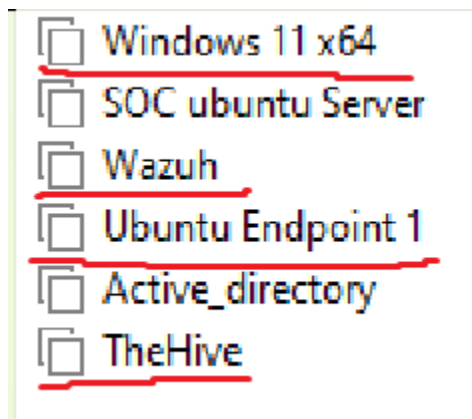


Before starting the installation of Wazuh, I went and created three separate VM's 3 linux, and 1 windows.

You're going to have a Wazuh manager, theHive Case Management, Linux and windows Endpoints. This will give a view on managing two different operating systems utilising Wazuh.



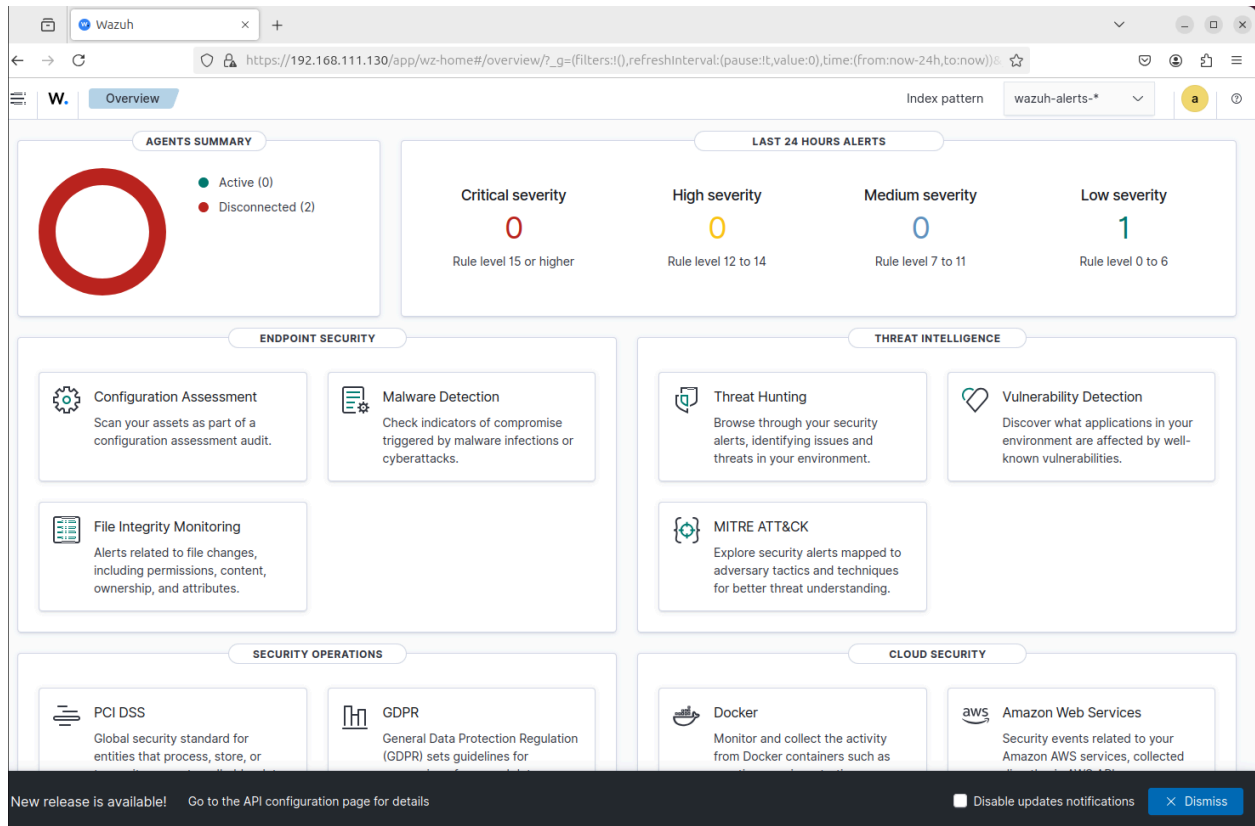
Setting up Wazuh is pretty easy, I've gone with the quickstart installation

