

Wazuh SIEM - Installation and Configuration

Submitted By: Muhammed Irshad

Disclaimer

This project, "Wazuh SIEM Installation and Configuration," reflects my own ideas, creativity, and personal contributions. While undertaking this project, I drew inspiration from various sources, including articles, YouTube videos, walk-throughs, and other publicly available materials. I want to acknowledge the valuable contributions of the wider community that provided insights into Wazuh SIEM.

It's important to note that Wazuh SIEM is an open-source and freely available software. The project is not affiliated with the official Wazuh project, and any references or adaptations from external sources are duly credited.

This work is a product of my individual efforts, and I encourage others to explore and contribute to the wealth of knowledge available within the open-source community.

Table Of Contents

1. Introduction

- 1.1 Project Overview
- 1.2 Project Objectives
- 1.3 Project Scope

2. Wazuh SIEM Installation

- 2.1 Overview
- 2.2 System Requirements
- 2.3 Installation using OVA File

3. Agent Deployment & Configuration

- 3.1 Windows Agent
- 3.2 Connecting Agents to Wazuh Manager
- 3.3 Configuring Email Alerts
- 3.4 Report Generation

4. Conclusion

1. Introduction

1.1 Project Overview:

This project, "Wazuh SIEM Installation and Configuration," focuses on implementing a Security Information and Event Management (SIEM) solution using Wazuh. The primary objectives include installing Wazuh SIEM through an OVA file, deploying agent on Windows machine and configuring email alerts and report generation. This hands-on project combines individual creativity with insights gathered from various sources, while acknowledging that Wazuh SIEM is an open-source tool. The goal is to enhance cybersecurity measures and provide practical experience in configuring a robust SIEM environment.

1.2 Project Objectives:

- **Install and Configure Wazuh OVA:**
Deploy the Wazuh pre-built Virtual Machine Image (OVA) for the SIEM system.
- **Deploy Wazuh Agents:**
Install Wazuh Agents on all compatible workstations within the ownership.
- **Explore Wazuh Interface:**
Navigate and familiarize with the Wazuh interface for monitoring and managing security information.
- **Security Information Output:**
Investigate and analyze the security information output generated by Wazuh for the deployed agents.

1.3 Project Scope:

This project's scope encompasses the installation and configuration of Wazuh SIEM, agent deployment on Windows and the setup of alerts and report generation. Future enhancements may include refining rule customization, expanding monitoring capabilities, and integrating additional security tools for a more comprehensive defense posture. The project lays the foundation for ongoing improvements in threat detection and response within the Wazuh SIEM environment.

2. Wazuh SIEM Installation

2.1 Overview

A Security Information and Event Management (SIEM) tool is a cybersecurity solution that helps organizations manage and analyze security events in real-time. It collects and aggregates log data generated throughout the organization's technology infrastructure, such as networks, servers, and applications. The SIEM system then identifies and prioritizes security incidents, providing a centralized platform for monitoring and responding to potential threats. By correlating and analyzing diverse data sources, SIEM tools enable organizations to detect and respond to security incidents more efficiently, enhancing overall cybersecurity posture.

Wazuh is a free and open-source security platform that helps organizations safeguard their IT infrastructure across physical, virtual, containerized, and cloud environments. Think of it as a vigilant watchdog, constantly monitoring all your systems for threats, vulnerabilities, and suspicious activity. It combines the functionalities of endpoint security agents, a central server for data analysis, and powerful visualization tools to give you a clear picture of your security posture. Wazuh helps you detect intrusions, respond to incidents, and ensure compliance with various security regulations, making it a valuable asset for businesses of all sizes.

For more details: <https://wazuh.com/>

The Wazuh logo is displayed on a solid black rectangular background. The word "wazuh" is written in a white, lowercase, sans-serif font. A small blue dot serves as the period at the end of the word.

Wazuh offers a pre-built virtual machine image, known as an Open Virtual Appliance (OVA), as an alternative to manual installation. This readily available package contains all the essential components for deploying Wazuh's centralized security analysis system on your infrastructure. Packed with Amazon Linux 2, Wazuh manager and indexer, Filebeat-OSS, and the Wazuh dashboard, the OVA streamlines deployment, saving you time and effort. However, note that this single-machine virtual appliance prioritizes ease of use over high availability and scalability. For advanced configurations, consider distributed deployments.

