CICSA PROJECT

REPORT ON INSTALLATION OF



SUBMITTED TO: Rinto M Prince (Trainer)

SUBMITTED ON: 09-02-2024

BATCH: 9.30 – 11.30

Submitted By,

1. Arifa M A

**CONTENTS**

*Introduction…………………………………………………………….3*

*Why wazuh …………………………………………………………4*

*Requirements ……………..……………………………………………5*

*Download and installation of wazuh ………………………………...7*

*Installing wazuh agent on windows …………………………………11*

*Log Analysis…………………………………………………………14*

*Conclusion………………………………………………….……….16*

**INTRODUCTION**

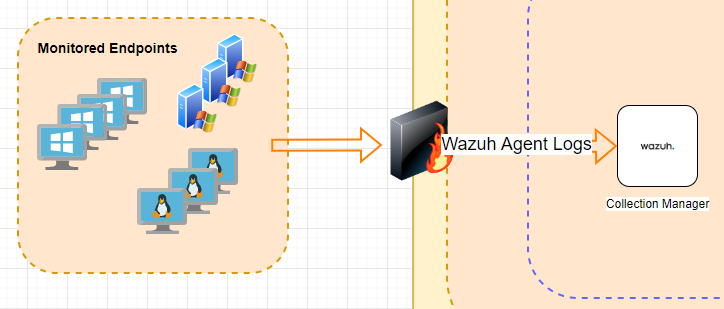
Endpoint Detection and Response (EDR) is an integrated, layered approach to endpoint protection that combines real-time continuous monitoring and endpoint data analytics with rule-based automated response. We need an EDR that will record the activities and events taking place on endpoints and all workloads, providing us with the visibility to uncover incidents that would otherwise remain invisible. An EDR solution needs to provide continuous and comprehensive visibility into what is happening on endpoints in real time.

EDRs are usually made up of two key pieces:

* Endpoint Agent — Collects logs from Endpoints
* Collection Manager — Receives logs from endpoints and analyses for malicious activity

Rather than having to log onto every endpoint to view security events like a noob, we now have a central collector that allows us to manage and scale out our endpoints.

**WHY Wazuh?**



Basic Data Flow

Wazuh is the best open source EDR currently available (in my opinion). Wazuh provides a platform that allows us monitor our endpoints, integrate with 3rd party applications, meet compliance standards, provide multi-tenant support, and more! Wazuh supports the most common operating systems and provides the below features right out of the box!

* Log Data Analysis
* File Integrity Monitoring
* Vulnerability Detection
* CIS Benchmark Assessment
* Regulatory Compliance
* Container Security

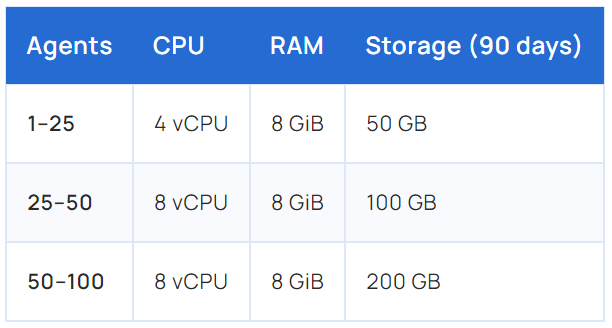
In Brief, Wazuh is a security platform that integrates and manages diverse endpoints is critical for contemporary security operations. As businesses move towards cloud infrastructure, containerized applications, and a broader set of workstation options for employees, XDR solutions are becoming a staple. Wazuh offers an open-source alternative to existing XDR and SIEM solutions. It incorporates and extends multiple free and open-source components to make a cohesive and proven platform. Wazuh also allows us to create our own detection rules, integrations, and configurations to fit any use case.

**REQUIREMENTS**

* **Hardware requirements:**

Highly depend on the number of protected endpoints and cloud workloads. This number can help estimate how much data will be analyzed and how many security alerts will be stored and indexed.

Following this quick start implies deploying the Wazuh server, the Wazuh indexer, and the Wazuh dashboard on the same host. This is usually enough for monitoring up to 100 endpoints and for 90 days of queryable/indexed alert data. The table below shows the recommended hardware for a quick start deployment.



* **BROWSER COMPATIBILITY**

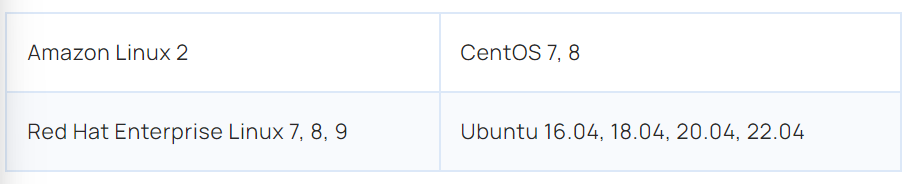
Wazuh dashboard supports the following web browsers:

* Chrome 95 or later
* Firefox 93 or later
* Safari 13.7 or later

Other Chromium-based browsers might also work. Internet Explorer 11 is not supported.

