


Les ACL ou Access Control List

- Objet : Les ACL, gestion fines des droits
- Niveau requis : [avisé](#)
- Commentaires : Vous voulez créer un dossier partagé entre toto, titi et tata, mais vous ne souhaitez que certains sous-dossiers ne soient accessibles qu'à toto et d'autre à tata. Sans les ACL, c'est vite un casse tête.
- Suivi :
 - [à-tester, à-completer](#)
 - Création par  [smolski](#) le 02/12/2011
 - Testé par <...> le <...>
- Commentaires sur le forum : [ici](#)¹⁾

Introduction

La mise en place des ACL permet une gestion fine des accès des utilisateurs, des groupes, aux répertoires et aux fichiers d'une partition qui dispose d'un "file system" qui accepte les acl. (par ex: Ext3).

Il faut installer le paquetage acl

```
apt-get update && apt-get install acl
```



Puis il faut déclarer la prise en charge des acl dans le fichier /etc/fstab en ajoutant ",acl" après "defaults" de la partition concernée:



Plus nécessaire sous Wheezy le 16/01/2014

```
/dev/VOLUME/5 /donnees ext3 defaults,acl 1 2
```

Vous redémarrez ensuite votre serveur.

La mise en place des ACL implique trois notions principales:

1. ACL « minimale - Composée exclusivement d'éléments de type propriétaire, groupe et « reste du monde », l'ACL minimale est une traduction « en ACL » des droits d'accès traditionnels Unix.
2. ACL étendue - L'ACL étendue prolonge les droits de l'ACL minimale. Elle contient au moins un élément de type mask et peut contenir des éléments de type utilisateur et/ou groupe.
3. ACL par défaut - Les ACL par défaut ne peuvent être appliquées qu'aux répertoires et définissent de quels droits un objet du système de fichiers devra hériter (de son répertoire parent) lors de sa création.

Les commandes

Le paquetage acl permet de disposer de deux nouvelles commandes:

getfacl

Cette commande permet l'affichage des acl

```
getfacl nom_de_repertoire # affiche les acl de nom_de_repertoire
```

Le format de sortie de getfacl ressemble à ceci :

Pour un répertoire qui ne dispose que des acl "minimales"

[retour de la commande](#)

```
# file: nom_de_repertoire
# owner: root
# group: root
  user::rwx
  group::rwx
  other::---
```

Ce qui correspond au :

```
ls -al nom_de_repertoire
      drwxrwx--- 1 root root 596354 sep  4 20:59
nom_de_repertoire
```

Pour un répertoire qui dispose d'acl étendues et d'acl par défaut :

[retour de la commande](#)

```
# file: nom_de_repertoire
# owner: root
# group: root
  user::rwx                # Les droits du propriétaire
  user:joe:rwx             # Les droits de l'utilisateur
supplémentaire joe
  group::rwx                # Les droits du groupe du propriétaire
  group:cool:rwx           # Les droits du groupe supplémentaire cool
  group:hot:r-x            # Les droits du groupe supplémentaire hot
  group:cold:---           # Les droits du groupe cold
  mask:rwx                 # Les droits les plus élevés
  other:---                # Les droits des "autres"
  default:user::rwx        # Les droits par défaut sont attribués
automatiquement pour
  default:user:joe:rwx     # les nouveaux fichiers et répertoires
```

```
créés.  
  default:group::rwx      # Les acl par défaut ne concernent donc  
que les répertoires  
  default:group:hot:r-x  
  default:group:cold:---  
  default:mask:rwx  
  default:other:---
```

Il est utile d'enregistrer l'ensemble des acl quand on a un serveur de fichiers dans une communauté de travail hétérogène (des centaines d'utilisateurs et de groupes). Cette manipulation peut se faire grâce à la commande:

```
getfacl -R /donnees > nom_de_fichier      # L'option -R permet la  
récursivité sur tous les répertoires,      # sous-répertoires et fichiers  
de la partition /donnees                  # L'enregistrement de  
l'ensemble de ces acl est effectué dans    # le fichier nom_de_fichier
```

setfacl

Cette commande permet l'attribution des acl. Voici quelques explications sur son utilisation.

Attribution des acl étendues

```
setfacl -m g:cool:rwx nom_de_repertoire  # Pour ajouter le groupe cool et  
ses droits pour le                        # répertoire non_de_repertoire
```

```
setfacl -m g:cool:rwx nom_de_fichier      # Pour ajouter le groupe cool et  
ses droits pour le                        # fichier non_de_fichier
```

```
setfacl -m u:fany:rwx nom_de_repertoire  # Pour ajouter l'utilisateur fany  
et ses droits pour le                    # répertoire non_de_repertoire
```

En utilisant -R pour la récursivité,

```
setfacl -R -m g:cool:rwx nom_de_repertoire # Pour ajouter le groupe cool et  
ses droits pour le                        # répertoire, l'ensemble des  
sous-répertoires et                      # fichiers du répertoire  
non_de_repertoire
```

Attribution des acl par défaut

```
setfacl -m d:g:cool:rwX nom_de_repertoire # Pour ajouter le groupe cool et  
ses droits par défaut  
non_de_repertoire # pour le répertoire
```

En utilisant -R pour la récursivité :

```
setfacl -R -m d:g:cool:rwX nom_de_repertoire # Pour ajouter le groupe cool  
et ses droits par défaut  
l'ensemble des sous-répertoires # pour le répertoire,  
non_de_repertoire # et fichiers du répertoire
```

Attribution des acl à l'aide d'un fichier

Il est possible de restituer l'ensemble des acl d'une partition grâce au fichier obtenu par la commande :

```
getfacl -R /donnees > nom_de_fichier
```

Pour ce faire, il suffit de se placer à la racine et d'exécuter la commande :

```
setfacl --restore=nom_de_fichier
```

S'il s'agit de restituer les acl sur une arborescence plus petite on peut utiliser:

```
setfacl -R -M nom_de_fichier repertoire
```

Suppression des acl

Pour supprimer tous les acl:

```
setfacl -b repertoire # Suppression juste pour le répertoire
```

```
setfacl -b fichier # Suppression juste pour le fichier
```

```
setfacl -R -b repertoire # Suppression pour le répertoire, les sous-  
répertoires et fichiers
```

Pour supprimer les acl par défaut :

```
setfacl -k repertoire # Suppression juste pour le répertoire
```

```
setfacl -R -k repertoire # Suppression pour le répertoire, les sous-
```

répertoires

Conclusion

Je vous laisse imaginer l'ensemble des possibilités (grâce aux man setfacl, man getfacl) et si l'on couple cela avec le SGID. Tout est faisable.... et peu de système d'exploitation offre un tel panel d'outils.

Comme lecture sur le sujet, une page du site Léa-Linux : [Gestion des ACL](#).

1)

N'hésitez pas à y faire part de vos remarques, succès, améliorations ou échecs !

From:

<http://debian-facile.org/> - **Documentation - Wiki**

Permanent link:

<http://debian-facile.org/doc:systeme:acl>

Last update: **19/03/2017 20:47**

