Wazuh Deployment in Docker – Windows System

Objective: This project demonstrates hands-on SIEM experience by deploying Wazuh using Docker, onboarding endpoints, collecting logs, and investigating security alerts relevant to a SOC environment.

Tool Explanation: Wazuh is a platform (Security Information and Event Management) which provides XDR (Extended Detection and response) to protect cloud, container, and server workloads. Features include:

- Log Data Analysis
- Intrusion Detection
- Malware Detection
- Configuration management
- Vulnerability Detection
- Regulatory Compliance Support

Wazuh has a multi-platform Wazuh agent and 3 main components:

- Wazuh Server: Analyzes data received from the agent, processes through decoders and rules.
- Wazuh Indexer: Storage room – Stores all data and alerts, makes data fast to search.
- Wazuh Dashboard: A web interface which displays alerts, graphs, security status.

Simple understanding:

Easy analogy (real-life example)

House security system:

- **Agent** = Cameras & sensors in rooms
- **Server** = Control center that checks alarms
- **Indexer** = Recorded footage storage
- **Dashboard** = Monitor screen for the guard

How everything works together

1. Agent watches the computer
2. Agent sends data → Server
3. Server analyzes → sends results
4. Indexer stores the data
5. Dashboard shows it to you

Prerequisite

- Docker Desktop
- Git for windows
- Minimum 4 GB ram
- 10 GB free disk space

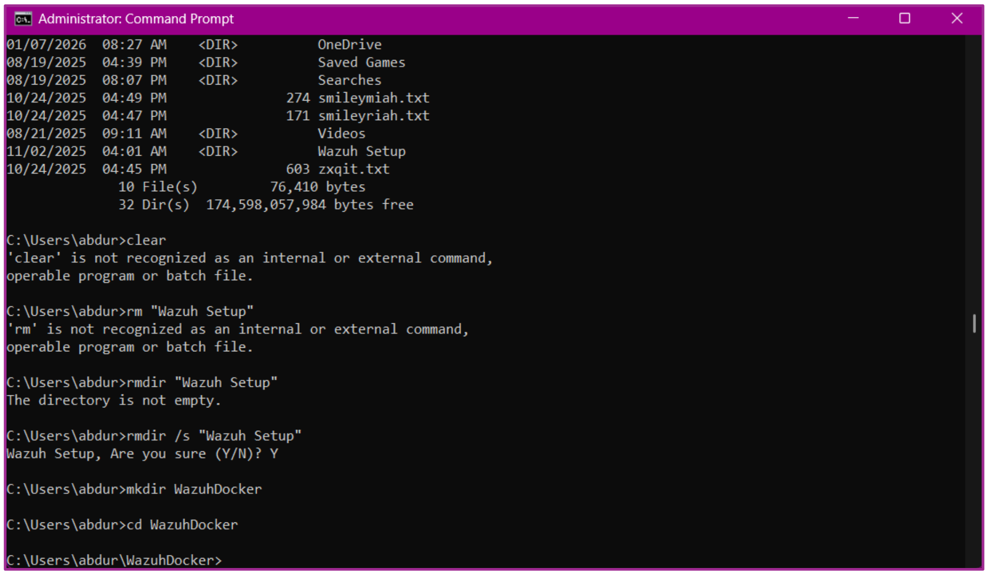
Deployment Choice: Docker – Single node stack

A single-node deployment runs all Wazuh central components on **one host** using Docker containers. Each core component runs in its own container, but all containers **share the same** underlying system resources.

Let’s move on to deployment:

Step 1: Open CMD as administrator.

