2.1 Release Notes

This section shows the most relevant new features of Wazuh v2.1. You will find more detailed information in our changelog file.

New features:

- Anti-flooding mechanism
- Labels for agent alerts
- Improved Authd performance
- New features for internal logs
- Updated external libraries
- Wazuh API
- Ruleset

Anti-flooding mechanism

This mechanism is designed to prevent disruptively large bursts of events on an agent from negatively impacting the network or the manager. It uses a leaky bucket queue that collects all generated events, and sends them to the manager at a rate not exceeding a configurable events per second threshold.

Learn more about this new mechanism at Anti-flooding mechanism.

Labels for agent alerts

This feature allows agent-specific attributes to be included in each alert involving a given agent. This could include things like who is in charge of a particular agent, or the installation date of that agent. This provides a simple method to add valuable metadata to alert records.

For more details about this new feature see our Labels section.

Improved Authd performance

The Authd program has been improved in this version. Before Wazuh 2.1, the Wazuh API and the `manage_agents` tools could not register an agent while `ossec-authd` was running. Now agent registration is simultaneously supported via all of these methods.

Additionally, since this new version of ossec-authd runs in the background, it can be enabled using the command `ossec-control enable auth`. Its options can be configured in the auth section of `ossec.conf`. The documentation includes a good configuration example.

Finally, the new `force_insert` and `force_time` options in Authd (`-F<time>` from the `ossec-authd` command line) allow for automatic deletion of any agents that match the name or IP address of a newly registered agent.

New features for internal logs

It is widely known that JSON is one of the most popular logging formats. Because of this, it is now possible to have internal logs written in JSON format, plain text, of both. This can be configured in the logging section of `ossec.conf`.

In addition, internal logs are rotated and compressed daily, simplifying their management. To control disk space use, there is also a configurable threshold for how long to retain rotated logs before automatic deletion. These parameters are configured in the `monitord` section of Internal configuration.

Updated external libraries

External libraries used by Wazuh have been updated to improve their integration with our components.

Wazuh API

The request `/agents` returns information about the OS.

Also, it is possible to delete or restart a list of specific agents.

Ruleset

The previous Windows decoders extracted a wrong user (the subject user). New decoders for Windows extract the proper user and new fields.