Configuración dos permisos con ACLs

Nesta sección veremos como superar as limitacións do tradicional sistema de permisos de UNIX. Veranse as Listas de Control de Acceso (ACLs), que permiten indicar que conxunto de grupos e/ou usuarios poden acceder a un arquivo e/ou carpeta, sen estar limitados a Usuario Propietario, Grupo Propietario e Outros.

As ACLs aplicadas sobre un sistema arquivos exportado por NFS ou CIFS tamén son efectivas nos clientes.

Sumario

- 1 Introdución ás ACLs
  - 1.1 ACLs
- 2 Comandos para a xestión das ACLs
  - 2.1 getfacl
  - 2.2 setfacl
- 3 Facer que os usuarios de Samba4 sexan recoñecidos no servidor
- 4 Exemplos de manexo das ACLs
- 5 Axustar permisos do noso esqueleto
- 6 Permisos para as carpetas persoais dos usuarios

Introdución ás ACLs

Como xa vimos, o sistema tradicional de permisos de GNU/Linux só permite afinar os permisos dunha carpeta ou arquivo para o usuario e o grupo propietario dos mesmos. Para os demais queda un grupo chamado *outros* que non permite facer ningún axuste fino.

ACLs

As Listas de Control de Acceso (ACLs) permiten un acceso máis granular ao sistema de arquivos de GNU/Linux, permitindo indicar que varios usuarios e varios grupos teñan acceso en modo lectura a unha carpeta, por exemplo. Tamén se pode indicar cales deses usuarios ou grupos se deben herdar para os obxectos secundarios (ficheiros e subcarpetas) que se creen dentro desa carpeta.

As acls por agora non veñen de *serie* coa instalación de GNU/Linux. Hai que instalar o paquete (como fixemos no apartado anterior) e configurar o sistema de arquivos sobre o que se desexan aplicar no momento de montalo (co parámetro *acl*, como tamén fixemos no apartado anterior).

Tomemos por exemplo unha carpeta chamada **dam1** que alberga as carpetas persoais de todo o alumnado dese grupo. Interesa que a esa carpeta só entre o root (control total) e os alumnos de *dam1*, para logo que cada quen acceda á súa carpeta particular. Finalmente os profesores dese curso poden entrar na carpeta *dam1*, e en todas as subcarpetas e ficheiros (actuais e futuros) en modo lectura.

Para iso esa carpeta *dam1*, terá a seguinte acl:

```
# file: dam1                    -- carpeta/ficheiro sobre o que hai unha acl.
# owner: root                   -- usuario propietario: root
# group: root                   -- grupo propietario: root
user::rwx                       -- Permisos do usuario propietario: rwx
group::---                      -- Permisos do grupo propietario: ningún
group:g-dam1-alum:r-x           -- Grupos que hai na acl: g-dam1-alum:rx . Este grupo non se herdará a
                                -- obxectos secundarios, porque non aparece en default.
group:g-dam1-profes:r-x         -- Grupos que hai na acl: g-dam1-profes:r . Este grupo herdarase a obxectos
                                -- secundarios, porque SI aparece en default.

mask::rwx                       -- limita os permisos efectivos que se conceden aos usuarios e grupos enumerados.
                                -- Os permisos do dono e de "others" non se ven afectados por mask
other::---                      -- Permisos da clase outros: ningún
                                -- Nas seguintes substitúase default por herdar e entenderase mellor.
                                   E pénsese nun obxecto secundario (subcarpeta ou ficheiro)
                                   que se cre dentro da da carpeta dam1.

default:user::rwx               -- Permisos que herdará o usuario propietario: rwx
default:group::---              -- Permisos que herdará o grupo propietario: ningún
default:group:g-dam1-profes:r-x -- Entrada que herdarán obxectos secundarios futuros: g-dam1-profes: rx.
                                -- PERO OLLO: aquí só aparecen as entradas herdables, pero polo feito de estar
                                   como herdable só afecta ós obxectos secundarios que se creen nun futuro, non
                                   son permisos que ten a carpeta principal. Para asignar os mesmos permisos á
```

```
                                    carpeta principal débese indicar explicitamente como na entrada superior:
                                    group:g-dam1-profes:r--


default:mask::r--
default:other::---              -- Permisos que herdará a clase outros: ningún
```

Observar:

- Que o grupo *g-dam1-profes* aparece dúas veces, unha para os permisos da propia carpeta **dam1** e outra para que os permisos sexan propagados ás subcarpetas e arquivos futuros que se creen dentro de **dam1**.
- Pola contra, o grupo *g-dam1-alum* só ten permisos de lectura en *dam1* e non aparece a maiores nas entradas **default**, por tanto, esa entrada non será propagada aos obxectos secundarios que se creen dentro de **dam1**.

