Wazuh

Table of contents:

Getting started with Wazuh

Wazuh is a free and open source security platform that unifies XDR and SIEM capabilities. It protects workloads across on-premises, virtualized, containerised, and cloud-based environments.

Wazuh helps organisations and individuals to protect their data assets against security threats. It is widely used by thousands of organisations worldwide, from small businesses to large enterprises.

Check this Getting Started for an overview of the Wazuh platform components, architecture, and common use cases.

Wazuh has one of the largest open source security communities in the world.

- Slack channel: Wazuh community channel to chat with the developers and technical team in a close to real-time experience.
- Google group: Here you can share questions and learn from other Wazuh users. It is easy to subscribe via email.
- GitHub repositories: Get access to the Wazuh source code, report issues, and contribute to the project. We happily review and accept pull requests.

Installation Guide

Installing the Wazuh central components

You can choose between two installation methods for each Wazuh central component. Both options provide instructions to install the central components on a single host or on separate hosts.

The Wazuh indexer and Wazuh server can be installed on a single host or be distributed in cluster configurations.

Requirements

Hardware

Hardware requirements highly depend on the number of protected endpoints and cloud workloads. This number can help estimate how much data will be analyzed and how many security alerts will be stored and indexed.

Following this quickstart implies deploying the Wazuh server, the Wazuh indexer, and the Wazuh dashboard on the same host. This is usually enough for monitoring up to 100 endpoints and for 90 days of queryable/indexed alert data. The table below shows the recommended hardware for a quickstart deployment:

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

For larger environments we recommend a distributed deployment. Multi-node cluster configuration is available for the Wazuh server and for the Wazuh indexer, providing high availability and load balancing.

Operating system

Wazuh central components can be installed on a 64-bit Linux operating system. Wazuh recommends any of the following operating system versions:

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

Browser compatibility

Wazuh dashboard supports the following web browsers:

- Chrome 95 or later
- Firefox 93 or later
- Safari 13.7 or later

Other Chromium-based browsers might also work. Internet Explorer 11 is not supported.

Installing Wazuh

1. Download and run the Wazuh installation assistant.

```
curl -sO https://packages.wazuh.com/4.3/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

Once the assistant finishes the installation, the output shows the access credentials and a message that confirms that the installation was successful.

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

You now have installed and configured Wazuh.

2. Access the Wazuh web interface with `https://<wazuh-dashboard-ip>` and your credentials:
    - Username: admin
    - Password: <ADMIN_PASSWORD>

When you access the Wazuh dashboard for the first time, the browser shows a warning message stating that the certificate was not issued by a trusted authority. This is expected and the user has the option to accept the certificate as an exception or, alternatively, configure the system to use a certificate from a trusted authority.

You can find the passwords for all the Wazuh indexer and Wazuh API users in the `wazuh-passwords.txt` file inside `wazuh-install-files.tar`. To print them, run the following command:

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

If you want to uninstall the Wazuh central components, run the Wazuh installation assistant using the option `-u` or `--uninstall`.

Next steps

Now that your Wazuh installation is ready, you can start deploying the Wazuh agent. This can be used to protect laptops, desktops, servers, cloud instances, containers, or virtual machines. The agent is lightweight and multi-purpose, providing a variety of security capabilities.

Wazuh agent

The Wazuh agent is multi-platform and runs on the endpoints that the user wants to monitor. It communicates with the Wazuh server, sending data in near real-time through an encrypted and authenticated channel.

The agent was developed considering the need to monitor a wide variety of different endpoints without impacting their performance. It is supported on the most popular operating systems, and it requires 35 MB of RAM on average.

The Wazuh agent provides key features to enhance your system's security.

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

To install a Wazuh agent, select your operating system and follow the instructions.

Deploying Wazuh agents on Linux endpoints

The agent runs on the host you want to monitor and communicates with the Wazuh server, sending data in near real-time through an encrypted and authenticated channel.

1. Install the GPG key:

```
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring -
-keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644
/usr/share/keyrings/wazuh.gpg
```

2. Add the repository:

```
echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg]
https://packages.wazuh.com/4.x/apt/ stable main" | tee -a
/etc/apt/sources.list.d/wazuh.list
```

3. Update the package information:

```
    apt-get update
```

> Note

For Debian 7, 8, and Ubuntu 14 systems import the GCP key and add the Wazuh repository (steps 1 and 2) using the following commands.

```
apt-get install gnupg apt-transport-https

curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | apt-key add -

echo "deb https://packages.wazuh.com/4.x/apt/ stable main" | tee -a
/etc/apt/sources.list.d/wazuh.list
```

Deploy a Wazuh agent

1. To deploy the Wazuh agent on your endpoint, select your package manager and edit the `WAZUH_MANAGER` variable to contain your Wazuh manager IP address or hostname.

