

Objectives

1. Install and configure a Security Information and Event Management (SIEM).
2. Use a SIEM to monitor changes made to files and folders.

Introduction

Wazuh is an open-source security platform that provides unified security monitoring threat detection and compliance management across different environments, such as on-premises, cloud and hybrid infrastructures. It is widely used for security operations, log analysis and monitoring of endpoints and applications.

Features of Wazuh

- 1. Host Based Intrusion Detection System (HIDS)**
Monitors endpoints for suspicious activities, unauthorised access and policy violations by analysing logs, file integrity and system configurations.
- 2. Log Data Analysis**
Collects, centralizes and analyses logs from various sources, including operation systems, applications and network devices to detect security treats.
- 3. Threat Detection and Response**
Identifies potential threats by correlation log data with security rules and external threat intelligence feeds
- 4. File Integrity Monitoring (FIM).**
Tracks changes in critical systems files and directories to detect unauthorised modifications or tempering.
- 5. Compliance Management**
Helps organisations meet regulatory and industry standards such as GDPR, HIPAA, to mention a few by providing security controls, reporting and monitoring.
- 6. Threat Intelligence Integration**
Leverages threat intelligence feeds to identify and respond to emerging threats
- 7. Agent Based Architecture**
Deploys lightweight agents on endpoints to monitor activities and enforce policies
- 8. Centralised Management**
Offers a user friendly interface for managing security events configuring and generating reports from centralised location.

Wazuh Architecture.

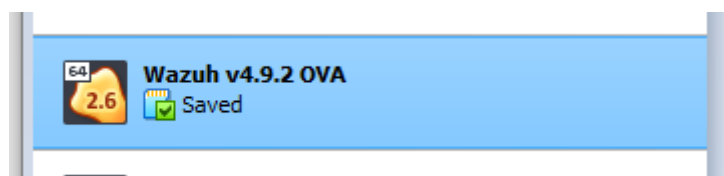
Wazuh typically operates as a three-tier system

1. **Agents:** Agents are installed on monitored devices to collect data
2. **Server:** Processes the data collected by agents, applies detection rules and generated alerts.
3. **Dashboard:** Web based interface for visualising alerts, logs and other security metrics

Installation and Configuring of Wazuh

Wazuh provides a pre-built virtual machine image (OVA) that you can directly import using VirtualBox or other OVA compatible virtualization systems. This can be found here [Installation alternatives · Wazuh documentation](#)

Download the **wazuh.x.x.x.ova** (x being the version of Wazuh) file on to your computer
Import the ova to the virtual environment (VirtualBox, VMware).



Once the importing is complete power on the machine. After boot up login with default credentials username **wazuh-user** password **wazuh**. For the dashboard login at the browser <https://<ipaddress of Wazuh server>> e.g. <https://172.20.10.4> for this demo

For security reason these credentials should be changed at the first opportunity. To the password of wazuh-user

```
[root@wazuh-server tools]#  
[root@wazuh-server tools]#  
[root@wazuh-server tools]# passwd wazuh-user  
Changing password for user wazuh-user.  
New password:  
Retype new password:  
Sorry, passwords do not match.  
new password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[root@wazuh-server tools]#
```

use the commands **sudo bash** to become root user

passwd wazuh-user to change the password enter the password again to confirm

To change the password for the admin, Navigate to the directory **/usr/share/wazuh-indexer/plugins/opensearch-security/tools** Run the script **wazuh-passwords-tools.sh** issue the command **bash wazuh-password-tool.sh -u admin -p <password>**

```
[root@wazuh-server tools]#  
[root@wazuh-server tools]# bash wazuh-passwords-tool.sh -u admin -p  
12/01/2025 17:22:35 INFO: updating the internal users.  
12/01/2025 17:22:38 INFO: A backup of the internal users has been saved in the /etc/wazuh-indexer/internalusers-backup folder.  
12/01/2025 17:22:38 INFO: Generating password hash  
12/01/2025 17:22:42 WARNING: The user and password configured in the filebeat.yml file will be updated and stored in Filebeat Keystore.  
12/01/2025 17:22:42 INFO: The filebeat.yml file has been updated to use the Filebeat Keystore username and password.  
12/01/2025 17:23:11 WARNING: Password changed. Remember to update the password in the Wazuh dashboard, Wazuh server, and Filebeat nodes if necessary, and restart the services.  
[root@wazuh-server tools]#  
[root@wazuh-server tools]#  
[root@wazuh-server tools]#  
[root@wazuh-server tools]#  
[root@wazuh-server tools]#  
[root@wazuh-server tools]#  
[root@wazuh-server tools]# pwd  
/usr/share/wazuh-indexer/plugins/opensearch-security/tools  
[root@wazuh-server tools]#
```

