

Wazuh Configuration

First add the Wazuh repository to your system.

```
sam@redback1:~/tpotce$ echo "deb [signed-by=/etc/apt/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | sudo tee /etc/apt/sources.list.d/wazuh.list
deb [signed-by=/etc/apt/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main
sam@redback1:~/tpotce$
```

Added repository

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

```
sam@redback1:~/tpotce$ sudo apt update
Get:1 https://packages.wazuh.com/4.x/apt stable InRelease [17.3 kB]
Hit:2 https://download.docker.com/linux/ubuntu focal InRelease
Get:3 https://packages.wazuh.com/4.x/apt stable/main amd64 Packages [41.6 kB]
Hit:4 http://ppa.launchpad.net/oisf/suricata-stable/ubuntu focal InRelease
Hit:5 http://archive.ubuntu.com/ubuntu focal InRelease
Hit:6 http://archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:7 http://archive.ubuntu.com/ubuntu focal-backports InRelease
Hit:8 http://archive.ubuntu.com/ubuntu focal-security InRelease
Fetched 58.8 kB in 2s (30.0 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
1 package can be upgraded. Run 'apt list --upgradable' to see it.
sam@redback1:~/tpotce$
```

Kernel PTI	Disabled
Uptime	1 Day 09 H

Package updated

Next we can install the Wazuh manager.

```
sam@redback1:~/tpotce$ sudo apt install wazuh-manager
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  golang-1.13-go golang-1.13-race-detector-runtime golang-1.13-src golang-race-detector-runtime golang-src
Use 'sudo apt autoremove' to remove them.
Suggested packages:
  expect
The following packages will be REMOVED:
  wazuh-agent
The following NEW packages will be installed:
  wazuh-manager
0 upgraded, 1 newly installed, 1 to remove and 0 not upgraded.
Need to get 333 MB of archives.
After this operation, 872 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 https://packages.wazuh.com/4.x/apt stable/main amd64 wazuh-manager amd64 4.9.2-1 [333 MB]
Fetched 333 MB in 5s (66.5 MB/s)
(Reading database ... 153365 files and directories currently installed.)
Removing wazuh-agent (4.5.0-1) ...
Selecting previously unselected package wazuh-manager.
(Reading database ... 153015 files and directories currently installed.)
Preparing to unpack .../wazuh-manager_4.9.2-1_amd64.deb ...
Unpacking wazuh-manager (4.9.2-1) ...
Setting up wazuh-manager (4.9.2-1) ...
Processing triggers for systemd (245.4-4ubuntu3.24) ...
sam@redback1:~/tpotce$
```

Uptime	1 Day 09 Hours 15 Minutes 03 Seconds
Current date/time	Tue Nov 26 12:48:20 UTC 2024

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 can check the status.

```
sam@redback1:~$ sudo systemctl start wazuh-manager
sam@redback1:~$ sudo systemctl enable wazuh-manager
sam@redback1:~$ sudo 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 Tue 2024-11-26 13:02:31 UTC; 49s ago
     Tasks: 213 (limit: 38410)
    Memory: 5.9G
    CGroup: /system.slice/wazuh-manager.service
            └─2246688 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
               2246689 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
               2246692 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
               2246695 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
               2246736 /var/ossec/bin/wazuh-authd
               2246749 /var/ossec/bin/wazuh-db
               2246776 /var/ossec/bin/wazuh-execd
               2246787 /var/ossec/bin/wazuh-analysisd
               2246796 /var/ossec/bin/wazuh-syscheckd
               2246810 /var/ossec/bin/wazuh-remoted
               2246929 /var/ossec/bin/wazuh-logcollector
               2246945 /var/ossec/bin/wazuh-monitord
               2246957 /var/ossec/bin/wazuh-modulesd

Nov 26 13:02:26 redback1 env[2246609]: Started wazuh-analysisd ...
Nov 26 13:02:26 redback1 env[2246609]: Started wazuh-syscheckd ...
Nov 26 13:02:27 redback1 env[2246609]: Started wazuh-remoted ...
Nov 26 13:02:27 redback1 env[2246609]: Started wazuh-logcollector ...
Nov 26 13:02:28 redback1 env[2246609]: Started wazuh-monitord ...
Nov 26 13:02:28 redback1 env[2246955]: 2024/11/26 13:02:28 wazuh-modulesd:router: INFO: Loaded router module.
Nov 26 13:02:28 redback1 env[2246955]: 2024/11/26 13:02:28 wazuh-modulesd:content_manager: INFO: Loaded content_manager module.
Nov 26 13:02:29 redback1 env[2246609]: Started wazuh-modulesd ...
Nov 26 13:02:31 redback1 env[2246609]: Completed.
Nov 26 13:02:31 redback1 systemd[1]: Started Wazuh manager.
sam@redback1:~$
```

