Full credit is given to the above companies including the OS that this PDF file was generated!

Rocky Enterprise Linux 9.2 Manual Pages on command 'auditd-plugins.5'

$ man auditd-plugins.5

AUDITD-PLUGINS(5) System Administration Utilities AUDITD-PLUGINS(5)

NAME

auditd-plugins - realtime event receivers

DESCRIPTION

auditd can multiplex audit events in realtime. It takes audit events and distributes them to child programs that want to analyze events in realtime. When the audit daemon receives a SIGTERM or SIGHUP, it passes that signal to its child processes so that can reload the configuration or terminate.

The child programs install a configuration file in a plugins directory which defaults to /etc/audit/plugins.d. This can be controlled by a au? ditd.conf config option plugin_dir if the admin wished to locate plug? ins somewhere else. But auditd will install its plugins in the default location.

The plugin directory will be scanned and every plugin that is active
will be started. If the plugin has a problem and exits, it will be
started a maximum of max_restarts times as found in auditd.conf.

Config file names are not allowed to have more than one '.' in the name
or it will be treated as a backup copy and skipped. Config file options
are given one per line with an equal sign between the keyword and its
value. The available options are as follows:

active The options for this are yes or no.

direction

The option is dictated by the plugin. In or out are the only
choices. You cannot make a plugin operate in a way it wasn't de?
signed just by changing this option. This option is to give a
clue to the event dispatcher about which direction events flow.
NOTE: inbound events are not supported yet.

path This is the absolute path to the plugin executable. In the case
of internal plugins, it would be the name of the plugin.

type This tells the dispatcher how the plugin wants to be run.
Choices are builtin and always. Builtin should always be given
for plugins that are internal to the audit event dispatcher.
These are af_unix and syslog. The option always should be given
for most if not all plugins. The default setting is always.

args This allows you to pass arguments to the child program. Gener?
ally plugins do not take arguments and have their own config
file that instructs them how they should be configured. At the
moment, there is a limit of 2 args.

format The valid options for this are binary and string. Binary passes the data exactly as the audit event dispatcher gets it from the audit daemon. The string option tells the dispatcher to com? pletely change the event into a string suitable for parsing with the audit parsing library. The default value is string.

FILES

/etc/auditd/auditd.conf /etc/audit/plugins.d

SEE ALSO

auditd.conf(5), auditd(8).

AUTHOR

Steve Grubb

Red Hat Aug 2018 AUDITD-PLUGINS(5)