### OPERATING SYSTEM

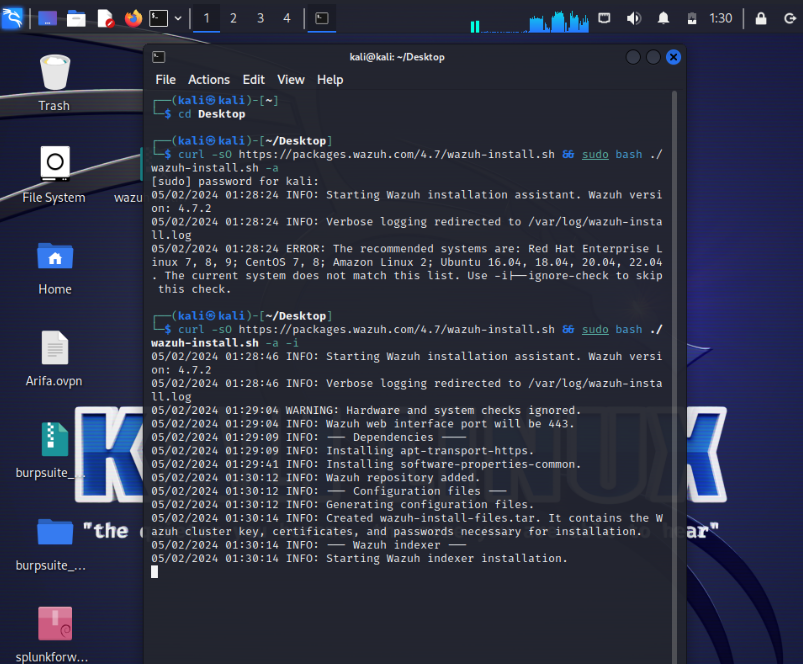
Wazuh central components can be installed on a 64-bit Linux operating system. Wazuh recommends any of the following operating system versions:



**DOWNLOAD AND INSTALLATION OF WAZUH**

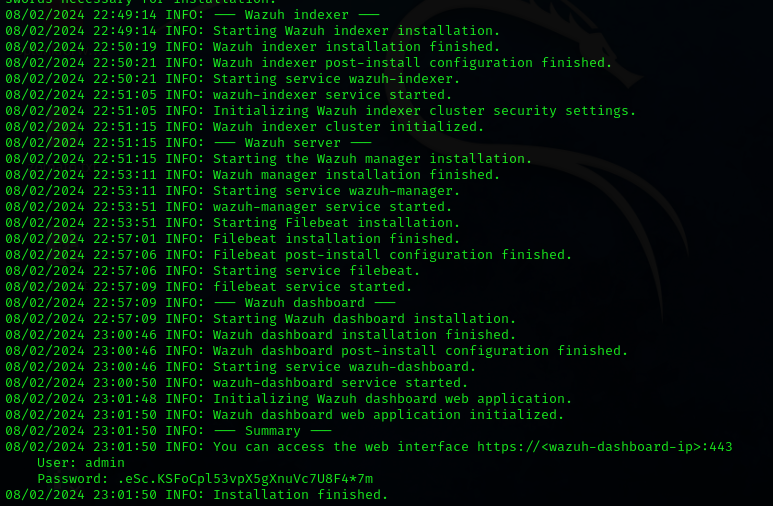
* WAZUH was downloaded from <https://wazuh.com/install/>
* Setup command to start the installation

*curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh-install.sh -a*

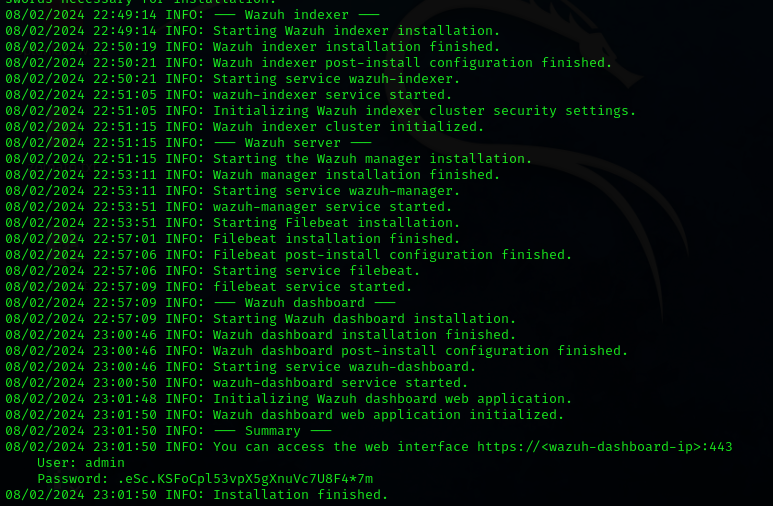


We found an error which says the system doesn’t match the configuration.

So adding -i (ignore) to the above used command to skip the configuration check.



