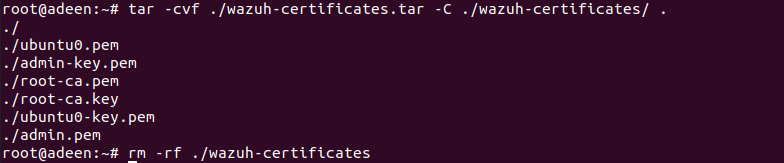
**WAZUH INDEXER**

1. **CERTIFICATES CREATION**





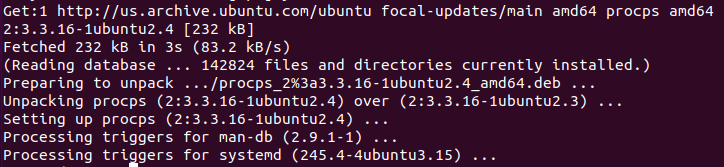
Copy the wazuh-certificates.tar file to all the nodes, including the Wazuh indexer, Wazuh server, and Wazuh dashboard nodes.

1. **NODES INSTALLATION**

# apt-get install debconf adduser procps

Adding the Wazuh repository

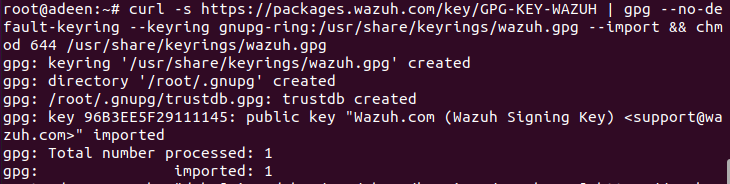
Install package



# apt-get install gnupg apt-transport-https

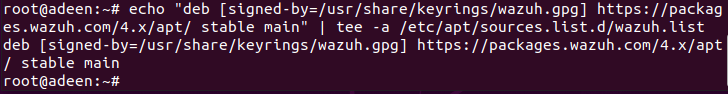
* Install the GPG key.

# curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg



* Add the repository.

# echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list

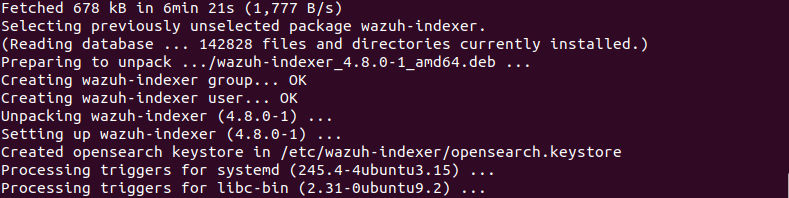


* Update the packages information.

# apt-get update

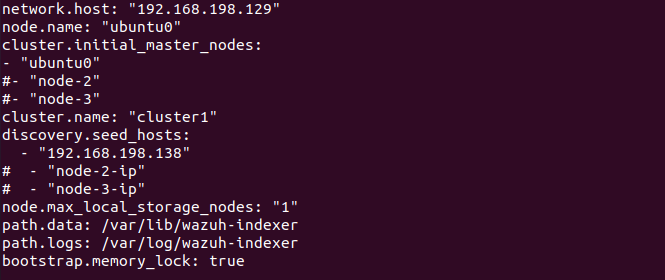
1. **Installing the Wazuh indexer**

Install the Wazuh indexer package.



1. **Configuring the Wazuh indexer**

Edit the /etc/wazuh-indexer/opensearch.yml



1. **Deploying certificates**

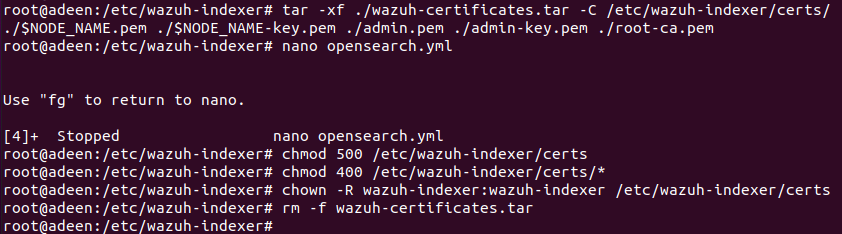
**Note** : copy of the wazuh-certificates.tar file, in your working directory.

Cd /etc/wazuh-indexer

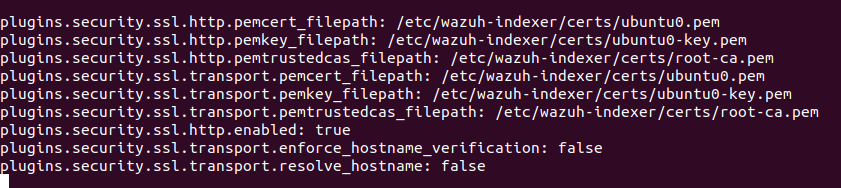
# NODE\_NAME=<indexer-node-name>

# mkdir /etc/wazuh-indexer/certs

# tar -xf ./wazuh-certificates.tar -C /etc/wazuh-indexer/certs/ ./$NODE\_NAME.pem ./$NODE\_NAME-key.pem ./admin.pem ./admin-key.pem ./root-ca.pem