2.2 System Requirements

System requirements for successfully deploying the Wazuh OVA:

Host System:

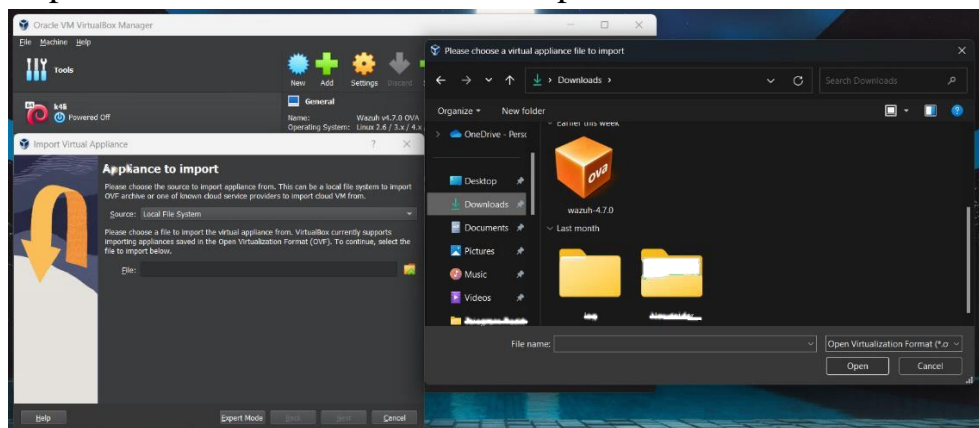
- Operating System: 64-bit system (Windows, macOS, Linux)
- Virtualization Platform: OVA-compatible platform like VirtualBox, VMware, or Hyper-V
- Network connectivity: Required for Wazuh to function and receive updates
- Browser compatibility: Chrome 95+, Firefox 93+, Safari 13.7 +

Recommended Hardware Resources:

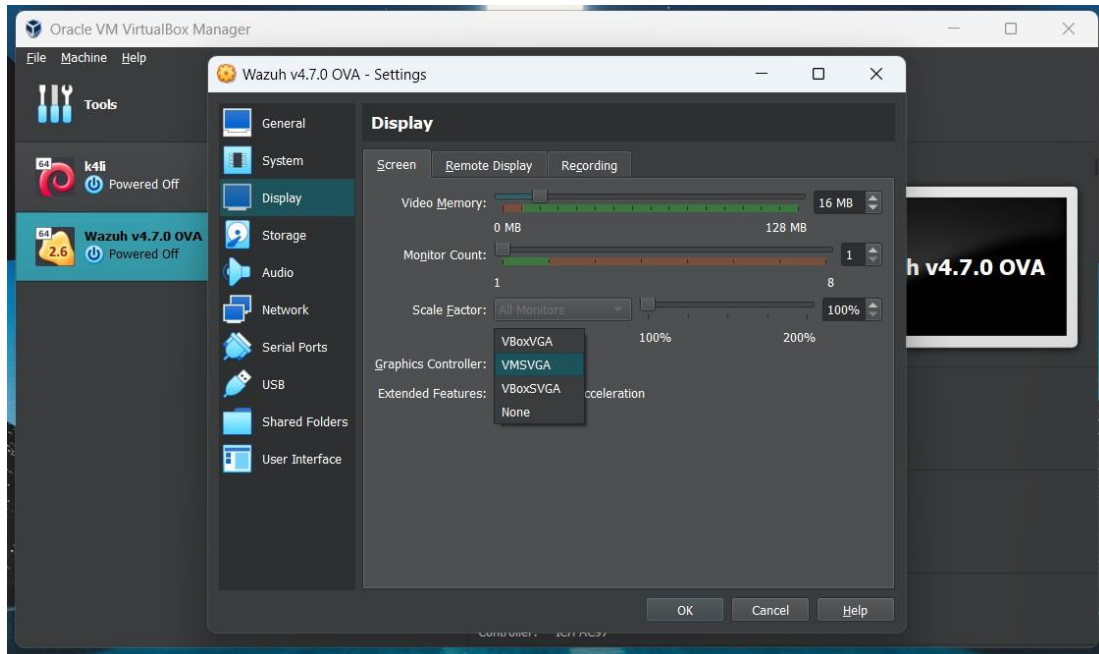
- CPU: 2 cores
- RAM: 4 GB
- Storage: 20 GB (for initial setup; adjust based on log volume and retention)

