# Partages ACL pour Linux et Windows

Partage réseaux avec ACL sous Linux

Permissions Unix

Les permissions Unix sont très performantes pour restreindre les accès, mais rendent la création d’un partage réseau impossible en pratique.

La solution classique serait de créer un groupe qui regroupe les utilisateurs et de faire en sorte que tous les fichiers partagés appartiennent à ce groupe. Ça fonctionne en théorie, mais dans la pratique, les utilisateurs créent, modifient ou copient des fichiers sans vouloir mettre à jour les permissions groupes. Et seul le propriétaire du fichier peut modifier la permission de groupe du fichier, ce qui rend la chose ingérable.

Le SGID n’est la solution pour propager les droits aux fichiers créés, car il ne se propage pas aux fichiers copiés par l’utilisateur vers
le dossier partagé.

Dans ce cas-ci, nous allons utiliser le contrôle des permissions via les ACL. Celles-ci seront propagées au travers des partages NFS et Samba en activant cette fonctionnalité dans plusieurs fichiers de configuration.

Partages réseaux via NFS et Samba

Pour la mise en place de cette solution compatible sous Linux et sous Windows, il faut choisir un groupe (GID) qui sera commun au contrôle des permissions ainsi qu’au partage Samba sous Windows. Le choix logique se tourne vers le groupe sambashare déjà prévu pour Samba.

Il faut s’assurer que le groupe sambashare utilise le même gid sur toutes les machines du réseau.

Sur Ubuntu le groupe sambashare par défaut au GID 111 alors que sur Solydxk c'est le GID 1001. Le GID 111 est utilisé pour pulseaudio et il y aura donc un conflit:

`cat /etc/group` sur Solydxk, nous renvoi les GID des groupes et on constate donc que 111 est bien attribué à pulse-access

```
pulse-access:x:111:
```

Il faut donc changer le GID de sambashare sur Ubuntu et sur Solydxk. J'ai choisi 150 qui n'est pas utilisé sur aucun des deux systèmes.

S.V.P., notez que le UID de tous les fichiers qui sont dans le répertoire personnel (home) d'un usager seront changés automatiquement dès que les usermod et groupmod seront lancées.

Toutefois, les fichiers situés ailleurs que dans le dossier personnel (home) doivent être changés manuellement avec les commandes respectives « find / -group » pour le GID et find / -user pour l'UID.

Sur le serveur Ubuntu (111), afin d'attribuer un nouveau GID au groupe sambashare, entrer:

`sudo groupmod -g 150 sambashare`

`sudo find / -group 111 -exec chgrp -h sambashare {} \;`

Sur les clients Solydxk (1001) afin d'attribuer un nouveau GID au groupe sambashare, entrer:

`sudo groupmod -g 150 sambashare`

`sudo find / -group 1001 -exec chgrp -h sambashare {} \;`

> *Note:*

> *S’il faut changer l’uid 1000 >> 1001 pour un usager alors utiliser les commandes suivantes*
> `sudo usermod -u 1001 olivier`
>
> `sudo find / -user 1000 -exec chown -h olivier {} \;`

## Pour utiliser le contrôle de permission par acl:

Sur le serveur:

Installer samba

`sudo apt-get install samba`

Il faut s’assurer que les différents éléments ont été compilés avec le support des ACL. La vérification s’effectue de la manière suivante:

`sudo su`

`grep ACL /boot/config-*`

```
/boot/config-3.13.0-71-generic:CONFIG_EXT4_FS_POSIX_ACL=y
/boot/config-3.13.0-71-generic:CONFIG_REISERFS_FS_POSIX_ACL=y
/boot/config-3.13.0-71-generic:CONFIG_JFS_POSIX_ACL=y
/boot/config-3.13.0-71-generic:CONFIG_XFS_POSIX_ACL=y
/boot/config-3.13.0-71-generic:CONFIG_BTRFS_FS_POSIX_ACL=y
/boot/config-3.13.0-71-generic:CONFIG_FS_POSIX_ACL=y
/boot/config-3.13.0-71-generic:CONFIG_GENERIC_ACL=y
/boot/config-3.13.0-71-generic:CONFIG_TMPFS_POSIX_ACL=y
/boot/config-3.13.0-71-generic:CONFIG_HFSPLUS_FS_POSIX_ACL=y
/boot/config-3.13.0-71-generic:CONFIG_F2FS_FS_POSIX_ACL=y
/boot/config-3.13.0-71-generic:CONFIG_NFS_V3_ACL=y
/boot/config-3.13.0-71-generic:CONFIG_NFSD_V2_ACL=y
/boot/config-3.13.0-71-generic:CONFIG_NFSD_V3_ACL=y
/boot/config-3.13.0-71-generic:CONFIG_NFS_ACL_SUPPORT=m
/boot/config-3.13.0-71-generic:CONFIG_CIFS_ACL=y
/boot/config-3.13.0-71-generic:CONFIG_9P_FS_POSIX_ACL=y
/boot/config-3.13.0-73-generic:CONFIG_EXT4_FS_POSIX_ACL=y
/boot/config-3.13.0-73-generic:CONFIG_REISERFS_FS_POSIX_ACL=y
```

```
/boot/config-3.13.0-73-generic:CONFIG_JFS_POSIX_ACL=y
/boot/config-3.13.0-73-generic:CONFIG_XFS_POSIX_ACL=y
/boot/config-3.13.0-73-generic:CONFIG_BTRFS_FS_POSIX_ACL=y
/boot/config-3.13.0-73-generic:CONFIG_FS_POSIX_ACL=y
/boot/config-3.13.0-73-generic:CONFIG_GENERIC_ACL=y
/boot/config-3.13.0-73-generic:CONFIG_TMPFS_POSIX_ACL=y
/boot/config-3.13.0-73-generic:CONFIG_HFSPLUS_FS_POSIX_ACL=y
/boot/config-3.13.0-73-generic:CONFIG_F2FS_FS_POSIX_ACL=y
/boot/config-3.13.0-73-generic:CONFIG_NFS_V3_ACL=y
/boot/config-3.13.0-73-generic:CONFIG_NFSD_V2_ACL=y
/boot/config-3.13.0-73-generic:CONFIG_NFSD_V3_ACL=y
/boot/config-3.13.0-73-generic:CONFIG_NFS_ACL_SUPPORT=m
/boot/config-3.13.0-73-generic:CONFIG_CIFS_ACL=y
/boot/config-3.13.0-73-generic:CONFIG_9P_FS_POSIX_ACL=y
/boot/config-3.13.0-74-generic:CONFIG_EXT4_FS_POSIX_ACL=y
/boot/config-3.13.0-74-generic:CONFIG_REISERFS_FS_POSIX_ACL=y
/boot/config-3.13.0-74-generic:CONFIG_JFS_POSIX_ACL=y
/boot/config-3.13.0-74-generic:CONFIG_XFS_POSIX_ACL=y
/boot/config-3.13.0-74-generic:CONFIG_BTRFS_FS_POSIX_ACL=y
/boot/config-3.13.0-74-generic:CONFIG_FS_POSIX_ACL=y
/boot/config-3.13.0-74-generic:CONFIG_GENERIC_ACL=y
/boot/config-3.13.0-74-generic:CONFIG_TMPFS_POSIX_ACL=y
/boot/config-3.13.0-74-generic:CONFIG_HFSPLUS_FS_POSIX_ACL=y
/boot/config-3.13.0-74-generic:CONFIG_F2FS_FS_POSIX_ACL=y
/boot/config-3.13.0-74-generic:CONFIG_NFS_V3_ACL=y
/boot/config-3.13.0-74-generic:CONFIG_NFSD_V2_ACL=y
/boot/config-3.13.0-74-generic:CONFIG_NFSD_V3_ACL=y
/boot/config-3.13.0-74-generic:CONFIG_NFS_ACL_SUPPORT=m
/boot/config-3.13.0-74-generic:CONFIG_CIFS_ACL=y
/boot/config-3.13.0-74-generic:CONFIG_9P_FS_POSIX_ACL=y
/boot/config-3.19.0-33-generic:CONFIG_EXT4_FS_POSIX_ACL=y