Editing opensearch.yml



chmod 500 /etc/wazuh-indexer/certs

chmod 400 /etc/wazuh-indexer/certs/\*

chown -R wazuh-indexer:wazuh-indexer /etc/wazuh-indexer/certs

1. **Memory locking**

nano /usr/lib/systemd/system/wazuh-indexer.service

**Starting the Wazuh indexer**

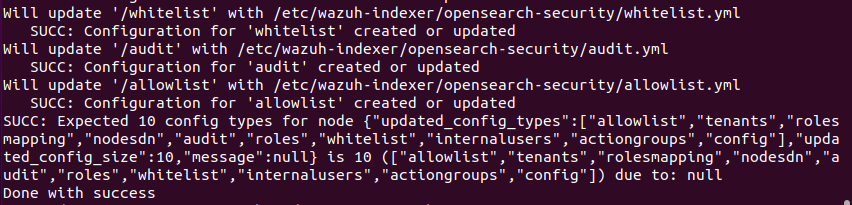
systemctl daemon-reload

systemctl enable wazuh-indexer

systemctl start wazuh-indexer

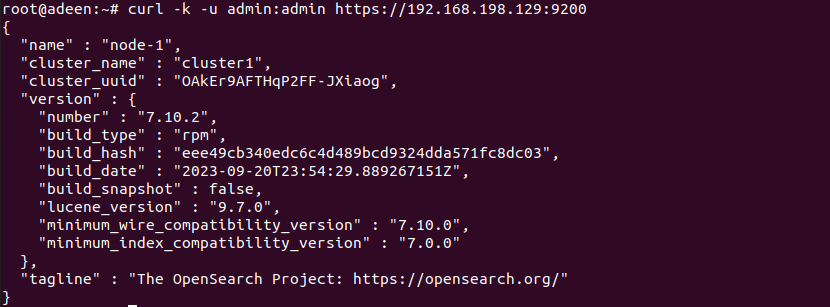
1. **Cluster Initialization**

# /usr/share/wazuh-indexer/bin/indexer-security-init.sh



confirm that the installation is successful

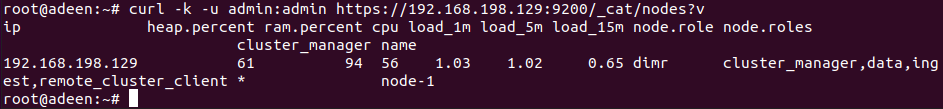
# curl –k –u admin:admin https://192.168.198.129:9200



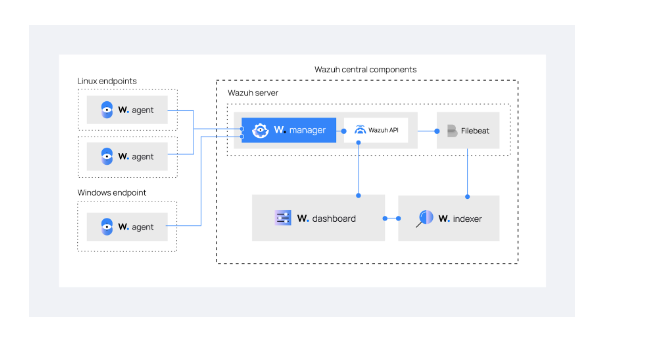


 check if the single-node or multi-node cluster is working correctly.

# curl –k –u admin:admin https://192.168.198.129:9200/\_cat/nodes?v

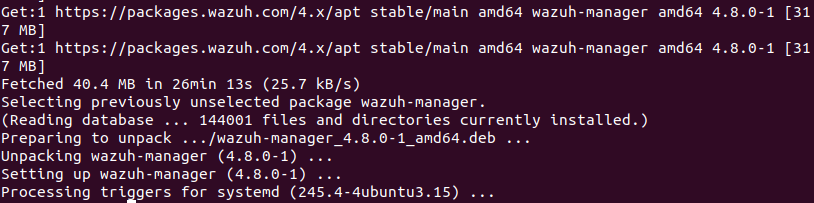


**WAZUH SERVER/MANAGER**



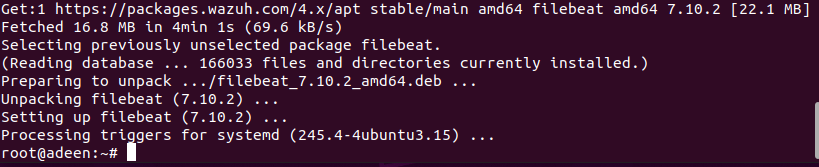
1. **INSTALLING WAZUH MANAGER**

apt-get -y install wazuh-manage



1. **INSTALLING FILEBEAT**

apt-get -y install filebeat

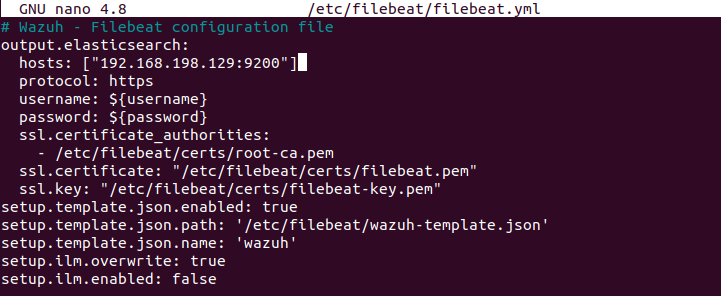


1. **CONFIGURING FILEBEAT**

* Download the preconfigured Filebeat configuration file.

# curl -so /etc/filebeat/filebeat.yml https://packages.wazuh.com/4.8/tpl/wazuh/filebeat/filebeat.yml

* Edit the **/etc/filebeat/filebeat.yml** configuration file



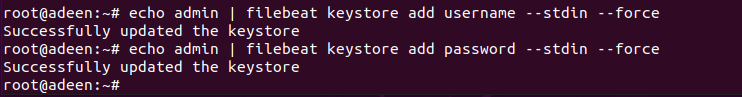
* Create a Filebeat keystore to securely store authentication credentials.

# filebeat keystore create

* Add the default username and password admin:admin to the secrets keystore.