<https://documentation.wazuh.com/current/quickstart.html>

After setting up for the wazuh manager for the linux machine you'll be shown a username and password on the terminal, it'll be something like this.

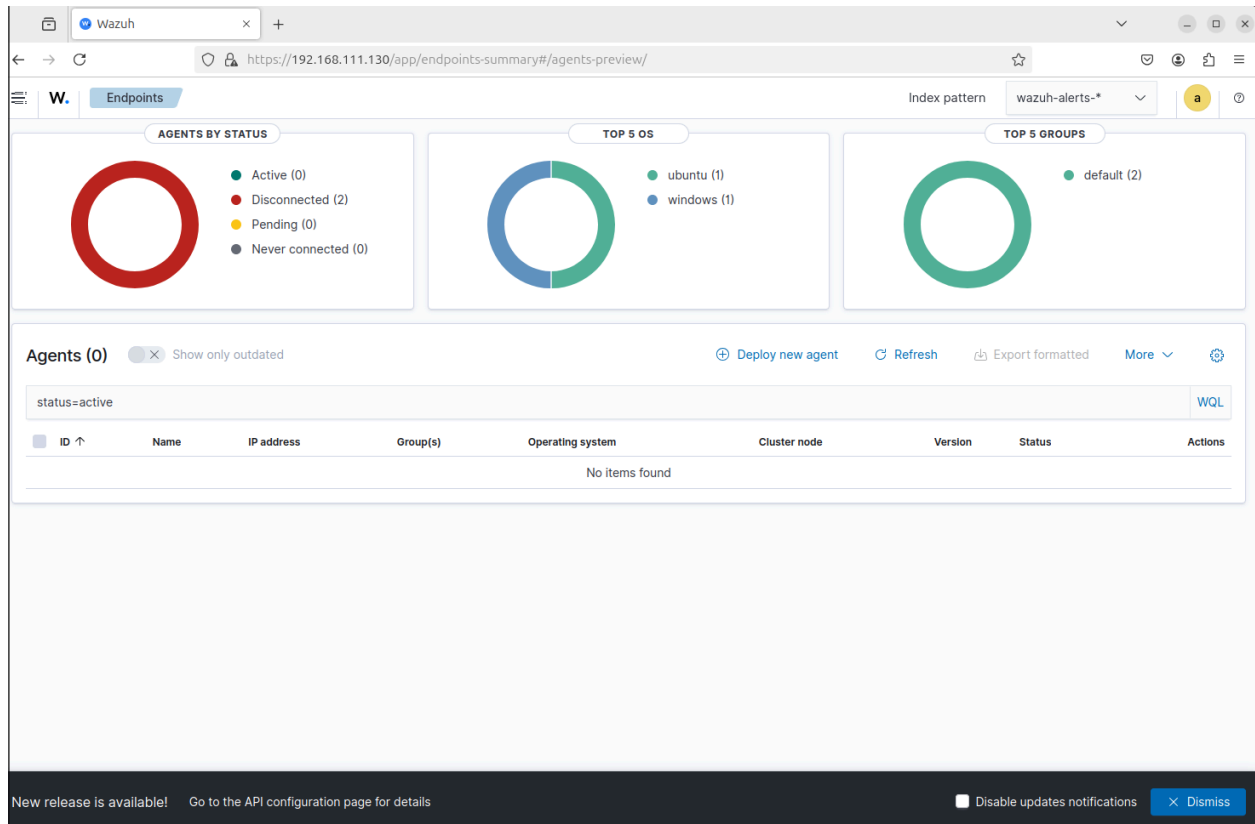
After installation go to wazuh dashboard in your preferred browser, this should be your local IP address which you would find with the command **ip addr**, and it usually the ens33 where you'll find your own IP address, Type this into the URL of your browser and you'll get the Wazuh dashboard if installation of wazuh manager is successful.

