

Log data collection

Log data collection is the real-time process of making sense out of the records generated by servers or devices. This component can receive logs through text files or Windows event logs. It can also directly receive logs via remote syslog (useful for firewalls, etc...) The purpose of this process is the identification of application or system errors, misconfigurations, intrusion attempts, policy violations or security issues.

The memory and CPU requirements of the Wazuh agent are insignificant because it mostly just forwards events to the manager. However, on the Wazuh manager, CPU and memory consumption can increase quickly depending on the events per second (EPS) that the manager has to analyze.

Contents

- [How it works](#)
 - [Log collection](#)
 - [Analysis](#)
 - [Alert](#)
- [Configuration](#)
 - [Basic usage](#)
 - [Monitoring logs using regular expressions for file names](#)
 - [Monitoring date-based logs](#)
 - [Reading logs from Windows Event Log](#)
 - [Reading events from Windows Event Channel](#)
 - [Filtering events from Windows Event Channel with queries](#)
 - [Using environment variables](#)
- [FAQ](#)
 - [Are the logs analyzed on each agent?](#)
 - [How often does the manager monitor the logs?](#)
 - [How long are the logs stored on the server?](#)
 - [How does this help me with regulatory compliance?](#)
 - [What is the CPU usage like on the agents?](#)
 - [From where can Wazuh get log messages?](#)
 - [Can I send firewall, VPN, authentication logs to Wazuh?](#)
 - [What information should Wazuh extract from my logs?](#)
 - [Can I ignore events that are not important?](#)