# echo admin | filebeat keystore add username --stdin –force

# echo admin | filebeat keystore add password --stdin –force



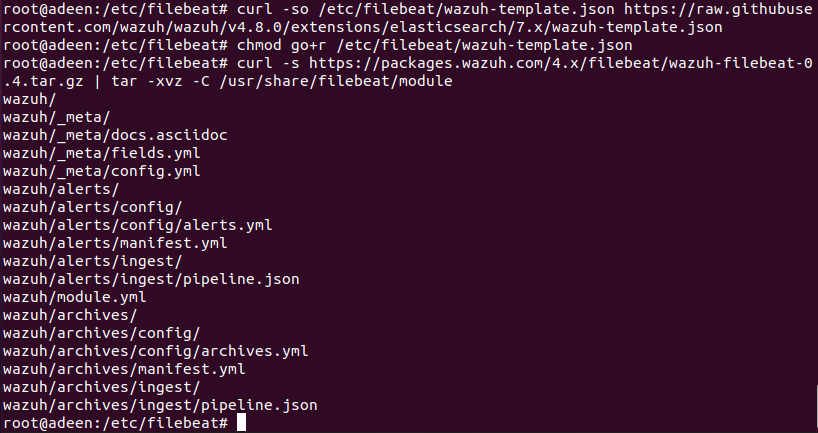
* Download the alerts template for the Wazuh indexer.

# curl -so /etc/filebeat/wazuh-template.json <https://raw.githubusercontent.com/wazuh/wazuh/v4.8.0/extensions/elasticsearch/7.x/wazuh-template.json>

# chmod go+r /etc/filebeat/wazuh-template.json

* Install the Wazuh module for Filebeat.

# curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat-0.4.tar.gz | tar -xvz -C /usr/share/filebeat/module



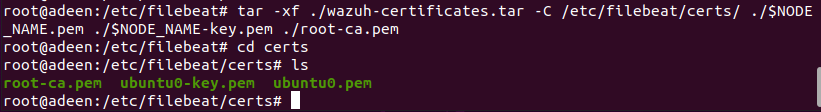
1. **DEPLOYING CERTIFICATES**

Replace <SERVER\_NODE\_NAME> with your Wazuh server node certificate name, the same one used in config.yml when creating the certificates. Then, move the certificates to their corresponding location.

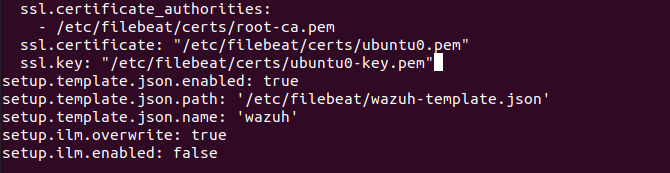
# NODE\_NAME=ubuntu0

# mkdir /etc/filebeat/certs

# tar -xf ./wazuh-certificates.tar -C /etc/filebeat/certs/ ./$NODE\_NAME.pem ./$NODE\_NAME-key.pem ./root-ca.pem



Edit filebeat.yml file



Ensure the Filebeat certificate and key name match the certificate files in /etc/filebeat/certs.

# chmod 500 /etc/filebeat/certs

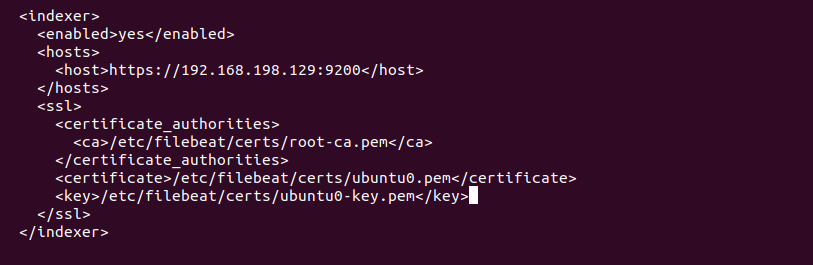
# chmod 400 /etc/filebeat/certs/\*

# chown -R root:root /etc/filebeat/certs

1. **CONFIGURING**

Edit /var/ossec/etc/ossec.conf to configure the indexer connection.

