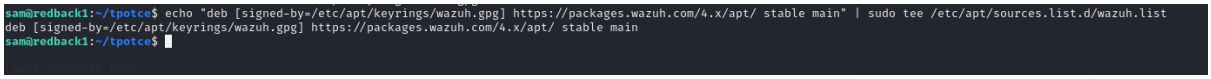
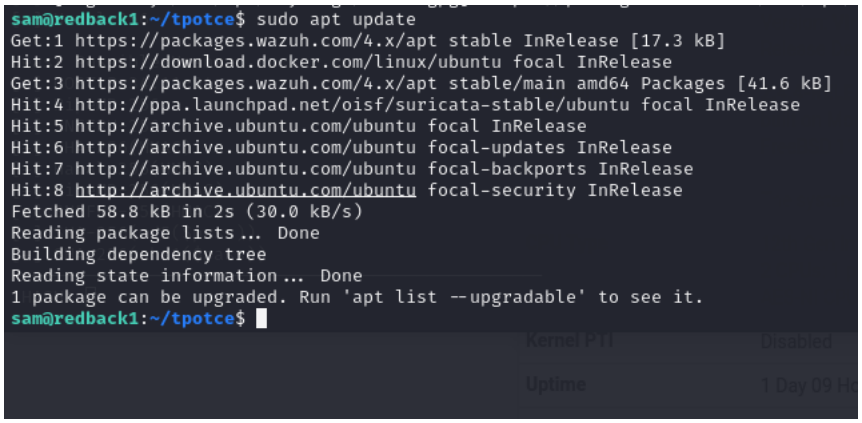
Wazuh Configurtion

First add the Wazuh repository to your system.



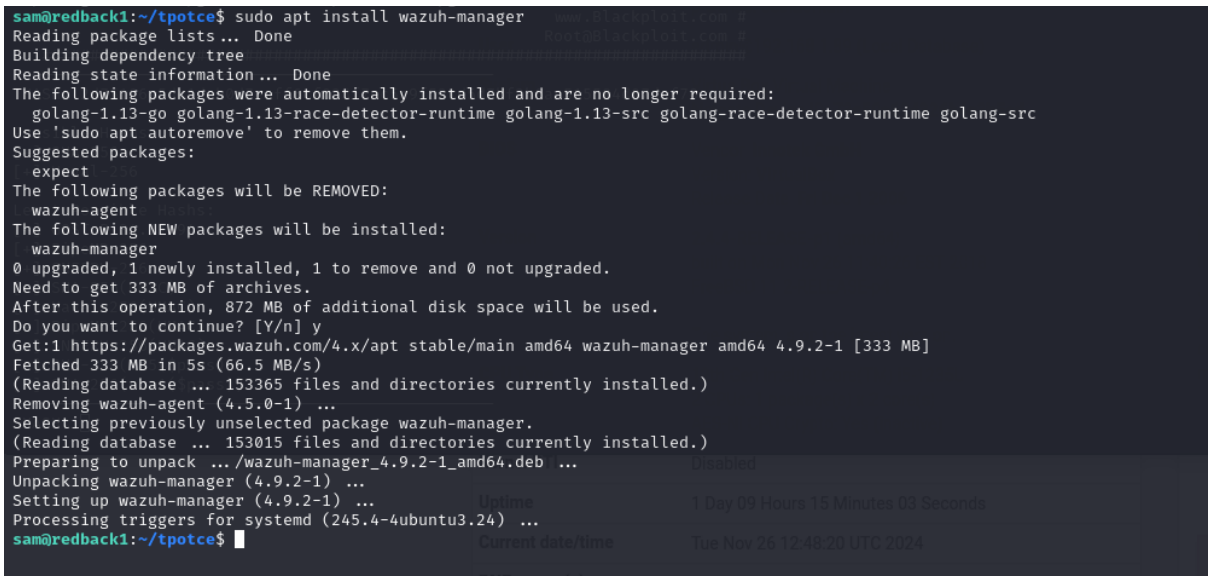
Added repository

Now update the package list by “sudo apt update”.