2.3 Installation using OVA File

1. Import the OVA to the virtualization platform.

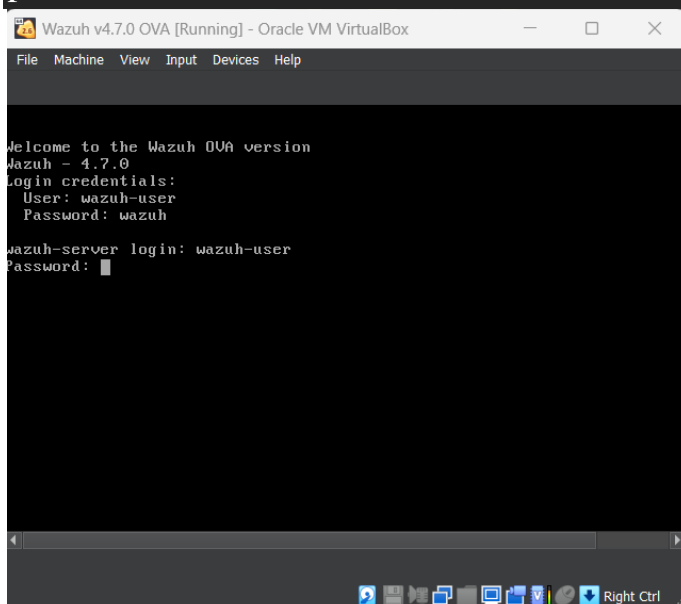


2. If you're using VirtualBox, set the **VMSVGA** graphic controller. Setting another graphic controller freezes the VM window.
 - a. Select the imported VM.
 - b. Click Settings > Display
 - c. In Graphic controller, select the **VMSVGA** option



3. Start the machine.
4. Access the virtual machine using the following user and password. You can use the virtualization platform or access it via SSH.

user: wazuh-user
password: wazuh



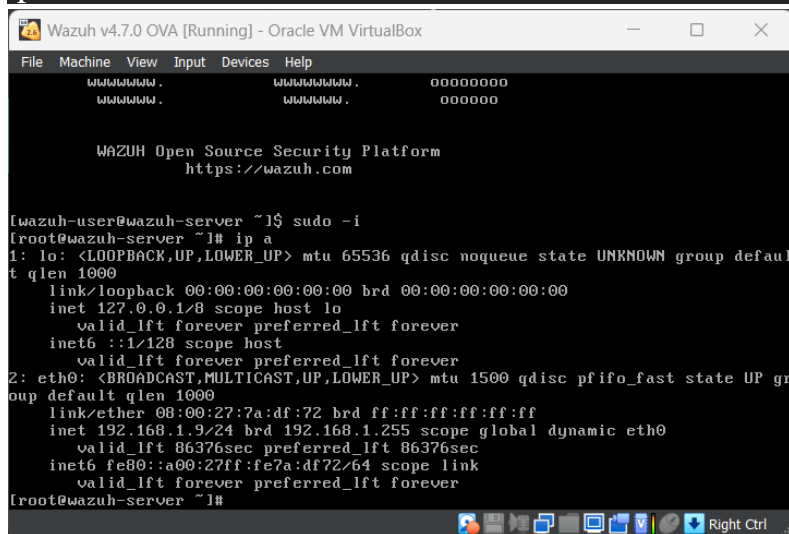
SSH **root** user login has been deactivated; nevertheless, the **wazuh-user** retains sudo privileges. Root privilege escalation can be achieved by executing the following command:

```
sudo -i
```

Access the Wazuh dashboard: Shortly after starting the VM, the Wazuh dashboard can be accessed from the web interface.