Login in with the credentials that was given before on the terminal and you'll be shown the dashboard



Most of the online tutorials that you use for Wazuh is going to have the old dashboard, it's going to look different and you may need to experiment around but majority of the task utilised in the tutorials will be in the threat Hunting section

Clicking on the agents summary you'll get moved into the endpoints section of wazuh.



Here is where you'll configure the agent to the specific operating system, so going ahead and clicking on the "deploy new agent"

Wazuh

https://192.168.111.130/app/endpoints-summary#/agents-preview/deploy

Endpoints Deploy new agent

Index pattern wazuh-alerts-\*

### Deploy new agent

**1 Select the package to download and install on your system:**

**LINUX**

☐ RPM amd64 ☐ RPM aarch64

☐ DEB amd64 ☐ DEB aarch64

**WINDOWS**

☐ MSI 32/64 bits

**macOS**

☐ Intel ☐ Apple silicon

[For additional systems and architectures, please check our documentation.](#)

**2 Server address:**

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).

**Assign a server address**

192.168.111.130

☒ Remember server address

**3 Optional settings:**

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

**Assign an agent name:**

depending upon what operating system you want to install the wazuh agent on, wazuh will have dedicated choices for its specific installation.

You're going to be prompted with a couple of options

**1 Select the package to download and install on your system:**

**LINUX**

☐ RPM amd64 ☐ RPM aarch64

☐ DEB amd64 ☐ DEB aarch64

**WINDOWS**

☐ MSI 32/64 bits

**macOS**

☐ Intel ☐ Apple silicon

[For additional systems and architectures, please check our documentation.](#)

this is for choosing your operating system

**2 Server address:**

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).

**Assign a server address**

192.168.111.130

☒ Remember server address

Pretty self explanatory, this simply just the IP address the wazuh agent is going to connect to, this should be your main host IP address like the one shown in the image, but the ip will need to be specific to yours

### 3 Optional settings:

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

Assign an agent name: ?

Agent name

ⓘ The agent name must be unique. It can't be changed once the agent has been enrolled. ↗

Select one or more existing groups: ?

Default

This step is optional but this will be the naming of the wazuh agent, and also the option of grouping it, say for example you have a large network of operating systems that specific to employees, you could put the new wazuh agent you're configuring into this group for better organisation when you need to access said agent.

### 4 Run the following commands to download and install the agent:

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.10.1-1_and64.deb && sudo WAZUH_MANAGER='192.168.111.138' dpkg -i ./wazuh-agent_4.10.1-1_and64.deb
```

#### ⓘ Requirements

- You will need administrator privileges to perform this installation.
- Shell Bash is required.

Keep in mind you need to run this command in a Shell Bash terminal.

### 5 Start the agent:

```
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```

lastly these two steps will be the installation and running of the wazuh agent to the system, you'll paste the commands into the operating system and it should connect to the wazuh manager

# Windows

For the windows side of configuration the installation will be about the same, but windows machine out of the package do not come with all the security log collection unless you install it and configure it to detect.

In your windows machine you must search up sysmon, which is a windows specific addon that extends the log collections and monitoring that default windows doesn't come with. installation is pretty easy, just go into sysmon windows and click the download and extract the zip file.