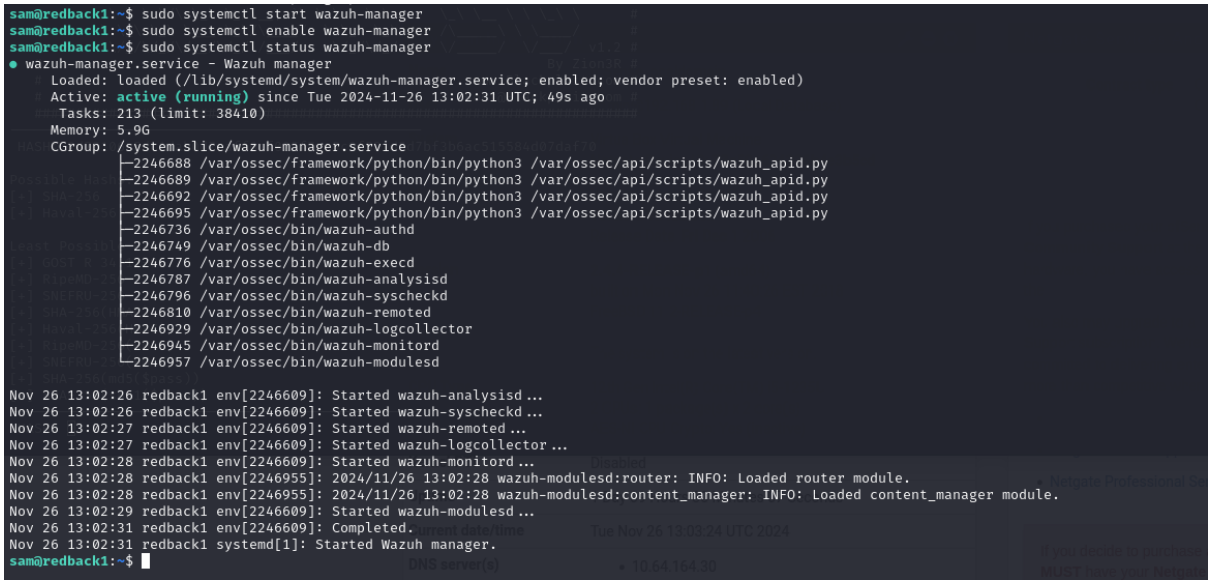
Package updated

Next we can install the Wazuh manager.



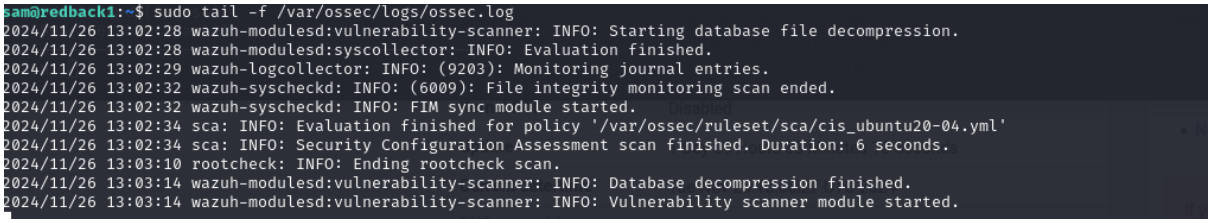
Wazuh manager installed

We can now start and enable wazuh manager by “sudo systemctl start wazuh-manager” and “sudo systemctl enable wazuh-manager”. And then we csn check the status.

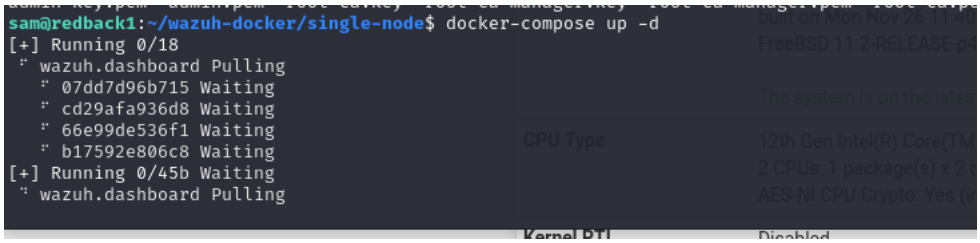


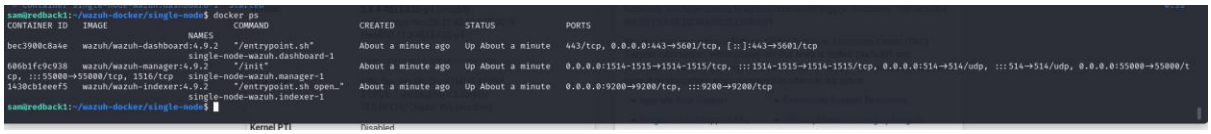
Wazuh Manager Running

We can verify the full functionality of Wazuh by checking its logs or performing some test actions by “sudo tail -f /var/ossec/logs/ossec.log”.



