Bangladesh University of Engineering and Technology

Department of Computer Science and Engineering

Academic Year 2023–2024

CSE 406
Computer Security Sessional

Wazuh: A Comprehensive Look at its XDR and SIEM Capabilities for Enhanced Security

---

Submitted by:

1905001 — Mohammad Sadat Hossain

1905004 — Asif Azad

1905005 — Md. Ashrafur Rahman Khan

Supervisor: Abdur Rashid Tushar

Submission date: March 9, 2024

Contents

Wazuh: A Comprehensive Look at its XDR and SIEM Capabilities for Enhanced Security

1 INTRODUCTION TO WAZUH

1.1 WHAT IS WAZUH?

Wazuh stands as a free and open-source security platform, wielding the combined power of XDR (extended detection and response) and SIEM (security information and event management). This potent combination safeguards data across diverse environments, from traditional on-premise setups to the modern world of cloud, virtual, and containerized systems.

Wazuh builds upon the capabilities of OSSEC (an open-source intrusion detection system), further enhancing its functionality with additional features, richer APIs, and improved integration capabilities. Trusted by organizations of all sizes, Wazuh offers a reliable defense against ever-present security threats.

1.2 WAZUH COMPONENTS

Wazuh primarily comprises of 2 components: the Wazuh Agent and the Wazuh Manager.

1.2.1 WAZUH AGENT

The Wazuh agent, a multi-platform component, runs on user-designated endpoints for monitoring purposes. It transmits data to the Wazuh server in near real-time via an encrypted and authenticated channel. Designed with performance in mind for diverse endpoints, the agent supports popular operating systems (like Windows, Linux, macOS, Solaris etc.) and requires a modest average of 35 MB RAM.

The Wazuh agent empowers users with a range of security-enhancing features, including:

- Log collection
- Command execution
- File integrity monitoring (FIM)
- Security configuration assessment (SCA)
- System inventory
- Malware detection
- Active response

- Container security
- Cloud security

1.2.2 WAZUH MANAGER

The Wazuh Manager, also known as the 'Central Component' acts as the core of the Wazuh system. It comprises three key elements:

1. **Wazuh Indexer:** This highly scalable engine serves as a full-text search and analytics platform. It indexes and stores alerts generated by the Wazuh server, enabling efficient retrieval and analysis.

2. **Wazuh Server:** Functioning as the data processing center, the Wazuh server analyzes information received from agents. It employs decoders, rules, and threat intelligence to identify potential security breaches based on known indicators of compromise (IOCs). A single server can handle data from hundreds or thousands of agents, with the capability to scale horizontally in a cluster configuration. Additionally, the Wazuh server manages the agents, allowing for remote configuration and upgrades.

3. **Wazuh Dashboard:** This web-based user interface provides a platform for data visualization and analysis. Pre-configured dashboards offer insights into security events, regulatory compliance (PCI DSS, GDPR, CIS, HIPAA, NIST 800-53, etc.), detected vulnerabilities, file integrity monitoring data, configuration assessment results, cloud infrastructure events, and more. It also facilitates Wazuh configuration management and status monitoring.