5. Find <wazuh_server_ip> by typing the following command in the VM:

```
ip a
```



```
Wazuh v4.7.0 OVA [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Wazuh Open Source Security Platform
https://wazuh.com

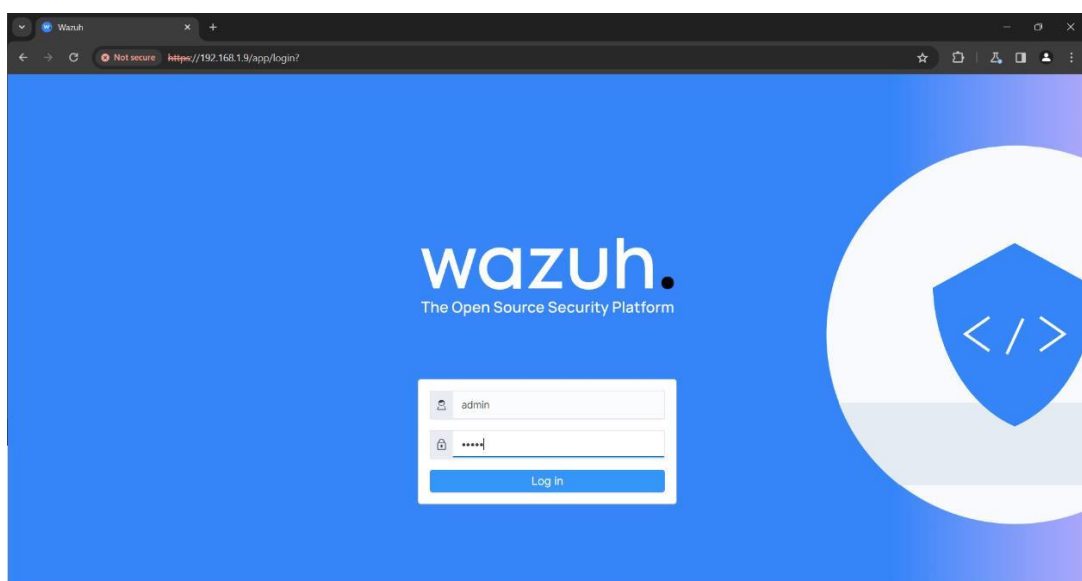
[wazuh-user@wazuh-server ~]$ sudo -i
[root@wazuh-server ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:7a:df:72 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.9/24 brd 192.168.1.255 scope global dynamic eth0
        valid_lft 86376sec preferred_lft 86376sec
    inet6 fe80::a00:27ff:fe7a:df72/64 scope link
        valid_lft forever preferred_lft forever
[root@wazuh-server ~]#
```

6. Open any browser and use the following credentials:

URL: https://<wazuh_server_ip>

user: admin

password: admin



For more details: <https://documentation.wazuh.com/current/deployment-options/virtual-machine/virtual-machine.html>

