1 Administración de usuarios do dominio con Samba

1.1 Sumario

1.2 Introdución

- Neste apartado imos usar as utilidades anteriores para administrar os usuarios do dominio samba, tendo en conta que o servidor samba está tomando os usuarios do servidor LDAP.

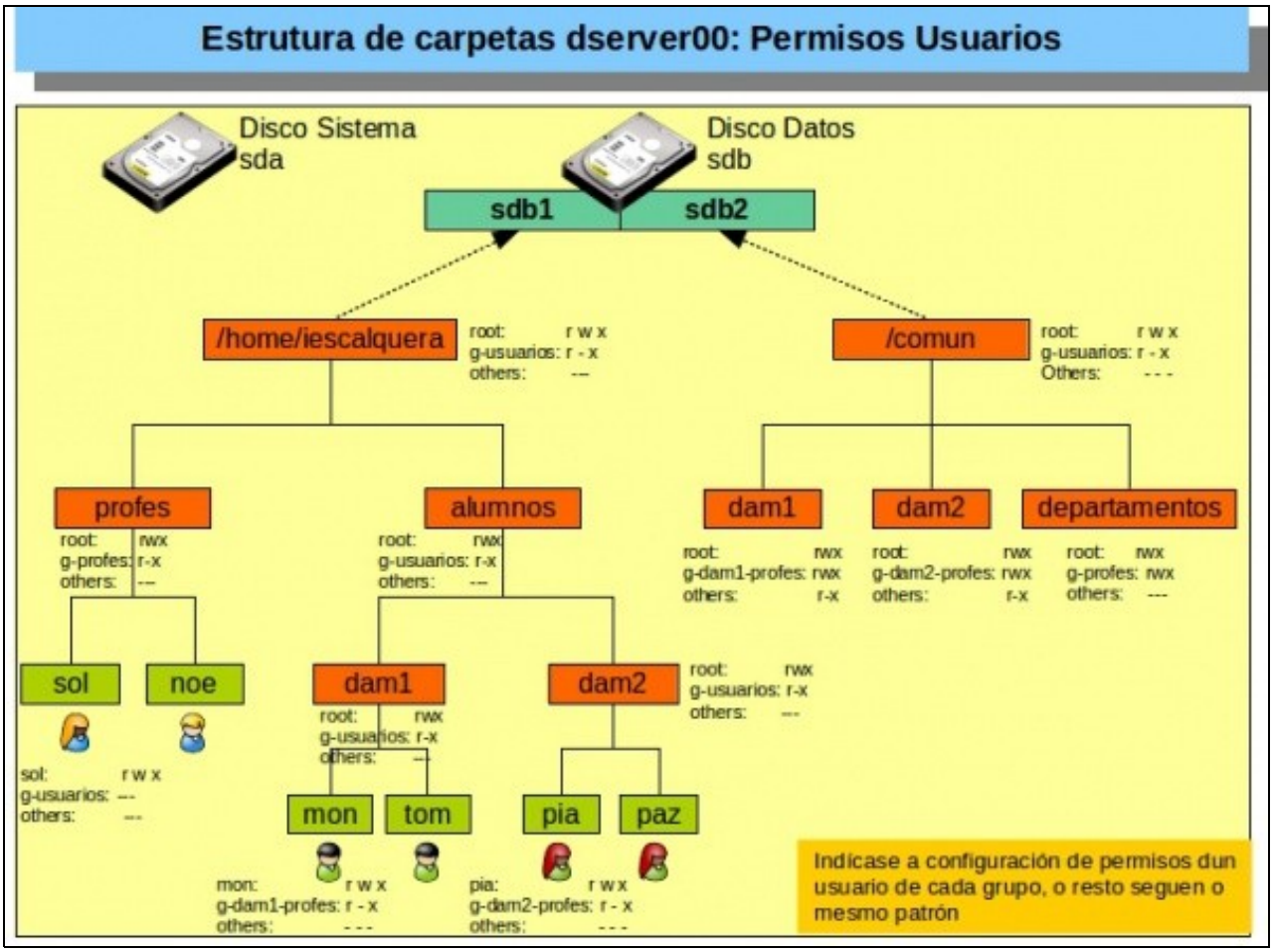
- Engadiremos aos grupos e aos usuarios xa existentes os atributos propios do esquema samba.

- Engadiremos a usuaria *paz* que falta por incluír no sistema co seu directorio home

USUARIOS E GRUPOS

Grupos Usuarios	Nome Completo	g-usarios (10000)	g-profes (10001)	g-dam1-profes (10002)	g-dam2-profes (10003)	g-alum (10004)	g-dam1-alum (10005)	g-dam2-alum (10006)
Descric.		Tódolos usuarios de LDAP	Todo o profesorado	Profesorado de 1º da DAM	Profesorado de 2º DAM	Todo o alumnado	Alumnado de 1º da DAM	Alumnado de 2º da DAM
sol (10000)	Profe - Sol Lúa	✔(1º)	✔	✔	✔			
noe (10001)	Profe - Noé Ras	✔(1º)	✔		✔			
mon (10002)	Dam1 - Mon Mon	✔(1º)				✔	✔	
tom (10003)	Dam1 - Tom Tom	✔(1º)				✔	✔	
pia (10004)	Dam2 - Pía Glez	✔(1º)				✔		✔
paz (10005)	Dam2 - Paz Fdez	✔(1º)				✔		✔

