

Configuración dos recursos compartidos en Samba4

- Nesta sección imos ver como compartir con Samba4 as carpetas persoais dos usuarios e a carpeta común, así como a configuración necesaria para que os clientes, tanto Windows como Linux, accedan de forma automática a estas carpetas.
- Por último, veremos tamén como configurar os perfís móbiles dos usuarios para que a súa configuración persoal de escritorio, programas, etc. se mova con eles dun equipo a outro dentro do dominio.

Sumario

- 1 Definir recursos compartidos no servidor samba
- 2 Configurar as carpetas persoais centralizadas
 - ◆ 2.1 Configuración para os clientes Windows
 - ◇ 2.1.1 Con RSAT
 - ◇ 2.1.2 Con samba-tool
 - ◆ 2.2 Configuración para os clientes Linux
- 3 Configurar a conexión automática de outras carpetas compartidas
 - ◆ 3.1 Conexión automática dende os clientes Windows
 - ◇ 3.1.1 Con RSAT
 - ◇ 3.1.2 Con samba-tool
 - ◆ 3.2 Conexión automática dende os clientes Linux
- 4 Perfís móbiles
 - ◆ 4.1 Configuración para os clientes Windows
 - ◇ 4.1.1 Con RSAT
 - ◇ 4.1.2 Con samba-tool
 - ◆ 4.2 Configuración para os clientes Linux

Definir recursos compartidos no servidor samba

- O primeiro paso será engadir no ficheiro de configuración de samba as carpetas compartidas. Abrimos o ficheiro **/etc/samba/smb.conf** e engadimos no final as seguintes liñas:

```
[usuarios]
    path=/srv/samba/usuarios
    read only = No

[comun]
    path=/srv/samba/comun
    read only = No
```

- Un parámetro moi interesante que podemos engadir ao final da sección *[global]* é **hide unreadable**, para que as carpetas inaccesibles para un usuario xa non aparezan cando acceda a elas a través de samba:

```
[global]
    ....
    ....
    hide unreadable = yes
```

- Executamos o seguinte comando para recargar a configuración de samba:

```
smbcontrol all reload-config
```

Configurar as carpetas persoais centralizadas

- O que pretendemos neste apartado é que todo usuario do dominio teña accesible a súa carpeta persoal, tanto dende un equipo Windows como Linux.

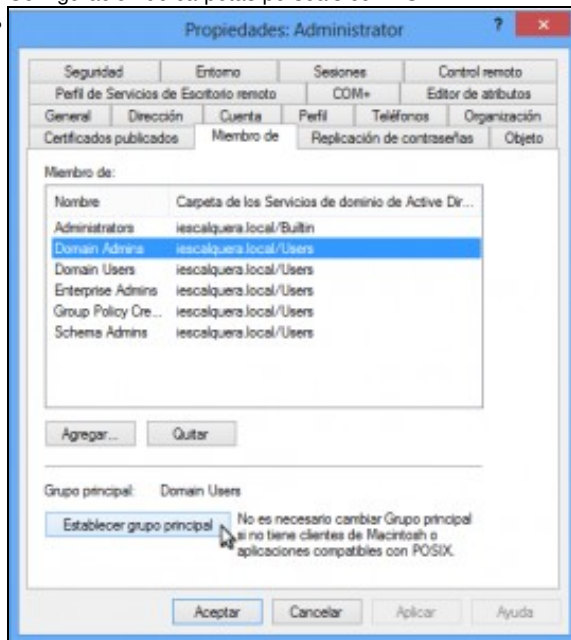
Configuración para os clientes Windows

- Imos ver como configurar a carpeta persoal dos usuarios para os clientes Windows do dominio utilizando RSAT, comprobando o seu funcionamento dende *wclient01*.

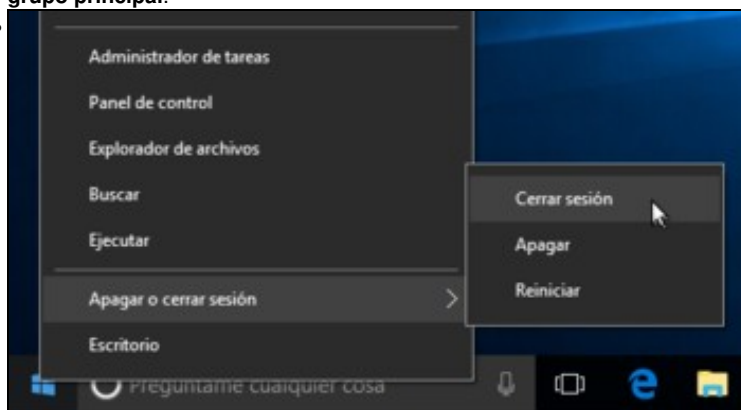
- Logo explicaremos tamén como podemos configurar a carpeta persoal con *samba-tool*.