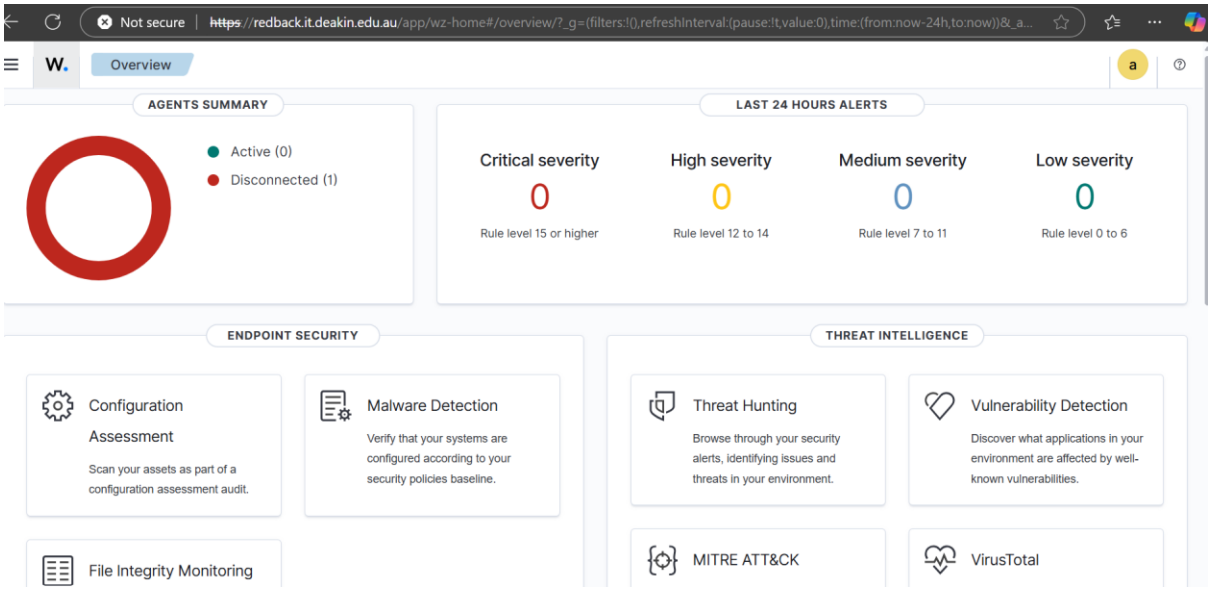
Wazuh running





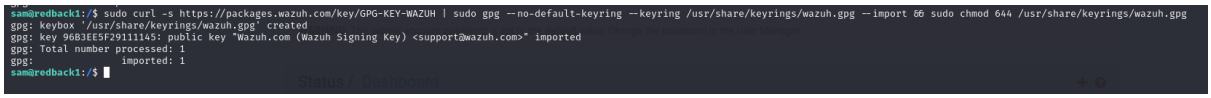
Dockers up

Now log in to Wazuh. UserName-‘kibanaserver’ and Password-“kibanaserver”.



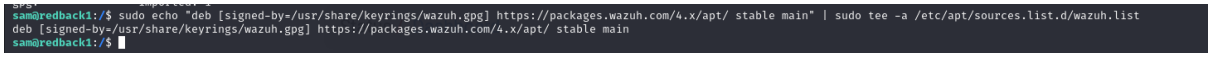
Wazuh DashBoard

Now we can download Wazuh Agent on Endpoint. To add the Wazuh repository we use “sudo curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo gpg --no-default-keyring --keyring /usr/share/keyrings/wazuh.gpg --import && sudo chmod 644 /usr/share/keyrings/wazuh.gpg”.



