WAZUH

The Wazuh Security Information and Event Management (SIEM) solution provides monitoring, detection, and alerting of security events and incidents.

It is a free and open source software used for log analysis, File integrity monitoring, vulnerability assessment etc.

It consists of 3 central components:

- Wazuh indexer
- Wazuh server
- Wazuh Dashboard

Wazuh indexer: It is used to index and store alerts generated by Wazuh server and provides real time data search and analytics.

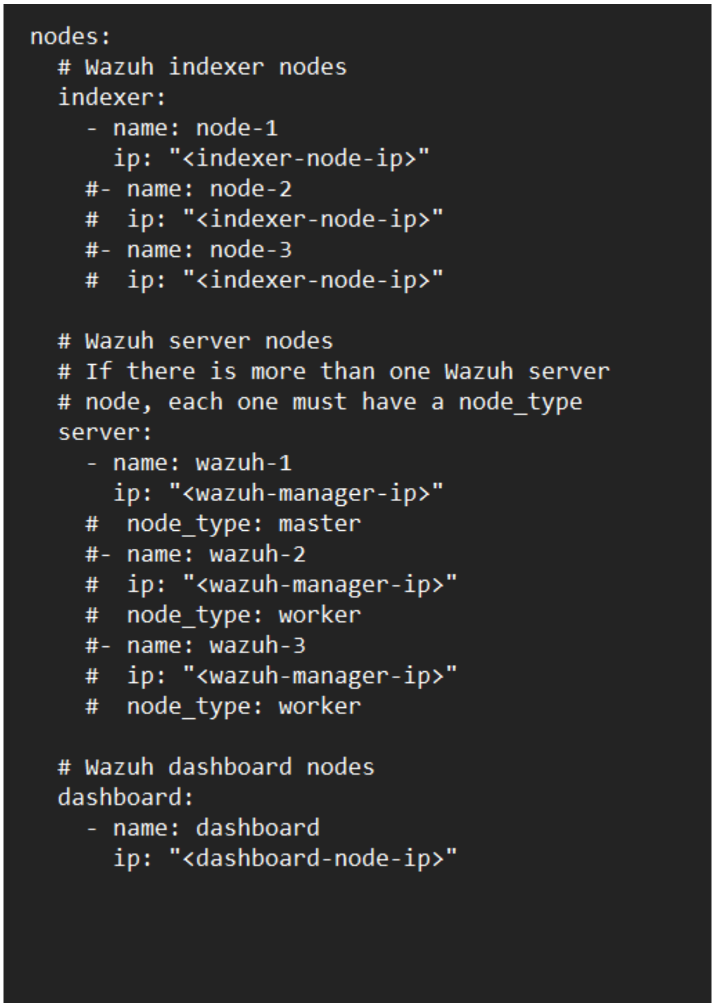
Wazuh Server: It analyzes the data received from agents, triggers alerts when threats/anomalies are detected.

Wazuh Dashboard: It is a web interface to analyze and visualize Security data, vulnerabilities and check regulatory compliance.

Installation guide:

To install Wazuh all central components, we can go to wazuh installation documentation to see each and every tool we are downloading to run this software.

In short, we use curl to download the files from there website And firstly we configure the config.yml file where we give our server, dashboard and indexer ip. Then we generate its config files.



```
nodes:
  # Wazuh indexer nodes
  indexer:
    - name: node-1
      ip: "<indexer-node-ip>"
    #- name: node-2
    #  ip: "<indexer-node-ip>"
    #- name: node-3
    #  ip: "<indexer-node-ip>"

  # Wazuh server nodes
  # If there is more than one Wazuh server
  # node, each one must have a node_type
  server:
    - name: wazuh-1
      ip: "<wazuh-manager-ip>"
    #  node_type: master
    #- name: wazuh-2
    #  ip: "<wazuh-manager-ip>"
    #  node_type: worker
    #- name: wazuh-3
    #  ip: "<wazuh-manager-ip>"
    #  node_type: worker

  # Wazuh dashboard nodes
  dashboard:
    - name: dashboard
      ip: "<dashboard-node-ip>"
```