Change the ip and the certs name as well

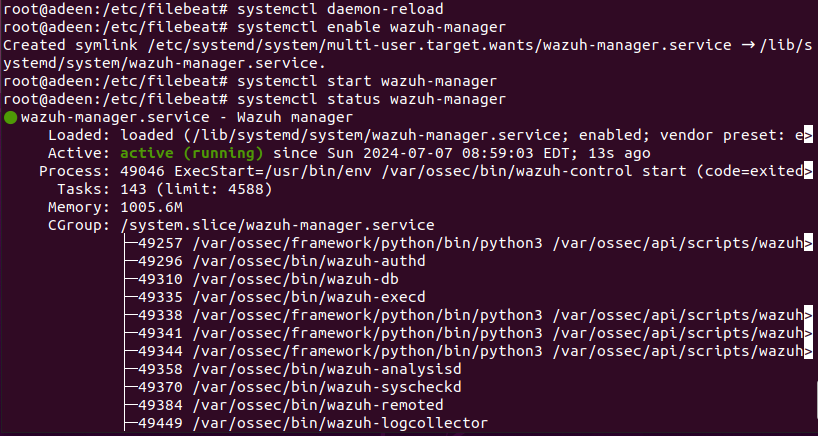


1. **STARTING THE MANAGER AND FILEBEAT**

# systemctl daemon-reload

# systemctl enable wazuh-manager

# systemctl start wazuh-manager



systemctl daemon-reload

systemctl enable filebeat

systemctl start filebeat

Filebeat test output



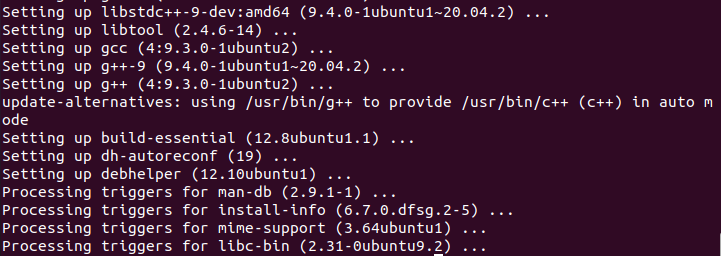
**WAZUH DASHBOARD**

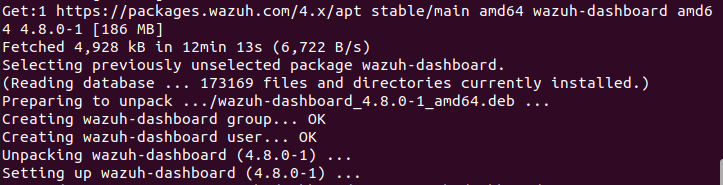
1. **INSTALLING WAZUH DASHBOARD**

Install the Wazuh dashboard package.

# apt-get install debhelper tar curl libcap2-bin #debhelper version 9 or later

# apt-get -y install wazuh-dashboard

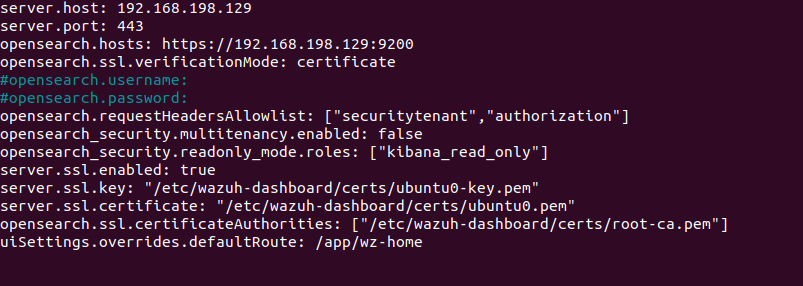




1. **CONFIGURING WAZUH DASHBOARD**

Configuring the Wazuh dashboard

Edit the /etc/wazuh-dashboard/opensearch\_dashboards.yml



1. **DEPLOYING CERTIFICATES**

# NODE\_NAME=ubuntu0

# mkdir /etc/wazuh-dashboard/certs

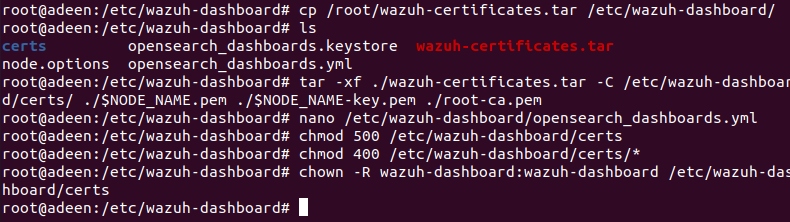
# tar -xf ./wazuh-certificates.tar -C /etc/wazuh-dashboard/certs/ ./$NODE\_NAME.pem ./$NODE\_NAME-key.pem ./root-ca.pem