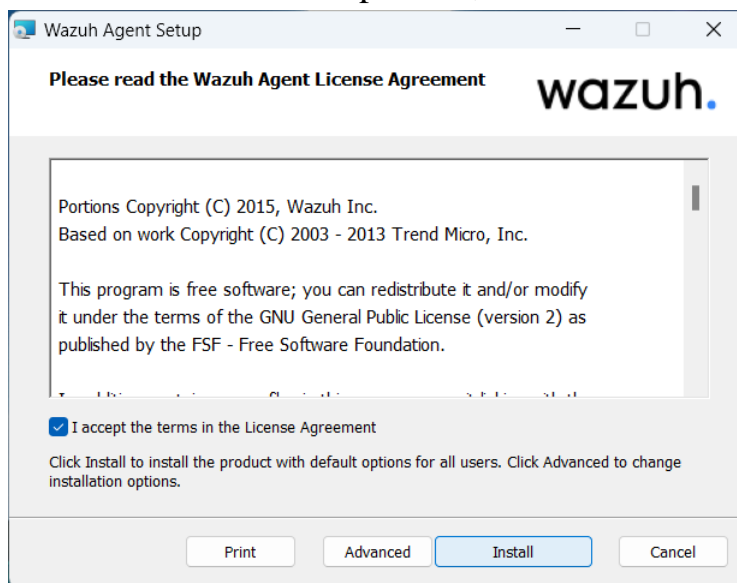
3. Agent Deployment & Configuration

3.1 Windows Agent

Installing Wazuh agents on Windows endpoints

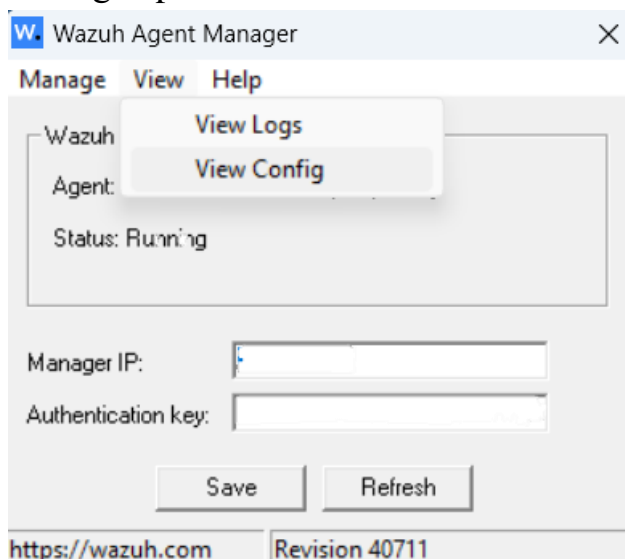
The agent runs on the endpoint you want to monitor and communicates with the Wazuh server, sending data in near real-time through an encrypted and authenticated channel. Monitor your Windows systems with Wazuh, from Windows XP to the latest available versions including Windows 11 and Windows Server 2022.

To start the installation process, download the Windows installer and install it.

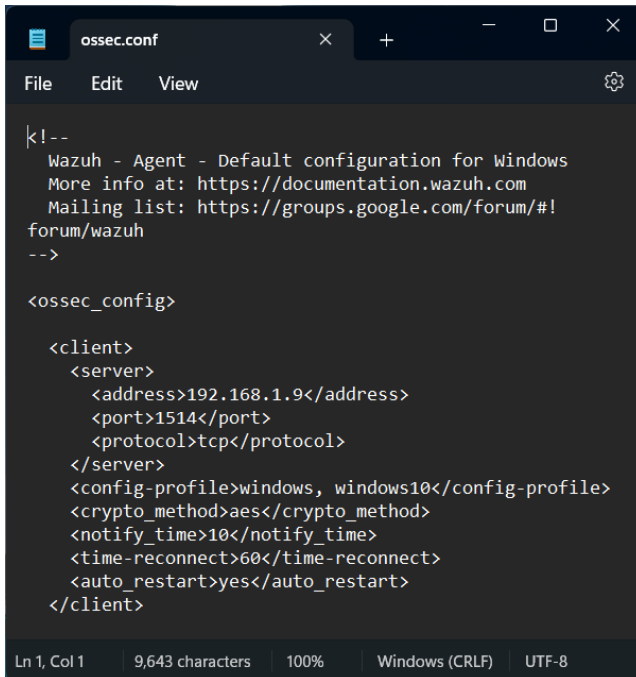


3.2 Connecting Agents to Wazuh Manager

1. After installation. Wazuh Agent Manager dialog box appear. Select “View > View Config” option.



2. “ossec.conf” named notepad appear, change the <address>_._._.</address> to our server address. Here it is 192.168.1.9, then save and close it.



```
Wazuh - Agent - Default configuration for Windows
More info at: https://documentation.wazuh.com
Mailing list: https://groups.google.com/forum/#!forum/wazuh

<ossec_config>

  <client>
    <server>
      <address>192.168.1.9</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>windows, windows10</config-profile>
    <crypto_method>aes</crypto_method>
    <notify_time>10</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
  </client>
```

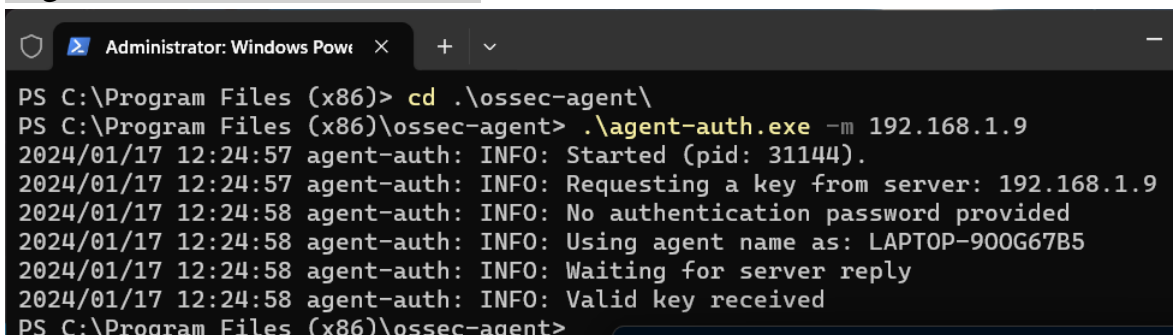
3. Click “Refersh” button on the Wazuh Agent Manager.