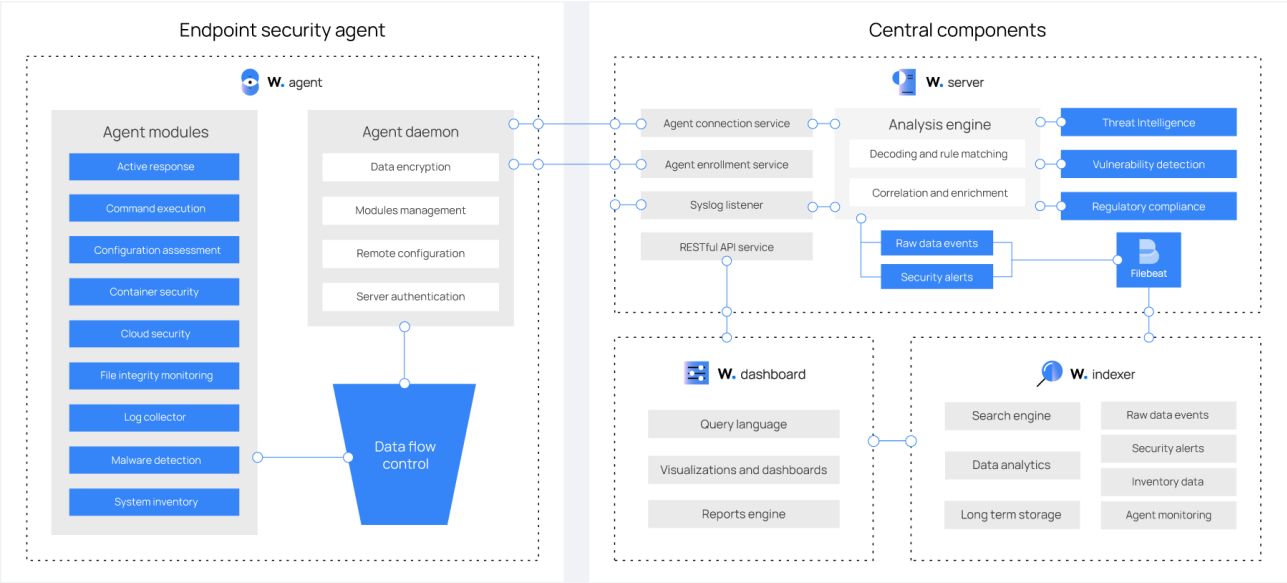

Figure 1: Wazuh Components and Data flow

1.3 WAZUH ARCHITECTURE

The foundational structure of the Wazuh system hinges on two primary components: agents and servers. Agents, installed on monitored systems, relay security data back to the centralized server. The system also accommodates agentless devices like firewalls and routers, enabling these to transmit log data through various protocols such as Syslog and SSH, or directly via APIs.

Upon receipt, the central server undertakes the decoding and analysis of this data, thereafter dispatching it to the Wazuh indexer. The indexer, potentially a single-node for smaller setups or a multi-node cluster for larger, data-intensive operations, is tasked with data indexing and preservation.

Particularly in production settings, segregating the server and indexer onto separate platforms enhances system integrity. Within this framework, Filebeat plays a critical role, securely shuttling alerts and archives from the Wazuh server to the indexer, all the while safeguarded by TLS encryption.

Illustrated below, the deployment architecture schema delineates the interplay between server and indexer within the ecosystem, underscoring the potential for cluster configurations to achieve scalability and fault tolerance.