Con RSAT

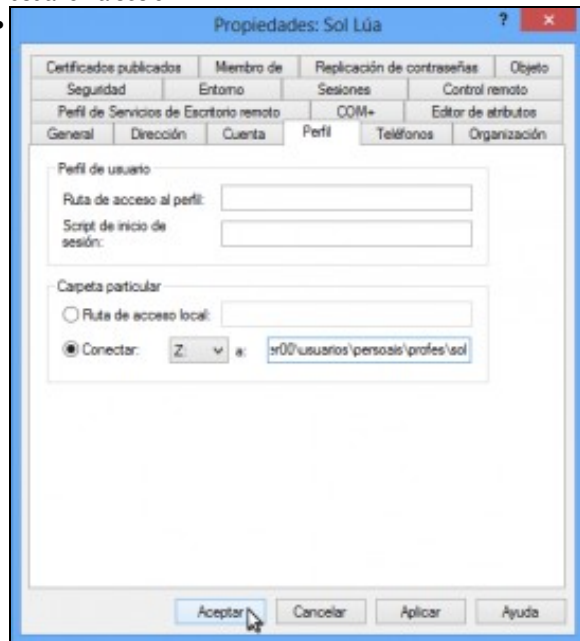
- Iniciaremos sesión no equipo *wclient01* como *Administrator* (recórdese que para poder administrar os usuarios o usuario ten que ser membro de do grupo *Domain Admins*) e lanzamos a ferramenta de **Usuarios e equipos de Active Directory**.
- No momento en que configuremos a carpeta persoal do usuario con RSAT, esta vaise crear de forma automática utilizando as credenciais do usuario co que iniciamos sesión (*Administrator*). Desta maneira, o usuario propietario da carpeta será *Administrator*, e o grupo propietario o grupo principal deste usuario. O máis conveniente sería que este grupo fose *Domain Admins*, e así só accederían ás carpetas ademais dos propios usuarios (e os profes ás dos alumnos dos seus grupos), os administradores do dominio.
- Por iso antes de nado imos facer un axuste nas propiedades do usuario *Administrator*, para establecer o grupo *Domain Admins* como principal.
- Configuración de carpetas persoais con RSAT



Nas propiedades do usuario *Administrator*, imos á pestana **Miembro de** para seleccionar o grupo *Domain Admins* e picar sobre **Establecer grupo principal**.



Pechamos a sesión do usuario *Administrator* e abrimola de novo, para que o cliente Windows cargue a nova configuración de grupos para o usuario na sesión.



Imos ás propiedades do usuario *sol* para configurar a súa carpeta persoal. Na pestana **Perfil**, dentro da sección de **Carpeta particular** activamos a opción de **Conectar**: e seleccionamos a letra da unidade na que queremos á que se conecte a carpeta persoal do usuario (deixamos Z:). Na caixa de texto introducimos a ruta á carpeta persoal do usuario, que no caso de *sol* será `\\dserver00\usuarios\persoais\profes\sol`. Aceptamos.

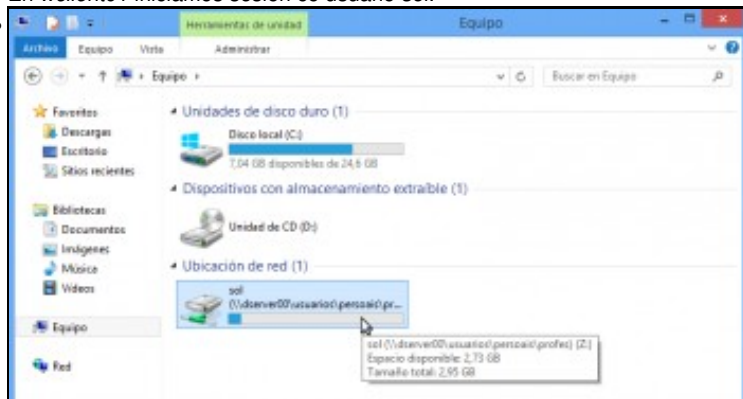
- Despois de configurar a carpeta persoal para *sol* e *noe*, podemos ver en *dserver00* as carpetas creadas e os seus permisos. Fixémonos en que en cada carpeta só pode entrar cada usuario, ademais dos administradores:

```
root@dserver00:~# ls -lh /srv/samba/usuarios/persoais/profes/
total 16K
drwxrwx---+ 2 3000003 users 4,0K Mai 17 20:15 noe
drwxrwx---+ 2 3000003 users 4,0K Mai 17 20:15 sol
root@dserver00:~/scripts_samba4# getfacl /srv/samba/usuarios/persoais/profes/sol
getfacl: Eliminando '/' iniciais en nomes de ruta absolutos
# file: srv/samba/usuarios/persoais/profes/sol
# owner: 3000003
# group: users
user::rwx
user:sol:rwx
group:---
group:users:---
group:3000003:rwx
mask::rwx
other:---
default:user::rwx
default:user:sol:rwx
default:user:3000003:rwx
default:group:---
default:group:users:---
default:group:3000003:rwx
default:mask::rwx
default:other:---
```

