Agents configuration report

SAMEER HASSAN

Wazuh lab

Github-link: GitHub - sameerhassancode/Wazuh-labs

Linkedin: https://www.linkedin.com/in/sameer-hassan-15a428255/

What is Wazuh?

Wazuh is a free and open-source security platform used for threat detection, compliance monitoring, and incident response. It helps organizations monitor their infrastructure in real-time by collecting and analyzing data from endpoints (like servers, desktops, or cloud instances). Wazuh works as a **SIEM (Security Information and Event Management)** and **XDR (Extended Detection and Response)** solution.

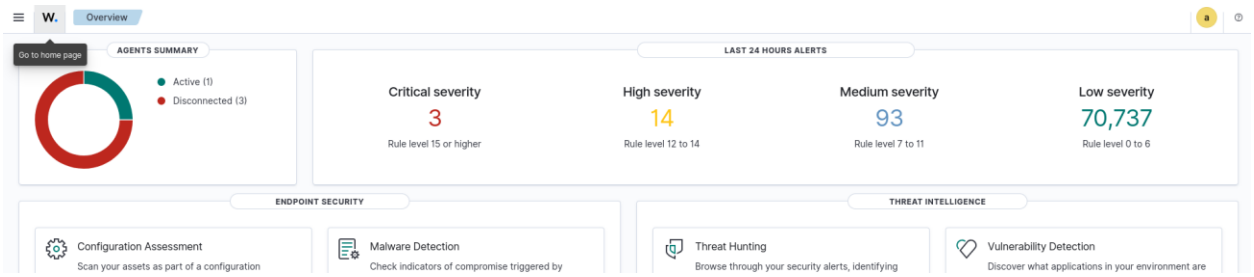
What is the Wazuh Agent?

The **Wazuh Agent** is a lightweight piece of software installed on endpoints (such as Linux, Windows, or macOS machines). Its primary job is to:

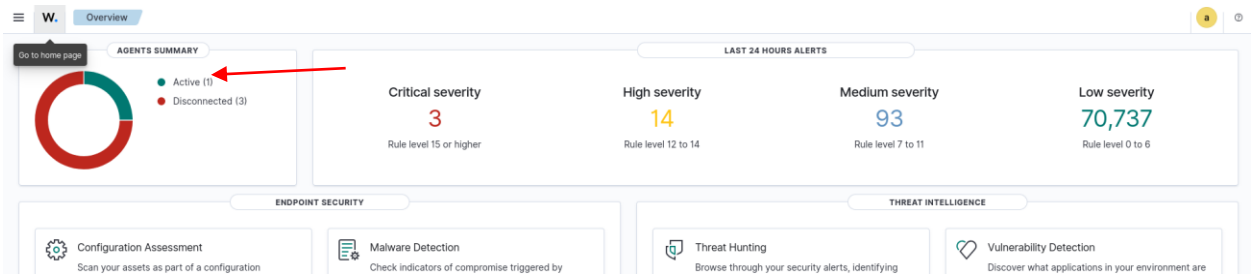
- **Collect system data** (logs, events, file changes, etc.)
- **Send that data** securely to the Wazuh Manager
- **Enforce active response rules** (like blocking malicious IPs or restarting services)

Each endpoint you want to monitor needs to have the Wazuh agent installed and configured.

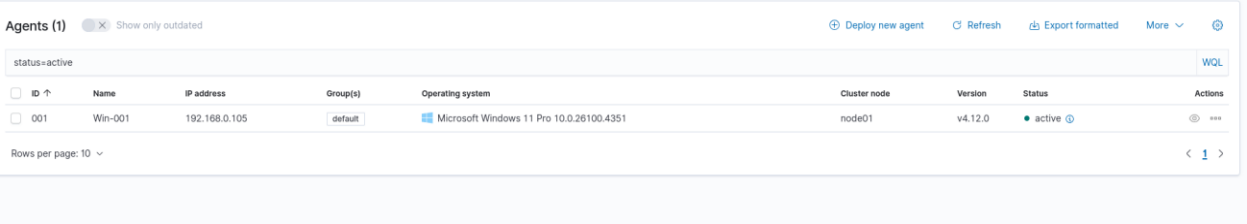
Wazuh-Dashboard:



