Fiche n° :1

diafor
organisation

Epreuve de Pratique des Techniques Informatiques

Nom et prénom : **ALO David**

Nature de l'activité

Partage de fichiers avec Samba et configuration des droits avec ACL POSIX

Contexte : Une entreprise avec plusieurs employés décide que chacun d'eux peut partager des documents afin de faciliter les échanges. Cependant, des restrictions doivent être proposées car certaines personnes ont des droits plus limités que d'autres.

Objectifs :

- Attribuer des droits spécifiques à chaque répertoire
- Créer un serveur de partage

Compétences mises en œuvre pour la réalisation de cette activité

C22	Installer et configurer un réseau
C25	Installer un applicatif
C31	Assurer les fonctions de base de l'administration d'un réseau
C32	Assurer les fonctions de l'exploitation

Conditions de réalisations

Matériels :	Logiciels :
- 1 serveur - 1 poste	- Debian Etch - Windows XP
Durée : 45 mn	

Autres contraintes et difficultés : les fichiers créés doivent avoir les mêmes droits que les répertoires parents

Description de l'activité réalisée

Situation initiale : les fichiers sont dispatchés sur les PC des salariés

Situation finale : Les documents sont partagés et sécurisés

I. Installation de Samba

L'installation de Samba est extrêmement simple. Il suffit de passer la commande suivante :

```
> aptitude install samba
```

II. Installation de ACL POSIX

Il faut dans un premier temps vérifier s'il est possible de l'installer. En effet, tous les formats de partition n'acceptent pas l'intégration de droit ACL.
Pour vérifier si notre noyau les accepte, il faut chercher dans le fichier /boot/config*

```
> cat /boot/config* | grep _ACL
```

De cette façon, nous pourrons distinguer l'association partition/ACL acceptée par notre noyau, il faut maintenant vérifier si nous avons bien le type de partition qui convient.

```
> df -T
```

Si cela nous convient, il ne reste plus qu'à installer ACL POSIX et monter dans fstab pour une utilisation dès le démarrage de l'ordinateur

```
> aptitude install acl
> vim /etc/fstab
    /dev/hda1      /       ext3            default,acl       0          0
```

Nous devons alors redémarrer l'ordinateur pour prendre les informations en compte.

III. Création des utilisateurs, des groupes et des répertoires

Pour commencer, il faut créer les groupes :

```
> addgroup direction adminitratif commercial machines
```

Puis les utilisateurs avec leurs groupes associés. Il nous faut les créer deux fois chacun. En effet, ils doivent être présents dans l'annuaire UNIX (/etc/passwd) ainsi que dans l'annuaire SAMBA (/etc/samba/smbpasswd)

```
> adduser jeanyves --ingroup direction
> adduser stef --ingroup administratif
> adduser tanguy --ingroup commercial
> smbpasswd -a root
> smbpasswd -a jeanyves
> smbpasswd -a stef
> smbpasswd -a tanguy
```

Ajouter la machine sur laquelle on va travailler

```
> adduser machinetest$ --ingroup machines –no-create-home --force-badname
> smbpasswd -a -m machinetest
```

Enfin créer les répertoires qui seront à partager

```
/home> mkdir direction administratif commercial
```

IV. Configuration de Samba

Samba est assez simple à configurer, il a juste un fichier de configuration dans lequel il faut rajouter ou décommenter des lignes
Ce fichier se trouve dans /etc/samba/smb.conf

```
[global]
   workgroup = PTITEST                  (nom du domaine)
   wins support = yes                   (support de serveur WINS)
   netbios name = randy                 (nom du netbios du serveur)
   dns proxy = no                       (utilisation du proxy)
   name resolve order = wins lmhosts host bcast      (ordre de recherche de résolution de nom)

##Autentification##
   security = user                      (oblige chaque utilisateur à avoir un compte samba)

##Domains##
   domain logons = yes                  (pour que samba fasse contrôleur de domaine)

##Misc##
   domain master = auto                 (automatisation de l'attribution "explorateur maître de domaine. le maitre de
domaine recueille les listes d'exploration de chaque explorateur qui le contacte et fournit les listes à ceux qui lui la
demande)

##Share##
[direction]
   browseable = yes
   path = /home/direction
   writeable = yes
[administratif]
   browseable = yes
   path = /home/administratif
   writeable = yes
[commercial]
   browseable = yes
   path = /home/commercial
   writeable = yes
```

Pour une vérification de la bonne configuration du fichier smb.conf, nous pouvons exécuter l'utilitaire « testparm ».

Pour actualiser samba

```
> /etc/init.d/samba restart
```

Il est désormais possible de se connecter sous windows sur le domaine nouvellement créé.

Il suffit de faire un clic droit sur le poste de travail et allez dans propriété, puis l'onglet « nom de l'ordinateur » puis « modifier ». Changer alors le domaine. Windows vous demande un nom d'utilisateur et un mot de passe qui sont les informations « root ».
Il accepte l'intégration et vous demande de redémarrer.
Avant de redémarrer, exécuter la commande « gpedit.msc » et changer les propriétés du profil itinérant. Sinon, un message d'erreur risque d'apparaitre pour dire qu'il ne trouve pas le profil itinérant. Il est normal de ne pas en trouver puisque nous n'avons pas configuré samba pour cela.
A ce niveau, chaque utilisateur peut donc se connecter au domaine et créer des documents dans son répertoire propre. Les autres n'ont pas encore eu leurs attributions de droit et donc ne sont pas modifiable par les utilisateurs. Pour y remédier, nous allons attribuer des droits à chaque groupe sur leurs répertoires respectif.

```
/home > chgrp administratif administratif/
/home > chgrp direction direction/
/home > chgrp commercial commercial/
/home > chmod 770 administratif/ direction/ commercial/
/home > ls -l
```

Par mesure de sécurité, nous ne mettons aucun accès pour le reste du monde.

Nous avons alors atteint la limite des droits accordés par Linux. Pour les affiner d'avantage, il faut utiliser ACL Posix.

V. Configuration des droits ACL

Les ACL permettent de mettre en place des stratégies de sécurité qui ne seraient pas réalisable avec les mécanismes standards. Pour l'examen, nous allons utiliser un scénario simplifié :
On décide que la direction a un droit de regard et d'écriture sur tous les répertoires existants. Les instances administratives et commerciales ont un droit de regard et d'écriture sur leurs propres répertoires uniquement.

Si l'on veut que la direction puisse avoir un accès en écriture et lecture sur tous les dossiers :

```
/home > setfacl -R -m g:direction:rwx administratif/ commercial/
```

Pour vérifier l'ajout de la nouvelle définition:

```
/home >getfacl administratif/ commercial/
```

Cependant, les documents, nouvellement créé par la direction dans un répertoire autre que le sien, auront comme propriétaire « jean-yves » et comme groupe « direction ». Le groupe originel du répertoire ne pourra donc pas modifier le document créé. Les caractéristiques données par les ACL ne sont pas étendues aux nouveaux fichiers. Pour avoir des droits sur les futurs documents, il faut mettre en place une ACL par défaut.

```
/home > setfacl -m d:g:administratif:rwx administratif/
/home > setfacl -m d:g:commercial:rwx commercial/
/home > setfacl -m d:g:direction:rwx direction/ administratif/ commercial/
```

Analyse des résultats obtenus
Objectif atteint : Chaque utilisateur est rattaché au domaine et peux créer des documents avec les droits correspondants
Bilan de l'activité : Le domaine est fonctionnel ainsi que les partages. Le tout est sécurisé par des droits choisis avec précaution.