NAME

audisp-syslog − plugin to push audit events into syslog

SYNOPSIS

audisp-syslog [*OPTIONS*]

DESCRIPTION

audisp-syslog is a plugin for the audit event dispatcher that wraps audit events back around to syslog. It can be passed three options: one which is the syslog facility, one that is the syslog level that all events are logged with, and one that determines if events should be interpreted. Valid facilities are LOG_LOCAL0 through 7, LOG_AUTH, LOG_AUTHPRIV, LOG_DAEMON, LOG_SYSLOG, and LOG_USER. Valid levels are LOG_DEBUG through LOG_EMERG. Setting these options is done in the /etc/audit/syslog.conf file on the args line.

If it is desired that events are interpreted, add the word **interpret** to the args line. This will cause all events to be interpreted. The drawback to this approach is that naive parsers can be tricked by an adversary that has the ability to name files, processes, or other user controlled objects.

If you are aggregating multiple machines, you should edit auditd.conf to set the name_format to something meaningful and the log_format to enriched. This way you can tell where the event came from and have the user name and groups resolved locally before it is sent off of the machine.

FILES

/etc/audit/plugins/syslog.conf /etc/audit/auditd.conf

SEE ALSO

auditd.conf(8), **auditd-plugins**(5), **syslog**(3).

AUTHOR

Steve Grubb