WAZUH

Quick Start Guide for Installing and Configuring Your Wazuh Server

Created by **Amir Raza**

Follow me: https://www.linkedin.co/ in/amirsoc

Wazuh Server Installation and Agent Onboarding

1. Introduction

This document provides a simple and clear quick start guide for installing the Wazuh security platform on a single host and connecting a Kali Linux machine as an agent. The goal is to help you understand how to set up Wazuh for system monitoring, log analysis, and threat detection.

2. What is Wazuh?

Wazuh is an open-source security platform that combines XDR (Extended Detection and Response) and SIEM (Security Information and Event Management) capabilities. It helps organizations monitor and protect their endpoints and cloud workloads.

Wazuh is composed of the following components:

- **Wazuh Server:** Manages security policies and collects data from agents.
- **Wazuh Indexer:** Stores and organizes collected logs for analysis.
- **Wazuh Dashboard:** Web interface to view and manage alerts, visualizations, and data.
- **Wazuh Agent:** Installed on endpoints (like Kali Linux) to send data to the server.

Wazuh is completely free and open-source, licensed under GNU GPLv2 and Apache License 2.0.

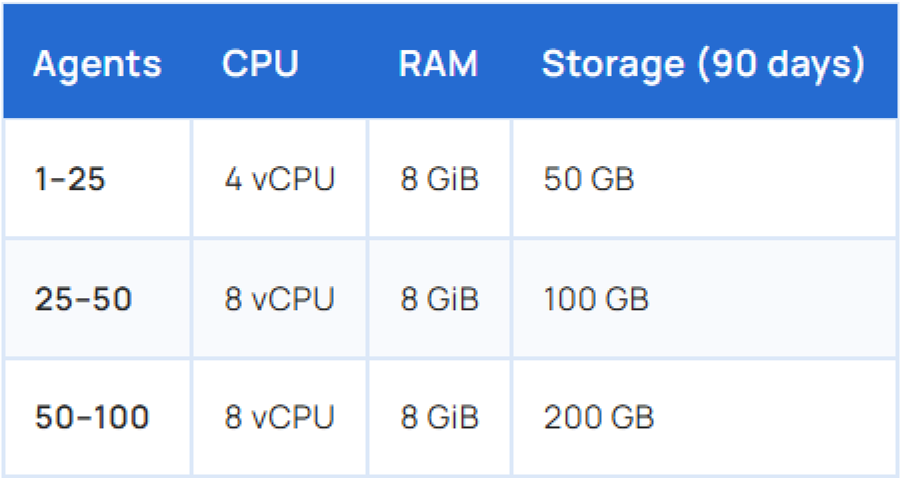
3. Purpose of This Guide

This guide uses the Wazuh "Quick Start" installation method, which sets up all main components on a single machine using an installation assistant script. This is the easiest and fastest way to deploy Wazuh for testing or small environments.

4. System Requirements

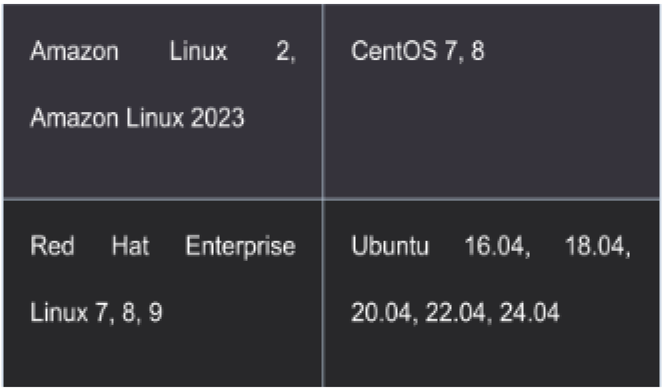
Before installation, ensure your system meets the following minimum requirements:

Hardware:



Agents	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

Supported Operating Systems:



Amazon Linux 2, Amazon Linux 2023	CentOS 7, 8
Red Hat Enterprise Linux 7, 8, 9	Ubuntu 16.04, 18.04, 20.04, 22.04, 24.04

- Ubuntu 20.04 / 22.04
- Debian 10 / 11
- CentOS 7 / 8
- Rocky Linux
- Amazon Linux 2

Installation Overview

The Quick Start method installs the following components:

- Wazuh Server
- Wazuh Indexer (OpenSearch)
- Wazuh Dashboard
- Filebeat (for log forwarding)

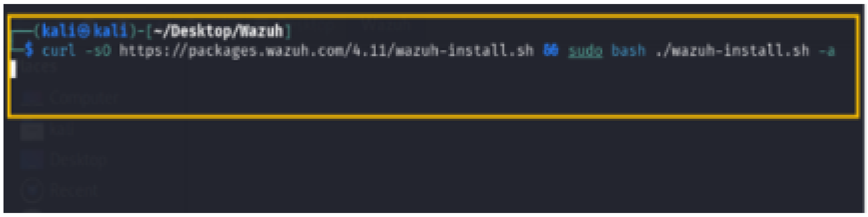
The installation assistant simplifies the process by installing and configuring everything automatically on one host.

