

# Xestión de usuarios e grupos en Samba4

Neste apartado veremos dúas formas de xestionar os usuarios e grupos en Samba4: utilizando as Ferramentas de Administración Remota do Servidor (RSAT) de Microsoft instaladas nun cliente Windows integrado no dominio, ou coa ferramenta *samba-tool*.

## Sumario

- 1 Esquema dos usuarios e grupos do dominio
- 2 Xestión dos usuarios e grupos con RSAT
  - ◆ 2.1 Instalación de RSAT
  - ◆ 2.2 Estrutura do dominio e xestión de unidades organizativas
  - ◆ 2.3 Xestión de grupos de usuarios
  - ◆ 2.4 Xestión de usuarios
  - ◆ 2.5 Creación de usuarios a partir dun modelo
- 3 Xestión dos usuarios e grupos con *samba-tool*
  - ◆ 3.1 Características de *samba-tool*
  - ◆ 3.2 Xestión de grupos de usuarios
  - ◆ 3.3 Xestión de usuarios
  - ◆ 3.4 Script para a creación masiva de usuarios
  - ◆ 3.5 Xestión da política de contrasinais

## Esquema dos usuarios e grupos do dominio

- En primeiro lugar, recordemos o esquema dos usuarios e grupos do noso dominio:

USUARIOS E GRUPOS								
								
Grupos Usuarios	Nome Completo	g-usuarios (10000)	g-profes (10001)	g-dam1-profes (10002)	g-dam2-profes (10003)	g-alum (10004)	g-dam1-alum (10005)	g-dam2-alum (10006)
Descric.		Todos 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)				✓	✓	
pla (10004)	Dam2 - Pla Glez	✓(1º)				✓		✓
paz (10005)	Dam2 - Paz Fdez	✓(1º)				✓		✓

## Xestión dos usuarios e grupos con RSAT

- Comezaremos vendo a administración dos usuarios dende un cliente Windows usando as *RSAT*. Instalaremos esta ferramenta nun equipo integrado no dominio, como *wclient01*.

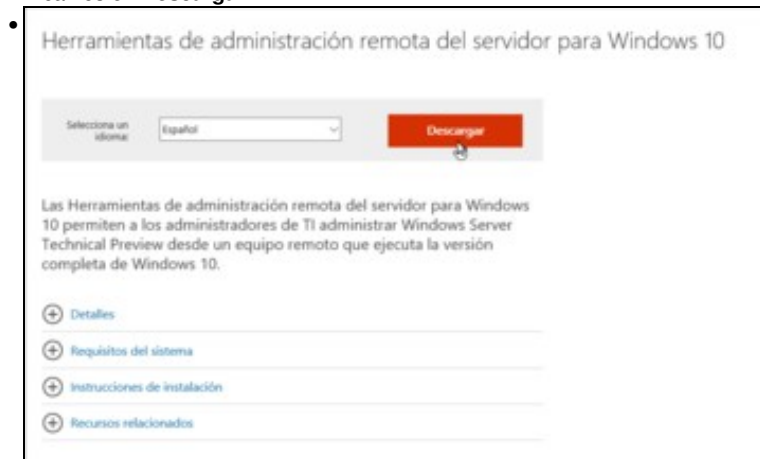
### Instalación de RSAT

- Descargamos as RSAT correspondente á versión de Windows que teñamos na máquina:
  - ◆ Para Windows 7: <https://www.microsoft.com/es-es/download/details.aspx?id=7887> (En Windows 7 pode ser necesario activar as ferramentas de AD DS despois da instalación do paquete das RSAT - <https://uftech.wordpress.com/2013/05/15/instalar-administrador-de-active-directory-en-windows-7/>)
  - ◆ Para Windows 8: <http://www.microsoft.com/es-es/download/details.aspx?id=28972>
  - ◆ Para Windows 8.1: <http://www.microsoft.com/es-es/download/details.aspx?id=39296>
  - ◆ Para Windows 10: <https://www.microsoft.com/es-ES/download/details.aspx?id=45520>
- Téñase en conta que é moi importante ter o sistema operativo actualizado antes de instalar as RSAT, xa que temos detectado sobre todo en Windows 10 que de non ter actualizado o sistema as ferramentas non funcionan correctamente.
- Móstrase a continuación os pasos da instalación en Windows 10:

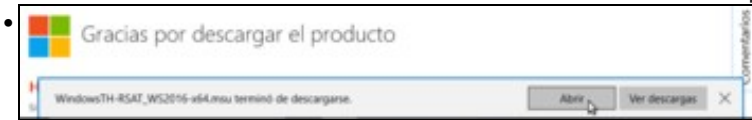
#### Instalación de RSAT



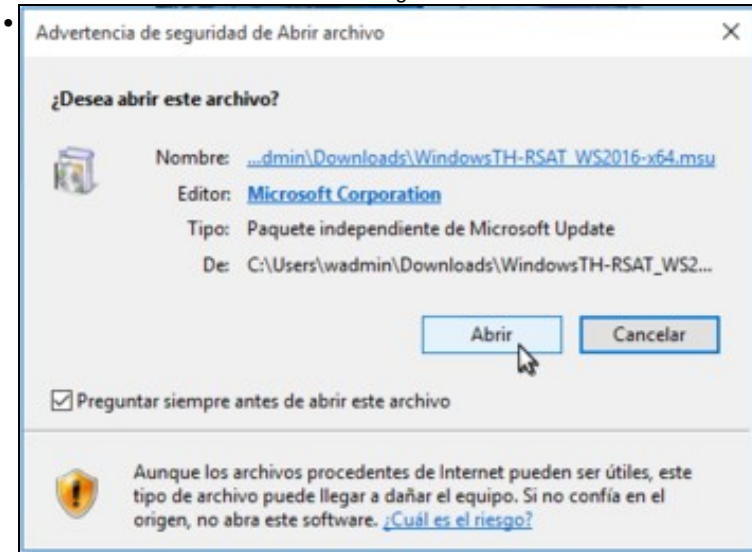
Picamos en **Descargar**.



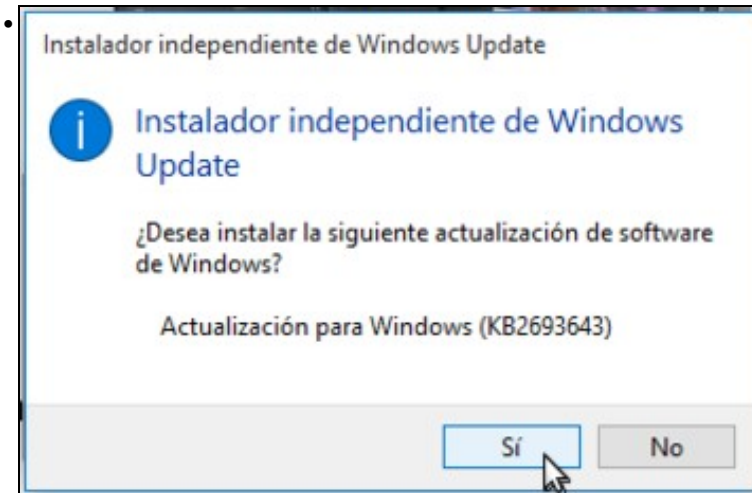
Seleccionamos a versión de 64 ou 32 bits en función da versión do sistema operativo que teñamos na máquina



Abrimos o ficheiro de instalación descargado.



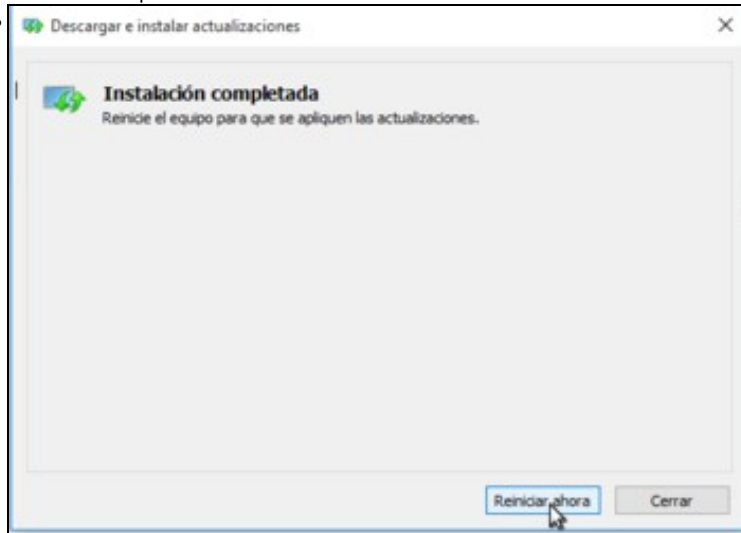
Picamos en **Abrir...**



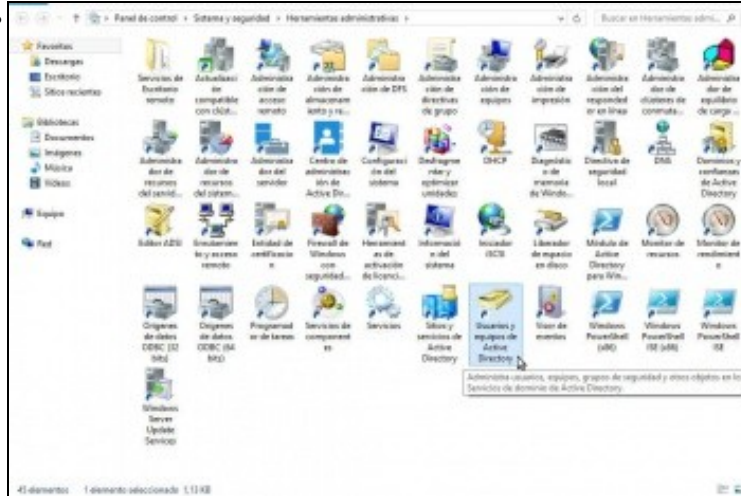
e confirmamos a instalación.



