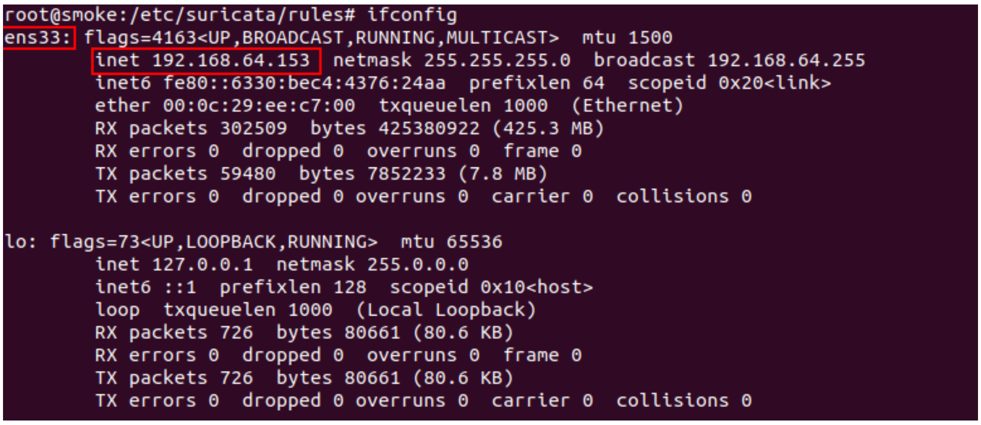
View all the Suricata rules in the rule's directory.



```
root@smoke:/tmp# cd /etc/suricata/rules/
root@smoke:/etc/suricata/rules# ls
3coresec.rules                  emerging-deleted.rules          emerging-p2p.rules
app-layer-events.rules          emerging-dns.rules              emerging-phishing.rules
botcc.portgrouped.rules         emerging-dos.rules              emerging-policy.rules
botcc.rules                     emerging-exploit_kit.rules      emerging-pop3.rules
ciarmy.rules                    emerging-exploit.rules          emerging-rpc.rules
compromised.rules               emerging-ftp.rules              emerging-scada.rules
decoder-events.rules            emerging-games.rules            emerging-scan.rules
dhcp-events.rules               emerging-hunting.rules          emerging-shellcode.rules
dnp3-events.rules               emerging-icmp_info.rules        emerging-smtp.rules
dns-events.rules                emerging-icmp.rules             emerging-snmp.rules
drop.rules                      emerging-imap.rules             emerging-sql.rules
dshield.rules                   emerging-inappropriate.rules    emerging-telnet.rules
emerging-activex.rules          emerging-info.rules             emerging-tftp.rules
emerging-adware_pup.rules       emerging-ja3.rules              emerging-user_agents.rules
emerging-attack_response.rules  emerging-malware.rules          emerging-voip.rules
emerging-chat.rules             emerging-misc.rules             emerging-web_client.rules
emerging-coinminer.rules        emerging-mobile_malware.rules   emerging-web_server.rules
emerging-current_events.rules   emerging-netbios.rules          emerging-web_specific_apps.rules
```

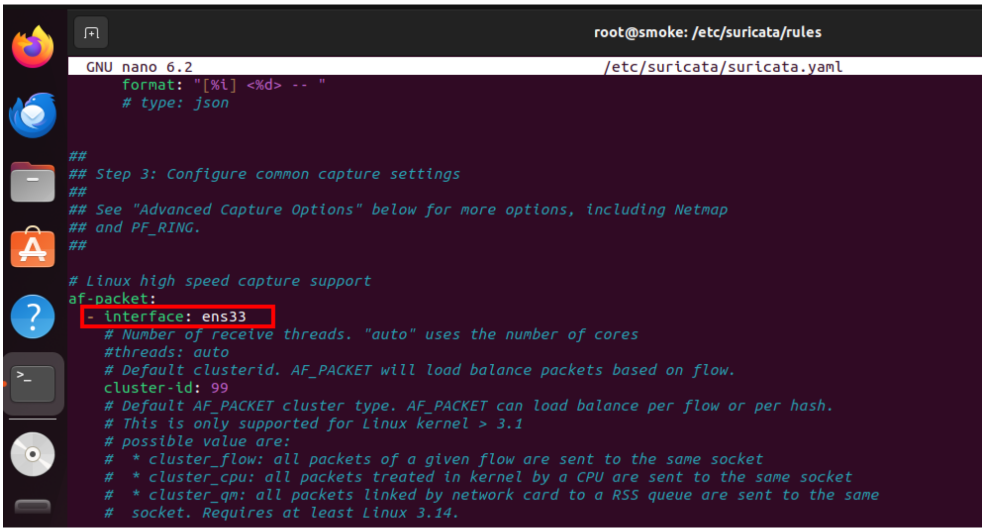
3. Modify Suricata settings in the **/etc/suricata/suricata.yaml** file and set the following variables.

Check the network interface and ubuntu agent IP using the **ifconfig** command for future use.



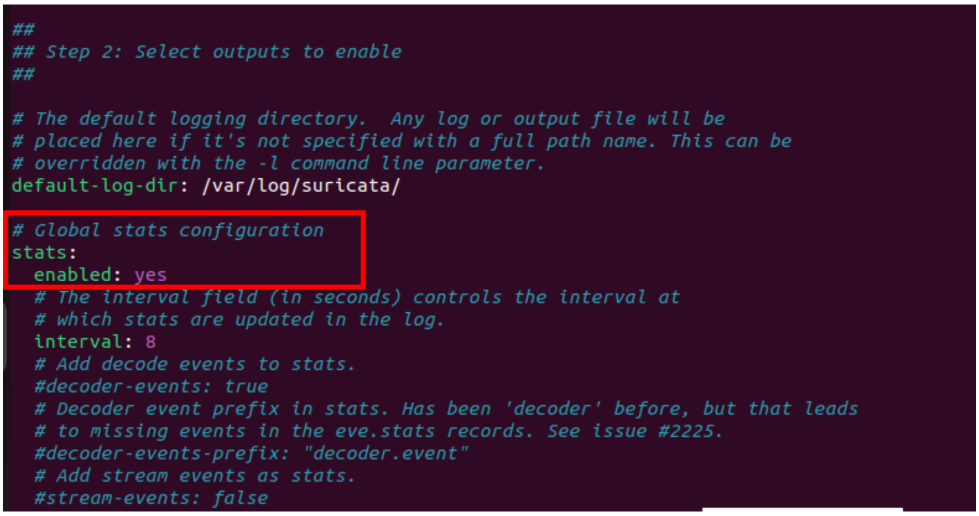
```
root@smoke:/etc/suricata/rules# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.64.153  netmask 255.255.255.0  broadcast 192.168.64.255
        inet6 fe80::6330:bec4:4376:24aa  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:ee:c7:00  txqueuelen 1000  (Ethernet)
        RX packets 302509  bytes 425380922 (425.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 59480  bytes 7852233 (7.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 726  bytes 80661 (80.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 726  bytes 80661 (80.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

i. Change the network interface to your own interface. In my case my network interface in **ens33**.



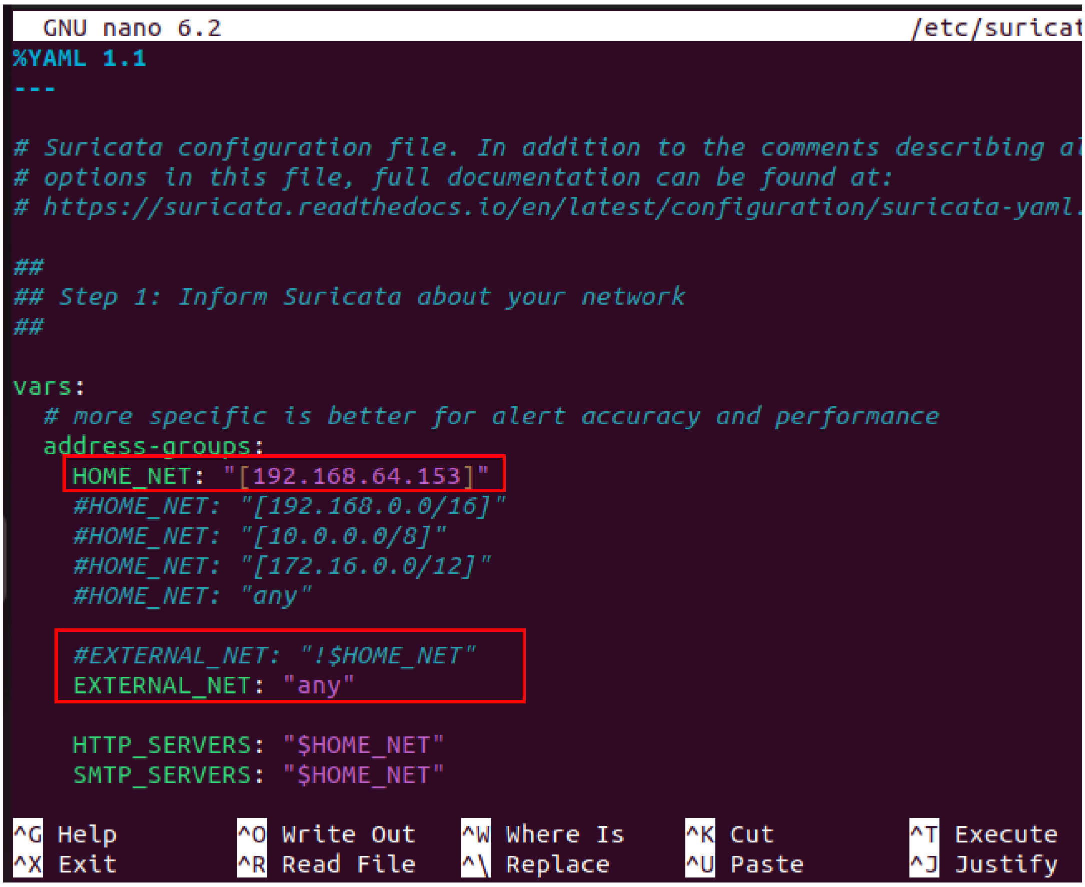
```
GNU nano 6.2                                    /etc/suricata/suricata.yaml
      format: "[%i] <%d> -- "
      # type: json