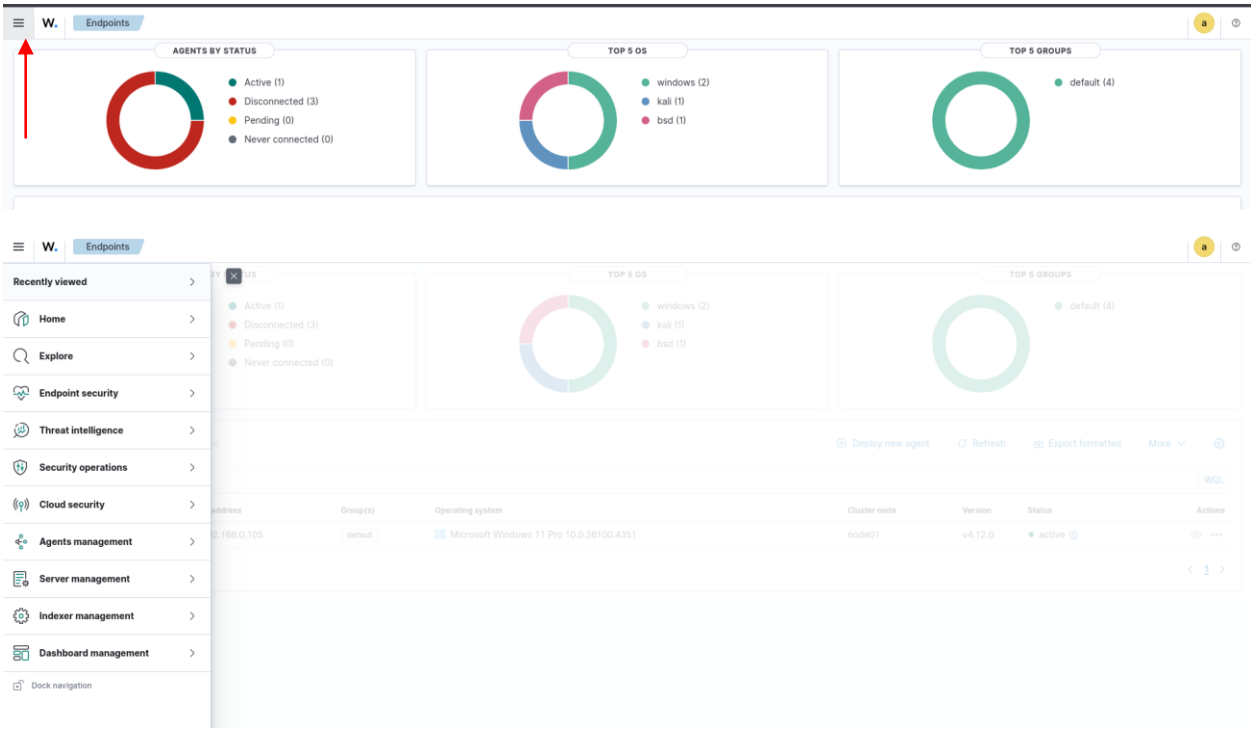
Click on active



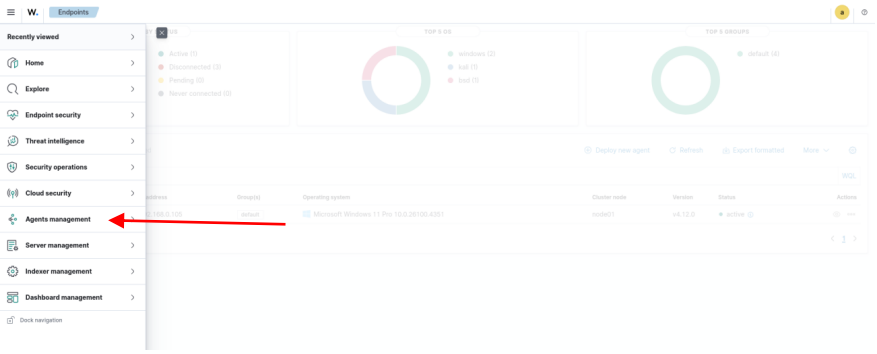
It’s showing 1 active agent.