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`”.

```
sam@redback1:~$ sudo tail -f /var/ossec/logs/ossec.log
2024/11/26 13:02:28 wazuh-modulesd:vulnerability-scanner: INFO: Starting database file decompression.
2024/11/26 13:02:28 wazuh-modulesd:syscollector: INFO: Evaluation finished.
2024/11/26 13:02:29 wazuh-logcollector: INFO: (9203): Monitoring journal entries.
2024/11/26 13:02:32 wazuh-syscheckd: INFO: (6009): File integrity monitoring scan ended.
2024/11/26 13:02:32 wazuh-syscheckd: INFO: FIM sync module started.
2024/11/26 13:02:34 sca: INFO: Evaluation finished for policy '/var/ossec/ruleset/sca/cis_ubuntu20-04.yml'
2024/11/26 13:02:34 sca: INFO: Security Configuration Assessment scan finished. Duration: 6 seconds.
2024/11/26 13:03:10 rootcheck: INFO: Ending rootcheck scan.
2024/11/26 13:03:14 wazuh-modulesd:vulnerability-scanner: INFO: Database decompression finished.
2024/11/26 13:03:14 wazuh-modulesd:vulnerability-scanner: INFO: Vulnerability scanner module started.
```

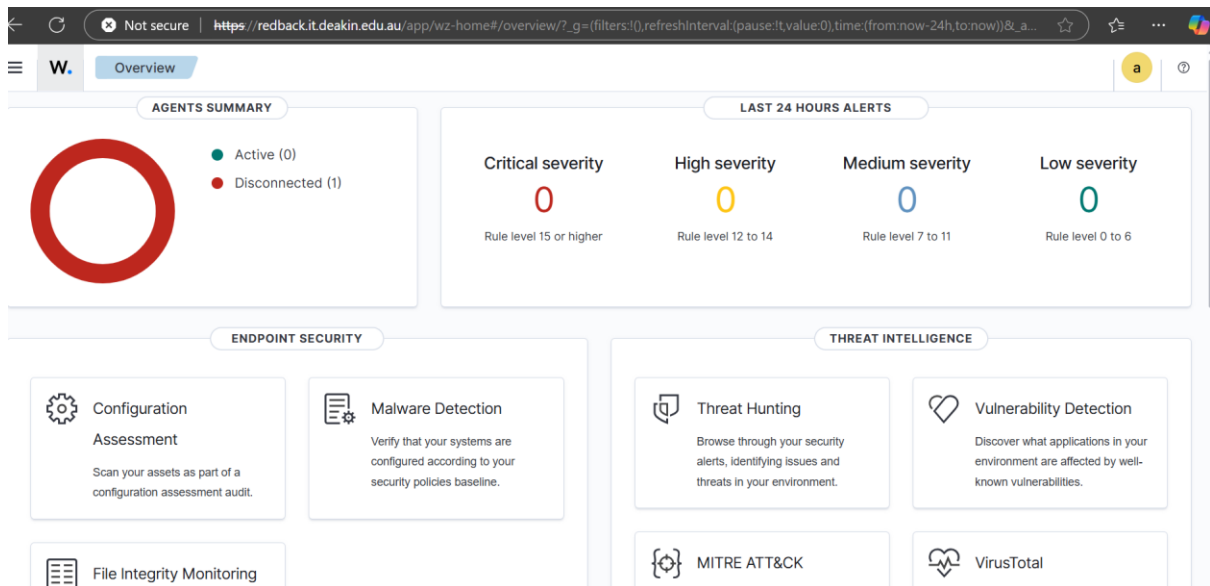
Wazuh running

```
sam@redback1:~/wazuh-docker/single-node$ docker-compose up -d
[+] Running 0/18
   " wazuh.dashboard Pulling
     " 07dd7d96b715 Waiting
     " cd29afa936d8 Waiting
     " 66e99de536f1 Waiting
     " b17592e806c8 Waiting
[+] Running 0/45b Waiting
   " wazuh.dashboard Pulling
```