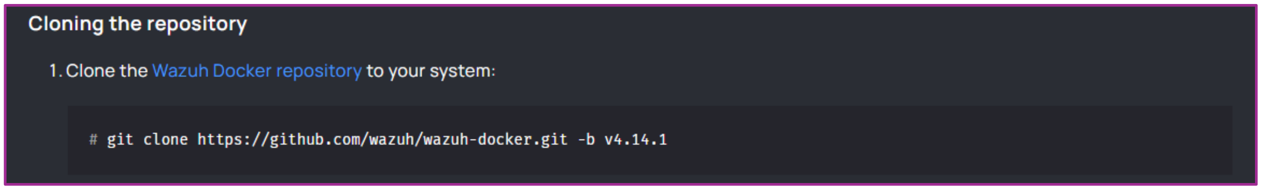
Step 2: Create a folder, for this task I named a folder ‘WazuhDocker’



```
01/07/2026  08:27 AM    <DIR>          OneDrive
08/19/2025  04:39 PM    <DIR>          Saved Games
08/19/2025  08:07 PM    <DIR>          Searches
10/24/2025  04:49 PM               274 smileymiah.txt
10/24/2025  04:47 PM               171 smileyriah.txt
08/21/2025  09:11 AM    <DIR>          Videos
11/02/2025  04:01 AM    <DIR>          Wazuh Setup
10/24/2025  04:45 PM               603 zxqit.txt
              10 File(s)         76,410 bytes
              32 Dir(s)  174,598,057,984 bytes free

C:\Users\abdur>clear
'clear' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\abdur>rm "Wazuh Setup"
'rm' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\abdur>rmdir "Wazuh Setup"
The directory is not empty.

C:\Users\abdur>rmdir /s "Wazuh Setup"
Wazuh Setup, Are you sure (Y/N)? Y

C:\Users\abdur>mkdir WazuhDocker

C:\Users\abdur>cd WazuhDocker

C:\Users\abdur\WazuhDocker>
```

Step 3: In Wazuh documentation scroll down and copy the '**Clone the repository**' code and paste it in CMD.

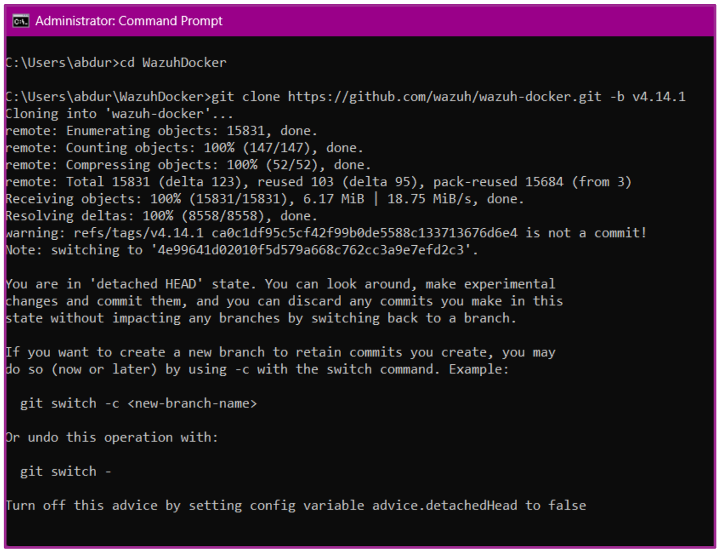
Link: *https://documentation.wazuh.com/current/deployment-options/docker/wazuh-container.html*



Cloning the repository

1. Clone the Wazuh Docker repository to your system:

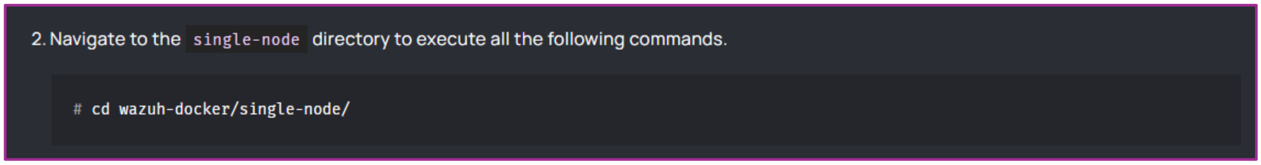
```
# git clone https://github.com/wazuh/wazuh-docker.git -b v4.14.1
```