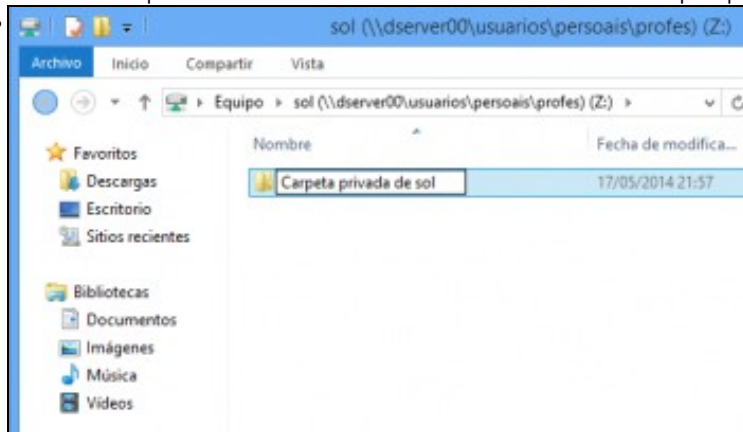
- Imos probar agora o efecto nos clientes Windows do dominio:
- Carpetas persoais para clientes Windows



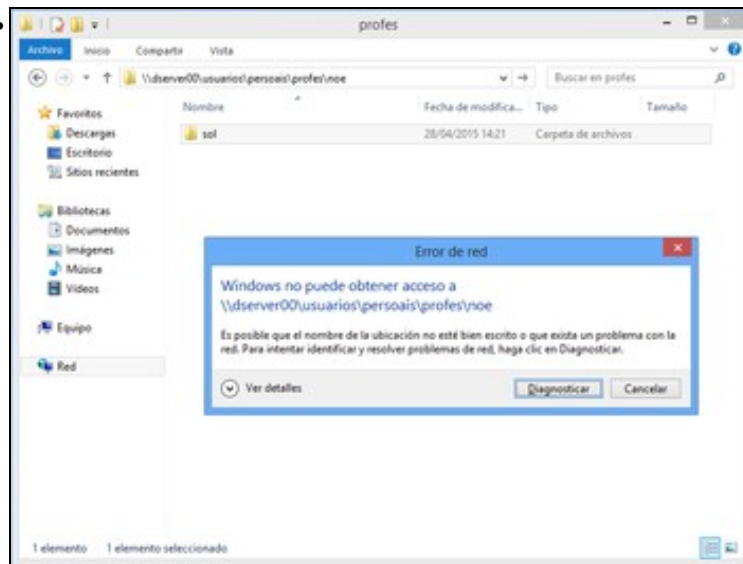
En *wclient01* iniciamos sesión co usuario *sol*.



Podemos ver que xa temos conectada a unidade de rede Z: á nosa carpeta persoal.



Comprobamos que podemos acceder e escribir dentro da carpeta.



Intentamos fisgonear na carpeta persoal de outro usuario. Comprobamos que non se nos permite.

Con samba-tool

- Se usamos *samba-tool* para a creación dos usuarios, podemos utilizar os seguintes parámetros para configurar a carpeta persoal:
 - ♦ **--home-drive=letra_da_unidade** (indicamos a letra a unidade na que se conectará a carpeta persoal)
 - ♦ **--home-directory=ruta_carpeta_persoal** (a ruta da carpeta persoal do usuario como a introduciríamos en RSAT pero introducindo o carácter de escape (\) antes de cada \, de forma que haberá que duplicar cada \. Por exemplo, a ruta da carpeta persoal de *sol* introduciríamola como: `\\\\dserver00\usuarios\persoais\profes\\sol`)
- Neste caso, teremos que crear a carpeta persoal de forma manual, xa que *samba-tool* non creará a carpeta de forma automática. Tamén teremos que establecer os permisos adecuados para que o usuario poida acceder á súa carpeta persoal, preferentemente utilizando ACLs.

Configuración para os clientes Linux

- Nos clientes Linux a configuración será diferente, xa que será nos clientes onde realizaremos a configuración necesaria para que monten unha carpeta por CIFS cando o usuario inicia sesión.
- Para poder montar a carpeta coas credenciais que introduce o usuario ao iniciar sesión, utilizaremos o paquete *libpam-mount*.
- Instalamos o paquete *libpam-mount*, e o paquete *cifs-utils* para poder montar carpetas por CIFS.

```
sudo apt-get install libpam-mount cifs-utils
```

- Abrimos como *root* o ficheiro de configuración do paquete *libpam-mount*, `/etc/security/pam_mount.conf.xml` para engadir as liñas marcadas antes da etiqueta de peche `</pam_mount>`:

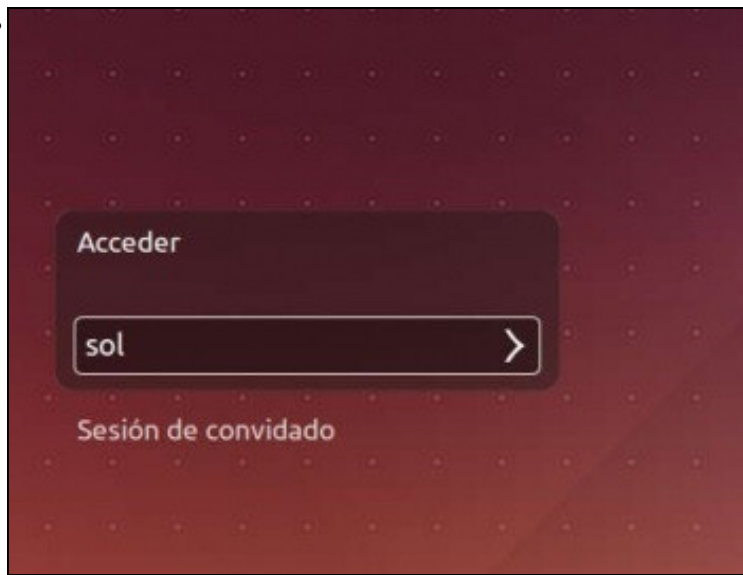
```
...
<logout wait="0" hup="0" term="0" kill="0" />

<mkmountpoint enable="1" remove="true" />

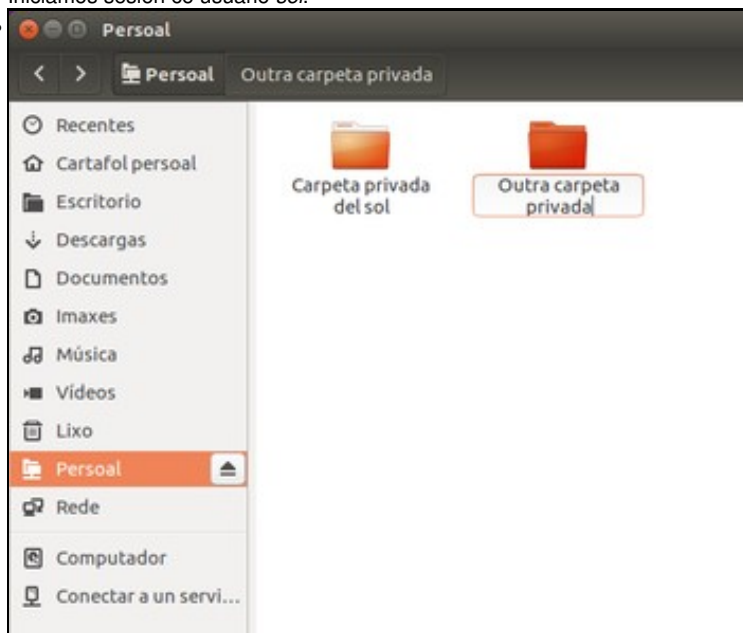
<volume sgrp="g-profes" fstype="cifs" server="dserver00.iescalquera.local" path="/usuarios/persoais/profes/%(USER)" mountpoint="/media/usuarios/persoais/profes/%(USER)" />
<volume sgrp="g-dam1-alum" fstype="cifs" server="dserver00.iescalquera.local" path="/usuarios/persoais/alumnos/dam1/%(USER)" mountpoint="/media/usuarios/persoais/alumnos/dam1/%(USER)" />
<volume sgrp="g-dam2-alum" fstype="cifs" server="dserver00.iescalquera.local" path="/usuarios/persoais/alumnos/dam2/%(USER)" mountpoint="/media/usuarios/persoais/alumnos/dam2/%(USER)" />

</pam_mount>
```

- O que estamos facendo é montar, en función do grupo no que estea o usuario a súa carpeta persoal en `/media/usuario/Persoal`.
- Vexamos o efecto da configuración:
- Carpetas persoais para clientes Linux



Iniciamos sesión co usuario *sol*.



Iniciamos o explorador de ficheiros e veremos no panel lateral un enlace á carpeta Persoal. Accedemos a ela e veremos a carpeta creada no cliente Windows. Comprobamos que podemos escribir dentro da carpeta.

Configurar a conexión automática de outras carpetas compartidas

- Ademais das carpetas persoais de cada usuario, é moi habitual que dentro do dominio teñamos carpetas comúns ás que poden acceder distintos usuarios.
- No noso caso, xa temos creada a carpeta compartida *comun* e os usuarios poderían acceder manualmente a ela co explorador de ficheiros tanto dende os clientes Windows como Linux, pero imos ver como podemos conectar automaticamente un acceso a esas carpetas.

Conexión automática dende os clientes Windows

- Nos clientes Windows, imos facer uso dun script de inicio de sesión que conecte as carpetas comúns que nos interesen.
- Como xa vimos na parte V, os clientes Windows buscarán ese script dentro dunha carpeta compartida co nome *netlogon* no controlador do dominio.
- Se vemos o contido do ficheiro de configuración de samba, esta carpeta xa está compartida:

```
....
[netlogon]
    path = /var/lib/samba/sysvol/iescalquera.local/scripts
```

```
read only = No
....
```

- Pois imos crear dentro desa carpeta o script de inicio de sesión **inicio.bat**, que será tamén moi similar ao que definimos na parte V, simplemente adaptando a ruta das carpetas persoais dos alumnos:

- **SCRIPT /var/lib/samba/sysvol/iescalquera.local/scripts/inicio.bat:**

```
@echo off
REM Ficheiro de inicio de sesion

REM Mapeamos comun para todo usuario que inicie sesion
net use R: \\dserver00\comun /persistent:no

REM Miramos se o usuario que inicia sesion e un profesor
REM Se é un profesor mapeamos alumnos a S:
    net user /domain %username% | findstr /C:"g-profe" && (
        net use S: \\dserver00\usuarios\persoais\alumnos /persistent:no
    )

REM Miramos se o usuario que inicia sesion e un alumno
REM Se e un alumno abrimos un aviso (Como facer dobre clic sobre o ficheiro: st$
    net user /domain %username% | findstr /C:"g-alum" && (
        start \\dserver00\netlogon\avisos\aviso_alumnos.html
    )
```

- Creamos a carpeta de avisos e o ficheiro *aviso_alumno.html* coa mensaxe de benvida:

```
mkdir /var/lib/samba/sysvol/iescalquera.local/scripts/avisos
nano /var/lib/samba/sysvol/iescalquera.local/scripts/avisos/aviso_alumnos.html
```

- **Ficheiro /var/lib/samba/sysvol/iescalquera.local/scripts/avisos/aviso_alumnos.html:**

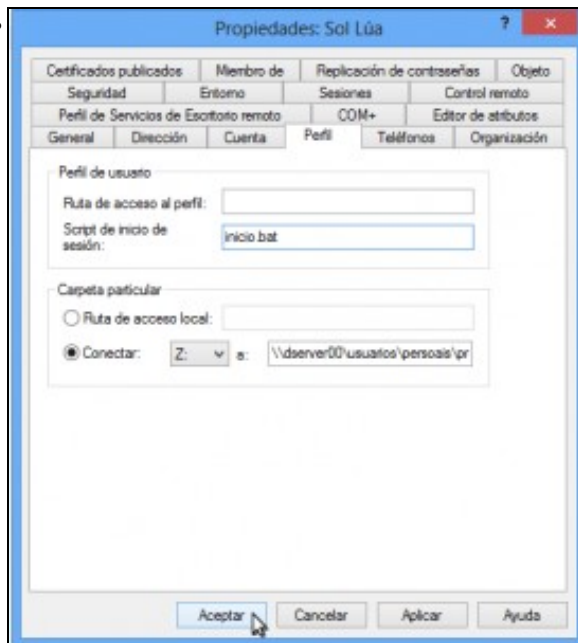
```
Benvidos/as ao IES Calquera
```

- Imos establecer os permisos de toda a carpeta na que gardamos o script e o seu contido (de forma recursiva), para que todos os usuarios poidan ler e executar o seu contido:

```
setfacl -Rm g:g-usuarios:rx /var/lib/samba/sysvol/iescalquera.local/scripts/
```

Con RSAT

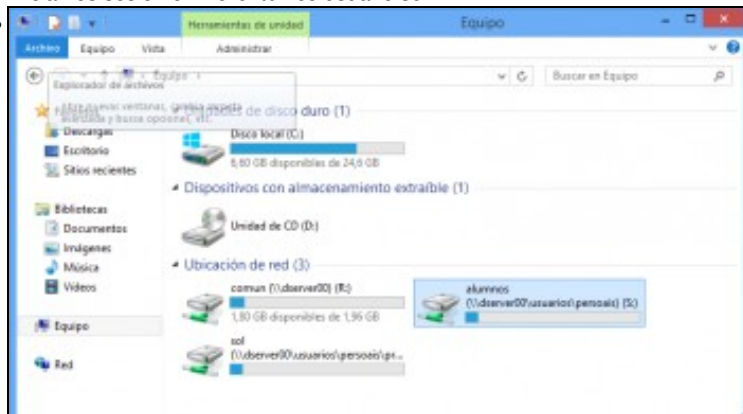
- Unha vez que xa temos o script creado no servidor, imos configurar os usuarios para que executen o script no inicio da sesión.
- Script de inicio de sesión



Imos ás propiedades do usuario *sol* para ir á pestana **Perfil** e na caixa de **Script de inicio de sesión** introducir o nome do script. Ollo!! só o nome do script, non hai que engadir ningunha ruta porque os clientes xa o van buscar dentro de *netlogon*.



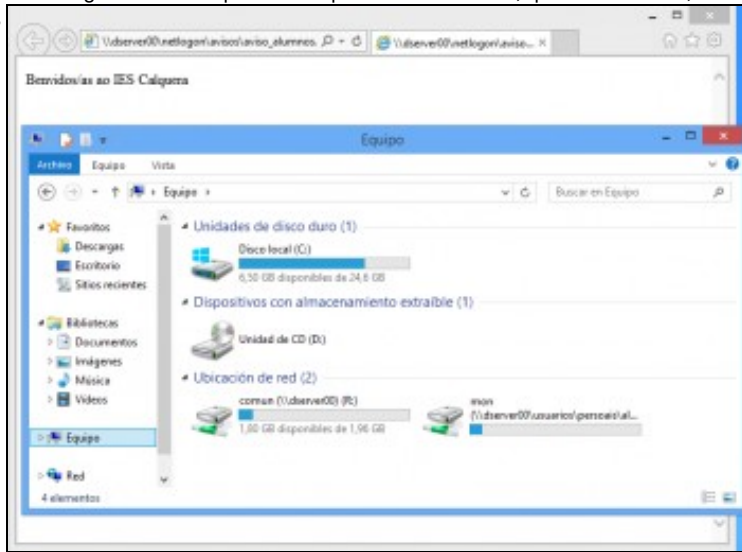
Iniciamos sesión en *wclient01* co usuario *sol*.