CONTAINER ID	IMAGE	NAMES	COMMAND	CREATED	STATUS	PORTS
bec390c84e	wazuh/wazuh-dashboard:4.9.2	single-node-wazuh-dashboard-1	"/entrypoint.sh"	About a minute ago	Up About a minute	443/tcp, 0.0.0.0:443->5601/tcp, :::443->5601/tcp
680b1fc938	wazuh/wazuh-manager:4.9.2	single-node-wazuh-manager-1	"init"	About a minute ago	Up About a minute	0.0.0.0:1514-1515->1514-1515/tcp, :::1514-1515->1514-1515/tcp, 0.0.0.0:1514->514/udp, :::1514->514/udp, 0.0.0.0:55000->55000/tcp, :::55000->55000/tcp, 1516/tcp
1430c31ee75	wazuh/wazuh-indexer:4.9.2	single-node-wazuh-indexer-1	"/entrypoint.sh open."	About a minute ago	Up About a minute	0.0.0.0:9200->9200/tcp, :::9200->9200/tcp

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`”.

```
sam@redback1:/$ 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
gpg: keybox '/usr/share/keyrings/wazuh.gpg' created
gpg: key 96B3E5F2911145: public key 'Wazuh.com (Wazuh Signing Key) <support@wazuh.com>' imported
gpg: Total number processed: 1
gpg:   imported: 1
sam@redback1:/$
```

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`”.

```
sam@redback1:/$ 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
deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main
sam@redback1:/$
```

Added Repository

Now we can update package Information.

```
sam@redback1:/$ sudo apt-get update
Hit:1 http://archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:3 http://archive.ubuntu.com/ubuntu focal-backports InRelease
Hit:4 http://archive.ubuntu.com/ubuntu focal-security InRelease
Get:5 https://packages.wazuh.com/4.x/apt stable InRelease [17.3 kB]
Hit:6 https://download.docker.com/linux/ubuntu focal InRelease
Get:7 https://packages.wazuh.com/4.x/apt stable/main amd64 Packages [41.6 kB]
Hit:8 http://ppa.launchpad.net/oisf/suricata-stable/ubuntu focal InRelease
Fetched 58.8 kB in 11s (5,348 B/s)
Reading package lists... Done
sam@redback1:/$
```

