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