Debemos aceptar a licenza de instalación das RSAT.



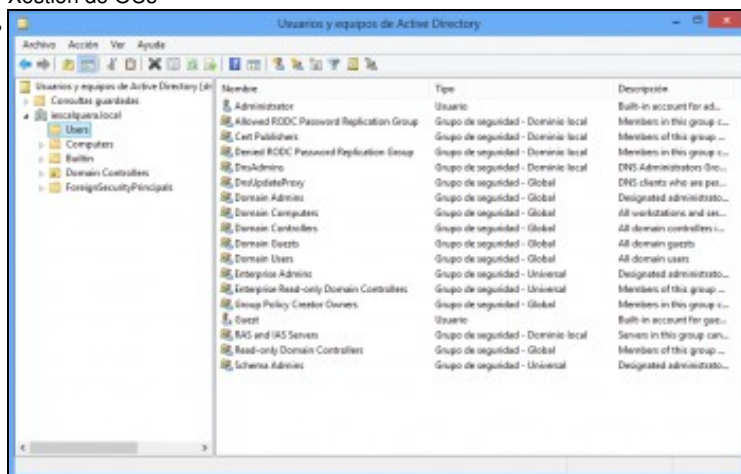
Listo!! Instalación completa. Se nos pide reiniciar, reiniciamos o equipo para aplicar os cambios. Se non simplemente pechamos.



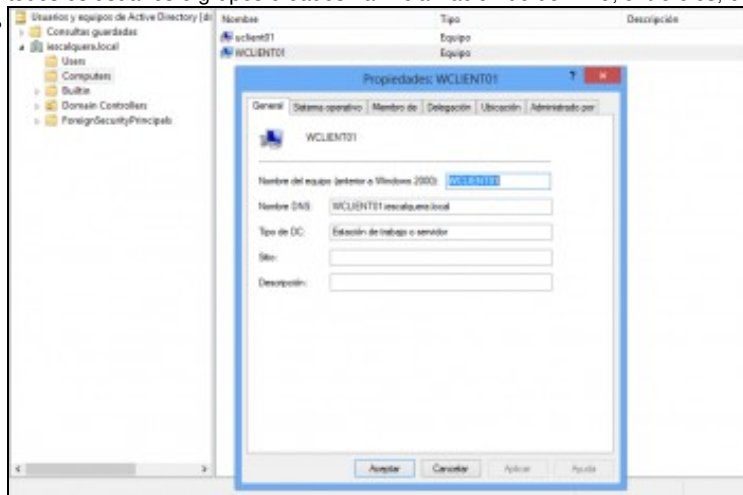
No apartado de **Sistema e Seguridade** do **Panel de control**, atoparemos as ferramentas dentro de **Ferramentas administrativas**. Por exemplo, fixarse en que aparece a ferramenta de *Usuarios e equipos de Active Directory*.

## Estrutura do dominio e xestión de unidades organizativas

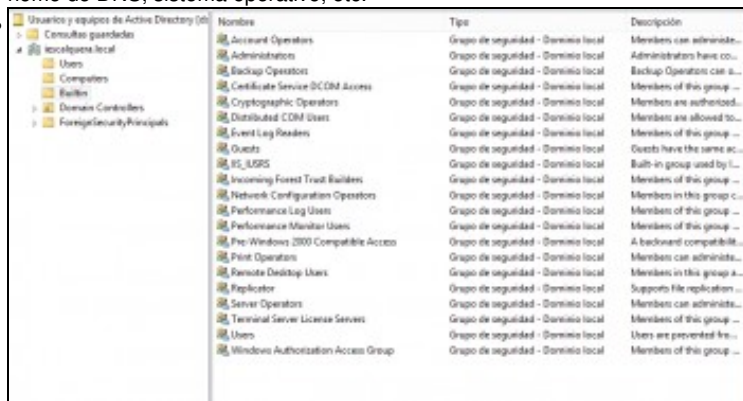
- Comezaremos vendo a estrutura do LDAP que almacena os usuarios e grupos do dominio, e como definir as unidades organizativas que queiramos para organizalos.
- Para poder xestionar os usuarios e grupos do dominio con RSAT, iniciaremos sesión en *wclient01* co usuario *Administrator*, xa que é polo momento o único que temos cos privilexios suficientes para administrar o dominio (é dicir, membro do grupo *Domain Admins*).
- Xestión de OUs



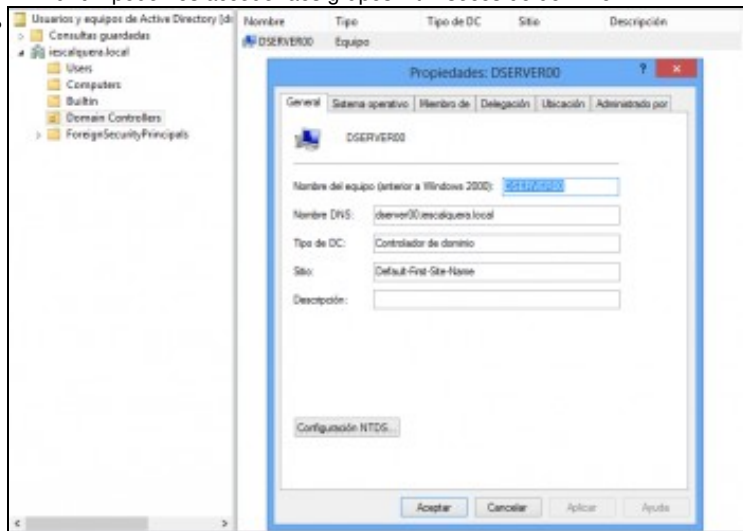
Iniciamos a ferramenta de **Usuarios e equipos de Active Directory**. Dentro do noso dominio, picamos na carpeta **Users**, e podemos ver todos os usuarios e grupos creados na inicialización do dominio; entre eles, o usuario *Administrator*.



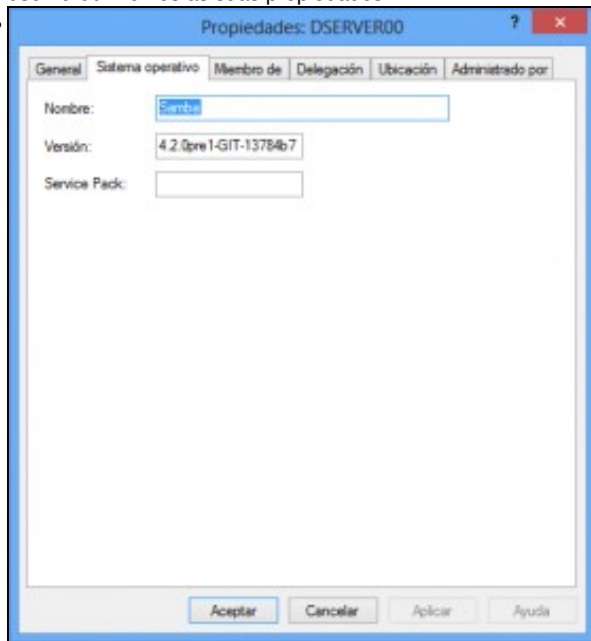
Na carpeta **Computers** podemos ver os equipos que foron integrados dentro do dominio. Nas propiedades dun equipo podemos ver o seu nome de DNS, sistema operativo, etc.



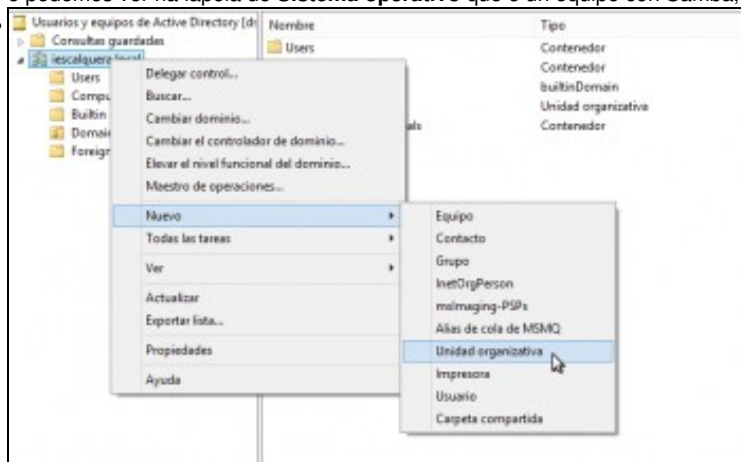
En **Builtin** podemos acceder aos grupos intrínsecos do dominio.