##
## Step 3: Configure common capture settings
##
## See "Advanced Capture Options" below for more options, including Netmap
## and PF_RING.
##

# Linux high speed capture support
af-packet:
  - interface: ens33
    # Number of receive threads. "auto" uses the number of cores
    #threads: auto
    # Default clusterid. AF_PACKET will load balance packets based on flow.
    cluster-id: 99
    # Default AF_PACKET cluster type. AF_PACKET can load balance per flow or per hash.
    # This is only supported for Linux kernel > 3.1
    # possible value are:
    #  * cluster_flow: all packets of a given flow are sent to the same socket
    #  * cluster_cpu: all packets treated in kernel by a CPU are sent to the same socket
    #  * cluster_qm: all packets linked by network card to a RSS queue are sent to the same
    #  socket. Requires at least Linux 3.14.
```

ii. Enable Global stats.



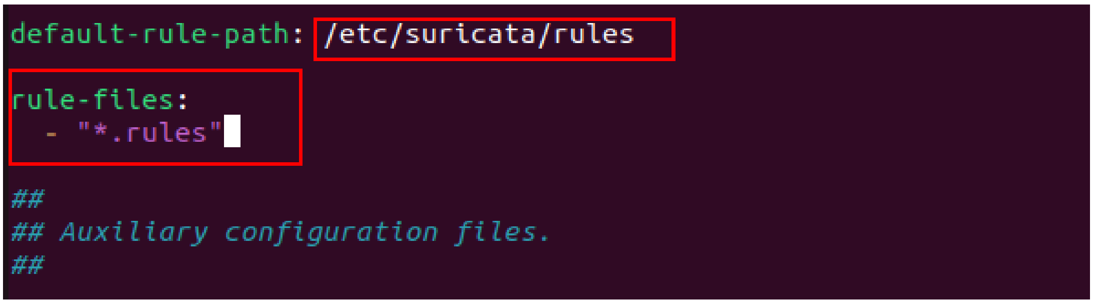
```
##
## Step 2: Select outputs to enable
##

# The default logging directory.  Any log or output file will be
# placed here if it's not specified with a full path name. This can be
# overridden with the -l command line parameter.
default-log-dir: /var/log/suricata/

# Global stats configuration
stats:
  enabled: yes
  # The interval field (in seconds) controls the interval at
  # which stats are updated in the log.
  interval: 8
  # Add decode events to stats.
  #decoder-events: true
  # Decoder event prefix in stats. Has been 'decoder' before, but that leads
  # to missing events in the eve.stats records. See issue #2225.
  #decoder-events-prefix: "decoder.event"
  # Add stream events as stats.
  #stream-events: false
```

Fix your Home NET IP to Ubuntu agent’s IP.



```
  GNU nano 6.2                                                 /etc/suricat
%YAML 1.1
---

# Suricata configuration file. In addition to the comments describing al
# options in this file, full documentation can be found at:
# https://suricata.readthedocs.io/en/latest/configuration/suricata-yaml.

##
## Step 1: Inform Suricata about your network
##

vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[192.168.64.153]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"

    #EXTERNAL_NET: "!$HOME_NET"
    EXTERNAL_NET: "any"

    HTTP_SERVERS: "$HOME_NET"
    SMTP_SERVERS: "$HOME_NET"

^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify
```

iii. Give it the file directory and use the wildcard * with rules to include all the rules files.

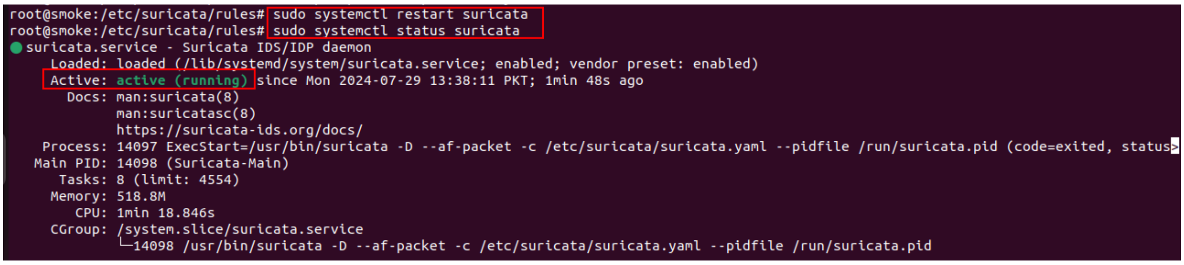


```
default-rule-path: /etc/suricata/rules

rule-files:
  - "*.rules"

##
## Auxiliary configuration files.
##
```

4. Restart the Suricata Deamon to save the changes and then check the suricata service status.

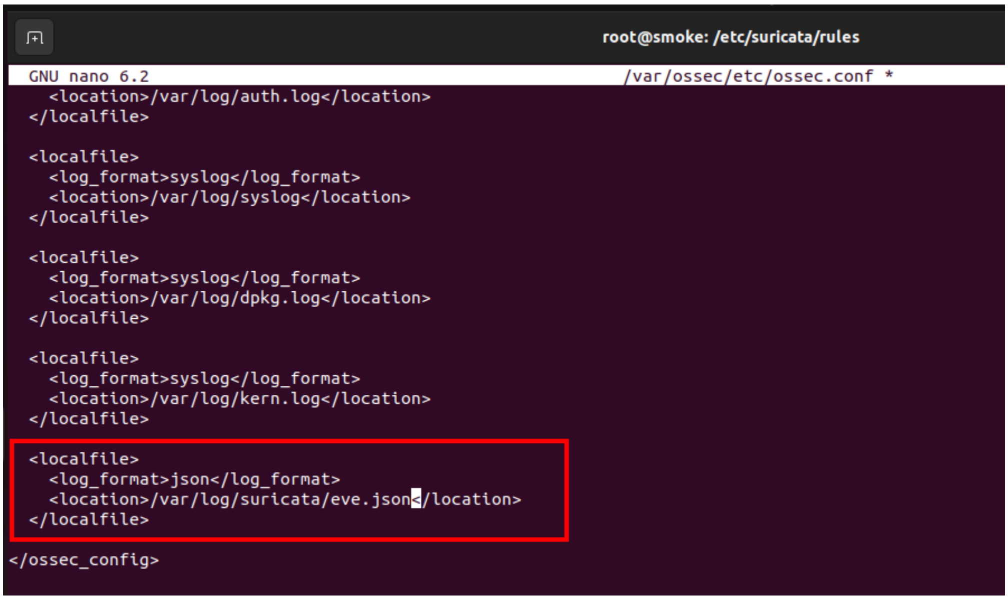
sudo systemctl restart suricata

sudo systemctl status suricata



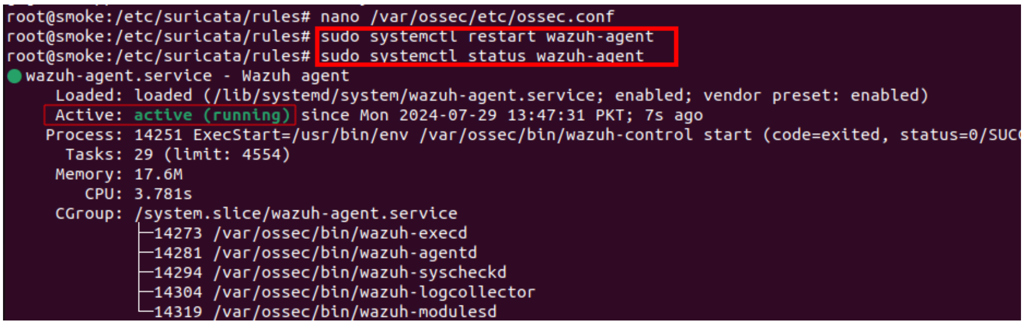
```
root@smoke:/etc/suricata/rules# sudo systemctl restart suricata
root@smoke:/etc/suricata/rules# sudo systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
     Loaded: loaded (/lib/systemd/system/suricata.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2024-07-29 13:38:11 PKT; 1min 48s ago
       Docs: man:suricata(8)
             man:suricatasc(8)
             https://suricata-ids.org/docs/
    Process: 14097 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid (code=exited, status>
   Main PID: 14098 (Suricata-Main)
      Tasks: 8 (limit: 4554)
     Memory: 518.8M
        CPU: 1min 18.846s
     CGroup: /system.slice/suricata.service
             └─14098 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid
```

5. Call the Suricata file in ossec.conf file



```
GNU nano 6.2                                          /var/ossec/etc/ossec.conf *
    <location>/var/log/auth.log</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/syslog</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/dpkg.log</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/kern.log</location>
  </localfile>

  <localfile>
    <log_format>json</log_format>
    <location>/var/log/suricata/eve.json</location>
  </localfile>

</ossec_config>
```

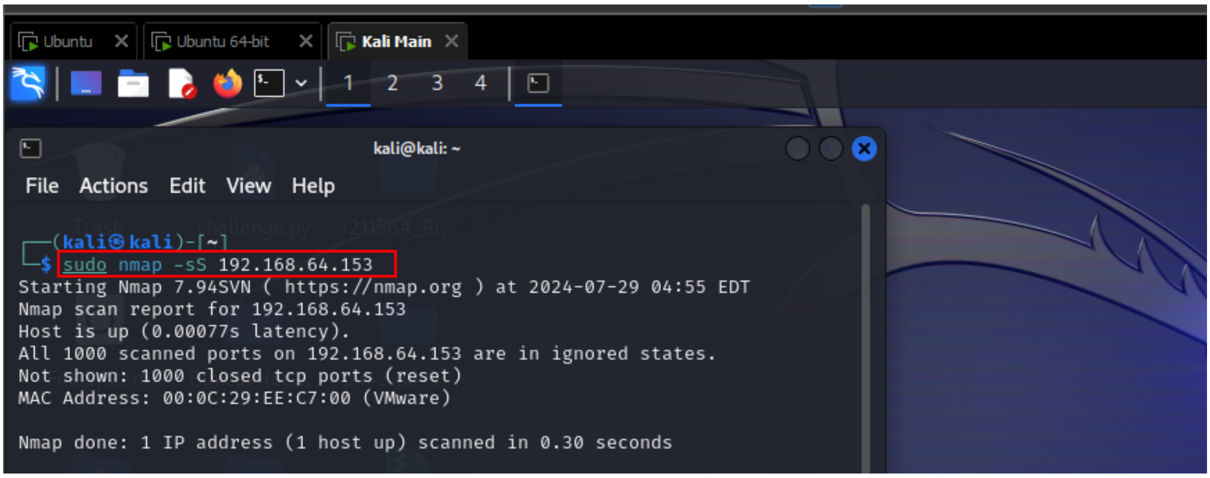
To take effect of this change, restart the wazuh agent and check its status.