- Na seguinte imaxe amosa onde estará a carpeta persoal de *paz*:



1.3 Utilidades smbldap-tools

- Como xa vimos o paquete *smbldap-tools* ofrece un conxunto de scripts para a administración dos usuarios e grupos do dominio samba.
- Comentaremos as operacións máis importantes a continuación, aínda que no noso caso recomendamos utilizar unha ferramenta gráfica, a ser posible.
- A continuación amósanse os comandos asociados á utilidade:

```
smbldap-
  smbldap-groupadd   smbldap-groupshow  smbldap-userdel    smbldap-usershow
  smbldap-groupdel   smbldap-passwd     smbldap-userinfo
  smbldap-grouplist  smbldap-populate   smbldap-userlist
  smbldap-groupmod   smbldap-useradd    smbldap-usermod
```

1.4 Xestion de grupos

- Imos a continuación ver tanto con smb-tools como con LAM como xestionar grupos

1.4.1 Listar os grupos

```
smbldap-grouplist -?
  Usage: /usr/sbin/smbldap-grouplist [dtS?] [user template]
  -d     Show displayName
  -t     Show samba group type
  -S     Show samba SID
  -?     show the help message

smbldap-grouplist -tS
gid  |cn                  |sambaGroupType|sambaSID                                  |

10000 |g-usuarios           |-|-|
10001 |g-profes             |-|-|
10002 |g-dam1-profes        |-|-|
```

```
10003 |g-dam2-profes        |-|-|
10004 |g-alum               |-|-|
10005 |g-dam1-alum          |-|-|
10006 |g-dam2-alum          |-|-|
 512 |Domain Admins        |domain        |S-1-5-21-3472892566-1518861306-3316237868-512  |
 513 |Domain Users         |domain        |S-1-5-21-3472892566-1518861306-3316237868-513  |
 514 |Domain Guests        |domain        |S-1-5-21-3472892566-1518861306-3316237868-514  |
 515 |Domain Computers     |domain        |S-1-5-21-3472892566-1518861306-3316237868-515  |
 544 |Administrators       |local         |S-1-5-32-544                                   |
 548 |Account Operators    |local         |S-1-5-32-548                                   |
 550 |Print Operators      |local         |S-1-5-32-550                                   |
 551 |Backup Operators     |local         |S-1-5-32-551                                   |
 552 |Replicators          |local         |S-1-5-32-552
```

```
ldapsearch -x -LLL -b dc=iescalquera,dc=local cn="g-usuarios"
ou
smbldap-groupshow g-usuarios

  dn: cn=g-usuarios,ou=grupos,dc=iescalquera,dc=local
  objectClass: posixGroup
  cn: g-usuarios
  gidNumber: 10000

ldapsearch -x -LLL -b dc=iescalquera,dc=local cn="Domain U*"
  dn: cn=Domain Users,ou=grupos,dc=iescalquera,dc=local
  objectClass: top
  objectClass: posixGroup
  objectClass: sambaGroupMapping
  cn: Domain Users
  gidNumber: 513
  description: Netbios Domain Users
  sambaSID: S-1-5-21-3472892566-1518861306-3316237868-513
  sambaGroupType: 2
  displayName: Domain Users

smbldap-groupshow "Domain Users"
  dn: cn=Domain Users,ou=grupos,dc=iescalquera,dc=local
  objectClass: top,posixGroup,sambaGroupMapping
  cn: Domain Users
  gidNumber: 513
  description: Netbios Domain Users
  sambaSID: S-1-5-21-3472892566-1518861306-3316237868-513
  sambaGroupType: 2
  displayName: Domain Users
```

