****

|  |
| --- |
| *BS Cyber Security Department AU* |

|  |  |
| --- | --- |
| **Registration ID** | **233026** |
| **Submitted By** | **Muhammad Sohaib Rafiq** |
| **Submitted To** | **Iram Fatima Hashmi** |
| **Date of Submission** | **06/12/2025** |
| **Lab NO.** | **10** |
| **Subject** | **NS LAB** |

# ****Wazuh Deployment****

## **Table of Contents**

1. **Abstract**
2. **Introduction**
3. **Importance of Wazuh in SOC and SIEM**
4. **Installation and Setup**
   * 4.1 sudo curl Installation
   * 4.2 JDK Default Installation
   * 4.3 Wazuh Server Cluster Installation
   * 4.4 Downloading the Wazuh Installation Assistant
   * 4.5 Running bash wazuh-install.sh -a
   * 4.6 Backup Folder
5. **Platform Access**
   * 5.1 Wazuh IP Address and Port Number
   * 5.2 Accessing the Wazuh Web Interface
6. **Agent Deployment**
   * 6.1 Starting the Wazuh Agent
   * 6.2 Connecting Windows Host
   * 6.3 Windows Agent Logs
7. **Security Operations**
   * 7.1 Vulnerability Detection
   * 7.2 Adding Rules
   * 7.3 Static Tab and Dashboard Overview
8. **Wazuh Architecture Diagram**
9. **Conclusion**

## **1. Abstract**

This report documents the installation, configuration, and operation of the Wazuh Security Information and Event Management (SIEM) system. It explains how Wazuh enhances visibility across endpoints, detects vulnerabilities, and strengthens the organization's security operations through effective log analysis, threat detection, and compliance monitoring.

## **2. Introduction**

Wazuh is a powerful open-source SIEM and XDR platform that integrates endpoint detection and response (EDR), log analysis, file integrity monitoring, and vulnerability detection into a single unified interface. It is built on top of the Elastic Stack and is commonly deployed in SOCs to monitor infrastructure in real time.

## **3. Importance of Wazuh in SOC and SIEM**

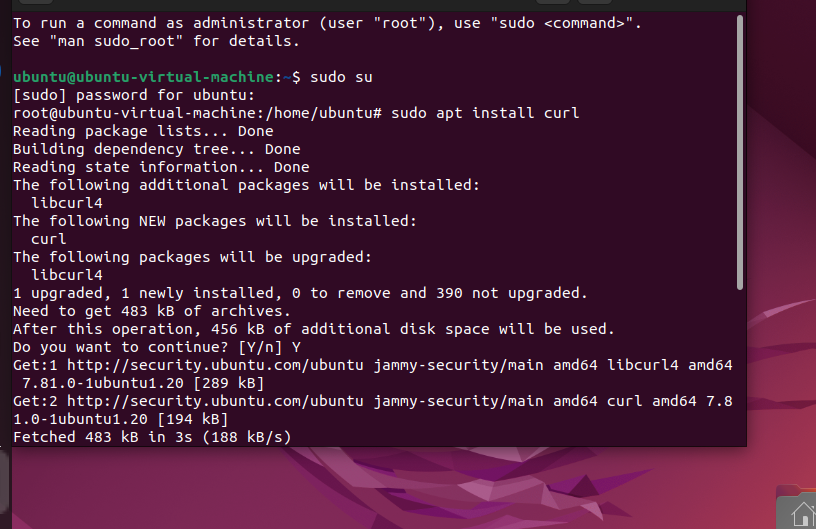
* **Real-time Monitoring:** Detects suspicious activity across the network.
* **Log Collection & Analysis:** Gathers logs from servers, firewalls, endpoints, and more.
* **Threat Intelligence:** Correlates data with threat feeds to identify potential compromises.
* **Compliance:** Supports standards like PCI-DSS, HIPAA, and GDPR.
* **XDR & EDR Capabilities:** Helps blue teams defend endpoints effectively.
* **Custom Rule Sets:** Organizations can tune detection rules as per their environment.

****

## **4. Installation and Setup**

### 4.1 sudo curl Installation:

sudo apt install curl -y



### 4.2 JDK Default Installation:

Wazuh uses Java for parts of its stack (especially Elasticsearch).

bash

Copy code

sudo apt install default-jdk -y

This installs the Java Development Kit necessary for Elasticsearch and Kibana.

### 4.3 Wazuh Server Cluster Installation:

A Wazuh cluster typically involves:

* **Wazuh Server** (Analysis and Rules)
* **Wazuh Indexer** (Elasticsearch replacement)
* **Wazuh Dashboard** (Web interface)
* **Wazuh Agents** (Endpoint log collectors)

## 

### 4.4 Downloading the Wazuh Installation Assistant:

You would’ve run:

bash

Copy code

curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh

This downloads the all-in-one Wazuh installation assistant.