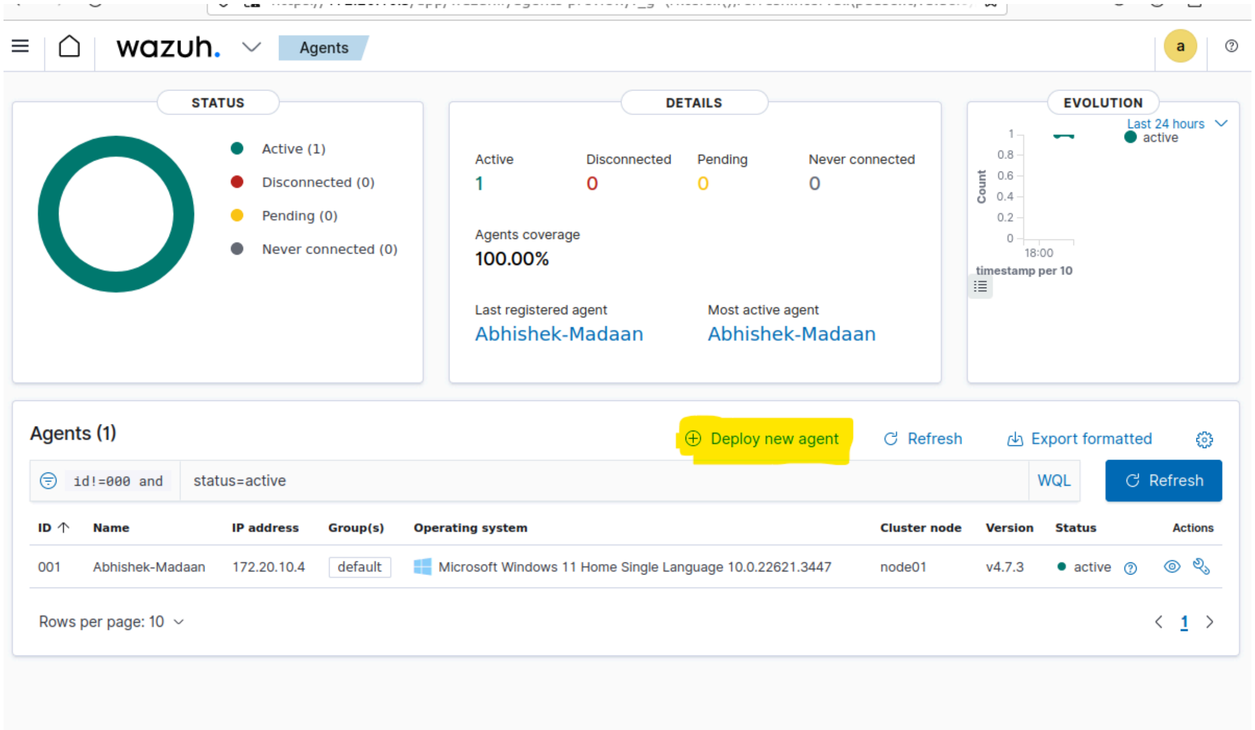
Fig: showing config.yml file

For Wazuh indexer:
We download wazuh-install.sh from the web server and run that file with “--wazuh-indexer node-1” to download the indexer and then we start the cluster to get the login username and password.

For Wazuh Server:
 We download wazuh-install,sh from the web server and run it with “--wazuh-server wazuh-1” to download the server.

For Wazuh Dashboard:
We download wazuh-install.sh from the web server and run it with “--wazuh-dashboard dashboard” to download the server.

To use wazuh we need to add agents first.



