auditd

Service d'audit Linux

auditd est le composant userspace du système d'audit Linux. Il est responsable de l'écriture des enregistrements d'audit sur disque.

OPTIONS

-F Ne lance pas en tâche de fond

-l Autorise à suivre les liens symboliques pour les fichiers de configuration

-n ne fork pas

-s=ENABLE_STATE Indique si auditd devrait changer la valeur courante du flag enabled du kernel (disable, enable ou nochange).

Signaux

SIGHUP reconfigure auditd

SIGTERM Stop l'audit, écrit un évènement d'arrêt, et quitte

SIGUSR1 rotation automatique des logs

SIGUSR2 tente de relancer le logging

Fichiers

/etc/audit/auditd.conf Fichier de configuration pour auditd

/etc/audit/audit.rules Règles d'audit à charger au démarrage

/etc/audit/rules.d/ Jeux de règles individuels à compiler par augenrules

Notes

Le paramètre de boot audit=1 devrait être ajouté pour s'assurer que tous les processus qui sont lancés avant le service auditd soient marqués comme auditable par le kernel. Noter que faire cela rend quelques processus impossible à auditer.

auditd peut reçevoir des évènements depuis d'autres services auditd via le plugin audisp-remote. auditd peut être liés avec tcp_wrappers pour contrôler quelles machines peuvent s'y connecter.