Disques auto-chiffrant

Présentation

- Un disque dur chiffrant (Self-Encrypting Drive) est une solution matérielle de chiffrement intégral du disque. Lorsque le chiffrement n'est pas activé, le disque se comporte comme un disque dur ordinaire. Quand le chiffrement est activée, une phase d'authentification est nécessaire au démarrage pour déverrouiller l'accès au disque, qui est inutilisable autrement.
- Ces disques répondent aujourd'hui à la norme OPAL, éditée par le Trusted Computing Group.

TEST

- Acquisition d'un DELL E6530 avec l'option : " Passage au disque dur Flash SSD 256 Go Chiffré" Problème : il est marqué sur le site DELL que cette option est incompatible avec Windows 8 ...
- Le disque est un SSD 256 Samsung
- Utilitaire à utiliser : "Dell Data Protection Access" version Win7 64B. La version livré est la 2.3

Coût

- Ces disques sont disponibles aujourd'hui sur le marché Dell, pour un surcoût d'une vingtaine d'euros. Le logiciel de gestion est pré-installé si la machine est livrée sous Windows.
- Il est techniquement possible d'acheter ces disques séparément et de les mettre en place sur n'importe quelle autre machine. Cependant, l'utilisation sans logiciel de gestion associé n'est pas possible.

Installation et administration

- La gestion du disque impose l'utilisation d'un composant logiciel. Bien que ce type de disque soit normalisé, le seul identifié à ce jour est Trusted Drive Manager, un composant de la suite logicielle Wave Embassy, qui n'est disponible que sous Windows.
- Dell fournit une version de cet outil intégrée à sa propre suite logicielle consacrée à la sécurité, dénommée "Dell Data Protection Access". C'est cette version qui est pré-installée sur les machines.
- Le chiffrement peut se mettre en place sur un système déjà installé sans problème. Il peut être suspendu temporairement si nécessaire.

Utilisation

- Le déverrouillage du disque passe par une étape d'authentification au démarrage, via un chargeur de démarrage (bootloader) spécifique. Celui-ci gère une liste de comptes utilisateurs, avec pour chacun une identification par mot de passe et/ou empreinte digitale.
- Démarrer depuis un autre composant matériel que le disque court-circuite ce chargeur, et ne permet pas de déverrouiller le disque. L'installation d'un second système ne peut donc se faire que si le chiffrement n'est pas activé.
- Le verrouillage du disque n'est effectif que pour un cycle d'extinction complet, un simple reboot n'est pas suffisant. Cette situation permet d'installer un double-boot avec Linux.
- Certains disques semblent gérer également la mise en veille, qui est bloquée autrement par le logiciel de gestion. (testé sur Windows mais pas linux)

Sauvegarde et recouvrement

- Il n'y a pas de mesure spécifique de recouvrement, mais il est possible de déclarer plusieurs comptes utilisateurs, l'un d'entre eux peut donc y être consacré.

En bref

Bien que portable, l'intérêt de cette solution est étroitement lié au système d'exploitation utilisé :

- Sous Windows, le système est simple à mettre en place, et il peut se configurer pour n'avoir aucun impact à l'utilisation
- Sous Linux, le système est à la rigueur utilisable si Windows est également installé en double-boot, avec un impact à l'utilisation (double authentification, aucune administration possible)

Plus d'informations

- Documentation : http://dell.wave.com/dell-complete-hardware-self-encrypting-drive-sed-solution
- Dell Data Protection Access" version Win7 64B : http://www.dell.com/support/drivers/fr/fr/frbsdt1/DriverDetails/Product/latitude-e6430?driverId=TDC1K&osCode=W764&fileId=3089900301

EncFS

Présentation

- EncFS est une solution logicielle de chiffrement de répertoire et de partition sous Linux. Cette solution est également utilisable sur un support externe, qu'il est possible de lire depuis Linux et Windows (en utilisant un portage d'encfs http://members.ferrara.linux.it/freddy77/encfs.html).

Plus d'informations

- le site du projet: http://www.arg0.net/encfs
- Wikipedia : http://en.wikipedia.org/wiki/EncFS
- EncFS sur Ubuntu : http://doc.ubuntu-fr.org/encfs

Coût et licence

- Cette solution est basée sur des logiciels libres, le coût est donc nul.