Active 1
Disconnected 0
Pending 0
Never connected 0

Agents coverage
100.00%

Last registered agent
Abhishek-Madaan

Most active agent
Abhishek-Madaan

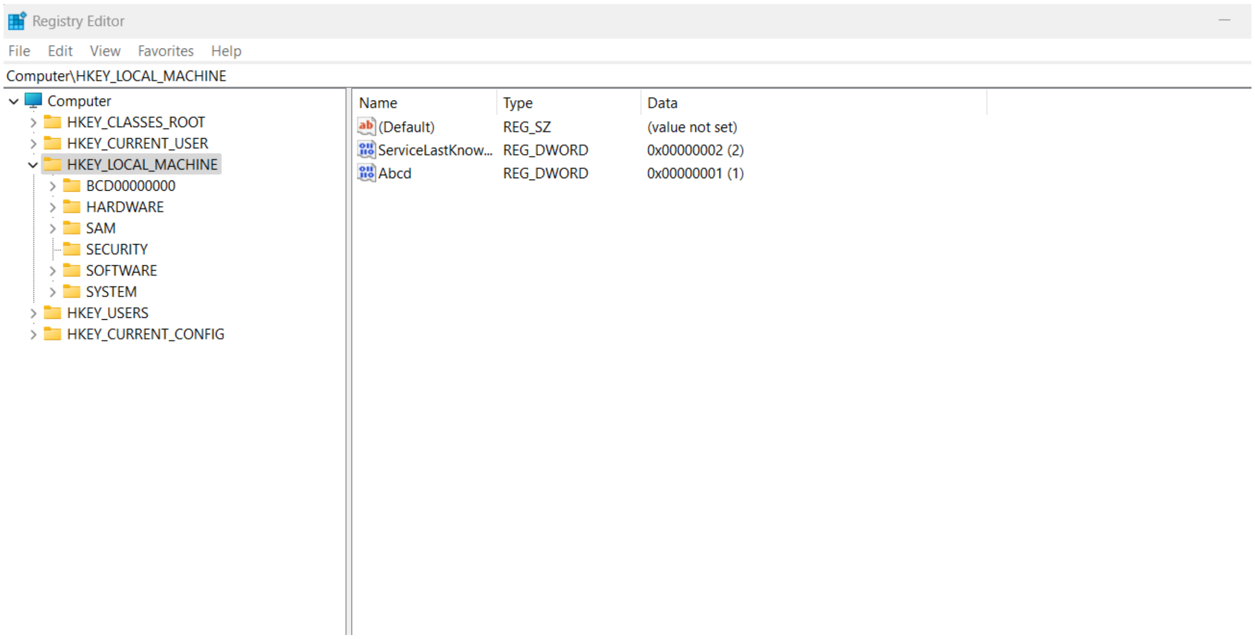
Agents (1)

id!=000 and status=active

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	Abhishek-Madaan	172.20.10.4	default	Microsoft Windows 11 Home Single Language 10.0.22621.3447	node01	v4.7.3	● active	

To add the agents we need to select their OS, and then enter your server Ip address and it will give a code which we can run on terminal (for linux) or powershell (for windows).

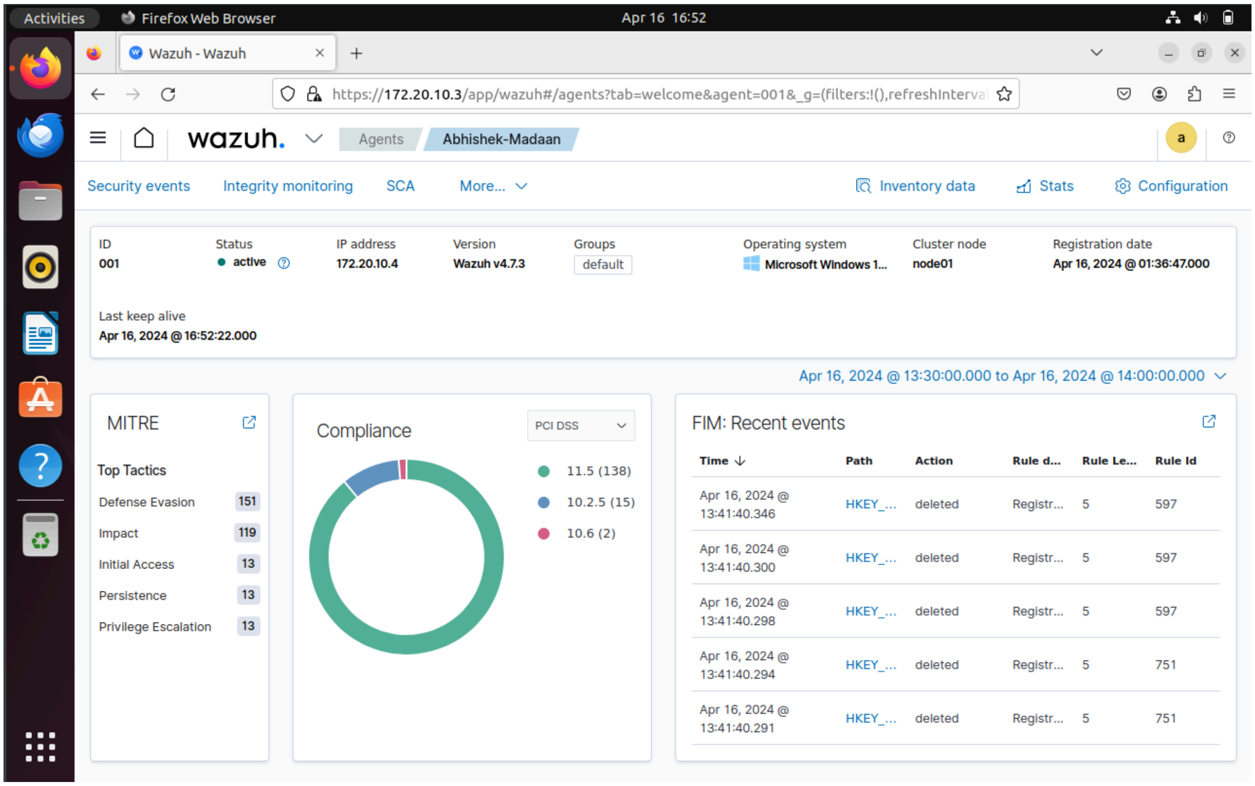
After adding the agents we can check if wazuh is working properly or not



