Wazuh Installation & FIM Monitoring

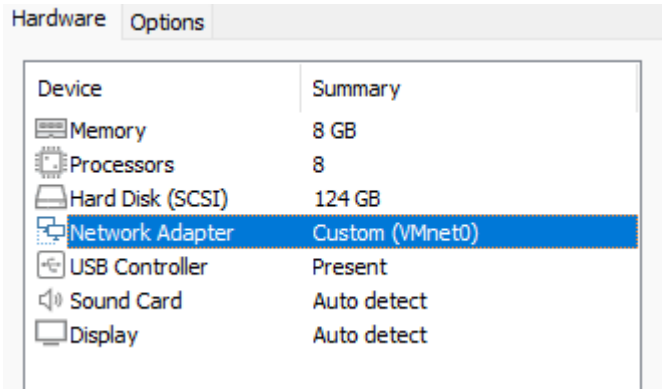
Talal Ahmed | Team Lambda

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.

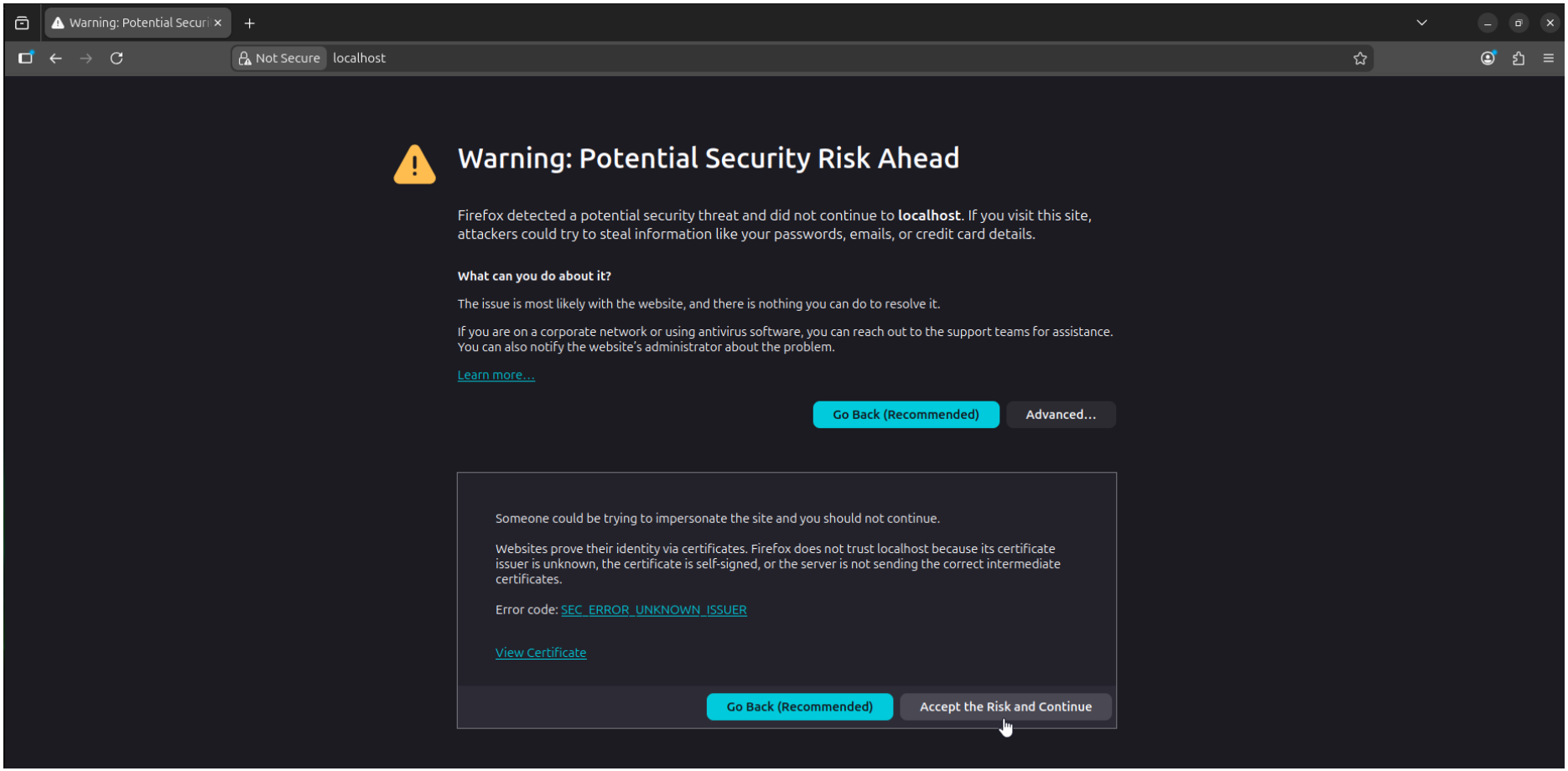
```
$ curl -sO https://packages.wazuh.com/4.14/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