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

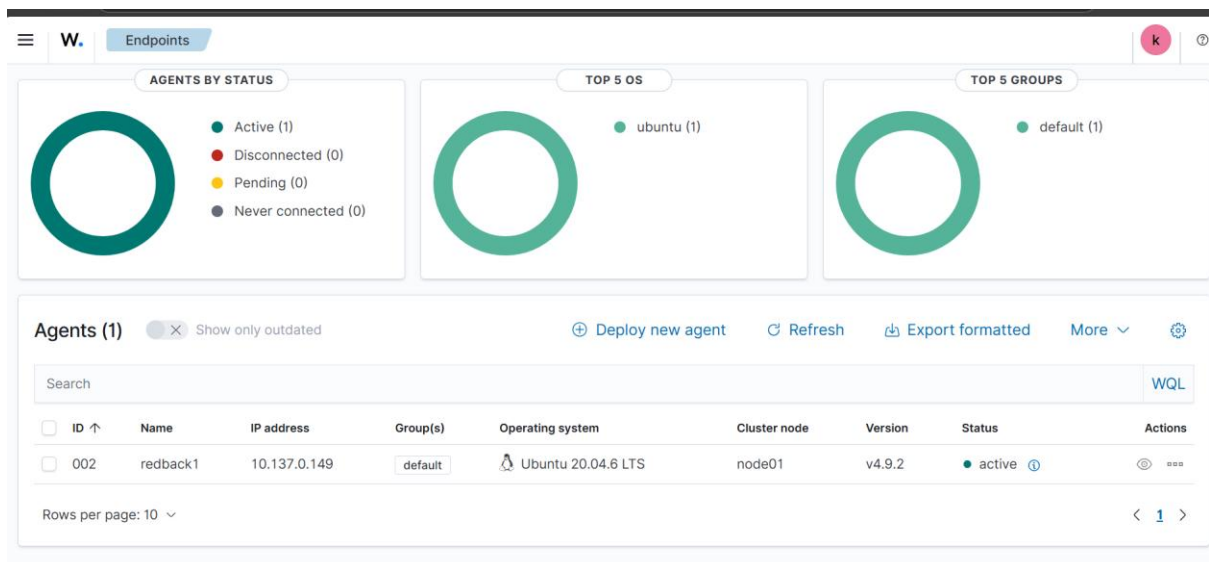
```

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 03:46:37 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

