

Les ACL (Access Control Lists) sous Linux

Par op414



www.openclassrooms.com

*Licence Creative Commons 6 2.0
Dernière mise à jour le 20/05/2011*

Sommaire

Sommaire	2
Lire aussi	1
Les ACL (Access Control Lists) sous Linux	3
Avant de commencer... ..	3
Vérifier la configuration du noyau	3
Installation du paquet acl	4
setfacl : Modifier les ACL	4
Ajouter une ACL	4
Supprimer une ACL	6
getfacl : voir les ACL en place	7
Le masque	7
Annexes	8
Copie des ACL (cp et mv)	8
Monter les partitions avec l'option acl	8
Exemple d'utilisation concret	9
ACL et interface graphique	10
Q.C.M.	11
Partager	12

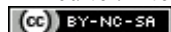


Les ACL (Access Control Lists) sous Linux



Mise à jour : 20/05/2011

Difficulté : Intermédiaire Durée d'étude : 1 heure



Vous avez une machine sous Linux chez vous que toute la famille utilise ?
Ou tout simplement un ordinateur partagé ?

Dans ce cas, vous avez sûrement déjà été confronté à un problème de permissions de fichiers et dossiers, par exemple vous voulez créer un dossier partagé, mais vous ne souhaitez que certains sous-dossiers ne soient accessibles qu'à certains utilisateurs, modifiables par d'autres, etc...

Dans ce cas, le système de permissions de Linux basé sur les utilisateurs et les groupes devient vite un casse-tête sans nom 😞 qui peut conduire à des problèmes de sécurité 😞

Les Access Control Lists (ACL) vous permettent de créer des permissions à la carte, fini la prise de tête 😊, toutes les combinaisons sont possibles.



Il est nécessaire d'avoir suivi le [tutoriel sur Linux de M@teo21](#) jusqu'au chapitre 7 de la partie 2 pour pouvoir suivre ce tutoriel.

Sur ce, commençons 😊

Sommaire du tutoriel :



- [Avant de commencer...](#)
- [setfacl : Modifier les ACL](#)
- [getfacl : voir les ACL en place](#)
- [Annexes](#)
- [Q.C.M.](#)

Avant de commencer...

Vérifier la configuration du noyau

Tout d'abord, sachez que les ACL ne peuvent être utilisées que si le noyau le supporte 😞 ; pour savoir si c'est votre cas, loguez-vous en tant que root avec `sudo su` si vous êtes sous (k)Ubuntu ou `su -` sous debian et les autres distribs. Tapez ensuite :

Code : Console

```
grep ACL /boot/config-*  
  
CONFIG_EXT2_FS_POSIX_ACL=y  
CONFIG_EXT3_FS_POSIX_ACL=y  
CONFIG_EXT4DEV_FS_POSIX_ACL=y  
CONFIG_REISERFS_FS_POSIX_ACL=y
```

```
CONFIG_JFS_POSIX_ACL=y
CONFIG_FS_POSIX_ACL=y
CONFIG_XFS_POSIX_ACL=y
CONFIG_GENERIC_ACL=y
CONFIG_TMPFS_POSIX_ACL=y
CONFIG_JFFS2_FS_POSIX_ACL=y
CONFIG_NFS_V3_ACL=y
CONFIG_NFSD_V2_ACL=y
CONFIG_NFSD_V3_ACL=y
CONFIG_NFS_ACL_SUPPORT=m
```

La ligne suivante indique que le support général des ACL est présent :

Code : Console

```
CONFIG_FS_POSIX_ACL=y
```

Ensuite des lignes du type suivant permettent de savoir pour quels systèmes de fichiers les ACL sont disponibles :

Code : Console

```
CONFIG_SysDeFichiers_FS_POSIX_ACL=y
```

On remarque que chez moi, Les ACL fonctionnent sur les volumes formatés en EXT2, EXT3, EXT4 et pleins d'autres formats exotiques 😊

Les ACL ne sont pas disponibles sur les systèmes vfat (FAT16 et FAT32), vous ne pourrez donc pas utiliser les ACL sur une clé USB formatée pour Windows 😞 Cela ne devrait toutefois pas poser problème 😊.