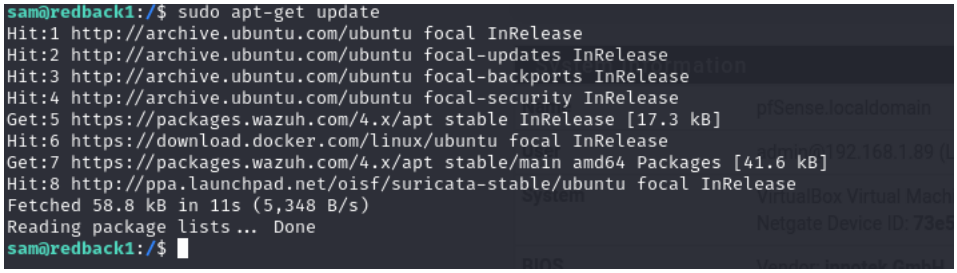
Installed GPG Key

Now we need to add the repository by “sudo echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | sudo tee -a /etc/apt/sources.list.d/wazuh.list”.



Added Repository

Now we can update package Information.



Updated Package Information

Now we can install Wazuh Agent by “WAZUH_MANAGER="10.137.0.149" apt-get install wazuh-agent”.

```
sam@redback1:/$ sudo WAZUH_MANAGER="10.137.0.149" apt-get install wazuh-agent
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
The following package was automatically installed and is no longer required:
  wmdocker
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  wazuh-agent
0 upgraded, 1 newly installed, 0 to remove and 14 not upgraded.
Need to get 10.8 MB of archives.
After this operation, 37.3 MB of additional disk space will be used.
Get:1 https://packages.wazuh.com/4.x/apt stable/main amd64 wazuh-agent amd64 4.9.2-1 [10.8 MB]
Fetched 10.8 MB in 10s (1,043 kB/s)
Preconfiguring packages ...
Selecting previously unselected package wazuh-agent.
(Reading database ... 143405 files and directories currently installed.)
Preparing to unpack .../wazuh-agent_4.9.2-1_amd64.deb ...
Unpacking wazuh-agent (4.9.2-1) ...
Setting up wazuh-agent (4.9.2-1) ...
Processing triggers for systemd (245.4-4ubuntu3.24) ...
sam@redback1:/$
```

Wazuh-Agent Installed

Now Enable and Start the Wazuh Agent Service.

```
File  Actions  Edit  View  Help
sam@redback1:/$ sudo systemctl daemon-reload
sam@redback1:/$ sudo systemctl enable wazuh-agent
sam@redback1:/$ sudo systemctl start wazuh-agent
sam@redback1:/$
```