/boot/config-3.19.0-33-generic:CONFIG_REISERFS_FS_POSIX_ACL=y
/boot/config-3.19.0-33-generic:CONFIG_JFS_POSIX_ACL=y
/boot/config-3.19.0-33-generic:CONFIG_XFS_POSIX_ACL=y
/boot/config-3.19.0-33-generic:CONFIG_BTRFS_FS_POSIX_ACL=y
/boot/config-3.19.0-33-generic:CONFIG_FS_POSIX_ACL=y
/boot/config-3.19.0-33-generic:CONFIG_TMPFS_POSIX_ACL=y
/boot/config-3.19.0-33-generic:CONFIG_HFSPLUS_FS_POSIX_ACL=y
/boot/config-3.19.0-33-generic:CONFIG_JFFS2_FS_POSIX_ACL=y
/boot/config-3.19.0-33-generic:CONFIG_F2FS_FS_POSIX_ACL=y
/boot/config-3.19.0-33-generic:CONFIG_NFS_V3_ACL=y
/boot/config-3.19.0-33-generic:CONFIG_NFSD_V2_ACL=y
```

```
/boot/config-3.19.0-33-generic:CONFIG_NFSD_V3_ACL=y
/boot/config-3.19.0-33-generic:CONFIG_NFS_ACL_SUPPORT=m
/boot/config-3.19.0-33-generic:CONFIG_CEPH_FS_POSIX_ACL=y
/boot/config-3.19.0-33-generic:CONFIG_CIFS_ACL=y
/boot/config-3.19.0-33-generic:CONFIG_9P_FS_POSIX_ACL=y
/boot/config-3.19.0-39-generic:CONFIG_EXT4_FS_POSIX_ACL=y
/boot/config-3.19.0-39-generic:CONFIG_REISERFS_FS_POSIX_ACL=y
/boot/config-3.19.0-39-generic:CONFIG_JFS_POSIX_ACL=y
/boot/config-3.19.0-39-generic:CONFIG_XFS_POSIX_ACL=y
/boot/config-3.19.0-39-generic:CONFIG_BTRFS_FS_POSIX_ACL=y
/boot/config-3.19.0-39-generic:CONFIG_FS_POSIX_ACL=y
/boot/config-3.19.0-39-generic:CONFIG_TMPFS_POSIX_ACL=y
/boot/config-3.19.0-39-generic:CONFIG_HFSPLUS_FS_POSIX_ACL=y
/boot/config-3.19.0-39-generic:CONFIG_JFFS2_FS_POSIX_ACL=y
/boot/config-3.19.0-39-generic:CONFIG_F2FS_FS_POSIX_ACL=y
/boot/config-3.19.0-39-generic:CONFIG_NFS_V3_ACL=y
/boot/config-3.19.0-39-generic:CONFIG_NFSD_V2_ACL=y
/boot/config-3.19.0-39-generic:CONFIG_NFSD_V3_ACL=y
/boot/config-3.19.0-39-generic:CONFIG_NFS_ACL_SUPPORT=m
/boot/config-3.19.0-39-generic:CONFIG_CEPH_FS_POSIX_ACL=y
/boot/config-3.19.0-39-generic:CONFIG_CIFS_ACL=y
/boot/config-3.19.0-39-generic:CONFIG_9P_FS_POSIX_ACL=y
/boot/config-3.19.0-41-generic:CONFIG_EXT4_FS_POSIX_ACL=y
/boot/config-3.19.0-41-generic:CONFIG_REISERFS_FS_POSIX_ACL=y
/boot/config-3.19.0-41-generic:CONFIG_JFS_POSIX_ACL=y
/boot/config-3.19.0-41-generic:CONFIG_XFS_POSIX_ACL=y
/boot/config-3.19.0-41-generic:CONFIG_BTRFS_FS_POSIX_ACL=y
/boot/config-3.19.0-41-generic:CONFIG_FS_POSIX_ACL=y
/boot/config-3.19.0-41-generic:CONFIG_TMPFS_POSIX_ACL=y
/boot/config-3.19.0-41-generic:CONFIG_HFSPLUS_FS_POSIX_ACL=y
/boot/config-3.19.0-41-generic:CONFIG_JFFS2_FS_POSIX_ACL=y
/boot/config-3.19.0-41-generic:CONFIG_F2FS_FS_POSIX_ACL=y
/boot/config-3.19.0-41-generic:CONFIG_NFS_V3_ACL=y
/boot/config-3.19.0-41-generic:CONFIG_NFSD_V2_ACL=y
/boot/config-3.19.0-41-generic:CONFIG_NFSD_V3_ACL=y
/boot/config-3.19.0-41-generic:CONFIG_NFS_ACL_SUPPORT=m
/boot/config-3.19.0-41-generic:CONFIG_CEPH_FS_POSIX_ACL=y
/boot/config-3.19.0-41-generic:CONFIG_CIFS_ACL=y
/boot/config-3.19.0-41-generic:CONFIG_9P_FS_POSIX_ACL=y
```