Si votre noyau ne supporte pas les ACL, vous devez le recompiler. Je n'ai pas eu ce problème, je ne peux donc que vous orienter vers [cet article](http://www.lea-linux.org) du site <http://www.lea-linux.org>

Installation du paquet acl

Les ACL sont activées, mais nous ne pouvons toujours pas les modifier, pour cela nous devons installer le paquet acl :

Code : Console

```
# apt-get install acl
```

Le plus dur est fait, nous pouvons enfin nous servir des ACL 😎



Il est possible que ces manipulations ne suffisent pas pour pouvoir utiliser les ACL, si vous rencontrez des problèmes avec les commandes sous-citées, rendez-vous à l'annexe "*Monter les partitions avec l'option acl*"

setfacl : Modifier les ACL

Ajouter une ACL

Droits classiques

Pour ajouter une ACL, vous devez utiliser la commande `setfacl` avec l'option `-m` :

Code : Console

```
setfacl -m permissions fichierOuDossier
```

les permissions s'écrivent sous cette forme :

Code : Console

```
préfixe:[utilisateurOuGroupe:]droits
```

- Les préfixes disponibles sont :
 - **u:** : Pour modifier les droits d'un utilisateur
 - **g:** : Pour modifier les droits d'un groupe
 - **o:** : Pour modifier les droits du reste du monde (other)
- Pour le préfixe **o:**, il ne faut pas spécifier d'utilisateur (logique, puisque ces droits s'appliquent au reste du monde, qui n'est pas un utilisateur précis 😊)(d'où le `utilisateurOuGroupe:` entre crochets pour ceux qui ne connaissent pas les expressions régulières)
- Les droits s'écrivent sous la forme d'un triplet **rwX** que vous devez déjà connaître :
 - **r** = droit de lecture
 - **w** = droit d'écriture
 - **x** = droit d'exécution pour les fichiers, pour les dossiers, c'est le droit "d'entrée" dans le dossier

Pour ne pas attribuer un droit, vous pouvez ne pas écrire sa lettre correspondante ou la remplacer par un tiret (`r--` est équivalent à `r`)

Code : Console - Exemple

```
setfacl -m u:bernard:rw- test
```

... donnera les droits de lecture et d'écriture à `bernard` pour le fichier `test`.

Ajouter l'option **-R** permet d'appliquer des droits à tout un répertoire :

Code : Console

```
setfacl -Rm u:bernard:rw RepertoireDeTest/
```

... effectuera la même opération que tout à l'heure mais sur tout le dossier `RepertoireDeTest`




L'option **-R** doit être spécifiée avant l'option **-m**

Vous pouvez bien sûr spécifier des permissions pour plusieurs utilisateurs/groupes à la fois 😊, pour cela, séparez-les par une virgule :

Code : Console


```
setfacl -m u:bernard:rw,u:patrice:rwX,g:amis:r,o:--- test
```




`setfacl` permet aussi de modifier les droits classiques (comme `chmod`)  Il faut spécifier un nom vide :

Code : Console

```
setfacl -m u::rwx,g::r--,o:--- test
```

... donnera les droits `rwxr-----` au fichier `test` 

Doits par défaut et héritage

Avec ce que je vous ai appris, si vous appliquez une ACL à un dossier, les fichiers créés ensuite dans ce dossier n'hériteront pas de son ACL. Heureusement, l'héritage des ACL est possible , il suffit de rajouter le préfixe `d:` (comme default) au début de l'ACL :

Code : Console

```
setfacl -m d:u:bernard:rw RepertoireDeTest/
```

Code : Console

```
setfacl -m d:u:bernard:rw,o:--- RepertoireDeTest/
```



Dans cette ACL, seul `u:bernard:rw` sera un droit par défaut ; si vous souhaitez que les fichiers héritent aussi de `o:---`, vous devez taper :

Code : Console

```
setfacl -m d:u:bernard:rw,d:o:--- RepertoireDeTest/
```

Il est cependant possible de se passer du préfixe `d:`, grâce à l'option `-d`, dans ce cas, toutes les permissions spécifiées seront des permissions par défaut :


Code : Console

```
setfacl -dm u:bernard:rw,o:--- RepertoireDeTest/
```

... aura le même effet que le code précédent.