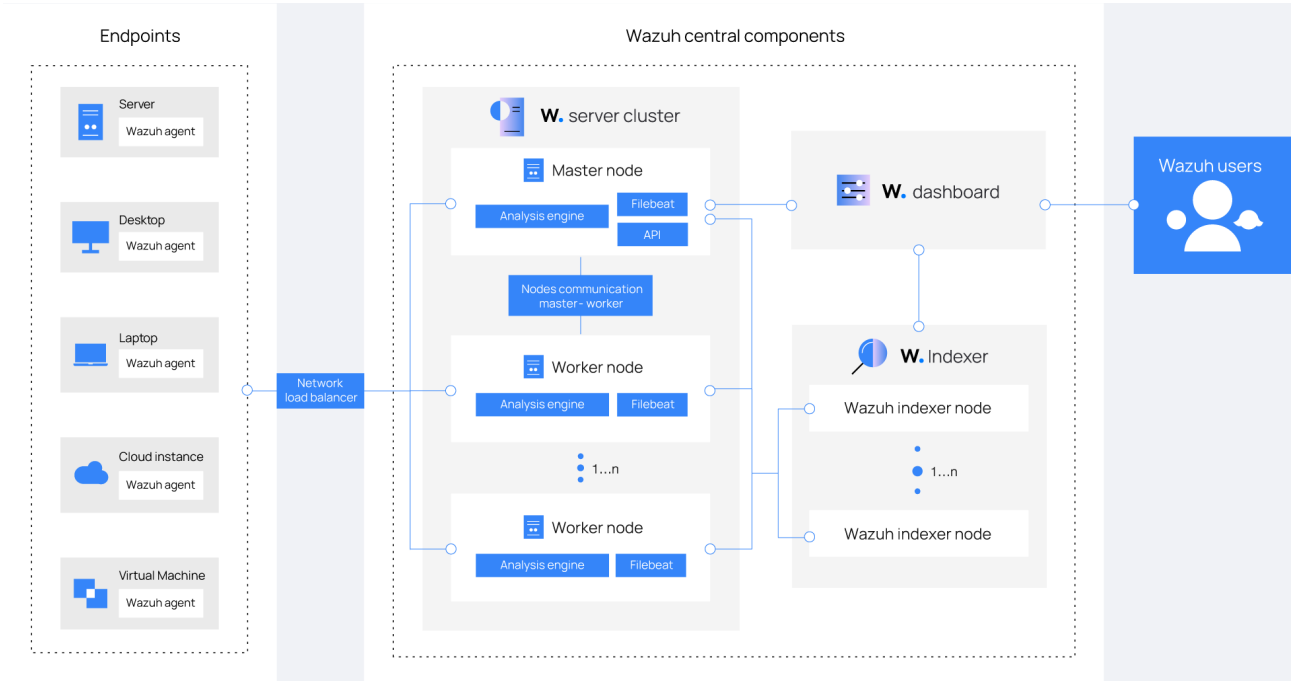

Figure 2: Overview of Wazuh Deployment Architecture

2 INSTALLATION PREREQUISITES

2.1 SYSTEM REQUIREMENTS

2.1.1 HARDWARE SPECIFICATIONS

The scale of hardware requisite directly correlates with the quantity of endpoints and cloud services to be secured. This correlation aids in estimating the volume of data analysis and the accumulation of security alerts.

For typical use cases, the consolidation of the Wazuh server, indexer, and dashboard within a single host configuration usually suffices, as this is adequate for supervising no more than 100 endpoints and maintaining ninety days of accessible alert data. The following table delineates the advisable hardware for an initial setup:

Endpoints	**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

Table 1: Recommended Hardware for Quickstart Deployment

In scenarios involving broader infrastructures, a segmented deployment is suggested. The Wazuh server and indexer can be configured into multi-node clusters to enhance scalability and facilitate load distribution.

2.1.2 OPERATING SYSTEM COMPATIBILITY

The Wazuh core components necessitate a 64-bit Linux-based installation environment. The subsequent versions of operating systems are endorsed in the official documentation:

- Amazon Linux 2
- CentOS 7, 8
- Red Hat Enterprise Linux 7, 8, 9
- Ubuntu 16.04, 18.04, 20.04, 22.04

2.1.3 WEB BROWSER SUPPORT

The Wazuh dashboard is compatible with the following browsers:

- Chrome 95 or newer

- Firefox 93 or newer
- Safari 13.7 or newer

2.2 CONFIGURING THE MACHINES

2.2.1 WAZUH SERVER

- **Computer Name:** wazuh-server
- **Operating System:** Linux 20.04 (V1 x64)
- **Size:** Standard B2s, 2 VCPUs, 4GB RAM
- **Public IP:** 20.2.220.92
- **Private IP:** 10.0.0.5

2.2.2 WAZUH AGENTS

Agent ID: 001

- **Computer Name:** wazuh-agent-linux-1
- **Operating System:** Ubuntu 22.04.3 LTS
- **Size:** Standard B2s, 2 VCPUs, 4GB RAM
- **Public IP:** N/A
- **Private IP:** 10.0.0.6

Agent ID: 002

- **Computer Name:** wazuh-agent-win
- **Operating System:** Microsoft Windows 11 Pro 10.0.22000.2538
- **Size:** Standard B2s, 2 VCPUs, 4GB RAM
- **Public IP:** N/A
- **Private IP:** 10.0.0.4

