Installing Wazuh Agent on Linux (Ubuntu/Debian)

Overview

This guide outlines the procedure for installing the Wazuh agent on Debian-based systems. It includes the standard repository method for local LAN devices, as well as a direct package installation method for devices on restricted networks (e.g., forced OpenVPN tunnels) where standard DNS or APT updates fail.

Prerequisites

- Root or **sudo** privileges on the target Linux machine.
- Connectivity to the Wazuh Manager.
- Port **1514/tcp** (data) and **1515/tcp** (enrollment) open on the Manager's firewall.

Method 1: Standard APT Installation (Main Network)

Use this method for standard servers that have unrestricted outbound internet access to resolve and update package lists.

1. Repository Configuration

Import the Wazuh GPG key and add the official repository to your package manager's sources.

```
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo gpg --no-default-keyring --keyring g

echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable m

sudo apt-get update
```

2. Agent Installation

Install the agent while passing the Manager's FQDN as an environment variable.

```
sudo WAZUH_MANAGER='wazuh.goonersnas.com' apt-get install wazuh-agent
```

Method 2: Direct Package Installation (VPN/Restricted Networks)

Use this method if the host is behind a strict VPN that blocks or fails to resolve standard APT update servers. This bypasses the package manager entirely.

1. Download the Package

Fetch the specific .deb installer directly from the Wazuh servers.

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.14.5-1_amd64.deb
```

2. Force Installation via DPKG

Install the downloaded package, passing the local IP address instead of the domain name to bypass local DNS resolution failures.

```
sudo WAZUH_MANAGER='192.168.0.153' dpkg -i wazuh-agent_4.14.5-1_amd64.deb
```

Service Activation & Verification

Once the agent is installed, enable it to start on boot and initiate the service.

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

Troubleshooting Common Issues

1. Error: "Job for wazuh-agent.service failed because a timeout was exceeded"

On newer Linux kernels or slower hardware, the systemd default timeout is often too short for the Wazuh initialization process. Extend the timeout with an override file:

```
sudo mkdir -p /etc/systemd/system/wazuh-agent.service.d/
echo -e "[Service]\nTimeoutStartSec=300" | sudo tee /etc/systemd/system/wazuh-agent.service.d/ti
sudo systemctl daemon-reload
sudo systemctl restart wazuh-agent
```

2. Manual Enrollment (If client.keys is empty)

If the agent installs but fails to retrieve a key from the manager, trigger enrollment manually:

```
sudo /var/ossec/bin/agent-auth -m 192.168.0.153
```

3. Fix: Agent Stuck in "Pending" or "Never Connected" Status

If the agent shows as registered in the dashboard but is "never connected", or if checking the local state (`sudo grep ^status /var/ossec/var/run/wazuh-agentd.state`) shows `status='pending'`, the agent cannot resolve or reach the Manager's address. Update the configuration to use the static IP.

Step A: Edit the configuration file

```
sudo nano /var/ossec/etc/ossec.conf
```

Step B: Locate the <client> block and update the <address> to the Manager's IP

```
<client>
  <server>
    <address>192.168.0.153</address>
    <port>1514</port>
    <protocol>tcp</protocol>
  </server>
</client>
```

Step C: Restart the agent to apply changes

```
sudo systemctl restart wazuh-agent
```

Revision #4
Created 2026-03-28 03:24:39 UTC by Francis
Updated 2026-04-24 21:39:03 UTC by Francis