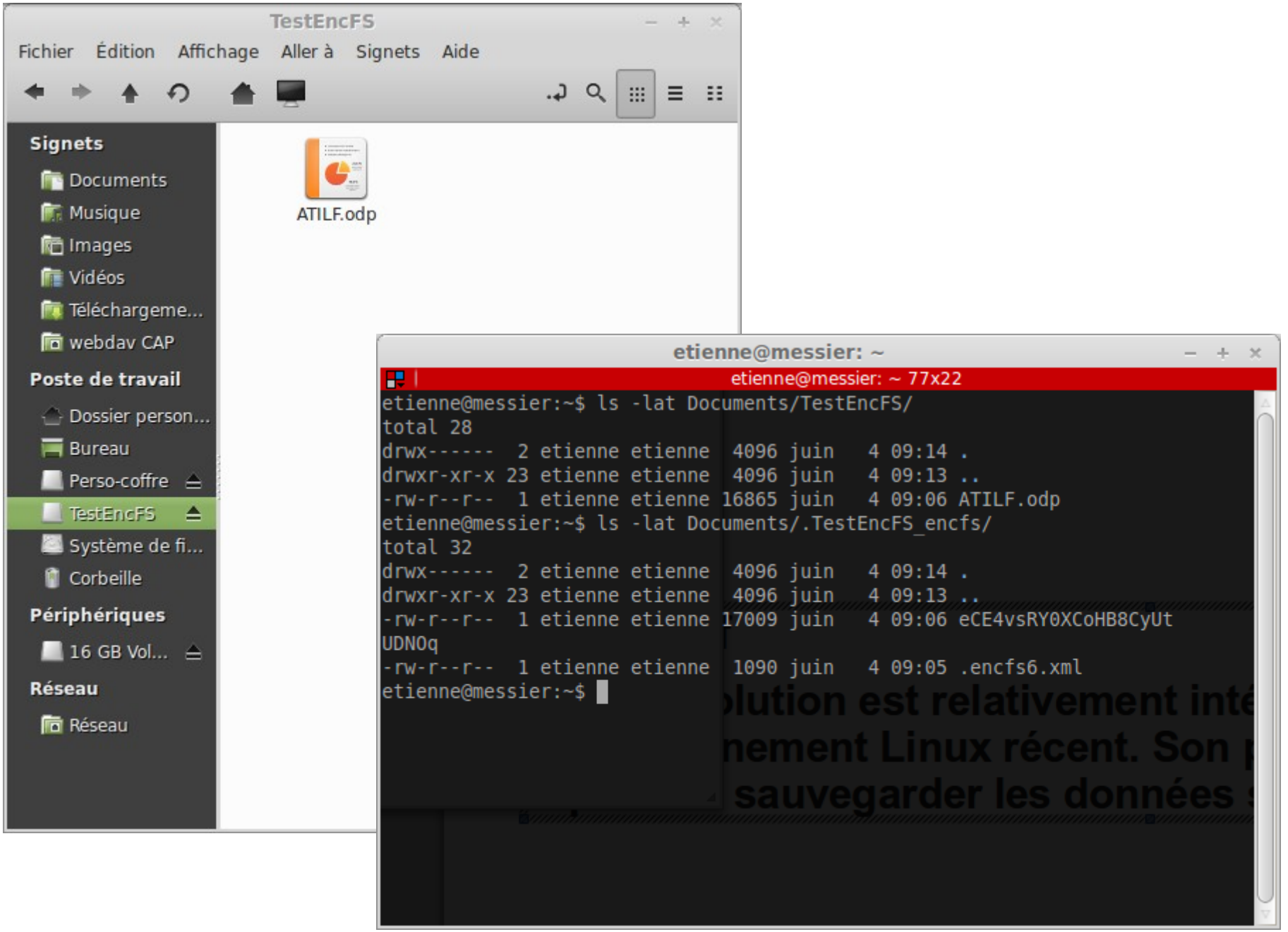
Utilisation

- Cette solution repose sur Fuse, un système générique de système de fichier en espace utilisateur, il faut donc s'attendre à un impact sur les performances.
- Il faut installer le paquetage encfs et fuse-utils.
- Il existe également une interface graphique, cryptkeeper, se matérialisant par une applet dans la barre des tâches, permettant d'automatiser les actions de création et le montage des répertoires chiffrés.

Sauvegarde et recouvrement

- Les données chiffrées sont stockées sous forme de fichiers natifs dans un répertoire d'un système de fichiers. Elles sont donc sauvegardables sans avoir à les déchiffrer au préalable, puisque les métadonnées (liste de fichiers, dates de modifications) sont accessibles depuis le système.

  Il faut néanmoins prendre garde à sauvegarder la clé de chiffrement, contenue dans le fichier .encfs.xml, situé à la base du répertoire source.
- Il n'y aucune procédure de recouvrement possible.


TestEncFS
Fichier Édition Affichage Aller à Signets Aide
Signets
Documents
Musique
Images
Vidéos
Téléchargeme...
webdav CAP
Poste de travail
Dossier person...
Bureau
Perso-coffre
TestEncFS
Système de fi...
Corbeille
Périphériques
16 GB Vol...
Réseau
Réseau
ATILF.odp
etienne@messier: ~
etienne@messier: ~ 77x22
etienne@messier:~$ ls -lat Documents/TestEncFS/
total 28
drwx------ 2 etienne etienne 4096 juin 4 09:14 .
drwxr-xr-x 23 etienne etienne 4096 juin 4 09:13 ..
-rw-r--r-- 1 etienne etienne 16865 juin 4 09:06 ATILF.odp
etienne@messier:~$ ls -lat Documents/.TestEncFS_encfs/
total 32
drwx------ 2 etienne etienne 4096 juin 4 09:14 .
drwxr-xr-x 23 etienne etienne 4096 juin 4 09:13 ..
-rw-r--r-- 1 etienne etienne 17009 juin 4 09:06 eCE4vsRY0XCoHB8CyUt
UDNOq
-rw-r--r-- 1 etienne etienne 1090 juin 4 09:05 .encfs6.xml
etienne@messier:~$

En bref

- Cette solution est relativement intégrée avec un environnement Linux récent. Son principal intérêt est de pouvoir sauvegarder les données sans les déchiffrer.