

Wazuh Installation & FIM Monitoring

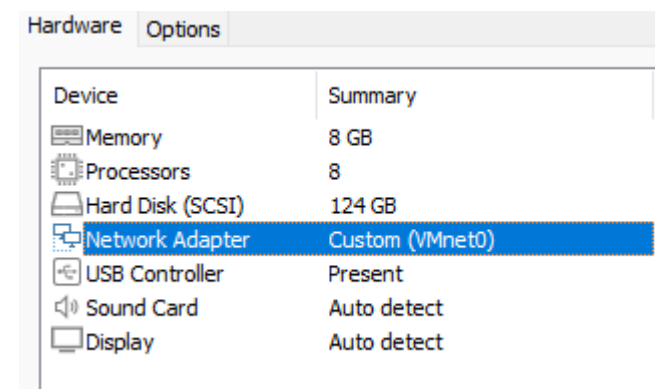
Talal Ahmed | Team Lambda

Installing Wazuh Manager

To install Wazuh, first make sure you meet the system requirements.

I will use Ubuntu on VMWare for the host. I have given this VM plenty of RAM and Processors.

Agents	CPU	RAM	Storage (90 days)
1-25	4 vCPU	8 GiB	50 GB
25-50	8 vCPU	8 GiB	100 GB
50-100	8 vCPU	8 GiB	200 GB



Wazuh documentation provides a simple installation assistant. The following command is used to run the installation assistant.

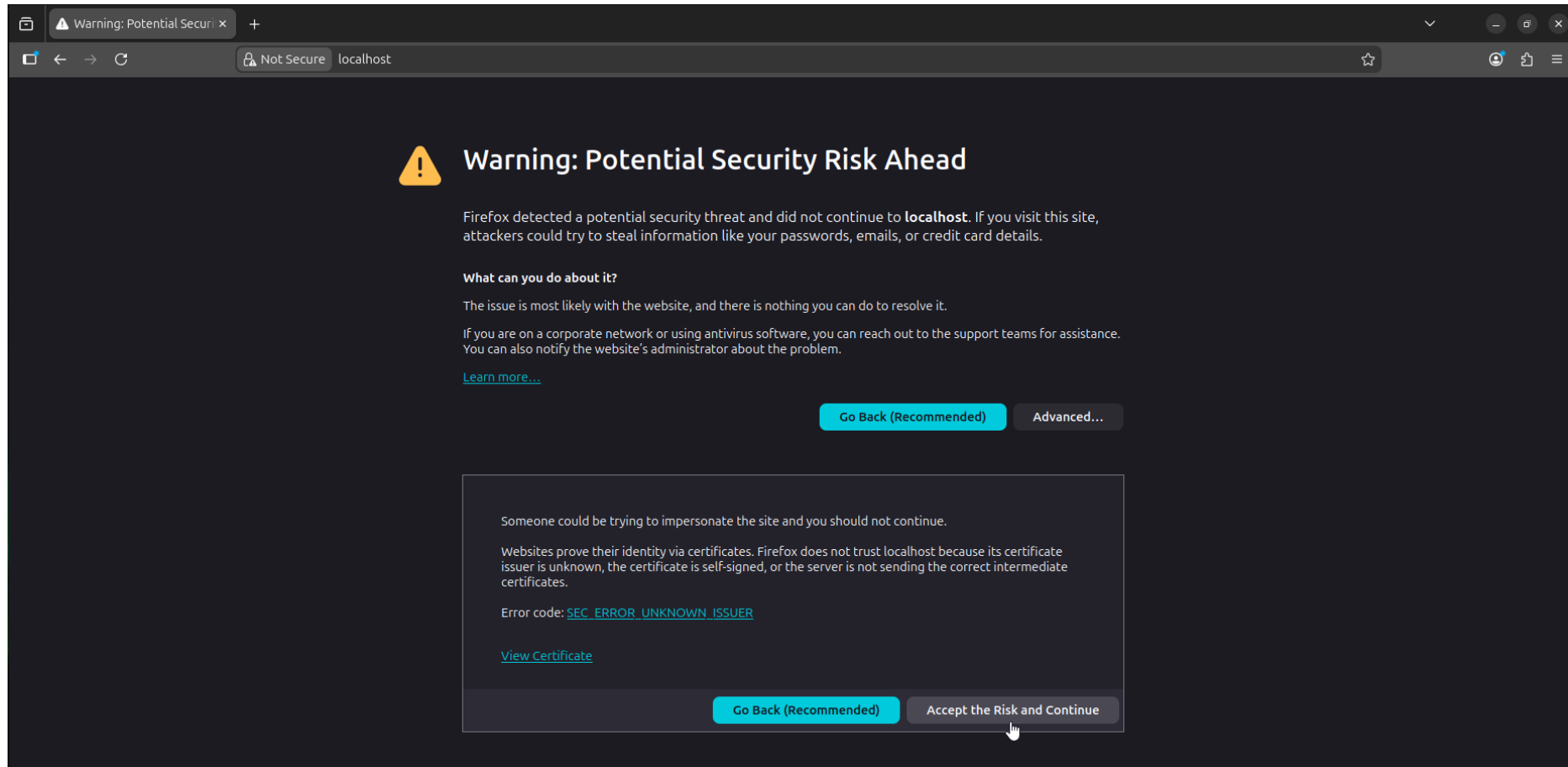
```
$ curl -sO https://packages.wazuh.com/4.14/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