```
root@smoke:/etc/suricata/rules# nano /var/ossec/etc/ossec.conf
root@smoke:/etc/suricata/rules# sudo systemctl restart wazuh-agent
root@smoke:/etc/suricata/rules# sudo systemctl status wazuh-agent
● wazuh-agent.service - Wazuh agent
     Loaded: loaded (/lib/systemd/system/wazuh-agent.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2024-07-29 13:47:31 PKT; 7s ago
    Process: 14251 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUC
      Tasks: 29 (limit: 4554)
     Memory: 17.6M
        CPU: 3.781s
     CGroup: /system.slice/wazuh-agent.service
             ├─14273 /var/ossec/bin/wazuh-execd
             ├─14281 /var/ossec/bin/wazuh-agentd
             ├─14294 /var/ossec/bin/wazuh-syscheckd
             ├─14304 /var/ossec/bin/wazuh-logcollector
             └─14319 /var/ossec/bin/wazuh-modulesd
```

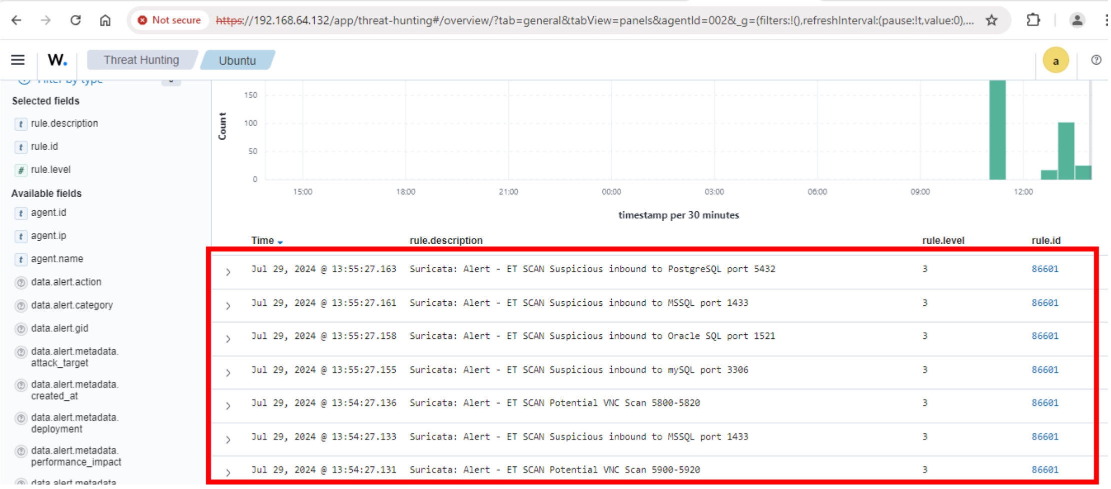
4.2 Testing Suricata Rules by performing attacks.

1. Nmap scan
    a. Performed nmap scan from another VM connected tot he same network.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.64.153
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-29 04:55 EDT
Nmap scan report for 192.168.64.153
Host is up (0.00077s latency).
All 1000 scanned ports on 192.168.64.153 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:0C:29:EE:C7:00 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

b. Wazuh detects Suricata scans and generate events for it.



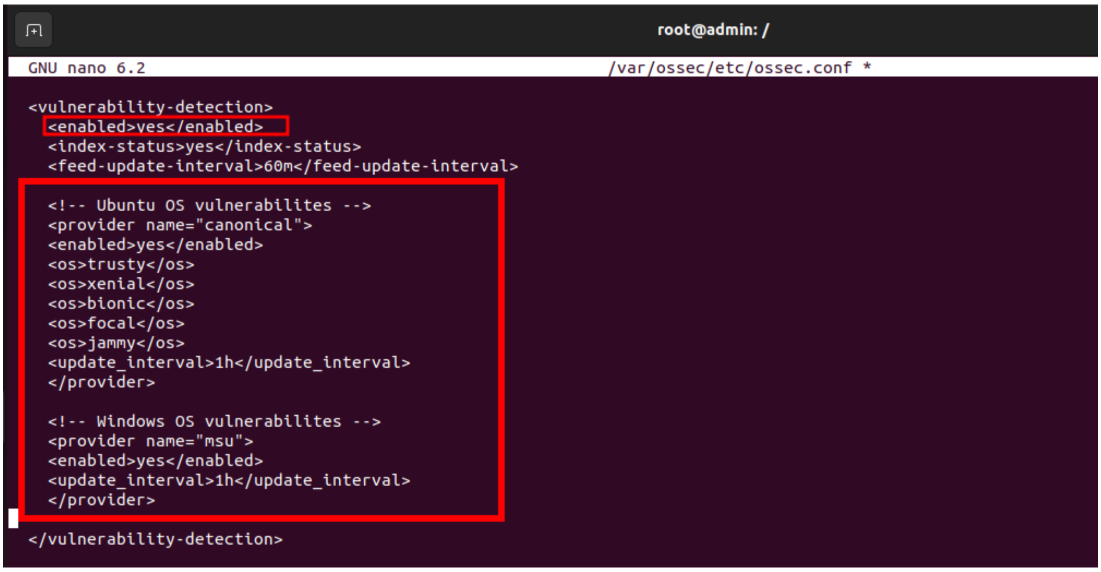
Not secure
https://192.168.64.132/app/threat-hunting#/overview/?tab=general&tabView=panels&agentId=002&_g=(filters:!(),refreshInterval:(pause:!t,value:0),...
W.
Threat Hunting
Ubuntu
a
Selected fields
rule.description
rule.id
rule.level
Available fields
agent.id
agent.ip
agent.name
data.alert.action
data.alert.category
data.alert.gid
data.alert.metadata.attack_target
data.alert.metadata.created_at
data.alert.metadata.deployment
data.alert.metadata.performance_impact
Count
150
100
50
0
15:00
18:00
21:00
00:00
03:00
06:00
09:00
12:00
timestamp per 30 minutes

Time	rule.description	rule.level	rule.id
Jul 29, 2024 @ 13:55:27.163	Suricata: Alert - ET SCAN Suspicious inbound to PostgreSQL port 5432	3	86601
Jul 29, 2024 @ 13:55:27.161	Suricata: Alert - ET SCAN Suspicious inbound to MSSQL port 1433	3	86601
Jul 29, 2024 @ 13:55:27.158	Suricata: Alert - ET SCAN Suspicious inbound to Oracle SQL port 1521	3	86601
Jul 29, 2024 @ 13:55:27.155	Suricata: Alert - ET SCAN Suspicious inbound to mySQL port 3306	3	86601
Jul 29, 2024 @ 13:54:27.136	Suricata: Alert - ET SCAN Potential VNC Scan 5800-5820	3	86601
Jul 29, 2024 @ 13:54:27.133	Suricata: Alert - ET SCAN Suspicious inbound to MSSQL port 1433	3	86601
Jul 29, 2024 @ 13:54:27.131	Suricata: Alert - ET SCAN Potential VNC Scan 5900-5920	3	86601

5. Detecting Vulnerabilities on Wazuh Agent

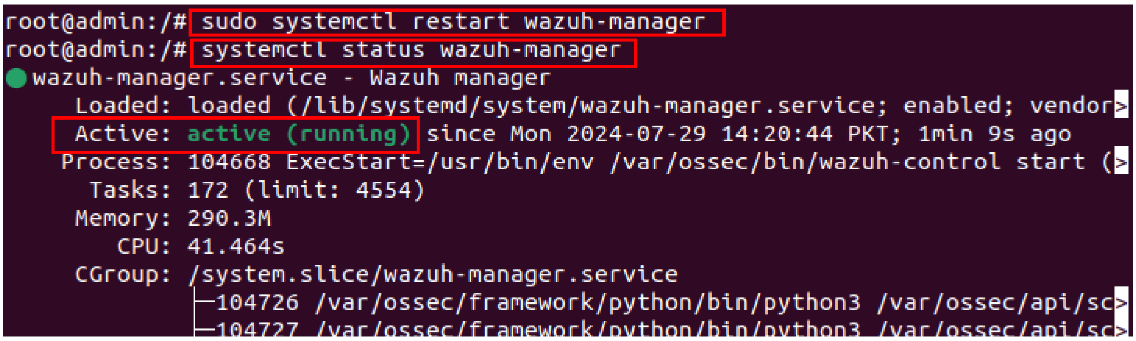
5.1 Update the ossec.conf file in Wazuh manager

1. Update the ossec.conf file in wazuh manager so that it detects Windows & Ubuntu vulnerabilities.



