NAME

audisp-filter − plugin to filter audit events and forward them to other plugins

SYNOPSIS

audisp-filter *MODE CONFIG_FILE BINARY* [*BINARY_ARGS*]

DESCRIPTION

audisp-filter is an audit event dispatcher plugin designed to filter out specific events based on its provided configuration. Moreover, it possesses the capability to forward the remaining logs to other plugins. The plugin is universally compatible, allowing seamless integration with any existing audit plugin that expects audit messages on its standard input. Currently it supports the following arguments:

MODE
: The operational mode can be either allowlist or blocklist. In allowlist mode, the plugin forwards everything except for events that match the specified ausearch expressions in the configuration. Conversely, in blocklist mode, it refrains from forwarding anything except for events listed in the configuration.

CONFIG_FILE
: Path to the main configuration file containing ausearch expressions.

BINARY
: Path to an external program that will consistently receive filtered audit events through its standard input.

BINARY_ARGS
: Optionally, you can pass additional arguments to the external program.

CONFIGURATION AND RULES EVALUATION

Every single plugin that wants to benefit from the event filtering capability needs to create its own configuration file. It's a good practice to place this file inside the audit config directory, following the naming convention audisp-filter-pluginname.conf, for instance, **audisp-filter-syslog.conf** to filter audit events before sending them to syslog.

Each line within a configuration represents an ausearch-expression (5). Internally, these expressions are joined using the OR operator. Therefore, every expression is substituted with (PE || CE), where PE represents the previous expression and CE denotes the current expression being processed. Lines starting with a **'#'** character are treated as comments and do not influence the final rule set.

Upon the creation of an audit event, the filtering engine goes through the list of expressions, constructing the final expression representing our rule set. The event in question will be searched using this expression. The decision to forward an audit event to the configured binary depends on two factors: the operational mode of audisp-filter and whether the expression matches the ongoing event.

EXAMPLE

Example1: Do not syslog audit events containing unsuccessful openat syscalls.

First, in the plugin config, make sure that operation mode is set to allowlist, the binary points to /sbin/audispFyslog and provide any additional arguments if needed. Next, create the plugin specific config file with the content below. Before enabling the audit plugin, always make sure the syntax is correct. This can be checked by calling audisp-filter --check path/to/config/file.

(type r= SYSCALL && syscall i= openat && success r= yes)

FILES

/etc/audit/plugins/filter.conf /etc/audit/auditd.conf

SEE ALSO

auditd.conf(8), **ausearch-expression**(5), **auditd-plugins**(5).

AUTHOR

Attila Lakatos