Je crois que oui!

`sudo apt-get install acl`

On crée un dossier en root /media/nas1 et 2. Personne ne peut y accéder à part root. Jusqu'ici rien de spécial.

`cd /media`

`sudo mkdir /media/nas1`

`sudo mkdir /media/nas2`

`sudo chmod 770 /media/nas1`

`sudo chmod 770 /media/nas2`

Activation du support ACL:

Configuration de NFS (Serveur: De Linux à Linux) :

Sur la machine serveur :

`sudo apt-get install nfs-kernel-server`

Adapter le fichier /etc/exports pour les partages NFS

Afin d'éviter de créer une foule d'utilisateurs sur tous les différents ordinateurs du réseau et de devoir s'assurer que les UID et GID soient identiques, nous utiliserons l'option all_squash combinée à anonuid et anongid afin de se faire tous passer pour l'utilisateur nas sur les partages NFS

`sudo nano /etc/exports`

```
# /etc/exports: the access control list for filesystems which may be exported
# to NFS clients. See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes hostname1(rw,sync,no_subtree_check)
hostname2(ro,sync,no_subtree_check)
```

```
#
/media/nas1
192.168.0.0/24(rw,sync,no_subtree_check,all_squash,anonuid=1000,anongid=150)
/media/nas2
192.168.0.0/24(rw,sync,no_subtree_check,all_squash,anonuid=1000,anongid=150)
/home/nas
192.168.0.0/24(rw,sync,no_subtree_check,all_squash,anonuid=1000,anongid=1000)
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes gss/krb5i(rw,sync,no_subtree_check)
#
```

Pour déactiver les ACL sur les partages NFS lors de la configuration du serveur, ajouter l'option no_acl dans le fichier /etc/exports.

On peut mettre chaque adresse ip: 192.168.0.10(rw,sync,no_subtree_check) 192.168.0.11(rw,sync,no_subtree_check) ou si on mets *.reseau.maison à la place de l'adresse ip, tous les ordinateurs du réseau pourront se brancher. Vous pouvez remplacer * par l'un des formats de nom d'hôte. La formulation du nom d'hôte devrait être la plus précise possible pour éviter que des systèmes indésirables puissent accéder aux points de montage NFS.

Note: il n'est pas possible de partager en NFS des disques NTFS (Windows)

`service nfs-kernel-server restart`

ajouter `,acl` au montage des disques:

`sudo nano /etc/fstab`

```
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point> <type> <options> <dump> <pass>
```

```
# / was on /dev/sda2 during installation
UUID=987b3b37-0b57-41c6-85a6-362d272ff34d / ext4 discard,errors=remount-ro 0 1
# /home was on /dev/sda4 during installation
UUID=53c7ee74-c5ac-4149-a6a9-cd6fe3436604 /home ext4 discard,defaults,acl 0 2
# swap was on /dev/sda3 during installation
UUID=cca42254-bb12-4c61-9bec-50fc1dbd60cd none swap sw 0 0

# /media/nas1
UUID=6edc9052-a976-419c-9741-d60e58b7df62 /media/nas1 ext4 defaults,acl 0 2

# /media/nas2
UUID=c5612a29-102b-4100-aff6-9a1e9912f137 /media/nas2 ext4 defaults,acl 0 2



#mp3fs mount
mp3fs#/media/nas1/Audio/Musique/ /media/nas1/Audio/sub_mp3-128/ -ogainmode=1,fuse
allow_other,ro,bitrate=128 0 0
```

Une ligne vide doit terminer le fichier /etc/fstab sinon il y aura une erreur

Les répertoires /media/nas1 et /media/nas2 du point de montage doit exister. Il ne devrait y avoir ni fichiers ni sous-répertoires dans ces répertoires.