Administrator: Command Prompt

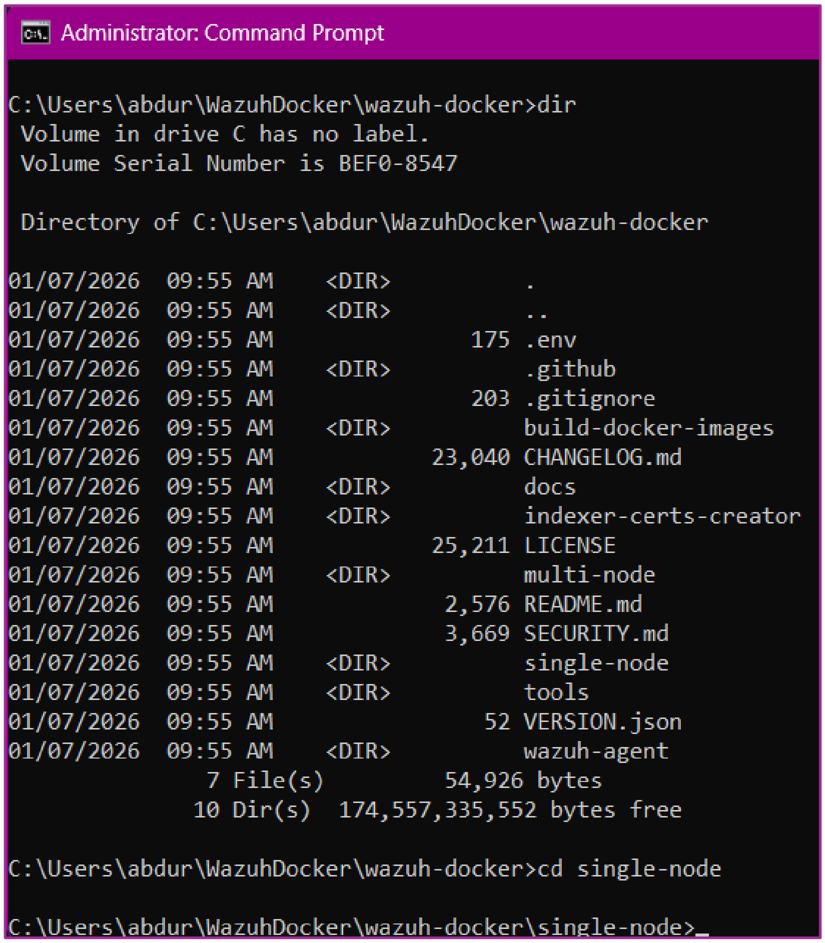
```
C:\Users\abdur>cd WazuhDocker

C:\Users\abdur\WazuhDocker>git clone https://github.com/wazuh/wazuh-docker.git -b v4.14.1
Cloning into 'wazuh-docker'...
remote: Enumerating objects: 15831, done.
remote: Counting objects: 100% (147/147), done.
remote: Compressing objects: 100% (52/52), done.
remote: Total 15831 (delta 123), reused 103 (delta 95), pack-reused 15684 (from 3)
Receiving objects: 100% (15831/15831), 6.17 MiB | 18.75 MiB/s, done.
Resolving deltas: 100% (8558/8558), done.
warning: refs/tags/v4.14.1 ca0c1df95c5cf42f99b0de5588c133713676d6e4 is not a commit!
Note: switching to '4e99641d02010f5d579a668c762cc3a9e7efd2c3'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to false
```

Step 4: After the repository cloning is done, Enter the folder and look for '**single-node**' folder then go inside the folder.



2. Navigate to the `single-node` directory to execute all the following commands.

```
# cd wazuh-docker/single-node/
```