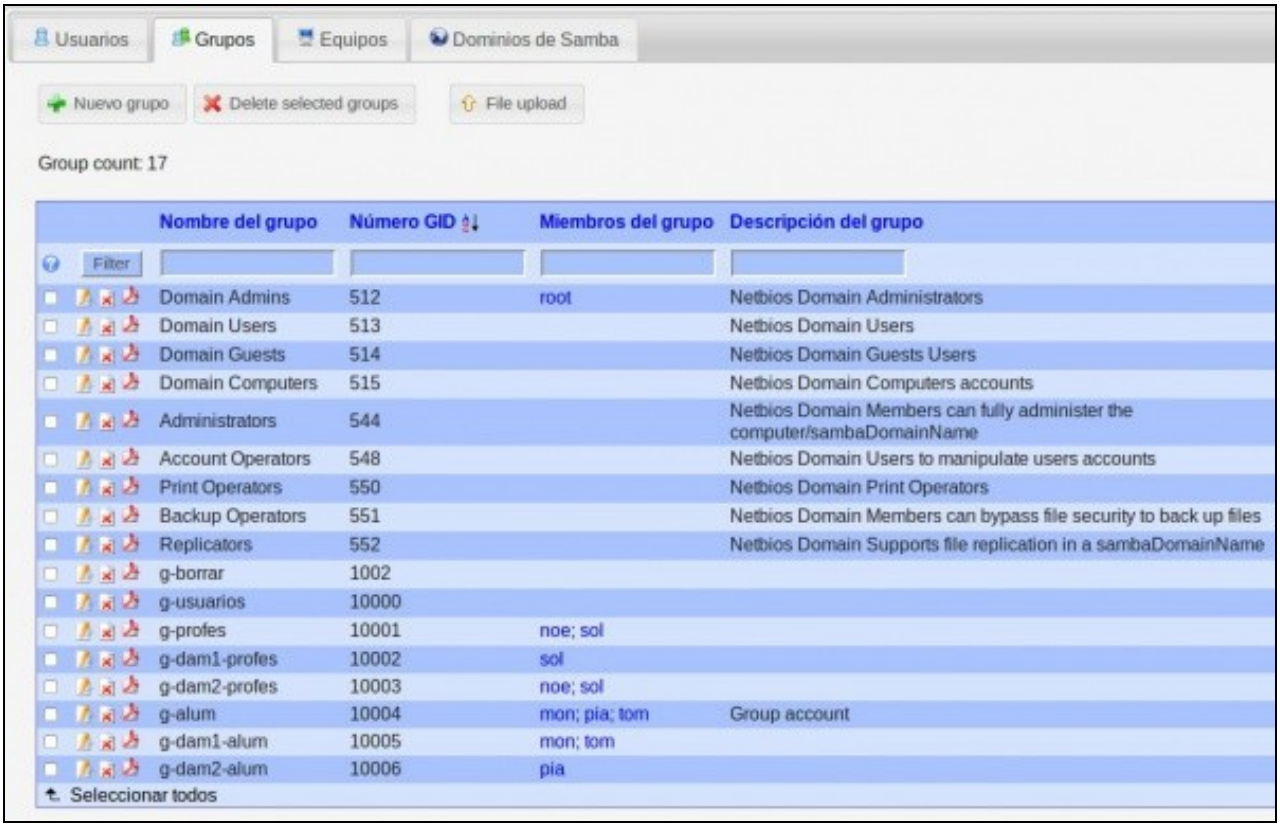
1.4.2 Engadir un grupo. Engadir atruibutos SAMBA

- Neste apartado imos ver como engadir un novo grupo e como engadir atributos samba a un grupo xa creado.

```
smbldap-groupadd -?
  (c) Jerome Tournier - (jtournier@gmail.com)- Licensed under the GPL
  Usage: /usr/sbin/smbldap-groupadd [-abgoprst?] groupname
    -a   add automatic group mapping entry
    -b   create a AIX group
    -g   gid
    -o   gid is not unique
    -p   print the gidNumber to stdout
    -r   group-rid
    -s   group-sid
    -t   group-type
    -?   show this help message

smbldap-groupadd -a g-borrar

#Amosar info sobre o grupo
smbldap-groupshow g-borrar
```

```
dn: cn=g-borrar,ou=grupos,dc=iescalquera,dc=local
objectClass: top,posixGroup,sambaGroupMapping
cn: g-borrar
gidNumber: 1002
sambaSID: S-1-5-21-3472892566-1518861306-3316237868-3005
sambaGroupType: 2
displayName: g-borrar
```

- En LAM podemos ver os grupos, os seus GIDs, etc.

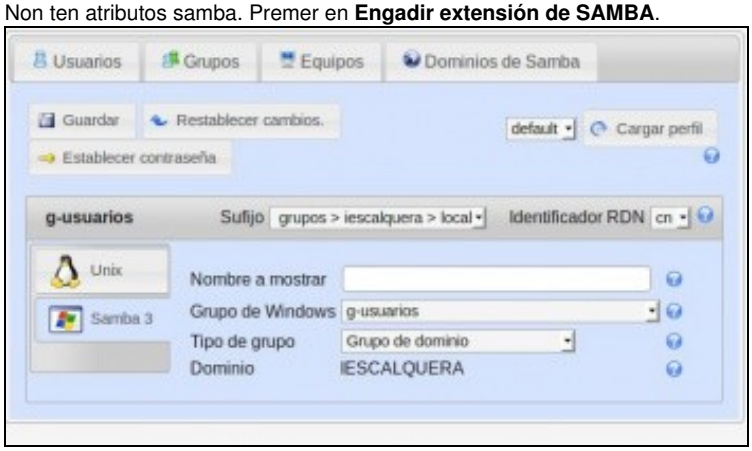


- Engadir atributos samba a un grupo
- 

O grupo **g-usuarios** amosando os atributos Unix

- 

Non ten atributos samba. Premer en **Engadir extensión de SAMBA**.

- 

O grupo xa ten os atributos SAMBA. Premer en **Gardar**.

- Para engadir os atributos samba a un grupo LDAP existente tamén poderíamos usar un ficheiro LDIF como fixemos en partes anteriores do curso.

- Non sería preciso engadir atributos SAMBA aos grupos existentes, pois o acceso ás carpetas do esqueleto é controlado polo servidor *dserver00*, e aí xa están definidos a que grupos pertence o usuario e que a que carpetas poden acceder os grupos aos que pertence. Pero se non engadíramos os atributos samba eses grupos non se van poder manexar dende clientes Windows, por exemplo para dar permisos a unha carpeta, controlar a que grupos pertence un usuario, etc.