Pour déactiver les ACL des partages NFS lors du montage sur un client, utiliser l’option no_acl via la ligne de commande ou dans le fichier /etc/fstab.

Une fois fait, remontez le point de montage.

`sudo mount -o remount,acl /home`

`sudo mount -o remount,acl /`

Configuration de base pour Samba (Serveur: De Linux à Windows) :

Si le groupe sambashare n’existe pas, il faut alors le créer

`sudo addgroup --gid 150 sambashare`

L’utilisateur nas a déjà son compte créé lors de l’installation, mais pour que

chacun des autres utilisateurs Windows puisse s'authentifier sous Samba, il faut créer des utilisateurs sans dossier personnel (home) et sans accès au shell. Il faudra ajouter chacun des nouveaux utilisateurs sur les clients Windows du réseau pour une gestion fine des permissions ou encore utiliser le compte virtuel.

L'utilisateur « virtuel » pourra être utilisé sous Windows pour effectuer la connexion au serveur de fichiers Ubuntu ceci limitera le nombre d'utilisateurs à créer et à ajouter au fichier de configuration de Samba.

Énumérer les usagers déjà présents sur le système

`cat /etc/passwd`

```
nas:x:1000:1000:nas,,,:/home/nas:/bin/bash
```

Ajouter l'utilisateur générique qui sera utilisé sous Windows

`sudo useradd -s /bin/false -d /dev/null -g sambashare virtuel`

Énumérer les usagers présents sur le système suite aux ajouts

`cat /etc/passwd`

```
virtuel:x:1001:150::/dev/null:/bin/false
nas:x:1000:1000:nas,,,:/home/nas:/bin/bash
```

ou

`cut -d: -f1 /etc/passwd`

Afin de mettre en place le contrôle d'accès aux fichiers, il faut ajouter chacun des utilisateurs au groupe sambashare incluant les services démarrés sous un autre nom d'utilisateur tel que LMS, Mediatomb, Deluge car on veut que ces services puissent lire ou écrire des listes de lectures, fichiers en

téléchargement etc.:

`sudo usermod -a -G sambashare nas`

`sudo usermod -a -G sambashare squeezeboxserver`

`sudo usermod -a -G sambashare mediatomb`

`sudo usermod -a -G sambashare deluge`

`sudo usermod -a -G sambashare virtuel`

Pour vérifier les associations via la console:

`cat /etc/group`

```
sambashare:x:150:nas,virtuel,squeezeboxserver,mediatomb,deluge
```

> *note:*
> *Les commandes suivantes peuvent s'avérer utiles durant la configuration*
>
> *`sudo adduser denis sambashare ou usermod -a -G sambashare denis`*
>
> *Si erreurs:*
> *`sudo deluser --remove-home denis`*
>
> *`sudo groupdel sambashare`*

Dernière chose à faire avant de pouvoir accéder au répertoire partagé de votre machine sous Samba (Windows), il faut créer des mots de passe pour les comptes qui auront accès à ceux-ci. Samba n'utilise pas les mots de passe du système, mais a son propre fichier pour stocker ceux-ci (/etc/smbpasswd).

Pour créer les mots de passe samba pour chaque utilisateur du partage :

```
sudo smbpasswd -a  (remplacer)
```

`sudo smbpasswd -a nas`

`sudo smbpasswd -a virtuel`

```
New SMB password:
Retype new SMB password:
Added user username.
```

Ensuite, effectuer la configuration de Samba pour la mise en place du partage sous Windows