Comandos para a xestión das ACLs

Imos ver os dous comandos fundamentais para manipular as ACLs.

getfacl

- **Descrición**: amosa a lista de control de acceso dunha carpeta ou ficheiro. Este comando ven co paquete acl.

- **Sintaxe**:

```
Emprego: getfacl [OPCIÓNS]... FICHEIRO/CARPETA

 Opcións máis comúns
  -R, --recursive: opera sobre ficheiros e directorios recursivamente.
  -d,  amosa só as entradas herdables da lista de control de acceso.

Exemplos:
  getfacl -R /u         Amosa os permisos básicos e estendidos do directorio /u e do seu contido recursivamente.
```

setfacl

- **Descrición**: introduce, elimina ou modifica entradas da lista de control de acceso.

- **Sintaxe**:

```
Emprego: setfacl [OPCIÓNS] usuario/grupo:permisos FICHEIRO/CARPETA

 Opcións máis comúns
  -b ?- borra tódalas entradas das acl.
  -k ?- borra tódalas entradas herdables da acl.
  -d  -- modificador que afecta ás entradas herdables.
  -R, --recursive: opera sobre ficheiros e directorios recursivamente.

  -m, --modifica a acl.
  -x,  -- elimina unha entrada da acl.

  Usuario: u:usuario
  grupo: g:grupo
  outros: o:

  permisos: r | w | x

Exemplos:
  setfacl -Rm g:users:rx /u    Introduce na acl de /u de tódolos
                               seus subdirectorios e ficheiros permisos
                               de lectura e escritura para o grupo users.
                               Que o faga recursivo só afecta ás carpetas/ficheiros actuais e non ás futuras.

  setfacl -Rdm g:users:rx /u   Igual que caso anterior, pero agora cando
                               se cree unha carpeta/ficheiro dentro de /u
                               tamén vai herdar a entrada da acl onde se
                               indica que os membros do grupo users podes ler e executar.
```

```
setfacl -dx g:users /u       Borra a entrada anterior da acl.
```

Facer que os usuarios de Samba4 sexan recoñecidos no servidor

- Para poder establecer os permisos para os usuarios e grupos do dominio Samba4 temos que solucionar un lixeiro inconveniente: que eses usuarios e grupos existan no servidor. Se non é así, teríamos que establecer os permisos usando os ids dos usuarios e os grupos, e a xestión dos permisos sería moi incómoda e complexa.

- Podemos comprobar no servidor executando o comando **getent passwd**, que non aparece ningún usuario do dominio (*sol*, *noe*, etc.).

- Para conseguilo, imos utilizar o servizo nslcd, que permite tomar os usuarios do sistema Linux dun servizo LDAP.

- Antes de comezar coa instalación e configuración do servizo *nslcd*, imos facer engadir un parámetro ao final da sección *[global]* ficheiro de configuración de Samba (*/etc/samba/smb.conf*), para permitir que o servizo do LDAP de samba permita conexións de autenticación sen cifrar (téñase en conta que neste caso imos facer o autenticación dende o propio equipo, polo que a información non vai circular pola rede). Engadimos a liña que se mostra a continuación:

```
[global]
        ....
        ....
        ldap server require strong auth = no
```

- E detemos e iniciamos de novo o servizo de Samba para recargar a súa configuración:

```
root@dserver00:~# systemctl stop samba-ad-dc
root@dserver00:~# systemctl start samba-ad-dc
```

- Agora si, instalamos o paquete *nslcd*:

```
apt-get install nslcd
```

- Na instalación do paquete pedirásenos unha serie de información para obter os usuarios do LDAP de Samba4. Introduciremos os seguintes datos (moitos xa virán cos valores por defecto axeitados):
    - Enderezo do servidor ldap: **ldap://dserver00.iescalquera.local**
    - Base de buscas LDAP: **dc=iescalquera,dc=local**
    - Servizos nos que activar o servizo LDAP no ficheiro /**etc**/**nsswitch.conf**: Marcar **group**, **passwd** e **shadow**.

- Pero imos facer un cambio na configuración que o paquete *nslcd* fai no ficheiro */etc/nsswitch.conf*. Editamos este ficheiro e cambiamos para as entradas **passwd**, **group** e **shadow** a opción *compat* por *files*, para que o sistema recoñeza correctamente os usuarios e grupos do LDAP:

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

#passwd:         compat ldap
#group:          compat ldap
#shadow:         compat ldap
passwd:         files ldap
group:          files ldap
shadow:         files ldap
gshadow:        files

hosts:          files dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

Modificación no ficheiro */etc/nsswitch.conf*

- Editamos o ficheiro de configuración do paquete nslcd, /**etc/nslcd.conf**, e engadimos ao final o seguinte contido:

```
# Some settings for AD
pagesize 1000
referrals off

# Filters (only required if your accounts doesn't have objectClass=posixAccount
# and your groups haven't objectClass=posixGroup. This objectClasses won't be added
# by ADUC. So they won't be there automatically!)
filter  passwd  (objectClass=user)
filter  group   (objectClass=group)

# Attribut mappings (depending on your nslcd version, some might not be
# necessary or can cause errors and can/must be removed)
map     passwd  uid             sAMAccountName
map     passwd  homeDirectory   unixHomeDirectory
map     passwd  gecos           displayName
map     passwd  gidNumber       primaryGroupID

# LDAP bind (Account in AD that is used from nslcd to bind to the directory)
binddn cn=Administrator,cn=Users,dc=iescalquera,dc=local
bindpw abc123.
```

