Auteur: P. Petit	*Titre: TD Unix utilisateurs locaux*	*Version: 1.0*
Date: 21/09/2010	Licence: Gnu Free Documentation Licence	Durée: 1h00

Utilisateurs locaux et droits d'accès sous unix

Objectifs

- gestion des utilisateurs et des groupes sous unix
- gestion des droits d'accès aux dossiers ou aux fichiers sous unix

Configuration initiale

Ce TD est à réaliser avec une station sous linux ubuntu ou debian ou une machine solaris 10.

Prérequis

- pratique de base d'unix, pratique du shell et des commandes de base, pratique d'un éditeur de texte

Exercice 1: gestion des utilisateurs et des groupes

1. creéz les utilisateurs test1, test2, test3 et test4 de mots de passe respectif: passtest1, passtest2, passtest3 et passtest4 à l'aide de la commande adduser.
2. Quel est le shell de connexion de vos utilisateurs. Changer celui de test3 pour /bin/sh
3. créez un groupe nommé **projet1** à l'aide de la commande addgroup. Consultez le fichier /etc/group pour trouver son gid et la liste des utilisateurs y appartenant.
4. ajoutez les utilisateurs test1 et test2 au groupe **projet1** en utilisant la commande useradd.

Exercice 2: gestion des droits d'accès: chmod

1. ouvrez un session en tant que test1 et créez un dossier **Projets** dans votre dossier personnel. Créez deux dossiers **Projet1** et **Projet2** dans **Projets**.
2. On souhaite avoir les accès suivant placé sur ces dossiers :
    - test1 a un accès en écriture à Projets; test1, test2 et test3 peuvent s'y déplacer et en lister le contenu
    - test1 et test2 ont un accès en lecture, écriture et peuvent se déplacer dans Projet1. test3 peut seulement s'y déplacer mais ne peut en lister le contenu ni y créer de fichiers
    - test1 est seul à avoir accès à projet2; test2 et test3 n'y ont aucun accès.

Exercice 3: gestion des droits d'accès

Créez un fichier test.txt à l'aide d'un éditeur de texte. Executez ensuite la commande « chmod 070 test.txt ». Quel accès avez-vous à ce fichier ? Expliquez en tenant compte que les membres de votre groupe ont un accès RWX à ce fichier.

Exercice 4: acl posix: mise en place du support (Linux seulement)

Les acl posix permettent de gérer des listes de contrôle d'accès. Une entrée d'une telle liste est une autorisation (RWX) qui s'applique à un utilisateur nommé ou à un groupe nommé. Le nombre d'entrée d'une acl dépend du système de fichiers: 32 sous ext3fs, 8191 sous XFS ou ReiserFS. Le

support des ACL suppose trois choses : 1) que le système d'exploitation les supportent (OK pour linux 2.6 et pour les dernièrs 2.4), 2) que le système de fichier les supportent (OK pour ext3FS, ReiserFS, ...) et 3) que les outils de manipulation de fichiers les supportent (là, on n'est loin du compte). La mise en oeuvre des acl sous linux debian sarge ou linux Ubuntu avec système de fichier ext3fs nécessite deux choses :

1. que les systèmes de fichiers soient montés avec l'option acl. Ajoutez l'option acl aux systèmes de fichiers mentionnés dans le fichier /etc/fstab. Quand cette option sera-t-elle prise en compte ? Une autre solution consiste à changer les options d'une partition montée à l'aide de la commande mount avec les options ad hoc : « mout -o remount,acl / ». Après avoir expliqué cette commande et ses options, utilisez la. Vérifiez ensuite que l'option acl a bien été prise en compte.
2. que le package acl soit installé:
    - après avoir donné à la variable d'environnement http_proxy la valeur du proxy à utiliser si nécessaire (http://proxy-www.miage.info.univ-evry.fr:3128/ pour le dept informatique),
    - lancez l'installation par « apt-get install acl » ou via l'outil aptitude (graphique en mode texte, F10 pour avoir le menu) ou synaptic (graphique sous gnome).

Exercice 5: acl posix: une première approche de leur utilisation (solaris et Linux)

On parlera dans cet exercice et dans les suivants des ACL POSIX (Linux, Solaris 10). Les acl proposées par SOLARIS 10/zfs ont un fonctionnement différent et ne sont pas décrites ici.

Les commandes setfacl et getfacl permettent respectivement de modifier et d'afficher les acl d'un fichier. Il est possible d'ajouter une entrée pour un utilisateur ou un groupe à une acl de la façon suivante :

- setfacl -m u:uid:perm fichier : l'utilisateur uid (nom ou numérique) obtient les permissions perm (symbolique ou numérique) sur le fichier m. ex: setfacl -m u:petit:rwx test (petit obtient les droits rwx sur test).
- setfacl -m g:gid:perm : idem pour un groupe. Ex.: setfacl -m g:projet1:rwd p1 (le groupe projet1 obtient les droits rwx sur le fichier g1)

L'acl par défaut d'un dossier (se positionne avec le paramètre -d en plus de -m) est l'acl qu'auront les objets créés dans un dossier. Elle est indépendante des autres acl définies sur un objet.

Il est possible de consulter les acl d'un fichier avec la commande fgetacl. On peut effacer une entrée avec l'option -x de setfacl.

1. ouvrez une session en tant que test2. Créez un dossier P1.
2. comparer le résultat des commandes « ls -l » et « getfacl » appliquées à P1. Cette acl est appelée l'acl minimale.
3. donnez le droit de lecture et parcours à test3 sur P1.
4. donnez le droit de lecture, écriture et parcours aux membres du groupe TD sur P1.
5. Vérifiez dans les deux cas précédents le résultat de votre commande :
    - à l'aide de getfacl

- en ouvrant des sessions en tant que test2 et test3 et en testant ce que vous pouvez faire sur/dans P1.

6. Définissez comme acl par défaut sur P1:
   - lecture/écrire/parcours pour le groupe TD
   - lecture/parcours pour le reste du monde
7. créez un dossier SP1 dans P1 et vérifiez l'effet de votre ACL par défautls.
   - lecture/écrire/parcours pour le groupe TD
   - lecture/parcours pour le reste du monde