`sudo nano /etc/samba/smb.conf`

```
#======================= Global Settings =======================

[global]

#Ajout pour le support ACL
 vfs objects = acl_xattr
 map acl inherit = yes
 store dos attributes = yes
 #socket options = TCP_NODELAY IPTOS_LOWDELAY SO_RCVBUF=8192 SO_SNDBUF=8192
 name resolve order = bcast host
 #rlimit_max= 16384

## Browsing/Identification ###

# Change this to the workgroup/NT-domain name your Samba server will part of
 workgroup = WORKGROUP

# server string is the equivalent of the NT Description field
 server string = %h server (Samba, Ubuntu)
 hide files = /lost+found/.Trash*/
 # Windows Internet Name Serving Support Section:
 # WINS Support - Tells the NMBD component of Samba to enable its WINS Server
 # wins support = no
```

```
# WINS Server - Tells the NMBD components of Samba to be a WINS Client
 # Note: Samba can be either a WINS Server, or a WINS Client, but NOT both
 ; wins server = w.x.y.z

# This will prevent nmbd to search for NetBIOS names through DNS.
 dns proxy = no

#### Networking ####

# The specific set of interfaces / networks to bind to
 # This can be either the interface name or an IP address/netmask;
 # interface names are normally preferred
 ; interfaces = 127.0.0.0/8 eth0

# Only bind to the named interfaces and/or networks; you must use the
 # 'interfaces' option above to use this.
 # It is recommended that you enable this feature if your Samba machine is
 # not protected by a firewall or is a firewall itself. However, this
 # option cannot handle dynamic or non-broadcast interfaces correctly.
 ; bind interfaces only = yes

#### Debugging/Accounting ####

# This tells Samba to use a separate log file for each machine
 # that connects
 log file = /var/log/samba/log.%m

# Cap the size of the individual log files (in KiB).
 max log size = 1000

# If you want Samba to only log through syslog then set the following
 # parameter to 'yes'.
 # syslog only = no

# We want Samba to log a minimum amount of information to syslog. Everything
 # should go to /var/log/samba/log.{smbd,nmbd} instead. If you want to log
 # through syslog you should set the following parameter to something higher.
 # syslog = 0

# Do something sensible when Samba crashes: mail the admin a backtrace
 panic action = /usr/share/samba/panic-action %d
```

```
####### Authentication #######

# Server role. Defines in which mode Samba will operate. Possible
 # values are "standalone server", "member server", "classic primary
 # domain controller", "classic backup domain controller", "active
 # directory domain controller".
 #
 # Most people will want "standalone sever" or "member server".
 # Running as "active directory domain controller" will require first
 # running "samba-tool domain provision" to wipe databases and create a
 # new domain.
 server role = standalone server
 security = user
 #valid users = nas, virtuel, @sambashare
 valid users = @sambashare
 encrypt passwords = true

# If you are using encrypted passwords, Samba will need to know what
 # password database type you are using.
 passdb backend = tdbsam

obey pam restrictions = yes

# This boolean parameter controls whether Samba attempts to sync the Unix
 # password with the SMB password when the encrypted SMB password in the
 # passdb is changed.
 unix password sync = yes

# For Unix password sync to work on a Debian GNU/Linux system, the following
 # parameters must be set (thanks to Ian Kahan <<kahan@informatik.tu-muenchen.de>
for
 # sending the correct chat script for the passwd program in Debian Sarge).
 passwd program = /usr/bin/passwd %u
 passwd chat = *Enter\snew\s*\spassword:* %n\n *Retype\snew\s*\spassword:* %n\n
*password\supdated\ssuccessfully* .

# This boolean controls whether PAM will be used for password changes
 # when requested by an SMB client instead of the program listed in
 # 'passwd program'. The default is 'no'.
 pam password change = yes

# This option controls how unsuccessful authentication attempts are mapped
```

```
 # to anonymous connections
 map to guest = bad user

########## Domains ###########

#
 # The following settings only takes effect if 'server role = primary
 # classic domain controller', 'server role = backup domain controller'
 # or 'domain logons' is set
 #

# It specifies the location of the user's
 # profile directory from the client point of view) The following
 # required a [profiles] share to be setup on the samba server (see
 # below)
 ; logon path = \\%N\profiles\%U