- Reiniciamos o servizo *nslcd*:

```
service nslcd restart
```

- E comprobamos que xa aparecen os usuarios e grupos do dominio cos comando **getent passwd** e **getent group** respectivamente. **Fixarse en que só aparecerán aqueles usuarios e grupos que teñan asignado algún valor nos seus identificadores POSIX.** Tendo en conta que imos poñer os permisos sobre os grupos de usuarios, non pasa nada porque os usuarios non teñan establecido o *uidNumber*; o que si é importante é que os grupos teñan identificador asignado, polo que será necesario ter asignado un *gidNumber* a cada grupo sobre o que imos configurar permisos.

- A continuación móstrase o que debería devolver o comando **getent group** nas súas últimas liñas:

```
root@dserver00:~# getent group
...
...
g-dam1-profes:*:10002:sol
```

```
g-dam2-profes:*:10003:noe,sol
Domain Admins:*:10010:Administrator
g-dam1-alum:*:10005:tom,mon
g-dam2-alum:*:10006:paz,pia
g-usuarios:*:10000:
g-profes:*:10001:noe,sol
g-alum:*:10004:paz,tom,mon,pia
```

- Observar que tamén se lle asignou un identificador de grupo ao grupo **Domain Admins** (o 10010). Isto é necesario porque imos utilizalo para permitir que calquera usuario deste grupo poida crear as carpetas persoais dos usuarios. Se este grupo non aparece, obteremos un erro cando intentemos introducilo nos permisos dalgunha carpeta.

Exemplos de manexo das ACLs

Para comezar a familiarizarnos coas ACLs, imos estudar con distintos exemplos a inserción, modificación e borrado de acls así como a propagación de permisos.

- No servidor, movémonos á carpeta /**srv**/**samba** e comprobamos os permisos do seu contido (isto que estamos facendo agora simplemente é unha proba, así que non pasa nada porque os permisos por defecto que haxa nas carpetas non coincidan cos que aquí aparecen):

```
root@dserver00:~# cd /srv/samba/
root@dserver00:/srv/samba# ls -l
total 8
drwxrwx--- 6 root root 4096 Mai 17 18:20 comun
drwxrwx--- 5 root root 4096 Mai 17 16:51 usuarios
```

- Obtemos a acl de *comun*. Observar a información anterior disposta doutra forma.

```
root@dserver00:/srv/samba# getfacl comun
# file: comun
# owner: root
# group: root
user::rwx
group::rwx
other::---
```

- Permitir ao grupo **g-profes** que poida ler e acceder (r-x) á carpeta *comun*, só a esa carpeta. (-m)

```
root@dserver00:/srv/samba# setfacl -m g:g-profes:rx comun
root@dserver00:/srv/samba#
root@dserver00:/srv/samba# getfacl comun
# file: comun
# owner: root
# group: root
user::rwx
group::rwx
group:g-profes:r-x
mask::rwx
other::---
```

Observar como aparece o grupo **g-profes** con permisos r-x.

- Listamos carpetas con acls: Observar o carácter **+**, que indica que esa carpeta ten unha acl.

```
root@dserver00:/srv/samba# ls -lh
total 8,0K
drwxrwx---+ 6 root root 4,0K Mai 17 18:20 comun
drwxrwx---  5 root root 4,0K Mai 17 16:51 usuarios
```

- Creamos unha subcarpeta en *comun*: **comun**/**exames**, e obtemos as acls de esa carpeta.

```
root@dserver00:/srv/samba# mkdir comun/exames
root@dserver00:/srv/samba#
root@dserver00:/srv/samba# getfacl comun/exames/
# file: comun/exames/
# owner: root
# group: root
user::rwx
```

```
group::r-x
other::r-x
```

Observar como ao crear a carpeta **exames** non se herdou **g-profes** de **comun**.

- Engadimos unha acl para **g-alum** con permisos (r-x), que se propaguen polas subcarpetas e arquivos existentes en *comun*. (-R)

```
root@dserver00:/srv/samba# setfacl -Rm g:g-alum:rx comun
root@dserver00:/srv/samba#
root@dserver00:/srv/samba# getfacl comun
# file: comun
# owner: root
# group: root
user::rwx
group::rwx
group:g-profes:r-x
group:g-alum:r-x
mask::rwx
other::---

root@dserver00:/srv/samba# getfacl comun/exames/
# file: comun/exames/
# owner: root
# group: root
user::rwx
group::r-x
group:g-alum:r-x
mask::r-x
other::r-x
```

O grupo **g-alum:r-x** está na acl de comun e na da subcarpeta **exames**.