The screenshot shows the Microsoft Learn website for Sysmon v15.15. The page has a dark header with the text "Connect, code, and grow" and a "Register now" button. Below the header is a navigation bar with "Learn", "Discover", "Product documentation", "Development languages", and "Topics". The main content area is titled "Sysmon v15.15" and includes a "Filter by title" search bar. On the left, there is a sidebar with a tree view of Sysinternals tools, including "Sysmon". The main article content includes the title "Sysmon v15.15", the date "07/23/2024", and the number of contributors "8 contributors". It also features a "Feedback" button, a "Download Sysmon" button (4.6 MB), and a link to "Download Sysmon for Linux (GitHub)". The article text describes Sysmon as a Windows system service and device driver that monitors and logs system activity. It mentions that Sysmon collects events using Windows Event Collection or SIEM agents and analyzes them to identify malicious or anomalous activity. The article also includes a note that Sysmon does not provide analysis of the events it generates, nor does it attempt to hide itself from attackers. On the right side, there are "Additional resources" including a "Training" module titled "Connect Windows hosts to Microsoft Sentinel - Training" and a "Certification" link for "Microsoft Certified: Security Operations Analyst Associate - Certifications".

Sysmon also isn't configured but can be through adding additional rules. A great pre-made configuration by olafhartong - sysmon modular (<https://github.com/olafhartong/sysmon-modular>)

). By scrolling down and finding the sysmonconfig.xml file

.gitignore	revocation check added	7 years ago
Merge-SysmonXml.ps1	FileExeDetect added	2 years ago
README.md	Update README.md for V15	2 years ago
exclude_desktop_central.xml	exclude_desktop_central	3 years ago
license.md	Create license.md	7 years ago
merge_sysmon_configs.py	merge script now forces top level groupprelation=or	2 years ago
sysmonconfig-excludes-only.xml	Updated after successful CICD run 09/20/2023 07:33:02 UTC	2 years ago
sysmonconfig-mde-augment.xml	Updated after successful CICD run 09/20/2023 07:33:02 UTC	2 years ago
sysmonconfig-research.xml	adding reseach config	3 years ago
sysmonconfig-with-filedelete.xml	Updated after successful CICD run 09/20/2023 07:33:02 UTC	2 years ago
<b>sysmonconfig.xml</b>	Updated after successful CICD run 09/20/2023 07:33:02 UTC	2 years ago

README MIT license

## sysmon-modular | A Sysmon configuration repository for everybody to customise

license MIT maintained no! (as of 2023) last commit September 2023 Build Sysmon config with all modules no status Follow

51 ONLINE

This is a Microsoft Sysinternals Sysmon [download here](#) configuration repository, set up modular for easier maintenance and generation of specific configs.

Please keep in mind that any of these configurations should be considered a starting point, tuning per environment is **strongly** recommended.

**Note:** to get even more value out of the FileExecutable event, consider getting the most up to date version of the LOLdrivers config merged into the config as well. You can easily do that by grabbing the file and adding it in the 29\_file\_execute\_detected folder and generate a new config.

The sysmonconfig.xml within the repo is automatically generated after a successful merge by the PowerShell script and a successful load by Sysmon in an Azure Pipeline run. More info on how to generate a custom config.