4. Next open-up Windows PowerShell as “Run as Administrator”

By default, all agent files are stored in C:\Program Files (x86)\ossec-agent after the installation.

5. Comment these commands.

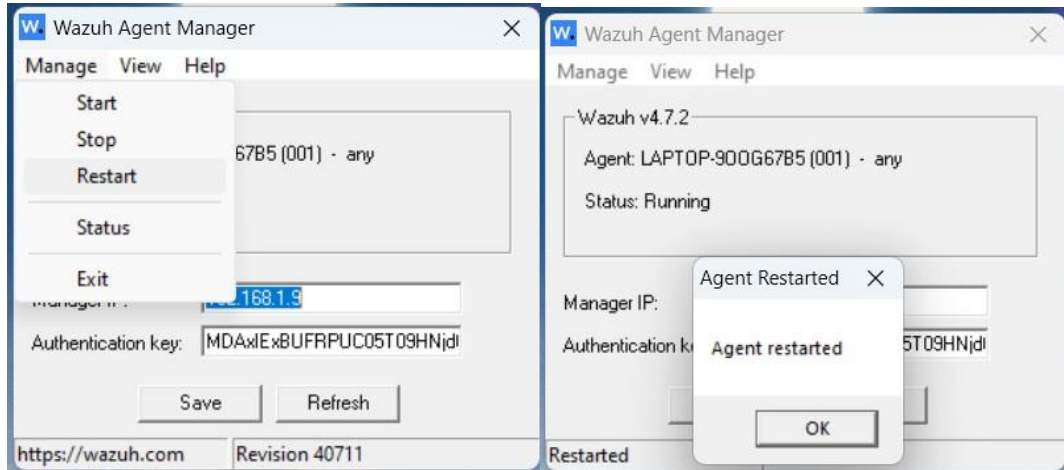
```
cd 'C:\Program Files (x86)\'
cd .\ossec-agent\
./agent-auth.exe -m 192.168.1.9
```