### 4.5 Running bash wazuh-install.sh -a

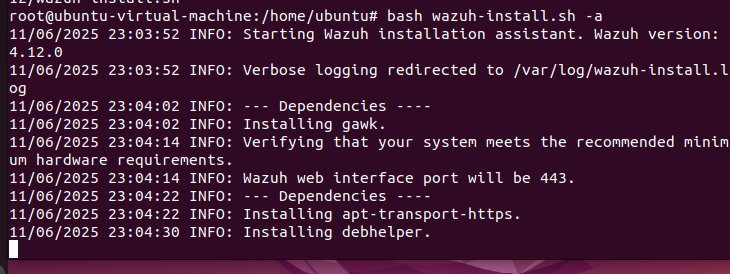
This command starts the automated deployment of the full Wazuh Stack:

bash

Copy code

bash wazuh-install.sh -a

It sets up the Wazuh manager, indexer, and dashboard on one node.



### 4.6 Backup Folder:

**A common backup step before re-installation:**

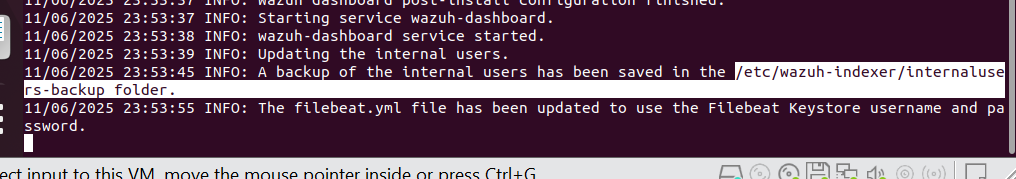
bash

Copy code

mkdir ~/wazuh\_backup

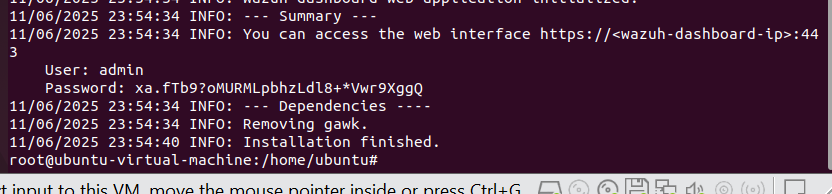
cp -r /var/ossec ~/wazuh\_backup

Ensures that agent keys and rules are preserved.