```
root@admin: /
GNU nano 6.2                                   /var/ossec/etc/ossec.conf *

<vulnerability-detection>
  <enabled>yes</enabled>
  <index-status>yes</index-status>
  <feed-update-interval>60m</feed-update-interval>

  <!-- Ubuntu OS vulnerabilites -->
  <provider name="canonical">
  <enabled>yes</enabled>
  <os>trusty</os>
  <os>xenial</os>
  <os>bionic</os>
  <os>focal</os>
  <os>jammy</os>
  <update_interval>1h</update_interval>
  </provider>

  <!-- Windows OS vulnerabilites -->
  <provider name="msu">
  <enabled>yes</enabled>
  <update_interval>1h</update_interval>
  </provider>

</vulnerability-detection>
```

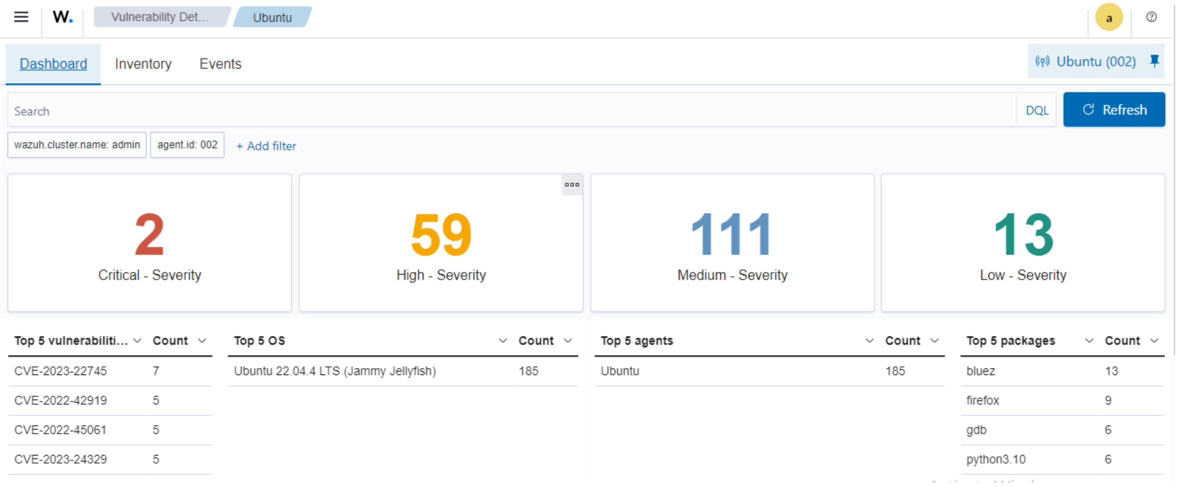
2. Restart Wazuh manager to save the changes and check the wazuh manager status.