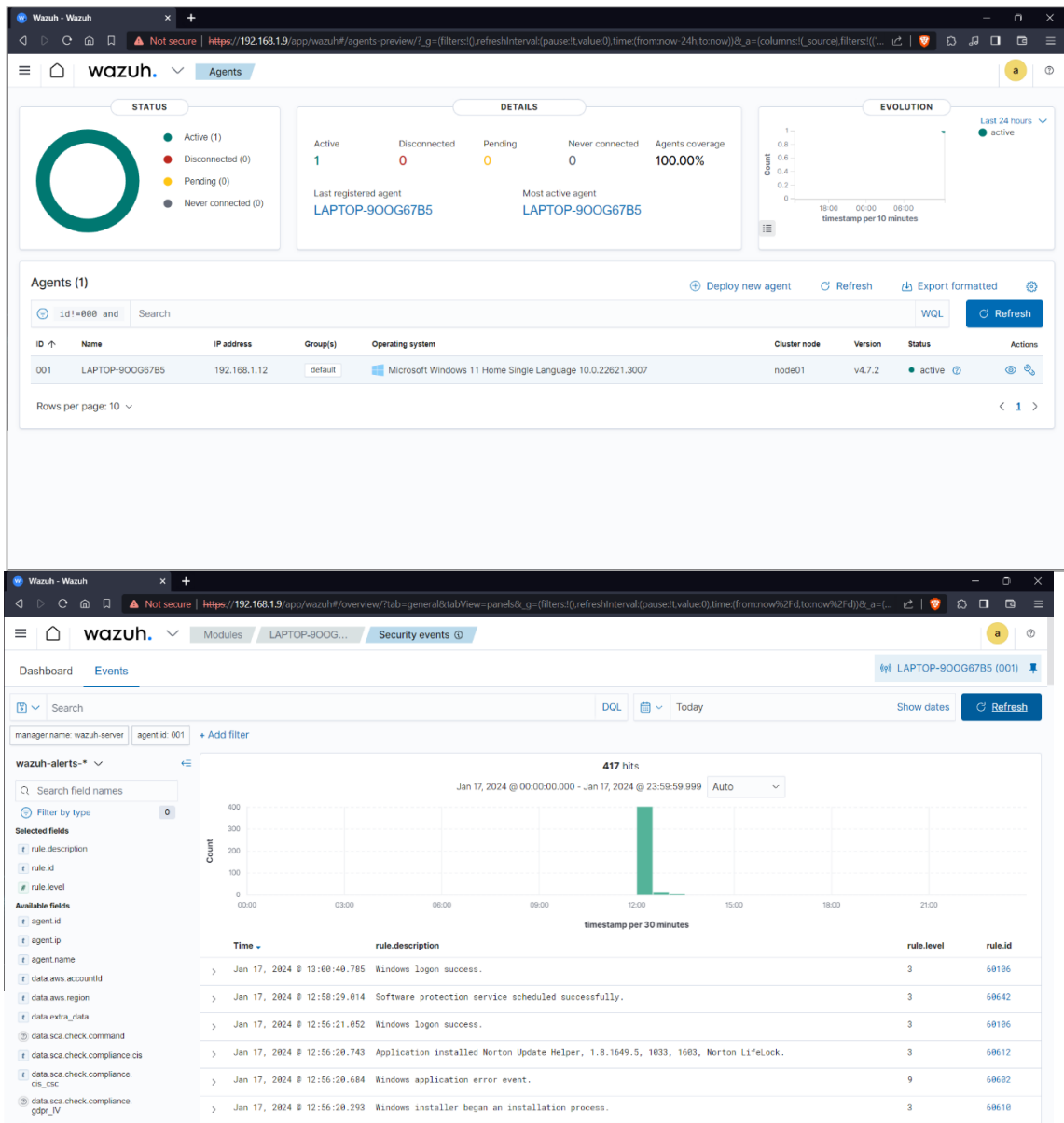
```
PS C:\Program Files (x86)> cd .\ossec-agent\
PS C:\Program Files (x86)\ossec-agent> .\agent-auth.exe -m 192.168.1.9
2024/01/17 12:24:57 agent-auth: INFO: Started (pid: 31144).
2024/01/17 12:24:57 agent-auth: INFO: Requesting a key from server: 192.168.1.9
2024/01/17 12:24:58 agent-auth: INFO: No authentication password provided
2024/01/17 12:24:58 agent-auth: INFO: Using agent name as: LAPTOP-900G67B5
2024/01/17 12:24:58 agent-auth: INFO: Waiting for server reply
2024/01/17 12:24:58 agent-auth: INFO: Valid key received
PS C:\Program Files (x86)\ossec-agent>
```

6. Then press Enter, from this we get agent name & valid authentication key in the Wazuh Agent Manager by clicking the “Refersh” button.

7. Then click “Manage > Restart”, the agent will restart.



8. Open our Wazuh server, click agent. Here we can see our windows agent.



3.3 Configuring Email Alerts

Wazuh can be configured to send email alerts to one or more email addresses when certain rules are triggered or for daily event reports.

In order to configure Wazuh to send email alerts, the email settings must be configured in the <global> section of the ossec.conf file:

```
<ossec_config>
<global>
<email_notification>yes</email_notification>
<email_to>me@test.com</email_to>
<smtp_server>mail.test.com</smtp_server>
<email_from>agent01@test.com</email_from>
</global>
...
</ossec_config>
```

Once the above has been configured, the email_alert_level needs to be set to the minimum alert level that will trigger an email. By default, this level is set to 12.

```
<ossec_config>
<alerts>
<email_alert_level>10</email_alert_level>
</alerts>
</ossec_config>
```

After the alert level has been configured, Wazuh needs to be restarted for the change to take effect.

```
systemctl restart wazuh-manager
```

EMAIL OUTPUT

From: Wazuh <agent01@test.com> 5:03 PM (2 minutes ago)

to: me

Wazuh Notification.

2023 Dec 26 17:03:05

Received From: localhost->/var/log/secure

Rule: 5503 fired (level 5) -> "PAM: User login failed."