Computer\HKEY_LOCAL_MACHINE

Name	Type	Data
(Default)	REG_SZ	(value not set)
ServiceLastKnow...	REG_DWORD	0x00000002 (2)
Abcd	REG_DWORD	0x00000001 (1)

We changed our registry editor and now in next agent scan, we check whether it is scanning file properly



ID	Status	IP address	Version	Groups	Operating system	Cluster node	Registration date
001	● active	172.20.10.4	Wazuh v4.7.3	default	Microsoft Windows 1...	node01	Apr 16, 2024 @ 01:36:47.000

Last keep alive
Apr 16, 2024 @ 16:52:22.000

Apr 16, 2024 @ 13:30:00.000 to Apr 16, 2024 @ 14:00:00.000

MITRE

Top Tactics

Defense Evasion	151
Impact	119
Initial Access	13
Persistence	13
Privilege Escalation	13

Compliance

PCI DSS

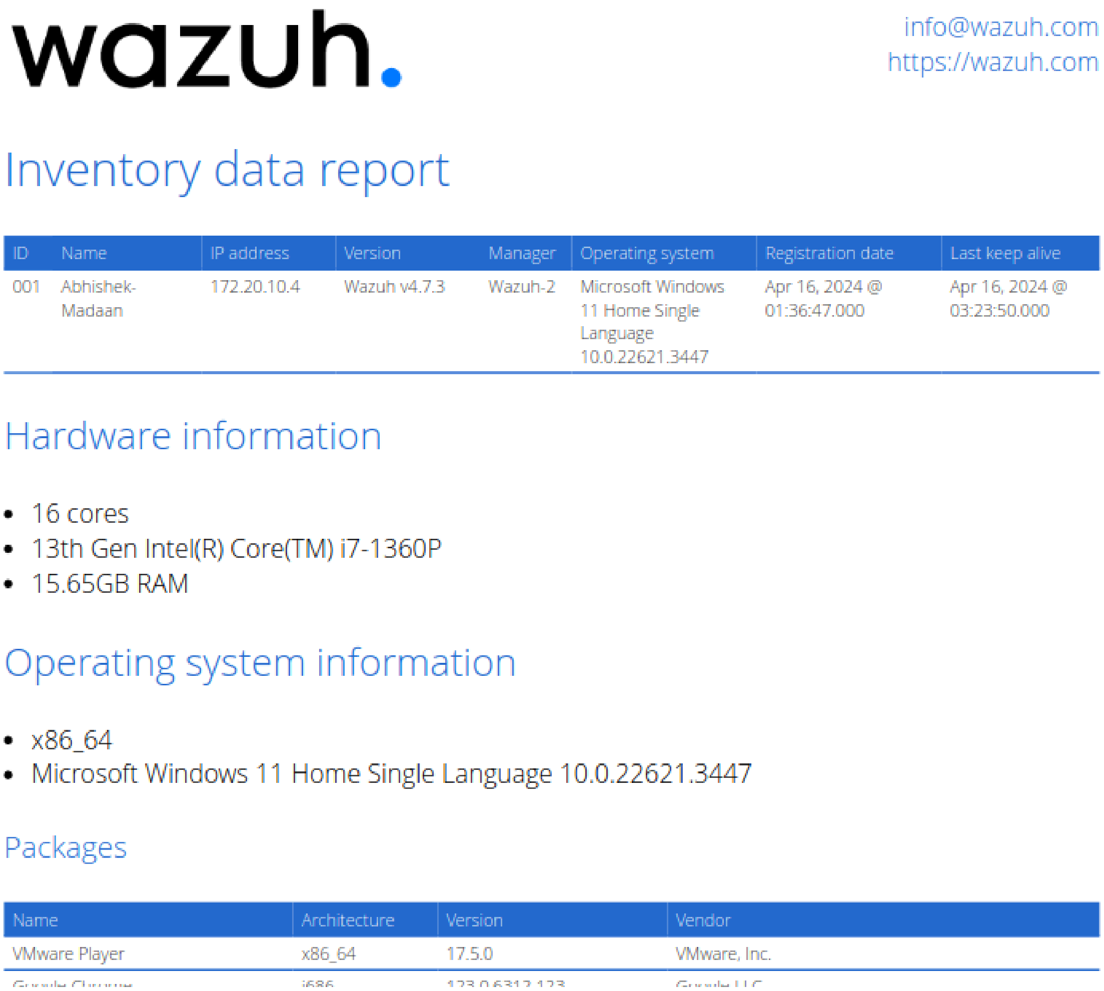
- ● 11.5 (138)
- ● 10.2.5 (15)
- ● 10.6 (2)

