Présentation OSSIR
FileAudit

Comment exploiter efficacement les journaux d'audit de Windows ?

CoperNet

Microsoft CERTIFIED Partner

L’audit NTFS

- Windows NT est capable de stocker un historique d’événements relatifs à la sécurité.

- Les principaux événements sont:
  - Connexions et déconnexions de comptes utilisateurs sur les contrôleurs de domaine
  - Accès aux fichiers sur des partitions NTFS

Filtre et recherche

- Windows ne permet pas de rechercher efficacement une liste d'événements audités pour un fichier donné.

- Il n'y a pas de moyen simple pour retrouver depuis quel machine un accès fichier a eu lieu à moins de rechercher l'audit de génération du jeton d'accès utilisé pour faire l'opération sur le fichier. La recherche doit alors se faire sur chaque contrôleur de domaine.

FileAudit

- FileAudit permet d'automatiser directement depuis l'explorateur et par un simple clic droit:
  - La recherche d'événements d'audit par fichier ou dossier
  - Le tri de ces événements pas type d'accès, utilisateur, date…
  - La recherche sur les volumes dynamiques de Windows 2000

- Par ailleurs, FileAudit possède une option permettant de rechercher sur quelle machine était connecté l'utilisateur qui a fait un accès fichier au moment de l'accès.

CoperNet

Microsoft CERTIFIED Partner