```
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.
```

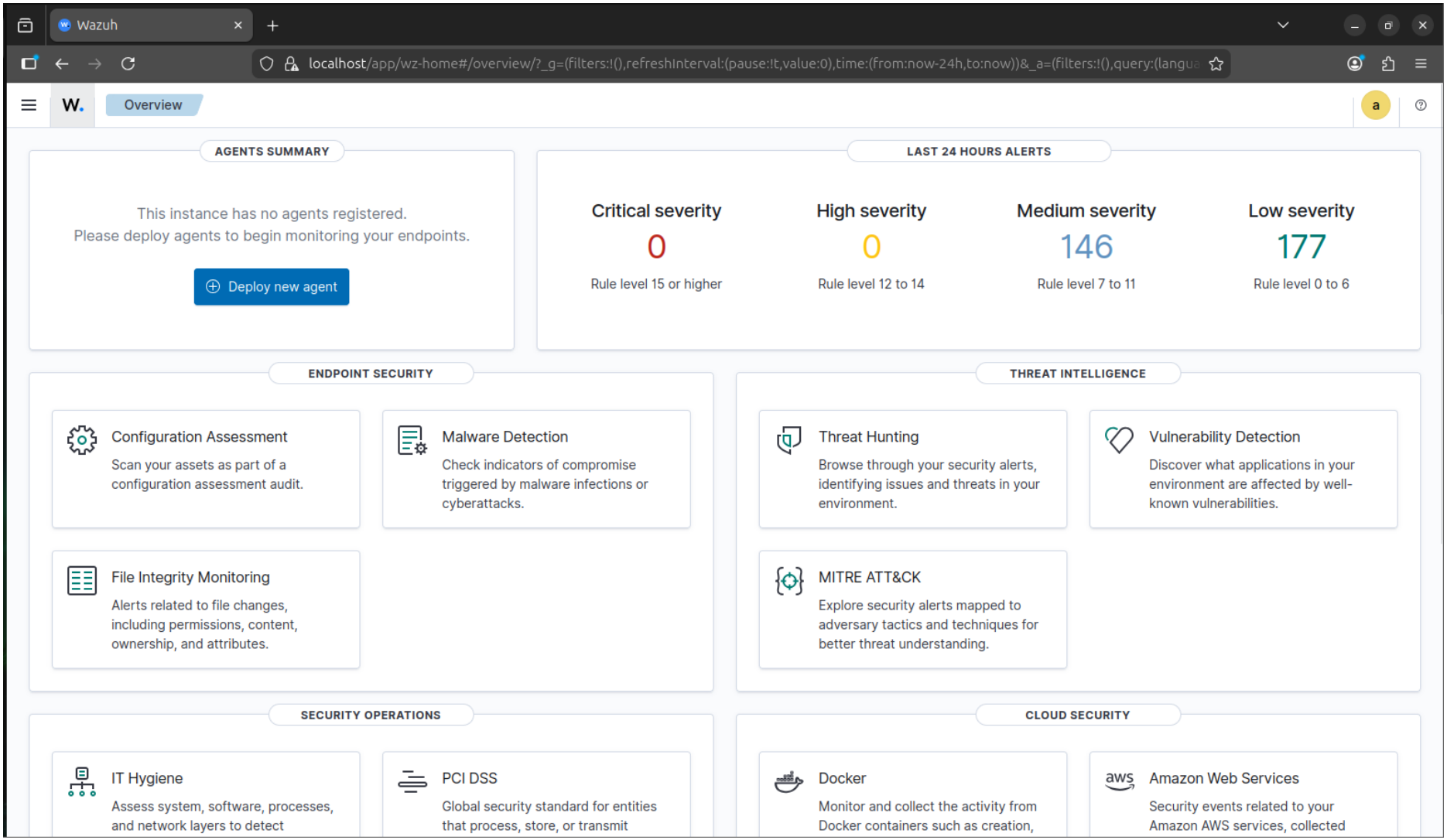
The installation takes some time and at the end it outputs the default username and password.