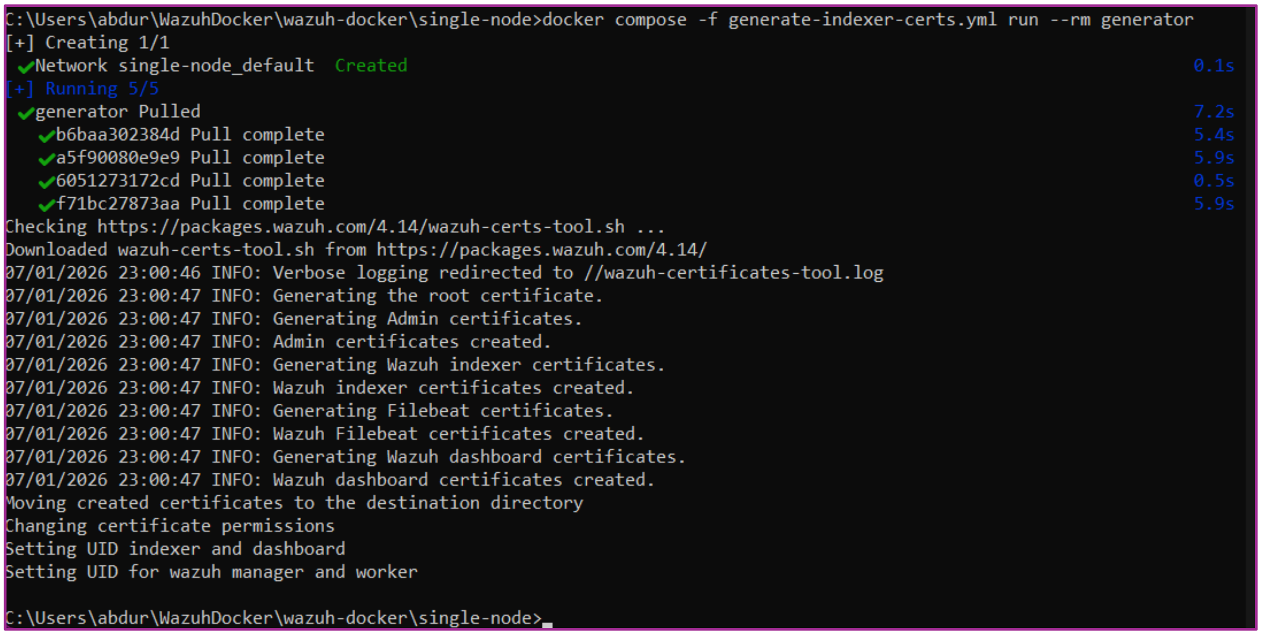
```
C:\Users\abdur\WazuhDocker\wazuh-docker>dir
 Volume in drive C has no label.
 Volume Serial Number is BEF0-8547

 Directory of C:\Users\abdur\WazuhDocker\wazuh-docker

01/07/2026  09:55 AM    <DIR>          .
01/07/2026  09:55 AM    <DIR>          ..
01/07/2026  09:55 AM               175 .env
01/07/2026  09:55 AM    <DIR>          .github
01/07/2026  09:55 AM               203 .gitignore
01/07/2026  09:55 AM    <DIR>          build-docker-images
01/07/2026  09:55 AM            23,040 CHANGELOG.md
01/07/2026  09:55 AM    <DIR>          docs
01/07/2026  09:55 AM    <DIR>          indexer-certs-creator
01/07/2026  09:55 AM            25,211 LICENSE
01/07/2026  09:55 AM    <DIR>          multi-node
01/07/2026  09:55 AM             2,576 README.md
01/07/2026  09:55 AM             3,669 SECURITY.md
01/07/2026  09:55 AM    <DIR>          single-node
01/07/2026  09:55 AM    <DIR>          tools
01/07/2026  09:55 AM                52 VERSION.json
01/07/2026  09:55 AM    <DIR>          wazuh-agent
               7 File(s)         54,926 bytes
              10 Dir(s)  174,557,335,552 bytes free

C:\Users\abdur\WazuhDocker\wazuh-docker>cd single-node

C:\Users\abdur\WazuhDocker\wazuh-docker\single-node>_
```

Step 5: Certificate generation - To secure communication between nodes in the Wazuh stack, certificates must be created and configured for each node. There are two simple options available:

- Wazuh self-signed certificates – Recommended for quick setup and testing.
- Your own certificates – Use certificates issued by your organization or a trusted Certificate Authority.