- Por tanto, é aconsellable engadir os atributos SAMBA ao resto dos grupos creados previamente no LDAP:

- E obter esta lista:

```
smbldap-grouplist -tS
gid  |cn                  |sambaGroupType|sambaSID                                      |

10000 |g-usuarios           |domain        |S-1-5-21-3472892566-1518861306-3316237868-21001|
10001 |g-profes             |domain        |S-1-5-21-3472892566-1518861306-3316237868-21003|
10002 |g-dam1-profes        |domain        |S-1-5-21-3472892566-1518861306-3316237868-21005|
10003 |g-dam2-profes        |domain        |S-1-5-21-3472892566-1518861306-3316237868-21007|
10004 |g-alum               |domain        |S-1-5-21-3472892566-1518861306-3316237868-21009|
10005 |g-dam1-alum          |domain        |S-1-5-21-3472892566-1518861306-3316237868-21011|
10006 |g-dam2-alum          |domain        |S-1-5-21-3472892566-1518861306-3316237868-21013|
 512 |Domain Admins        |domain        |S-1-5-21-3472892566-1518861306-3316237868-512  |
 513 |Domain Users         |domain        |S-1-5-21-3472892566-1518861306-3316237868-513  |
 514 |Domain Guests        |domain        |S-1-5-21-3472892566-1518861306-3316237868-514  |
 515 |Domain Computers     |domain        |S-1-5-21-3472892566-1518861306-3316237868-515  |
 544 |Administrators       |local         |S-1-5-32-544                                   |
 548 |Account Operators    |local         |S-1-5-32-548                                   |
 550 |Print Operators      |local         |S-1-5-32-550                                   |
 551 |Backup Operators     |local         |S-1-5-32-551                                   |
 552 |Replicators          |local         |S-1-5-32-552                                   |
1002 |g-borrar             |domain        |S-1-5-21-3472892566-1518861306-3316237868-3005 |
```

1.4.3 Eliminar un grupo

- Pódese eliminar un grupo dende LAM/JXplorer, coas utilidades, etc.

```
smbldap-groupdel g-borrar
```

1.5 Xestión de usuarios

- Imos facer agora o propio coa xestión de usuarios

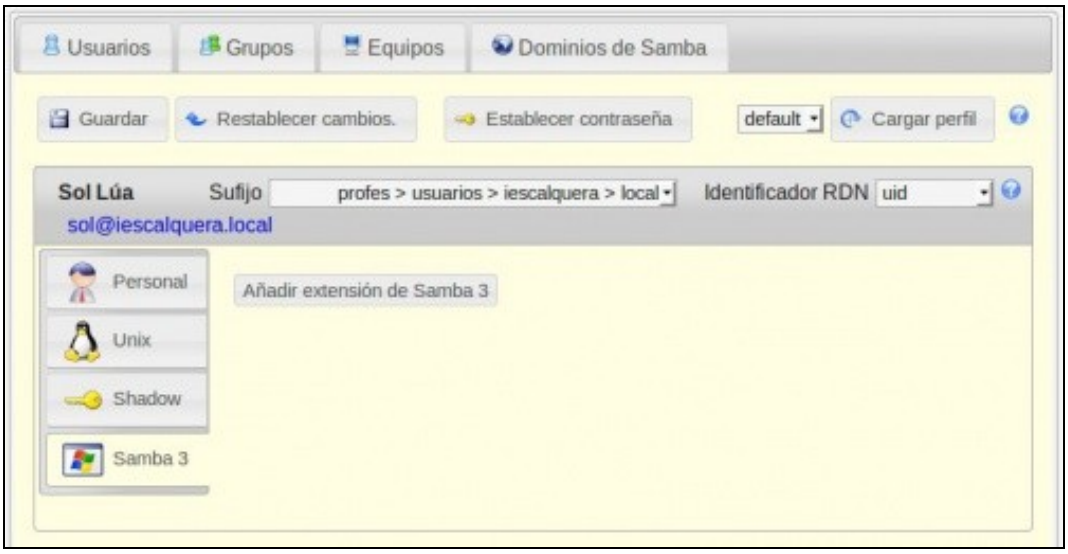
1.5.1 Listar os usuarios

```
smbldap-userlist -u
uid  |username

10000 |sol                  |
10001 |noe                  |
10002 |mon                  |
10003 |tom                  |
10004 |pia                  |
    0 |root                 |
65534 |nobody               |
```

```
ldapsearch -x -LLL -b dc=iescalquera,dc=local uid=sol
dn: uid=sol,ou=profes,ou=usuarios,dc=iescalquera,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: sol
sn:: TMO6YQ==
cn:: UHJvZmUgLSBTb2wgTMO6YQ==
givenName: Sol
uidNumber: 10000
gidNumber: 10000
loginShell: /bin/bash
mail: sol@iescalquera.local
initials: SL
shadowExpire: -1
gecos: "Profe - Sol Lua"
homeDirectory: /home/iescalquera/profes/sol
```

```
smbldap-usershow sol
dn: uid=sol,ou=profes,ou=usuarios,dc=iescalquera,dc=local
objectClass: inetOrgPerson,posixAccount,shadowAccount,sambaSamAccount
uid: sol
sn: Lúa
cn: Profe - Sol Lúa
givenName: Sol
uidNumber: 10000
gidNumber: 10000
loginShell: /bin/bash
mail: sol@iescalquera.local
initials: SL
shadowExpire: -1
gecos: "Profe - Sol Lua"
homeDirectory: /home/iescalquera/profes/sol
```

- En LAM tamén se ve que a usuaria sol non ten atributos SAMBA.
- Non llos imos engadir por agora



1.5.2 Engadir atributos SAMBA aos usuarios existentes no LDAP

- Como antes, cos grupos, aos usuarios existentes no LDAP hai que engadirlle os atributos SAMBA no LDAP e poñerlle o contrasinal SAMBA.