```
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.

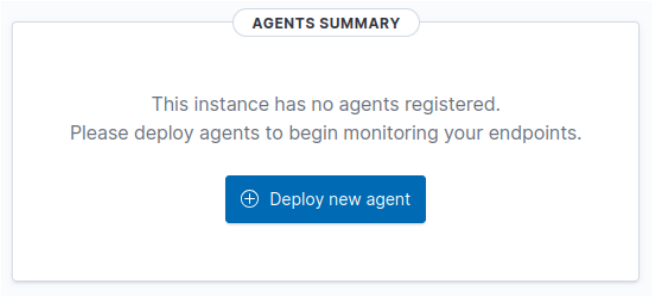


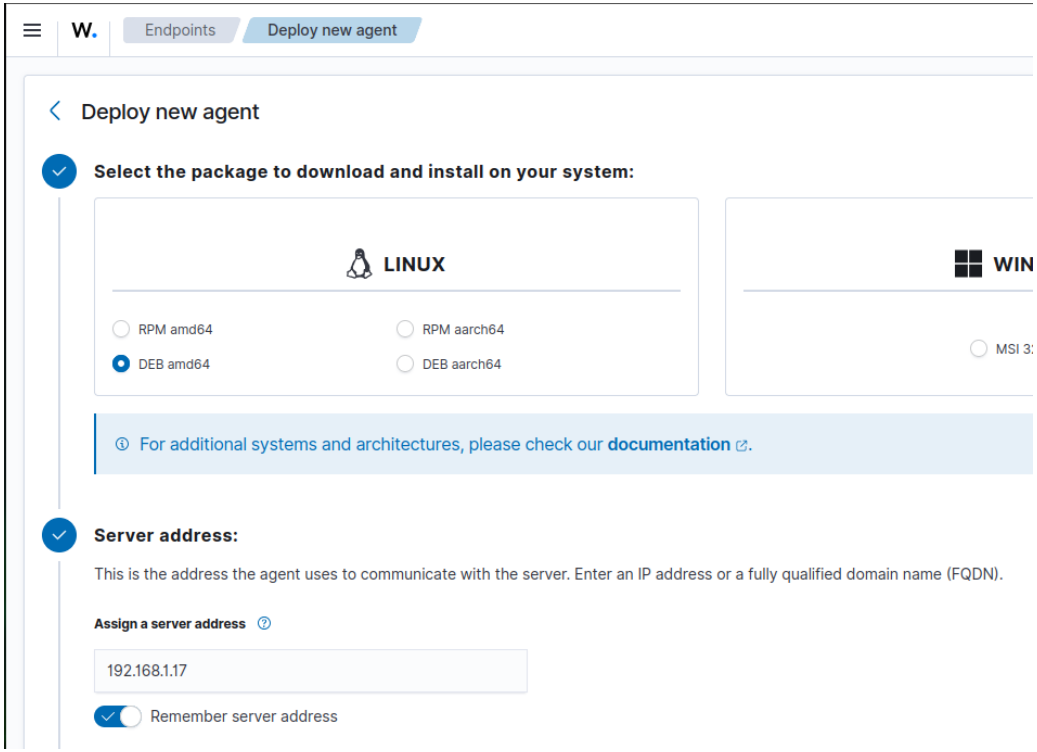
And just like that we have successfully installed Wazuh.

Install Wazuh Agent

I will use Ubuntu again for Wazuh agent. To install the Wazuh Agent on a machine, click “Deploy new agent” from Wazuh dashboard.