- Imos agora a engadir unha entrada á acl, grupo **g-profes:rwx**, que sexa herdable, de xeito que cando no futuro se cre un ficheiro ou subcarpeta-ficheiro en *comun* herde esa entrada automaticamente (-d).

```
root@dserver00:/srv/samba# setfacl -dm g:g-profes:rwx comun
root@dserver00:/srv/samba# mkdir comun/practicas
root@dserver00:/srv/samba# getfacl comun/
# file: comun/
# owner: root
# group: root
user::rwx
group::rwx
group:g-profes:r-x
group:g-alum:r-x
mask::rwx
other::---
default:user::rwx
default:group::rwx
default:group:g-profes:rwx
default:mask::rwx
default:other::---

root@dserver00:/srv/samba# getfacl comun/exames/
# file: comun/exames/
# owner: root
# group: root
user::rwx
group::r-x
group:g-alum:r-x
mask::r-x
other::r-x

root@dserver00:/srv/samba# getfacl comun/practicas/
# file: comun/practicas/
# owner: root
# group: root
user::rwx
group::rwx
group:g-profes:rwx
mask::rwx
```

```
other::---
default:user::rwx
default:group::rwx
default:group:g-profes:rwx
default:mask::rwx
default:other::---
```

- Observar:
  - **o grupo g-profes**: non ten permisos de escritura sobre **comun** pois só está como herdable para futuros obxectos secundarios (neste caso *practicas*). Co cal un usuario do grupo **g-profes** pode escribir en *comun/practicas*, pero non en **comun**.
  - **o grupo g-profes**: non está en **comun**/**exames**, pero si na carpeta **practicas** que se creou despois de introducir a acl en *comun*. **default** indica que esa entrada é herdable. **g-profes** non aparece en *exames*, porque esa subcarpeta xa estaba creada antes de meter a entrada na acl.

- Para que un usuario de **g-profes** poida escribir na carpeta **comun** é preciso modificar a súa ACL:

```
root@dserver00:/srv/samba# setfacl -m g:g-profes:rwx comun
root@dserver00:/srv/samba# getfacl comun/
# file: comun/
# owner: root
# group: root
user::rwx
group::rwx
group:g-profes:rwx
group:g-alum:r-x
mask::rwx
other::---
default:user::rwx
default:group::rwx
default:group:g-profes:rwx
default:mask::rwx
default:other::---
```

Agora si, un usuario de **g-profes** pode escribir en *comun* e nas subcarpetas nas que teña permisos.

- Como borrar unha acl?: eliminarase o grupo **g-alum** da acl. Primeiro de *comun* e logo recursivamente de todas as subcarpetas. (-x)

```
root@dserver00:/srv/samba# setfacl -x g:g-alum comun
root@dserver00:/srv/samba#
root@dserver00:/srv/samba# getfacl comun
# file: comun
# owner: root
# group: root
user::rwx
group::rwx
group:g-profes:rwx
mask::rwx
other::---
default:user::rwx
default:group::rwx
default:group:g-profes:rwx
default:mask::rwx
default:other::---

root@dserver00:/srv/samba# getfacl comun/exames
# file: comun/exames
# owner: root
# group: root
user::rwx
group::r-x
group:g-alum:r-x
mask::r-x
other::r-x

root@dserver00:/srv/samba# getfacl comun/practicas/
# file: comun/practicas/
# owner: root
# group: root
user::rwx
group::rwx
```

```
group:g-profes:rwx
mask::rwx
other::---
default:user::rwx
default:group::rwx
default:group:g-profes:rwx
default:mask::rwx
default:other::---
```

Observar que **g-alum** está eliminado da acl de *comun* pero non da subcarpeta *exames*.

- Para eliminalo de *comun* e de todas as súas subcarpetas e arquivos hai que facelo recursivamente: (-Rx)

```
root@dserver00:/srv/samba# setfacl -Rx g:g-alum comun
root@dserver00:/srv/samba#
root@dserver00:/srv/samba# getfacl comun
# file: comun
# owner: root
# group: root
user::rwx
group::rwx
group:g-profes:rwx
mask::rwx
other::---
default:user::rwx
default:group::rwx
default:group:g-profes:rwx
default:mask::rwx
default:other::---

root@dserver00:/srv/samba# getfacl comun/exames
# file: comun/exames
# owner: root
# group: root
user::rwx
group::r-x
mask::r-x
other::r-x

root@dserver00:/srv/samba# getfacl comun/practicas/
# file: comun/practicas/
# owner: root
# group: root
user::rwx
group::rwx
group:g-profes:rwx
mask::rwx
other::---
default:user::rwx
default:group::rwx
default:group:g-profes:rwx
default:mask::rwx
default:other::---
```