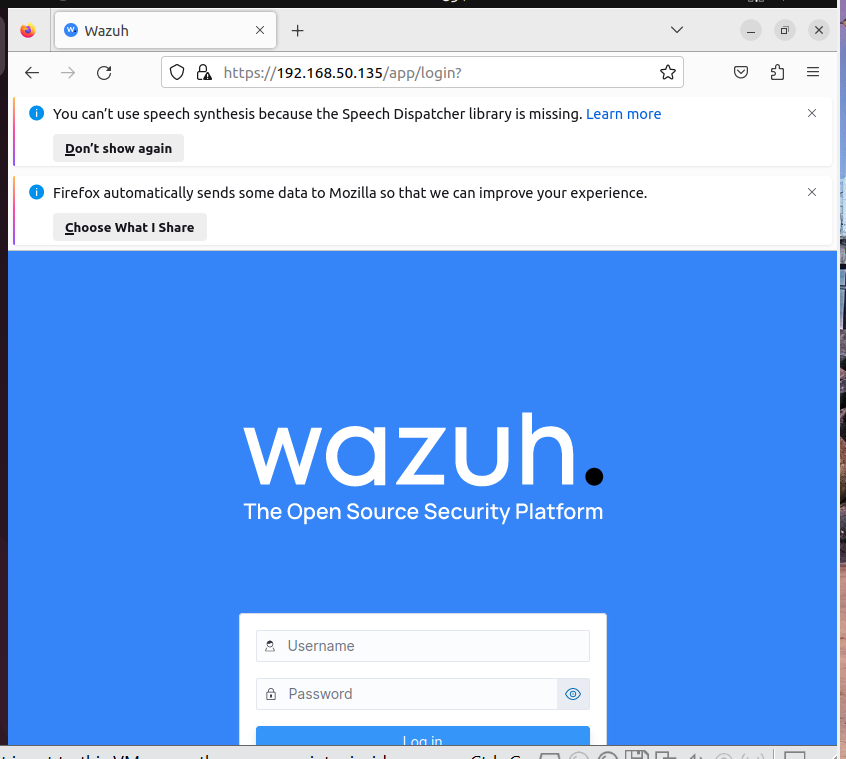


## **5. Platform Access**

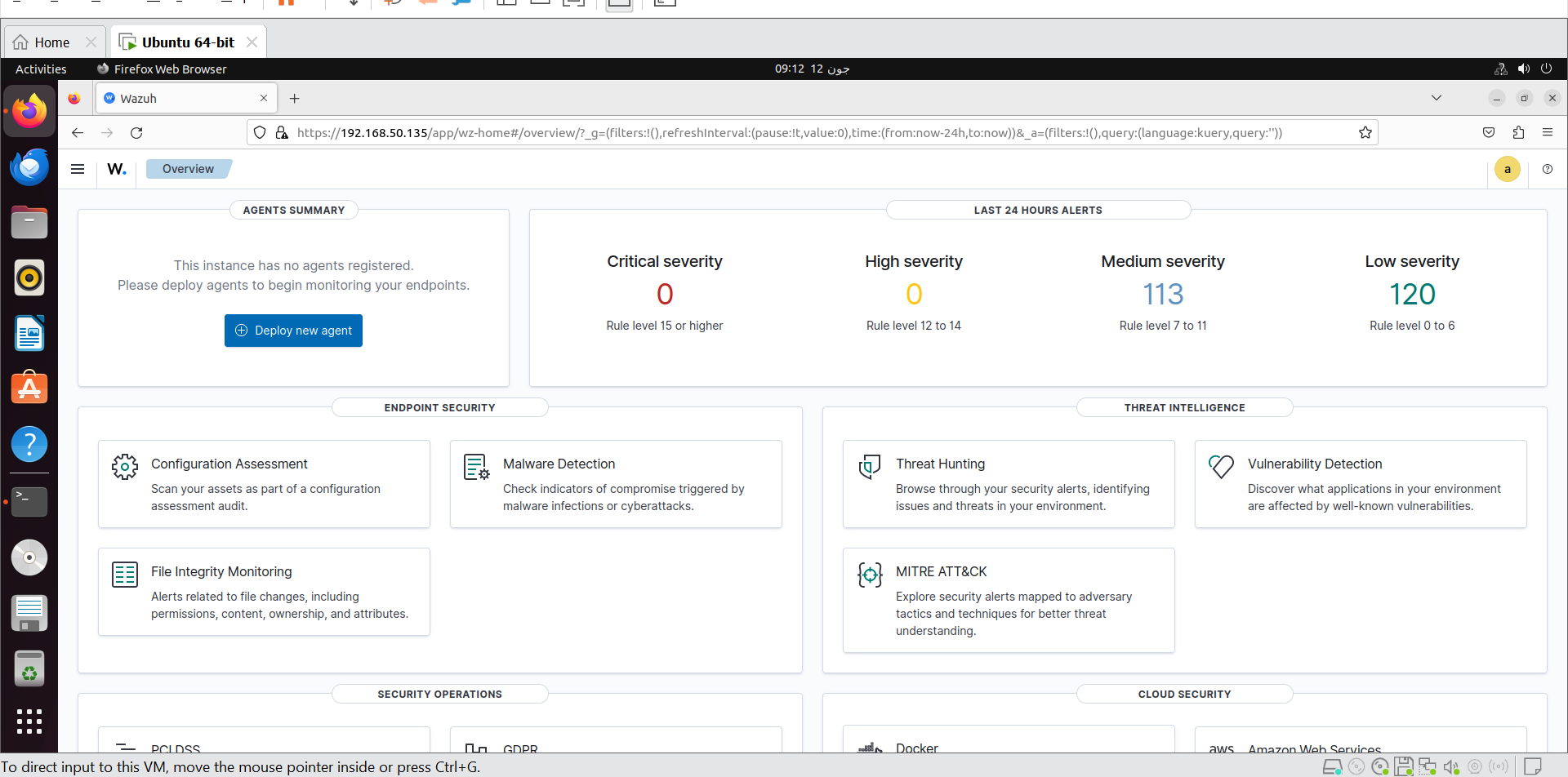
### 5.1 Wazuh IP Address and Port Number:



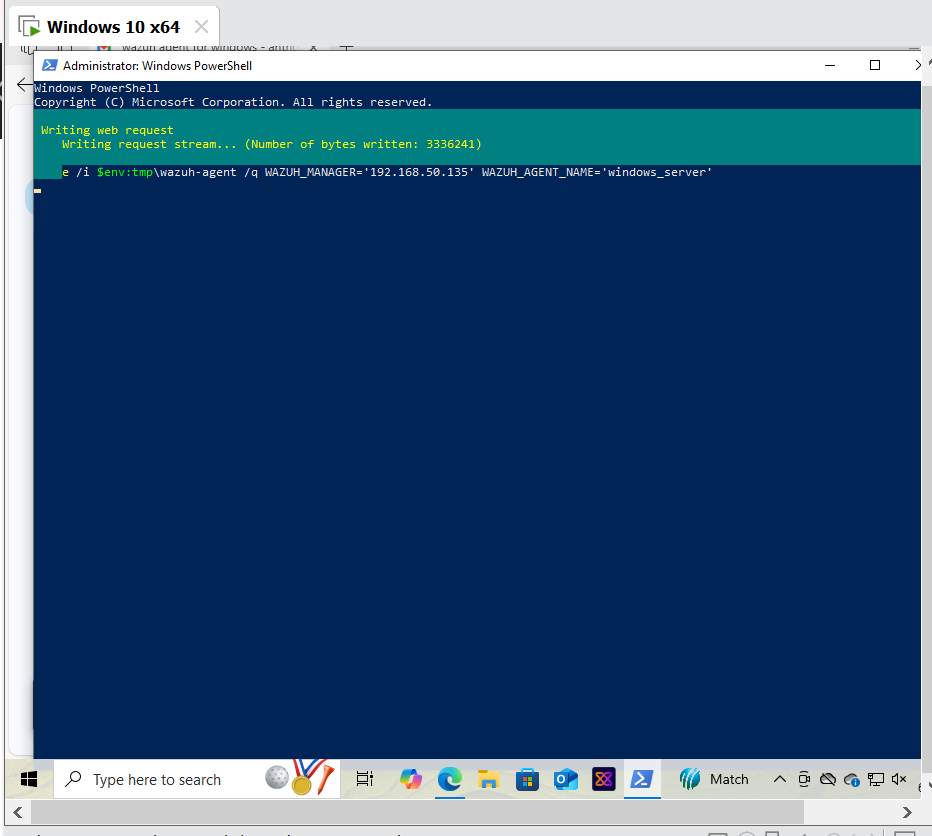
### 5.2 Accessing the Wazuh Web Interface:

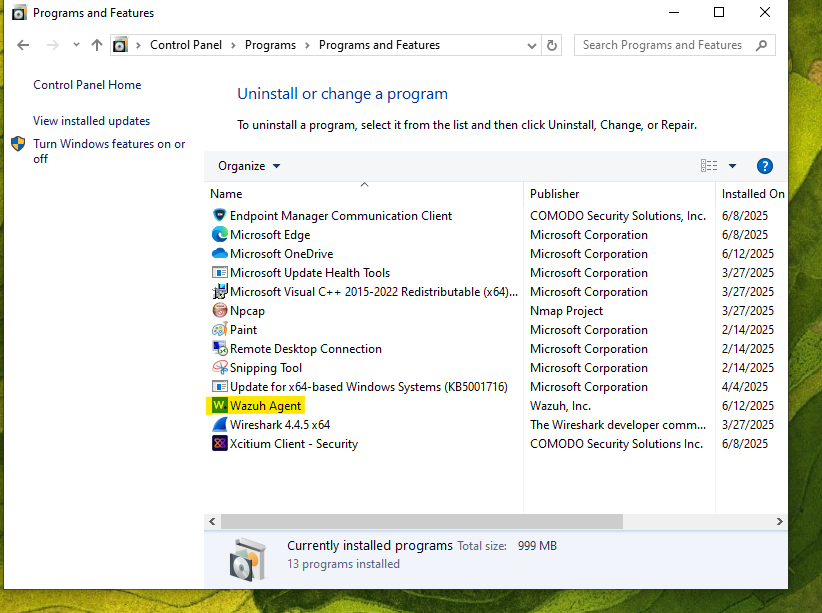


**Wazuh web interface:**

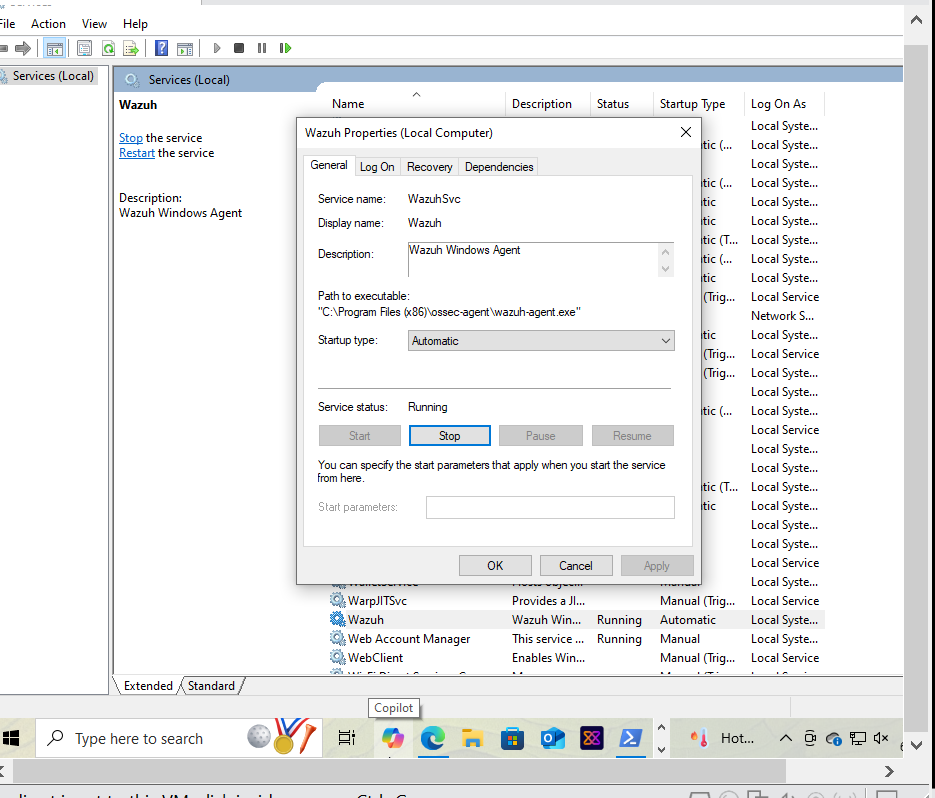


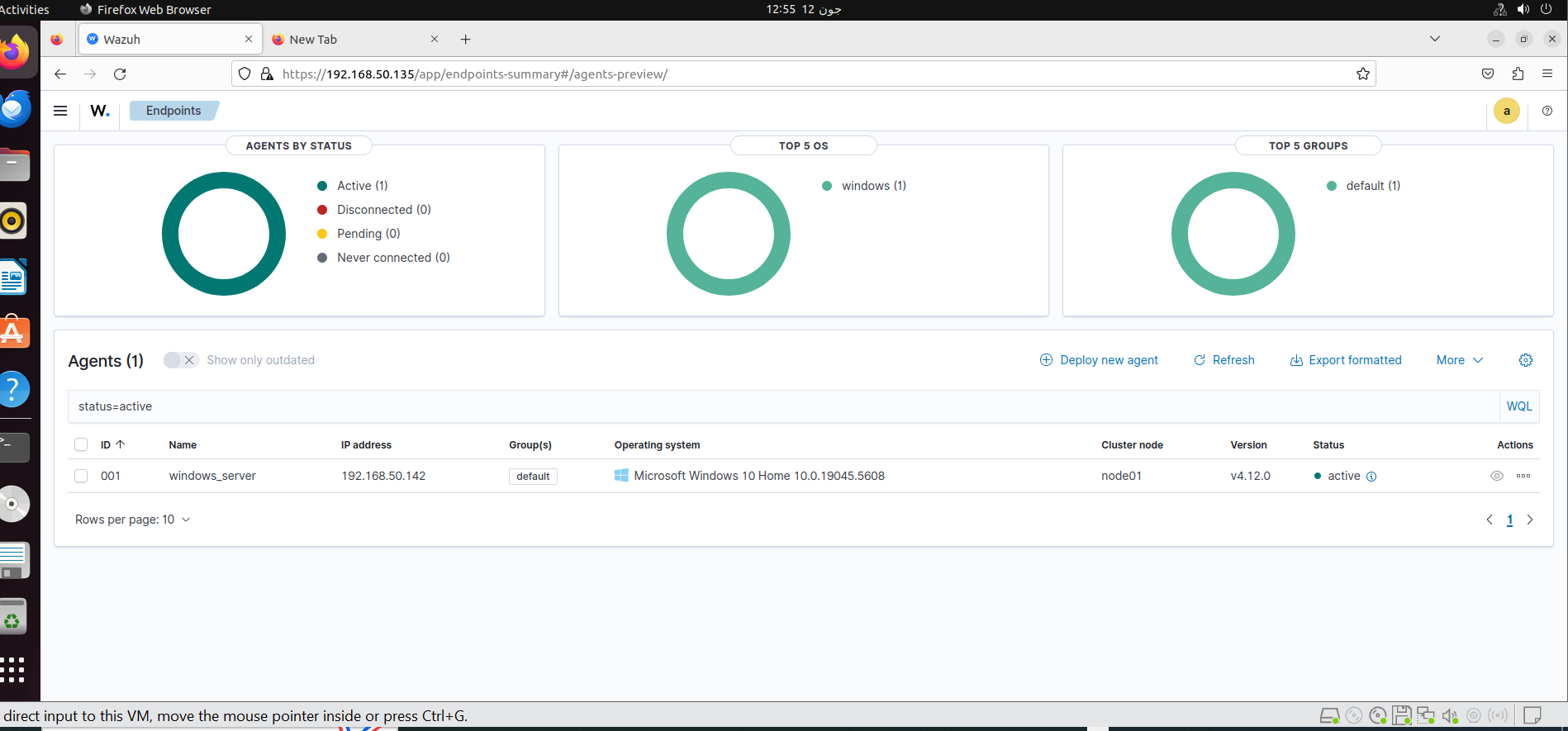
**6. Agent Deployment**



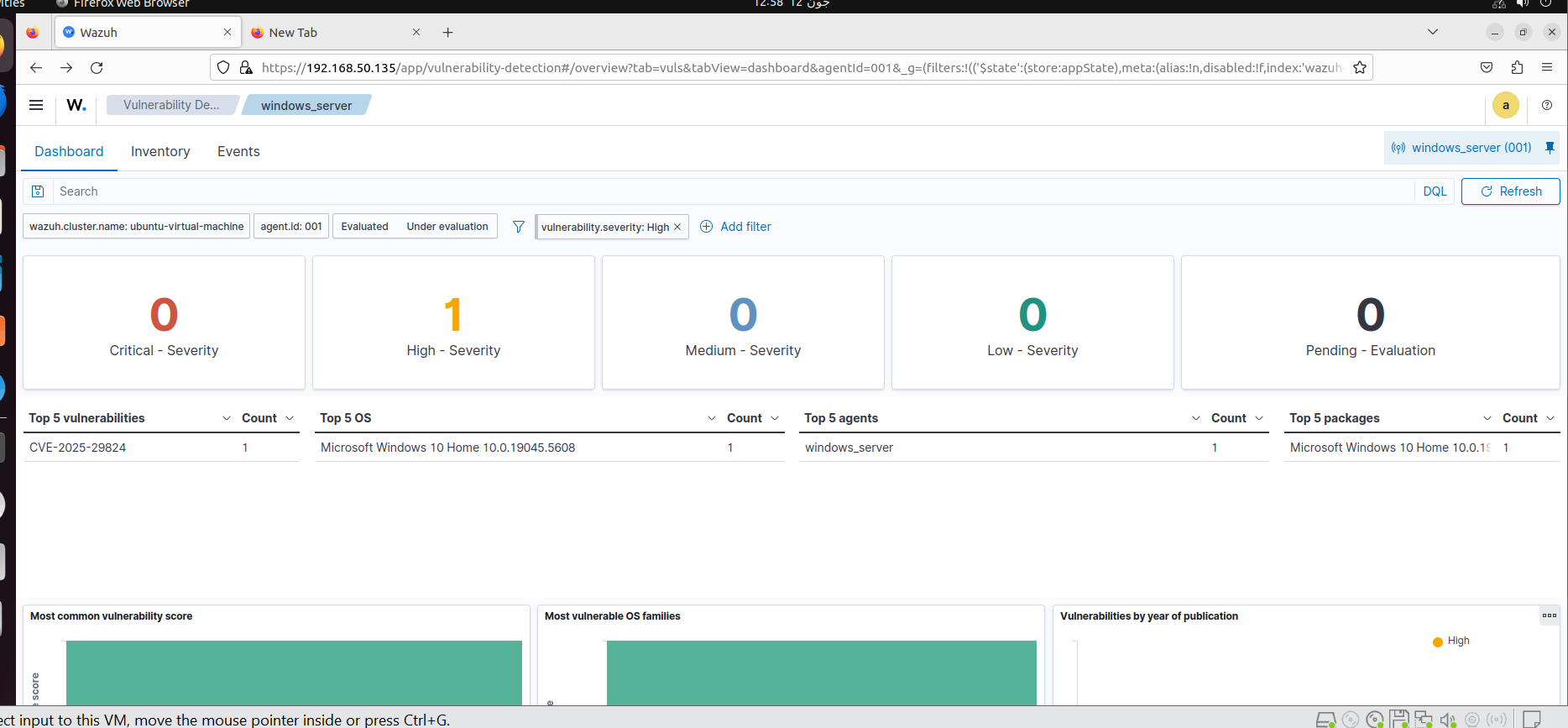