log out of the browser then log back in with the new password.

Installation and Configuring Wazuh Agent

On the device that wazuh server will be monitoring download the wazuh agent from [Wazuh agent - Installation guide · Wazuh documentation](#). Select the appropriate matching your OS. In this demo windows- download the windows installer. And install the agent make sure the check the box to run the installer at the finish stage of the installation.

In the space of Manager IP fill in the IP address of the wazuh server.

On the wazuh server the agent needs to be enrolled. Issue the command

/var/ossec/bin/manage_agents

- From the option select A to add/enrol and agent
- Enter the hostname and IP address of the device. Press enter to confirm the details entered

```
[wazuh-user@wazuh-server ~]$ sudo bash
[root@wazuh-server wazuh-user]#
[root@wazuh-server wazuh-user]# /var/ossec/bin/manage_agents

*****
* Wazuh v4.9.2 Agent manager.                *
* The following options are available:        *
*****
(A)dd an agent (A) .
(E)xtract key for an agent (E) .
(L)ist already added agents (L) .
(R)emove an agent (R) .
(Q)uit.
Choose your action: A,E,L,R or Q: A

- Adding a new agent (use '\q' to return to the main menu) .
Please provide the following:
  * A name for the new agent: WinSR-2019
  * The IP Address of the new agent: 172.20.10.3
```

Next a ssh key is required this is for authentication and allow communication between the wazuh server and the agent

To generate this key select E from the menu, Enter the ID number of the agent

```
*****
* Wazuh v4.9.2 Agent manager.                *
* The following options are available:        *
*****
(A)dd an agent (A) .
(E)xtract key for an agent (E) .
(L)ist already added agents (L) .
(R)emove an agent (R) .
(Q)uit.
Choose your action: A,E,L,R or Q: E

Available agents:
  ID: 001, Name: WinSR-2019, IP: 172.20.10.3
Provide the ID of the agent to extract the key (or '\q' to quit): 001

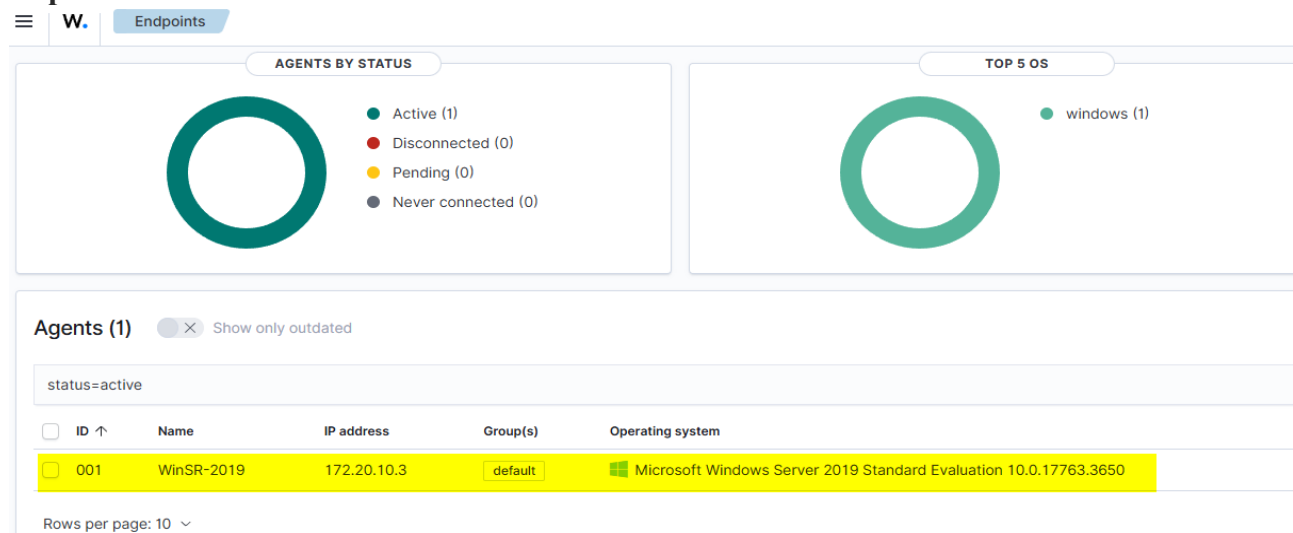
Agent key information for '001' is:
MDAxIFdpblNSLTiIwMTkgMTcyLjIwLjEwLjMgYjA4ZDJKMjZhNTRiYWRjOGVhYTB1ZjFiMTFhZmNlNGFh
N2MxMWRkNmRiYzY2ExNjc3MDg0NzY4MDhmOA==

** Press ENTER to return to the main menu.
```