- **Activar un usuario existente no LDAP como usuario samba** permite tomar un usuario xa existente no LDAP e activalo como usuario samba (o que implicará engadirlle unha serie de atributos no seu obxecto no LDAP definidos no esquema de samba).
- Hai que ter en conta que os usuarios que tiñamos xa dados de alta no LDAP non estarán activados como usuarios samba.
- O comando solicitará o contrasinal de samba para este usuario, que non ten por que coincidir co contrasinal propio do usuario no LDAP (aínda que normalmente é aconsellable que os usuarios teñan o mesmo contrasinal tanto para entrar en Windows como en Linux), e será o contrasinal que usará o usuario para acceder dende os equipos Windows:
- Nesta ocasión imos usar o comando **smbpasswd**

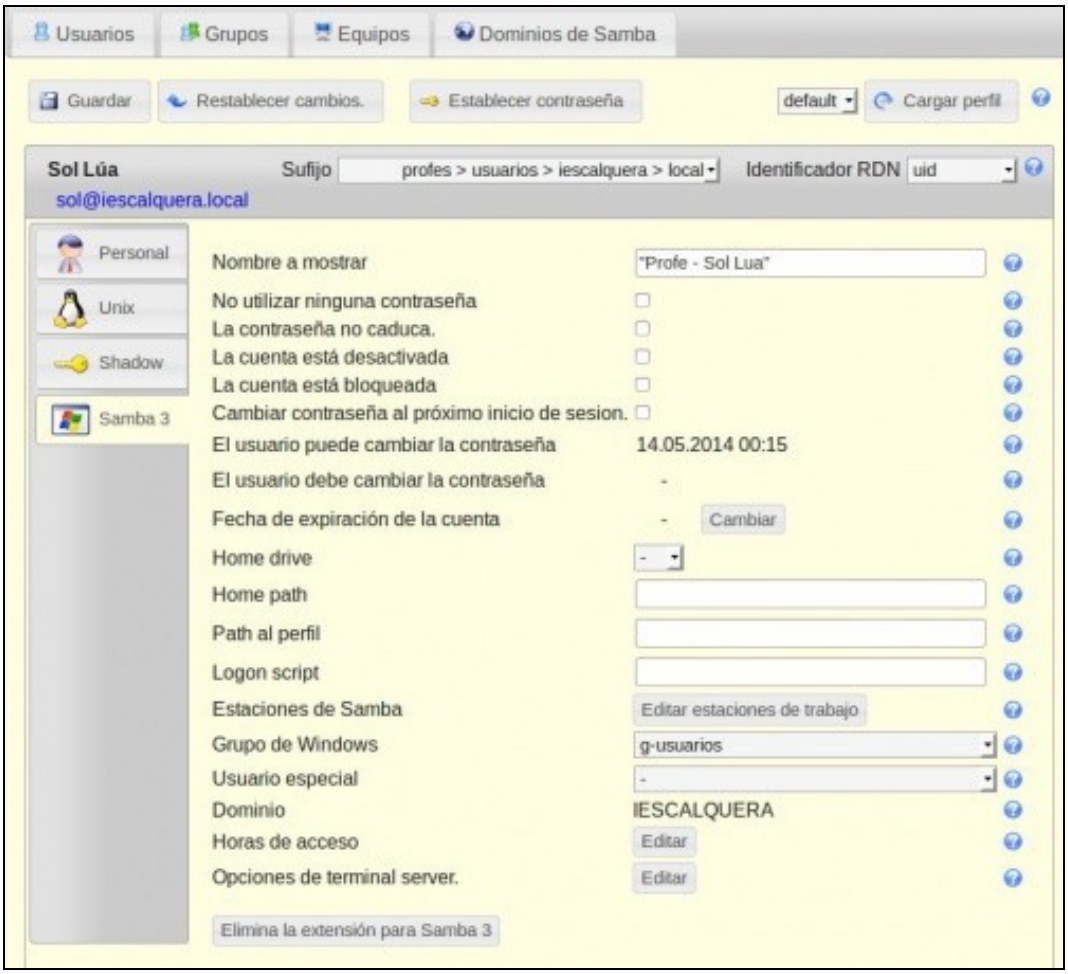
```
smbpasswd -h
When run by root:
    smbpasswd [options] [username]
otherwise:
    smbpasswd [options]

options:
  -L                   local mode (must be first option)
  -h                   print this usage message
  -s                   use stdin for password prompt
  -c smb.conf file     Use the given path to the smb.conf file
  -D LEVEL             debug level
  -r MACHINE           remote machine
  -U USER              remote username
extra options when run by root or in local mode:
  -a                   add user
  -d                   disable user
  -e                   enable user
  -i                   interdomain trust account
  -m                   machine trust account
  -n                   set no password
  -W                   use stdin ldap admin password
  -w PASSWORD          ldap admin password
  -x                   delete user
  -R ORDER             name resolve order
```

```
smbpasswd -a sol
New SMB password:
Retype new SMB password:
Added user sol.
```