- Por último, e como estas ACLs que configuramos son simplemente de proba e non son as que nos interesan para o noso esqueleto de carpetas, imos borrar todas as ACLs de *comun* e das súas subcarpetas:

```
root@dserver00:/srv/samba# setfacl -bR comun
root@dserver00:/srv/samba#
root@dserver00:/srv/samba# getfacl comun
# file: comun
# owner: root
# group: root
user::rwx
group::rwx
other::---

root@dserver00:/srv/samba# getfacl comun/exames
# file: comun/exames
# owner: root
# group: root
user::rwx
```

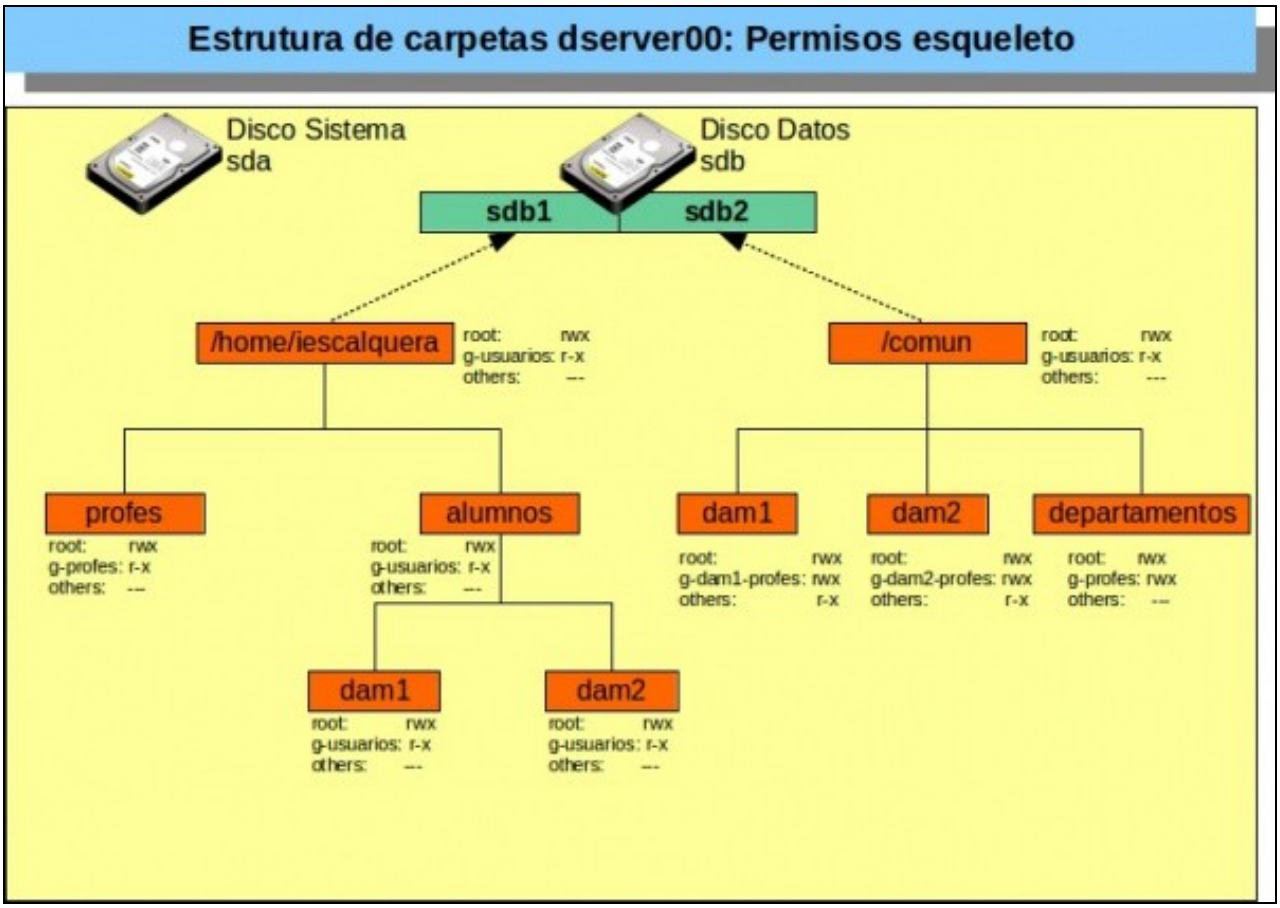
```
group::r-x
other::r-x

root@dserver00:/srv/samba# getfacl comun/practicas/
# file: comun/practicas/
# owner: root
# group: root
user::rwx
group::rwx
other::---
```

- Á vista dos exemplos anteriores:
    - Para traballar con usuarios no canto de grupos, usar: **u:usuario**
    - Non confundir recursividade (-R) con herdanza (-d). O primeiro afecta a carpeta e subcarpetas/arquivos existentes, o segundo non afecta á carpeta senón ás subcarpetas e arquivos que se creen nun futuro.
    - Para modificar os permisos do usuario propietario, pódese usar chmod ou: **setfacl -opcións u::permisos comun**. Para o grupo propietario sería semellante pero g:: no canto de u::.