Une fois encore, l'option `-d` doit être spécifiée avant l'option `-m`

Ajouter des droits par défaut ne modifie pas les droits existants , si vous souhaitez ajouter une ACL à tout un répertoire et ses sous-répertoires ET que cette ACL soit héritée par la suite, vous devez le faire de cette manière : (notez la présence de l'option `-R`)

Code : Console

```
setfacl -Rm d:u:bernard:rwx,d:g:amis:r--,d:o:---,u:bernard:rwx,g:amis:r--,o:--- RepertoireDeTest/
```

Voilà  Vous avez fait le plus dur, il ne vous reste qu'à savoir comment enlever et visualiser les ACL.

Supprimer une ACL

Pour supprimer une ACL, il suffit d'utiliser l'option **-b** ...

Code : Console

```
setfacl -b test
```

... supprimera toute l'ACL du fichier test 🧙

Vous pouvez supprimer une partie de l'ACL avec l'option **-x** :

Code : Console

```
setfacl -x u:patrick,g:bernard test
```

... supprimera les permission de l'utilisateur patrick et du groupe amis du fichier test 🧙



Pour supprimer UNIQUEMENT les autorisations par défaut, vous devez utiliser l'option **-k**, TOUTES les permissions par défaut seront supprimées

getfacl : voir les ACL en place

La commande **getfacl** vous permet de connaître les ACL en place :

Code : Console

```
getfacl repertoireDeTest/  
  
# file: repertoireDeTest/  
# owner: op414  
# group: op414  
user::rwx  
user:bernard:rwx  
user:patrick:r--  
group::rwx  
mask::rwx  
other::---  
default:user::rwx  
default:user:bernard:rwx  
default:user:patrick:r--  
default:group::rwx  
default:mask::rwx  
default:other::---
```

je ne m'entends pas sur les résultats, ils sont facile à comprendre 😊, hormis une notion : le masque (mask)

Le masque

Le masque vous permet de savoir quelles sont les autorisations maximales accordées à un fichier ou dossier (utilisateurs et groupes confondus), les droits classiques (chmod) ne sont pas comptabilisés.

Code : Console

```
getfacl test

# file: test
# owner: op414
# group: op414
user::rwx
user:bernard:rwx
user:patrick:r--
group::rwx
mask::rwx
other:--
```

Ici, le masque est rwx car bernard possède les droits rwx.

L'utilité du masque est de pouvoir enlever des permissions à tous les utilisateurs et groupes (sauf de l'utilisateur propriétaire, dont les droits sont définis par `chmod`):

Code : Console

```
setfacl -m m:r-- test
```

Vous remarquez qu'il faut utiliser le préfixe `m:` (comme mask). Refaisons un coup de `getfacl` sur le fichier 😊 :

Code : Console

```
getfacl test

# file: test
# owner: op414
# group: op414
user::rwx
user:bernard:rwx          #effective:r--
user:patrick:r--         #effective:r--
group::rwx                #effective:r--
mask::r--
other:---
```

On remarque que les droits de bernard, patrick et du groupe propriétaire n'ont pas été modifiés (ce qui permet de les rétablir en ré-augmentant le masque 😊). En revanche, il est maintenant écrit `#effective:r--` en face de leurs lignes. Cela signifie que leurs droits réellement appliqués sont r-- ! 😎

Annexes

Copie des ACL (cp et mv)

Les commandes `cp` et `mv` sont capables de conserver les ACL. Il suffit de spécifier l'option `-a` lors de l'utilisation de `cp`. `mv` le fait au-to-ma-ti-que-ment 😊. Bien entendu, le répertoire cible doit être situé sur une partition gérant les ACL 😊.