```
ubuntu@ubuntu2404:~$ curl -sO https://packages.wazuh.com/4.14/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
07/01/2026 04:21:39 INFO: Starting Wazuh installation assistant. Wazuh version: 4.14.1
07/01/2026 04:21:39 INFO: Verbose logging redirected to /var/log/wazuh-install.log
07/01/2026 04:21:49 INFO: --- Dependencies ---
07/01/2026 04:21:49 INFO: Installing gawk.
07/01/2026 04:21:55 INFO: Verifying that your system meets the recommended minimum hardware requirements.
07/01/2026 04:21:55 INFO: Wazuh web interface port will be 443.
07/01/2026 04:22:00 INFO: --- Dependencies ---
07/01/2026 04:22:00 INFO: Installing apt-transport-https.
07/01/2026 04:22:08 INFO: Installing debhelper.
07/01/2026 04:22:44 INFO: Wazuh repository added.
07/01/2026 04:22:44 INFO: --- Configuration files ---
07/01/2026 04:22:44 INFO: Generating configuration files.
07/01/2026 04:22:44 INFO: Generating the root certificate.
07/01/2026 04:22:45 INFO: Generating Admin certificates.
07/01/2026 04:22:45 INFO: Generating Wazuh indexer certificates.
07/01/2026 04:22:45 INFO: Generating Filebeat certificates.
07/01/2026 04:22:45 INFO: Generating Wazuh dashboard certificates.
07/01/2026 04:22:45 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and pass
words necessary for installation.
07/01/2026 04:22:46 INFO: --- Wazuh indexer ---
07/01/2026 04:22:46 INFO: Starting Wazuh indexer installation.
```

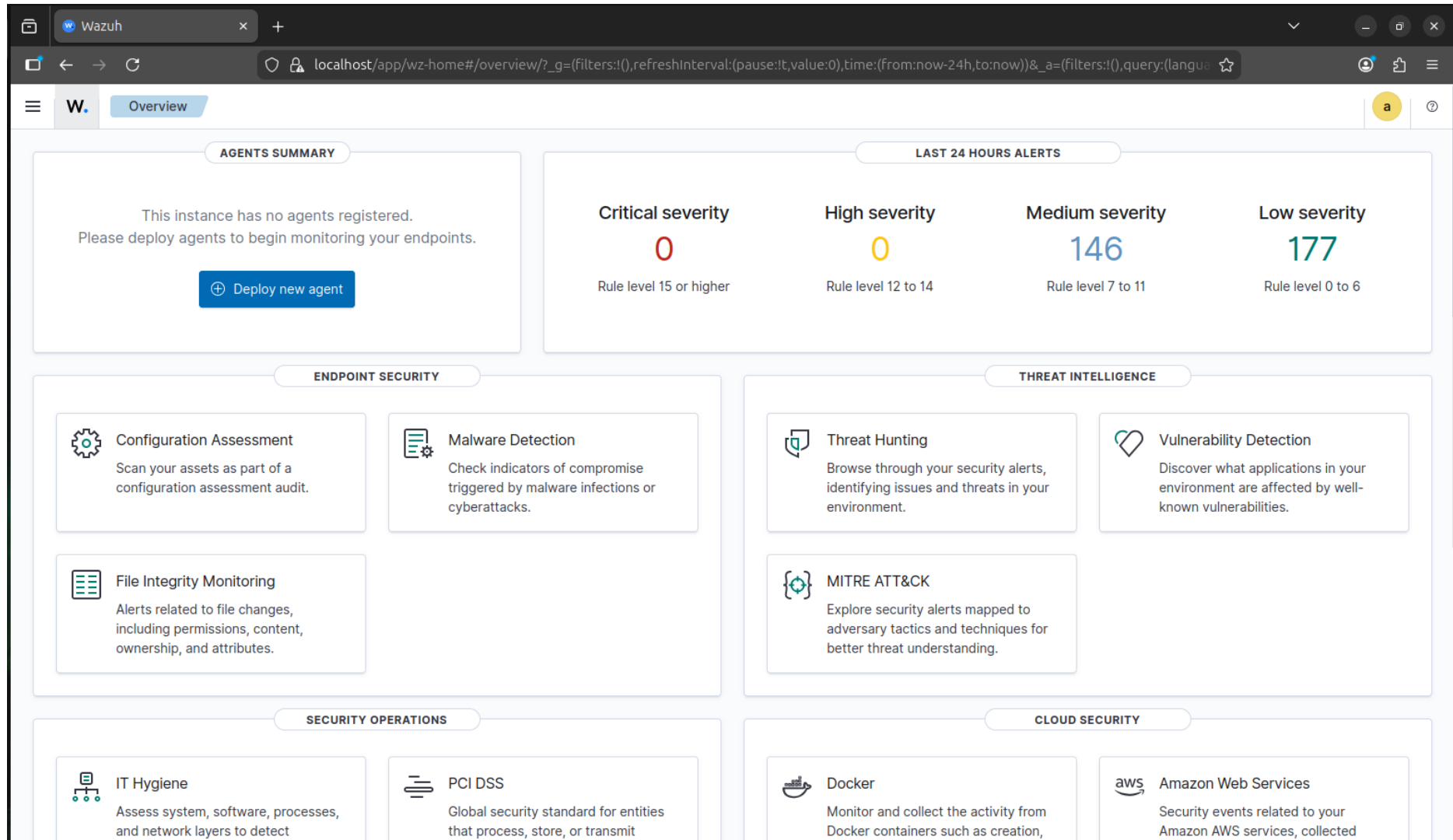
The installation takes some time and at the end it outputs the default username and password.