Vemos o efecto da execución do script, xa que *sol* pode acceder tanto a *comun* como ás carpetas persoais dos seus alumnos.



Se configuramos o script de inicio para o usuario *mon*, que é un alumno, e iniciamos sesión con el...



veremos a mensaxe de benvida, e só o acceso a *comun*.

Con samba-tool

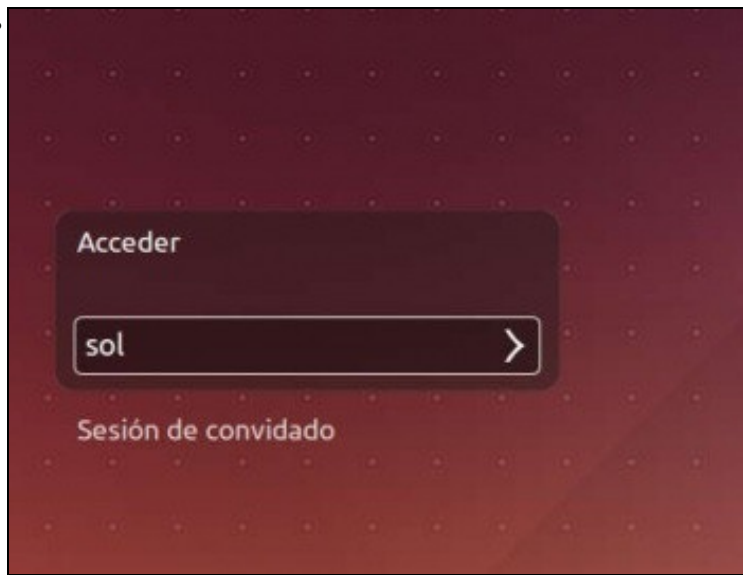
- Se usamos *samba-tool* para a creación dos usuarios, podemos establecer o script de inicio de sesión para o usuario co parámetro:
♦ **--script-path=nome_do_script**

Conexión automática dende os clientes Linux

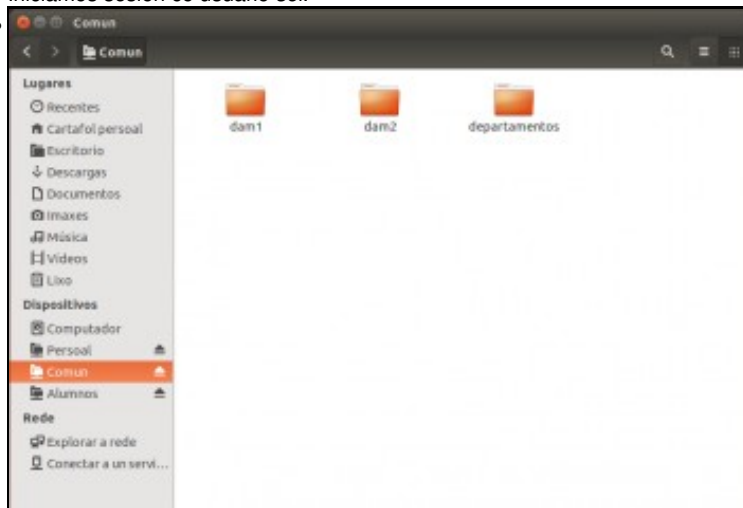
- Nos clientes Linux facemos uso de *pam-mount* para incluír o acceso en función do grupo ás carpetas que queiramos.
- Engadimos no ficheiro */etc/security/pam_mount.conf.xml* as liñas marcadas (antes do peche da etiqueta *</pam_mount>*):

```
...
<volume sgrp="g-usuarios" fstype="cifs" server="dserver00.iescalquera.local" path="comun" mountpoint="/media/(USER)/Comun" options="...
<volume sgrp="g-profes" fstype="cifs" server="dserver00.iescalquera.local" path="usuarios/persoais/alumnos" mountpoint="/media/(USER)...
</pam_mount>
```

- Vexamos o efecto iniciando sesión co usuario *sol*:
- Conexión a carpetas comúns dende Linux



Iniciamos sesión co usuario *sol*.



No explorador de ficheiros agora vemos debaixo de *Persoal* o acceso a *comun* e ás carpetas dos alumnos.



SCRIPT DE INICIO DE SESIÓN

Tamén poderíamos configurar un script de inicio de sesión (*inicio.sh*) para clientes Linux en netlogon conectando con *pam_mount* a carpeta *netlogon* e seguindo os mesmos pasos que se explican na [parte V](#).

Os pasos serían os mesmos, por iso agora omitímolo para non complicar a configuración.