**6.2 Connecting Windows Host:**

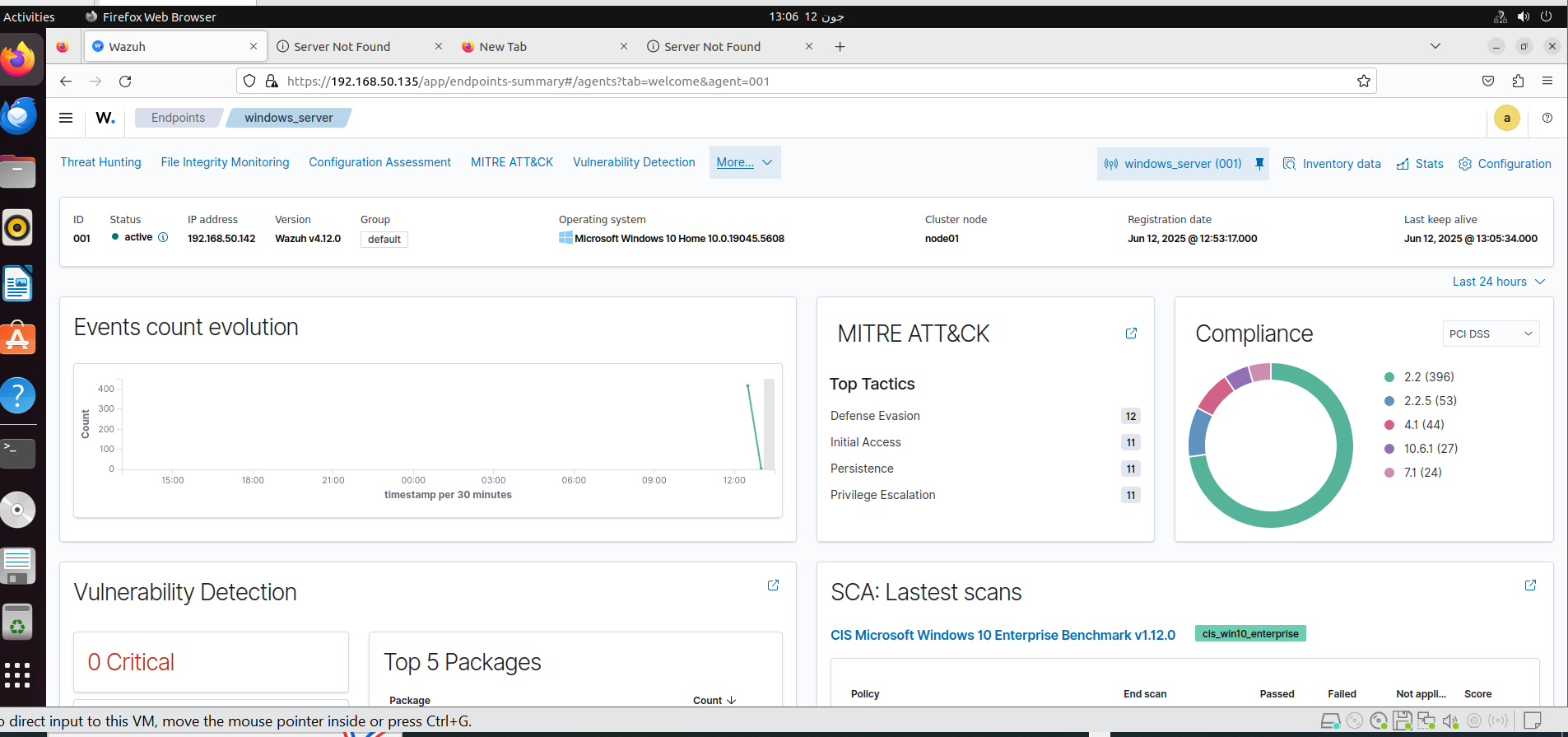




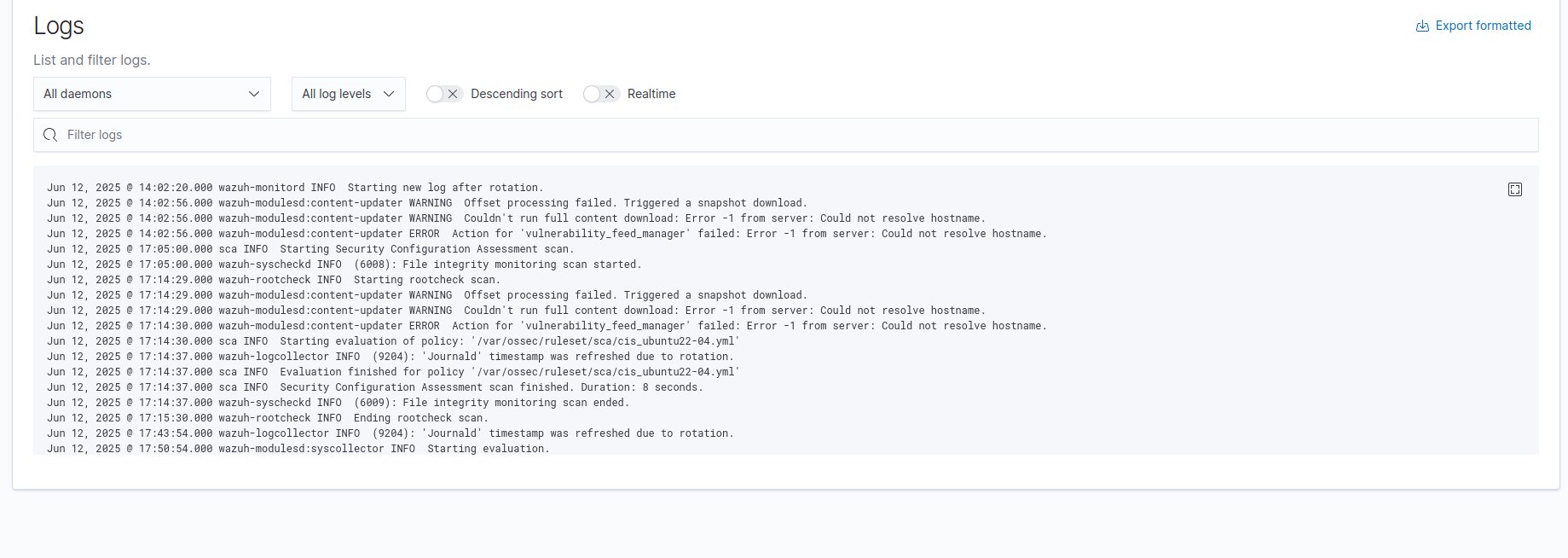
**Vulnerability detecting:**



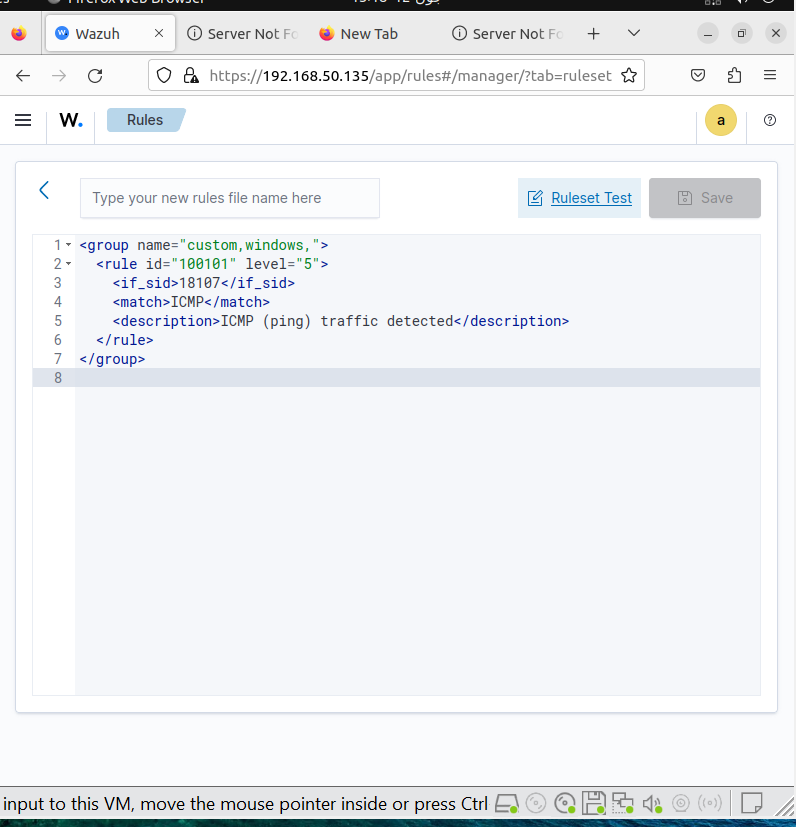
**Dashboard overview:**



Windows Agnest logs:

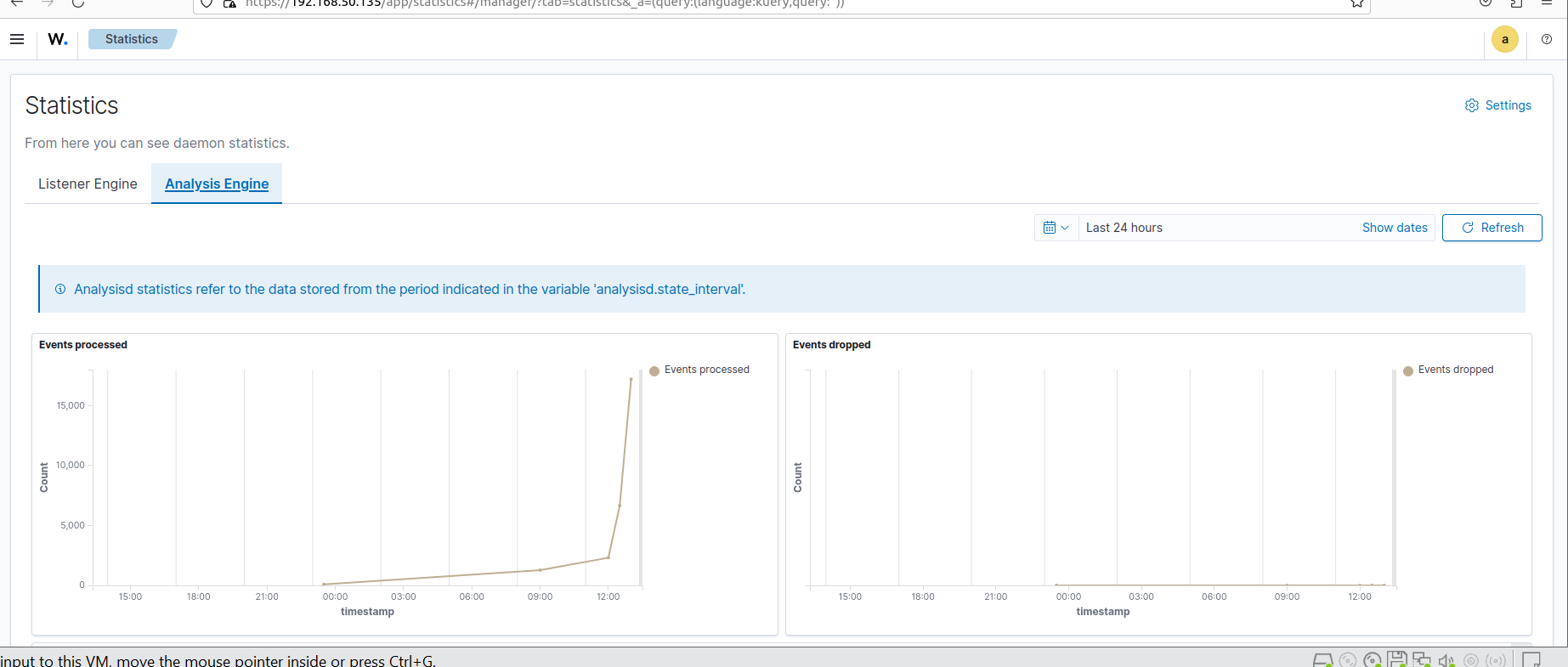


### 7.2 Adding Rules to Wazuh:



### 7.3 Static Tab and Dashboard Overview:

* **Overview Panel:** Provides real-time insights into alerts and agent status.
* **Security Events Tab:** Visualizes attack types, agents affected.
* **Statistics Tab:** Shows alert frequency, rule triggers, CVE stats.



## **9. Conclusion**

Wazuh provides an open-source, enterprise-grade solution for log analysis, threat detection, compliance monitoring, and security incident response. This deployment demonstrates how Wazuh enhances SOC capabilities and provides centralized control over security infrastructure.

Whether monitoring a small set of systems or scaling to an enterprise-wide deployment, Wazuh proves to be a reliable, extensible, and secure platform for modern cybersecurity operations.