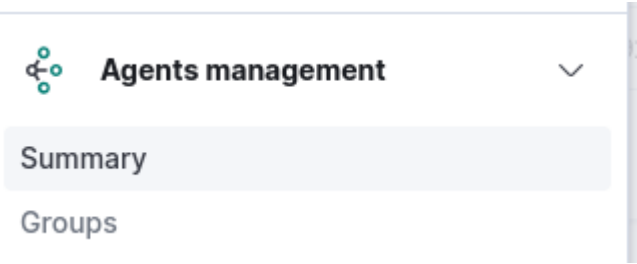
Now click on hamburger icon on the top left



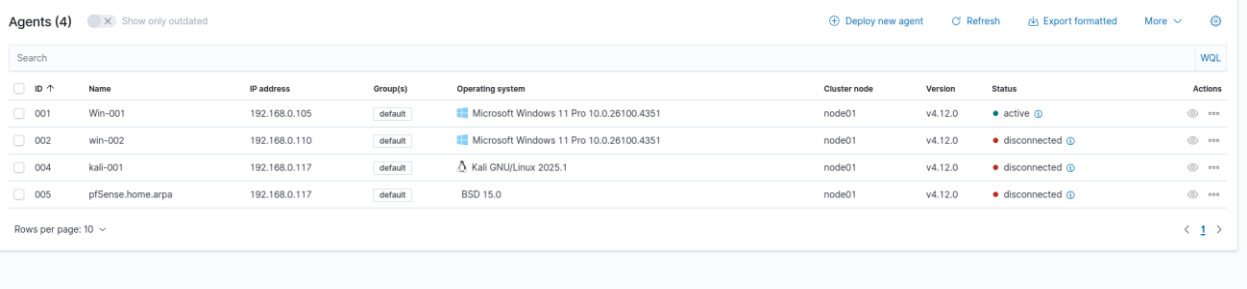
Now click on agents managements:



After clicking it will show two sub types:

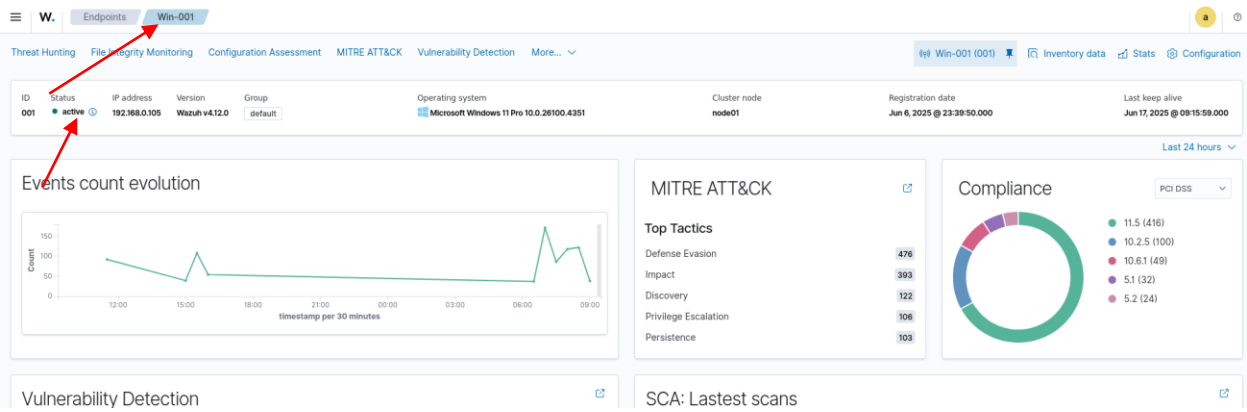


Click on Summary and it will redirect to page showing all agents:

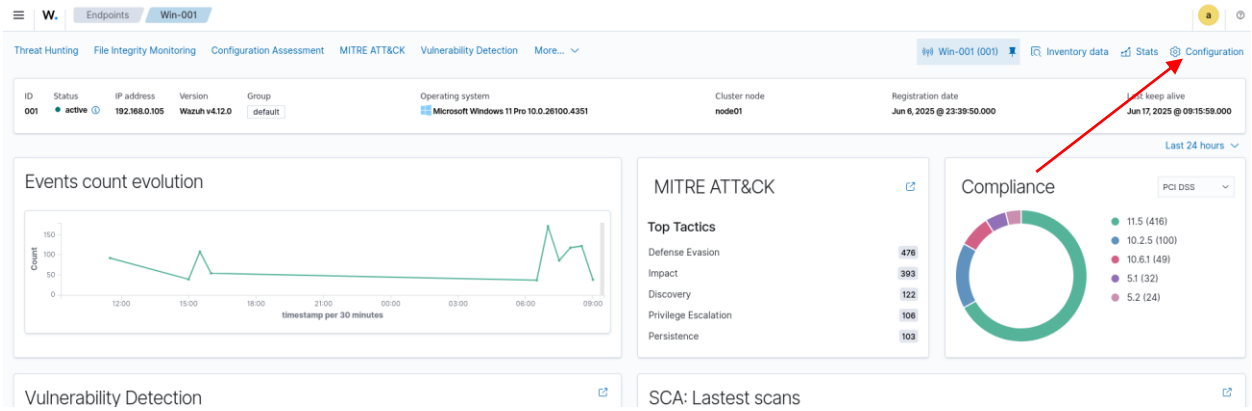


Click on any agent you want to generate report I am selecting active agent:

After selecting agent it will show you this page



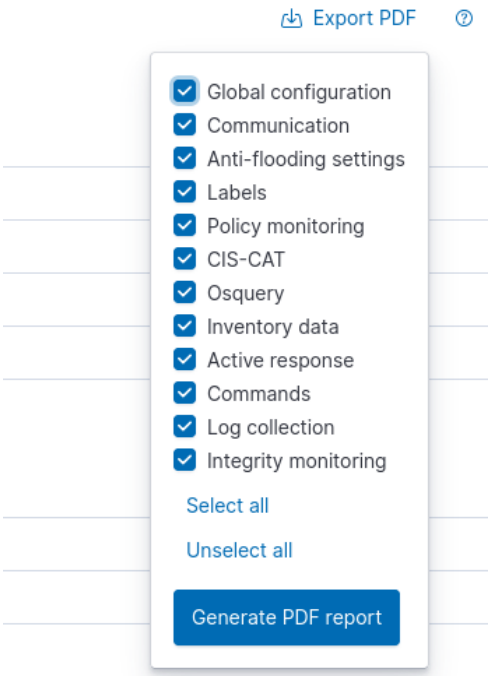
Now click on configuration icon:



Now it you can see the option to generate the report:

Click export PDF:

Check the options and generate pdf report



Report is successfully generated:

wazuh.

info@wazuh.com
https://wazuh.com

Agent 001 configuration

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	Win-001	192.168.0.105	Wazuh v4.12.0	wazuh-server	Microsoft Windows 11 Pro 10.0.26100.4351	Jun 7, 2025 @ 03:39:50.000	Jun 17, 2025 @ 13:20:07.000