FIM: Recent events

Time ↓	Path	Action	Rule d...	Rule Le...	Rule Id
Apr 16, 2024 @ 13:41:40.346	HKEY_...	deleted	Registr...	5	597
Apr 16, 2024 @ 13:41:40.300	HKEY_...	deleted	Registr...	5	597
Apr 16, 2024 @ 13:41:40.298	HKEY_...	deleted	Registr...	5	597
Apr 16, 2024 @ 13:41:40.294	HKEY_...	deleted	Registr...	5	751
Apr 16, 2024 @ 13:41:40.291	HKEY_...	deleted	Registr...	5	751

As we can see it show the changes in FIM(File Integrity Monitoring).

We can also generate report of any agent.



wazuh.

info@wazuh.com
https://wazuh.com

Inventory data report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	Abhishek-Madaan	172.20.10.4	Wazuh v4.7.3	Wazuh-2	Microsoft Windows 11 Home Single Language 10.0.22621.3447	Apr 16, 2024 @ 01:36:47.000	Apr 16, 2024 @ 03:23:50.000

Hardware information

- 16 cores
- 13th Gen Intel(R) Core(TM) i7-1360P
- 15.65GB RAM

Operating system information

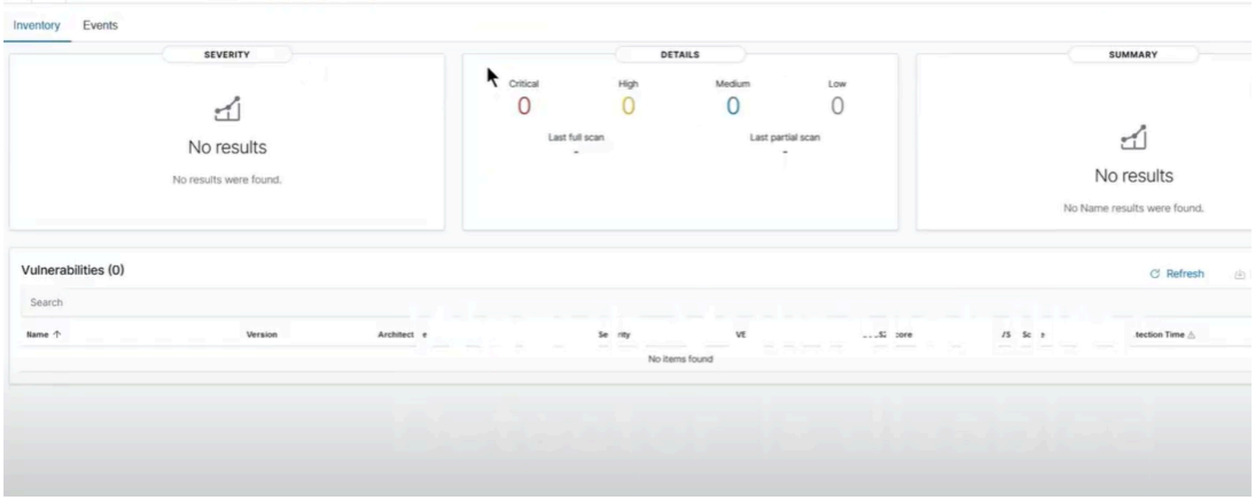
- x86_64
- Microsoft Windows 11 Home Single Language 10.0.22621.3447

