


Internal configuration

The main configuration is located in the *ossec.conf* file, however some internal configuration features are located in the `/var/ossec/etc/internal_options.conf` file.

Generally, this file is reserved for debugging issues and for troubleshooting. **Any error in this file may cause your installation to malfunction or fail to run.**

 Warning

This file will be overwritten during upgrades. In order to maintain custom changes, you must use the `/var/ossec/etc/local_internal_options.conf` file.

- [Agent](#)
- [Analysisd](#)
- [DBD](#)
- [Logcollector](#)
- [Maid](#)
- [Monitord](#)
- [Remoted](#)
- [Syscheck](#)
- [Rootcheck](#)
- [Wazuh_database](#)
- [Wazuh_modules](#)
- [Windows](#)

Agent

agent.tolerance	Description	Time in seconds since the agent is full until trigger a flooding alert.
	Default value	15
	Allowed value	Any integer between 0 and 600.
agent.warn_level	Description	Percentage of occupied capacity in Agent buffer to trigger a warning alert.
	Default value	90
	Allowed value	Any integer between 1 and 100.
agent.normal_level	Description	Percentage of occupied capacity in Agent buffer to come back to normal state.
	Default value	70
	Allowed value	Any integer between 0 and <i>agent.warn_level</i> - 1.
agent.min_eps	Description	Minimum events per second permitted in <code><client_buffer></code> configuration.
	Default value	50
	Allowed value	Any integer between 1 and 1000.
agent.debug	Description	Run the unix agent's processes in debug mode.
	Default value	0
	Allowed value	0 : No debug output
		1: Standard debug output
		2: Verbose debug outputNext,Previous

Analysisd

analysisd.default_timeframe	Description	Analysisd default rule timeframe.
	Default value	360
	Allowed value	Any integer between 60 and 360
analysisd.stats_maxdiff	Description	Analysisd stats maximum diff.
	Default value	999000
	Allowed value	Any integer between 10 and 99999
analysisd.stats_mindiff	Description	Analysisd stats minimum diff.
	Default value	1250
	Allowed value	Any integer between 10 and 999999
analysisd.stats_percent_diff	Description	Analysisd stats percentage (how much to differ from average).
	Default value	150
	Allowed value	Any integer between 5 and 9999
analysisd.fts_list_size	Description	Analysisd FTS list size.
	Default value	32
	Allowed value	Any integer between 12 and 512
analysisd.fts_min_size_for_str	Description	Analysisd FTS minimum string size.
	Default value	14
	Allowed value	Any integer between 6 and 128
analysisd.log_fw	Description	Analysisd Enable the firewall log (at logs/firewall/firewall.log).
	Default value	1
	Allowed value	0, 1
analysisd.decoder_order_size	Description	Maximum number of fields in a decoder (order tag).
	Default value	64
	Allowed value	Any integer between 10 and 64
analysisd.geoip_jsonout	Description	Output GeoIP data at JSON alerts.
	Default value	0
	Allowed value	0, 1
analysisd.label_cache_maxage	Description	Time in seconds without reload labels in cache from agents.
	Default value	0
	Allowed value	Any integer between 0 and 60.
analysisd.show_hidden_labels	Description	Make hidden labels visible in alerts.
	Default value	0
	Allowed value	0, 1
analysisd.debug	Description	Debug level (manager installations)
	Default value	0
	Allowed value	0: No debug output
		1: Standard debug output
		2: Verbose debug output

DBD

dbd.reconnect_attempts	Description	The number of times ossec-dbd will attempt to reconnect to the database.
	Default value	10
	Allowed value	Any integer between 1 and 9999

Logcollector

logcollector.loop_timeout	Description	File polling interval.
	Default value	2
	Allowed value	Any integer between 1 and 120
logcollector.open_attempts	Description	Number of attempts to open a log file.
	Default value	8
	Allowed value	Any integer between 2 and 298
logcollector.remote_commands	Description	Enable/disable Logcollector to accept remote commands from the manager.
	Default value	0
	Allowed value	0, 1
logcollector.vcheck_files	Description	Number of readings before checking files.
	Default value	64
	Allowed value	Any integer between 0 and 1024
logcollector.max_lines	Description	Maximum number of logs read from the same file in each iteration.
	Default value	10000
	Allowed value	Any integer between 100 and 100000.
logcollector.debug	Description	Debug level (used in manager or unix agent installations)
	Default value	0
	Allowed value	0: No debug output
		1: Standard debug output
		2: Verbose debug output

Maild

maild.strict_checking	Description	Toggle to enable or disable strict checking.
	Default value	1
	Allowed value	0, 1
maild.grouping	Description	Toggle to enable or disable grouping of alerts into a single email.
	Default value	1
	Allowed value	0, 1
maild.full_subject	Description	Toggle to enable or disable full subject in alert emails.