You'll get this beautiful config file in which you'll need to save the raw file of this config to be inserted into your windows sysmon, as said by the creator of the github, the sysmon config he created is just a starting point and should be fine tuned to the environment you are using as there are many blindspots or areas he decided not to look into.





```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Valer> cd .\Downloads\
PS C:\Users\Valer\Downloads> ls

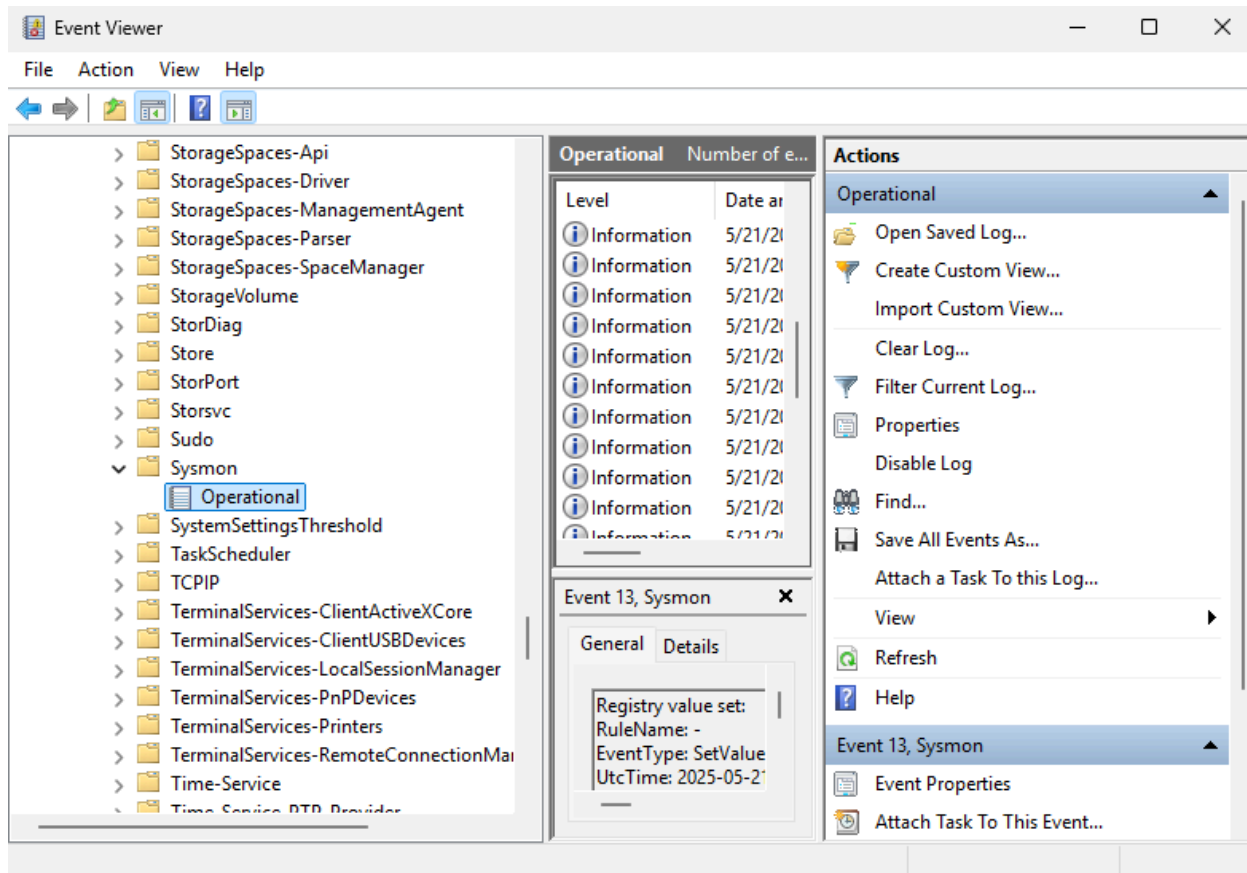
Directory: C:\Users\Valer\Downloads

Mode                LastWriteTime         Length Name
----                -
d-----          5/21/2025   4:27 AM              Sysmon
-a-----          5/21/2025   4:02 AM        4866436 Sysmon.zip

PS C:\Users\Valer\Downloads> cd .\Sysmon\
PS C:\Users\Valer\Downloads\Sysmon> .\Sysmon64.exe -i .\sysmonconfig.xml
```

