FICHE Ressource : Les ACL (Access Control List) sous Linux

Les ACL (Access Control List) sous Linux
Installation du paquet ACL
setfacl : Modifier les ACL
getfacl : voir les ACL en place

1. Les ACL (Access Control List) sous Linux

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

2. Installation du paquet ACL

Vérifiez votre connexion à Internet puis procédez à une mise à jour avant d'installer le paquet ACL

 # dnf install acl (CentOS)
 # apt install acl (Debian)
Ajouter les utilisateur suivants avec la commande adduser

3. setfacl : Modifier les ACL

3.1. Ajouter une ACL

- Droits classiques

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

setfacl -m permissions fichierOuDossier

les permissions s'écrivent sous cette forme :

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 connaitre :
  - `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)

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 :

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 spécifier des permissions pour plusieurs utilisateurs/groupes à la fois :) , pour cela, séparez-les par une virgule :

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 :

setfacl -m u::rwx,g::r--,o:--- test ==> donnera les droits rwxr----- au fichier test :)

- Droits 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 :

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

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

Il 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 :

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)

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

3.2. Supprimer une ACL

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

setfacl -b test ==> supprimera toute l'ACL du fichier test :magicien:

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

setfacl -x u:patrick,g:bernard test ==> supprimera les permission de l'utilisateur partick 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

4. getfacl : voir les ACL en place

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

```
getfacl reperoireDeTest/

# file: reperoireDeTest/
# 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::---
```

Attention le masque « mask » ne sera pas toujours présent dans le résultat de la commande getfacl ***s'il n'a pas été utilisé auparavant.***

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.

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`):

setfacl -m m:r-- test

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

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-- !