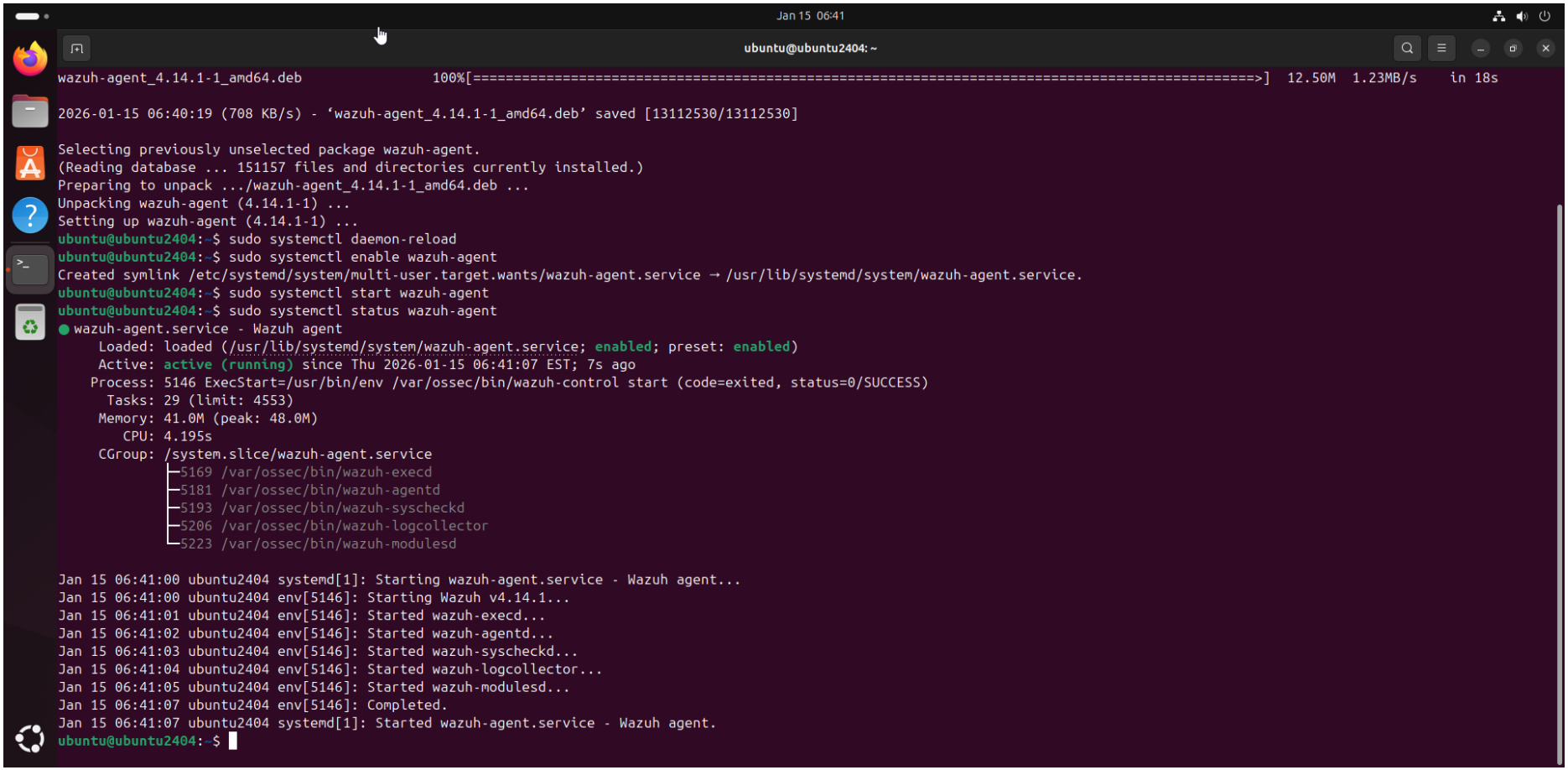
Then select the correct operating system. Input the IP of Wazuh Manager, then copy the command it generates.