- Observar como se crearon os atributos SAMBA para a usuaria *sol*:

```
smbldap-usershow sol
dn: uid=sol,ou=profes,ou=usuarios,dc=iescalquera,dc=local
objectClass: inetOrgPerson,posixAccount,shadowAccount,sambaSamAccount
uid: sol
sn: Lúa
cn: Profe - Sol Lúa
givenName: Sol
uidNumber: 10000
gidNumber: 10000
loginShell: /bin/bash
mail: sol@iescalquera.local
initials: SL
shadowExpire: -1
gecos: "Profe - Sol Lua"
homeDirectory: /home/iescalquera/profes/sol
shadowLastChange: 16203
shadowMax: 45
sambaSID: S-1-5-21-3472892566-1518861306-3316237868-1002
displayName: "Profe - Sol Lua"
sambaNTPassword: 3EC585243C919F4217175E1918E07780
sambaPasswordHistory: 0000000000000000000000000000000000000000000000000000000000000000
sambaAcctFlags: [U          ]
userPassword: {SSHA}8tX8CKF85hUblwb3OSeauSLsohH5gqlv
sambaPwdLastSet: 1400019331
```

- En LAM, a usuaria sol xa ten cubertos os seus atributos:



- Poderíanse engadir os atributos dende LAM.
- Pero non o imos facer pois non se cobren todos os campos e ademais tamén hai que axustar o contrasinal

- **O lector debe activar o resto dos usuarios LDAP como usuarios SAMBA.**

1.5.3 Engadir un novo usuario

- Podemos engadilo dende LAM, pero imos engadilo coas utilidades. Imos engadir a usuaria *paz*, que quedaba pendente:

USUARIOS E GRUPOS

Grupos Usuarios	Nome Completo	g-usarios (10000)	g-profes (10001)	g-dam1-profes (10002)	g-dam2-profes (10003)	g-alum (10004)	g-dam1-alum (10005)	g-dam2-alum (10006)
Descric.		Todolos usuarios de LDAP	Todo o profesorado	Profesorado de 1º da DAM	Profesorado de 2º DAM	Todo o alumnado	Alumnado de 1º da DAM	Alumnado de 2º da DAM
sol (10000)	Profe - Sol Lúa	✔(1º)	✔	✔	✔			
noe (10001)	Profe - Noé Ras	✔(1º)	✔		✔			
mon (10002)	Dam1 - Mon Mon	✔(1º)				✔	✔	
tom (10003)	Dam1 - Tom Tom	✔(1º)				✔	✔	
pia (10004)	Dam2 - Pía Glez	✔(1º)				✔		✔
paz (10005)	Dam2 - Paz Fdez	✔(1º)				✔		✔

- Para crear un novo usuario no LDAP xa activado como usuario samba, usamos o comando **smbldap-useradd**.
- As opcións son as seguintes:

```
smbldap-useradd -?
(c) Jerome Tournier - (jtournier@gmail.com)- Licensed under the GPL
Usage: /usr/sbin/smbldap-useradd [OPTIONS] USERNAME

Options:
  -a    is a Windows User (otherwise, Posix stuff only)
  -b    is a AIX User
  -c    gecos
  -d    home
  -g    gid
  -i    is a trust account (Windows Workstation)
  -k    skeleton dir (with -m)
  -m    creates home directory and copies /etc/skel
  --non-unique
        Allow the creation of a user account with a duplicate (non-unique) UID.
```

```
  -n    do not create a group
  -o    add the user in the organizational unit (relative to the user suffix. Ex: 'ou=admin,ou=all')
  -s    shell
  -t    time. Wait 'time' seconds before exiting (when adding Windows Workstation)
  -u    uid
  -w    is a Windows Workstation (otherwise, Posix stuff only)
  -W    is a Windows Workstation, with Samba atributes (otherwise, Posix stuff only)
  -A    can change password ? 0 if no, 1 if yes
  -B    must change password ? 0 if no, 1 if yes
  -C    sambaHomePath (SMB home share, like '\\PDC-SRV\homes')
  -D    sambaHomeDrive (letter associated with home share, like 'H:')
  -E    sambaLogonScript (DOS script to execute on login)
  -F    sambaProfilePath (profile directory, like '\\PDC-SRV\profiles\foo')
  -G    supplementary comma-separated groups
  -H    sambaAcctFlags (samba account control bits like '[NDHTUMWSLKI]')
  -M    e-mail address (comma separated)
  -N    given name
  -O    localMailAddress (comma separated)
  -P    ends by invoking smbldap-passwd
  -S    surname (Family name)
  -T    mailToAddress (forward address) (comma separated)
  -X    input encoding for givenname and surname (default UTF-8)
  -Z    set custom LDAP attributes, name=value pairs comma separated
  -h    show this help message
```

- Como exemplo imos engadir un usuario para logo borralo

```
smbldap-useradd -a -P u-borrar
  Changing UNIX and samba passwords for u-borrar
  New password:
  Retype new password:
```

- Imos agora engadir a usuaria *paz* engadindo todos os campos que lle engadimos aos outros usuarios.