# nano /etc/wazuh-dashboard/opensearch\_dashboards.yml

# chmod 500 /etc/wazuh-dashboard/certs

# chmod 400 /etc/wazuh-dashboard/certs/\*

# chown -R wazuh-dashboard:wazuh-dashboard /etc/wazuh-dashboard/certs

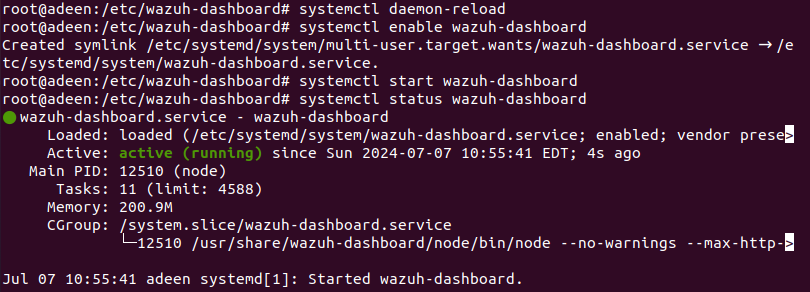


1. **STARTING THE SERVICE**

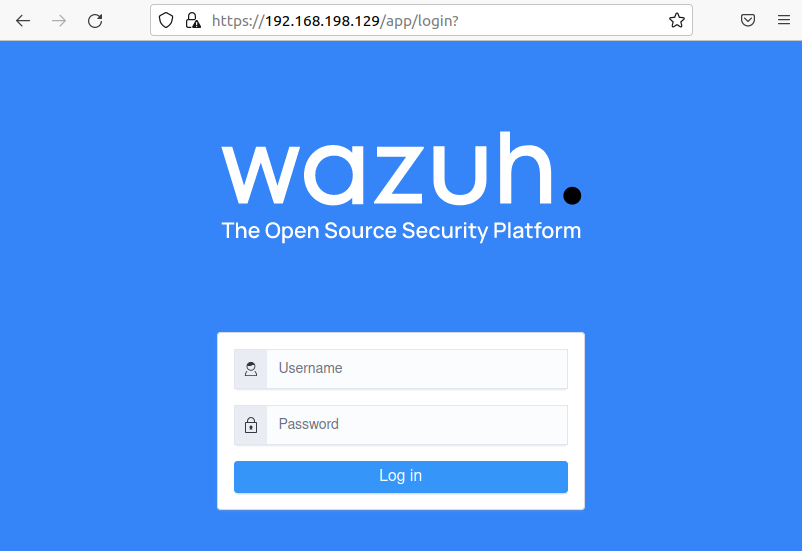
# systemctl daemon-reload

# systemctl enable wazuh-dashboard

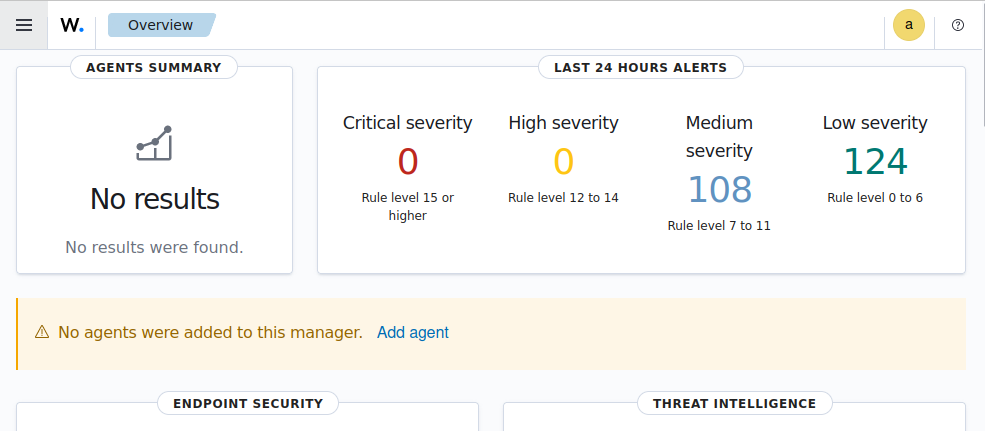
# systemctl start wazuh-dashboard



Navigate to the wazuh dashboard in browser



Login via admin:admin



Use the Wazuh passwords tool to change all the internal users' passwords.

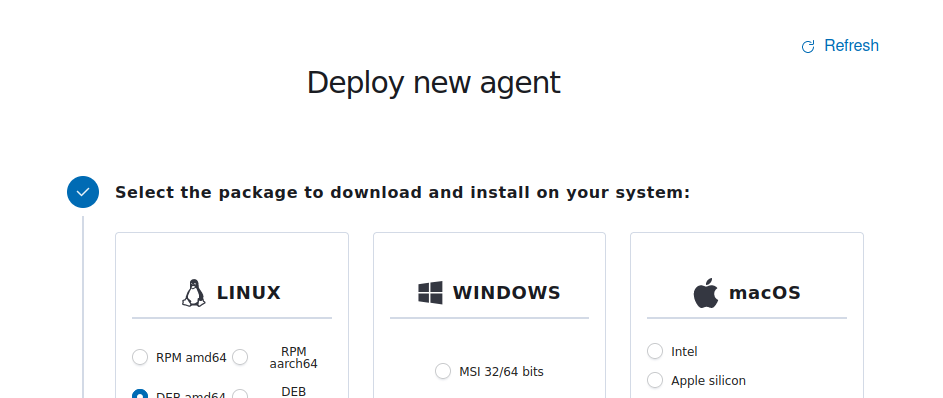
# /usr/share/wazuh-indexer/plugins/opensearch-security/tools/wazuh-passwords-tool.sh --change-all --admin-user wazuh --admin-password wazuh

**WAZUH AGENT**

1. **DEPLOTING NEW AGENT**

Go to wazuh dashboard >> agent and then deploy a new agent.

Linux agent



1. **RUN THE COMMAND ON AGENT**

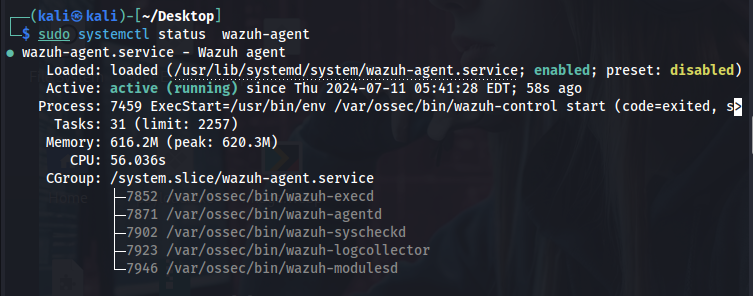
# wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent\_4.8.0-1\_amd64.deb && sudo WAZUH\_MANAGER='192.168.198.129' WAZUH\_AGENT\_NAME='kaliBB' dpkg -i ./wazuh-agent\_4.8.0-1\_amd64.deb