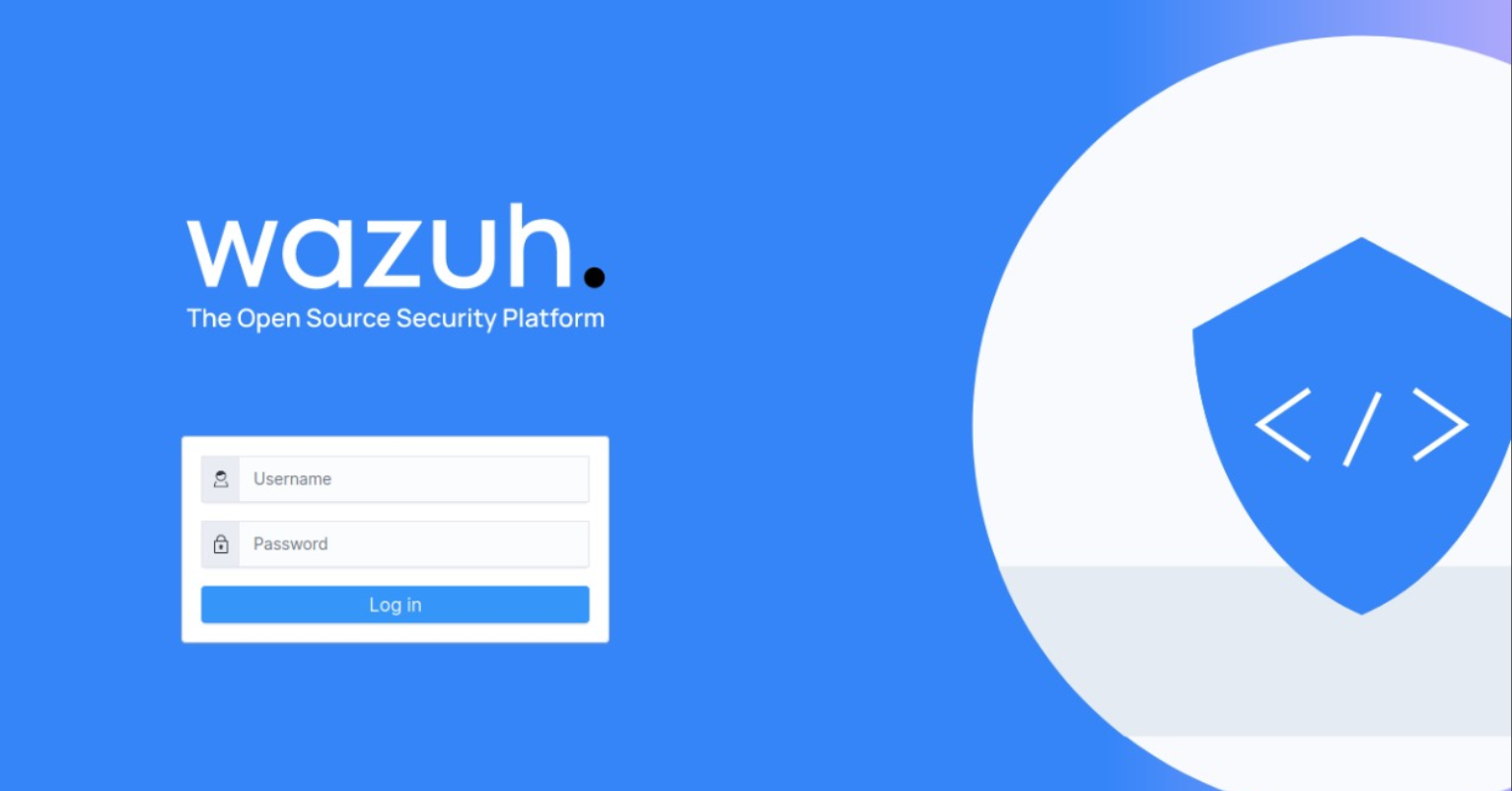
Upon completion of the installation process, the output will display the access credentials along with a confirmation message indicating the successful installation.



* To get the passwords for all Wazuh indexers, find the "wazuh-passwords.txt" file inside the "wazuh-install-files.tar".Then, use this command :

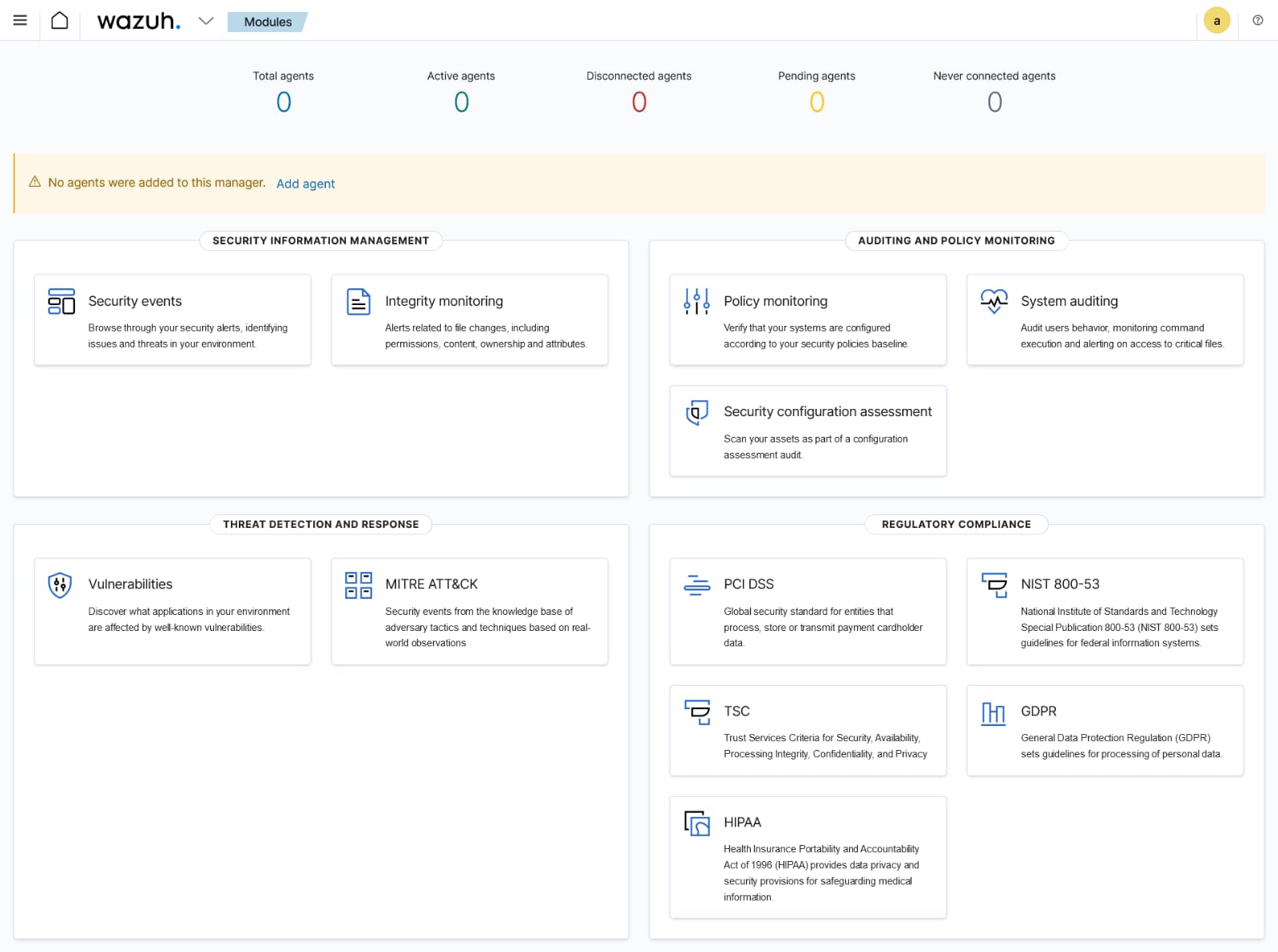
***sudo tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt***