```
WAZUH_MANAGER="10.0.0.2" apt-get install wazuh-agent
```

> Note: Alternatively, if you want to install an agent without registering it, omit the deployment variables. To learn more about the different registration methods, see the Wazuh agent enrollment section.

2. Enable and start the Wazuh agent service.

Systemd:

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

SysV init:

Choose one option according to your operating system.

a. RPM-based operating systems:

```
chkconfig --add wazuh-agent
service wazuh-agent start
```

b. Debian-based operating systems:

```
update-rc.d wazuh-agent defaults 95 10
service wazuh-agent start
```

The deployment process is now complete, and the Wazuh agent is successfully running on your Linux system.

- **Recommended action** - Disable Wazuh updates

Compatibility between the Wazuh agent and the Wazuh manager is guaranteed when the Wazuh manager version is later than or equal to that of the Wazuh agent. Therefore, we recommend disabling the Wazuh repository to prevent accidental upgrades. To do so, use the following command:

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

Alternatively, you can set the package state to `hold`. This action stops updates but you can still upgrade it manually using `apt-get install`.

```
echo "wazuh-agent hold" | dpkg --set-selections
```

Uninstall a Wazuh agent

To uninstall the agent, run the following commands:

1. Remove the Wazuh agent installation.

```
apt-get remove wazuh-agent
```

Some files are marked as configuration files. Due to this designation, the package manager does not remove these files from the filesystem. If you want to completely remove all files, run the following command:

```
apt-get remove --purge wazuh-agent
```

2. Disable the Wazuh agent service.

```
systemctl disable wazuh-agent
systemctl daemon-reload
```

The Wazuh agent is now completely removed from your Linux endpoint.

Deployment variables for Linux

For an agent to be fully deployed and connected to the Wazuh server, it needs to be installed, registered, and configured. The installers can use variables that allow configuration provisioning to make the process simple.

Below you can find a table describing the variables used by Wazuh installers and a few examples of how to use them.

Option	Description
WAZUH_MANAGER	Specifies the manager IP address or hostname. If you want to specify multiple managers, you can add them separated by commas. See address.
WAZUH_MANAGER_PORT	Specifies the manager connection port. See port.
WAZUH_PROTOCOL	Sets the communication protocol between the manager and the agent. Accepts UDP and TCP. The default is TCP. See protocol.
WAZUH_REGISTRATION_SERVER	Specifies the Wazuh registration server, used for the agent registration. See manager_address. If empty, the value set in `WAZUH_MANAGER` will be used.
WAZUH_REGISTRATION_PORT	Specifies the port used by the Wazuh registration server. See port.
WAZUH_REGISTRATION_PASSWORD	Sets password used to authenticate during register, stored in `etc/authd.pass`. See authorization_pass_path
WAZUH_KEEP_ALIVE_INTERVAL	Sets the time between agent checks for manager connection. See notify_time.
WAZUH_TIME_RECONNECT	Sets the time interval for the agent to reconnect with the Wazuh manager when connectivity is lost. See time-reconnect.
WAZUH_REGISTRATION_CA	Host SSL validation need of Certificate of Authority. This option specifies the CA path. See server_ca_path.
WAZUH_REGISTRATION_CERTIFICATE	The SSL agent verification needs a CA signed certificate and the respective key. This option specifies the certificate path. See agent_certificate_path.
WAZUH_REGISTRATION_KEY	Specifies the key path completing the required variables with WAZUH_REGISTRATION_CERTIFICATE for the SSL agent verification process. See agent_key_path.
WAZUH_AGENT_NAME	Designates the agent's name. By default, it will be the computer name. See agent_name.

Option	Description
WAZUH_AGENT_GROUP	Assigns the agent to one or more existing groups (separated by commas). See agent_groups.
ENROLLMENT_DELAY	Assigns the time that agentd should wait after a successful registration. See delay_after_enrollment.

Examples:

- Registration with password:

```
WAZUH_MANAGER="10.0.0.2" WAZUH_REGISTRATION_PASSWORD="TopSecret" \
     WAZUH_AGENT_NAME="apt-agent" apt-get install wazuh-agent
```

- Registration with password and assigning a group:

```
WAZUH_MANAGER="10.0.0.2" WAZUH_REGISTRATION_SERVER="10.0.0.2"
WAZUH_REGISTRATION_PASSWORD="TopSecret" \
     WAZUH_AGENT_GROUP="my-group" apt-get install wazuh-agent
```

- Registration with relative path to CA. It will be searched at your Wazuh installation folder:

```
WAZUH_MANAGER="10.0.0.2" WAZUH_REGISTRATION_SERVER="10.0.0.2"
WAZUH_AGENT_NAME="apt-agent" \
     WAZUH_REGISTRATION_CA="rootCA.pem" apt-get install wazuh-agent
```

- Registration with protocol:

```
WAZUH_MANAGER="10.0.0.2" WAZUH_REGISTRATION_SERVER="10.0.0.2"
WAZUH_AGENT_NAME="apt-agent" \
     WAZUH_PROTOCOL="udp" apt-get install wazuh-agent
```

- Registration and adding multiple addresses:

```
WAZUH_MANAGER="10.0.0.2,10.0.0.3" WAZUH_REGISTRATION_SERVER="10.0.0.2" \
     WAZUH_AGENT_NAME="apt-agent" apt-get install wazuh-agent
```

- Absolute paths to CA, certificate or key that contain spaces can be written as shown below:

```
WAZUH_MANAGER "10.0.0.2" WAZUH_REGISTRATION_SERVER "10.0.0.2"
WAZUH_REGISTRATION_KEY "/var/ossec/etc/sslagent.key" \
     WAZUH_REGISTRATION_CERTIFICATE "/var/ossec/etc/sslagent.cert" apt-get
install wazuh-agent
```

> Source: https://documentation.wazuh.com/current/index.html