**Gestion des ACL (Listes de Contrôle d'Accès) sous Linux**

**Objectifs du cours :**

* Comprendre ce que sont les ACL et leur utilité.
* Apprendre à configurer et gérer les ACL pour des fichiers et répertoires.
* Savoir utiliser les commandes getfacl et setfacl pour manipuler les ACL.
* Appliquer les ACL dans des scénarios réels, comme la gestion de répertoires collaboratifs.

**Module 1 : Introduction aux ACL**

**1.1. Qu'est-ce qu'une ACL ?**

* Une **ACL (Access Control List)** est un mécanisme qui permet de définir des permissions d'accès plus fines que les permissions standard (utilisateur, groupe, autres).
* Elle permet d'attribuer des permissions spécifiques à des utilisateurs ou groupes particuliers.

**1.2. Pourquoi utiliser les ACL ?**

* Les permissions standard (chmod) sont limitées à un seul utilisateur, un seul groupe, et les autres.
* Les ACL permettent :
  + D'ajouter plusieurs utilisateurs ou groupes avec des permissions différentes.
  + De définir des permissions spécifiques pour des cas complexes.

**1.3. Prérequis**

* Vérifiez que votre système de fichiers supporte les ACL (ext4, XFS, etc.).
* Installez les outils nécessaires :

sudo apt install acl # Pour Debian/Ubuntu

sudo yum install acl # Pour CentOS/RHEL

**Module 2 : Commandes de base pour les ACL**

**2.1. getfacl : Afficher les ACL**

* Affiche les permissions ACL d'un fichier ou répertoire.

getfacl fichier.txt

Exemple de sortie :

Copy

# file: fichier.txt

# owner: user1

# group: group1

user::rw-

user:user2:r--

group::r--

mask::rw-

other::r--

**2.2. setfacl : Modifier les ACL**

* Ajoute, modifie ou supprime des entrées ACL.
  + Ajouter une permission pour un utilisateur :

setfacl -m u:user2:rw fichier.txt

* + Ajouter une permission pour un groupe :

setfacl -m g:group2:r fichier.txt

* + Supprimer une entrée ACL :

setfacl -x u:user2 fichier.txt

**2.3. Options courantes de setfacl**

* -m : Modifie ou ajoute une entrée ACL.
* -x : Supprime une entrée ACL.
* -b : Supprime toutes les ACL.
* -R : Applique les ACL de manière récursive (pour les répertoires).
* -d : Définit des ACL par défaut pour les nouveaux fichiers/répertoires.

**Module 3 : Exemples pratiques**

**3.1. Exemple 1 : Ajouter des permissions pour un utilisateur**

1. Créez un fichier :

touch fichier.txt

1. Ajoutez une permission en lecture/écriture pour user2 :

setfacl -m u:user2:rw fichier.txt

1. Vérifiez les ACL :

getfacl fichier.txt

**3.2. Exemple 2 : Ajouter des permissions pour un groupe**

1. Créez un répertoire :

mkdir mon\_repertoire

1. Ajoutez une permission en lecture pour group2 :

setfacl -m g:group2:r mon\_repertoire

1. Vérifiez les ACL :

getfacl mon\_repertoire

**3.3. Exemple 3 : Supprimer une entrée ACL**

1. Supprimez l'entrée ACL pour user2 :

setfacl -x u:user2 fichier.txt

1. Vérifiez les ACL :

getfacl fichier.txt

**Module 4 : Ateliers pratiques (avec corrections)**

**4.1. Gestion des ACL pour un fichier**

**Objectif** : Créer un fichier, ajouter des ACL pour un utilisateur et un groupe, puis vérifier et supprimer les ACL.

**Étapes** :

1. Créez un fichier test.txt :

touch test.txt

1. Ajoutez une permission en lecture pour l'utilisateur user2 :

setfacl -m u:user2:r test.txt

1. Ajoutez une permission en écriture pour le groupe group2 :

setfacl -m g:group2:w test.txt

1. Affichez les ACL pour vérifier :

getfacl test.txt

1. Supprimez toutes les ACL du fichier :

setfacl -b test.txt

1. Vérifiez que les ACL ont été supprimées :

getfacl test.txt

**4.2. Gestion des ACL pour un répertoire**

**Objectif** : Créer un répertoire, ajouter des ACL pour un utilisateur et un groupe, appliquer les ACL de manière récursive, et vérifier.