```
10/01/2026 08:43:49 INFO: Starting Wazuh dashboard installation.
10/01/2026 08:47:05 INFO: Wazuh dashboard installation finished.
10/01/2026 08:47:06 INFO: Wazuh dashboard post-install configuration finished.
10/01/2026 08:47:06 INFO: Starting service wazuh-dashboard.
10/01/2026 08:47:07 INFO: wazuh-dashboard service started.
10/01/2026 08:47:09 INFO: Updating the internal users.
10/01/2026 08:47:18 INFO: A backup of the internal users has been saved in the /etc/wazuh-indexer/internalusers-backup folder.
10/01/2026 08:47:43 INFO: The filebeat.yml file has been updated to use the Filebeat Keystore username and password.
10/01/2026 08:48:25 INFO: Initializing Wazuh dashboard web application.
10/01/2026 08:48:26 INFO: Wazuh dashboard web application initialized.
10/01/2026 08:48:26 INFO: --- Summary ---
10/01/2026 08:48:26 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
    User: admin
    Password: FUIB*MsZD0uIX0ZLdmMk?ucH0ISOAEoM
10/01/2026 08:48:26 INFO: --- Dependencies ----
10/01/2026 08:48:26 INFO: Removing gawk.
10/01/2026 08:48:32 INFO: Installation finished.
ubuntu@ubuntu2404:~$
```

We can access the dashboard at <https://localhost:443>



This warning can be safely ignored.



Wazuh Overview

AGENTS SUMMARY

This instance has no agents registered.
Please deploy agents to begin monitoring your endpoints.

[+ Deploy new agent](#)

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	0	146	177
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	Rule level 0 to 6

ENDPOINT SECURITY

- Configuration Assessment**
Scan your assets as part of a configuration assessment audit.
- Malware Detection**
Check indicators of compromise triggered by malware infections or cyberattacks.
- File Integrity Monitoring**
Alerts related to file changes, including permissions, content, ownership, and attributes.

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.
- MITRE ATT&CK**
Explore security alerts mapped to adversary tactics and techniques for better threat understanding.

SECURITY OPERATIONS

- IT Hygiene**
Assess system, software, processes, and network layers to detect
- PCI DSS**
Global security standard for entities that process, store, or transmit

CLOUD SECURITY

- Docker**
Monitor and collect the activity from Docker containers such as creation,
- Amazon Web Services**
Security events related to your Amazon AWS services, collected

And just like that we have successfully installed Wazuh.

W.

Endpoints

Deploy new agent

<

Deploy new agent

✓

Select the package to download and install on your system:

 LINUX

☐ RPM amd64

☐ RPM aarch64

☒ DEB amd64

☐ DEB aarch64

 WIN

☐ MS

①

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 ①

192.168.1.17

✓

Remember server address



W.

Endpoints

Deploy new agent

a



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: [?](#)

[?](#) The agent name must be unique. It can't be changed once the agent has been enrolled. [?](#)

Select one or more existing groups: [?](#)



4

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_4.14.1-1_amd64.deb && sudo WAZUH_MANAGER='192.168.1.17' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='ubuntu' dpkg -i ./wazuh-agent_4.14.1-1_amd64.deb
```