Packages

Name	Architecture	Version	Vendor
VMware Player	x86_64	17.5.0	VMware, Inc.
Google Chrome	i686	123.0.6312.123	Google LLC

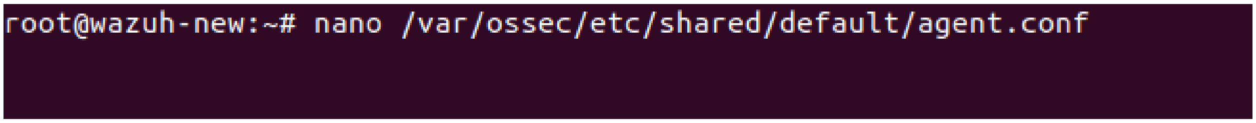
It is a big report with all of the agent data combined visualized in the report.

We can also add a Vulnerability scanner to the Wazuh, it is already installed but not configured by default. We need to configure it and enable it to use it.



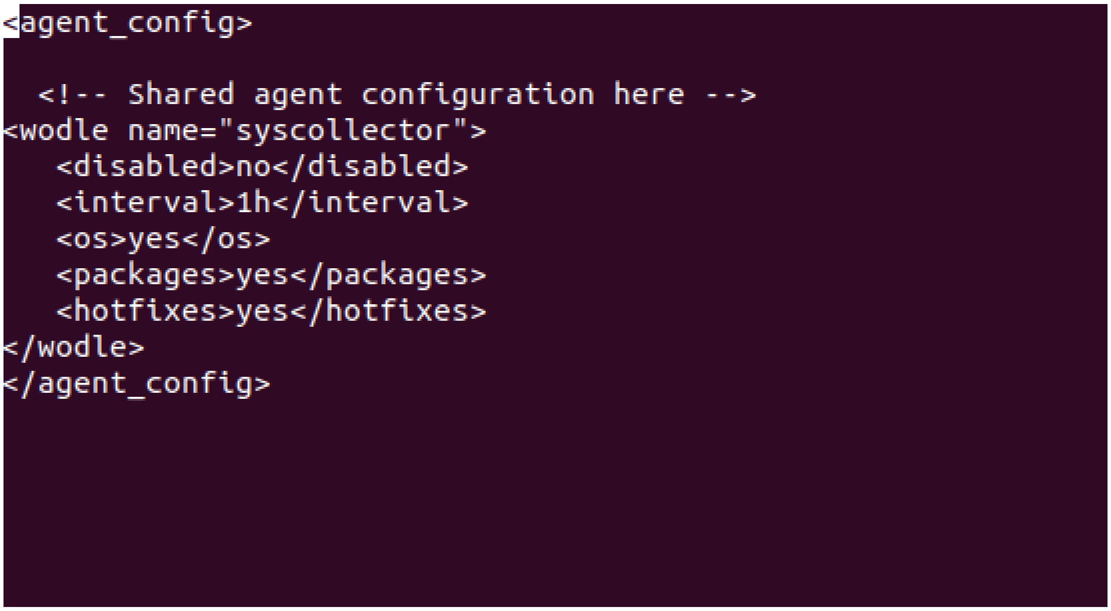
As you can see by default it is not scanning our agents for vulnerabilities.

Open the following file:



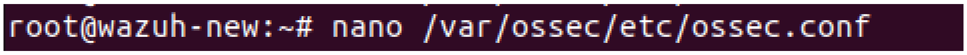
```
root@wazuh-new:~# nano /var/ossec/etc/shared/default/agent.conf
```

Add the configuration here:



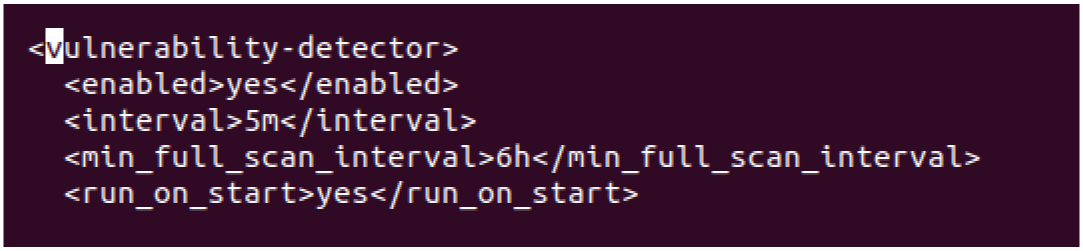
```
<agent_config>

  <!-- Shared agent configuration here -->
<wodle name="syscollector">
   <disabled>no</disabled>
   <interval>1h</interval>
   <os>yes</os>
   <packages>yes</packages>
   <hotfixes>yes</hotfixes>
</wodle>
</agent_config>
```