	Default value	0
	Allowed value	0, 1
maild.geoip	Description	Toggle to enable or disable GeoIP data in alert emails.
	Default value	1
	Allowed value	0, 1

Monitord

monitord.day_wait	Description	Amount of seconds to wait before compressing or signing the files.
	Default value	10
	Allowed value	Any integer between 5 and 240
monitord.compress	Description	Toggle to enable or disable log file compression.
	Default value	1
	Allowed value	0, 1
monitord.sign	Description	Toggle to enable or disable signing the log files.
	Default value	1
	Allowed value	0, 1
monitord.monitor_agents	Description	Toggle to enable or disable monitoring of agents.
	Default value	1
	Allowed value	0, 1
monitord.keep_log_days	Description	Number of days to keep rotated internal logs.
	Default value	31
	Allowed value	0, 500

Remoted


remoted.recv_counter_flush	Description	Flush rate for the receive counter.
	Default value	128
	Allowed value	Any integer between 10 and 999999
remoted.comp_average_printout	Description	Compression averages printout.
	Default value	19999
	Allowed value	Any integer between 10 and 999999
remoted.verify_msg_id	Description	Toggle to enable or disable verification of msg id.
	Default value	0
	Allowed value	0, 1
remoted.pass_empty_keyfile	Description	Toggle to enable or disable acceptance of empty client.keys.
	Default value	1
	Allowed value	0, 1
remoted.debug	Description	Debug level (manager installation)
	Default value	0
	Allowed value	0: No debug output

		1: Standard debug output
		2: Verbose debug output

Syscheck

syscheck.sleep	Description	Number of seconds to sleep after reading syscheck.sleep_after number of files.
	Default value	2
	Allowed value	Any integer between 0 and 64
syscheck.sleep_after	Description	Number of files to read before sleeping for syscheck.sleep seconds.
	Default value	15
	Allowed value	Any integer between 1 and 9999
syscheck.debug	Description	Debug level (used in manager and unix agent installations).
	Default value	0
	Allowed value	0: No debug output
		1: Standard debug output
		2: Verbose debug outputNext,Previous

Rootcheck


rootcheck.sleep	Description	Number of milliseconds to sleep after reading one PID or suspicious port.  New in version 2.1.
	Default value	50
	Allowed values	Any integer from 0 to 50.

Wazuh_database

The Wazuh core uses list-based databases to store information related to agent keys and FIM / Rootcheck event data. Such information is highly optimized to be handled by the core.

In order to provide well-structured data that could be accessed by the user or the Wazuh API, new **SQLite-based databases** have been introduced in the Wazuh manager. The Database Synchronization Module is a **user-transparent component** that collects the following information from the core:

- Agent’s name, address, encryption key, last connection time, operating system, agent version and shared configuration hash.
- FIM data: creation, modification and deletion of regular files and Windows registry entries.
- Rootcheck detected defects: issue message, first detection date and last alert time.
- Static core settings, such as maximum permitted agents or SSL being enabled for Authd.

 **Note**

The Wazuh Database Synchronization Module starts automatically on the server and local profiles and requires no configuration, however, some optional settings are available.

The module uses *inotify* from Linux to monitor changes to every log file in real-time. Databases will be updated as soon as possible when a change is detected. **If inotify is not supported**, (for example, on operating systems other than Linux) every log file will be scanned continuously, looking for changes, with a default delay of one minute between scans.

How to disable the module

To disable the Wazuh Database Synchronization Module, the sync directives must be set to 0 in the `etc/local_internal_options.conf` file as shown below:

```
wazuh_database.sync_agents=0
wazuh_database.sync_syscheck=0
wazuh_database.sync_rootcheck=0
```

Once these settings have been adjusted, save the file and **restart Wazuh**. With the above settings, the Database Synchronization Module will not be loaded when Wazuh starts.

wazuh_database.sync_agents	Description	Synchronize agent database with client.keys.
	Default value	1
	Allowed value	0, 1
wazuh_database.sync_syscheck	Description	Synchronize f.i.m. data with Syscheck database.
	Default value	1
	Allowed value	0, 1
wazuh_database.sync_rootcheck	Description	Synchronize policy monitoring data with Rootcheck database.
	Default value	1
	Allowed value	0, 1
wazuh_database.full_sync	Description	Full data synchronization.
	Default value	0
	Allowed value	0, 1
wazuh_database.sleep	Description	Interval to sleep between cycles. Only necessary if inotify not available.
	Default value	60
	Allowed value	Any integer between 0 and 86400 (seconds)
wazuh_database.max_queued_events	Description	Max number of queued events (only if inotify is available).
	Default value	0 (use system default value)
	Allowed value	Any integer between 0 and 2147483647

Wazuh_modules

wazuh_modules.task_nice	Description	Indicates the priority of the tasks. Lower Value, Higher priority.
	Default value	10
	Allowed value	Any integer between -20 and 19
wazuh_modules.max_eps	Description	Maximum number of events per second sent by OpenSCAP Wazuh Module.
	Default value	1000

	Allowed value	Any integer between 100 and 1000
wazuh_modules.debug	Description	Debug level
	Default value	0
	Allowed value	0: No debug output
		1: Standard debug output
		2: Verbose debug outputNext,Previous

Windows

windows.debug	Description	Debug level (used in windows agent installations).
	Default value	0
	Allowed value	0: No debug output
		1: Standard debug output
		2: Verbose debug outputNext,Previous