

# ossec-analysisd

The ossec-analysisd program receives the log messages and compares them to the rules. It then creates an alert when a log message matches an applicable rule.

-c <config>	Configuration file ossec-analysisd should use.
-D <dir>	Chroot to <dir>
-d	Run in debug mode. This option may be repeated to increase the verbosity of the debug messages.
-f	Run in the foreground.
-g <group>	Run as a group.
-h	Display the help message.
-t	Test configuration.
-u	Run as a user.
-V	Display the version and license information