We get the wazuh dashboard by requesting the IP of the host in the browser .Wazuh dashboard is a flexible and intuitive web interface for mining and visualizing security events and archives.



We can access wazuh by using the credentials that we obtained while successful installation.

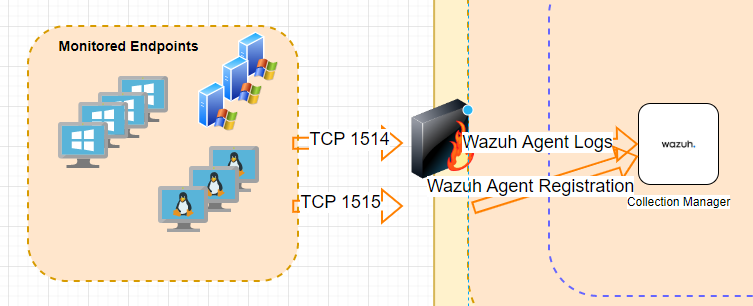
The Wazuh WUI provides a powerful user interface for data visualization and analysis. This interface can also be used to manage Wazuh configuration and to monitor its status.



With our Wazuh Manager now installed, we need to deploy our Wazuh Agents.

1. Wazuh Agent collects endpoint logs and sends to Manager.
2. Manager compares received logs against its rulesets. If there is a match, the log is written to