- Non faría falla usar todos os campos que veñen a continuación, pero para cumprir a premisa anterior:

```
smbldap-useradd -a -c "DAM2 Paz Fdez" -d "/home/iescalquera/alumnos/dam2/paz" -g 10000 -m -o 'ou=dam2,ou=alum' -u 10005 -G g-usuario
   User "paz" already member of the group "g-usuarios".
   Changing UNIX and samba passwords for paz
   New password:
   Retype new password:
```

- Observar o significado de cada campo na axuda superior.
- Non se engadiu o campo *displayName* porque dá un erro o script
- Comprobación:

```
smbldap-usershow paz
dn: uid=paz,ou=dam2,ou=alum,ou=usuarios,dc=iescalquera,dc=local
objectClass: top,person,organizationalPerson,posixAccount,shadowAccount,inetOrgPerson,sambaSamAccount
cn: Paz Fdez,DAM2 Paz Fdez
sn: Fdez
uid: paz
uidNumber: 10005
gidNumber: 10000
homeDirectory: /home/iescalquera/alumnos/dam2/paz
loginShell: /bin/bash
gecos: DAM2 Paz Fdez
givenName: Paz
initials: PF
mail: paz@iescalquera.local
sambaLogonTime: 0
sambaLogoffTime: 2147483647
sambaKickoffTime: 2147483647
sambaPwdCanChange: 0
displayName: Paz Fdez
sambaSID: S-1-5-21-3472892566-1518861306-3316237868-21010
sambaPrimaryGroupSID: S-1-5-21-3472892566-1518861306-3316237868-21001
sambaLogonScript: inicio.bat
```

```
sambaHomePath: \\dserver00\paz
sambaHomeDrive: Z:
sambaLMPassword: B7515DC140629D41AAD3B435B51404EE
sambaAcctFlags: [U]
sambaNTPassword: 3EC585243C919F4217175E1918E07780
sambaPwdLastSet: 1400134506
sambaPwdMustChange: 1404022506
userPassword: {SSHA}k5DdcrgfW7v0VCIWZH3uZHLmCJNnaTEv
shadowLastChange: 16205
shadowMax: 45
```

- Observar como o campo displayName, está composto polo nome e apelidos da usuaria.

- Comprobar se é un usuario co que poder entrar no sistema:

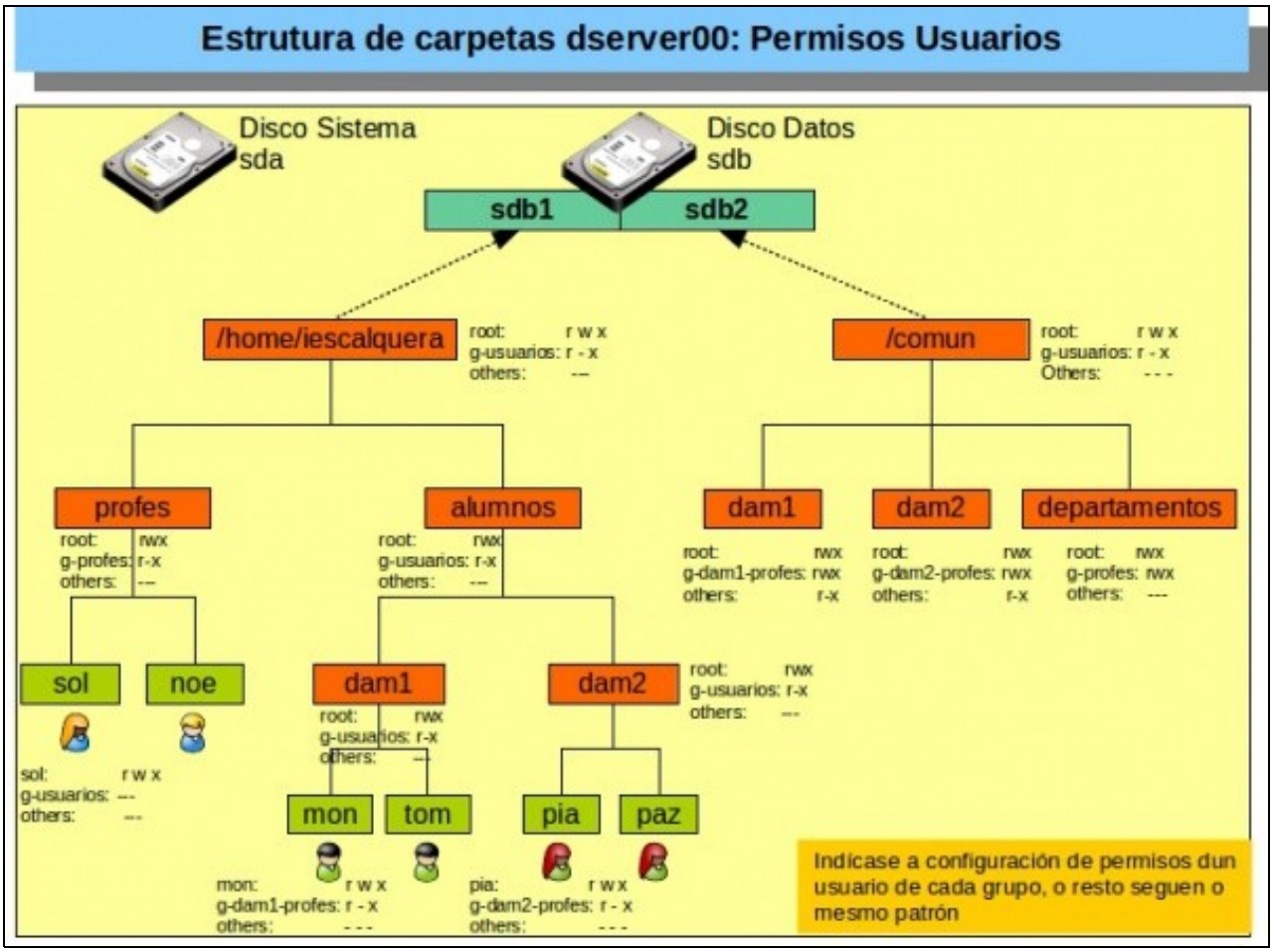
```
getent passwd | tail -n 1
paz:x:10005:10000:DAM2 Paz Fdez:/home/iescalquera/alumnos/dam2/paz:/bin/bash
```

