

# Partage Samba avec ACL

Dossier partagé entre un serveur Linux et un client Windows

La problématique est de mettre en place un partage par Samba.

Permissions Unix

Les permissions Unix sont très performantes pour restreindre les accès, mais rendent la création d'un répertoire partagé 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 pas 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 Samba en activant cette fonctionnalité dans plusieurs fichiers de configuration.

Dossier partagé entre ordinateurs via Samba

Pour utiliser le contrôle de permission par acl:

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

Sur le serveur:

```
sudo apt-get install samba
```

```
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!

```
exit
```

```
sudo apt-get install acl
```

On crée un dossier en root /home/nas/musique. Personne ne peut y accéder à part root. Jusqu'ici rien de spécial.

```
cd ~/
```

Si le répertoire à partager existe déjà, simplement modifier le propriétaire et les permissions au lieu d'en créer un nouveau

```
sudo chown root:root /home/nas/musique
```

```
sudo chmod 770 /home/nas/musique
```

Si la création est nécessaire:

```
sudo mkdir /home/nas/musique
```

```
sudo chmod 770 /home/nas/musique
```

ajouter `,acl` au montage des disques:

```
sudo nano /etc/fstab
```

```
# /etc/fstab: static file system information.
#
UUID=5614d371-1e4c-4732-8561-9a38ace22e7d / ext4 rw,errors=remount-ro,acl 0 1
UUID=762d2137-7b48-44ce-ae51-ece86bfff677 swap swap sw 0 0
UUID=0e1d7dee-f9b6-4836-baca-3a8221446ec3 /home ext4 rw,errors=remount-ro,acl 0 2
```

Une fois fait, remontez le point de montage.

```
sudo mount -o remount,acl /home
```

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

Assignment des droits ACL:

Pour la mise en place de cette solution, 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.

Sur Ubuntu le groupe `sambashare` par défaut au GID 111

```
sudo cat /etc/group
```

La commande retourne ce qui suit:

```
sambashare:x:111:nas
```

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

```
sudo addgroup --gid 111 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.

Énumérer les utilisateurs déjà présents sur le système

```
cat /etc/passwd
```

va retourner quelque chose du genre:

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

Ajouter l'utilisateur générique qui sera utilisé sous Windows

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

Énumérer les utilisateurs présents sur le système suite aux ajouts

```
cat /etc/passwd
```

va retourner quelque chose du genre:

```
virtuel:x:1001:111::/dev/null:/bin/false
```

ou

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

Noter le nom d'utilisateur: squeezeboxserver

Afin de mettre en place le contrôle d'accès aux fichiers, il faut ajouter

chacun des utilisateurs au groupe sambashare incluant LMS, car on veut que LMS puisse lire ou écrire des listes de lectures, etc.:

```
sudo usermod -a -G sambashare nas
```

```
sudo usermod -a -G sambashare squeezeboxserver
```

```
sudo usermod -a -G sambashare virtuel
```

Pour vérifier les associations via la console:

```
cat /etc/group
```

```
sambashare:x:111:nas,virtuel,squeezeboxserver
```

*note:*

*Les commandes suivantes peuvent s'avérer utiles durant la configuration*

```
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).

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

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

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

```
smbpasswd -a nas
```

```
smbpasswd -a virtuel
```

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

Il n'est pas nécessaire de créer un mot de passe pour squeezeboxserver puisqu'il n'utilise pas Samba pour ces accès aux données.

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

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

```
#  
# Sample configuration file for the Samba suite for Debian GNU/Linux.  
#  
#  
# This is the main Samba configuration file. You should read the  
# smb.conf(5) manual page in order to understand the options listed  
# here. Samba has a huge number of configurable options most of which  
# are not shown in this example  
#  
# Some options that are often worth tuning have been included as  
# commented-out examples in this file.  
# - When such options are commented with ";", the proposed setting  
# differs from the default Samba behaviour  
# - When commented with "#", the proposed setting is the default  
# behaviour of Samba but the option is considered important  
# enough to be mentioned here  
#  
# NOTE: Whenever you modify this file you should run the command
```



```
# "testparm" to check that you have not made any basic syntactic
# errors.

#===== 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
```

```
[nas3]
comment = Disque en partage sur host1
path = /media/nas3
read only = Yes
```

```
write list = @smbashare
#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 = @smbashare
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 = @smbashare
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 @smbashare (qui inclus tous les utilisateurs que l'on a ajoutés au groupe smbashare)

```
sudo service smb restart
```

```
sudo service nmb restart
```

Ici je ferais un reboot pour être certain que les acl sont activés sur tous les disques

Redémarrer le serveur

```
sudo reboot
```

Ajout des permissions avec ACL

```
sudo setfacl -Rm g:sambashare:rwX /home/nas/musique
```

```
sudo setfacl -Rm d:g:sambashare:rwX /home/nas/musique
```

```
sudo setfacl -Rm d:o:rx /home/nas/musique
```

```
sudo getfacl /home/nas/musique
```

```
# file: home/nas/musique
# owner: root
# group: root
user::rwx
group::rwx
group:sambashare:rwx
mask::rwx
other::r-x
default:user::rwx
default:group::rwx
default:group:sambashare:rwx
default:mask::rwx
default:other::r-x
```

Et voilà le reste est à titre de référence.

### *exemple:*

```
setfacl -m u:bernard:rw,u:patrice:rwx,g:sambashare:r,o:--- /home/nas/musique
```

*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 /home/nas/musique` 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 /home/nas/musique
```