```
root@admin:/# sudo systemctl restart wazuh-manager
root@admin:/# systemctl status wazuh-manager
● wazuh-manager.service - Wazuh manager
     Loaded: loaded (/lib/systemd/system/wazuh-manager.service; enabled; vendor>
     Active: active (running) since Mon 2024-07-29 14:20:44 PKT; 1min 9s ago
    Process: 104668 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (>
      Tasks: 172 (limit: 4554)
     Memory: 290.3M
        CPU: 41.464s
     CGroup: /system.slice/wazuh-manager.service
             ├─104726 /var/ossec/framework/python/bin/python3 /var/ossec/api/sc>
             ├─104727 /var/ossec/framework/python/bin/python3 /var/ossec/api/sc>
```

5.2 Testing Vulnerability detection using Wazuh Dashboard.

Now the vulnerability detection dashboard will detect OS vulnerabilities and further categorize them according to their severity level.



2 Critical - Severity

59 High - Severity

111 Medium - Severity

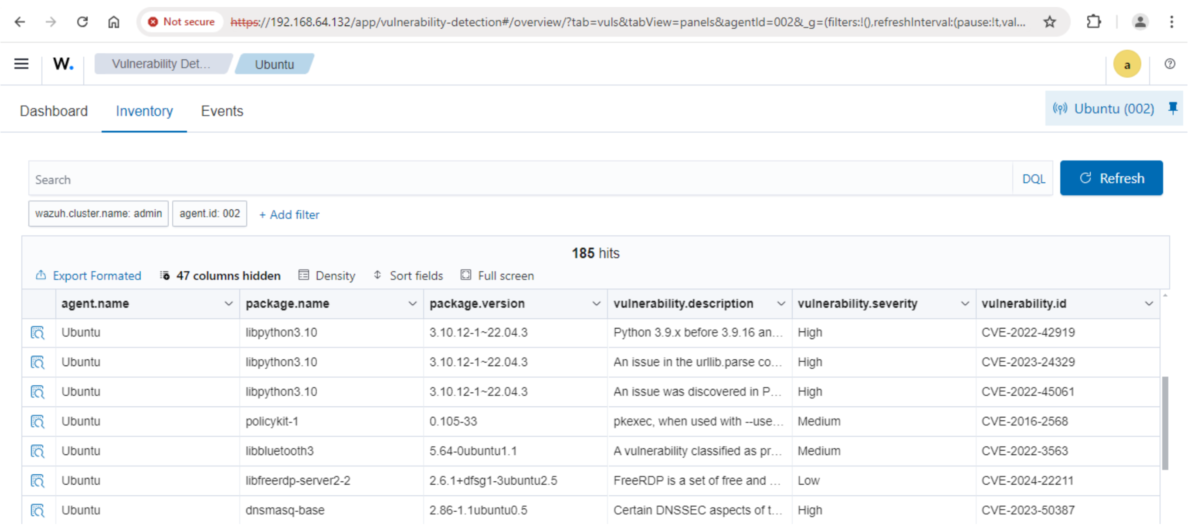
13 Low - Severity

Top 5 vulnerabiliti...	Count
CVE-2023-22745	7
CVE-2022-42919	5
CVE-2022-45061	5
CVE-2023-24329	5

Top 5 OS	Count
Ubuntu 22.04.4 LTS (Jammy Jellyfish)	185

Top 5 agents	Count
Ubuntu	185

Top 5 packages	Count
bluez	13
firefox	9
gdb	6
python3.10	6



https://192.168.64.132/app/vulnerability-detection#/overview/?tab=vuls&tabView=panels&agentId=002&_g=(filters:!(),refreshInterval:(pause:!t,val...

185 hits

agent.name	package.name	package.version	vulnerability.description	vulnerability.severity	vulnerability.id
Ubuntu	libpython3.10	3.10.12-1~22.04.3	Python 3.9.x before 3.9.16 an...	High	CVE-2022-42919
Ubuntu	libpython3.10	3.10.12-1~22.04.3	An issue in the urllib.parse co...	High	CVE-2023-24329
Ubuntu	libpython3.10	3.10.12-1~22.04.3	An issue was discovered in P...	High	CVE-2022-45061
Ubuntu	policykit-1	0.105-33	pkexec, when used with --use...	Medium	CVE-2016-2568
Ubuntu	libbluetooth3	5.64-0ubuntu1.1	A vulnerability classified as pr...	Medium	CVE-2022-3563
Ubuntu	libfreerdp-server2-2	2.6.1+dfsg1-3ubuntu2.5	FreeRDP is a set of free and ...	Low	CVE-2024-22211
Ubuntu	dnsmasq-base	2.86-1.1ubuntu0.5	Certain DNSSEC aspects of t...	High	CVE-2023-50387

6. Detecting Execution of Malicious Commands

6.1 Use Auditd to detect execution of malicious commands executed in Linux

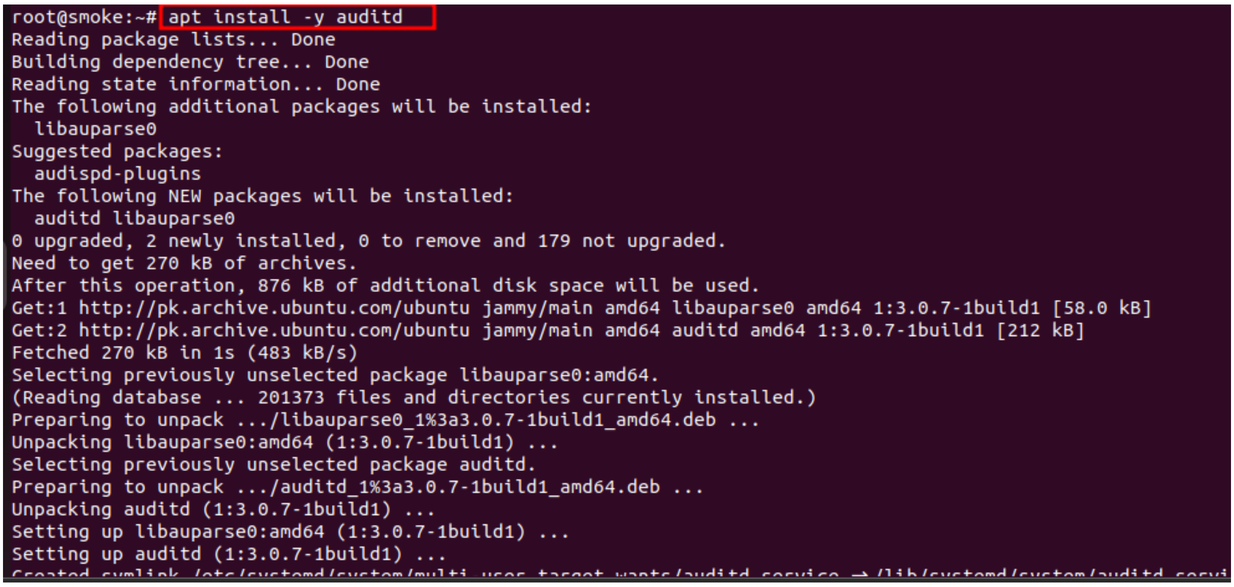
Auditd is the Linux auditing system’s user space component, used for monitoring & logging system activities. Auditd can perform the following functionalities.

a. System Call tracking: Logs system calls made by applications to the operating system.

b. User Activity Logging: Records user actions like logins, commands executions, and file accesses.

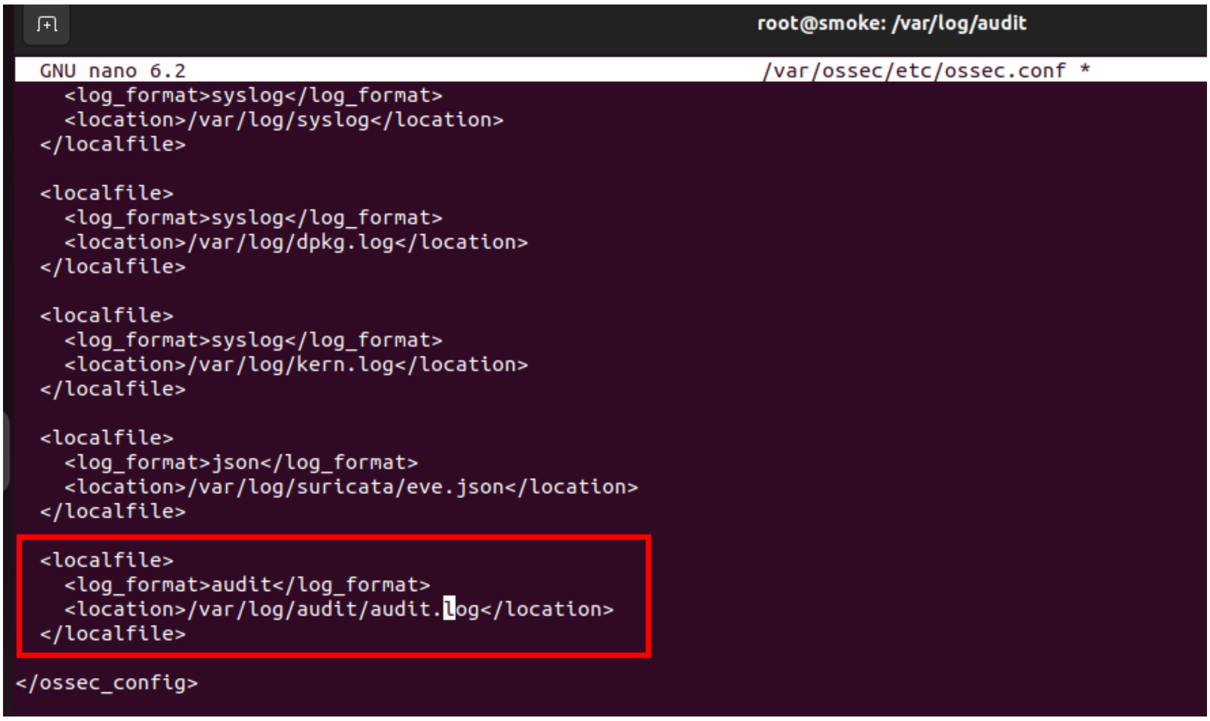
c. Security Monitoring: Enhances security by auditing access to sensitive parts of the system.

1. Install Auditd on wazuh client (ubunut).



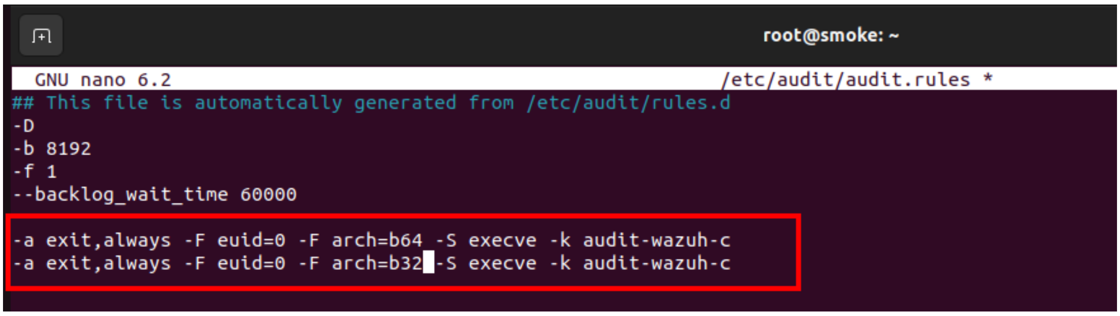
```
root@smoke:~# apt install -y auditd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libauparse0
Suggested packages:
  audispd-plugins
The following NEW packages will be installed:
  auditd libauparse0
0 upgraded, 2 newly installed, 0 to remove and 179 not upgraded.
Need to get 270 kB of archives.
After this operation, 876 kB of additional disk space will be used.
Get:1 http://pk.archive.ubuntu.com/ubuntu jammy/main amd64 libauparse0 amd64 1:3.0.7-1build1 [58.0 kB]
Get:2 http://pk.archive.ubuntu.com/ubuntu jammy/main amd64 auditd amd64 1:3.0.7-1build1 [212 kB]
Fetched 270 kB in 1s (483 kB/s)
Selecting previously unselected package libauparse0:amd64.
(Reading database ... 201373 files and directories currently installed.)
Preparing to unpack .../libauparse0_1%3a3.0.7-1build1_amd64.deb ...
Unpacking libauparse0:amd64 (1:3.0.7-1build1) ...
Selecting previously unselected package auditd.
Preparing to unpack .../auditd_1%3a3.0.7-1build1_amd64.deb ...
Unpacking auditd (1:3.0.7-1build1) ...
Setting up libauparse0:amd64 (1:3.0.7-1build1) ...
Setting up auditd (1:3.0.7-1build1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/auditd.service → /lib/systemd/system/auditd.servi
```

2. Add the log file path to ossec.conf file on wazuh client.



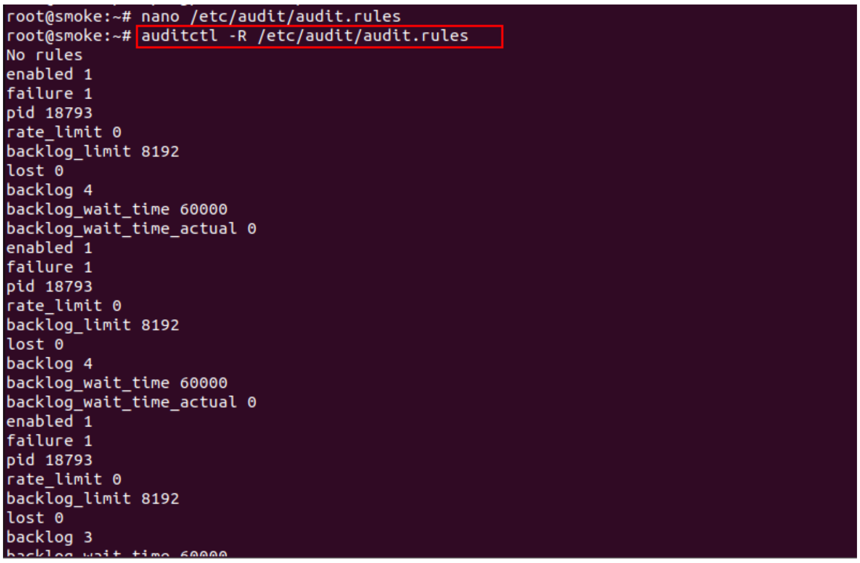
```
  GNU nano 6.2                                        /var/ossec/etc/ossec.conf *
    <log_format>syslog</log_format>
    <location>/var/log/syslog</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/dpkg.log</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/kern.log</location>
  </localfile>

  <localfile>
    <log_format>json</log_format>
    <location>/var/log/suricata/eve.json</location>
  </localfile>

  <localfile>
    <log_format>audit</log_format>
    <location>/var/log/audit/audit.log</location>
  </localfile>

</ossec_config>
```

3. **Use Case**: Add Rules to detect any command executed by root user.



```
  GNU nano 6.2                                  /etc/audit/audit.rules *
## This file is automatically generated from /etc/audit/rules.d
-D
-b 8192
-f 1
--backlog_wait_time 60000

-a exit,always -F euid=0 -F arch=b64 -S execve -k audit-wazuh-c
-a exit,always -F euid=0 -F arch=b32 -S execve -k audit-wazuh-c
```

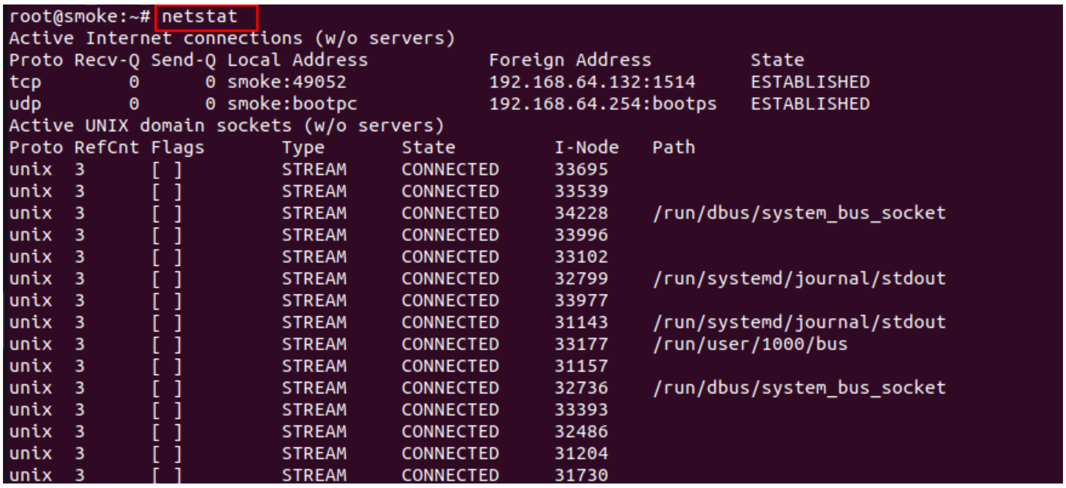
4. Restart the auditd rules.