5

Start the agent:

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

```

Jan 15 06:41
ubuntu@ubuntu2404: ~
wazuh-agent_4.14.1-1_amd64.deb 100%[=====] 12.50M 1.23MB/s in 18s
2026-01-15 06:40:19 (708 KB/s) - 'wazuh-agent_4.14.1-1_amd64.deb' saved [13112530/13112530]
Selecting previously unselected package wazuh-agent.
(Reading database ... 151157 files and directories currently installed.)
Preparing to unpack .../wazuh-agent_4.14.1-1_amd64.deb ...
Unpacking wazuh-agent (4.14.1-1) ...
Setting up wazuh-agent (4.14.1-1) ...
ubuntu@ubuntu2404:~$ sudo systemctl daemon-reload
ubuntu@ubuntu2404:~$ sudo systemctl enable wazuh-agent
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service → /usr/lib/systemd/system/wazuh-agent.service.
ubuntu@ubuntu2404:~$ sudo systemctl start wazuh-agent
ubuntu@ubuntu2404:~$ sudo systemctl status wazuh-agent
● wazuh-agent.service - Wazuh agent
   Loaded: loaded (/usr/lib/systemd/system/wazuh-agent.service; enabled; preset: enabled)
   Active: active (running) since Thu 2026-01-15 06:41:07 EST; 7s ago
     Process: 5146 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
    Tasks: 29 (limit: 4553)
   Memory: 41.0M (peak: 48.0M)
      CPU: 4.195s
   CGroup: /system.slice/wazuh-agent.service
           └─5169 /var/ossec/bin/wazuh-execd
              5181 /var/ossec/bin/wazuh-agentd
              5193 /var/ossec/bin/wazuh-syscheckd
              5206 /var/ossec/bin/wazuh-logcollector
              5223 /var/ossec/bin/wazuh-modulesd

Jan 15 06:41:00 ubuntu2404 systemd[1]: Starting wazuh-agent.service - Wazuh agent...
Jan 15 06:41:00 ubuntu2404 env[5146]: Starting Wazuh v4.14.1...
Jan 15 06:41:01 ubuntu2404 env[5146]: Started wazuh-execd...
Jan 15 06:41:02 ubuntu2404 env[5146]: Started wazuh-agentd...
Jan 15 06:41:03 ubuntu2404 env[5146]: Started wazuh-syscheckd...
Jan 15 06:41:04 ubuntu2404 env[5146]: Started wazuh-logcollector...
Jan 15 06:41:05 ubuntu2404 env[5146]: Started wazuh-modulesd...
Jan 15 06:41:07 ubuntu2404 env[5146]: Completed.
Jan 15 06:41:07 ubuntu2404 systemd[1]: Started wazuh-agent.service - Wazuh agent.
ubuntu@ubuntu2404:~$

```

We have successfully set up our first Wazuh Agent.

Jan 15 06:41

Wazuh

localhost/app/endpoints-summary#/agents-preview

Endpoints

AGENTS BY STATUS

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

TOP 5 OS

- ubuntu (1)

TOP 5 GROUPS

- default (1)

Agents (1)

Deploy new agent Refresh Export formatted More

Search WQL

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	ubuntu	192.168.170.130	default	Ubuntu 24.04 LTS	node01	v4.14.1	active	

Rows per page: 10

< 1 >

You can preview the agent on the agent summary page.