Copy the key generated and paste it into the space on the wazuh agent configuration and save
Start the wazuh agent in the services

On the Wazuh server web browser, you should be able to see the device that has the agent installed

https://172.20.10.4



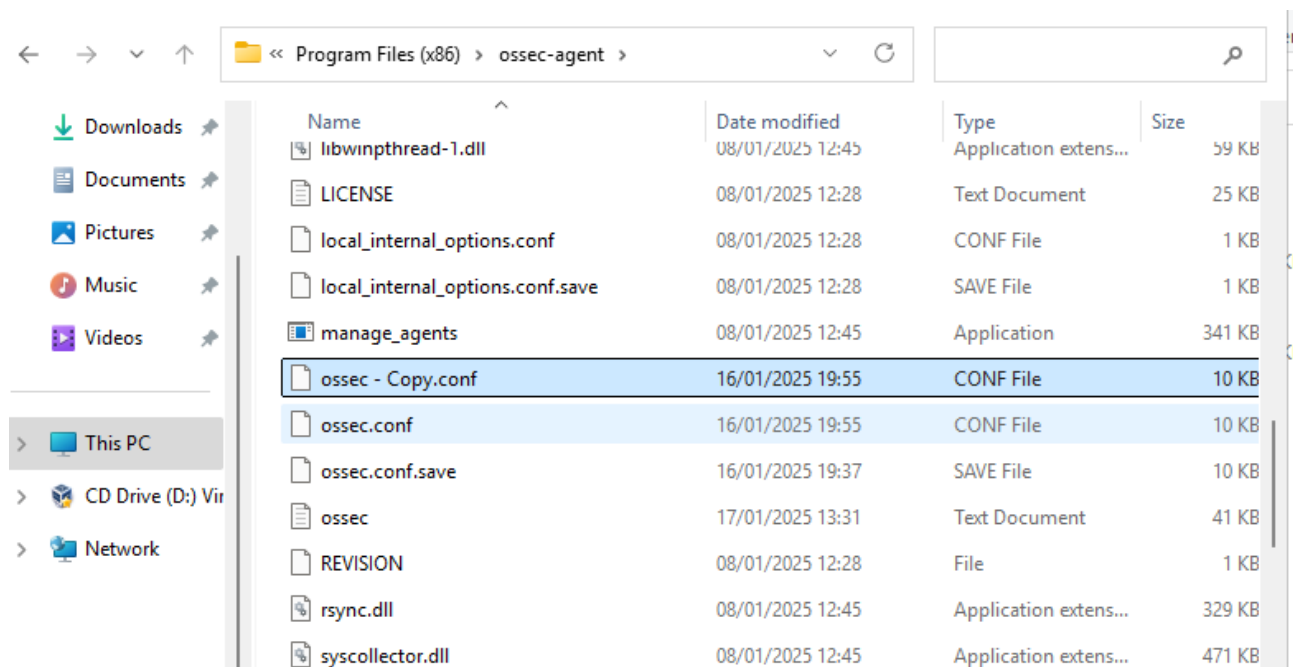
PART 2

File Integrity Management (FIM)

Wazuh can be used to monitor files that are on the device.