Perfís móbiles

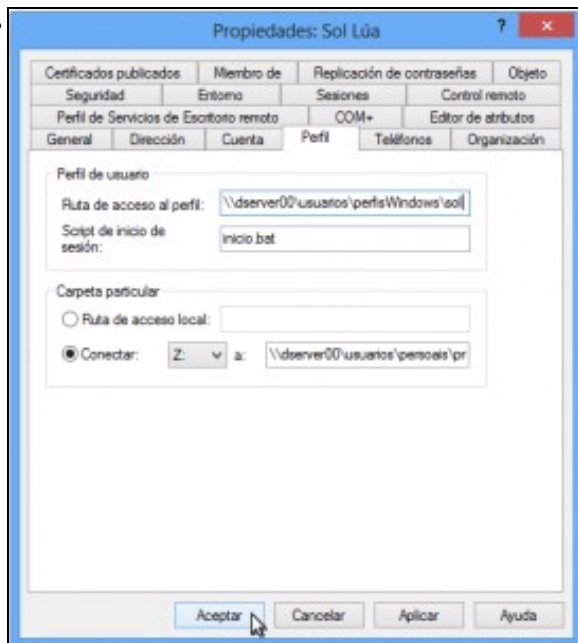
- Para rematar, imos ver como configurar perfís móbiles, tanto para clientes Windows como Linux.

Configuración para os clientes Windows

- Faremos a configuración con RSAT e comprobaremos no cliente, e explicaremos como configuralo utilizando *samba-tool*.

Con RSAT

- Perfís móbiles en Windows



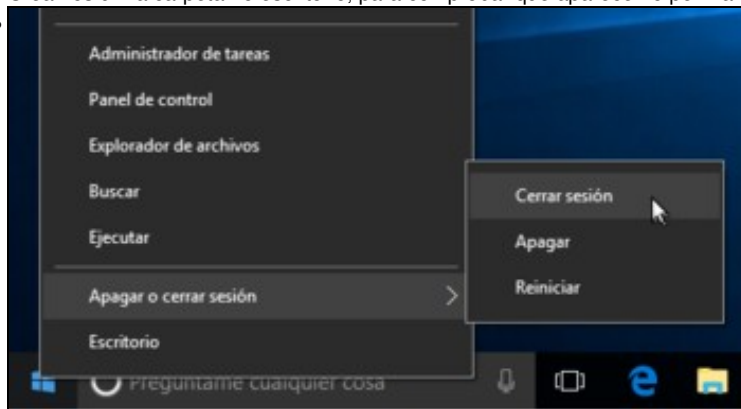
Nas propiedades de *sol*, dentro da pestana **Perfil** introducimos como **Ruta de acceso al perfil** a ruta ao perfil do usuario: `\\dserv00\usuarios\perfis\Windows\sol`. Aceptamos



Iniciamos sesión co usuario *sol*.



Creamos unha carpeta no escritorio, para comprobar que aparece no perfil almacenado no servidor.



Pechamos a sesión de *sol* no cliente, para que sincronice o perfil móbil co servidor.

- Comprobamos en *dserver00* que se creou carpeta do perfil de *sol* e a súa ACL. Podemos ver que o resto de usuarios non teñen permiso de acceso:

```
root@dserver00:~# ls -lh /srv/samba/usuarios/perfisWindows/
total 8,0K
drwxrwx---+ 14 sol g-usuarios 4,0K Feb  2 03:06 sol.V6
root@dserver00:~# getfacl /srv/samba/usuarios/perfisWindows/sol.V6/
getfacl: Eliminando '/' iniciais en nomes de ruta absolutos
# file: srv/samba/usuarios/perfisWindows/sol.V6/
# owner: sol
# group: g-usuarios
user::rwx
user:sol:rwx
user:3000001:rwx
group:---
group:g-usuarios:---
group:3000001:rwx
mask::rwx
other:---
default:user::rwx
default:user:sol:rwx
default:user:3000001:rwx
default:group:---
default:group:g-usuarios:---
default:group:3000001:rwx
default:mask::rwx
default:other:---
```

- Comprobamos que dentro da carpeta *Desktop* do perfil de *sol* está a carpeta creada dende o cliente:

```
root@dserver00:~# ls /srv/samba/usuarios/perfisWindows/sol.V6/Desktop/  
carpeta no escritorio de sol  desktop.ini
```

Con samba-tool

- Se usamos *samba-tool* para a creación dos usuarios, podemos establecer o script de inicio de sesión para o usuario co parámetro:
 - ♦ **--profile-path=ruta_do_perfil** (introducindo o carácter de escape (\) antes de cada \, de forma que haberá que duplicar cada \. Por exemplo, a ruta da carpeta persoal de *sol* introduciríamola como: `\\\\dserver00\\usuarios\\perfisWindows\\sol`).