Enter the command to generate a **Wazuh self-signed certificate:**

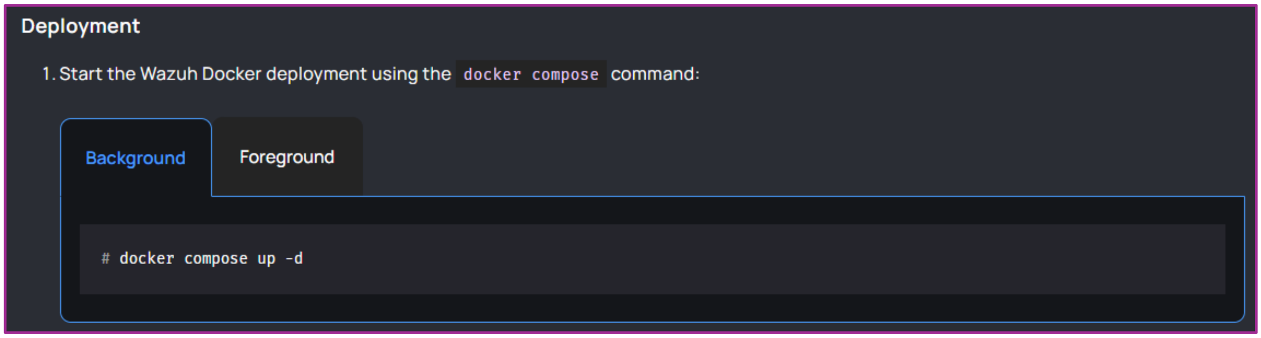
```
docker compose -f generate-indexer-certs.yml run --rm generator
```



```
C:\Users\abdur\WazuhDocker\wazuh-docker\single-node>docker compose -f generate-indexer-certs.yml run --rm generator
[+] Creating 1/1
 ✓Network single-node_default  Created                                                                          0.1s
[+] Running 5/5
 ✓generator Pulled                                                                                              7.2s
   ✓b6baa302384d Pull complete                                                                                  5.4s
   ✓a5f90080e9e9 Pull complete                                                                                  5.9s
   ✓6051273172cd Pull complete                                                                                  0.5s
   ✓f71bc27873aa Pull complete                                                                                  5.9s
Checking https://packages.wazuh.com/4.14/wazuh-certs-tool.sh ...
Downloaded wazuh-certs-tool.sh from https://packages.wazuh.com/4.14/
07/01/2026 23:00:46 INFO: Verbose logging redirected to //wazuh-certificates-tool.log
07/01/2026 23:00:47 INFO: Generating the root certificate.
07/01/2026 23:00:47 INFO: Generating Admin certificates.
07/01/2026 23:00:47 INFO: Admin certificates created.
07/01/2026 23:00:47 INFO: Generating Wazuh indexer certificates.
07/01/2026 23:00:47 INFO: Wazuh indexer certificates created.
07/01/2026 23:00:47 INFO: Generating Filebeat certificates.
07/01/2026 23:00:47 INFO: Wazuh Filebeat certificates created.
07/01/2026 23:00:47 INFO: Generating Wazuh dashboard certificates.
07/01/2026 23:00:47 INFO: Wazuh dashboard certificates created.
Moving created certificates to the destination directory
Changing certificate permissions
Setting UID indexer and dashboard
Setting UID for wazuh manager and worker

C:\Users\abdur\WazuhDocker\wazuh-docker\single-node>
```