To configure FIM, on the device to be monitored navigate to **C:\Program Files (x86)\ossec-agent** and edit the file **ossec.conf**

Be sure to make a copy of the file before making any adjustments, This copy will act as backup in case errors in making the adjustment occurs.



Using Notepad++ or any other text editor scroll to the section where file integrity management begins

```
<!-- File integrity monitoring -->
<syscheck>

  <disabled>no</disabled>

  <!-- Frequency that syscheck is executed default every 12 hour
  <frequency>43200</frequency>

  <!-- Default files to be monitored. -->
  <directories recursion_level="0" restrict="regedit.exe$|system

  <directories recursion_level="0" restrict="at.exe$|attrib.exe$
  <directories recursion_level="0">%WINDIR%\SysNative\drivers\e
  <directories recursion_level="0" restrict="WMIC.exe$">%WINDIR
  <directories recursion_level="0" restrict="powershell.exe$">%
```

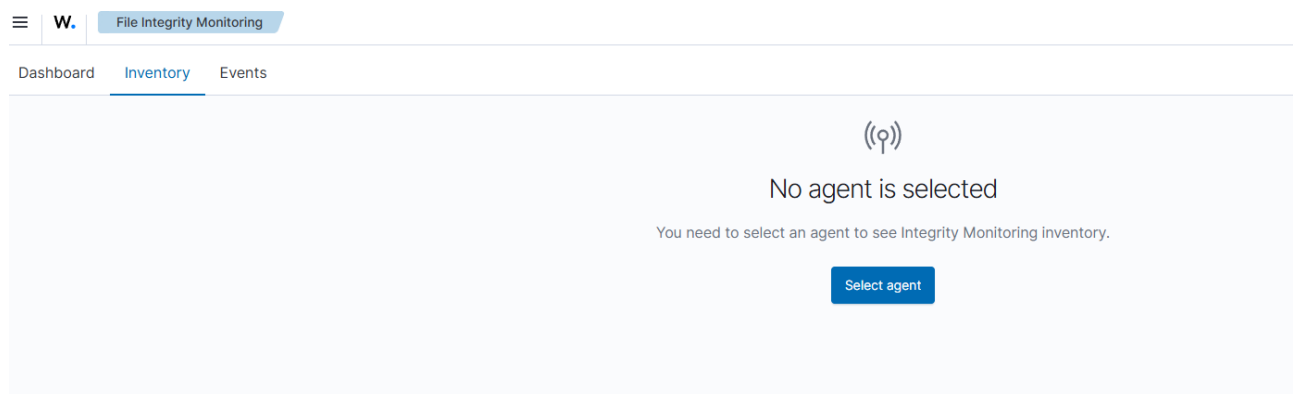
By default FIM is turned on the line **<disabled>no</disabled>**. The next line Frequency shows often File integrity management occurs. In this case 43200 sec equivalent to 12 hours. This can be adjusted so that FIM checks the files more regularly. It also could depend on the criticality of the documents.

For this demo, the folders under the public directory will be monitored for any addition, deletion or modification. Under **Default files to be monitored** add the line **C:\Users\Public**

```
76 <!-- Default files to be monitored. -->
77 <directories recursion_level="0" restrict="regedit.exe$|system.ini$
78 <directories>C:\Users\Public</directories>
79
```

Save and close the file. Restart the Wazuh service under services.

On the Wazuh navigate to File Integrity Management tab under inventory click on select agent and select the agent of the device on which FIM will monitor.



On the device on which FIM is configured after restarting the Wazuh service create folders/files in the Public directory or make some modifications. Then return to the Wazuh server in the File Integrity Management Tab under events any modifications an alert will be shown.