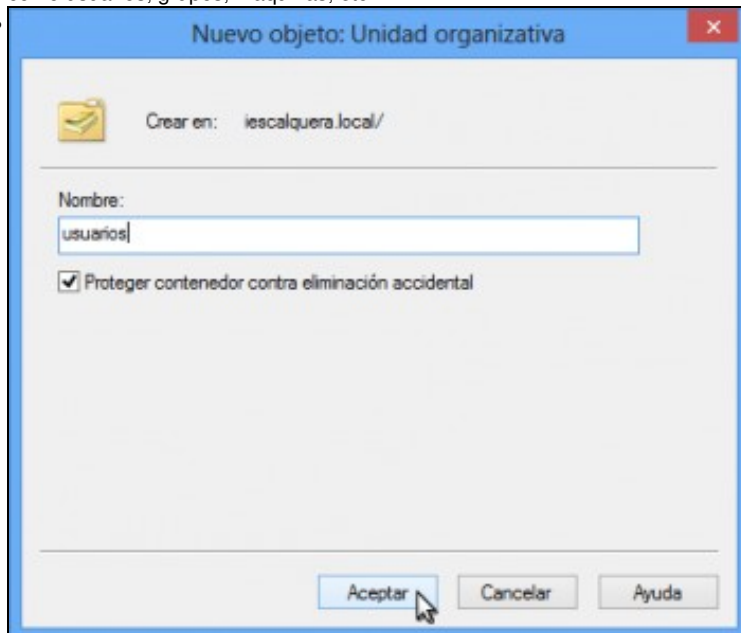
E no apartado de **Domain Controllers** veremos todos os controladores de dominio que haxa no dominio. No noso caso só temos un, que é *dserver00*. Vemos as súas propiedades...



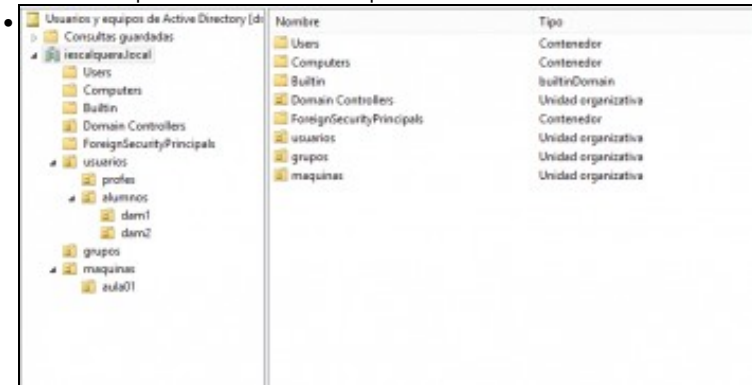
e podemos ver na lapela de **Sistema operativo** que é un equipo con Samba, así como a versión de samba que está executando.



Imos agora a crear unha Unidade Organizativa (OU), que simplemente é un contedor dentro da árbore LDAP na que almacenar obxectos como usuarios, grupos, máquinas, etc.



Poñémoslle por nome **usuarios**. Aceptamos.

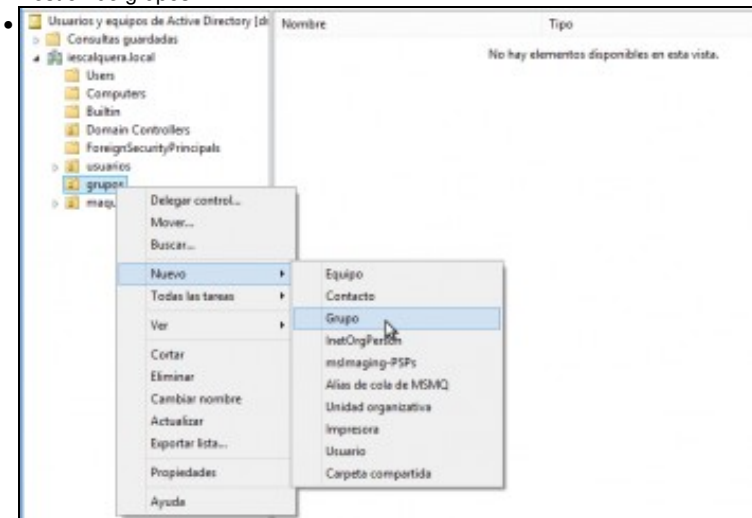


Vista de toda a estrutura de unidades organizativas, creadas para organizar o noso dominio da mesma forma que se creou a OU *usuarios*.

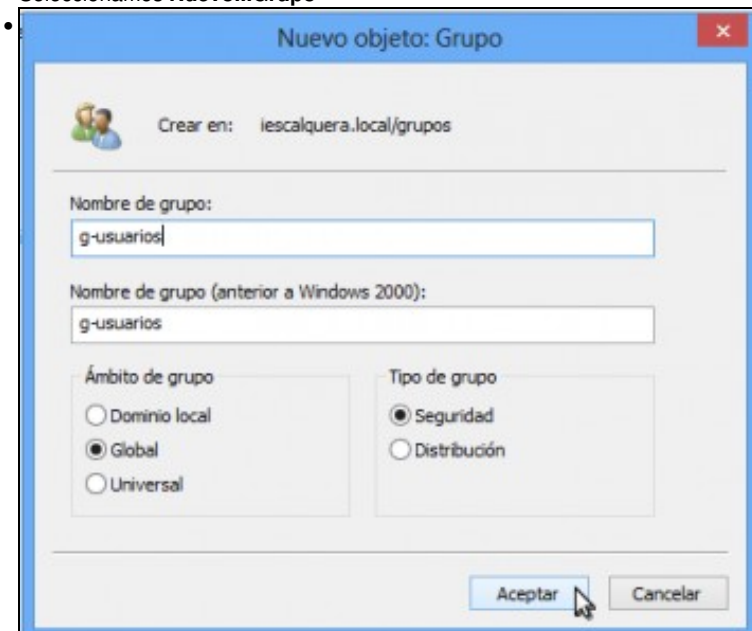
## Xestión de grupos de usuarios

- Imos ver como administrar grupos de usuarios coa ferramenta de **Usuarios e equipos de Active Directory**

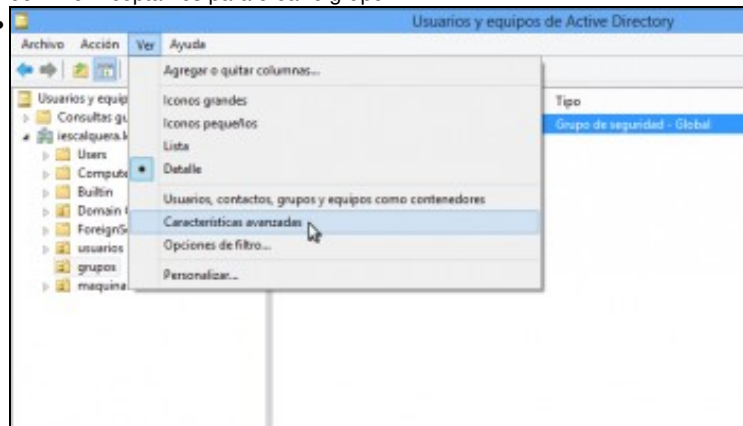
### Xestión de grupos



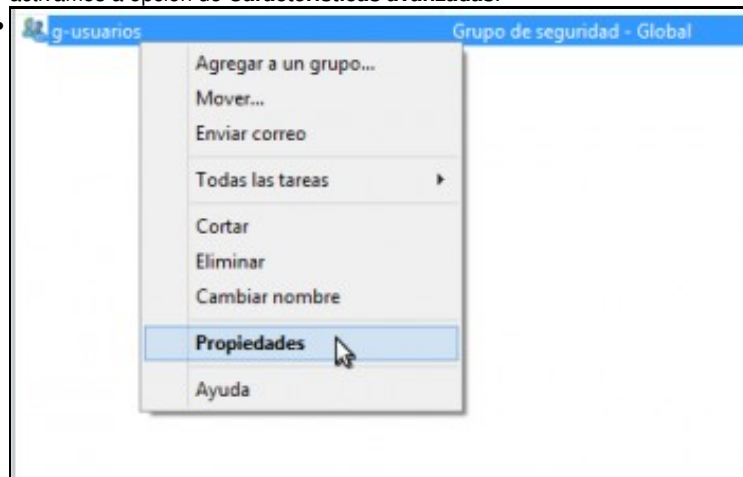
Picamos co botón dereito sobre a unidade organizativa *grupos*, que é a que imos utilizar para almacenar os grupos do noso dominio. Seleccionamos **Nuevo...Grupo**



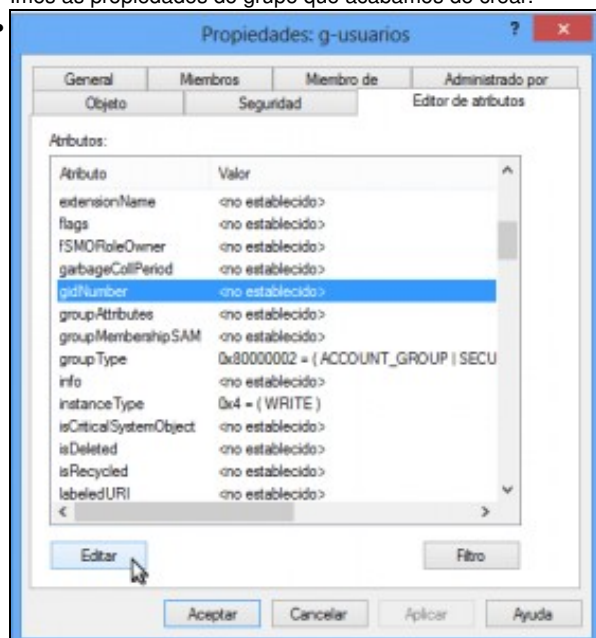
Introducimos o nome do grupo, neste caso *g-usuarios*. Será un grupo global de seguridade, xa que o utilizaremos para poñer permisos no dominio. Aceptamos para crear o grupo.