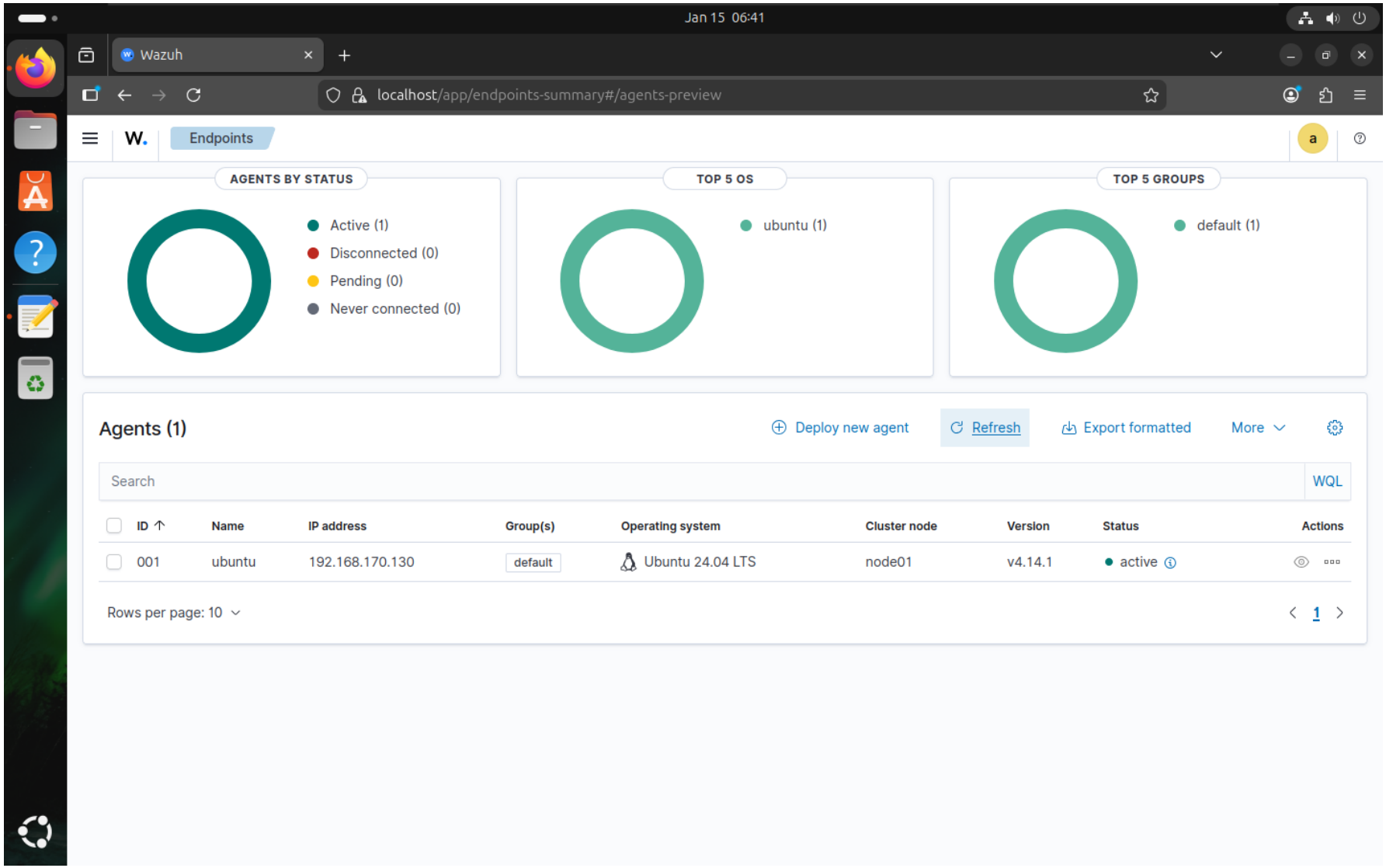


5 Start the agent:

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



We have successfully set up our first Wazuh Agent.



