Dossier partagé localement avec acl

Créer un répertoire partagé entre les utilisateurs d'un même ordinateur sous Linux.

Permissions Unix

Les permissions Unix sont très performantes pour restreindre les accès, mais rendent la création d'un répertoire partagé impossible en pratique.

La solution classique serait de créer un groupe qui regroupe les utilisateurs et de faire en sorte que tous les fichiers partagés appartiennent à ce groupe. Ça fonctionne en théorie, mais dans la pratique, les utilisateurs créent, modifient ou copient des fichiers sans vouloir mettre à jour les permissions groupes. Et seul le propriétaire du fichier peut modifier la permission de groupe du fichier, ce qui rend la chose ingérable.

Le SGID n'est la solution pour propager les droits aux fichiers créés, car il ne se propage pas aux fichiers copiés par l'utilisateur vers
le dossier partagé.

Dans ce cas-ci, nous allons utiliser le contrôle des permissions via les ACL.

Dossier partagé sur un même ordinateur entre utilisateurs sous Linux

On crée un dossier en root /home/Partage-local. Personne ne peut y accéder à part root. Jusqu'ici rien de spécial.

```
cd /home
```

```
sudo mkdir /home/Partage-local
```

```
sudo chmod 770 /home/Partage-local
```

On crée un groupe « partage » auquel on attribue le GID 151 et on ajoute les utilisateurs à ce groupe.

`sudo addgroup --gid 151 partage-local`

`sudo usermod -a -G partage-local nas`

`sudo usermod -a -G partage-local mathieu`

On ajoute des droits étendus pour que les membres du groupe « partage-local » puissent tout faire dans ce dossier. La deuxième ligne fait en sorte que les fichiers nouvellement créés héritent aussi de cette règle ACL.

`sudo setfacl -Rm g:partage-local:rwX /home/Partage-local`

`sudo setfacl -Rm d:g:partage-local:rwX /home/Partage-local`

On peut vérifier les droits finaux ainsi :

`sudo getfacl /home/Partage-local`

```
getfacl : suppression du premier « / » des noms de chemins absolus
# file: home/Partage-local
# owner: root
# group: root
user::rwx
group::rwx
group:partage:rwx
mask::rwx
other::---
default:user::rwx
default:group::rwx
default:group:partage-local:rwx
default:mask::rwx
default:other::---
```

Notes supplémentaires:

Par défaut, le /home/user des utilisateurs n’est pas privé sous Debian ! Si bien que Alice peut lire les fichiers dans /home/bob. Je vous recommande la lecture de ce document sur comment sécuriser Debian, surtout ces 2 points

4.11.13.1 Limiter l’accès aux informations d’autres utilisateurs
4.11.12 Positionner des umasks aux utilisateurs

Le plus important : Pour tous vos utilisateurs existants, assurez que le dossier home bloque bien l’accès aux autres utilisateurs :

`sudo chmod 750 /home/bob`

Ensuite, vous pouvez faire en sorte que soit créé automatiquement comme ça quand vous créez un utilisateur:

`sudo dpkg-reconfigure adduser`

et choisissez Non

Vous pouvez également faire en sorte que les utilisateurs créent par défaut des fichiers que seuls eux peuvent voir :

`sudo echo session optional pam_umask.so umask=027 >> /etc/pam.d/common-session`

Dans */etc/login.defs*, changez la valeur à UMASK

```
027
```

Pour vérifier les droits de l’utilisateur courant :
`sudo umask`