Document Details

[View surrounding documents](#)

[View single document](#)

TableJSON

t _index	wazuh-alerts-4.x-2025.01.17
t agent.id	003
t agent.ip	172.20.10.7
t agent.name	WinSR-2025
t decoder.name	syscheck_integrity_changed
t full_log	File 'c:\users\public\pictures\testing fim.txt' modified Mode: scheduled Changed attributes: size,mtime,md5,sha1,sha256 Size changed from '0' to '30' Old modification time was: '1737126091', now it is '1737128211' Old md5sum was: 'd41d8cd98f00b204e9800998ecf8427e' New md5sum is: '2a0764d7d8f9c23f5055687270hh27a0'
t id	1737128218.683100
t input.type	log

FIM can be configured to monitor the file in real-time so any changes made to the files are immediately highlighted in the Wazuh server.

To achieve this Windows Auditor in the local policy will need to be activated. By enabling this feature any adjustment will be monitored including who made the changes and what changes made.

Local Group Policy Editor

File Action View Help

Scripts (Startup/Shutdown)

Security Settings

- Account Policies
- Local Policies
- Windows Defender Firewall with Advanced Sec
- Network List Manager Policies
- Public Key Policies
- Software Restriction Policies
- Application Control Policies
- IP Security Policies on Local Computer
- Advanced Audit Policy Configuration
 - System Audit Policies - Local Group Policy
 - Account Logon
 - Account Management
 - Detailed Tracking
 - DS Access
 - Logon/Logoff
 - Object Access
 - Policy Change
 - Privilege Use
 - System
 - Global Object Access Auditing

Subcategory

Audit Application Generated

Audit Certification Services

Audit Detailed File Share

Audit File Share

Audit File System

Audit Filtering Platform Connection

Audit Filtering Platform Packet Drop

Audit Handle Manipulation

Audit Kernel Object

Audit Other Object Access Events

Audit Registry

Audit Removable Storage

Audit SAM

Audit Central Access Policy Staging

Audit Events

Not Configured

Not Configured

Not Configured

Not Configured

Success

Not Configured

Not Configured

Not Configured

Not Configured

Success

Not Configured

Not Configured

Not Configured

Not Configured

Not Configured

Ensure **Audit File system** and **Audit Handle Manipulation** have been configured to indicate “Success”



On the device edit the ossec.conf file adding the line **<whodata=”yes”>C:\Users\Public**

```
<disabled>no</disabled>

<!-- Frequency that syscheck is executed default every 12 hours -->
<frequency>10</frequency>

<!-- Default files to be monitored. -->
<directories recursion_level="0" restrict="regedit.exe|system.ini|win.ini">%WINDIR%</directories>
<directories whodata="yes">C:\Users\Public</directories>
```

Restart the Wazuh service and make modifications the folders. On the Wazuh server these changes will be indicated.

	Jan 17, 2025 @ 16:47:22.5...	WinSR-2025	c:\users\public\new text document.txt	deleted	File deleted.
	Jan 17, 2025 @ 16:47:22.5...	WinSR-2025	c:\users\public\tesing whodata.txt	added	File added to the system.
	Jan 17, 2025 @ 16:47:08.6...	WinSR-2025	c:\users\public\new text document.txt	added	File added to the system.

By selecting the occurrence in this case testing whodata.txt

Document Details

View surrounding documents 

Table	JSON
t _index	wazuh-alerts-4.x-2025.01.17
t agent.id	003
t agent.ip	172.20.10.7
t agent.name	WinSR-2025
t decoder.name	syscheck_new_entry
t full_log	File 'c:\users\public\tesing whodata.txt' added Mode: whodata
t id	1737132442.867705
t input.type	log
t location	syscheck
t manager.name	wazuh-server
t rule.description	File added to the system.

Lessons Learned

1. Install and Configure Wazuh server
3. Install wazuh agents to monitor Clients
4. Configure FIM to monitor any modifications of files and folders
5. Read alerts generated into Wazuh server