File Integrity Monitoring

Configuration for Wazuh agent is stored in `/var/ossec/etc/ossec.conf` on Linux. FIM is enabled by default.

```
GNU nano 7.2 /var/ossec/etc/ossec.conf *
<!-- File integrity monitoring -->
<syscheck>
  <disabled>no</disabled>

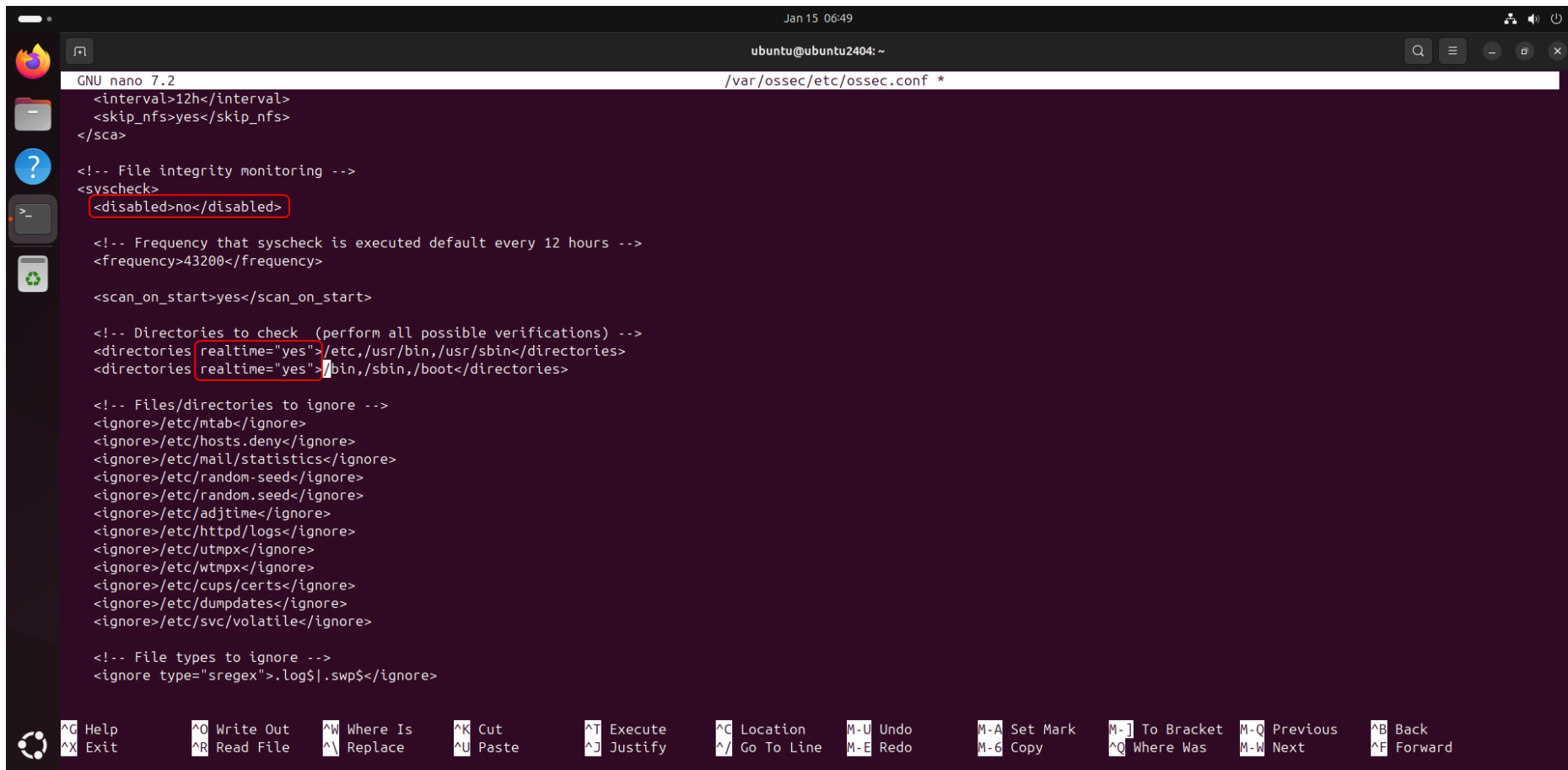
  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>43200</frequency>

  <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>

  <!-- 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>
  <ignore>/etc/adjtime</ignore>
  <ignore>/etc/httpd/logs</ignore>
  <ignore>/etc/utmpx</ignore>
  <ignore>/etc/wtmpx</ignore>
  <ignore>/etc/cups/certs</ignore>
  <ignore>/etc/dumpdates</ignore>
  <ignore>/etc/svc/volatile</ignore>
```