Step 6: Let's Launch Wazuh env using the command

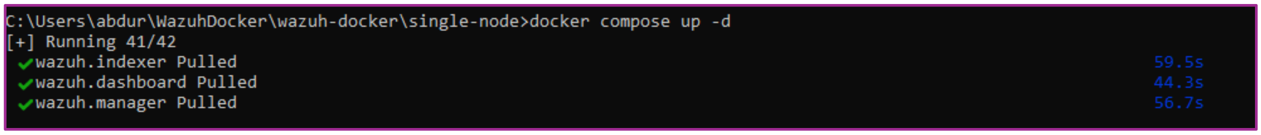
```
docker compose up -d
```



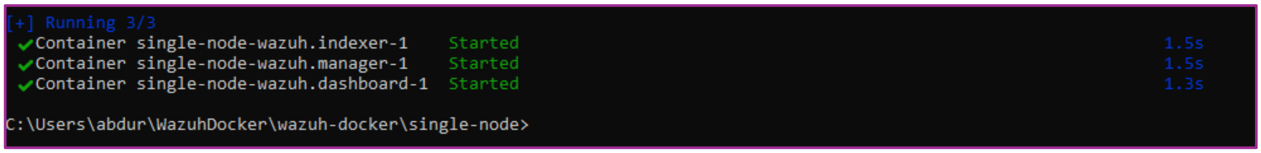
Deployment

1. Start the Wazuh Docker deployment using the `docker compose` command:

```
# docker compose up -d
```



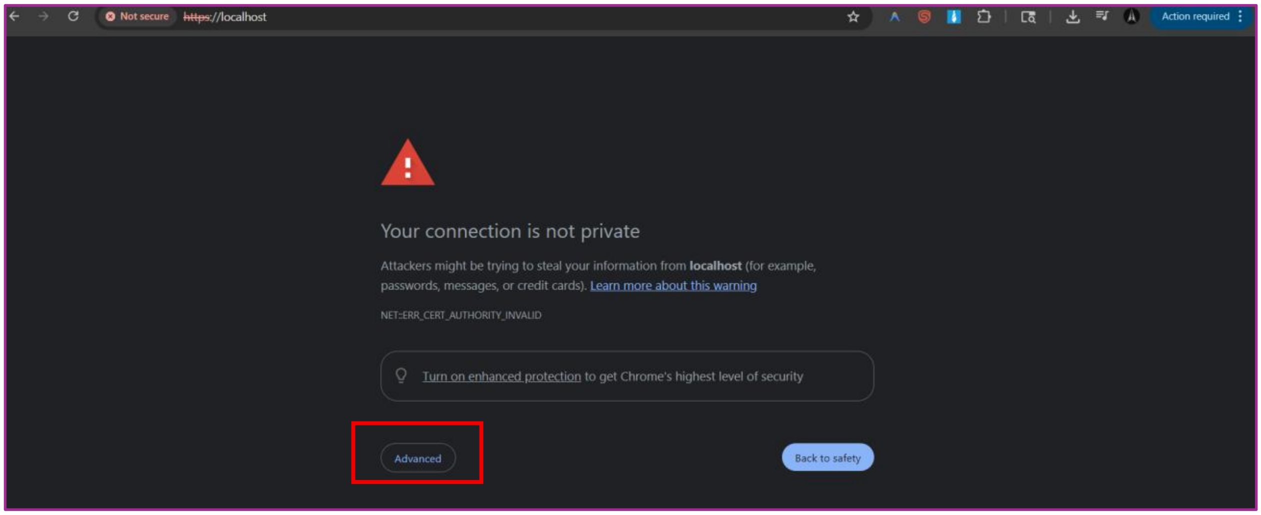
```
C:\Users\abdur\WazuhDocker\wazuh-docker\single-node>docker compose up -d
[+] Running 41/42
 ✓wazuh.indexer Pulled                                                                                       59.5s
 ✓wazuh.dashboard Pulled                                                                                     44.3s
 ✓wazuh.manager Pulled                                                                                       56.7s
```



```
[+] Running 3/3
 ✓Container single-node-wazuh.indexer-1    Started                                                            1.5s
 ✓Container single-node-wazuh.manager-1    Started                                                            1.5s
 ✓Container single-node-wazuh.dashboard-1  Started                                                            1.3s

C:\Users\abdur\WazuhDocker\wazuh-docker\single-node>
```

Step 7: In a browser, search https://localhost

You will be given a connection not being private error, this is normal as we are running Wazuh in docker locally.



