audispd

Multiplexeur d'évènement

audispd doit être démarré par auditd pour obtenir les évènements, qu'il distribut aux programmes enfants qui souhaitent analyser les évènements en temps réel. Quand auditd reçoit SIGTERM ou SIGHUP, il passe ce signal au dispatcher également, qui en retour le passe aux processus enfant.

Les programmes enfant installent un fichier de configuration dans un répertoire, /etc/audisp/plugins.d/. Les noms de fichier ne doivent pas avoir plus d'un '.' dans le nom sinon ils sont traités comme copie de sauvegarde et ignorés. Les options sont :

OPTIONS

active (bool)

direction Dicté par le plugin. (in, out)

path Chemin complet du plugin. Dans le cas des plugins internes, c'est juste le nom.

type Indique commment le plugin est lancé (builtin, always). builtin devrait toujours être spécifié pour les plugins internes, sinon always.

args Permet de passer des arguments au programme enfant. Il y a une limite de 2 arguments

format binary ou string. binary passe les données tel que audispd les a reçu. string est plus adapté au parsing