Desta forma o grupo xa está creado e podemos utilizalo para os usuarios do dominio. Pero non lle temos asignado o seu identificador de grupo POSIX (se revisamos o esquema de usuarios o grupo debería ter o *gid* 10000). Isto pode ter relevancia dependendo do sistema que usemos nos equipos cliente para obter os usuarios e grupos do dominio. Paquetes como LikewiseOpen ou PBISOpen que nós utilizamos non van facer caso deste identificador porque se inventarán eles o seu propio identificador para o usuario e grupo, usando unha función hash, pero outros paquetes como *nslcd* que usaremos no servidor non o farán, e só terán en conta os usuarios e grupo do dominio que teñan establecido un identificador POSIX. Imos ver como podemos asignarlle ao grupo o identificador POSIX que lle "toca": No menú **Ver**, activamos a opción de **Características avanzadas**.

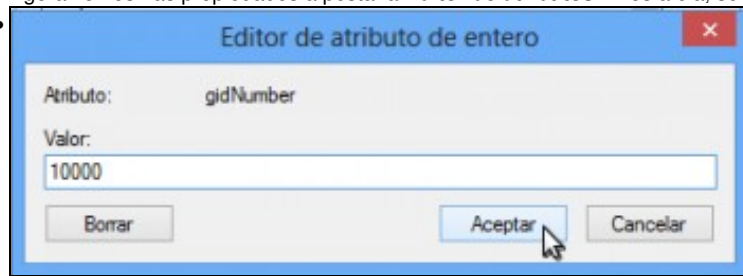


Imos as propiedades do grupo que acabamos de crear.

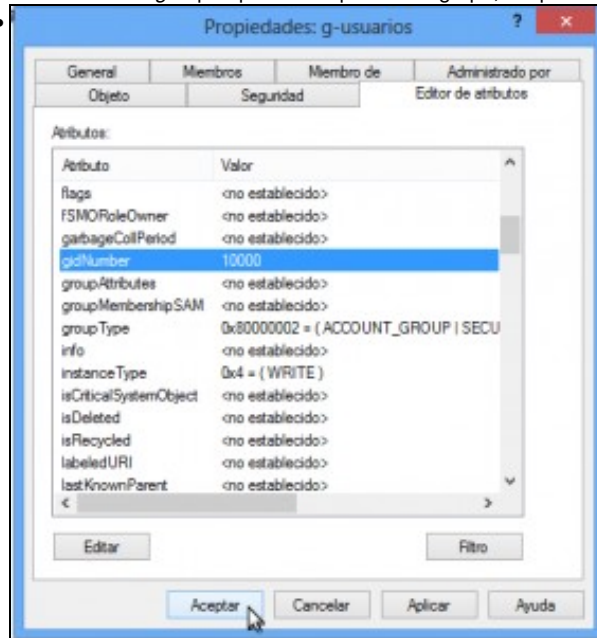




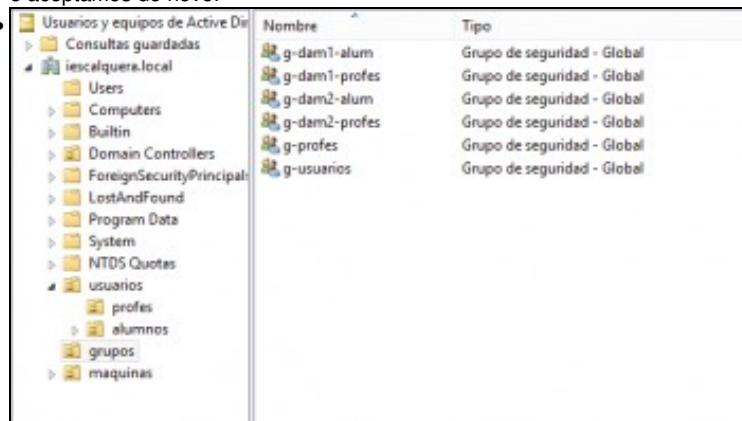
Agora vemos nas propiedades a pestana **Editor de atributos**. Imos a ela, seleccionamos o atributo **gidNumber** e picamos en **Editar**.



Introducimos o *gid* que queremos que teña o grupo, aceptamos...



e aceptamos de novo.

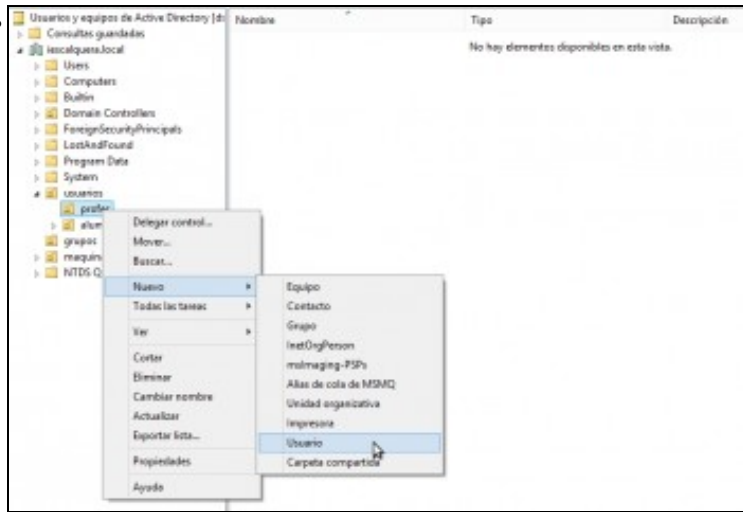


Na imaxe móstranse case todos os grupos do dominio xa creados tal e como se fixo con *g-usuarios*. Só deixamos intencionadamente sen crear o grupo *g-alum*, que crearemos utilizando a ferramenta *samba-tool*

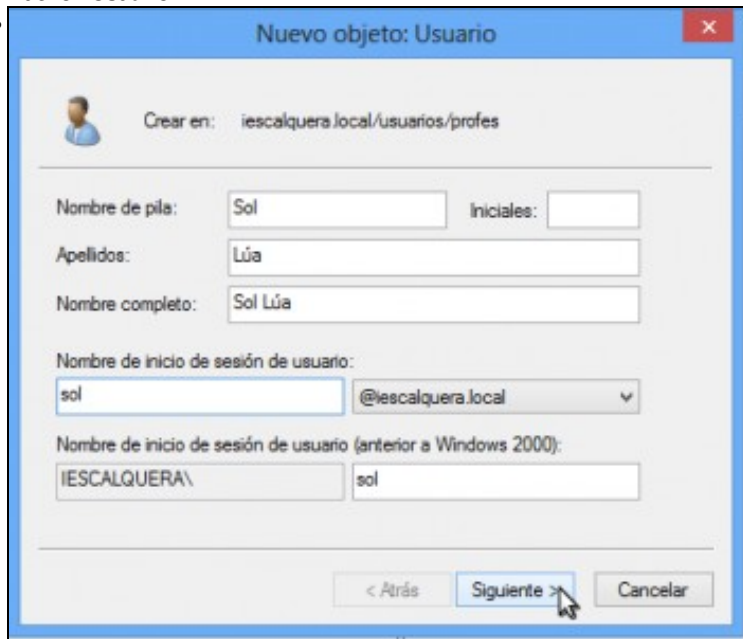
## Xestión de usuarios

Imos cos usuarios; vexamos como crear un usuario dentro dunha unidade organizativa concreta e introduciolo nos grupos que queiramos:

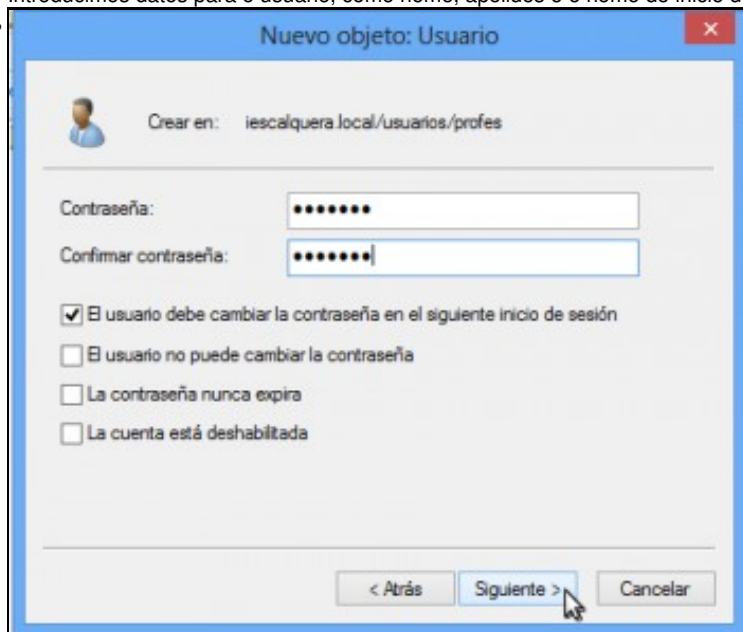
- Xestión de usuarios



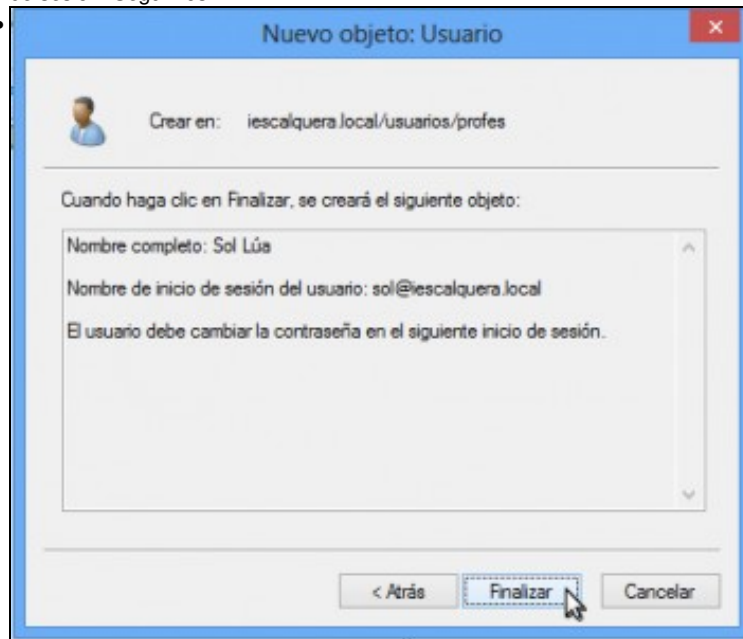
Crearemos o usuario *sol*, dentro da OU *profes* que está dentro da OU *usuarios*. Picamos co botón dereito sobre a OU e seleccionamos **Nuevo...Usuario**