```
root@smoke:~# nano /etc/audit/audit.rules
root@smoke:~# auditctl -R /etc/audit/audit.rules
No rules
enabled 1
failure 1
pid 18793
rate_limit 0
backlog_limit 8192
lost 0
backlog 4
backlog_wait_time 60000
backlog_wait_time_actual 0
enabled 1
failure 1
pid 18793
rate_limit 0
backlog_limit 8192
lost 0
backlog 4
backlog_wait_time 60000
backlog_wait_time_actual 0
enabled 1
failure 1
pid 18793
rate_limit 0
backlog_limit 8192
lost 0
backlog 3
backlog_wait_time 60000
```

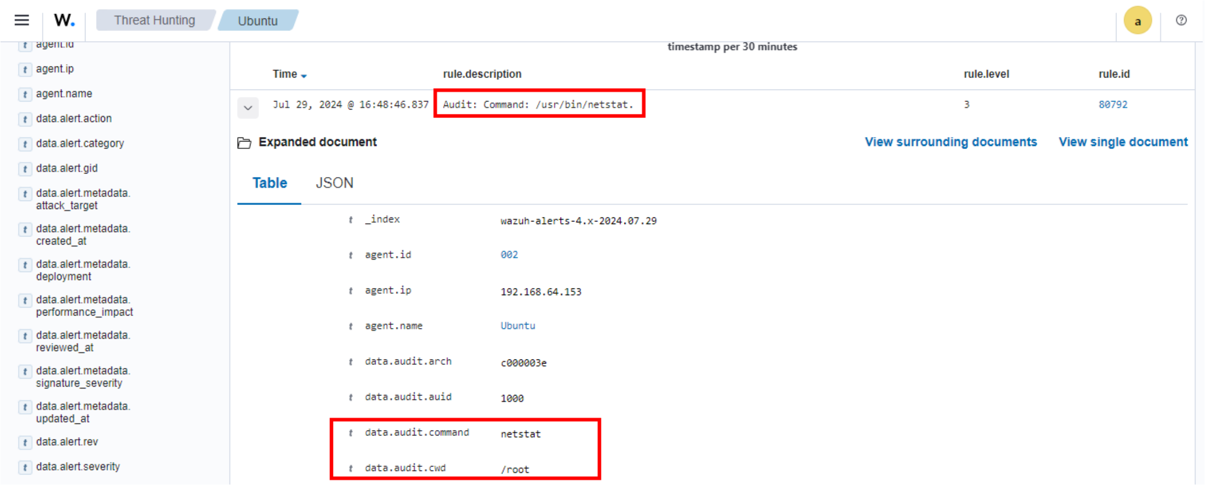
6.2 Testing by executing commands with root privileges

1. For testing I ran the netstat command.



```
root@smoke:~# netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 smoke:49052             192.168.64.132:1514     ESTABLISHED
udp        0      0 smoke:bootpc            192.168.64.254:bootps   ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         STREAM     CONNECTED     33695
unix  3      [ ]         STREAM     CONNECTED     33539
unix  3      [ ]         STREAM     CONNECTED     34228    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     33996
unix  3      [ ]         STREAM     CONNECTED     33102
unix  3      [ ]         STREAM     CONNECTED     32799    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     33977
unix  3      [ ]         STREAM     CONNECTED     31143    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     33177    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     31157
unix  3      [ ]         STREAM     CONNECTED     32736    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     33393
unix  3      [ ]         STREAM     CONNECTED     32486
unix  3      [ ]         STREAM     CONNECTED     31204
unix  3      [ ]         STREAM     CONNECTED     31730
```

2. Check the Wazuh dashboard.


W.
Threat Hunting
Ubuntu
a
agent.id
agent.ip
agent.name
data.alert.action
data.alert.category
data.alert.gid
data.alert.metadata.attack_target
data.alert.metadata.created_at
data.alert.metadata.deployment
data.alert.metadata.performance_impact
data.alert.metadata.reviewed_at
data.alert.metadata.signature_severity
data.alert.metadata.updated_at
data.alert.rev
data.alert.severity
timestamp per 30 minutes
Expanded document
View surrounding documents
View single document
Table
JSON

Time	rule.description	rule.level	rule.id
Jul 29, 2024 @ 16:48:46.837	Audit: Command: /usr/bin/netstat.	3	80792

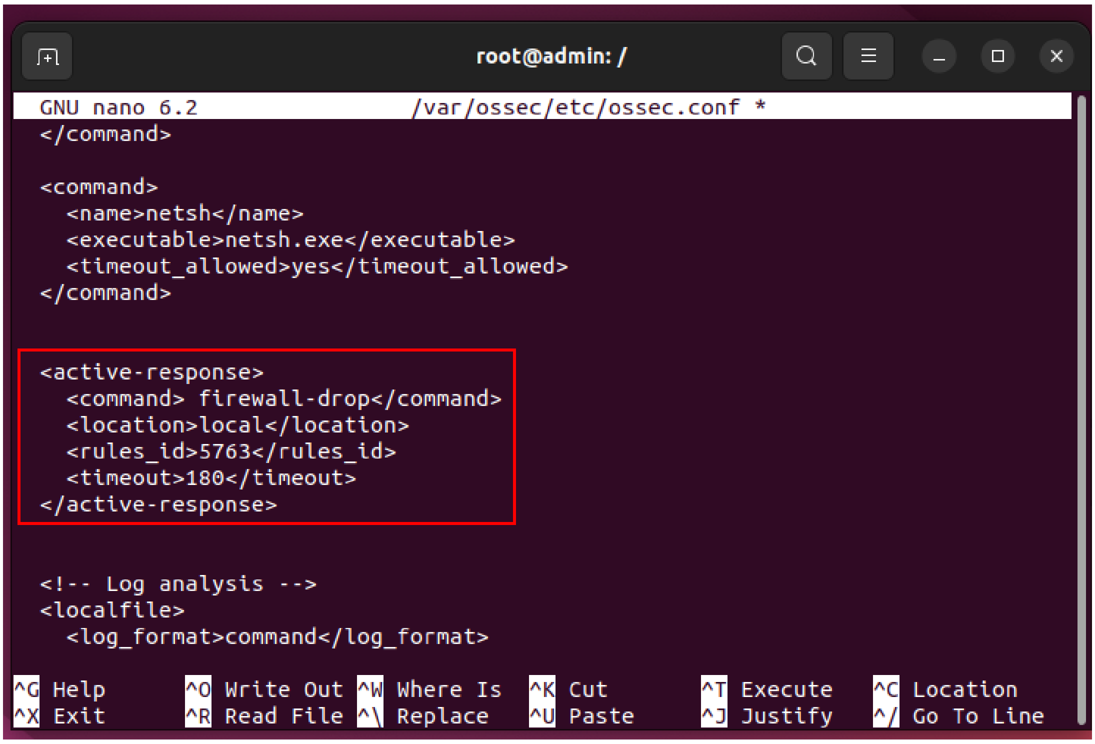
_index	wazuh-alerts-4.x-2024.07.29
agent.id	002
agent.ip	192.168.64.153
agent.name	Ubuntu
data.audit.arch	c000003e
data.audit.auid	1000
data.audit.command	netstat
data.audit.cwd	/root

7. Detection & Block SSH Brute force attacks.

7.1 Enabling Active Response: an inbuilt wazuh feature.

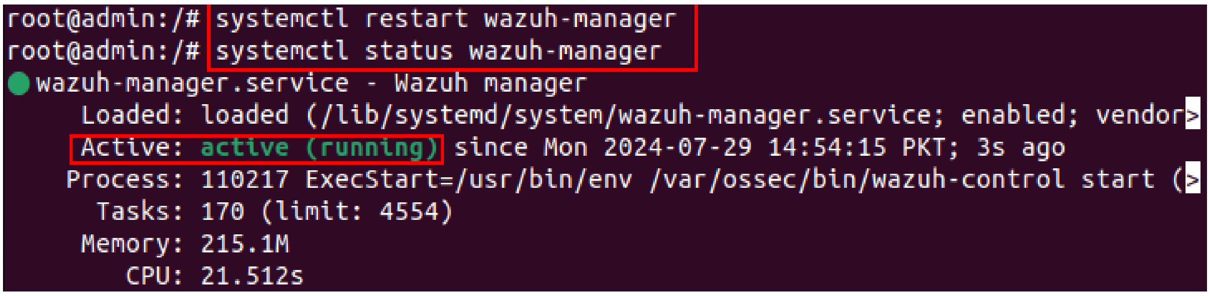
Wazuh has an inbuilt SSH rules to detect the brute force attack. Based on this detection, wazuh uses **active response** to stop these attacks.

1. Update the **ossec.conf** file on wazuh manager such that whenever the 5763 rule is triggered the following active response will be executed.