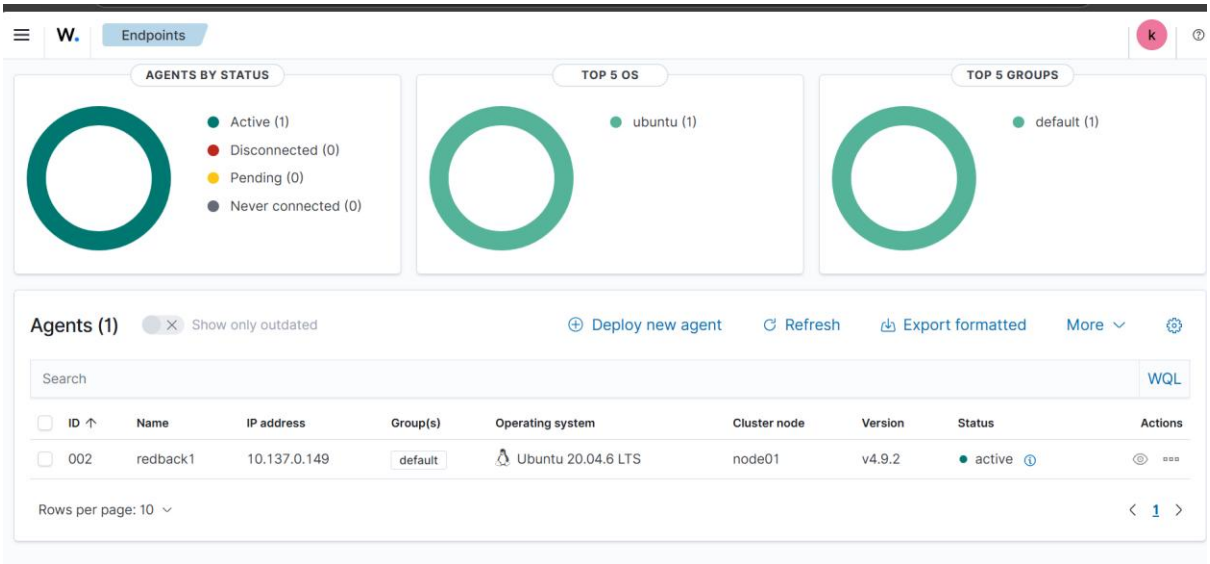
Enabled Wazuh-Agent

Now we can Verify Wazuh Agent Status

```
sam@redback1:/$ 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 Sat 2024-12-14 03:46:40 UTC; 3min 3s ago
    Process: 1758574 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
      Tasks: 38 (limit: 38410)
     Memory: 825.1M
     CGroup: /system.slice/wazuh-agent.service
             ├─1759052 /var/ossec/bin/wazuh-execd
             ├─1759060 /var/ossec/bin/wazuh-agentd
             ├─1759077 /var/ossec/bin/wazuh-syscheckd
             ├─1759087 /var/ossec/bin/wazuh-logcollector
             └─1759102 /var/ossec/bin/wazuh-modulesd

Dec 14 03:46:36 redback1 systemd[1]: Starting Wazuh agent ...
Dec 14 03:46:36 redback1 env[1758574]: Starting Wazuh v4.9.2 ...
Dec 14 03:46:36 redback1 env[1758574]: Started wazuh-execd ...
Dec 14 03:46:37 redback1 env[1758574]: Started wazuh-agentd ...
Dec 14 03:46:37 redback1 env[1758574]: Started wazuh-syscheckd ...
Dec 14 03:46:37 redback1 env[1758574]: Started wazuh-logcollector ...
Dec 14 03:46:38 redback1 env[1758574]: Started wazuh-modulesd ...
Dec 14 03:46:40 redback1 env[1758574]: Completed.
Dec 14 03:46:40 redback1 systemd[1]: Started Wazuh agent.
sam@redback1:/$
```

Wazuh Agent running



Wazuh agent connected

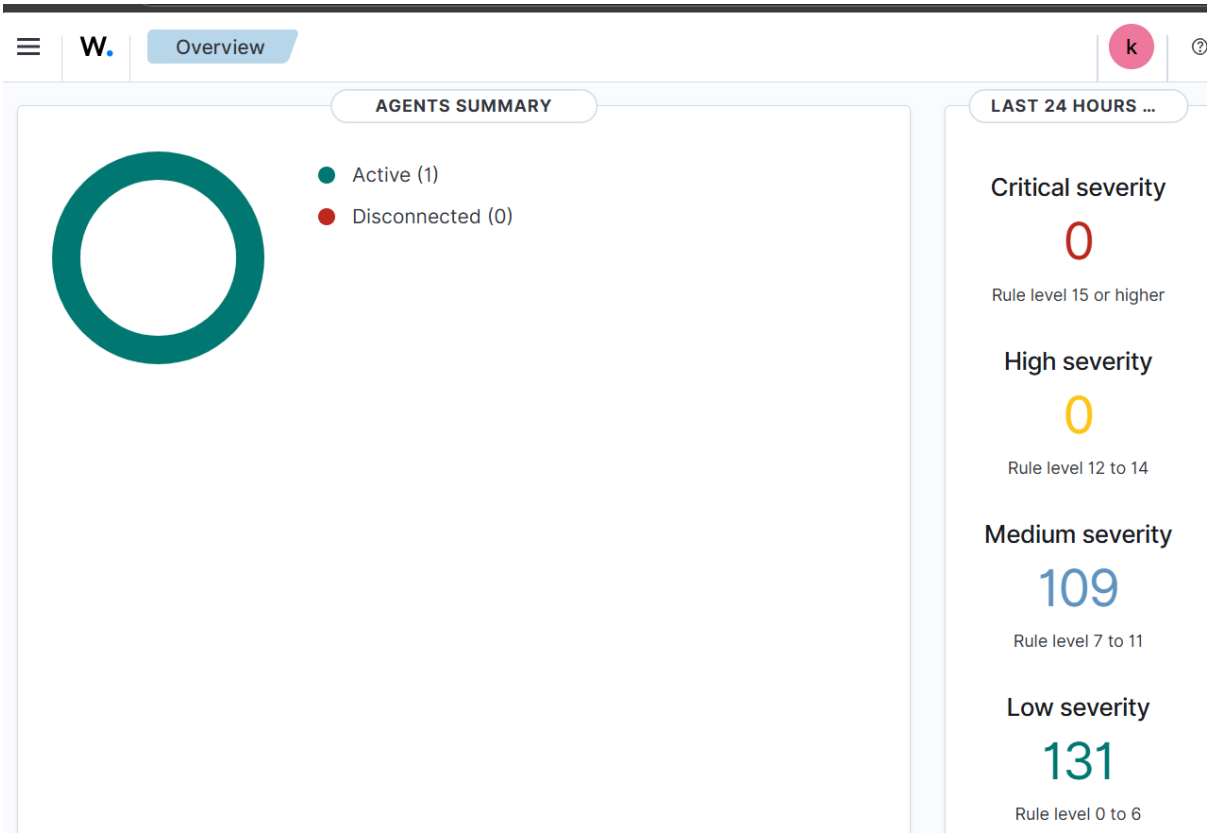
To prevent the agent from being accidentally upgraded and becoming incompatible with the Wazuh manager we can disable Wazuh updates.

```
sam@redback1:/$ sudo sed -i "s/^deb/#deb/" /etc/apt/sources.list.d/wazuh.list
```