Axustar permisos do noso esqueleto

O seguinte esquema representa a estrutura de permisos establecido no esqueleto de carpetas que deseñamos para o noso dominio na Parte III:



Esquema de carpetas do dominio con permisos POSIX

Isto podería ser suficiente en moitos casos, pero imos presentar algunhas situacións nas que o esquema de permisos de Linux non nos permite acadar unha solución e si poderíamos resolver co uso de ACLs:

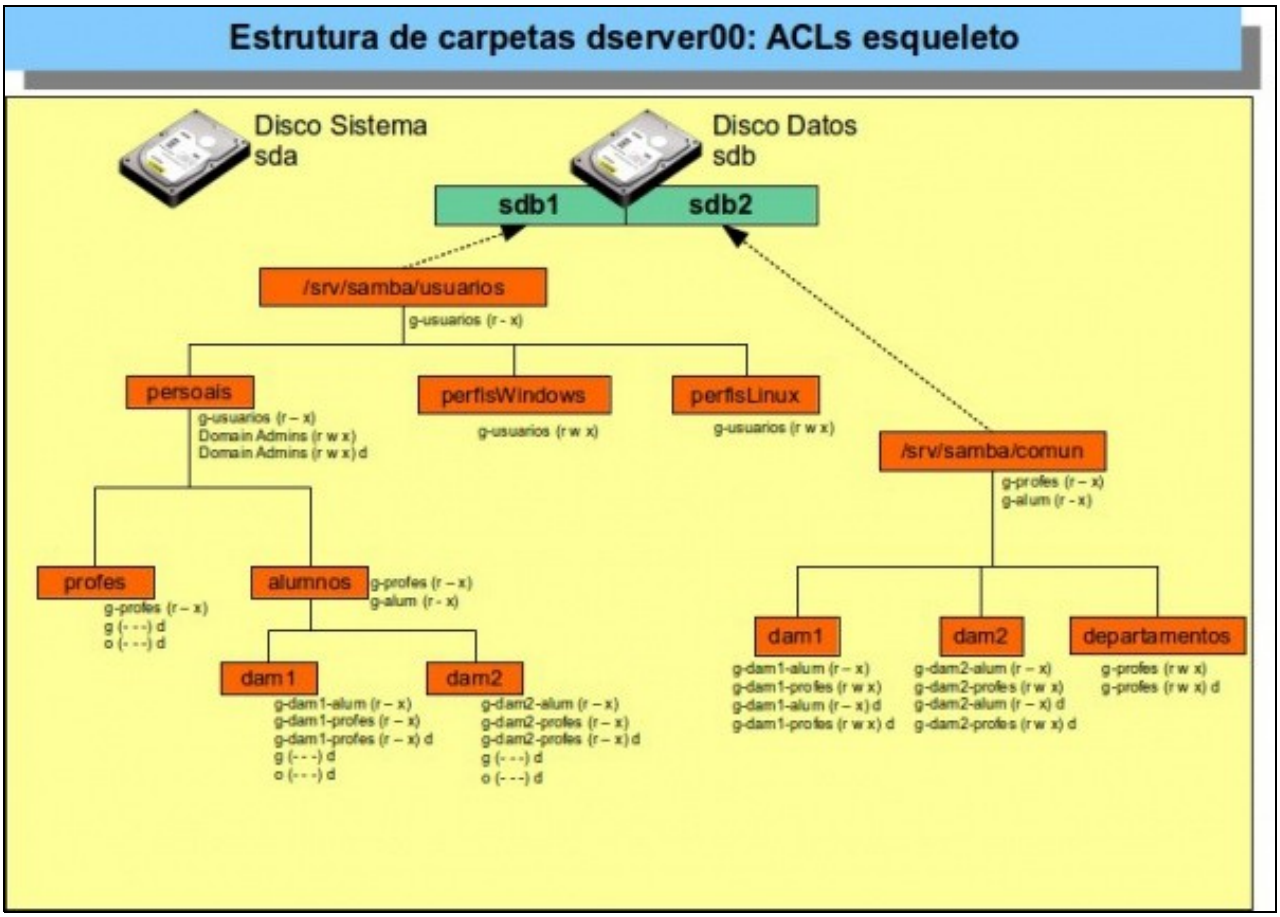
- Coa estrutura actual de permisos, calquera usuario do grupo *g-usuarios* podería entrar dentro da carpeta de /home/iescalquera/alumnos e ver o seu contido. Se houbese usuarios dentro deste grupo que non fosen profes nin alumnos isto non nos interesaría, e para evitalo teríamos que permitir a entrada á carpeta ao grupo *g-profes* e ao grupo *g-alum*, e denegar o acceso ao resto de usuarios.