Installing Wazuh

Download and run the Wazuh installation assistant

Using given below command:

curl -sO https://packages.wazuh.com/4.11/wazuh-install.sh && sudo bash ./wazuh-install.sh -a



```
┌──(kali㉿kali)-[~/Desktop/Wazuh]
└─$ curl -sO https://packages.wazuh.com/4.11/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

Wait Until Completion:

```
INFO: --- Summary —

INFO: You can access the web interface https://<WAZUH_DASHBOARD_IP_ADDRESS>

    User: admin

   Password: <ADMIN_PASSWORD>

INFO: Installation finished.
```

Access the Wazuh Interface with:

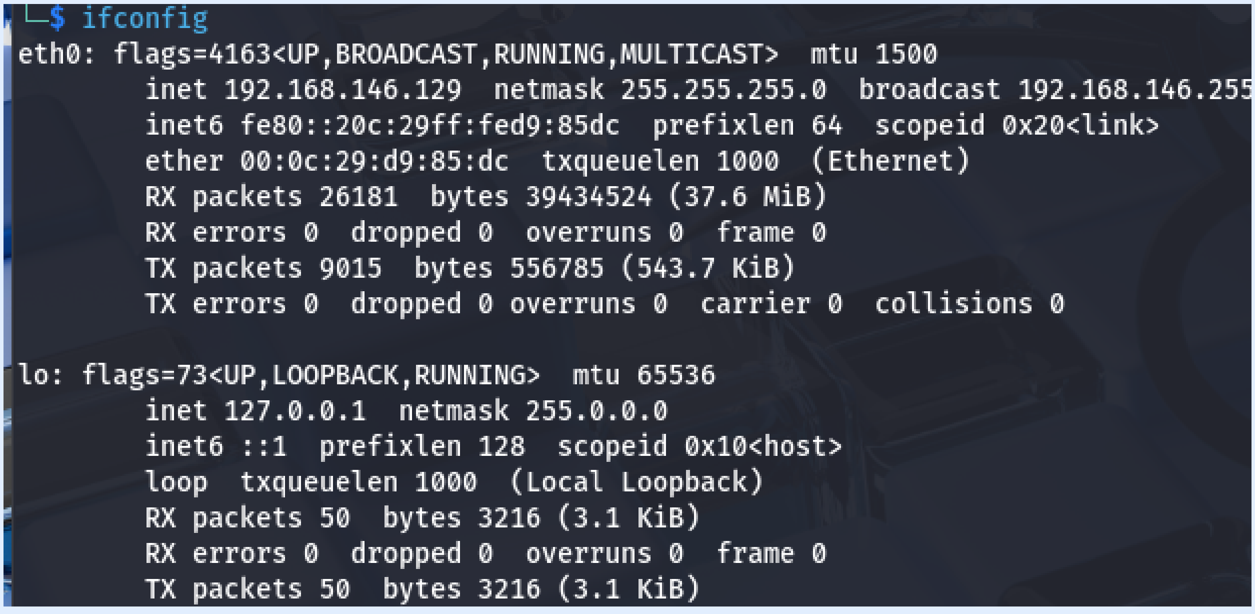
`https://<WAZUH_DASHBOARD_IP_ADDRESS>`

Username: `admin`

Password: `<ADMIN_PASSWORD>`

For ip run the following command:

```
Ifconfig
```

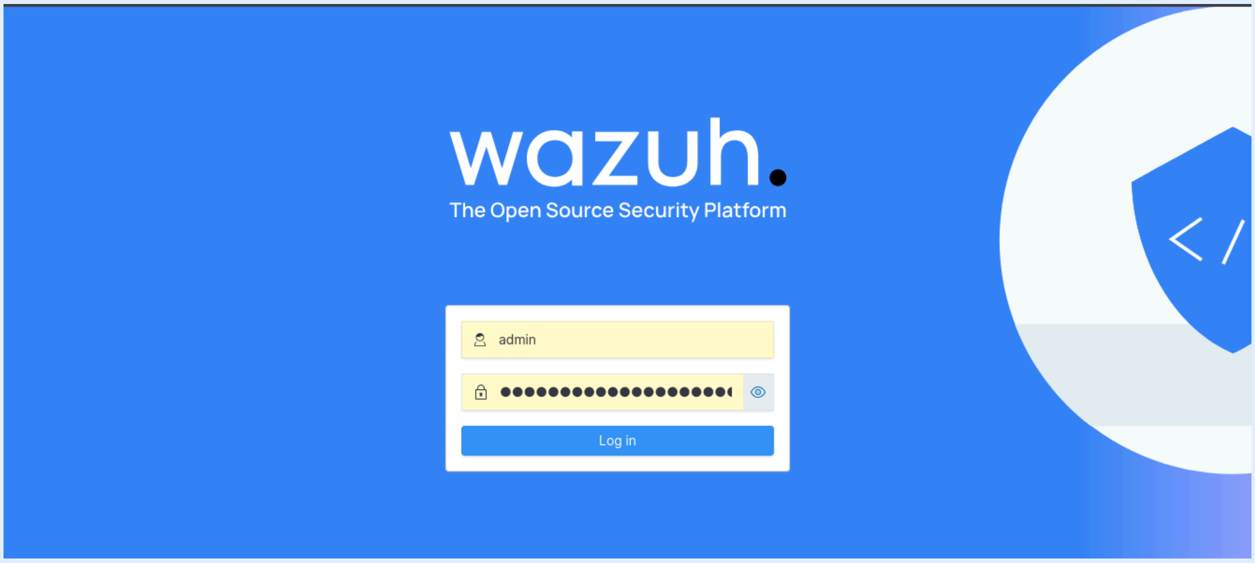


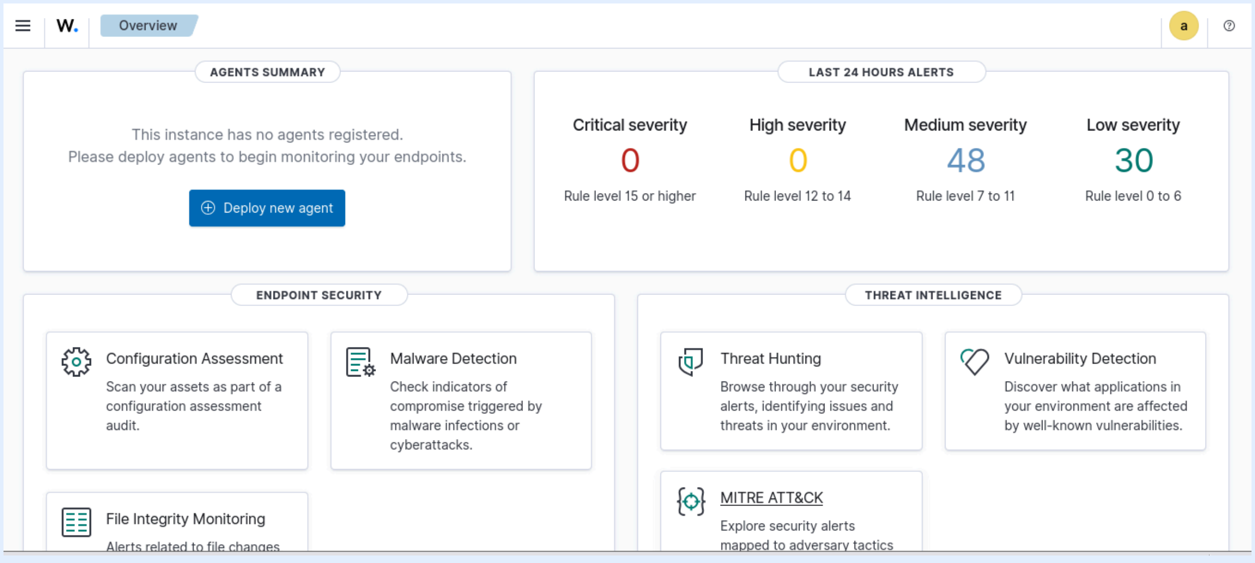
```
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.146.129  netmask 255.255.255.0  broadcast 192.168.146.255
        inet6 fe80::20c:29ff:fed9:85dc  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:d9:85:dc  txqueuelen 1000  (Ethernet)
        RX packets 26181  bytes 39434524 (37.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 9015  bytes 556785 (543.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 50  bytes 3216 (3.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 50  bytes 3216 (3.1 KiB)
```

When you first visit the Wazuh dashboard by going to https://<wazuh-dashboard-ip>, your browser might display a warning that the connection isn't secure. This happens because the certificate is self-signed and not issued by a trusted authority. This is completely normal. You can safely continue by accepting the warning, or later replace the certificate with one from a trusted provider to avoid this message.

Wazuh Installed Successfully:





Overview

AGENTS SUMMARY

This instance has no agents registered.
Please deploy agents to begin monitoring your endpoints.

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	0	48	30
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

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

Note:

After installing Wazuh, you can find all the passwords for the Wazuh Indexer and Wazuh API users in a file named wazuh-passwords.txt, which is located inside the wazuh-install-files.tar archive.

To view the passwords, run this command:

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

Uninstalling Wazuh:

If you ever need to remove the Wazuh central components, you can run the Wazuh installation assistant again using the -u or uninstall option.

Important:

It's recommended to disable Wazuh updates after installation. This helps avoid unexpected upgrades that might break your setup.

Run this command to disable the Wazuh repository:

```
sed -i "s/^deb/#deb/" /etc/apt/sources.list.d/wazuh.list
apt update
```

Now that Wazuh is installed and ready, you can begin setting up the Wazuh agent on your systems. The agent helps protect different types of devices like laptops, desktops, servers, virtual machines, containers, and cloud instances. It’s lightweight and versatile, offering a range of security features to monitor and secure your systems.