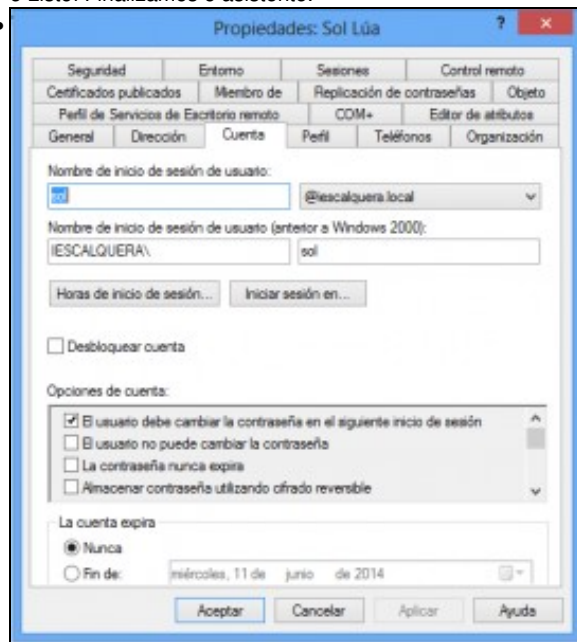
Introducimos datos para o usuario, como nome, apellidos e o nome de inicio de sesión. Seguimos



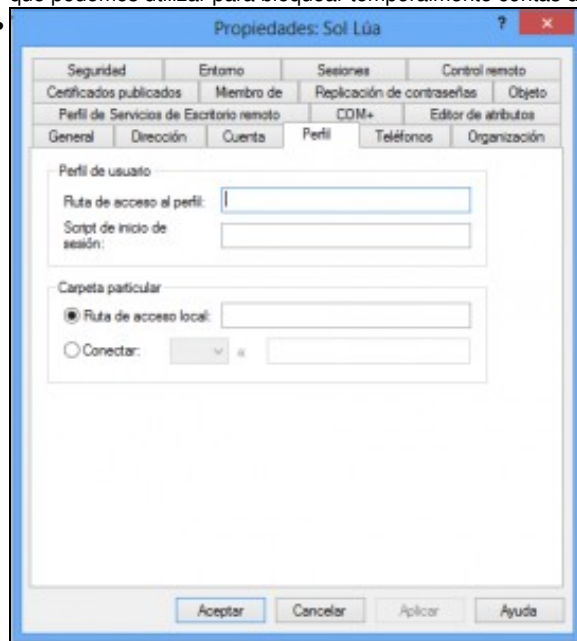
Establecemos un contrasinal para o usuario (por que non, *abc123*), e deixamos activada a opción de que o usuario cambie no seguinte inicio de sesión. Seguimos...



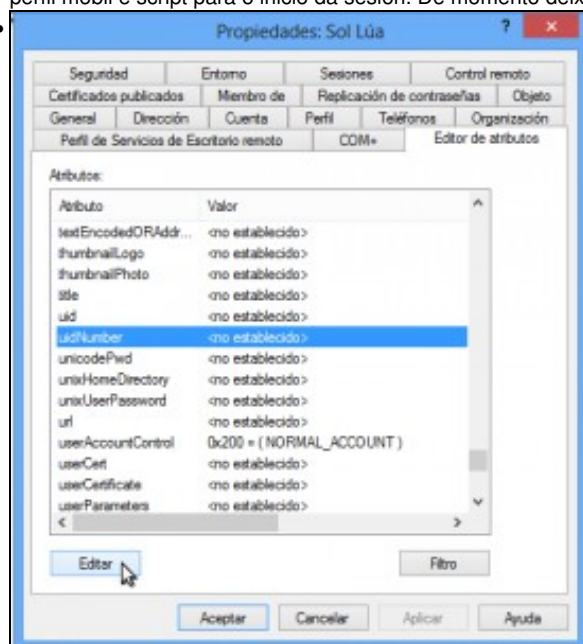
e Listo! Finalizamos o asistente.



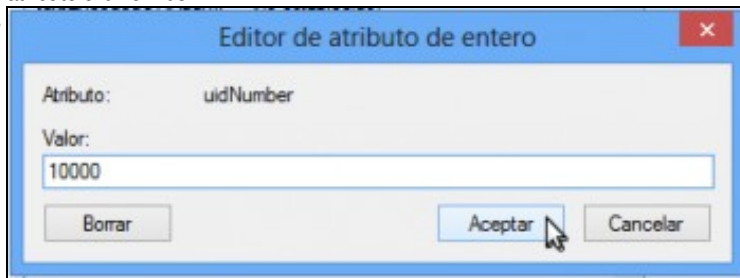
Vemos o usuario creado, e nas propiedades podemos ver, por exemplo na lapela **Cuenta** as opcións de inicio sesión que acabamos de introducir. Na lista de opcións que atopamos dentro de *Opciones de cuenta*, atoparemos a opción de establecer a conta como *deshabilitada* que podemos utilizar para bloquear temporalmente contas de usuarios.



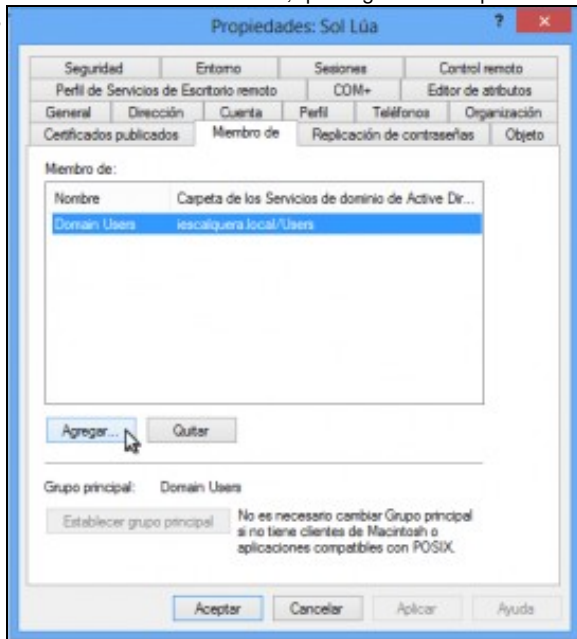
Otra lapela importante nas propiedades do usuario é a de **Perfil**, xa que aquí é onde podemos configurar a carpeta persoal do usuario, o perfil móbil e script para o inicio da sesión. De momento deixámolo así, máis adiante veremos como configurar todo isto.



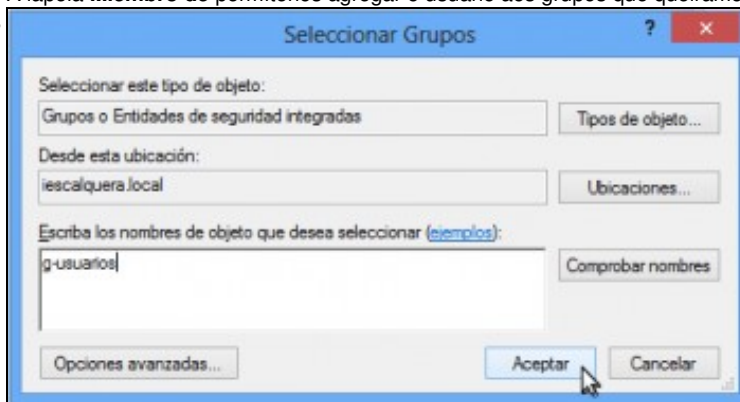
E da mesma forma que fixemos para o grupo, se nos interesa que o usuario teña un *uid* concreto nos clientes Linux do donio, editaremos o atributo **uidNumber**



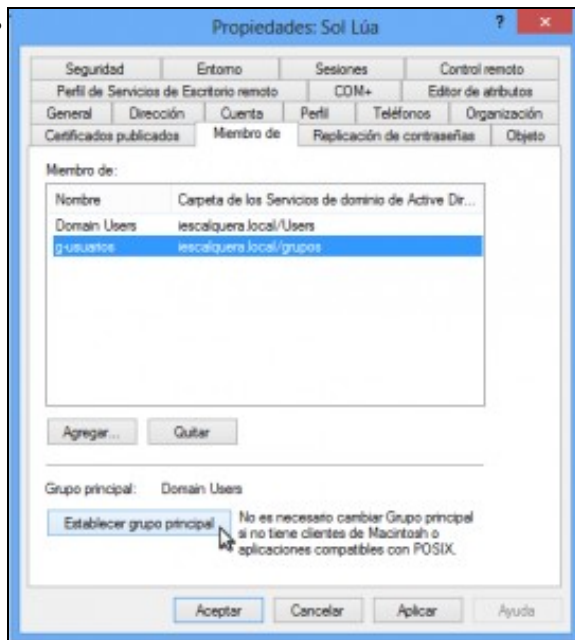
Introducimos o *uid* do usuario, que seguindo o esquema de usuarios sería 10000. Aceptamos



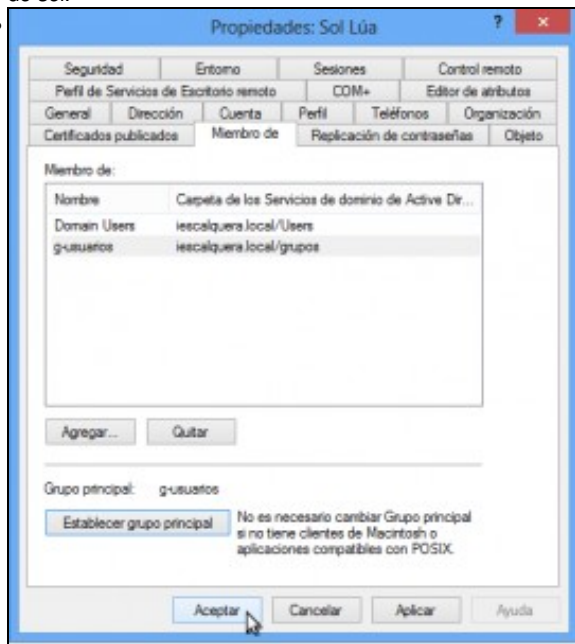
A lapela **Miembro de** permítenos agregar o usuario aos grupos que queiramos. Iremos agregar a *sol* a *g-usuarios*, picando en **Agregar**.