```
 GNU nano 6.2                /var/ossec/etc/ossec.conf *
 </command>

 <command>
   <name>netsh</name>
   <executable>netsh.exe</executable>
   <timeout_allowed>yes</timeout_allowed>
 </command>


 <active-response>
   <command> firewall-drop</command>
   <location>local</location>
   <rules_id>5763</rules_id>
   <timeout>180</timeout>
 </active-response>


 <!-- Log analysis -->
 <localfile>
   <log_format>command</log_format>

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

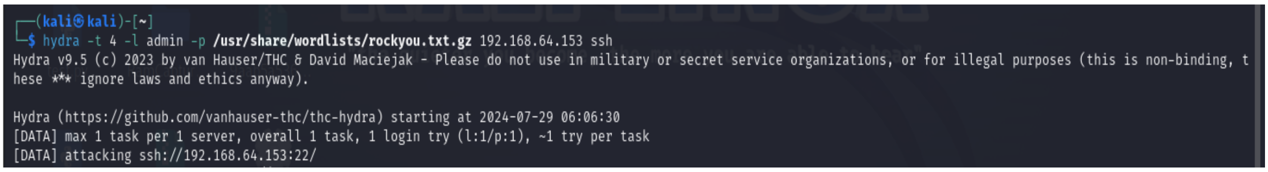
2. Restart the service to save the changes



```
root@admin:/# systemctl restart wazuh-manager
root@admin:/# systemctl status wazuh-manager
● wazuh-manager.service - Wazuh manager
     Loaded: loaded (/lib/systemd/system/wazuh-manager.service; enabled; vendor>
     Active: active (running) since Mon 2024-07-29 14:54:15 PKT; 3s ago
    Process: 110217 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (>
      Tasks: 170 (limit: 4554)
     Memory: 215.1M
        CPU: 21.512s
```

7.2 Launching a Brute Force attack on Wazuh agent

Use the **Hydra** tool in Kali Linux to launch a SSH brute force attack on Wazuh Ubuntu agent.

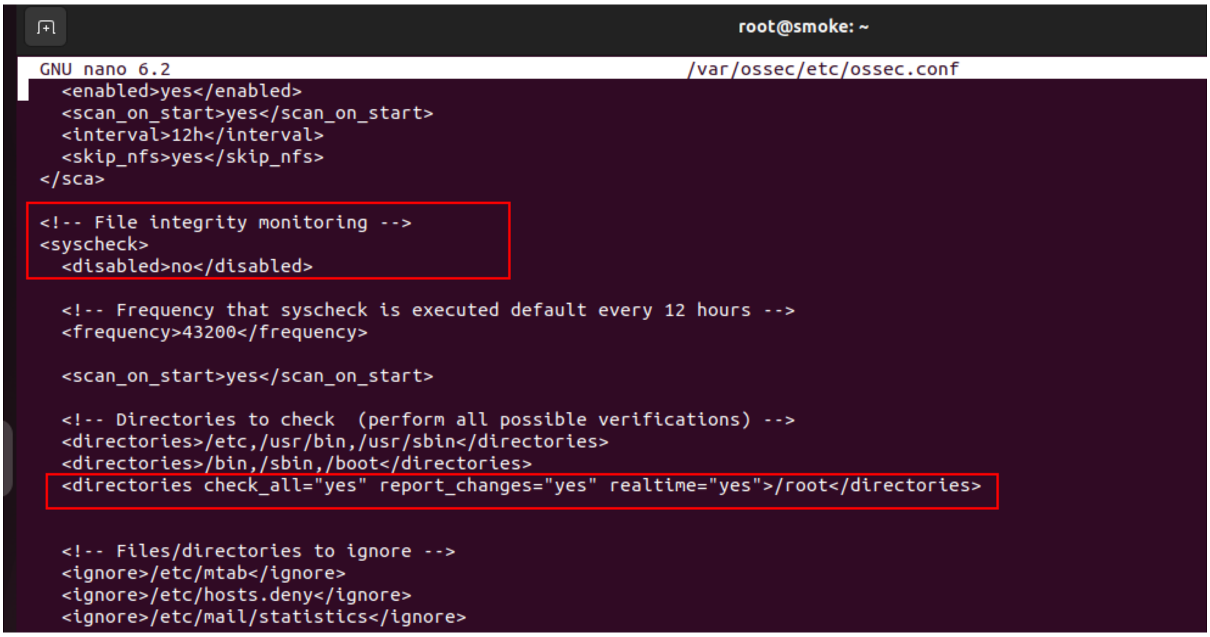


```
┌──(kali㉿kali)-[~]
└─$ hydra -t 4 -l admin -p /usr/share/wordlists/rockyou.txt.gz 192.168.64.153 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, t
hese *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-29 06:06:30
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.64.153:22/
```

8. Detecting Malicious Files using Virus total

8.1 File Integrity Check

1. Add syscheck in the root directory to look at the file changes happening in the root directory.
    a. File integrity check is enabled, and root directory is added.

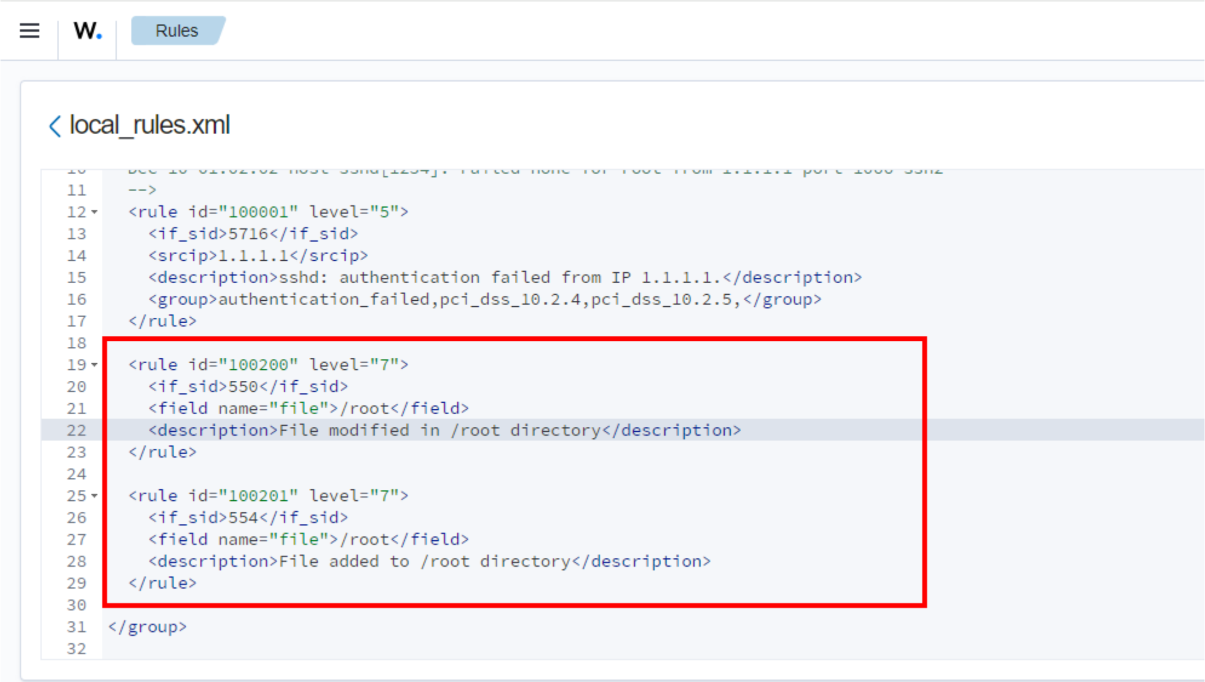


```
root@smoke: ~
 GNU nano 6.2                                         /var/ossec/etc/ossec.conf
    <enabled>yes</enabled>
    <scan_on_start>yes</scan_on_start>
    <interval>12h</interval>
    <skip_nfs>yes</skip_nfs>
  </sca>

  <!-- File integrity monitoring -->
  <syscheck>
    <disabled>no</disabled>

    <!-- Frequency that syscheck is executed default every 12 hours -->
    <frequency>43200</frequency>

    <scan_on_start>yes</scan_on_start>

    <!-- Directories to check  (perform all possible verifications) -->
    <directories>/etc,/usr/bin,/usr/sbin</directories>
    <directories>/bin,/sbin,/boot</directories>
    <directories check_all="yes" report_changes="yes" realtime="yes">/root</directories>

    <!-- Files/directories to ignore -->
    <ignore>/etc/mtab</ignore>
    <ignore>/etc/hosts.deny</ignore>
    <ignore>/etc/mail/statistics</ignore>
```

8.2 Wazuh Rules to detect File changes

Create Wazuh security rule to keep a track of all the changes happening in the root directory only.

i. Navigate to Server management → Rules → Manage Rule files → search for local.
ii. Local_rules.xml is a custom rule file. This is where we can add custom rules. Here
iii. In the local_rules.xml file we add two new rules. Trigger rule 550 & 554

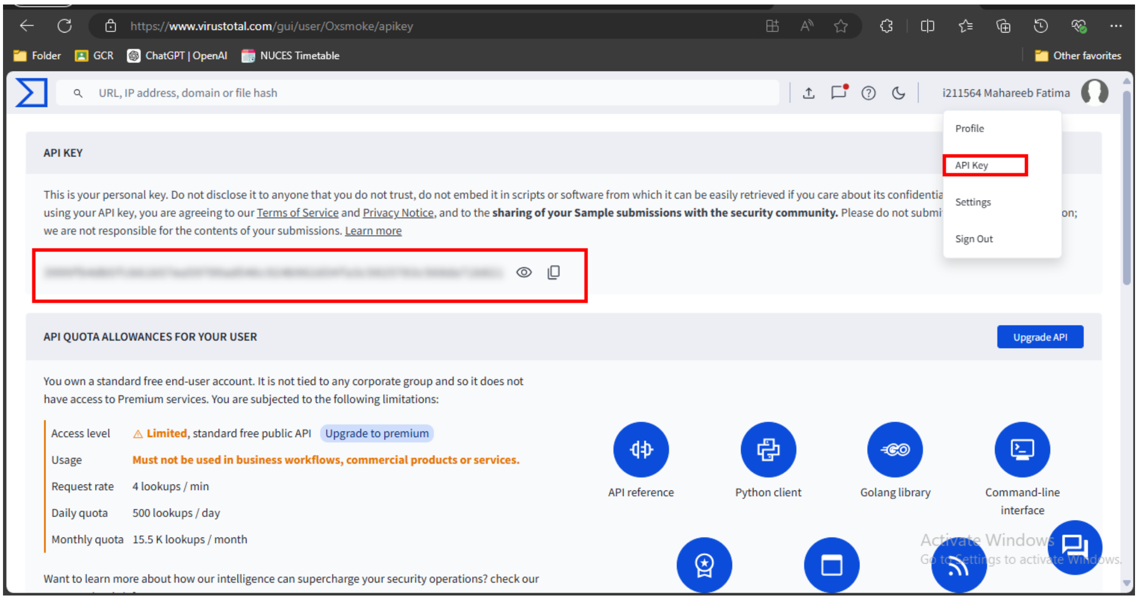


```
  Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066 ssh2
  -->
  <rule id="100001" level="5">
    <if_sid>5716</if_sid>
    <srcip>1.1.1.1</srcip>
    <description>sshd: authentication failed from IP 1.1.1.1.</description>
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
  </rule>

  <rule id="100200" level="7">
    <if_sid>550</if_sid>
    <field name="file">/root</field>
    <description>File modified in /root directory</description>
  </rule>

  <rule id="100201" level="7">
    <if_sid>554</if_sid>
    <field name="file">/root</field>
    <description>File added to /root directory</description>
  </rule>

</group>

```

8.3 Virus total

Trigger an integration tag for virus total, which is there is ossec.conf file of Wazuh manager.