 /var/ossec/logs/alerts/alerts.json



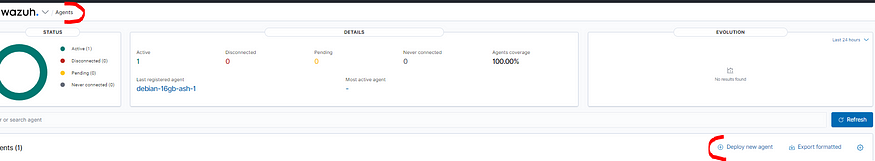
Agent to Manager Communication Flow

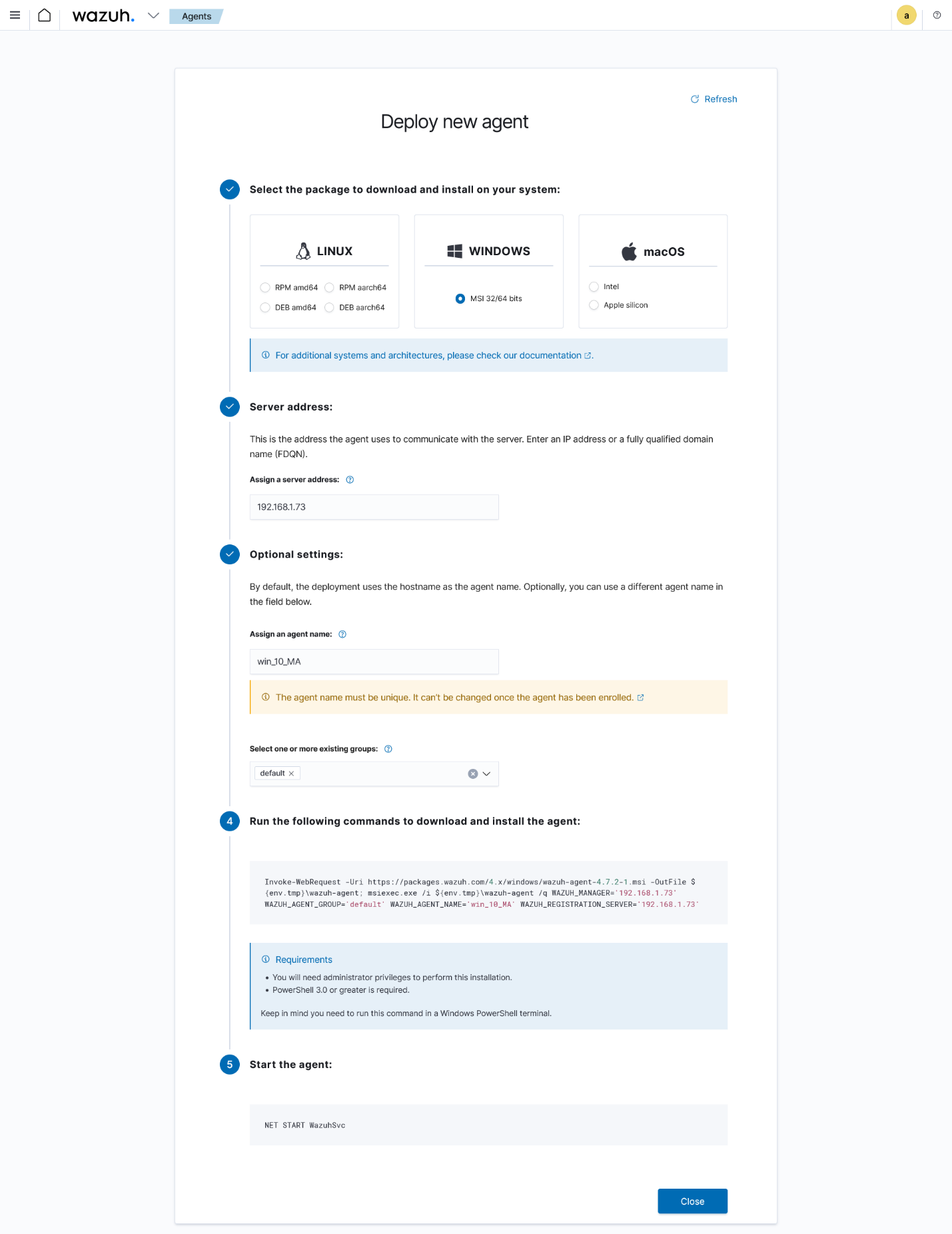
**INSTALLING WAZUH AGENT ON WINDOWS**

To install the Wazuh agent, initially select the operating system. Here we are going to install the agent in windows.

we can deploy a new agent from the Wazuh dashboard.

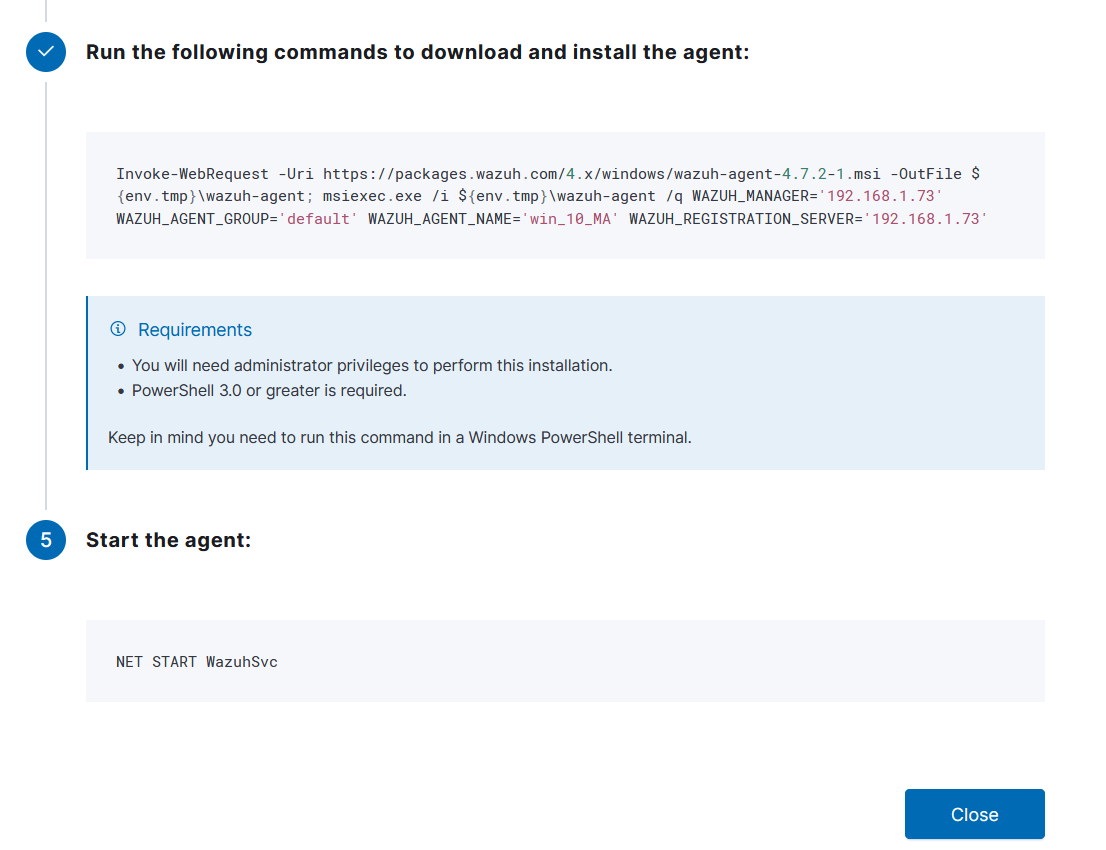
Wazuh has put together a cool tool for us to use through the Wazuh Web APP to build our single line install command. This will install the agent onto our endpoint and point to to use our manager.