Agent ID: 007

- **Computer Name:** seed-vm
- **Operating System:** Ubuntu 20.04.6 LTS
- **Size:** Standard B2s, 2 VCPUs, 4GB RAM
- **Public IP:** N/A
- **Private IP:** 10.0.0.4

Agent ID: 008

- **Computer Name:** Sadat-Linux
- **Operating System:** Ubuntu 20.04.6 LTS
- **Size:** Standard B2s, 2 VCPUs, 4GB RAM
- **Public IP:** N/A
- **Private IP:** 10.0.0.4

Agent ID: 009 Understably, macOS integration could not be done on a virtual machine. We used a physical machine for this purpose.

- **Computer Name:** fahad-air-42
- **Operating System:** macOS 13.5.2
- **Size:** Apple M1, 8-core CPU, 8GB RAM
- **Public IP:** N/A
- **Private IP:** 192.168.0.197

3 INSTALLATION

3.1 SETTING UP THE WAZUH SERVER

There are two methods to setup the Wazuh Server:

3.1.1 QUICKSTART INSTALLATION

We adopted this way to install the Wazuh Server. This is a straightforward all-in-one installation and is suitable for small-scale deployments. The following steps are involved in the installation process:

1. Download and run the Wazuh installation assistant.

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

2. Once the assistant finishes, the output will display the access credentials and confirm successful installation.

```
INFO: --- Summary ---
INFO: You can access the web interface https://<wazuh-dashboard-ip>
User: admin
Password: <ADMIN_PASSWORD>
INFO: Installation finished.
```

Make sure to save the credentials for future usage. It will be used to access the dashboard.

3. Access the Wazuh web interface at https://<wazuh-dashboard-ip> using the provided credentials:

```
Username: admin
Password: <ADMIN_PASSWORD>
```

4. Upon first access, a browser warning about the certificate may appear. This is normal because the certificate was not issued by a recognized authority. You may accept the certificate as an exception or configure a certificate from a trusted authority.

5. The passwords for all Wazuh indexer and Wazuh API users can be found in the file named `wazuh-passwords.txt`, which is inside `wazuh-install-files.tar`. To display them, execute:

```
sudo tar -O -xvf wazuh-install-files.tar &&
↪  wazuh-install-files/wazuh-passwords.txt
```

6. To uninstall Wazuh's central components, execute the installation assistant with the option `-u` or `--uninstall`.

3.1.2 STEP-BY-STEP INSTALLATION OF THE WAZUH INDEXER, MANAGER AND DASHBOARD

Please refer to the Wazuh official documentation page for the step-by-step installation of the Wazuh Server components. This provides more in-depth insight and fine-grained control over different details of the installation process.

3.2 REGISTERING AGENTS

Registering new agents becomes way too easy once the server is set up. The procedure is stated as follows:

- Go to Agents → Deploy New Agent as shown in the following image:

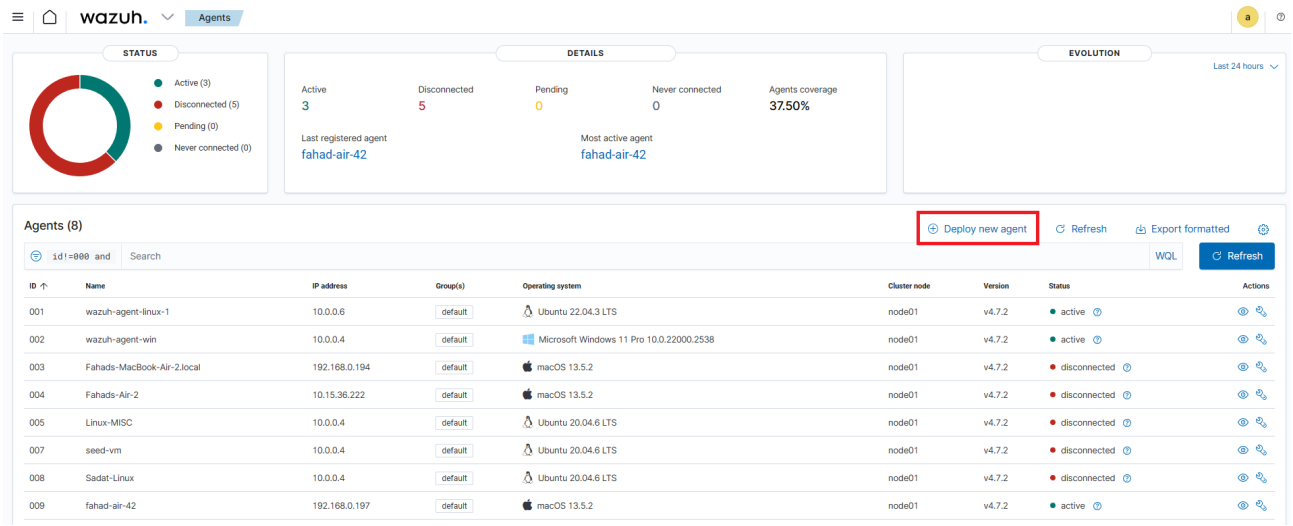

Figure 3: Wazuh Dashboard - Deploy New Agent

- There, provide the necessary information like Agent OS, Server address, Agent name and Agent group (last two are optional).

- Finally, two sets of commands will be shown, running which should be enough to install and initiate Wazuh Agent on the given machine.
  - **Linux:**

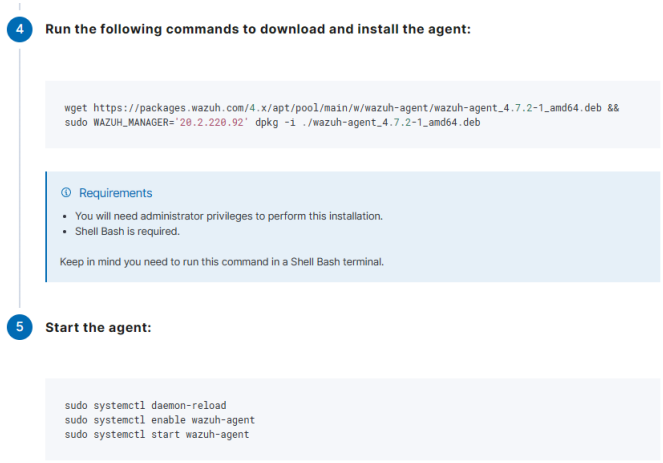

Figure 4: Wazuh Agent Installation Commands for a Linux Machine

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/waz⌋
↪  uh-agent_4.7.2-1_amd64.deb && sudo WAZUH_MANAGER='20.2.220.92'
↪  dpkg -i ./wazuh-agent_4.7.2-1_amd64.deb
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```

  - **MacOS:**

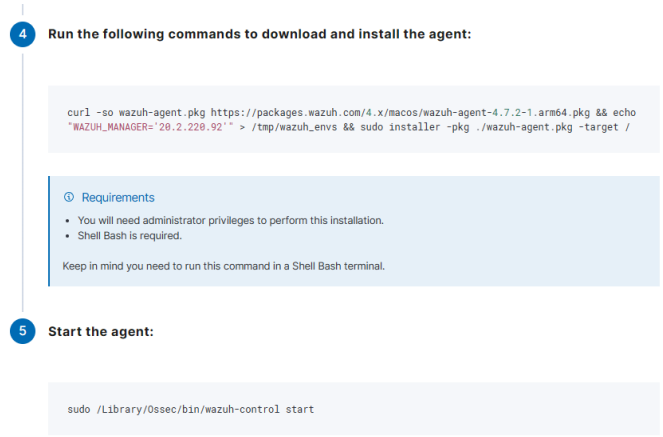

Figure 5: Wazuh Agent Installation Commands for a macOS Machine

```
curl -so wazuh-agent.pkg https://packages.wazuh.com/4.x/macos/wazuh
↪ -agent-4.7.2-1.arm64.pkg && echo "WAZUH_MANAGER='20.2.220.92'"
↪ > /tmp/wazuh_envs && sudo installer -pkg ./wazuh-agent.pkg
↪ -target /
sudo /Library/Ossec/bin/wazuh-control start
```

