autrace

Programme similaire à strace

autrace est un programme qui ajoute des règles d'audit pour tracer une processus, similairement à strace. Il exécute ainsi le programme en lui passant les arguments. Les informations d'audit résultant sont au format de log d'audit si auditd fonctionne ou syslog. Cette commande supprime toutes les règles d'audit avant d'exécuter le programme cible et après d'avoir exécuté. C'est une précaution, il ne se lance pas si les règles ne sont pas supprimées avec auditctl avant.

OPTIONS

-r Limite les appels système collectés à celles nécessaire pour l'analise d'utilisation de ressource.

Exemples

Exemple de session
autrace /bin/ls /tmp
ausearch –start recent -p 2442 -i
ou le mode d'utilisation de ressource
autrace -r /bin/ls
ausearch –start recent -p 2450 –raw | aureport –file –summary
ausearch –start recent -p 2450 –raw | aureport –host –summary