Single Line Command

For a Windows install, let’s open up PowerShell and run our single line install using command:

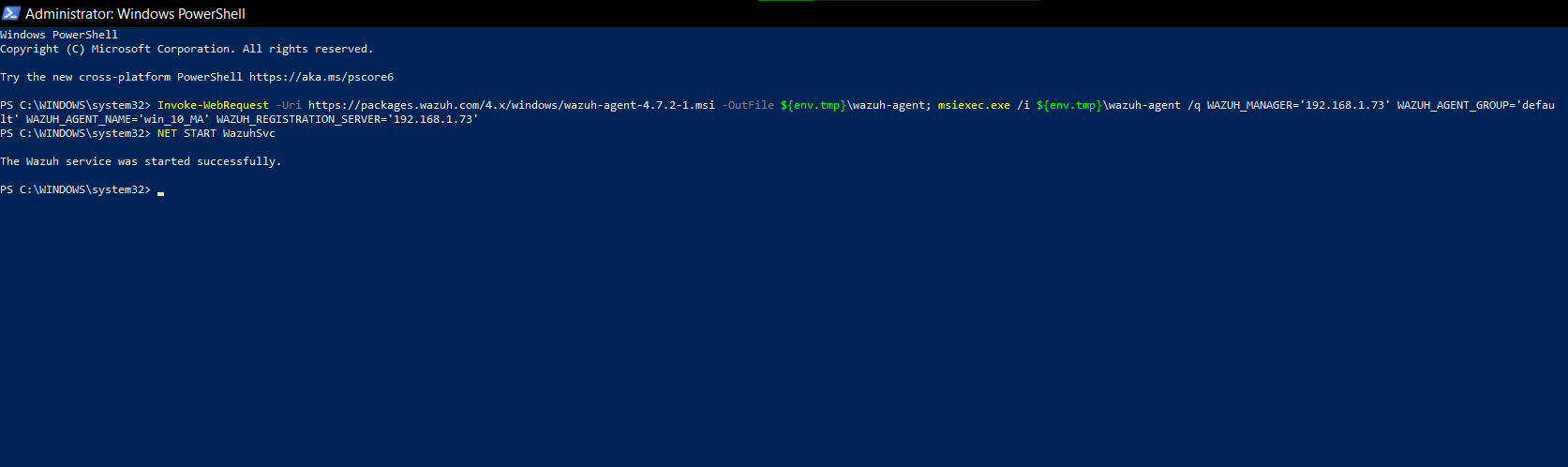


Windows Install Command

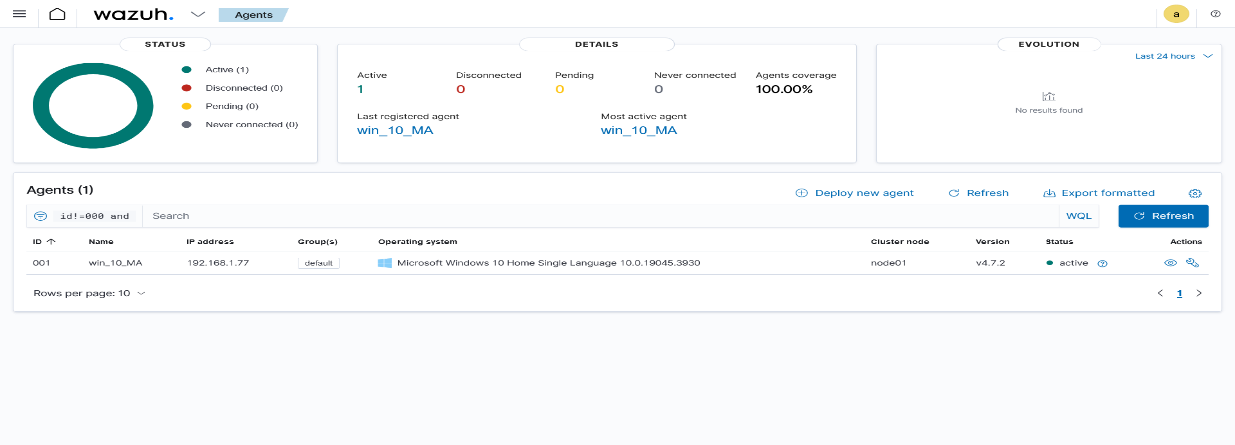
The installation process is now complete, and the Wazuh agent is successfully installed and configured. You can start the Wazuh agent from the GUI or by running:

*NET START Wazuh*

Once started, the Wazuh agent will start the enrollment process and register with the manager

