TD Samba

1 Installation de Samba

Il est conseillé d'effectuer ce TD en binôme

1.1 Installation d'une machine virtuelle Debian

Prévoir deux disques de machine virtuelle. Un pour le système, l'autre pour y ajouter des partages

Commandes utiles :

fdisk

mkfs.ext4

mount

Le deuxième disque doit être monté sous /disk pour la suite du TD

Mettre l'interface réseau en bridge sur eth0 ou wlan0 si connexion filaire ou wifi

Si besoin d'un ISO d'OS, demander au formateur

1.2 Installation de Samba

```
# apt update
# apt install samba
```

Par défaut, samba sera dans l'état démarré

```
root@samba1:~# ps ax
...
 1424 ?        Ss     0:00 /usr/sbin/smbd -D
 1452 ?        S      0:00 /usr/sbin/smbd -D
 1485 ?        Ss     0:00 /usr/sbin/nmbd -D
...
```

- Stopper le service Samba

Pour rappel, les commandes de base (gestion services)

```
Compatibilité SysV
/etc/init.d/samba start|stop|restart|reload

Avec Systemd
systemctl start|stop|restart|reload samba
```

Le fichier de configuration générale est présent ici : /etc/samba/smb.conf

Par défaut, ce fichier est doté de commentaires de configuration.

Pour obtenir un fichier propre, faire les commandes suivantes :

```
# mv /etc/samba/smb.conf /etc/samba/smb.conf.orig
# testparm -s /etc/samba/smb.conf.orig > /etc/samba/smb.conf
```

Fichier smb.conf obtenu

```
# Global parameters
[global]
	server role = standalone server
	map to guest = Bad User
	obey pam restrictions = Yes
	pam password change = Yes
	passwd program = /usr/bin/passwd %u
	passwd chat = *Enter\snew\s*\spassword:* %n\n *Retype\snew\s*\spassword:* %n\n
*password\supdated\ssuccessfully* .
	unix password sync = Yes
	syslog = 0
	log file = /var/log/samba/log.%m
	max log size = 1000
	dns proxy = No
	usershare allow guests = Yes
	panic action = /usr/share/samba/panic-action %d
	idmap config * : backend = tdb


[homes]
	comment = Home Directories
	valid users = %S
	create mask = 0700
	directory mask = 0700
	browseable = No


[printers]
	comment = All Printers
	path = /var/spool/samba
	create mask = 0700
	printable = Yes
	print ok = Yes
	browseable = No


[print$]
	comment = Printer Drivers
	path = /var/lib/samba/printers
```

Arrêtons-nous sur ce fichier ...

1.3 Création d'un partage public

Ajouter ce bloc au fichier /etc/samba/smb.conf

```
[public]
  comment = Partage public
  path = /disk/public
  read only = no
  public = yes
  guest ok = yes
```

Créer le dossier /disk/public et donner les droits :

```
# chmod 777 /disk/public
```

Enregistrer le fichier et recharger (ou redémarrer) Samba

1.4 Création et édition d'utilisateurs et groupes

Créer les utilisateurs suivants dans votre système Linux. Les groupes d'appartenance sont notés en face. Seul frank n'a pas de groupe, le groupe tmp n'est pas à créer. Il doit cependant avoir accès au répertoire “it” de façon temporaire.

alice : administration

bob : it, administration

charlie : it

dan : business

eve : communication, it

frank : (tmp)

Commandes utiles :

```
# useradd -m <nom_utilisateur>

# groupadd <nom_groupe>

# usermod -G <nom_groupe_1,nom_groupe_2> <nom_utilisateur>

# smbpasswd -a <nom_utilisateur> # permet de donner un mot de passe SMB à l'utilisateur UNIX

# pdbedit -Lv
```

1.5 Création d'un partage par groupe

```
[g_groupe]
  comment = g_groupe
  path = /disk/g_groupe
  read only = no
  writable = yes
  create mask = 0777
  directory mask = 0777
  write list = @g_groupe, u_utilisateur
  valid users = @g_groupe, u_utilisateur
```

Remplacer “g_groupe” par le nom du groupe.

Ajouter autant de partage que de groupes. Ces partages doivent porter le nom du groupe. Le groupe administration doit avoir accès à tous les partages

Créer tous les dossiers indiqués par “path”.

Donner les droits :

```
# chmod 777 /disk/g_groupe
```

Redémarrer Samba

Le contrôle d’accès se fait donc par le biais des options valid users et write list.

1.6 Commandes utiles

testparm : permet de tester la configuration de smb.conf, nettoie la configuration avec les options nécessaires (oublie les paramètres par défaut)

smbcontrol : substitue la gestion des services nativement

smbstatus : permet de voir quels utilisateurs sont connectés au serveur, les partages accèdés ainsi que les fichiers vérrouillés

smbpasswd : gestion de la table d'utilisateur locale samba, fonctionnant avec la table UNIX. Permet de mettre à jour les mots de passe dans la base SAM

pdbedit : Gestion très précise de la table des utilisateurs locaux

nmblookup : équivalent nslookup pour la résolution de nom NetBIOS

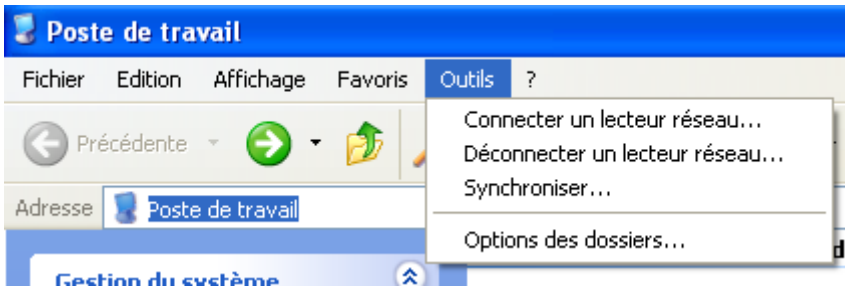
smbclient : client FTP-like pour le protocole SMB

