Wazuh Windows Agent Installation and Registration

This document describes the installation, registration, and verification of the Wazuh Agent on a Windows 10 endpoint and its successful communication with the Wazuh Server running on an Ubuntu VM.

Step 1: Windows Agent Installation

The Wazuh Agent version 4.7.5 MSI was downloaded and installed on the Windows 10 VM. During installation, the Ubuntu Wazuh Server IP address and authentication key were provided. The agent setup GUI accepted the key and displayed a status of Saved/Refreshed, confirming successful configuration.

Step 2: Agent Registration on Ubuntu Server

The Windows agent was added on the Ubuntu Wazuh Server using the manage_agents utility, and an Agent ID was assigned. The agent status was verified using the agent_control command, which confirmed that the Windows agent was listed and active.

Step 3: Agent Running and Log Verification

On the Windows system, the Wazuh Agent was running successfully either via the GUI or as a Windows service. Agent logs were generated at C:\Program Files (x86)\ossec-agent\logs\ossec.log. The presence of 'Connected to manager' messages confirmed successful communication between the Windows agent and the Wazuh Server.

With the agent connected and active, Windows security and Sysmon events are now forwarded to the Wazuh Server for centralized analysis and alerting, enabling real-world SOC-style endpoint monitoring.