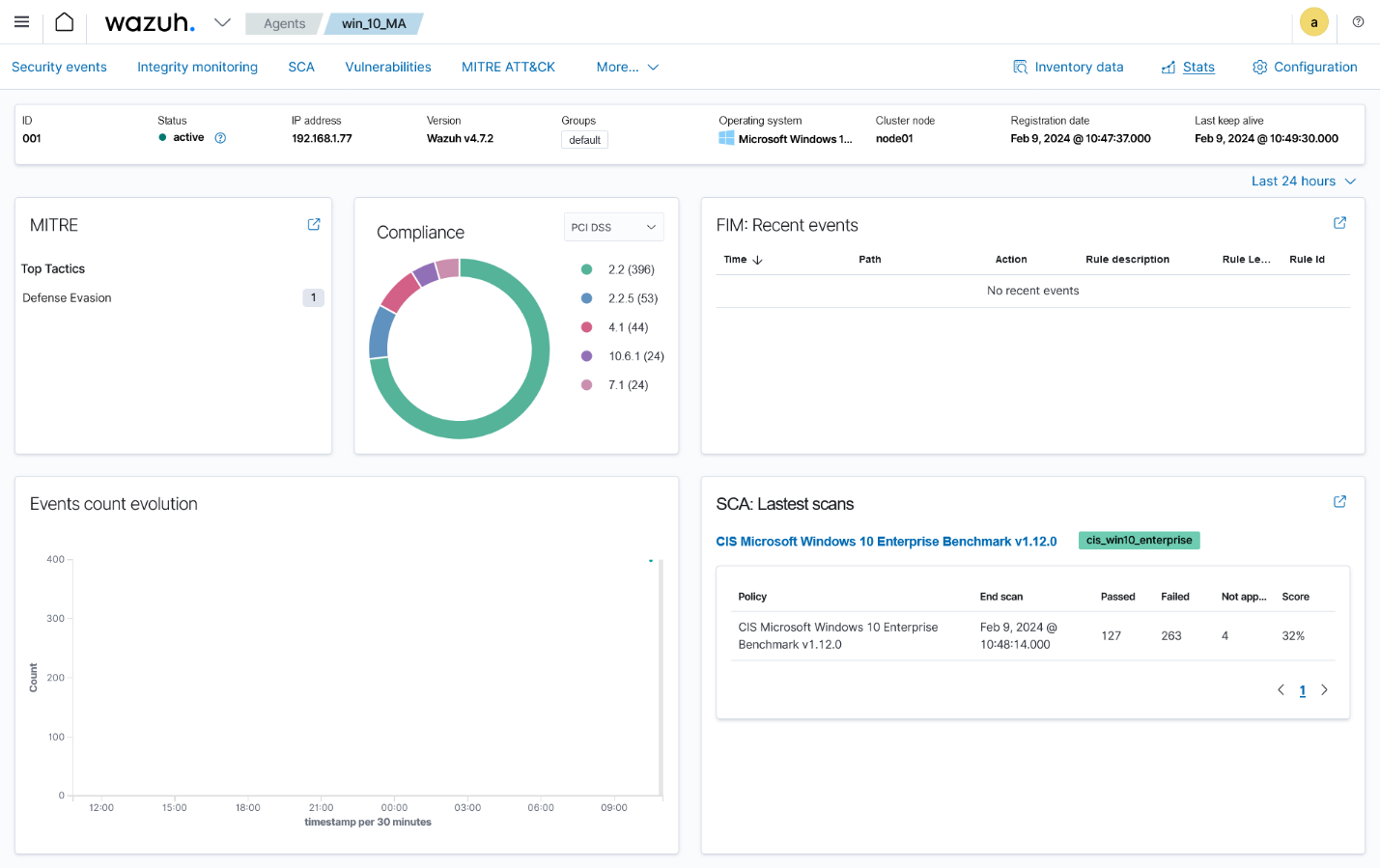


Now Our Dashboard is ready with an added agent and we can see the logs of or windows machine.