- Un alumno de *dam1* pode ver o contido da carpeta */home/iescalquera/alumnos/dam2* (aínda que non poida ver o contido das súas subcarpetas), cousa que non nos interesaría. O ideal é que nesa carpeta só poidan acceder os usuarios dos grupos *g-dam2-profes* e *g-dam2-alum*.

- Máis importante é o que ocorre na carpeta de */comun/dam2*, xa que un alumno de *dam1* podería acceder ao contido desta carpeta. Sería desexable que só puidesen entrar para ler e escribir os usuarios de *g-dam2-profes* e os de *g-dam2-alum* só para ler, mentres que o resto dos usuarios non debería poder acceder a esta carpeta.

- Por último, utilizando permisos herdables poderíamos configurar os permisos por defecto adecuados para as carpetas persoais dos usuarios sen necesidade dun script que os modifique expresamente.

O seguinte esquema de ACLs solventaría estes aspectos:



Esquema de carpetas do dominio con ACLs
Ademais das ACLs para resolver as cuestións indicadas, inclúense dúas entradas a maiores nas ACLs para axustar os permisos das carpetas persoais dos usuarios no caso de que se creen de forma automática con RSAT:

- Na carpeta **Persoais**, incluímos unha entrada herdable nas ACL que permite que os usuarios do grupo *Domain Admins* (os administradores do dominio) poidan ler e escribir nesa carpeta e en todas as súas subcarpetas.
- Nas carpetas onde se crearán as carpetas persoais dos usuarios (*profes*, *alumnos/curso*), engadimos dúas entradas herdables na ACL para evitar que calquera outro usuario que non sexa o propio usuario ou dun grupo de profes dese curso que debe ter permiso de lectura poida entrar na carpeta persoal dun usuario.

Para establecer as ACLs do esquema, podemos crear un script co seguinte contido.

SCRIPT: 02_axustar_acls_esqueleto.sh

```
#!/bin/bash

#Chamar ao script de variables
. ./00_variables.sh # Tamén podería ser: source ./00_variables.sh

#Establecemos de forma recursiva os permisos de Linux
chown -R root:root $DIR_USUARIOS
chmod -R 770 $DIR_USUARIOS
chown -R root:root $DIR_COMUN
chmod -R 770 $DIR_COMUN

#Cartafol de usuarios e subcartafoles
setfacl -m g:g-usuarios:rx $DIR_USUARIOS
setfacl -m g:"Domain Admins":rwx $DIR_USUARIOS
setfacl -m g:g-usuarios:rx $DIR_USUARIOS/persoais
setfacl -m g:"Domain Admins":rwx $DIR_USUARIOS/persoais
setfacl -dm g:"Domain Admins":rwx $DIR_USUARIOS/persoais
setfacl -m g:g-usuarios:rwx $DIR_USUARIOS/perfisWindows
setfacl -m g:g-usuarios:rwx $DIR_USUARIOS/perfisLinux

#Cartafol profes
setfacl -m g:"Domain Admins":rwx $DIR_USUARIOS/persoais/profes
setfacl -m g:g-profes:rx $DIR_USUARIOS/persoais/profes
setfacl -dm o:--- $DIR_USUARIOS/persoais/profes
setfacl -dm g::--- $DIR_USUARIOS/persoais/profes

#Cartafol alumnos
setfacl -m g:"Domain Admins":rwx $DIR_USUARIOS/persoais/alumnos
setfacl -m g:g-profes:rx $DIR_USUARIOS/persoais/alumnos
setfacl -m g:g-alum:rx $DIR_USUARIOS/persoais/alumnos

#Cartafoles cursos
for CURSO in $(cat f00_cursos.txt)
do
        setfacl -m g:g-$CURSO-alum:rx $DIR_USUARIOS/persoais/alumnos/$CURSO
        setfacl -m g:g-$CURSO-profes:rx $DIR_USUARIOS/persoais/alumnos/$CURSO
        setfacl -dm g:g-$CURSO-profes:rx $DIR_USUARIOS/persoais/alumnos/$CURSO
        setfacl -dm o:--- $DIR_USUARIOS/persoais/alumnos/$CURSO
        setfacl -dm g::--- $DIR_USUARIOS/persoais/alumnos/$CURSO
done

#Cartafol comun
setfacl -m g:g-profes:rx $DIR_COMUN
setfacl -m g:g-alum:rx $DIR_COMUN

#Subcartafol departamentos
setfacl -m g:g-profes:rwx $DIR_COMUN/departamentos
setfacl -dm g:g-profes:rwx $DIR_COMUN/departamentos

#Subcartafoles cursos
# O participante no curso á vista do esquema de permisos
# do exemplo de arriba debe ser quen de axustar
# os permisos de comun/cursos
```

