Wazuh Agent Deployment & Troubleshooting Guide

This guide documents the procedures for maintaining Wazuh agents on Ubuntu 22.04/24.04, with specific instructions for Docker monitoring and manual ID preservation.

---

1. Agent Version Control (Critical)

Constraint: The Wazuh Manager version must always be equal to or higher than the Agent version.

- **Manager Version:** v4.9.0
- **Target Agent Version:** v4.9.0

```
# Download the specific matching version
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.9.0-1_amd64.deb
sudo dpkg -i wazuh-agent_4.9.0-1_amd64.deb
```

---

2. Preserving Existing Agent IDs (e.g., ID 015)

Use this process when reinstalling an agent to ensure it keeps its historical data and ID.

Step A: Extract Key from Manager

Run this on the **Wazuh Manager** terminal:

```
sudo /var/ossec/bin/manage_agents -e 015
```

Copy the long alphanumeric string provided.

Step B: Import Key to Agent

Run this on the **Bookstack-LXC** terminal:

```
sudo /var/ossec/bin/manage_agents -i [PASTE_KEY_HERE]
```

---

3. Monitoring Authentik & Docker Containers

To populate the Docker dashboard and monitor Authentik logs, three components are required.

Step A: Python Dependencies (Ubuntu 24.04 Fix)

Ubuntu 24.04 prevents global pip installs by default. Use `--break-system-packages` to allow the agent's internal scripts to run.

```
sudo apt update && sudo apt install python3-pip -y
pip3 install docker==7.1.0 requests==2.32.2 --break-system-packages
sudo usermod -aG docker wazuh
```

Step B: Config Changes (ossec.conf)

Open `/var/ossec/etc/ossec.conf` and add these blocks before the final `</ossec_config>`.

```
<!-- Monitor Container Events (Starts/Stops) -->
<wodle name="docker-listener">
  <interval>1m</interval>
  <attempts>5</attempts>
  <run_on_start>yes</run_on_start>
  <disabled>no</disabled>
</wodle>

<!-- Monitor Authentik Container Logs -->
<localfile>
  <log_format>syslog</log_format>
  <location>/var/lib/docker/containers/*/*-json.log</location>
</localfile>
```

4. Troubleshooting Checklist

Error in ossec.log	Fix Action
Invalid server address: 'MANAGER_IP'	Update `<address>` in ossec.conf to `wazuh.msls.tech`.
Error reading XML file (line 0)	Check for nested or unclosed `<ossec_config>` tags.

Handling Duplicate Agents for the Same VM

If a VM appears twice (e.g., with two different IDs), follow these steps to keep the ID with historical data:

1. **Identify:** Find the ID you want to keep (ID_KEEP) and the one to delete (ID_DEL).
2. **Delete on Manager:** `sudo /var/ossec/bin/manage_agents -r [ID_DEL]`.
3. **Stop Agent Service:** `sudo systemctl stop wazuh-agent` on the VM.
4. **Refresh Key:** Extract the key for ID_KEEP from the manager (`-e`) and import it to the agent (`-i`).
5. **Restart:** `sudo systemctl restart wazuh-agent`.

Revision #4
Created 2025-12-31 14:52:46 UTC by joliveira
Updated 2025-12-31 15:15:54 UTC by joliveira