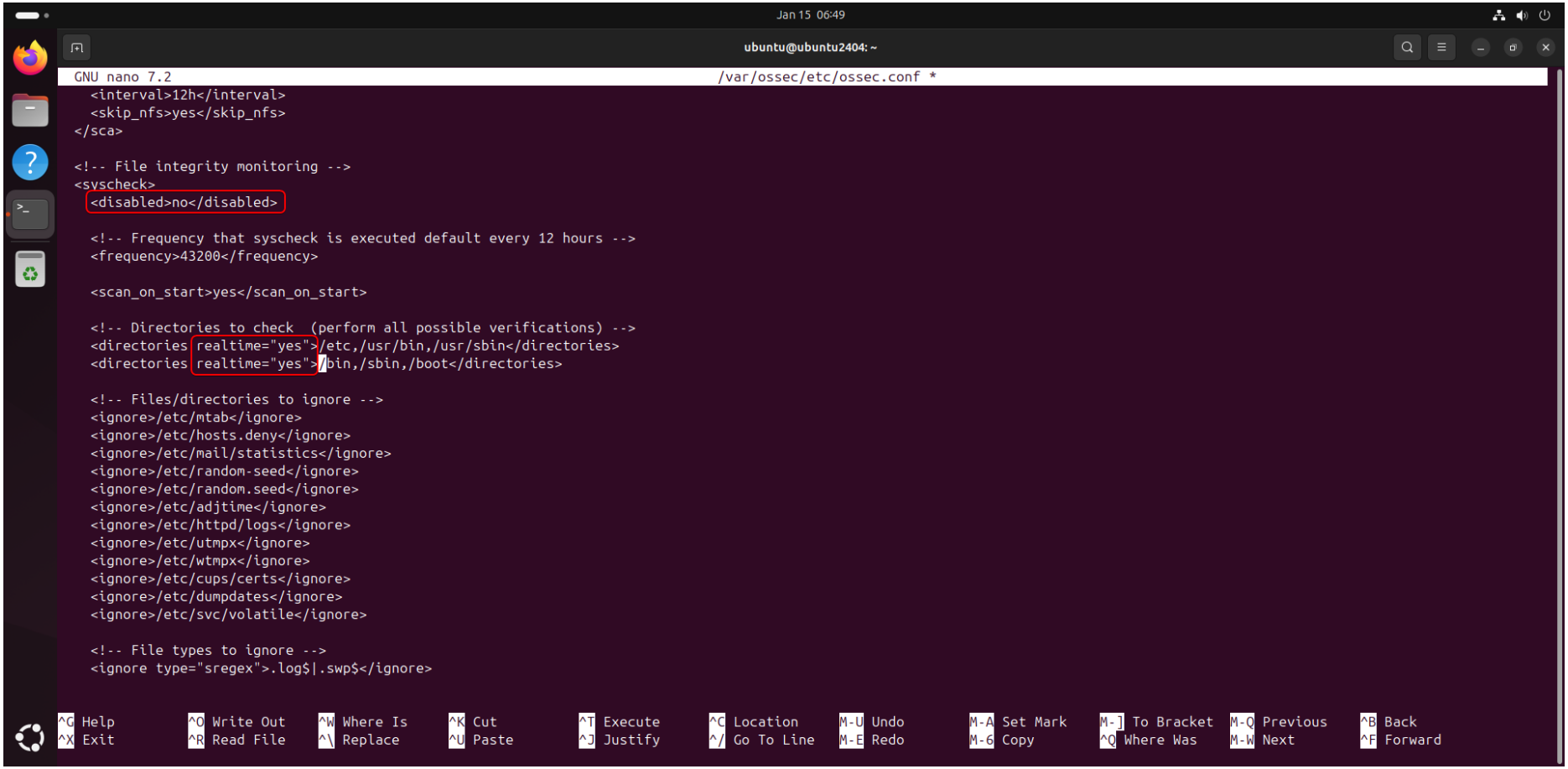
You can preview the agent on the agent summary page.