- Comprobar os grupos e os seus membros. Paz pertence aos grupos correctos.

```
getent group | grep g-
g-usuarios:*:10000:paz
g-profes:*:10001:noe,sol
g-dam1-profes:*:10002:sol
g-dam2-profes:*:10003:noe,sol
g-alum:*:10004:paz,tom,mon,pia
g-dam1-alum:*:10005:tom,mon
g-dam2-alum:*:10006:paz,pia
```

- O lector pode comprobar o resultado en LAM.

1.5.4 O cartafol persoal de paz




```
ls /home/iescalquera/alumnos/dam2 -l
  total 8
  drwx------  2 paz g-usuarios    4096 Mai 13 21:29 paz
  drwxr-x--- 18 pia g-dam2-profes 4096 Mai 15 06:36 pia

ls /home/iescalquera/alumnos/dam2/paz -la
  total 32
  drwx------ 2 paz  g-usuarios 4096 Mai 13 21:29 .
  drwxr-x--- 4 root g-usuarios 4096 Mai 15 08:14 ..
  -rw-r--r-- 1 paz  g-usuarios  220 Mai 13 21:29 .bash_logout
  -rw-r--r-- 1 paz  g-usuarios 3637 Mai 13 21:29 .bashrc
  -rw-r--r-- 1 paz  g-usuarios 8980 Mai 13 21:29 examples.desktop
  -rw-r--r-- 1 paz  g-usuarios  675 Mai 13 21:29 .profile
```

- Vemos que o cartafol de paz non ten o grupo de acordo ao esquema. Pero en cambio, os ficheiros de Skel foron copiados correctamente, os de Ubuntu.

- Para arranxar o problema dos permisos no cartafol de paz é sinxelo. Executar o script 03

```
scripts# sh 03_crear_home_usuarios_axustar_permisos.sh

ls /home/iescalquera/alumnos/dam2 -l
  total 8
  drwxr-x---  2 paz g-dam2-profes 4096 Mai  7 09:45 paz
  drwxr-x--- 18 pia g-dam2-profes 4096 Mai  7 09:45 pia
```

1.5.5 Manipulación de usuarios e grupos. Borrado usuarios

- **Engadir un usuario a un grupo**:
  - Usamos o comando *smbldap-groupmod*.
  - A opción *-m* permite introducir máis dun usuario separándoos por comas:

```
smbldap-groupmod -m usuario1,usuario2 grupo
```

- **Quitar un usuario dun grupo**:
    - Usamos tamén *smbldap-groupmod* pero coa opción *-x*:

```
smbldap-groupmod -x usuario1 grupo
```

- **Borrar un usuario do dominio**:
    - Onde a opción *-r* permite borrar tamén o directorio persoal do usuario.

```
smbldap-userdel -r u-borrar
```

1.6 Engadir un equipo no dominio

- Podemos usar o comando **smbldap-useradd** para engadir contas de equipo en samba.
    - A opción *-t 0* crea a conta sen retardo,
    - e *-w* indica que a conta de usuario é para un equipo.

- No noso caso non será necesario utilizar este comando, xa que coa configuración do servidor samba a conta crearase automaticamente ao introducir o equipo cliente no dominio.

```
smbldap-useradd -t 0 -w wexemplo10
```

1.7 Conclusións

- O curso vaise construíndo paso a paso, pero agora o lector pode concluír que se se precisan usuarios para equipos Windows e Linux, imos precisar os esquemas básicos do LDAP e o esquema de Samba.

- Ademais á hora de dar de alta os usuarios, por exemplo con LAM, xa podemos crear un modelo en formato CSV cos atributos necesarios para LDAP+SAMBA para dun só paso dar de alta os usuarios/grupos e dunha maneira sinxela.

- Tal e como estamos agora, o/a lector/a debe **activar os grupos e usuarios LDAP como grupos e usuarios SAMBA**.

-- Antonio de Andrés Lema e Carlos Carrión Álvarez