 # Another common choice is storing the profile in the user's home directory
 # (this is Samba's default)
 # logon path = \\%N\%U\profile

# The following setting only takes effect if 'domain logons' is set
 # It specifies the location of a user's home directory (from the client
 # point of view)
 ; logon drive = H:
 # logon home = \\%N\%U

# The following setting only takes effect if 'domain logons' is set
 # It specifies the script to run during logon. The script must be stored
 # in the [netlogon] share
 # NOTE: Must be store in 'DOS' file format convention
 ; logon script = logon.cmd

# This allows Unix users to be created on the domain controller via the SAMR
 # RPC pipe. The example command creates a user account with a disabled Unix
 # password; please adapt to your needs
 ; add user script = /usr/sbin/adduser --quiet --disabled-password --gecos "" %u

# This allows machine accounts to be created on the domain controller via the
 # SAMR RPC pipe.
 # The following assumes a "machines" group exists on the system
 ; add machine script = /usr/sbin/useradd -g machines -c "%u machine account" -d
/var/lib/samba -s /bin/false %u
```

```
# This allows Unix groups to be created on the domain controller via the SAMR
 # RPC pipe.
 ; add group script = /usr/sbin/addgroup --force-badname %g

########## Printing ##########

load printers = no
 printing = bsd
 printcap name = /dev/null
 disable spoolss = yes

############ Misc ############

# Using the following line enables you to customise your configuration
 # on a per machine basis. The %m gets replaced with the netbios name
 # of the machine that is connecting
 ; include = /home/samba/etc/smb.conf.%m

# Some defaults for winbind (make sure you're not using the ranges
 # for something else.)
 ; idmap uid = 10000-20000
 ; idmap gid = 10000-20000
 ; template shell = /bin/bash

# Setup usershare options to enable non-root users to share folders
 # with the net usershare command.

# Maximum number of usershare. 0 (default) means that usershare is disabled.
 ; usershare max shares = 100

# Allow users who've been granted usershare privileges to create
 # public shares, not just authenticated ones
 usershare allow guests = yes

#======================= Share Definitions =======================

[Serveur - Dossier home]
 comment = NAS - Répertoire home de host1
 path = /home/nas
 read only = no
 write list = nas
 #read list = utilisateur1, utilisateur2, @groupe12000
```

```
 create mask = 0775
 directory mask = 0770

#Partage des disques de la machine host1
 [Documents des enfants]
 comment = Dossier des documents des enfants sur host1
 path = /media/nas1/Documents/LesEnfants
 read only = yes
 write list = @sambashare
 #read list = utilisateur1, utilisateur2, @groupe12000
 create mask = 0775
 directory mask = 0775

[Documents des parents]
 comment = Dossier des documents des parents sur host1
 path = /media/nas1/Documents/LesParents
 read only = yes
 write list = nas, lafontaj, virtuel
 #read list = utilisateur1, utilisateur2, @groupe12000
 create mask = 0775
 directory mask = 0775

#Partage des disques de la machine host1
 [Downloads sur nas1]
 comment = Dossier de téléchargements sur host1
 path = /media/nas1/Download
 read only = yes
 write list = @sambashare
 #read list = utilisateur1, utilisateur2, @groupe12000
 create mask = 0775
 directory mask = 0775

#Partage des disques de la machine host1
 [nas1]
 comment = Disque en partage sur host1
 path = /media/nas1
 read only = yes
 write list = nas
 read list = @sambashare
 create mask = 0775
 directory mask = 0775
```

```
[nas2]
 comment = Disque en partage sur host1
 path = /media/nas2
 read only = Yes
 write list = @sambashare
 #read list = utilisateur1, utilisateur2, @groupe12000
 create mask = 0775
 directory mask = 0775

[submp3_128]
 comment = Disque en partage sur host1
 path = /media/nas1/Audio/sub_mp3-128
 read only = yes
 write list = nas
 read list = @sambashare
 create mask = 0775
 directory mask = 0775

[Scan]
 comment = Disque en partage sur host1
 path = /media/nas1/Documents/LesParents/Projets/Conjoint/Finance/scan/
 read only = yes
 write list = nas
 read list = @sambashare
 create mask = 0775
 directory mask = 0775
```

