

wazuh-modulesd

The wazuh-modulesd program manages the Wazuh modules described below.

Elastic Stack integration

Elastic Stack is a combination of popular open source projects for log management, including Elasticsearch, Logstash, Kibana, and others.

Wazuh Ruleset

Wazuh rules are based on of the OSSEC ruleset. This ruleset has been revised and expanded with enhancements, corrections and additions to deepen Wazuh functionality and detection capabilities.

RESTful API

The RESTful API controls the Wazuh manager using REST requests. This allows the Wazuh manager to be interacted with from a web browser, command line tool like cURL, or any script or program that can make web requests. This API may be used to easily perform everyday actions like adding an agent, restarting the manager/agent(s), or looking up syscheck details.

-d	Increase debug mode.
-f	Run in the foreground.
-h	Display the help message.
-t	Test configuration.