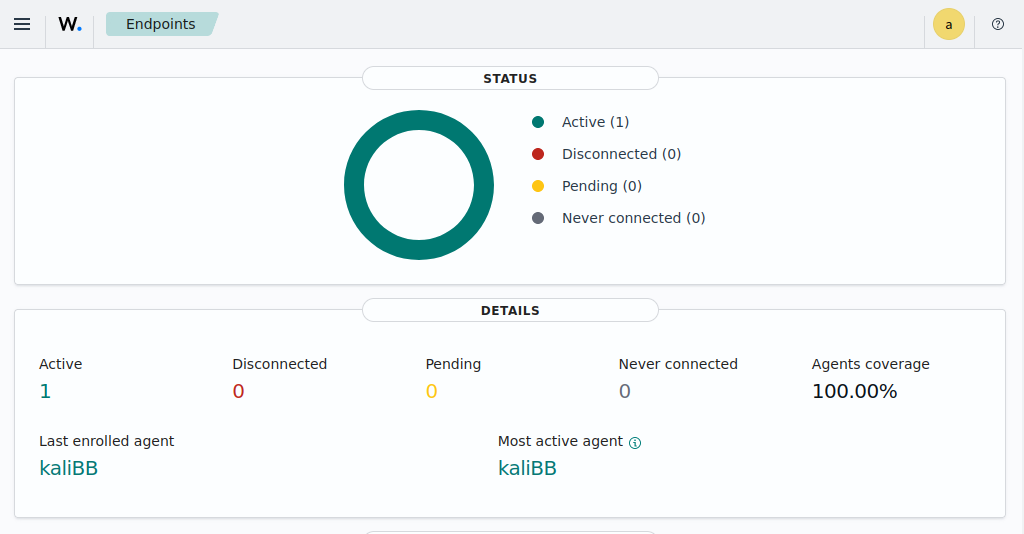
1. **START SERVICE ON AGENT**

sudo systemctl daemon-reload

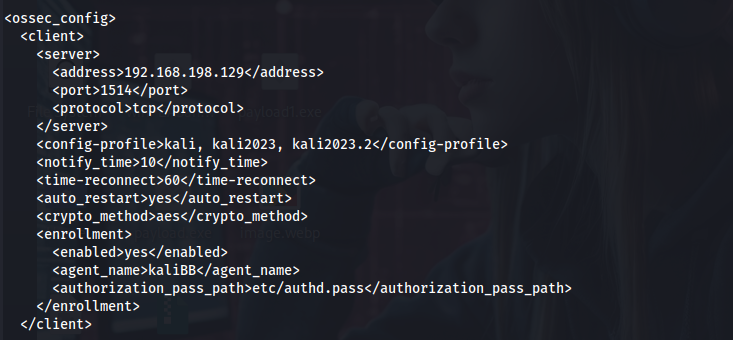
sudo systemctl enable wazuh-agent

sudo systemctl start wazuh-agent

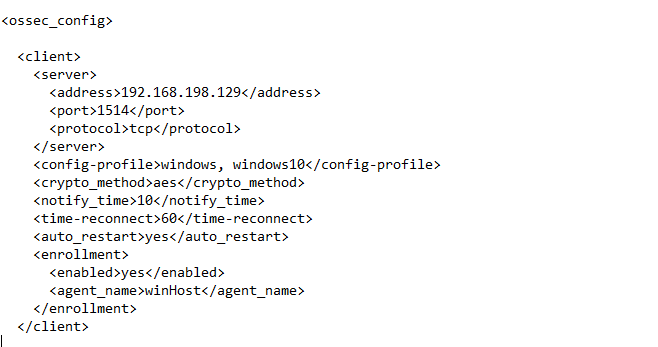




Check manager ip in agent’s /var/ossec/etc/ossec.conf

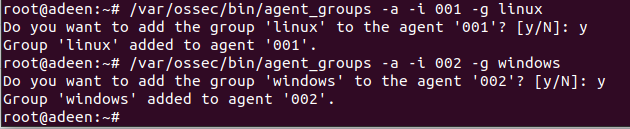


In windows



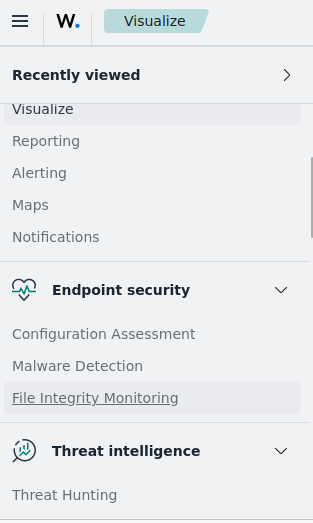
Assiging agents to multiple groups

# Assign group 'linux' to agent 001



Installing sysmon on endpoins and then telling wazuh to grab those logs.

**ENDPOINT SECURITY**



1. **FILE INTEGRITY MONITORING**

File Integrity Monitoring (FIM) is a security measure that checks if important files on your computer or network have been changed without permission.

It is a security process that validates the integrity of operating system and application files by constantly monitoring and verifying their current state against a known, trusted baseline.

The *primary goal* of FIM is to **detect unauthorized changes, such as modifications, deletions, or additions to files,** which may indicate potential security breaches, malware infections, or operational errors.

It keeps an eye on these files to make sure they stay the way they should, which helps catch problems like viruses or hacking attempts early.

**Linux Agent**

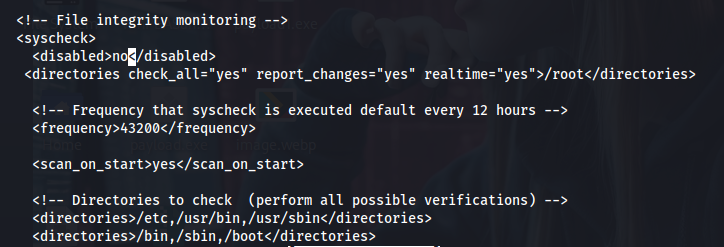
Edit the Wazuh agent /var/ossec/etc/ossec.conf

# nano /var/ossec/etc/ossec.conf

Enable the syscheck and add the *directories f*or monitoring within the ***<syscheck>*** block.