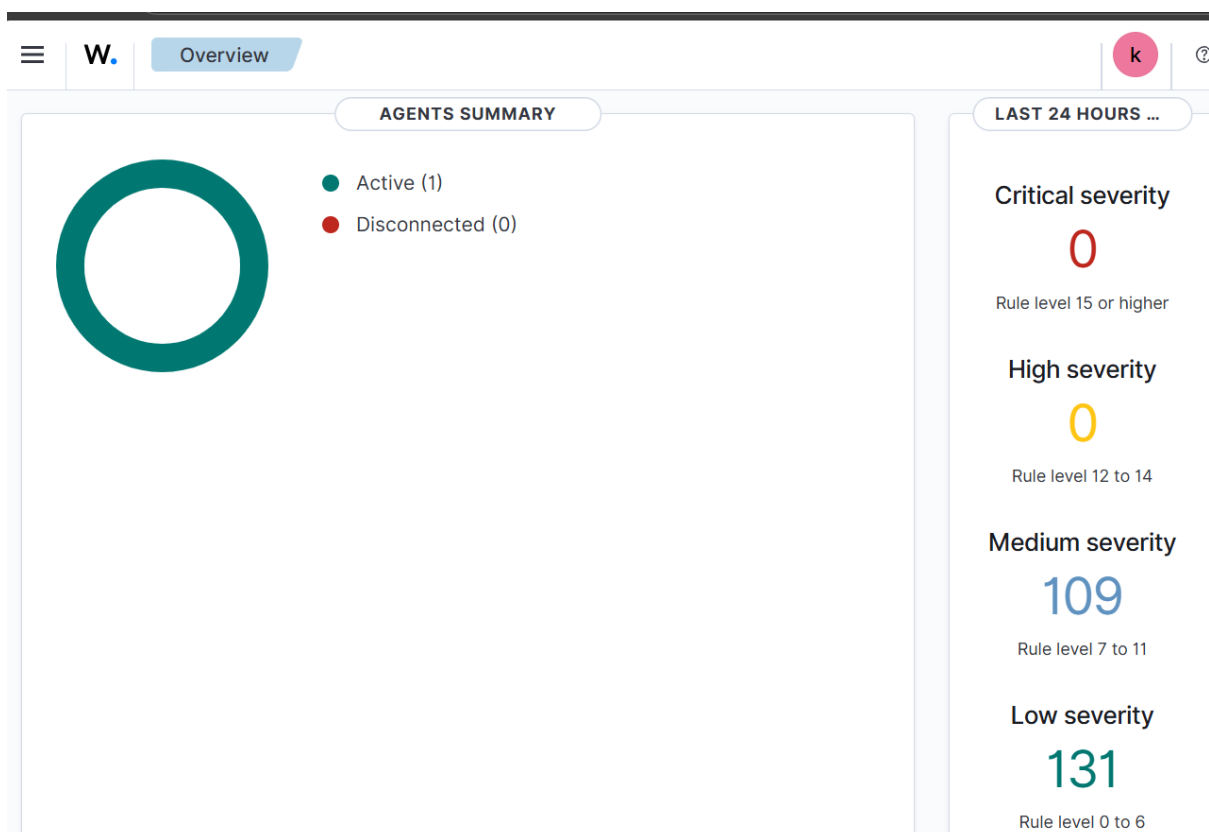
To prevent the agent from being accidentally upgraded and becoming incompatible with the Wazuh manager we can disable Wazuh updates.

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