File Integrity Monitoring

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

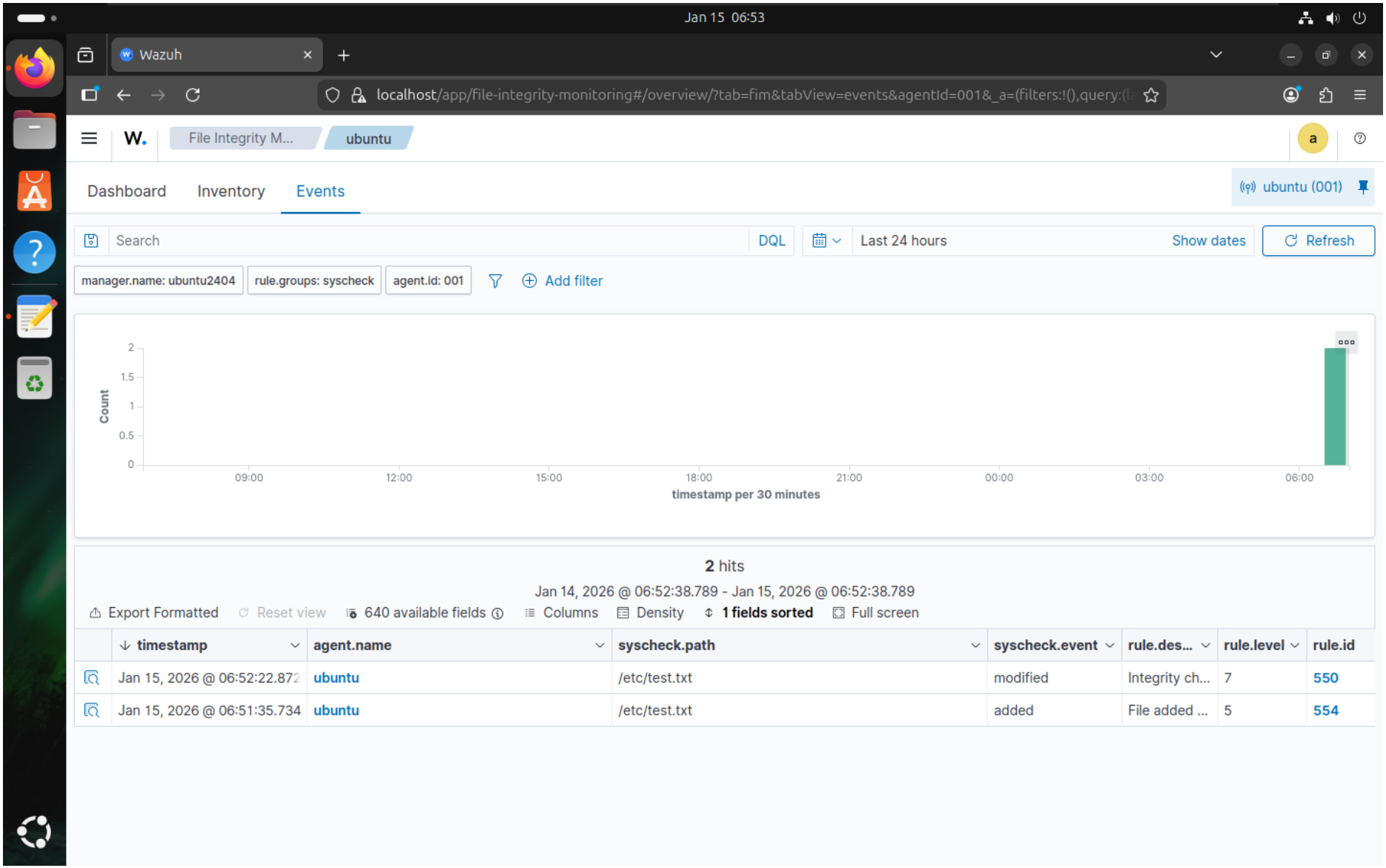
```
GNU nano 7.2                                        /var/ossec/etc/ossec.conf *
<!-- File integrity monitoring -->
<syscheck>
  <disabled>no</disabled>

  <!-- 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>
```

