NAME

audisp-af_unix − plugin to push audit events to an af_unix socket

SYNOPSIS

audisp-af_unix [*OPTIONS*]

DESCRIPTION

audisp-af_unix is a plugin for the audit event dispatcher that sends audit events to an af_unix socket where other applications can read events. The **args** line of the **af_unix.conf** file expects three arguments: access mode, socket path, and output format, and optionally a fourth argument specifying the queue depth. The access mode determines the permissions for the socket and defaults to 0640. The socket path specifies where the socket will be created, with the default location being /run/audit/audispd_events. The output format determines the format in which events are delivered to the socket and supports two options: "string" and "binary". The "string" format delivers events in a human-readable form, while the "binary" format delivers events in their binary representation, which is essential for applications that need to process events in binary and reconstruct headers accurately. If the output format is not specified, the plugin defaults to the "string" format. If no queue depth is specified, it defaults to 512.

The **af_unix.conf** file must also include the line **format = binary**. This setting specifies the input format that the **audisp-af_unix** plugin expects from the audit event dispatcher. It ensures that the input delivered to the plugin is in binary format, enabling the plugin to reconstruct headers in their proper binary structure.

When the plugin is sent **SIGUSR1**, it writes a state report to **af_unix.state**.

FILES

/etc/audit/plugins/af_unix.conf /run/audit/audispd_events /run/audit/af_unix.state /etc/audit/auditd.conf

SEE ALSO

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

AUTHOR

Steve Grubb