Let’s check root directories for now:

<directories check\_all="yes" report\_changes="yes" realtime="yes">/root</directories>

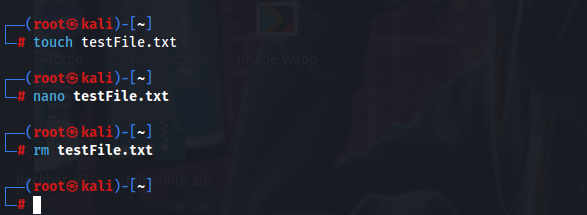


Restart the agent so that changes can take effect

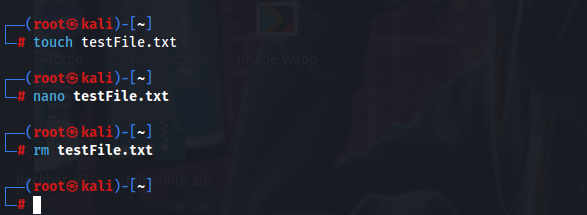
**Testing The Configuration**

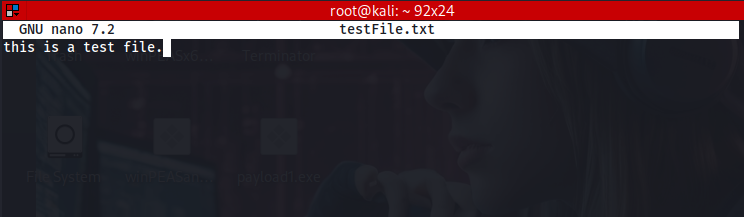
Let’s check the alerts of the file integrity monitoring. First generate a file in the directory that has been added to the <syscheck> block i.e root in our case and then alter the file.

Create a file

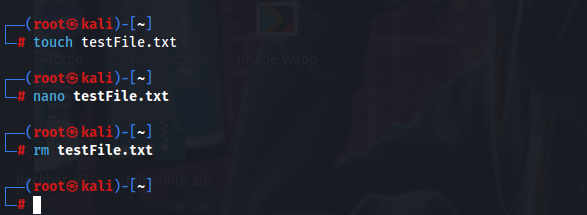


Edit the file

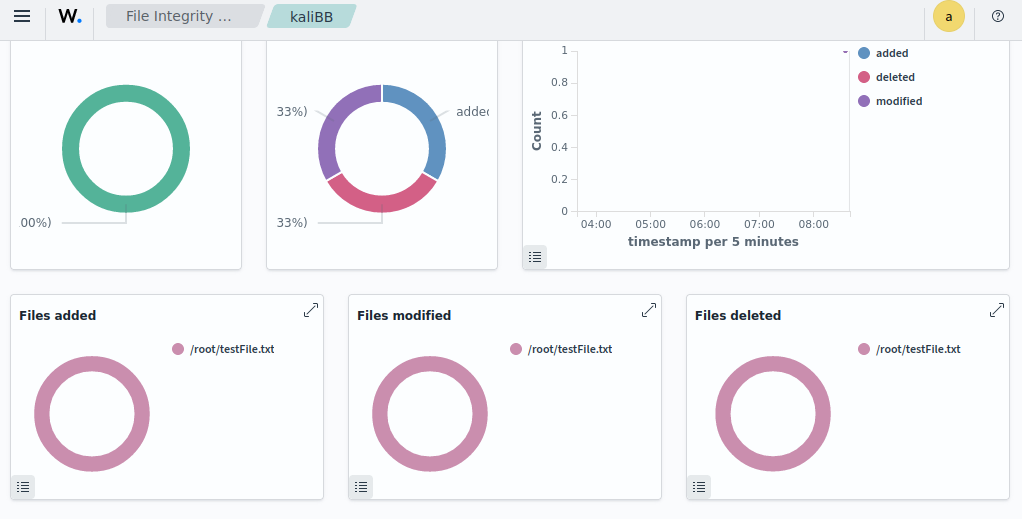


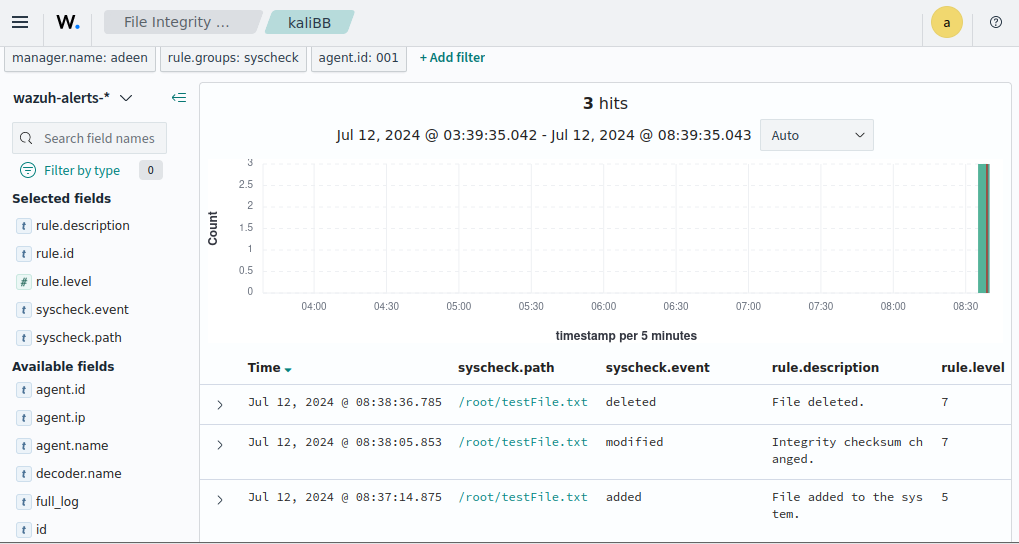


Delete the file.



Check the alerts in wazuh





**windows Agent**

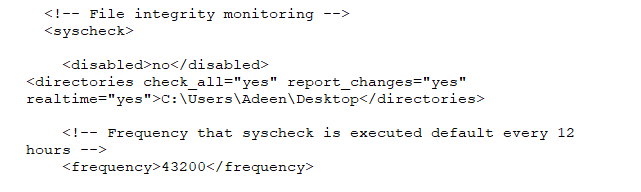
Edit the Wazuh agent C:\Program Files (x86)\ossec-agent\osse.conf file

Enable the syscheck and add the *directories f*or monitoring within the ***<syscheck>*** block.