1. Copy the API key from virus total account.



https://www.virustotal.com/gui/user/Oxsmoke/apikey

API KEY

This is your personal key. Do not disclose it to anyone that you do not trust, do not embed it in scripts or software from which it can be easily retrieved if you care about its confidentia using your API key, you are agreeing to our Terms of Service and Privacy Notice, and to the **sharing of your Sample submissions with the security community.** Please do not submi on; we are not responsible for the contents of your submissions. Learn more

[redacted]

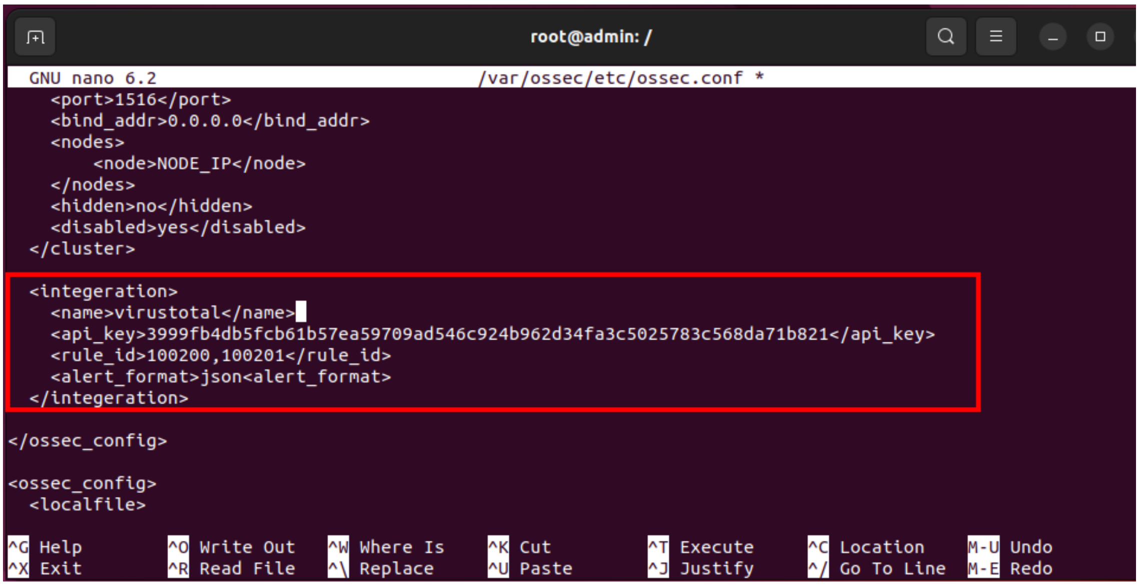
API QUOTA ALLOWANCES FOR YOUR USER

You own a standard free end-user account. It is not tied to any corporate group and so it does not have access to Premium services. You are subjected to the following limitations:

Access level	⚠ **Limited**, standard free public API Upgrade to premium
Usage	**Must not be used in business workflows, commercial products or services.**
Request rate	4 lookups / min
Daily quota	500 lookups / day
Monthly quota	15.5 K lookups / month

Want to learn more about how our intelligence can supercharge your security operations? check our

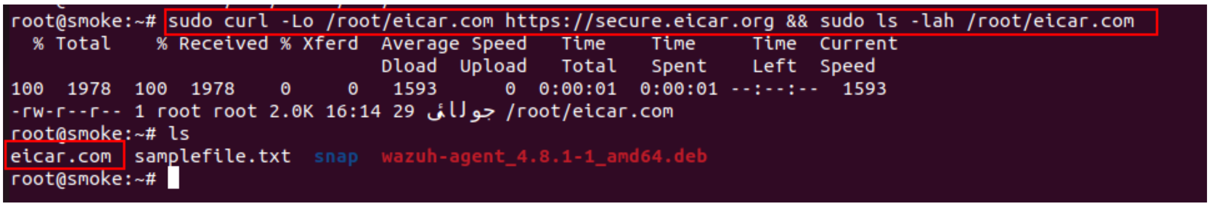
2. Integrate the Virus total API with the ossec.conf file in wazuh manger.



```
  GNU nano 6.2                        /var/ossec/etc/ossec.conf *
    <port>1516</port>
    <bind_addr>0.0.0.0</bind_addr>
    <nodes>
        <node>NODE_IP</node>
    </nodes>
    <hidden>no</hidden>
    <disabled>yes</disabled>
  </cluster>

  <integeration>
    <name>virustotal</name>
    <api_key>3999fb4db5fcb61b57ea59709ad546c924b962d34fa3c5025783c568da71b821</api_key>
    <rule_id>100200,100201</rule_id>
    <alert_format>json<alert_format>
  </integeration>

</ossec_config>

<ossec_config>
  <localfile>

^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo
```

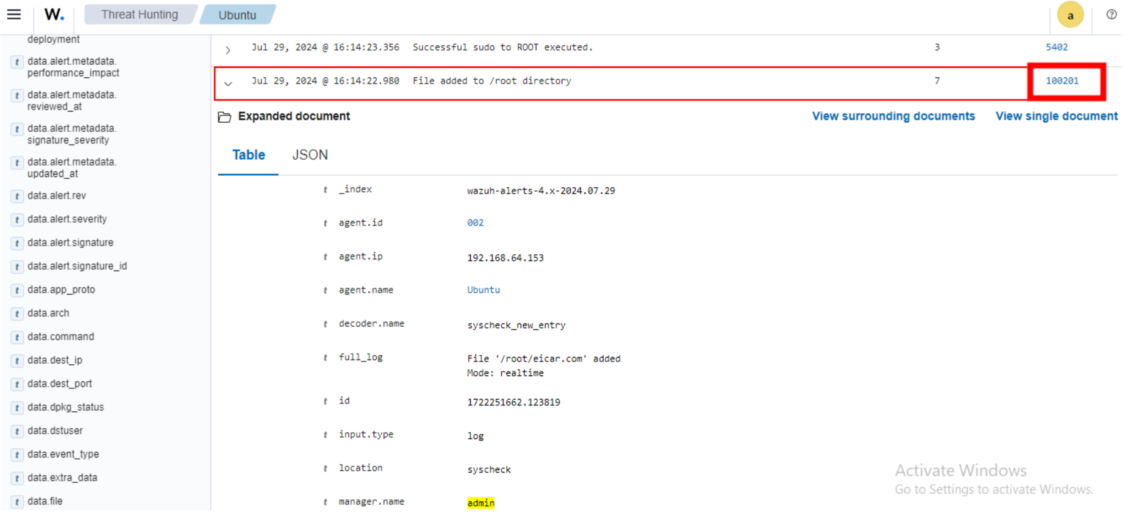
8.4 Testing using a sample malicious file: eicar malicious file

1. Security alert generated on Wazuh dashboard.
2. Download the test malware file using eicar on Wazuh agent & verify the eicar malicious file downloaded using **ls** command.



```
root@smoke:~# sudo curl -Lo /root/eicar.com https://secure.eicar.org && sudo ls -lah /root/eicar.com
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1978  100  1978    0     0   1593      0  0:00:01  0:00:01 --:--:--  1593
-rw-r--r-- 1 root root 2.0K 16:14 29 جولائی /root/eicar.com
root@smoke:~# ls
eicar.com  samplefile.txt  snap  wazuh-agent_4.8.1-1_amd64.deb
root@smoke:~# 
```

Wazuh Rule Detected



```
Jul 29, 2024 @ 16:14:23.356   Successful sudo to ROOT executed.    3    5402
Jul 29, 2024 @ 16:14:22.980   File added to /root directory        7    100201
```

```
_index          wazuh-alerts-4.x-2024.07.29
agent.id        002
agent.ip        192.168.64.153
agent.name      Ubuntu
decoder.name    syscheck_new_entry
full_log        File '/root/eicar.com' added
                Mode: realtime
id              1722251662.123819
input.type      log
location        syscheck
manager.name    admin
```

Conclusion

In conclusion, the deployment and configuration of Wazuh across Ubuntu and Windows systems decisively demonstrated its critical role in a robust security infrastructure. From file integrity monitoring to network intrusion detection with Suricata, and proactive threat responses like blocking SSH brute force attacks, Wazuh proved its capability to handle a wide range of security challenges. The integration with tools such as VirusTotal for detecting malicious files further solidifies Wazuh's position as an indispensable asset for any organization committed to a proactive and resilient cybersecurity posture.

References

- https://documentation.wazuh.com/4.8/user-manual/reference/ossec-conf/client.html#enrollment-agent-name
- https://github.com/0xrajneesh/Suricata-IDS-Home-Lab/blob/main/installing-suricata.md
- https://www.youtube.com/watch?v=vJZAVZOIpfA&list=PLBf0hzazHTGNcIS_dHjM2NgNUFMW1EZFx&index=24