– **Windows:**

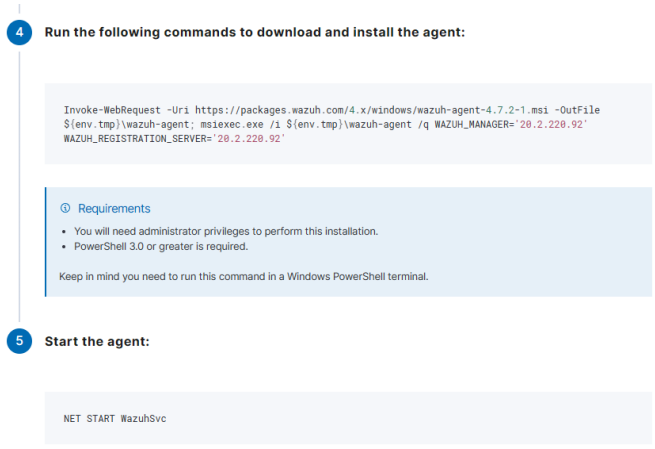

Figure 6: Wazuh Agent Installation Commands for a Windows Machine

```
Invoke-WebRequest -Uri
↪ https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.2-1.msi
↪ -OutFile ${env.tmp}\wazuh-agent; msiexec.exe /i
↪ ${env.tmp}\wazuh-agent /q WAZUH_MANAGER='20.2.220.92'
↪ WAZUH_REGISTRATION_SERVER='20.2.220.92'
NET START WazuhSvc
```

We installed all three types of agents, as said earlier. There were multiple iterations of setting up the agents. In some instances, the agent had to be reinstalled in the same device with a different name.

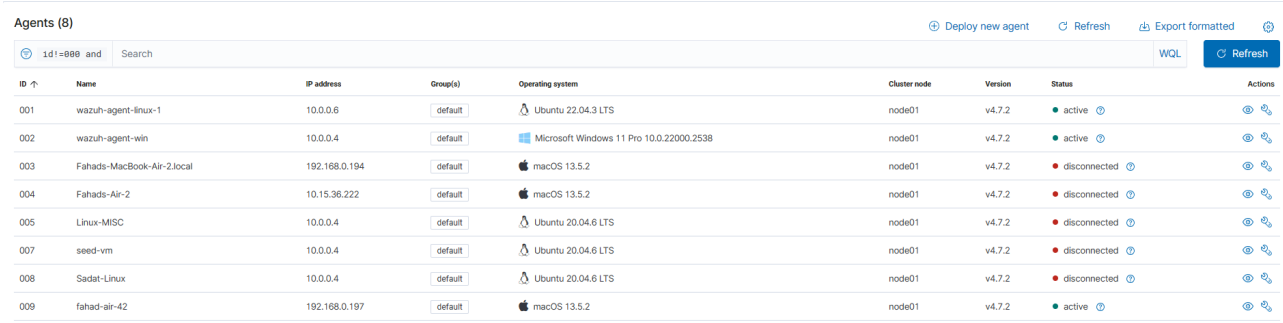

Figure 7: Installed Agents

Finally, we ended up working with the agent IDs as mentioned in 2.2.2.

4 WAZUH FEATURES AND USE-CASES

Wazuh provides several use-cases for monitoring the endpoints and data analysis. These include:

- Log collector
- Command execution
- File integrity monitoring (FIM)
- Security configuration assessment (SCA)
- System inventory
- Malware detection
- Active response
- Container security
- Cloud security

The following features have been explored in this report.