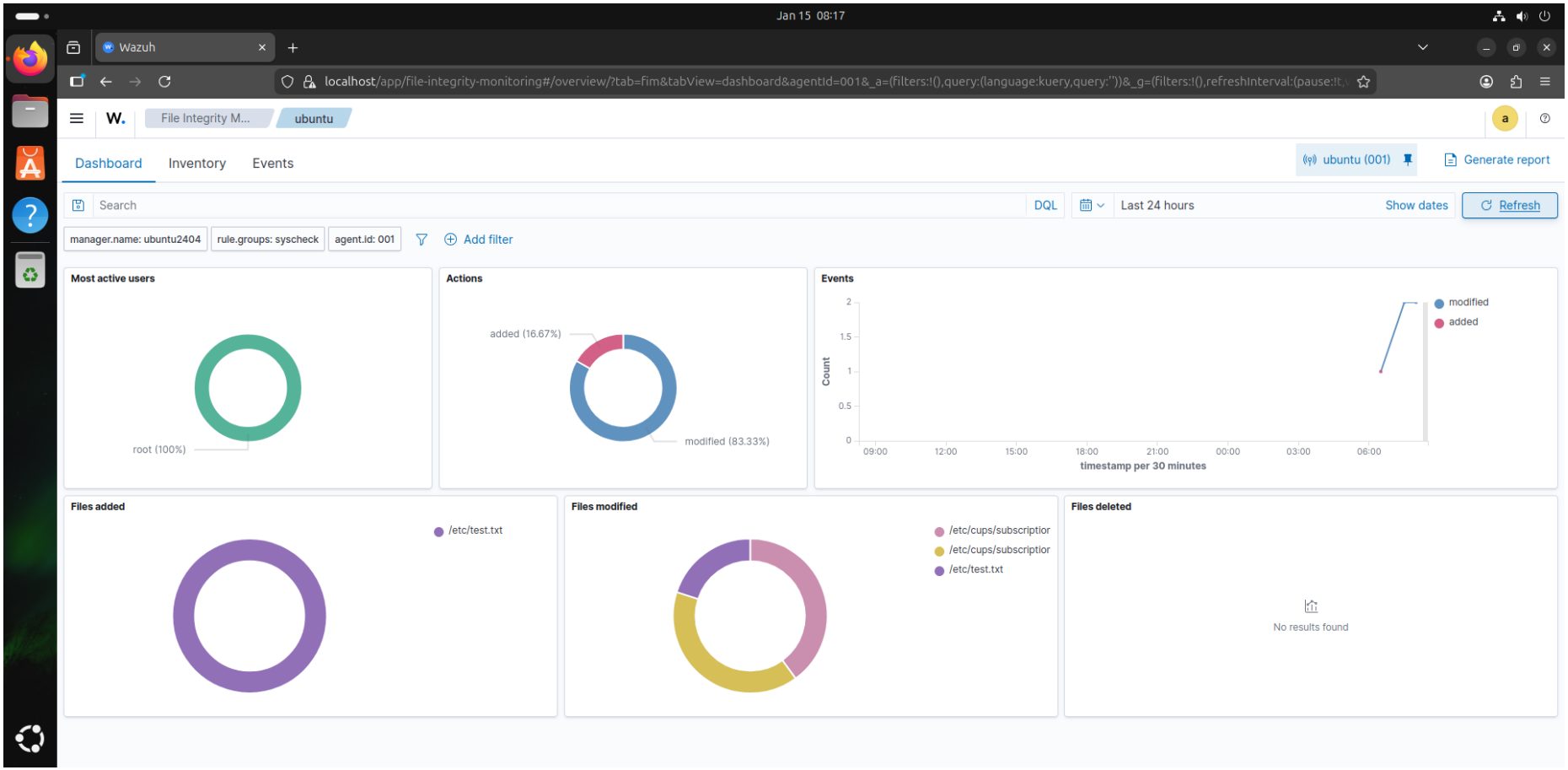
To enable realtime logs for important directories set the realtime property to yes.



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

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


Jan 15 06:53
Wazuh
localhost/app/file-integrity-monitoring#/overview/?tab=fim&tabView=events&agentId=001&_a=(filters:!(),query:(l
File Integrity M...
ubuntu
a
Dashboard
Inventory
Events
ubuntu (001)
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: ubuntu2404
rule.groups: syscheck
agent.id: 001
Add filter
Count
2
1.5
1
0.5
0
09:00
12:00
15:00
18:00
21:00
00:00
03:00
06:00
timestamp per 30 minutes
2 hits
Jan 14, 2026 @ 06:52:38.789 - Jan 15, 2026 @ 06:52:38.789
Export Formatted
Reset view
640 available fields
Columns
Density
1 fields sorted
Full screen
timestamp
agent.name
syscheck.path
syscheck.event
rule.des...
rule.level
rule.id
Jan 15, 2026 @ 06:52:22.872
ubuntu
/etc/test.txt
modified
Integrity ch...
7
550
Jan 15, 2026 @ 06:51:35.734
ubuntu
/etc/test.txt
added
File added ...
5
554



And now realtime logs are enabled for important system directories.