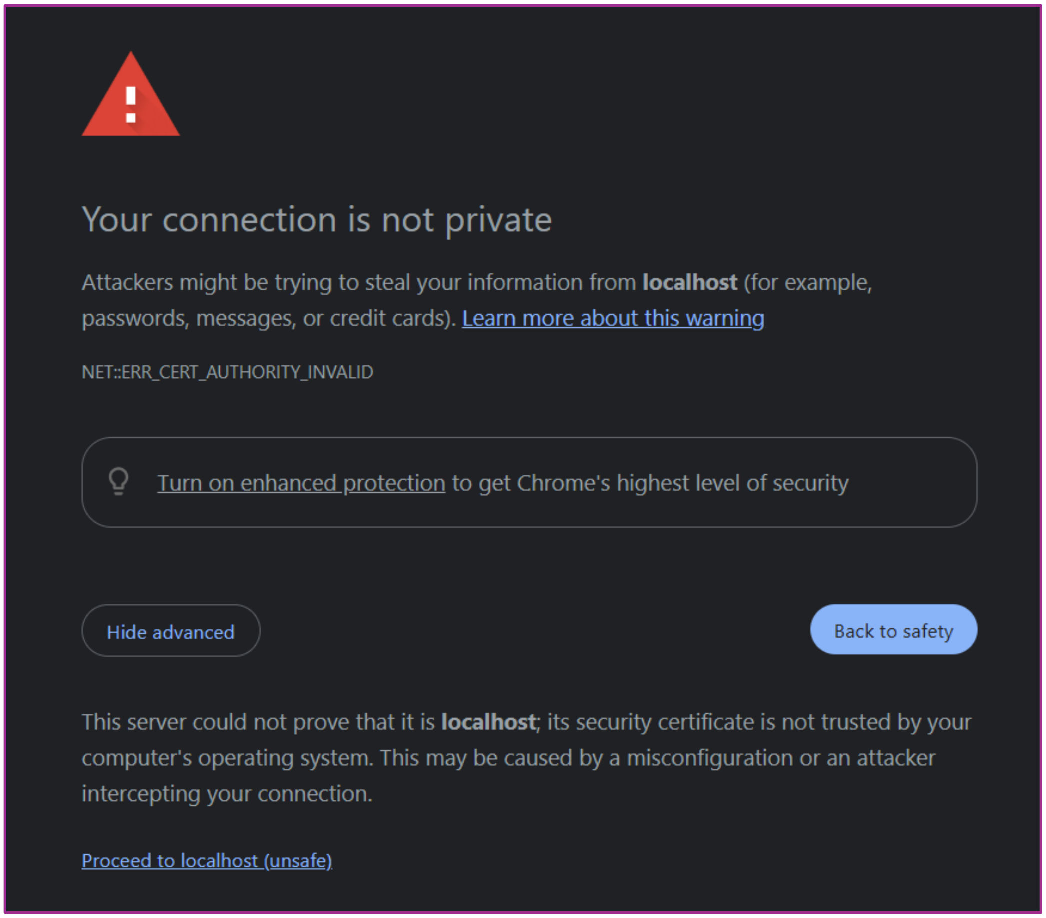
Your connection is not private

Attackers might be trying to steal your information from **localhost** (for example, passwords, messages, or credit cards). Learn more about this warning

NET::ERR_CERT_AUTHORITY_INVALID

Turn on enhanced protection to get Chrome's highest level of security

Click on Advanced – Proceed to localhost (unsafe)



Your connection is not private

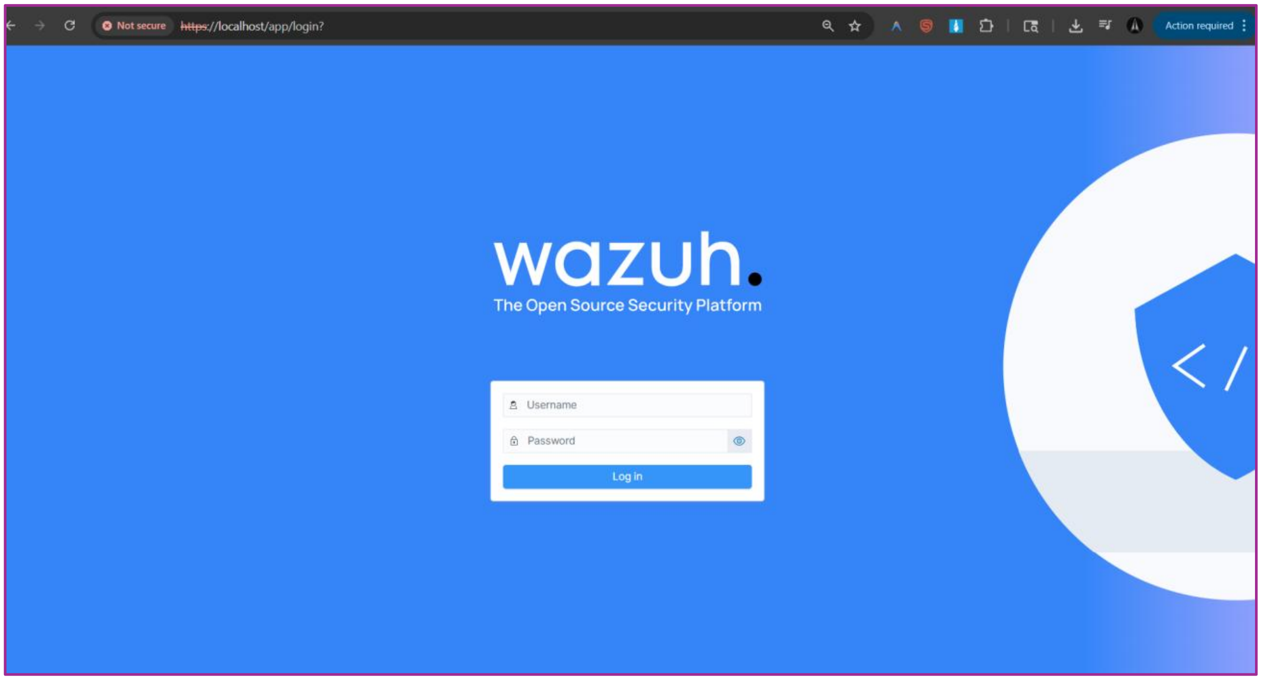
Attackers might be trying to steal your information from **localhost** (for example, passwords, messages, or credit cards). Learn more about this warning

