FAQ

Are the logs analyzed on each agent?

No, the manager gets the logs from all the agents and then analyzes the messages.

How often does the manager monitor the logs?

The manager monitors logs in real time.

How long are the logs stored on the server?

Archived logs are not automatically deleted. You choose when to manually or automatically (i.e., cron job) delete logs according to your own legal and regulatory requirements.

How does this help me with regulatory compliance?

Log analysis is a requirement for : PCI DSS Compliance, HIPAA Compliance, FISMA Compliance and SOX Compliance.

What is the CPU usage like on the agents?

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

From where can Wazuh get log messages?

Wazuh can read log messages from text log files, Windows event logs and event channels, and also via remote syslog. Logs are monitored in real time.

Can I send firewall, VPN, authentication logs to Wazuh?

Yes. Wazuh has the capability to receive and process logs from devices that send logs using the syslog protocol. You can create custom decoders and rules for your device-specific logs.

What information should Wazuh extract from my logs?

This depends on your needs. Once you know the format of your application logs and the typical events, you can create decoders and rules for them.

Can I ignore events that are not important?

You can configure the rules to ignore certain events. More info: Custom rules