Introducimos o nome do grupo e picamos en **Aceptar**.



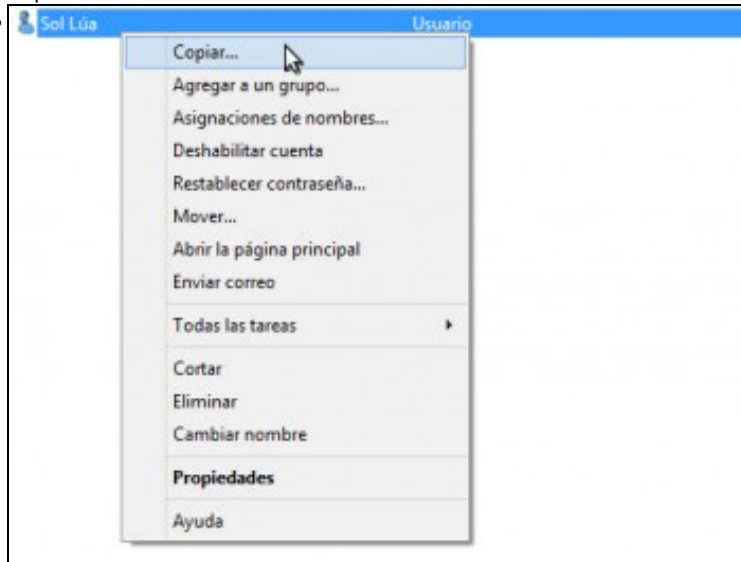
Xa podemos ver o grupo entre a listaxe de grupos do que *sol* é membro. Tamén será interesante para os clientes Linux do dominio establecer da listaxe de grupos o grupo principal do usuario. Seguindo o noso esquema de usuarios, *g-usuarios* debería ser o grupo principal de *sol*.



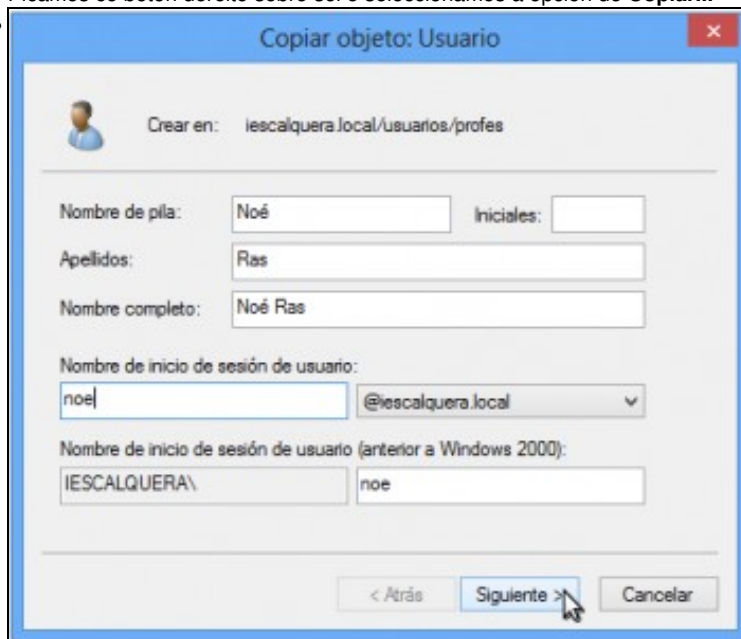
Aceptamos os cambios realizados.

## Creación de usuarios a partir dun modelo

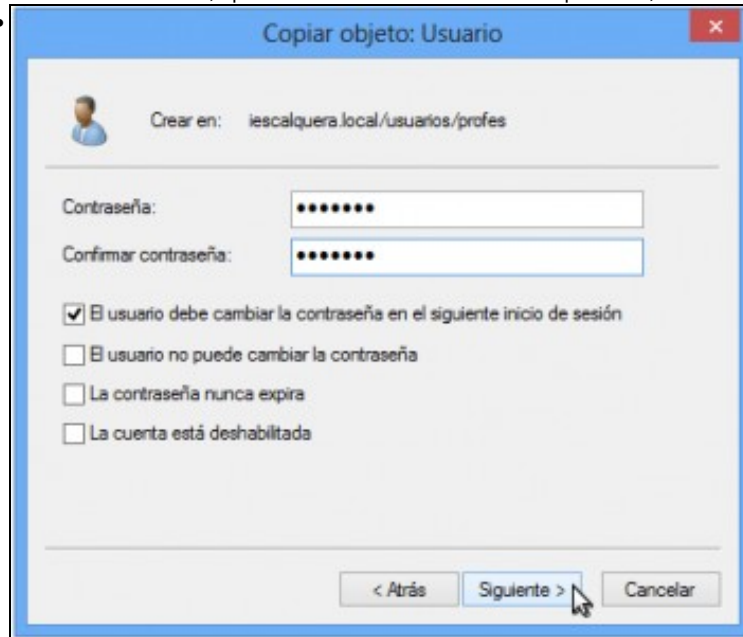
- En moitas ocasións, interésanos crear de usuarios a partir dun usuario de modelo para o que xa temos establecido unha configuración determinada de grupos, perfil, etc.
- Con RSAT podemos copiar un usuario e así pasaremos toda a configuración do usuario copiado ao novo usuario. A configuración de perfil, feita habitualmente en función do nome do usuario, será modificada co nome que lle poñamos ao novo usuario.
- Copiar usuarios con RSAT



*noe* é un usuario que comparte moitas características con *sol*, xa que as dúas son profes. Así que imos copiar o usuario *sol* para crear a *noe*. Picamos co botón dereito sobre *sol* e seleccionamos a opción de **Copiar...**

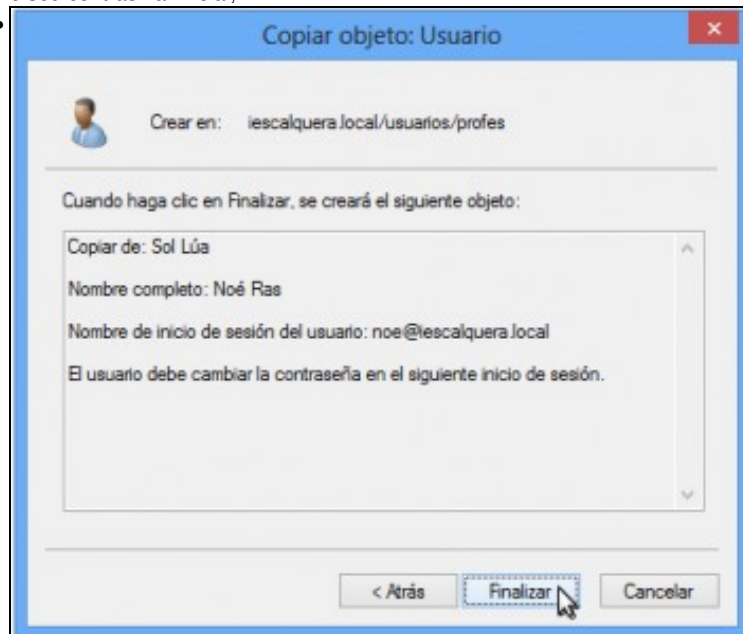


Introducimos o nome, apellidos e nome de inicio de sesión para *noe*,



The screenshot shows a dialog box titled "Copiar objeto: Usuario" with a close button in the top right corner. Below the title bar, there is a user icon and the text "Crear en: iescalquera.local/usuarios/profes". The main area contains two password input fields: "Contraseña:" and "Confirmar contraseña:", both filled with black dots. Below these fields are four checkboxes with the following labels: "El usuario debe cambiar la contraseña en el siguiente inicio de sesión" (checked), "El usuario no puede cambiar la contraseña", "La contraseña nunca expira", and "La cuenta está deshabilitada". At the bottom, there are three buttons: "< Atrás", "Sigüente >" (highlighted with a mouse cursor), and "Cancelar".