NET::ERR_CERT_AUTHORITY_INVALID

Turn on enhanced protection to get Chrome's highest level of security

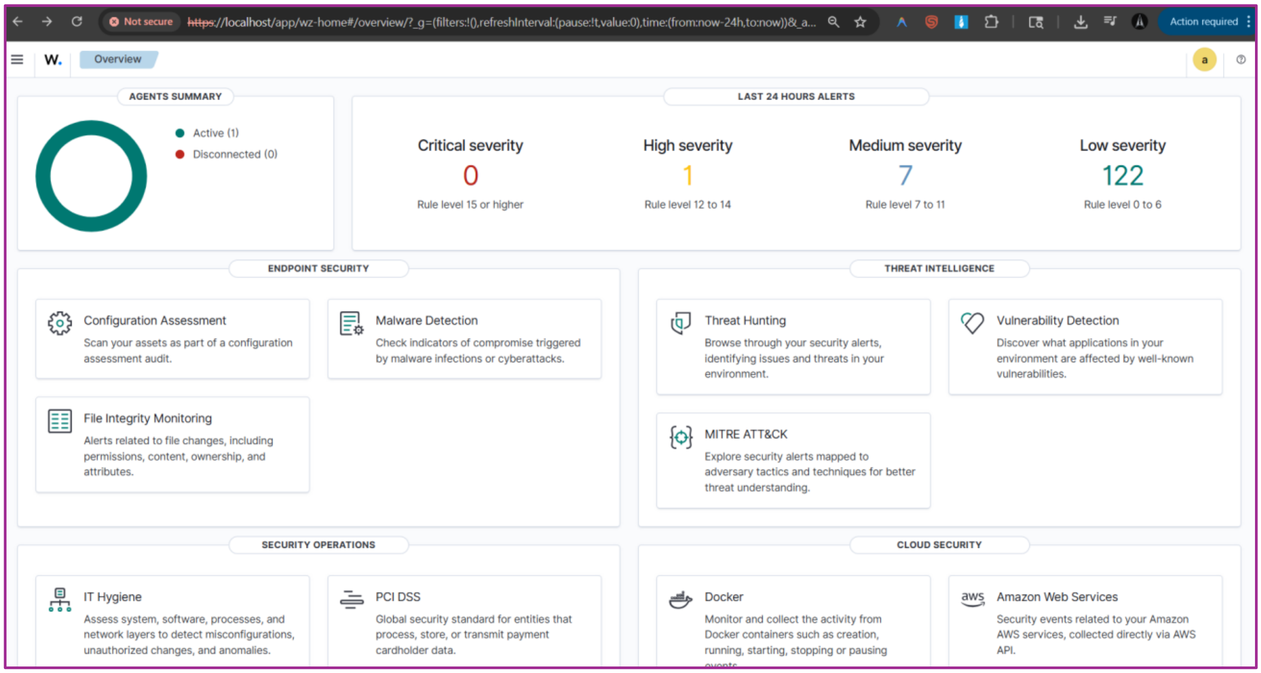
This server could not prove that it is **localhost**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to localhost (unsafe)


Not secure
https://localhost/app/login?
Action required
wazuh.
The Open Source Security Platform
Username
Password
Log in

Success in deploying Wazuh in docker, now log into Wazuh using default credentials – provided in the documentation.

Wazuh Successfully deployed in docker.


Not secure
https://localhost/app/wz-home#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a...
Action required
W.
Overview
a

AGENTS SUMMARY

● Active (1)
● Disconnected (0)

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	1	7	122
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	Rule level 0 to 6

ENDPOINT SECURITY

Configuration Assessment
Scan your assets as part of a configuration assessment audit.

Malware Detection
Check indicators of compromise triggered by malware infections or cyberattacks.

File Integrity Monitoring
Alerts related to file changes, including permissions, content, ownership, and attributes.

THREAT INTELLIGENCE

Threat Hunting
Browse through your security alerts, identifying issues and threats in your environment.

Vulnerability Detection
Discover what applications in your environment are affected by well-known vulnerabilities.

MITRE ATT&CK
Explore security alerts mapped to adversary tactics and techniques for better threat understanding.

SECURITY OPERATIONS

IT Hygiene
Assess system, software, processes, and network layers to detect misconfigurations, unauthorized changes, and anomalies.

PCI DSS
Global security standard for entities that process, store, or transmit payment cardholder data.

CLOUD SECURITY

Docker
Monitor and collect the activity from Docker containers such as creation, running, starting, stopping or pausing events.

Amazon Web Services
Security events related to your Amazon AWS services, collected directly via AWS API.

Next: Agent Deployment