- Executamos o script:

```
sh 02_axustar_acls_esqueleto.sh
```

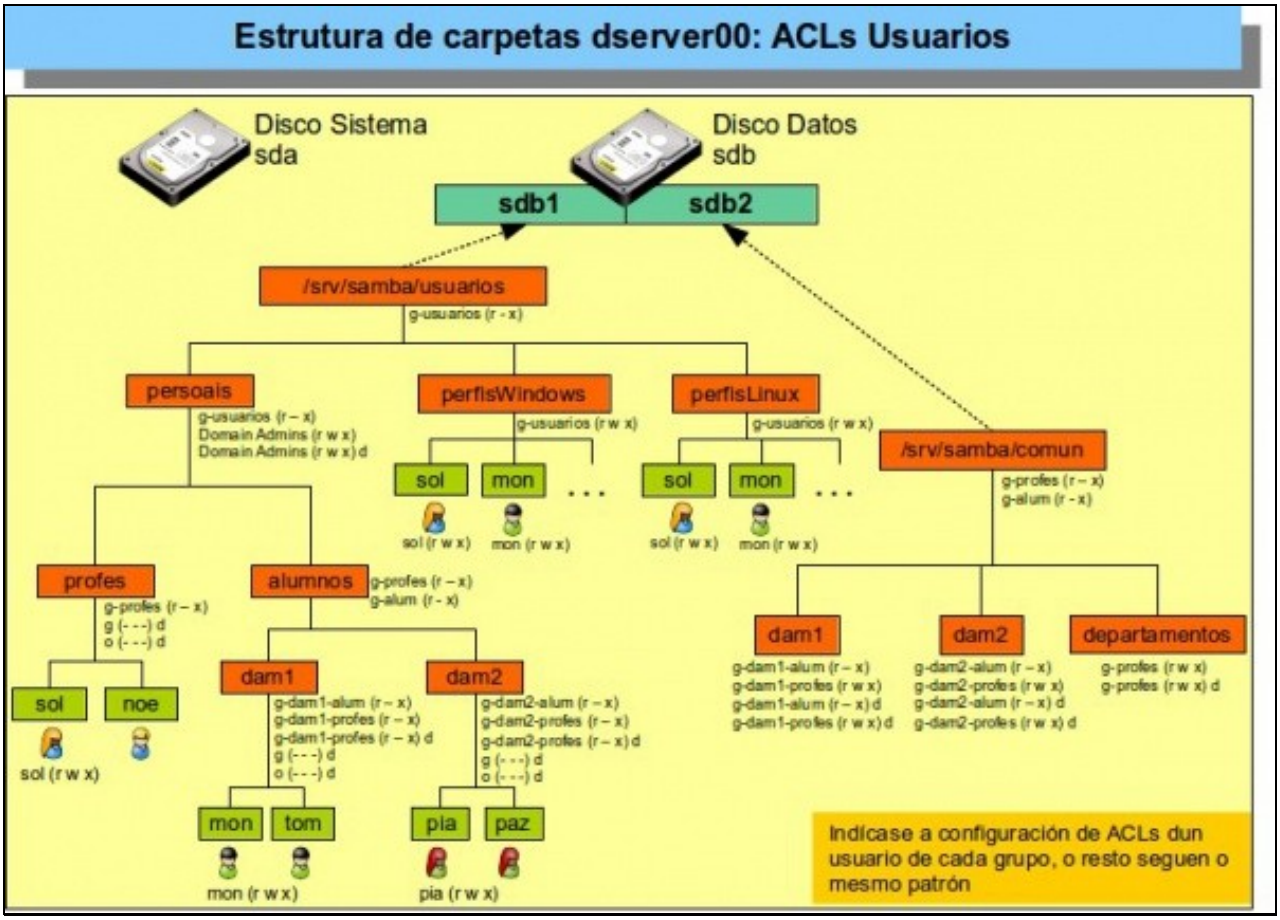
- Unha vez executado o script, recoméndase comprobar con **getfacl** que cada carpeta ten a ACL que lle corresponde.

Permisos para as carpetas persoais dos usuarios

- Con respecto ás carpetas persoais dos usuarios, agora o único necesario é que cada usuario teña permisos de lectura e escritura sobre a súa carpeta (e isto pódese facer cos permisos de Linux ou con ACLs).

- As carpetas de perfís vanse crear automaticamente cando o usuario inicie sesión, tanto nun cliente Windows como nun cliente Linux, e dado que se van a crear coas súas propias credenciais, os permisos que se establecerán xa serán os axeitados.

- O esquema completo incluíndo as carpetas persoais e de perfís sería o seguinte:



Esquema de carpetas persoais con ACLs

-- Antonio de Andrés Lema e Carlos Carrión Álvarez