Auto update disabled

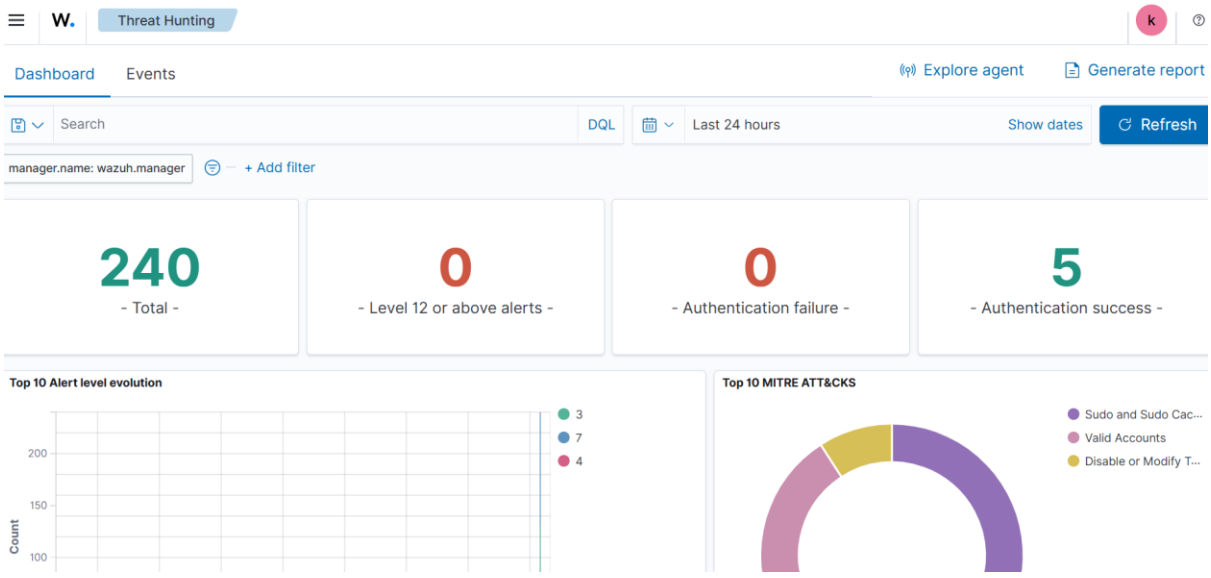
We can update the package again.

Now that the agent is running, verify that it is successfully registered with the Wazuh manager. We can check the agent's connection to the manager by reviewing the agent's log file.