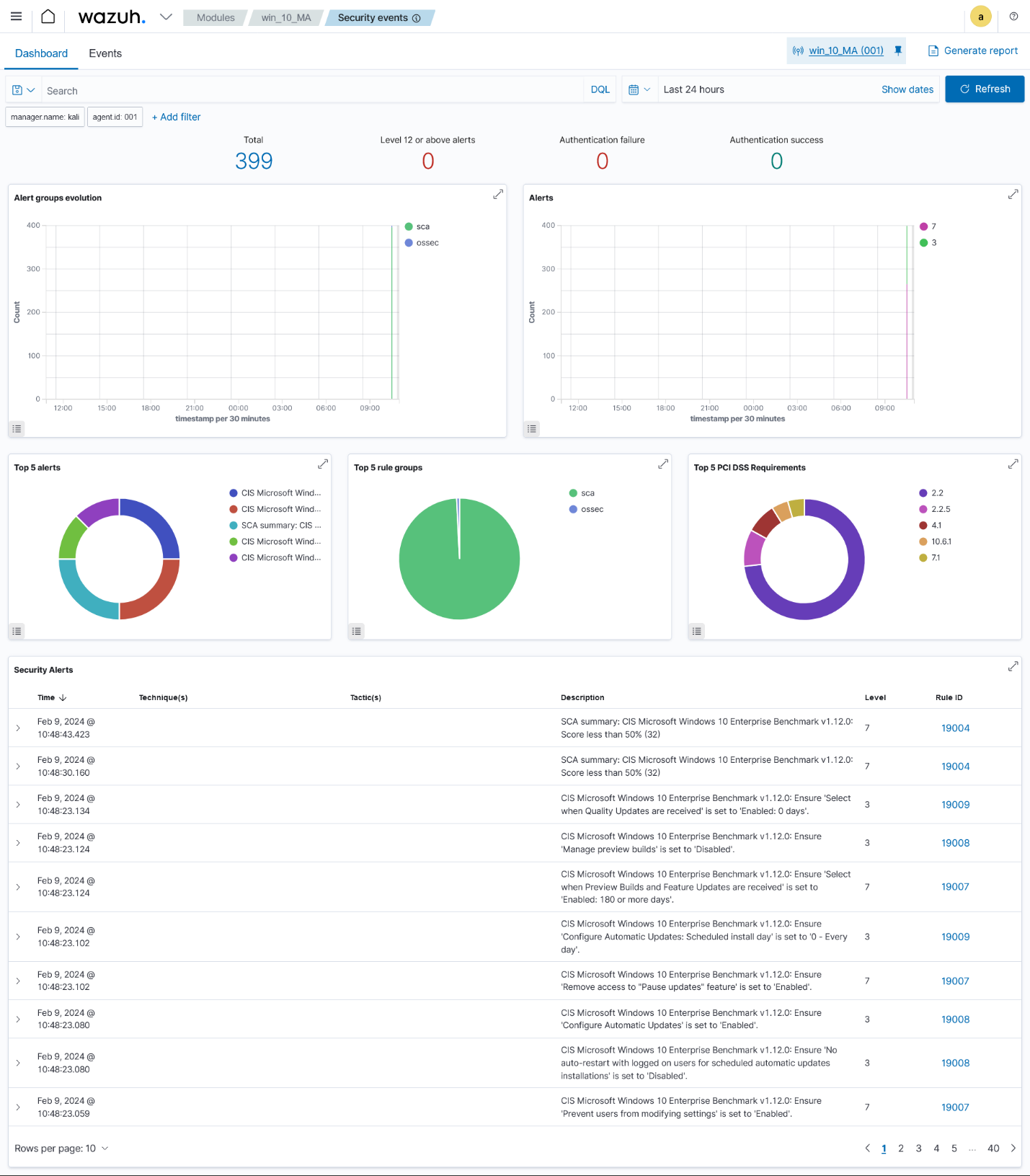


**LOG ANALYSIS**

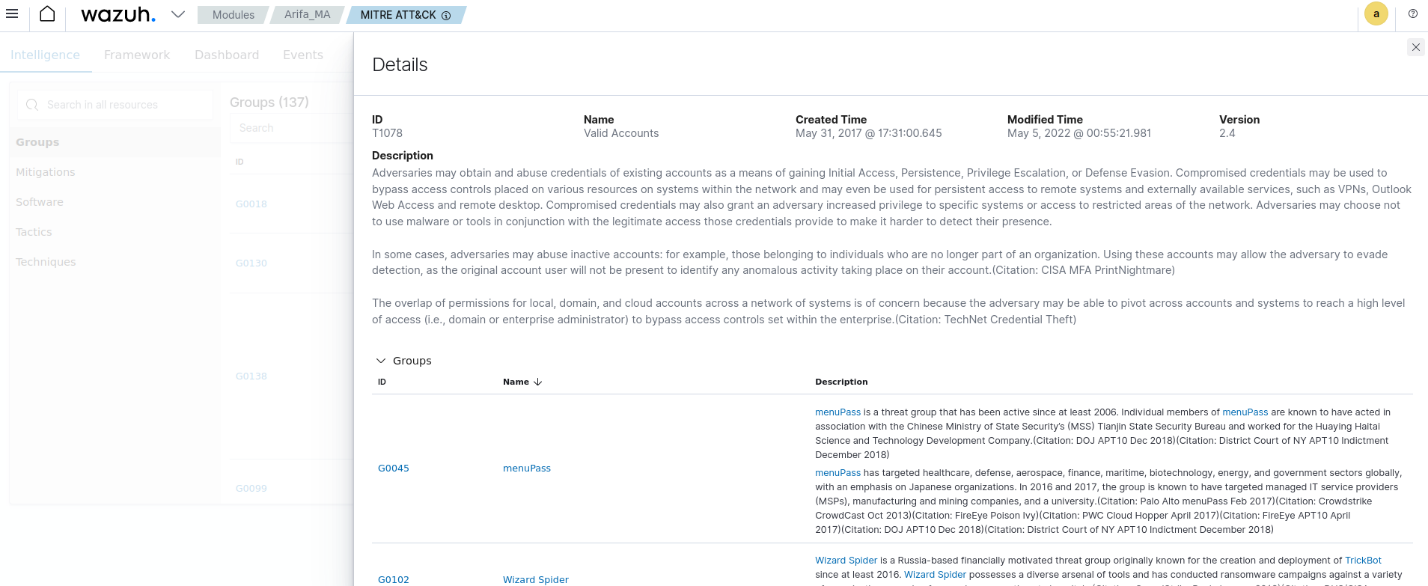
Now we could get the agent details as follows



Finally we can get seeing logs and can analyse the logs



By clicking on to each event ids we can get a detailed description and analysis of logs.



**Conclusion**

Through this project, we have successfully deployed a robust platform capable of monitoring, detecting, and responding to security incidents in real-time. Wazuh offers several advantages as a Security Information and Event Management (SIEM) tool:

1. Scalability

2. Real-time threat detection

3. Integration

4. Compliance

5. Customization

6. Centralized Management

7. Open-Source

8. Active Community

Overall, Wazuh offers a robust and cost-effective solution for organizations looking to enhance their security posture, improve threat detection and response capabilities, and achieve compliance with regulatory requirements. Its open-source nature, comprehensive features, scalability, and integration capabilities make it a compelling choice for modern cybersecurity operations.