**Étapes** :

1. Créez un répertoire mon\_dossier :

mkdir mon\_dossier

1. Ajoutez une permission en lecture/écriture pour l'utilisateur user3 :

setfacl -m u:user3:rw mon\_dossier

1. Ajoutez une permission en lecture pour le groupe group3 :

setfacl -m g:group3:r mon\_dossier

1. Appliquez les ACL de manière récursive :

setfacl -R -m u:user3:rw mon\_dossier

setfacl -R -m g:group3:r mon\_dossier

1. Vérifiez les ACL pour le répertoire :

getfacl mon\_dossier

**4.3. Suppression des ACL**

**Objectif** : Créer un fichier, ajouter plusieurs ACL, puis supprimer une entrée ACL spécifique et toutes les ACL.

**Étapes** :

1. Créez un fichier fichier\_acl.txt :

touch fichier\_acl.txt

1. Ajoutez des ACL pour plusieurs utilisateurs et groupes :

setfacl -m u:user4:rw fichier\_acl.txt

setfacl -m g:group4:r fichier\_acl.txt

setfacl -m u:user5:x fichier\_acl.txt

1. Vérifiez les ACL :

getfacl fichier\_acl.txt

1. Supprimez l'entrée ACL pour user4 :

setfacl -x u:user4 fichier\_acl.txt

1. Vérifiez les ACL après suppression :

getfacl fichier\_acl.txt

1. Supprimez toutes les ACL du fichier :

setfacl -b fichier\_acl.txt

1. Vérifiez que les ACL ont été supprimées :
2. getfacl fichier\_acl.txt

**Module 5 : Exemple complet avec répertoire collaboratif**

**Contexte**

Un répertoire partagé /projects/collab est configuré pour les groupes **devs** et **designers**. L'utilisateur **designer3** ne doit avoir qu'un accès en lecture seule.

**Étapes :**

1. Créez le répertoire partagé :

sudo mkdir -p /projects/collab

1. Définissez le groupe propriétaire sur **devs** :

sudo chgrp devs /projects/collab

1. Activez le bit **set-GID** :

sudo chmod g+s /projects/collab

1. Définissez les permissions de base :

sudo chmod 770 /projects/collab

1. Ajoutez des ACL pour le groupe **designers** :

sudo setfacl -m g:designers:rwx /projects/collab

1. Limitez l'accès de **designer3** à la lecture seule :

sudo setfacl -m u:designer3:r-x /projects/collab

1. Appliquez les ACL par défaut :

sudo setfacl -d -m g:designers:rwx /projects/collab

sudo setfacl -d -m u:designer3:r-x /projects/collab

**Vérification :**

1. Vérifiez les permissions et ACL :

ls -ld /projects/collab

getfacl /projects/collab

1. Testez les permissions avec les utilisateurs dev1, designer1, et designer3.

**Module 6 : Bonnes pratiques et pièges à éviter**

**6.1. Bonnes pratiques**

* Utilisez les ACL uniquement lorsque les permissions standard ne suffisent pas.
* Documentez les ACL pour éviter la confusion.
* Testez les ACL dans un environnement de test avant de les appliquer en production.

**6.2. Pièges à éviter**

* Évitez d'ajouter trop d'entrées ACL, car cela peut devenir difficile à gérer.
* N'oubliez pas de vérifier les ACL après les modifications.
* Assurez-vous que les utilisateurs et groupes existent avant d'ajouter des ACL.

**Évaluation**

**7.1. Questions théoriques**

1. Quelle commande permet d'afficher les ACL d'un fichier ?
2. Comment ajouter une permission en lecture pour un utilisateur avec setfacl ?
3. Quelle option de setfacl permet de supprimer toutes les ACL ?

**7.2. Exercice pratique**

1. Créez un fichier rapport.txt.
2. Ajoutez une permission en lecture/écriture pour un utilisateur et une permission en lecture pour un groupe.
3. Vérifiez les ACL avec getfacl.
4. Supprimez toutes les ACL du fichier.

**Conclusion**

Ce cours complet vous a permis de comprendre et de manipuler les ACL sous Linux. Vous êtes maintenant capable de configurer des permissions avancées pour des fichiers et répertoires, et de gérer des environnements collaboratifs complexes. Continuez à pratiquer pour maîtriser ces concepts !

**Ressources supplémentaires**

* Documentation : man getfacl, man setfacl.