Let’s check desktop directory of user adeen for now:

<directories check\_all="yes" report\_changes="yes" realtime="yes"> C:\Users\Adeen\Desktop </directories>

Restart the agent so that changes can take effect

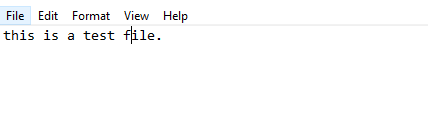
**Testing The Configuration**

Let’s check the alerts of the file integrity monitoring. First generate a file in the directory that has been added to the <syscheck> block i.e root in our case and then alter the file.

Create a file on desktop

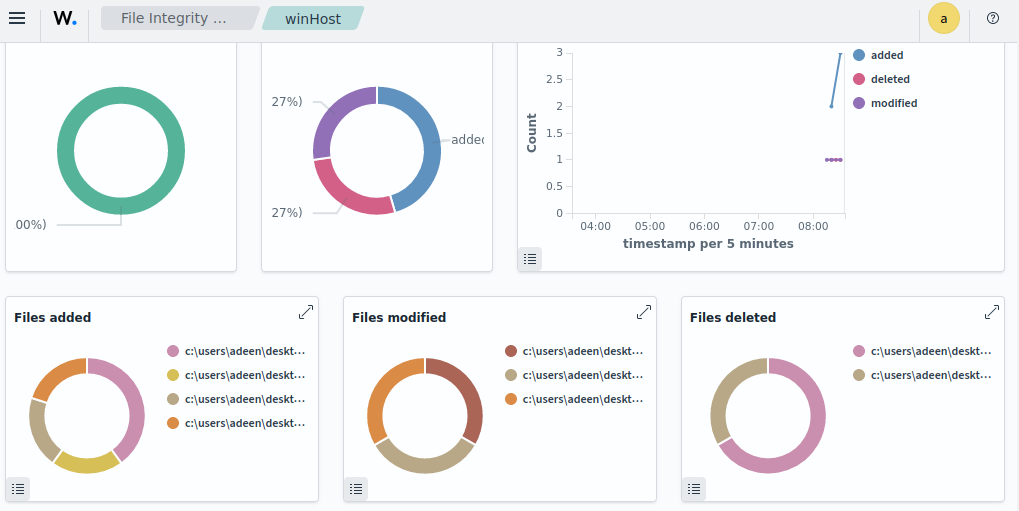


Edit the file

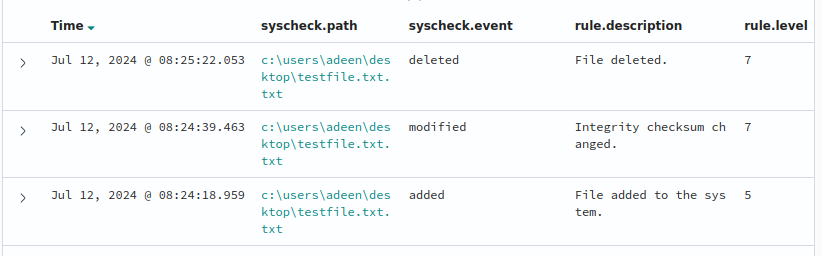


Delete the file.

Check the alerts in wazuh



events



**DETECTING A BRUTE FORCE ATTACK**

A brute force attack is a method used to gain unauthorized access to a system or account by trying every possible combination of passwords or encryption keys until the correct one is found.

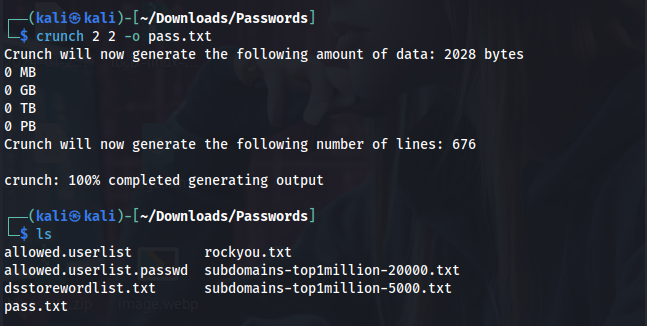
“Services like SSH on Linux endpoints and RDP on Windows endpoints are usually prone to brute-force attacks. Wazuh identifies brute-force attacks by correlating multiple authentication failure events.”

**Attacking Using Hydra**

From an attacker machine run hydra and perform brute forcing on one of the agents.

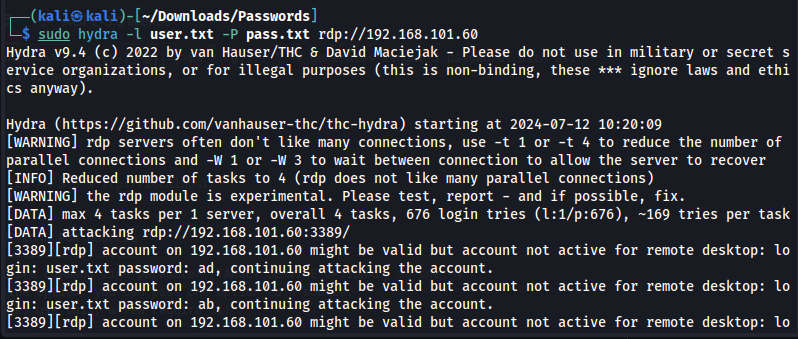
Creating a short text file with some passwords.

# crunch 2 2 –o pass.txt



Launch a brute force attack using the pass.txt file

# sudo hydra -l user.txt -P pass.txt rdp://192.168.101.60



**Windows Agent**

# sudo hydra -l user.txt -P pass.txt rdp://192.168.101.60

**Visualizing Alerts In Wazuh**