Un dernier point : quand un fichier possède une ACL et que vous faites un `ls -l`, l'ACL ne peut être écrite en entier ; le signe + s'affiche pour signifier la présence de l'ACL : `-rw-rw----+` 😊

Monter les partitions avec l'option acl



Si vous lisez cette sous-partie, c'est que les commandes `setfacl` et `getfacl` n'ont pas fonctionné chez vous. Ces manipulations doivent être effectuées en tant qu'utilisateur root

Pour que vous puissiez utiliser les ACL, les partitions doivent être montées avec l'option correspondante...

Code : Console

```
# mount -t ext3 -o defaults,acl /dev/hda1/ /home
```

... pour monter la partition 2 du premier disque, formatée en ext3 dans le répertoire /home

Vous pouvez remonter un partition déjà montée :

Code : Console

```
# mount -o remount,acl /home
```

Si vous voulez que le volume soit monté automatiquement avec l'option acl, vous devez modifier le fichier /etc/fstab

Code : Console

```
# nano /etc/fstab
```

Vous devez rajouter **,acl** dans la colonne "options" de la partition concernée :

Code : Console

```
/dev/sda1      /                  ext3    errors=remount-ro 0      1
```

devient chez moi :

Code : Console

```
/dev/sda1      /                  ext3    errors=remount-ro,acl 0      1
```

Voilà, ma partition principale sera automatiquement montée avec l'option acl au démarrage 🧙‍♂️ Si vous avez une partition /home séparée, vous devez bien entendu modifier sa ligne.

Il ne vous reste plus qu'à redémarrer ou remonter les partitions concernées comme vu précédemment 😊

Exemple d'utilisation concret

Voici un exemple d'utilisation des ACL, il est issu de ma propre utilisation de vos nouvelles meilleures amies 😊

Si vous créez un serveur web grâce à [ce tuto](#), vous risquez d'avoir un petit problème de permissions.

En effet, votre machine ne possède que deux **vrais** comptes utilisateur (le votre et le compte root), si vous vous loggez en FTP, le serveur vsFTPD utilise l'utilisateur www-data. Le compte **virtuel** d'administration a accès à tout le répertoire /home mais ne pourra pas entrer dans votre répertoire personnel car celui-ci appartient à votre compte utilisateur et non pas à www-data 😞

Pour palier ce problème, il suffit d'utiliser cette ACL :

Code : Console

```
setfacl -Rm d:u:www-data:rwX,d:u:op414:rwX,u:www-data:rwX,u:op414:rwX /home/op414
```

... dans le cas où votre compte utilisateur est op414

Le problème est résolu 😊

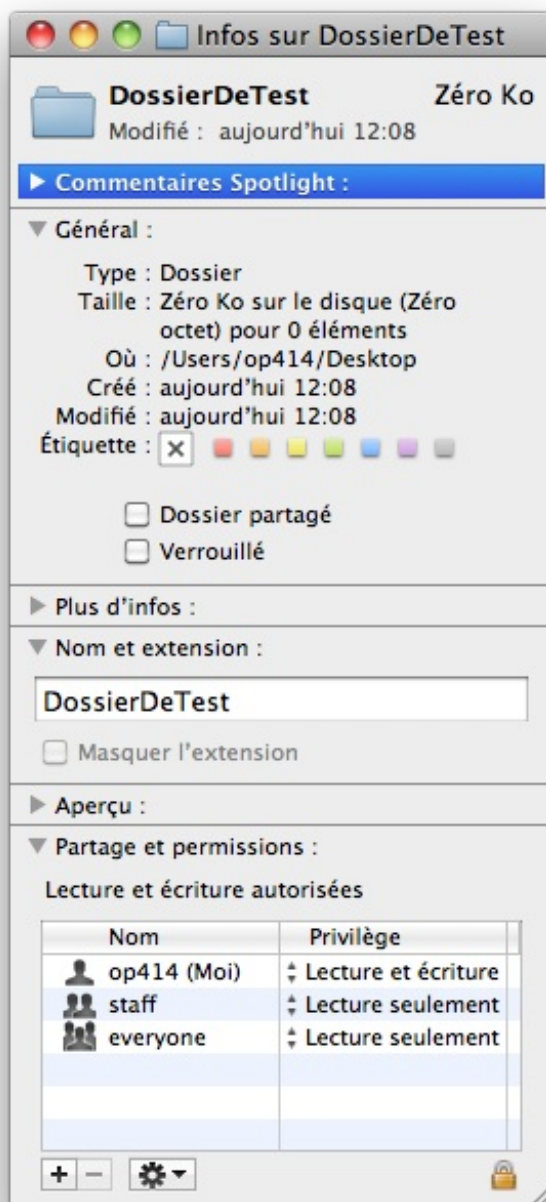
PS: Il aurait également été possible de supprimer votre compte utilisateur (A NE SURTOUT PAS FAIRE SOUS UBUNTU ET