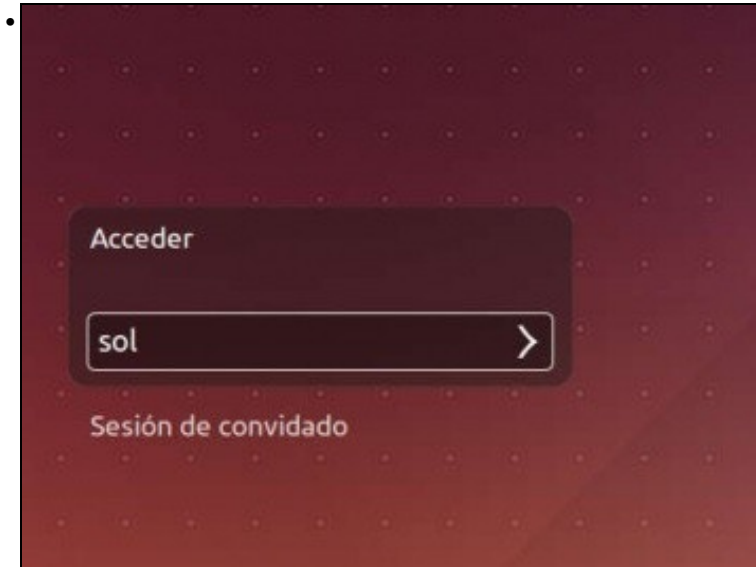
Configuración para os clientes Linux

- Nos clientes Linux o perfil almacénase na carpeta *home* do usuario, así que para dispoñer de perfís móbiles o que faremos é montar esta carpeta nunha carpeta compartida no servidor, facendo uso de *pam-mount*.
- Engadimos unha nova liña en **/etc/security/pam_mount.conf.xml** (antes do peche da etiqueta `</pam_mount>`):

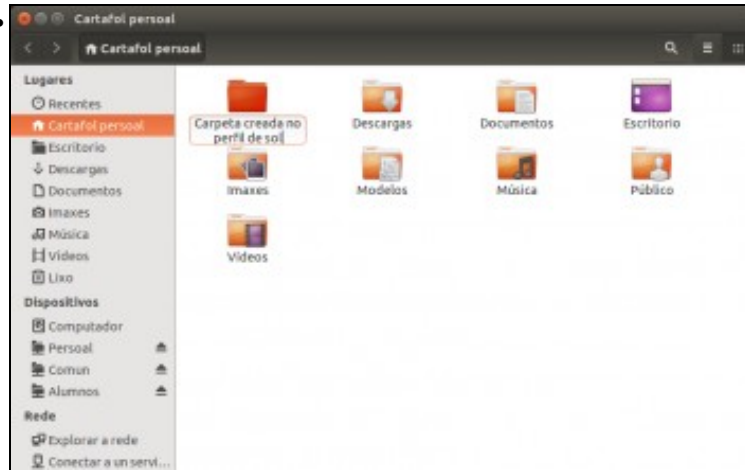
```
...  
<volume sgrp="g-usuarios" fstype="cifs" server="dserver00.iescalquera.local" path="usuarios/perfisLinux" mountpoint="/home/local/IESCALQUERA" />  
</pam_mount>
```

- Desta forma montamos sobre a carpeta */home/local/IESCALQUERA* (que é onde *PBISOpen* crea as carpetas dos usuarios) a carpeta dos perfís dos usuarios para Linux.
- Tendo en conta que *PBISOpen* crea automaticamente a carpeta persoal do usuario se non existe, o funcionamento será similar ao dos perfís de Windows, xa que o perfil de usuario crearse a primeira vez que inicie sesión nalgún cliente Linux do dominio. Tamén habería a opción de utilizar un script para dar de alta aos usuarios que crease automaticamente a carpeta do perfil do usuario na súa creación, escoller unha opción ou outra dependería sobre todo dos procedementos definidos para o mantemento dos usuarios no dominio.

- Perfís móbiles en Linux



Iniciamos sesión en *uclient01* co usuario *sol*.



Creamos unha carpeta no *Cartafol persoal* (non confundir con *Persoal*)

- Comprobamos en *dserver00* a carpeta creada do perfil de *sol* e os seus permisos, e que aparece creada a carpeta dende o cliente:

```
root@dserver00:~# getfacl /srv/samba/usuarios/perfisLinux/sol
getfacl: Eliminando '/' iniciais en nomes de ruta absolutos
# file: /srv/samba/usuarios/perfisLinux/sol
# owner: sol
# group: g-usuarios
user::rwx
user:sol:rwx
group:---
group:g-usuarios:r-x
mask::rwx
other:---
default:user::rwx
default:user:sol:rwx
default:group::r-x
default:group:g-usuarios:r-x
default:mask::rwx
default:other::r-x

root@dserver00:~# ls /srv/samba/usuarios/perfisLinux/sol/
Carpeta creada no perfil de sol  Documentos  Imaxes      Música      Vídeos
Descargas                       Escritorio  Modelos     Público
```



OUTRAS REFERENCIAS NA WEB

Nos seguintes enlaces podes atopar explicacións sobre a configuración de carpetas persoais compartidas e perfís móbiles con Samba4:

- https://wiki.samba.org/index.php/Samba_%26_Windows_Profiles
- https://wiki.samba.org/index.php/User_Home_Folders

-- Antonio de Andrés Lema e Carlos Carrión Álvarez