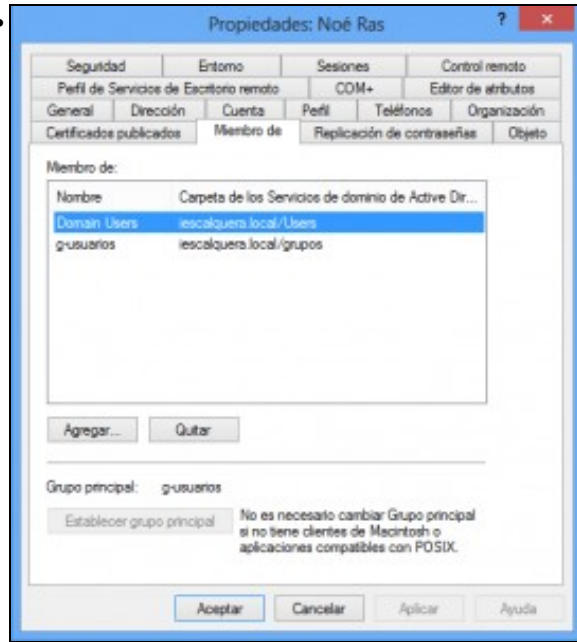
o seu contrasinal inicial,



The screenshot shows the same dialog box, but now it displays the details of the user to be created. The text "Cuando haga clic en Finalizar, se creará el siguiente objeto:" is followed by a scrollable area containing: "Copiar de: Sol Lúa", "Nombre completo: Noé Ras", "Nombre de inicio de sesión del usuario: noe@iescalquera.local", and "El usuario debe cambiar la contraseña en el siguiente inicio de sesión.". At the bottom, the buttons are "< Atrás", "Finalizar" (highlighted with a mouse cursor), and "Cancelar".



e finalizamos o asistente.



Podemos ver nas propiedades de *noe* que xa é membro de *g-usuarios*, como o é *sol*.

## Xestión dos usuarios e grupos con samba-tool

- Ata o de agora, utilizamos o comando *samba-tool* para inicializar a estrutura do dominio, utilizando os parámetros *domain provision*. Pero son moitísimas as opcións que admite este comando, e ímonos centrar neste apartado nas que podemos utilizar para administrar os usuarios e grupos.

### Características de samba-tool

- Tendo en conta o gran número de parámetros que podemos utilizar con *samba-tool*, é moi conveniente que saibamos utilizar a axuda que o propio comando inclúe para saber cales temos que introducir en función do que queiramos facer. Introducimos o comando **samba-tool -h** para ver os subcomandos que admite:

```
root@dserver00:~# samba-tool -h
Usage: samba-tool <subcommand>

Main samba administration tool.

Options:
  -h, --help          show this help message and exit

Version Options:
  -V, --version       Display version number

Available subcommands:
  dbcheck             - Check local AD database for errors.
  delegation          - Delegation management.
  dns                 - Domain Name Service (DNS) management.
  domain              - Domain management.
  drs                 - Directory Replication Services (DRS) management.
  dsacl               - DS ACLs manipulation.
  fsmo                - Flexible Single Master Operations (FSMO) roles management.
  gpo                 - Group Policy Object (GPO) management.
  group               - Group management.
  ldapcmp             - Compare two ldap databases.
  ntacl               - NT ACLs manipulation.
  processes           - List processes (to aid debugging on systems without setproctitle).
  rodc                - Read-Only Domain Controller (RODC) management.
  sites               - Sites management.
  spn                 - Service Principal Name (SPN) management.
  testparm            - Syntax check the configuration file.
  time                - Retrieve the time on a server.
```

```
user      - User management.
vampire   - Join and synchronise a remote AD domain to the local server.
For more help on a specific subcommand, please type: samba-tool <subcommand> (-h|--help)
```

- Podemos comprobar o gran número de funcións que podemos facer, que van dende comprobar erros na base de datos do dominio ata a xestión do DNS.
- Pero moitos dos subcomandos teñen á súa vez subcomandos, que nos permiten levar a cado diversas tarefas de administración. Por exemplo, podemos ver as opcións do subcomando *dns* con **samba-tool dns -h**:

```
root@dserver00:~# samba-tool dns -h
Usage: samba-tool dns <subcommand>

Domain Name Service (DNS) management.

Options:
-h, --help show this help message and exit
```

```
Available subcommands:
add      - Add a DNS record
delete   - Delete a DNS record
query    - Query a name.
roothints - Query root hints.
serverinfo - Query for Server information.
update   - Update a DNS record
zonecreate - Create a zone.
zonedelelete - Delete a zone.
zoneinfo - Query for zone information.
zonelist - Query for zones.
For more help on a specific subcommand, please type: samba-tool dns <subcommand> (-h|--help)
```

- E así poderíamos seguir, porque de novo atopamos subcomandos dentro de *samba-tool dns*. Seguro que o lector pode deducir que teríamos que introducir se quixéramos saber como usar o subcomando *samba-tool dns add* para engadir rexistros no DNS.

## Xestión de grupos de usuarios

- Se queremos administrar os grupos de usuarios do dominio, utilizamos o comando **samba-tool group**. Vemos a continuación as opcións deste comando:

```
Available subcommands:
add          - Creates a new AD group.
addmembers  - Add members to an AD group.
delete      - Deletes an AD group.
list        - List all groups.
listmembers - List all members of an AD group.
removemembers - Remove members from an AD group.
```

- Iremos crear o grupo *g-alum* dentro da OU *grupos*:

```
root@dserver00:~# samba-tool group add g-alum --groupou=OU=grupos
Added group g-alum
```

- Podemos ver con RSAT o grupo creado (prememos a tecla *F5* para actualizar a vista de RSAT se xa o tiñamos aberto):

Nombre	Tipo
g-alum	Grupo de seguridad - Global
g-dam1-alum	Grupo de seguridad - Global
g-dam1-profes	Grupo de seguridad - Global
g-dam2-alum	Grupo de seguridad - Global
g-dam2-profes	Grupo de seguridad - Global
g-profes	Grupo de seguridad - Global
g-usuarios	Grupo de seguridad - Global

Vista desde RSAT do grupo creado con samba-tool

## Xestión de usuarios

- A xestión dos usuarios farémola con **samba-tool user**:

```

add           - Create a new user.
create        - Create a new user.
delete        - Delete a user.
disable       - Disable an user.
enable        - Enable an user.
list          - List all users.
password      - Change password for a user account (the one provided in authentication).
setexpiry     - Set the expiration of a user account.
setpassword   - Set or reset the password of a user account.

```

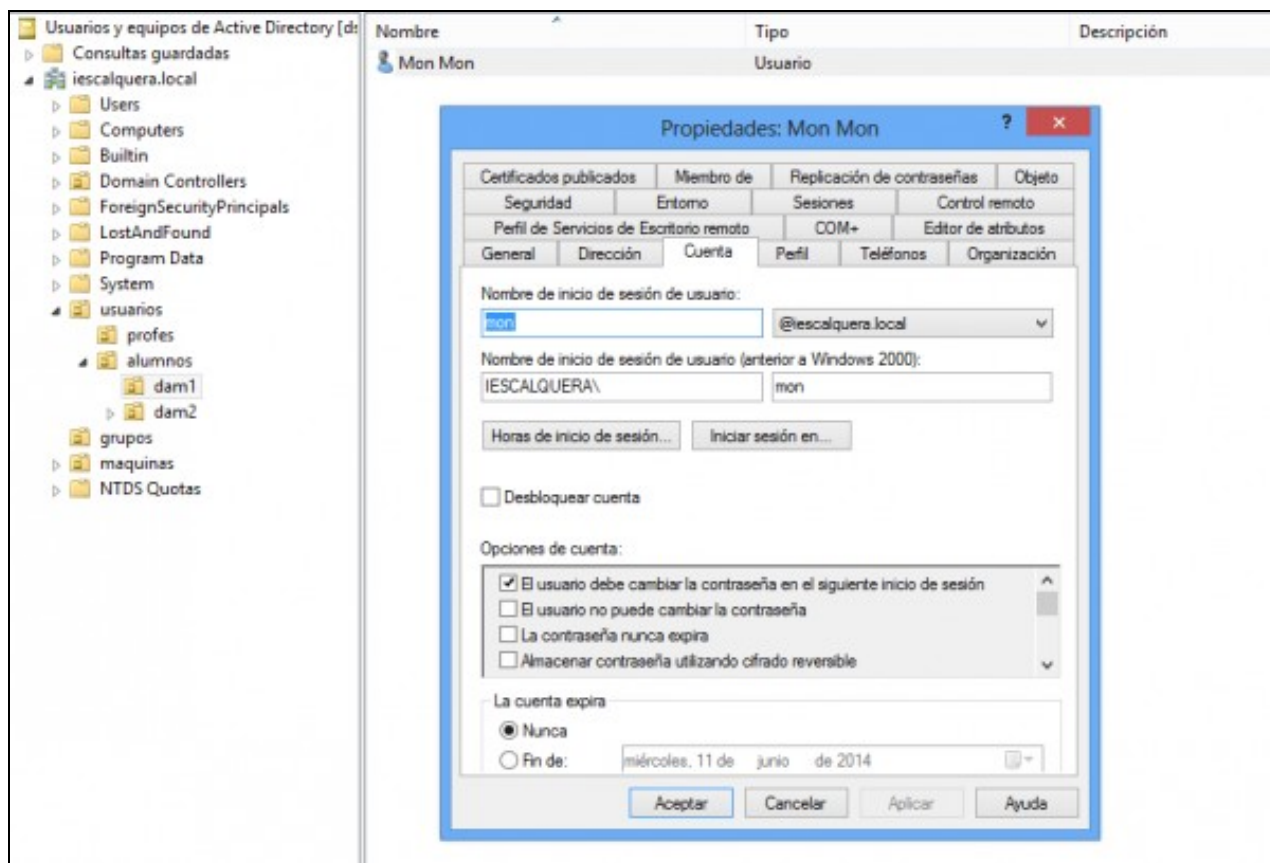
- O subcomando *create* admite moitísimos parámetros para o novo usuario que se crea (recoméndase comprobalos con *samba-tool user create -h*). O seguinte comando crea o usuario *mon*, con nome e apelidos *Mon Mon*, contrasinal inicial *abc123*. que debe cambiar no seguinte inicio de sesión, dentro da OU *dam1* (que está dentro da OU *alumnos* e que a súa vez está dentro da OU *usuarios*) e con *uid* 10002:

```

root@dserver00:~# samba-tool user create mon abc123. --given-name=Mon --surname=Mon --must-change-at-next-login --userou=OU=dam1,OU=
User 'mon' created successfully