Group: default

Main configurations

Global configuration

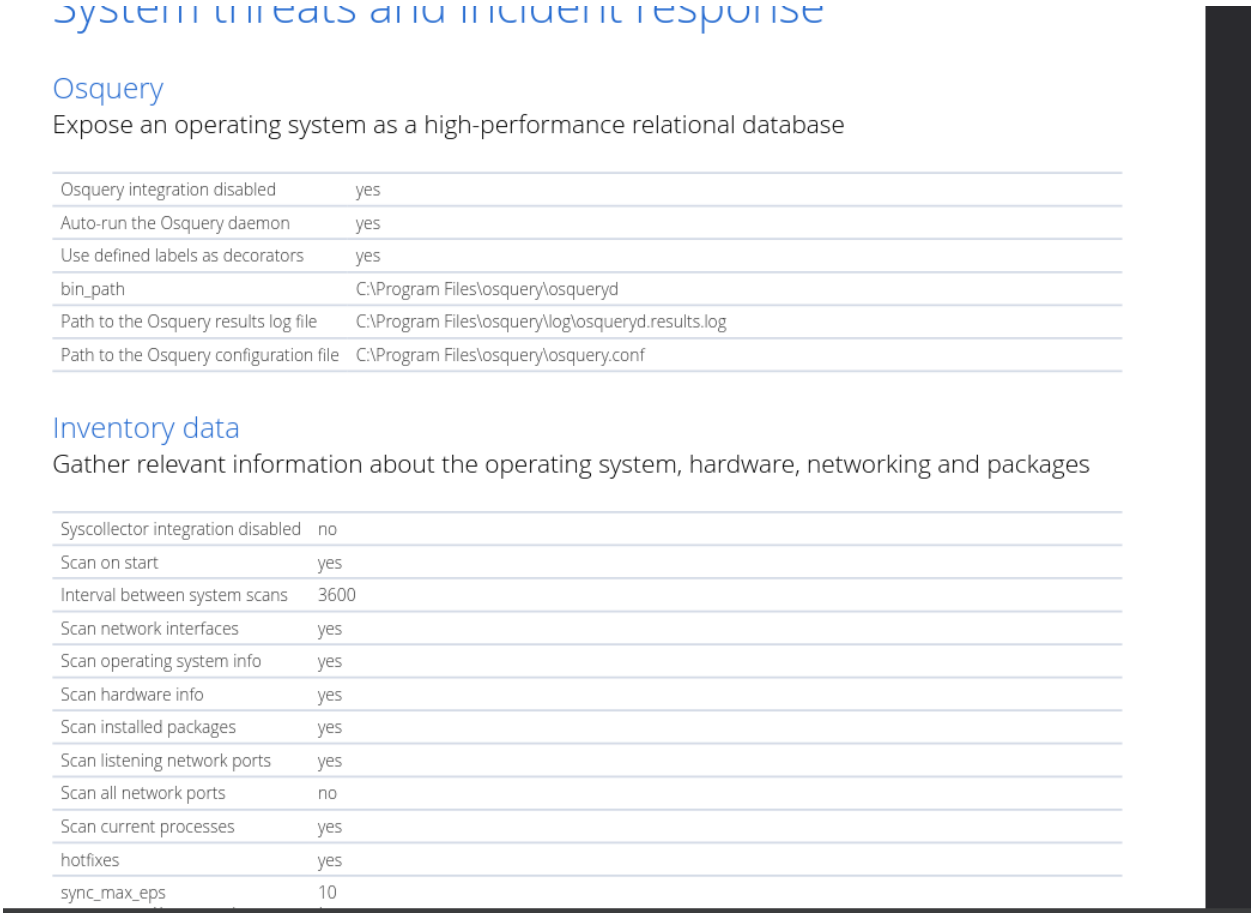
Logging settings that apply to the agent

Write internal logs in plain text	yes
Write internal logs in JSON format	no

Communication

Settings related to the connection with the manager

Showing all the configuration details



Summary:

Viewing or generating a Wazuh agent configuration report provides critical visibility into the security posture of an endpoint. It ensures the agent is properly connected to the Wazuh manager, verifies that essential modules like file integrity monitoring, vulnerability detection, and system inventory are enabled, and confirms that the setup complies with organizational or regulatory standards. This information is valuable for auditing, documentation, and troubleshooting, allowing security teams to quickly identify misconfigurations, coverage gaps, or disabled features. Overall, it strengthens endpoint monitoring and supports proactive threat detection and response.

Other SIEM

1. IBM Qradar

2. Splunk

3. Azure Sentinel