Src IP: 192.168.1.12

Portion of the log(s):

Dec 26 17:03:04 localhost sshd[67231]: pam_unix(sshd:auth): authentication failure;

logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.12

uid: 0

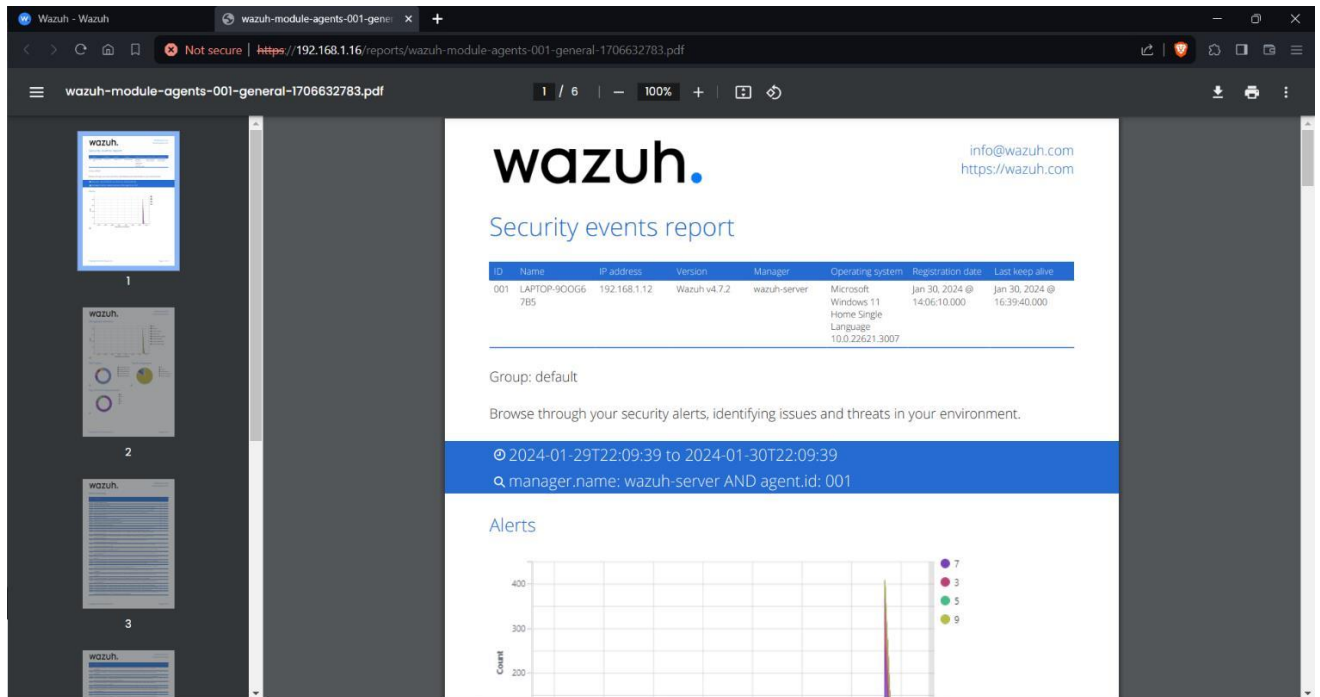
euid: 0

tty: ssh

--END OF NOTIFICATION

3.4 Report Generation

We can generate reports of logs, security events, alerts and everything included in the wazuh using generate report option and we can download it from reporting section of wazuh manager.



Report Generated By Wazuh Manager for the Security Events That Takes Place In Windows.

4. Conclusion

In concluding the SIEM Tool Configuration Project on my Windows system, we have achieved significant milestones in fortifying our cybersecurity defenses. Despite facing limitations in deploying agents directly on my system, the comprehensive installation using the OVA file and subsequent deployment of Windows agents on external systems have laid a robust foundation.

The successful connection of agents to the Wazuh Manager, coupled with the configuration of email alerts, ensures real-time monitoring and rapid response capabilities. The culmination of efforts in report generation provides valuable insights into the security landscape, facilitating informed decision-making.

While my system limitations presented challenges, the project's achievements underscore the adaptability and scalability of the implemented SIEM solution. Moving forward, the configured SIEM tool, orchestrated from my Windows environment, stands ready to vigilantly safeguard our digital assets against evolving cyber threats.

This project serves not only as a testament to the efficacy of the implemented solution but also as an acknowledgment of the need for flexibility in cybersecurity strategies. It highlights the importance of leveraging available resources to create a resilient security posture that aligns with organizational goals.