Overview

Wazuh is an open source project that provides security visibility, compliance and infrastructure monitoring capabilities. The project was born as a fork of OSSEC HIDS, and has evolved into a comprehensive solution by implementing new functionalities and integrating other tools like OpenSCAP and Elasticsearch.

This manual describes how to configure and use each one of Wazuh components: Wazuh server, Wazuh agent, and Elastic Stack.

Wazuh server

The Wazuh server is based on a suite of applications, every application/component is designed to accomplished certain task, but when they working together it could analyze the data receive from agents, triggering alerts when an event matches a rule, register new clients/agents, sending data to Elastic Stack server, all paired with a with a RESTful API.

Components

- **Wazuh Manager**: It receives data and analyzes data from the agents. To do that it uses decoders and rules that have been crafted to trigger security alerts. The manager is also used to distribute configuration files to the agents, and to monitor their status. In addition it can send control messages to trigger automatic actions at an agent level.
- **Registration Service**: It use a secure mechanisms to register a client without any intervention on server side.
- RESTful API: It provides an interface to manage and monitor the configuration of the manager and agents, also it could register clients/agents. It can be also used to inspect the manager log messages, decoders and rules. In addition it provides useful information related to the agents, including their status, operating system details, and file integrity monitoring and rootcheck alerts.
- **Filebeat**: It is used in distributed architectures (where the Wazuh server and Elastic Stack live in different systems) to forward the alerts data to Logstash. This component has its own documentation developed by Elastic.

Elastic Stack

Elastic Stack is used to indexing, browse and visualize Wazuh alerts data. In addition, the Wazuh app for Kibana can be used to visualize configuration settings, rules, and decoders, agents status, information, and provides dashboards for policy, compliance and file integrity monitoring.

Components

- **Wazuh app**: is a Kibana plugin designed to display Wazuh related information providing a RESTful API web interface making administration of Wazuh Manager and Wazuh Agents easy and powerful.
- **Logstash**: is used to ingest data coming from one or more Wazuh servers via Filebeat, feeding the Elasticsearch cluster. In addition it enriches alerts adding Geolocation metadata. More information at Logstash official documentation.
- **Elasticsearch**: is a highly scalable full-text search and analytics engine. It is used to index alerts data, and historical agents statuts information. More information at Elasticsearch official documentation.
- **Kibana**: is a flexible and intuitive web interface for mining, analyzing, and visualizing data. In combination with our Wazuh Kibana app, it is used as Wazuh web user interface (WUI). More information at Kibana official documentation.

Wazuh agents

The Wazuh agent runs on monitored systems and is in charge of collecting log and event data, performing policy monitoring scans, detecting malware and rootkits and alert when watched files are modified. It communicates with the Wazuh server through an encrypted and authenticated channel.

Components

- **Rootcheck**: perform rootkit and malware detection on every system where the agent is installed.
- **Log monitoring/analysis**: collect and analyze system logs on the system finding any suspicious activity.
- **Syscheck**: runs periodically to check if any configured file (or registry entry on Windows) has changed.

- **OpenSCAP**: designed to check weak and vulnerable applications and configurations.