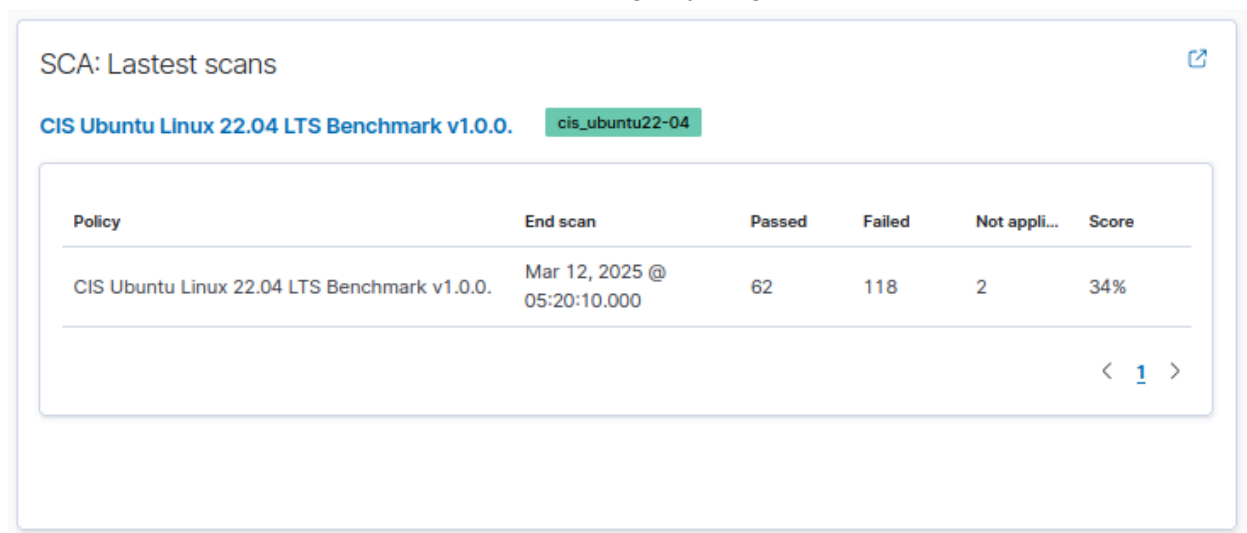
I'm going to assume you understand the difference between relative and absolute path, but for easy of use cause I'm lazy, I manually put the sysmonconfig.xml file in the sysmon folder because I wasn't bothered typing the entire path. But through this it'll tell sysmon to use this configuration, if done currently you'll be prompted by a EULA and it'll install. To confirm the service is running run event viewer on windows

event viewer > Applications and services log > Microsoft > Sysmon



## Troubleshooting.

There is a problem with the sca scan not showing anything



The Sca scan would be found where the **image before**, if there is nothing being shown like the image above. This could possibly be the configuration on the wazuh agent end, as wazuh needs

the precise operating. The solution is found by Wesly Khanh  
<https://groups.google.com/g/wazuh/c/cUjlf6g01Vk>

By going onto the wazuh agent operating system which mine is going to be linux, but the file is the same as windows so this problem will occur if the specific operating system for windows isn't the same as describe for example, the configuration file has windows 11 pro instead of windows 11 home

```
root@endpoint-1-VMware-Virtual-Platform:/var/ossec/ruleset/sca# pwd
/var/ossec/ruleset/sca
```

so having root access you want to go to this command `/var/ossec/ruleset/sca`

```
root@endpoint-1-VMware-Virtual-Platform:/var/ossec/ruleset/sca# ls
cis_ubuntu22-04.yml
```

once you ls you'll see the specific yaml file that is installed when you installed the wazuh agent, you'll want to edit this file with your choice of editor.

```
20 requirements:
21   title: "Check Ubuntu version."
22   description: "Requirements for running the SCA scan against Ubuntu Linux 22.04 LTS"
23   condition: all
24   rules:
25     - "f:/etc/os-release -> r:Ubuntu 24.04"
26     - "f:/proc/sys/kernel/ostype -> Linux"
27
```

On line 25, you'll want to change the os-release to your specific operating system, in the image above it has been changed already but originally it was **r:Ubuntu 24.02** instead of being **r:Ubuntu 24.04**. After you've made the changes you'll want to restart the wazuh agent with **systemctl restart wazuh-agent**