Auto update disabled

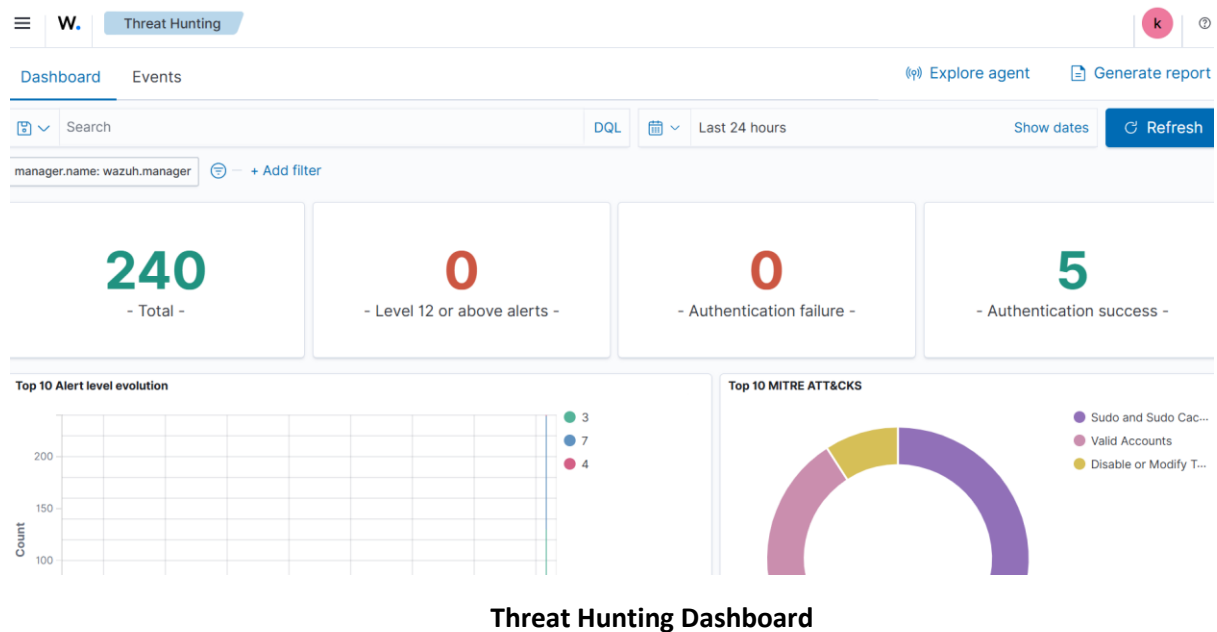
We can update the package again.

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.

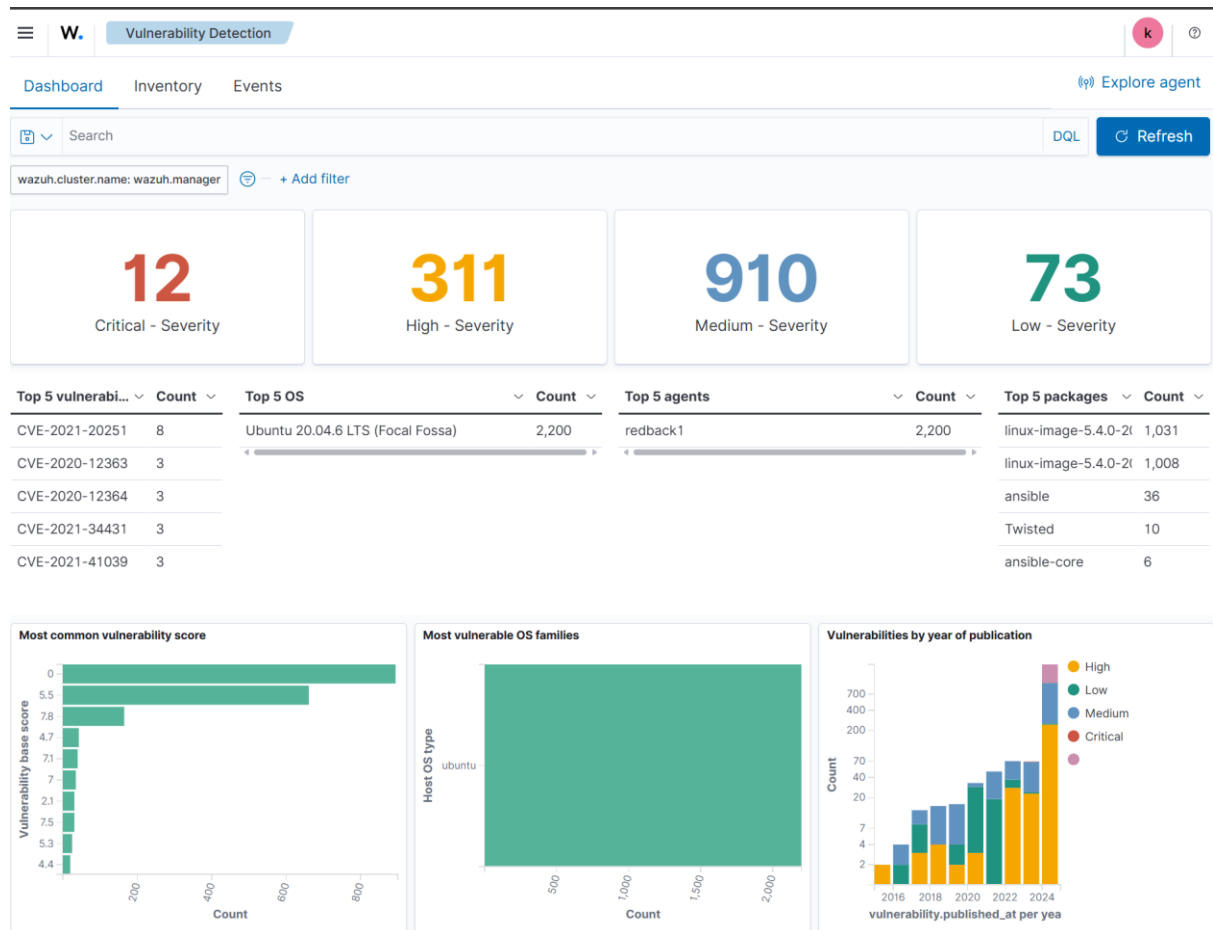