2 Accéder aux données via un lecteur réseau Windows et d'un client sur UNIX

2.1 Via Windows

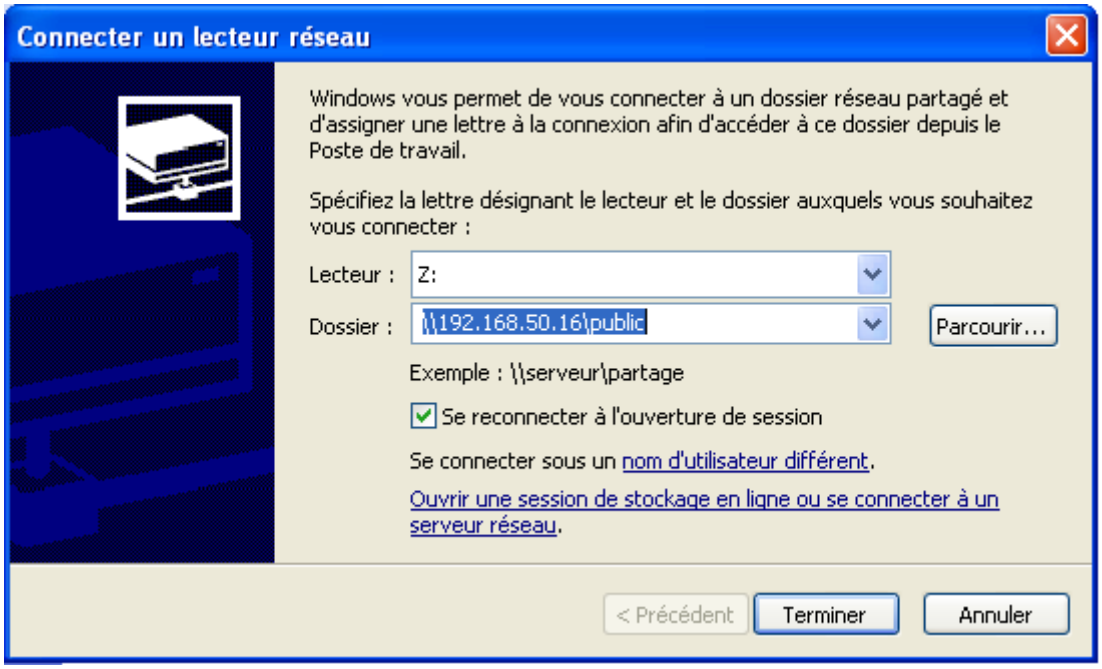
Prévoir l'installation d'une machine virtuelle Windows XP si peu de RAM, sinon Windows 7

Connecter le lecteur réseau : Aller dans l'explorateur, puis Outils > Connecter un lecteur réseau



Une fenêtre s'ouvre.

Indiquer le chemin UNC : \\adresse_ip\partage



S'il faut indiquer un utilisateur différent, cliquer sur “nom d'utilisateur différent”

2.2 Via UNIX

apt install cifs-utils smbclient

Via mount :

mount.cifs -o user=utilisateur,pass=password //ip_serveur/partage

Via smbclient (le mot de passe est demandé ensuite) :

smbclient -U utilisateur //ip_serveur/partage

Remarque : on doit utiliser des “/” normaux sur Linux car le “\” est réservé à l'échappement de caractères dans un shell UNIX

Tester ensuite les accès aux fichiers en binôme, en fonction des groupes, utilisateurs, partages créés. En déduire la cohérence des accès.

3 Pour aller plus loin

3.1 Gestion des ACL POSIX

Maintenant nous allons ajouter un partage supplémentaire nommé commun. Les droits donnés dans le partage vont permettre d'attribuer une sécurité différente que celle effectuée jusque là.

apt install acl

Dans le fichier fstab, ajouter acl dans la liste des options. Puis faire :

mount -o remount /disk

/disk est remonté avec les ACL

Sauvegarder votre fichier de configuration smb.conf à un autre endroit

Attention, à partir de là on supprime tous les droits existants sur /disk

```
# chmod -R 700 /disk/business /disk/it /disk/administration /disk/communication
# chown -R nobody:nogroup /disk/business /disk/it /disk/administration /disk/communication
```

On applique les acl par groupe. Refaire la même commande pour chaque groupe.

```
# setfacl -R -d -m group:g_groupe:rwx /disk/g_groupe
# setfacl -R -m group:g_groupe:rwx /disk/g_groupe
# setfacl -R -d -m user:u_utilisateur:rwx /disk/g_groupe
# setfacl -R -m user:u_utilisateur:rwx /disk/g_groupe
```

Études des options de setfacl / getfacl

Ensuite créer le partage suivant, tout simplement :

```
[commun]
  comment = commun
  path = /disk
  read only = no
  inherit acls = yes
  inherit owner = yes
  inherit permissions = yes
```

Accéder au partage par : \\ip_serveur\commun (Windows) ou //ip_serveur/commun (Linux)

Le contrôle d’accès est effectué par l’OS.

3.2 Active Directory

Monter un Samba 4 en mode Active Directory et mettre en place des utilisateurs, groupes, partages et des droits sur ces partages avec des ACL POSIX.