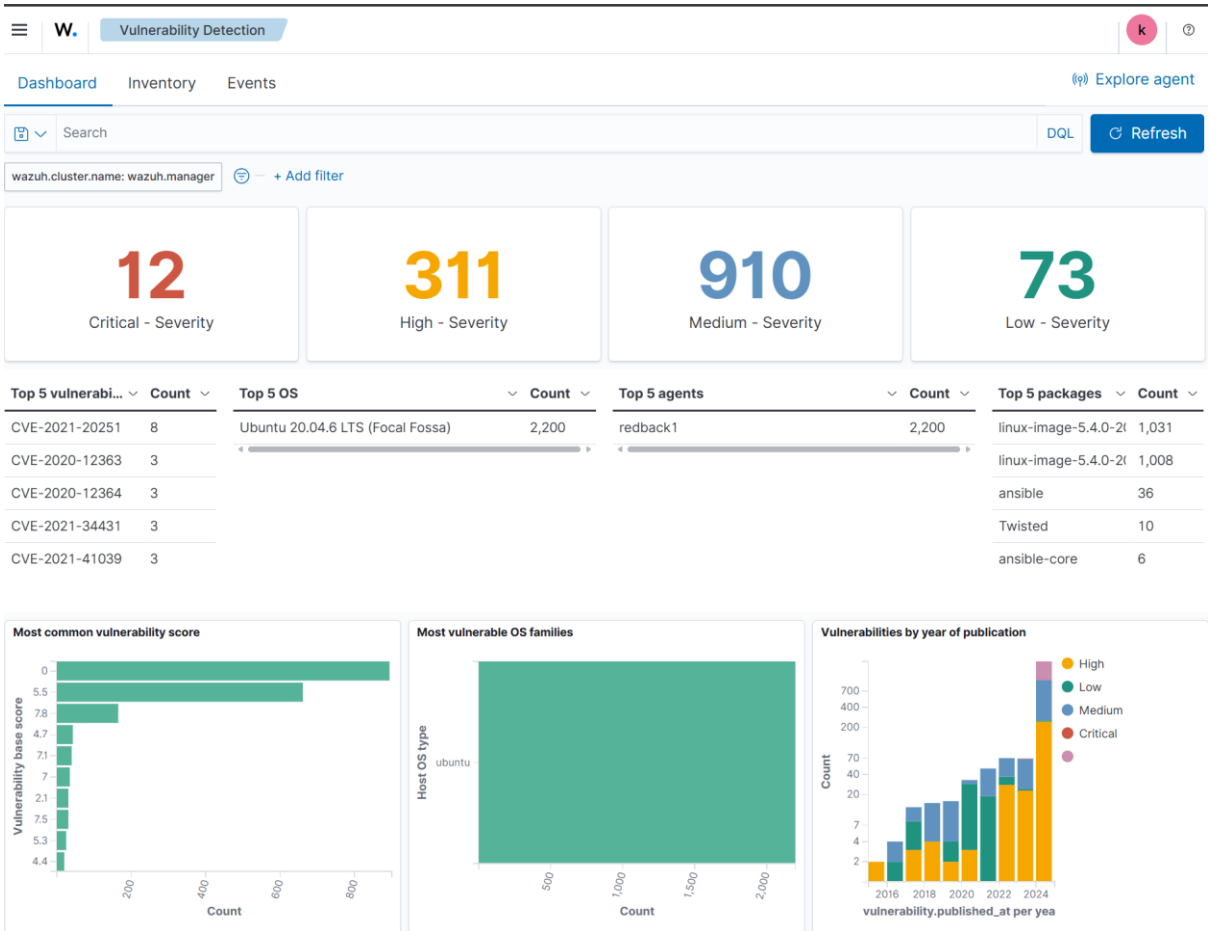


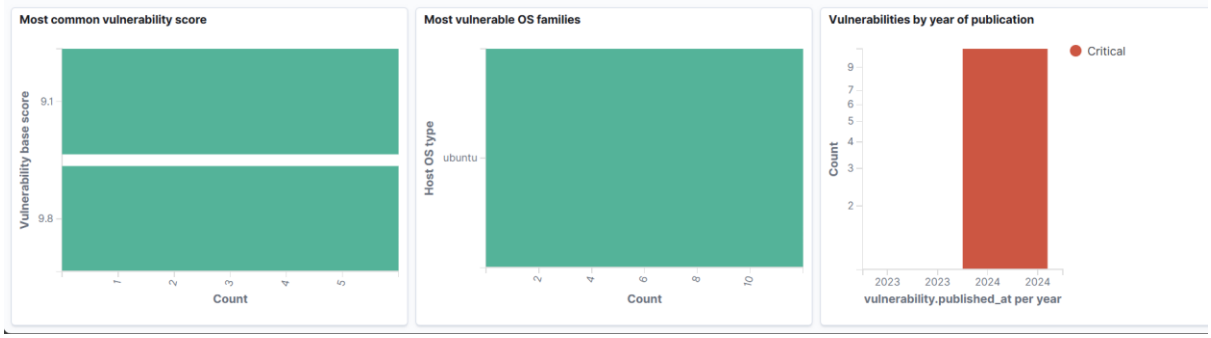
Agent Active

We can see now dashboard for Threat Hunting