```

- Podemos ver con RSAT o usuario creado:

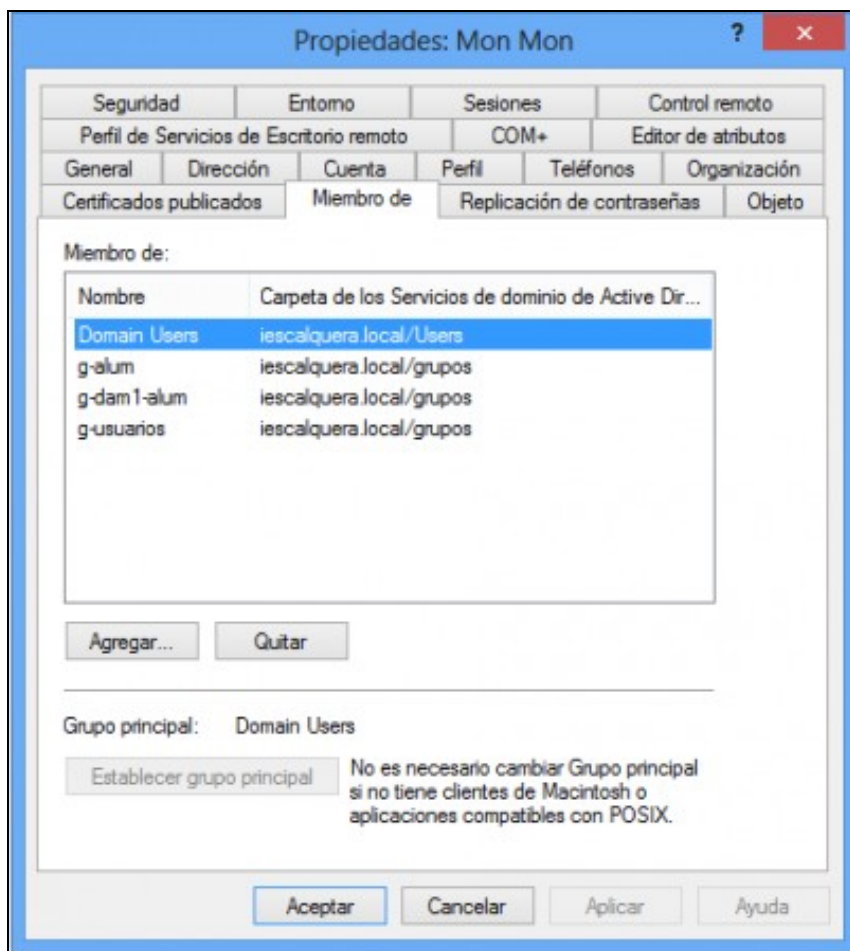


Vista desde RSAT do usuario creado con samba-tool

- Podemos xestionar os grupos dos que un usuario é membro con *samba-tool group*. Os seguinte comandos introducie a *mon* nos grupos *g-usuarios*, *g-alum* e *g-dam1-alum*:

```
root@dserver00:~# samba-tool group addmembers g-usuarios mon
Added members to group g-usuarios
root@dserver00:~# samba-tool group addmembers g-alum mon
Added members to group g-alum
root@dserver00:~# samba-tool group addmembers g-dam1-alum mon
Added members to group g-dam1-alum
root@dserver00:~#
```

- Podemos ver o efecto con RSAT:



Vista desde RSAT dos cambios nos grupos do usuario feitos con samba-tool

### Script para a creación masiva de usuarios

- Unha vantaxe de utilizar *samba-tool* para a xestión dos usuarios é que podemos facer de forma bastante simple un script que cree usuarios de forma masiva a partir dun ficheiro de texto cos datos dos usuarios.
- A continuación móstrase un exemplo de este script.
- **SCRIPT: crear\_alumnos.sh**

```
#!/bin/bash
# Script que da de alta os usuarios indicados nun ficheiro de texto

# Lemos cada liña do ficheiro que nos indiquen como parámetro
for i in `cat $1`; do
    # Extraemos os campos dos usuarios
    LOGIN=`echo $i | cut -f 1 -d :`
    NOME=`echo $i | cut -f 2 -d :`
    APELIDOS=`echo $i | cut -f 3 -d :`
    GRUPO=`echo $i | cut -f 4 -d :`
    UID=`echo $i | cut -f 5 -d :`

    # Engadimos o usuario con samba-tool e introducímolo nos grupos que lle corresponda
    echo -n "Engadindo usuario $LOGIN..."
    samba-tool user create $LOGIN abc123. --given-name=$NOME --surname=$APELIDOS --must-change-at-next-login --userou=OU=$GRUPO,
    samba-tool group addmembers g-usuarios $LOGIN
    samba-tool group addmembers g-alum $LOGIN
    samba-tool group addmembers g-$GRUPO-alum $LOGIN
    echo "[OK]"
done
```

- Creamos un ficheiro de texto cos dous alumnos de *dam2*:

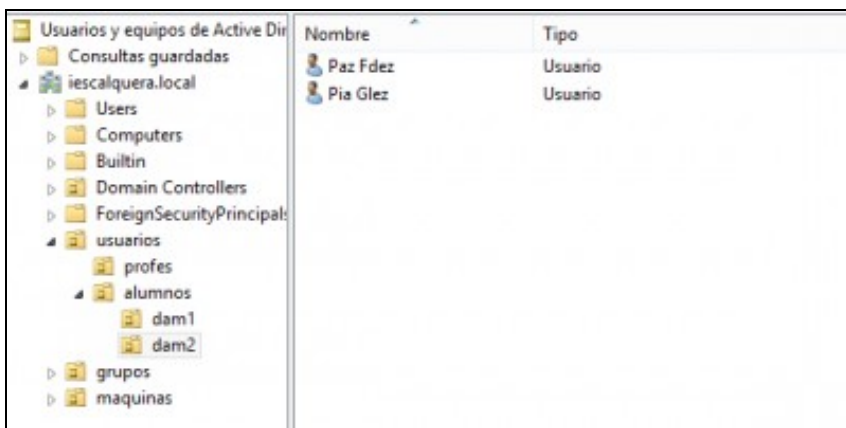
- **FICHEIRO DE USUARIOS: alumnos.txt**

```
pia:Pia:Glez:dam2:10004  
paz:Paz:Fdez:dam2:10005
```

- Executamos o script pasándolle como parámetro o nome do ficheiro cos datos dos alumnos:

```
root@dserver00:~# sh crear_alumnos.sh alumnos.txt  
Engadindo usuario pia...User 'pia' created successfully  
Added members to group g-usuarios  
Added members to group g-alum  
Added members to group g-dam2-alum  
[OK]  
Engadindo usuario paz...User 'paz' created successfully  
Added members to group g-usuarios  
Added members to group g-alum  
Added members to group g-dam2-alum  
[OK]
```

- Podemos ver o efecto da execución con RSAT (Recórdese premer *F5* para actualizar a vista de RSAT se xa estaba aberto):



Vista desde RSAT dos usuarios creados de forma masiva con samba-tool

## Xestión da política de contrasinais

- Un aspecto importante na seguridade do dominio é a política de contrasinais, que forzará a que os contrasinais dos usuarios teñan unha complexidade determinada, unha lonxitude mínima, que a cambien de forma periódica, etc.
- Samba4 xa ven por defecto con unha configuración que esixe unha lonxitude mínima e unha complexidade aos contrasinais, que podemos ver e modificar con *samba-tool domain passwordsettings*.
- O seguinte comando mostra as restricións de contrasinais que está configuradas neste momento:

```
root@dserver00:~# samba-tool domain passwordsettings show  
Password informations for domain 'DC=iescalquera,DC=local'  
  
Password complexity: on  
Store plaintext passwords: off  
Password history length: 24  
Minimum password length: 7  
Minimum password age (days): 1  
Maximum password age (days): 42  
Account lockout duration (mins): 30  
Account lockout threshold (attempts): 0  
Reset account lockout after (mins): 30
```

- Podemos ver que o contrasinal ten que ter unha lonxitude mínima de 7 caracteres. Vexamos o que pasa se intentamos crear o usuario *tom* con contrasinal *a*:

```
root@dserver00:~# samba-tool user create tom a --given-name=Tom --surname=Tom --must-change-at-next-login --userou=OU=dam1,OU=alumno  
ERROR(ldb): Failed to add user 'tom': - 0000052D: Constraint violation - check_password_restrictions: the password is too short. It
```

- O exemplo que se mostra a continuación elimina a restrición de complexidade dos contrasinais, e establece a lonxitude mínima a 1 carácter:

```
root@dserver00:~# samba-tool domain passwordsettings set --complexity=off --min-pwd-length=1
Password complexity deactivated!
Minimum password length changed!
All changes applied successfully!
```

- Podemos comprobar como agora podemos engadir o usuario *tom* co contrasinal *a*:

```
root@dserver00:~# samba-tool user create tom a --given-name=Tom --surname=Tom --must-change-at-next-login --userou=OU=dam1,OU=alumno
User 'tom' created successfully
```

-- Antonio de Andrés Lema e Carlos Carrión Álvarez