Pour faire simple, on n’indique pas les utilisateurs individuellement ds le write list et read list mais plutôt @sambashare (qui inclus tous les utilisateurs que l’on a ajoutés au groupe sambashare)

`sudo service smbd restart`

`sudo service nmbd restart`

Ajout des permissions avec ACL

`sudo setfacl -Rm g:sambashare:rwX /media/nas1`

`sudo setfacl -Rm g:sambashare:rwX /media/nas2`

`sudo setfacl -Rm g:sambashare:rwX /media/nas3`

`sudo setfacl -Rm d:g:sambashare:rwX /media/nas1`

`sudo setfacl -Rm d:g:sambashare:rwX /media/nas2`

`sudo setfacl -Rm d:g:sambashare:rwX /media/nas3`

`sudo setfacl -Rm d:o:rx /media/nas1`

`sudo setfacl -Rm d:o:rx /media/nas2`

`sudo setfacl -Rm d:o:rx /media/nas3`

`sudo getfacl /media/nas1`

`sudo getfacl /media/nas2`

`sudo getfacl /media/nas3`

Redémarrer le serveur

`sudo reboot`

> *exemple:*
> *`setfacl -m u:bernard:rw,u:patrice:rwx,g:sambashare:r,o:--- /media/nas1`*
>
> *Pour annuler tout ou partie d'une ACL : setfacl -b /media/nas1 ôte tout le contenu de l'ACL du fichier ou dossier, tandis que `setfacl -x u:nas,g:sambashare /media/nas1` retire les permissions propres à nas et au groupe sambashare.*
>
> *Les permissions ACL par défaut d'un répertoire (d:) s'annulent par `setfacl -k`.*
>
> *Enlever de façon récursive tout le contenu de l'ACL des fichiers ou dossiers*

> `sudo setfacl -bR /media/nas1`

Maintenant, configuration sur la machine client Linux:

`sudo apt-get install acl`

On crée un dossier en root /media/nas1 et 2. Personne ne peut y accéder à part root.

`sudo mkdir /media/nas1`

`sudo mkdir /media/nas2`

`sudo chmod 770 /media/nas1`

`sudo chmod 770 /media/nas2`

`sudo apt-get install nfs-common cifs-utils`

`su root`

`mousepad /home/lafontaj/.smbcredentials`

```
username=nas
password=votremotpasse
domain=WORKGROUP
```

`chmod 0600 /home/lafontaj/.smbcredentials`

Ajouter une ligne au fichier /etc/fstab. La ligne doit comporter le nom d’hôte du serveur NFS, le répertoire du serveur qui doit être partagé, et le répertoire de la machine locale où le partage NFS doit être monté.

ajouter `,acl` au montage nfs sur votre client NFS et utiliser la version 3 de nfs

`nano /etc/fstab`

```
# <file system> <mount point> <type> <options> <dump> <pass>
UUID=b3863150-aba7-472a-b41e-4cef578f6b06 / ext4 discard,rw,errors=remount-
ro,noatime 0 1
UUID=5fc186d6-e694-40c3-9e7c-ad982b625a78 /home ext4 discard,rw,errors=remount-
ro,noatime 0 2
UUID=f4fd21a7-8c3e-460c-8300-6ae30697eb65 swap swap sw 0 0


#Montage NFS de host1
192.168.0.11:/media/nas1 /media/nas1 nfs
nfsvers=3,bg,rw,hard,intr,proto=tcp,acl,users,exec,noauto 0 0
192.168.0.11:/media/nas2 /media/nas2 nfs
nfsvers=3,bg,rw,hard,intr,proto=tcp,acl,users,exec,noauto 0 0
192.168.0.11:/home/nas /media/host1_home nfs
nfsvers=3,bg,rw,hard,intr,proto=tcp,acl,users,exec,noauto 0 0

#Montage Samba
//192.168.0.130/memorycard /media/scan_epson cifs
user,credentials=/home/lafontaj/.smbcredentials,iocharset=utf8,uid=1000,gid=1000,
sec=ntlm,vers=1.0 0 0
//192.168.0.11/submp3_128 /media/sub_mp3-128 cifs
user,credentials=/home/lafontaj/.smbcredentials,iocharset=utf8,uid=1000,gid=1000,
sec=ntlm,vers=1.0 0 0
```

Ensuite, remonter chaque point de montage:

`sudo mount -o remount,acl /`

`sudo mount -o remount,acl /home`

`sudo mount -o remount,acl /media/nas1`

`sudo mount -o remount,acl /media/nas2`

Il n’est pas nécessaire d’ajouter les utilisateurs du client au groupe sambashare, car nous utilisons l’identité du compte serveur nas (anonuid=1000,anongid=150), défini dans le fichier /etc/exports du serveur.