DÉRIVÉS CAR IL EST IMPOSSIBLE DE SE LOGGER EN ROOT), mais le seul moyen de se connecter en SSH à votre serveur aurait été le compte root, ce qui est dangereux car il vaut mieux empêcher la possibilité de se connecter en root via SSH pour limiter les dégâts en cas d'attaque. Il est donc préférable de garder un compte utilisateur standard 😊

ACL et interface graphique

Sous Mac OS X

Sous Mac OS X, les ACL sont activées par défaut et paramétrables via l'interface graphique 😊 Il suffit de sélectionner un dossier ou fichier puis d'afficher le panneau d'informations (pomme + i ou cmd + i)



La section "Partage et Permissions" est celle qui nous intéresse. Le plus en bas à gauche permet d'ajouter une ACL pour un utilisateur, tandis que le moins permet de supprimer un utilisateur de la liste. L'icône d'engrenage permet d'appliquer l'ACL à tous les fichiers et dossiers d'un répertoire. Si vous n'êtes pas le propriétaire du fichier ou dossier, un mot de passe administrateur vous sera demandé 😊

Sous KDE (Dolphin)

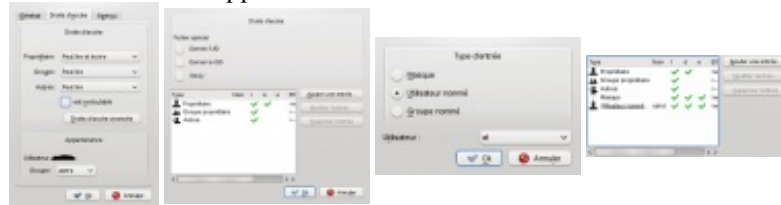
Les ACL peuvent aussi être modifiées via l'interface graphique 😊

Voilà comment faire sous KDE, muni de Dolphin, un explorateur de fichiers.



Merci à chaispaquichui pour les captures.

Allez dans les information du fichier, puis cliquez sur l'onglet «Droits d'accès» puis sur «Droits d'accès avancés». Vous pouvez ensuite ajouter des entrées, les modifier et les supprimer.



Q.C.M.

Le premier QCM de ce cours vous est offert en libre accès.
Pour accéder aux suivants

Connectez-vous Inscrivez-vous



Les ACL peuvent-elles être utilisées sur une volume formaté en *vfat* ?

- ☐ Oui
- ☐ Non



Quelle est l'option à utiliser pour modifier une ACL ?

- ☐ -R
- ☐ -m
- ☐ -f
- ☐ -b



Le masque est une synthèse de ...

- ☐ ... toutes les permissions
- ☐ ... les permissions de l'ACL



Quel est le préfixe pour modifier le masque ?

- ☐ u:
- ☐ m:
- ☐ g:
- ☐ o:

Correction !

Statistiques de réponses au QCM

Voilà, les ACL n'ont plus de secret pour vous 😊 J'espère que cela vous sera utile. Ceci est mon premier tutoriel, si vous avez des remarques ou des questions, n'hésitez pas à les écrire dans les commentaires de ce tuto 😊



Ce tutoriel bien que réécrit dans sa totalité a été largement inspiré par cet article du site <http://www.lea-linux.org/>, publié sous licence GNU par Vincent Ramos.

Partager