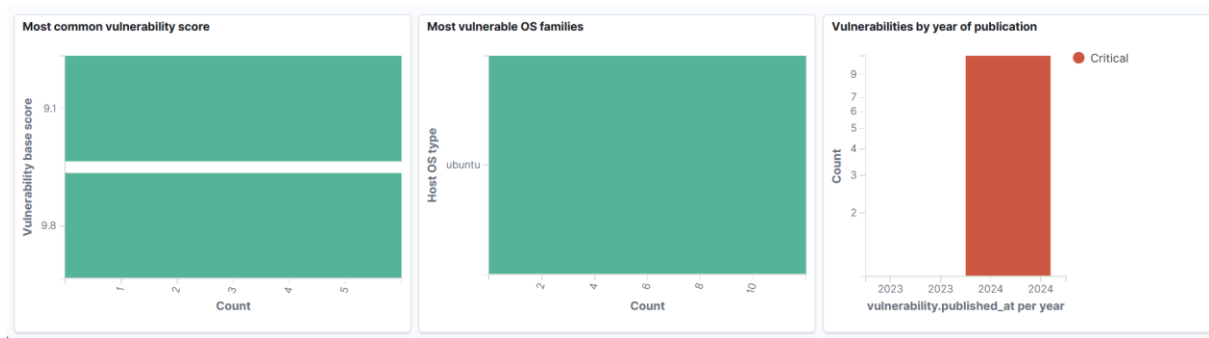
Agent Active

We can see now dashboard for Threat Hunting

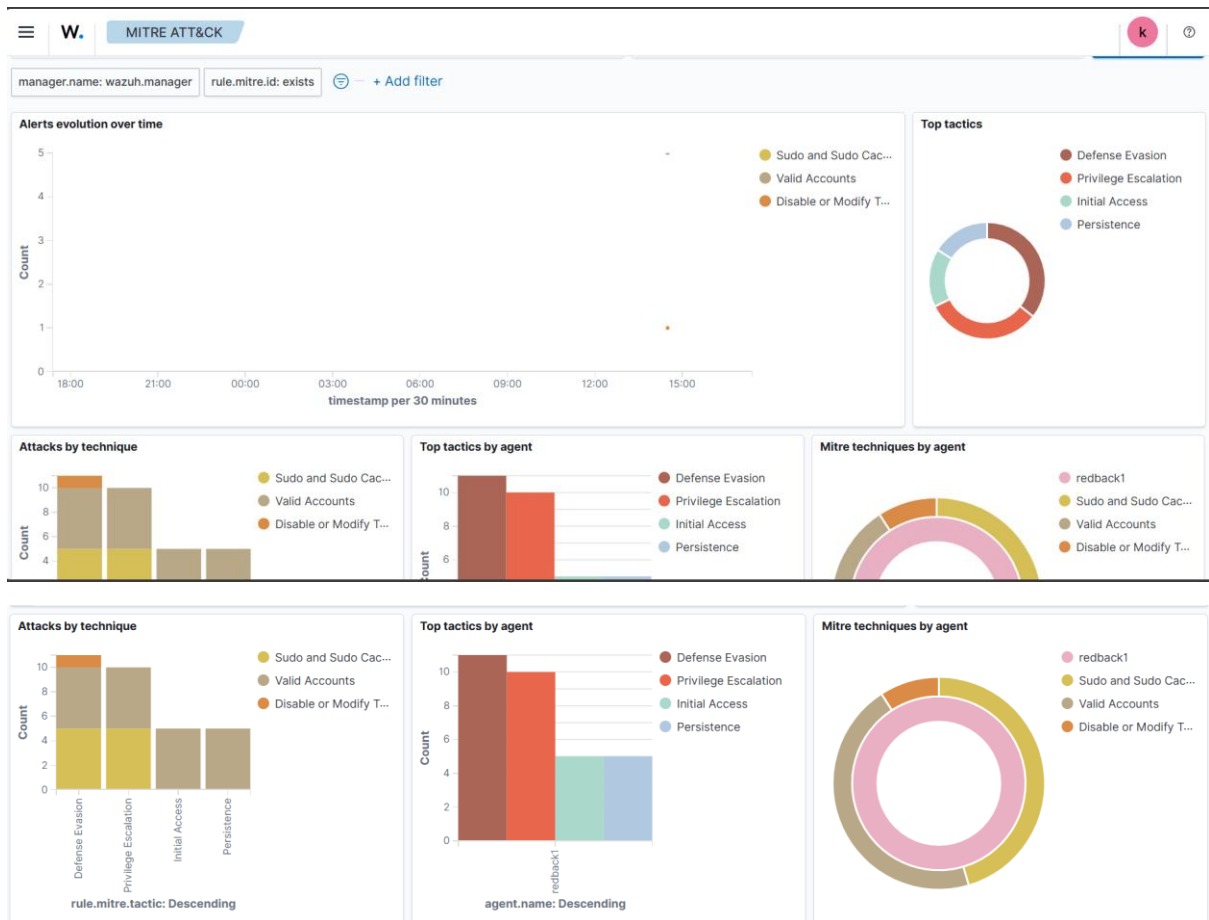


Threat Hunting Dashboard





Vulnerability Dashboard



MITTRE ATT&CK