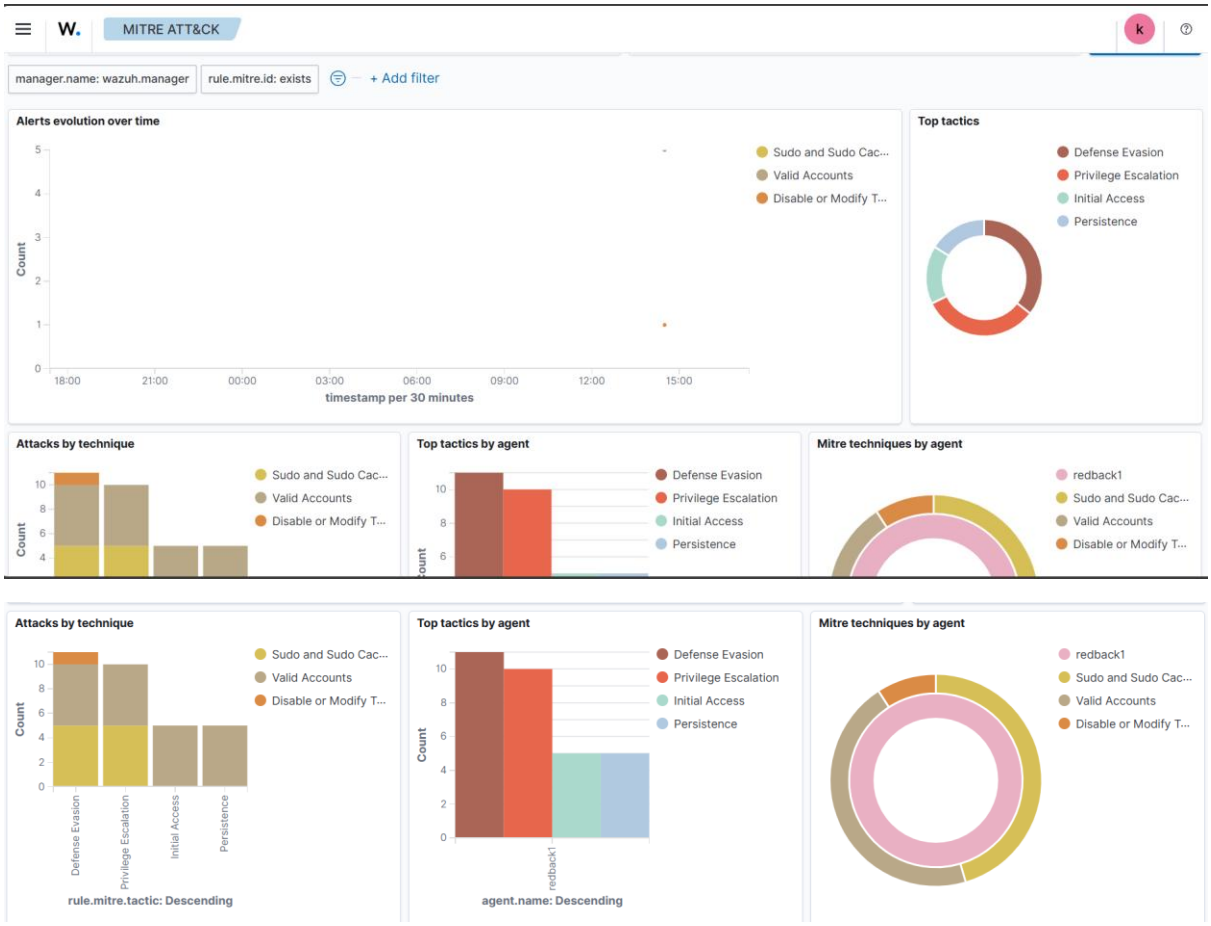


Threat Hunting Dashboard





Vulnerability Dashboard



MITTRE ATT&CK