Save it and then, open this file:



```
root@wazuh-new:~# nano /var/ossec/etc/ossec.conf
```

And search for vulnerability detector

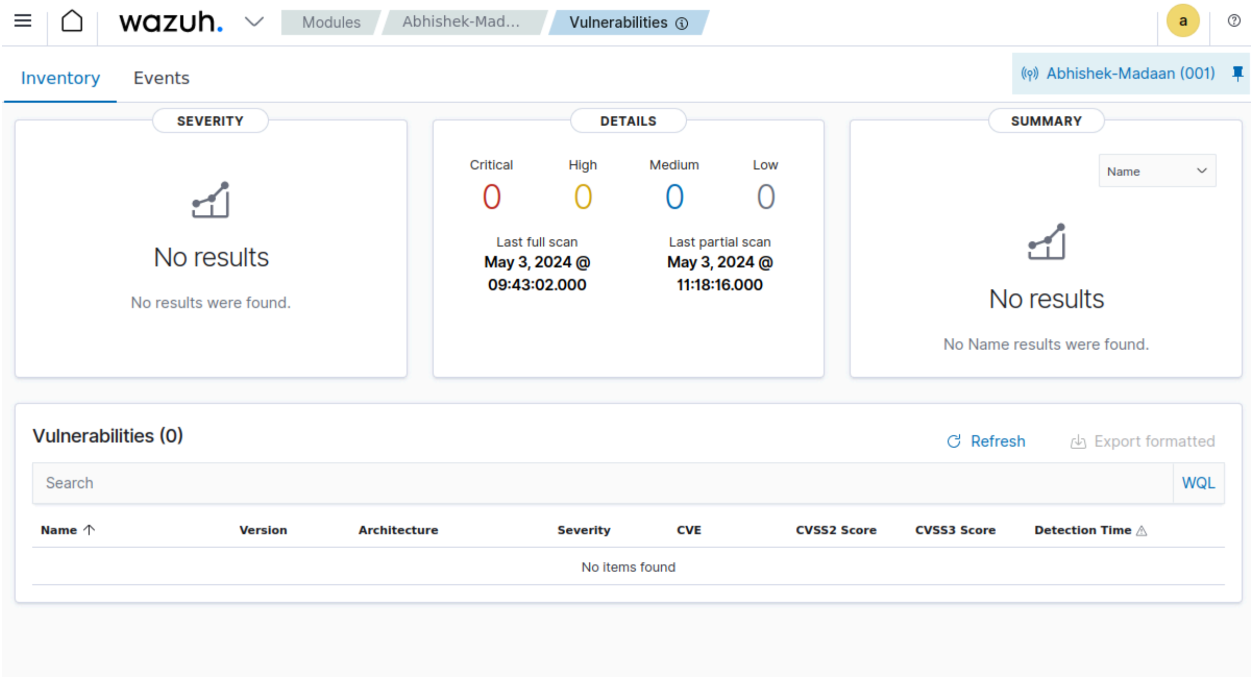


```
  <vulnerability-detector>
    <enabled>yes</enabled>
    <interval>5m</interval>
    <min_full_scan_interval>6h</min_full_scan_interval>
    <run_on_start>yes</run_on_start>
```

And change the “no” to “yes”.

And then restart the wazuh-manager service by following command:

Systemctl restart wazuh-manager.service .



SEVERITY

No results

No results were found.

DETAILS

Critical	High	Medium	Low
0	0	0	0

Last full scan
May 3, 2024 @ 09:43:02.000

Last partial scan
May 3, 2024 @ 11:18:16.000

SUMMARY

Name

No results

No Name results were found.

Vulnerabilities (0)

Name ↑	Version	Architecture	Severity	CVE	CVSS2 Score	CVSS3 Score	Detection Time ⚠
No items found							

As you can see now it is scanning my agent for any vulnerability and if there be any, it will show down in the list.