To enable realtime logs for important directories set the realtime property to yes.



```

GNU nano 7.2 /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>

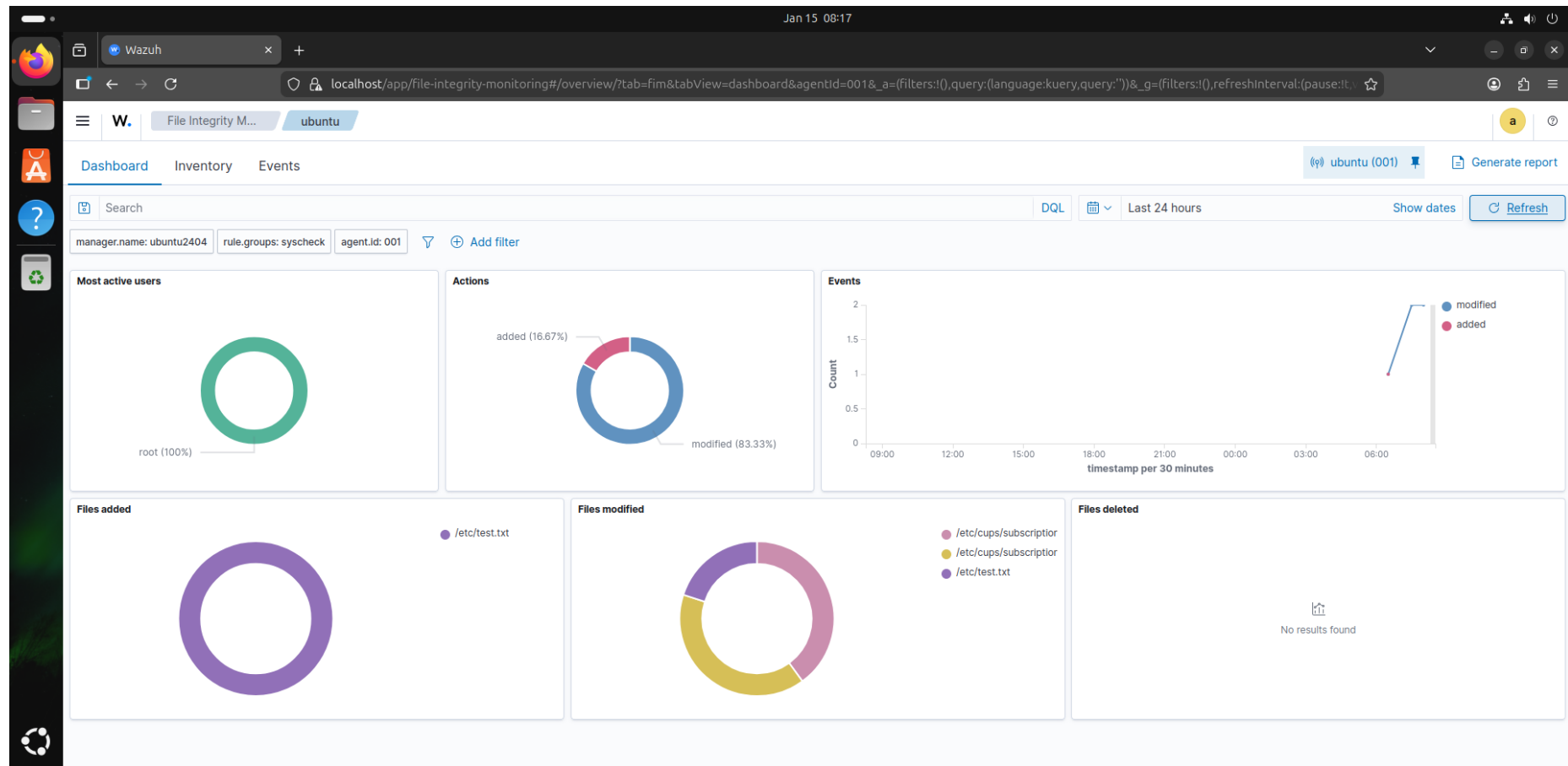
  <!-- Directories to check (perform all possible verifications) -->
  <directories> realtime="yes"</directories>
  <directories> realtime="yes"</directories>

  <!-- 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>
  <ignore>/etc/adjtime</ignore>
  <ignore>/etc/httpd/logs</ignore>
  <ignore>/etc/utmpx</ignore>
  <ignore>/etc/wtmpx</ignore>
  <ignore>/etc/cups/certs</ignore>
  <ignore>/etc/dumpdates</ignore>
  <ignore>/etc/svc/volatile</ignore>

  <!-- File types to ignore -->
  <ignore type="sregex">.log$|.swp$</ignore>
  
```

Then restart the Wazuh Agent with `sudo systemctl restart wazuh-agent`

To test the realtime logs, I created and edited test.txt in /etc.



And now realtime logs are enabled for important system directories.