Configuración e instalación do escenario complexo 6.2

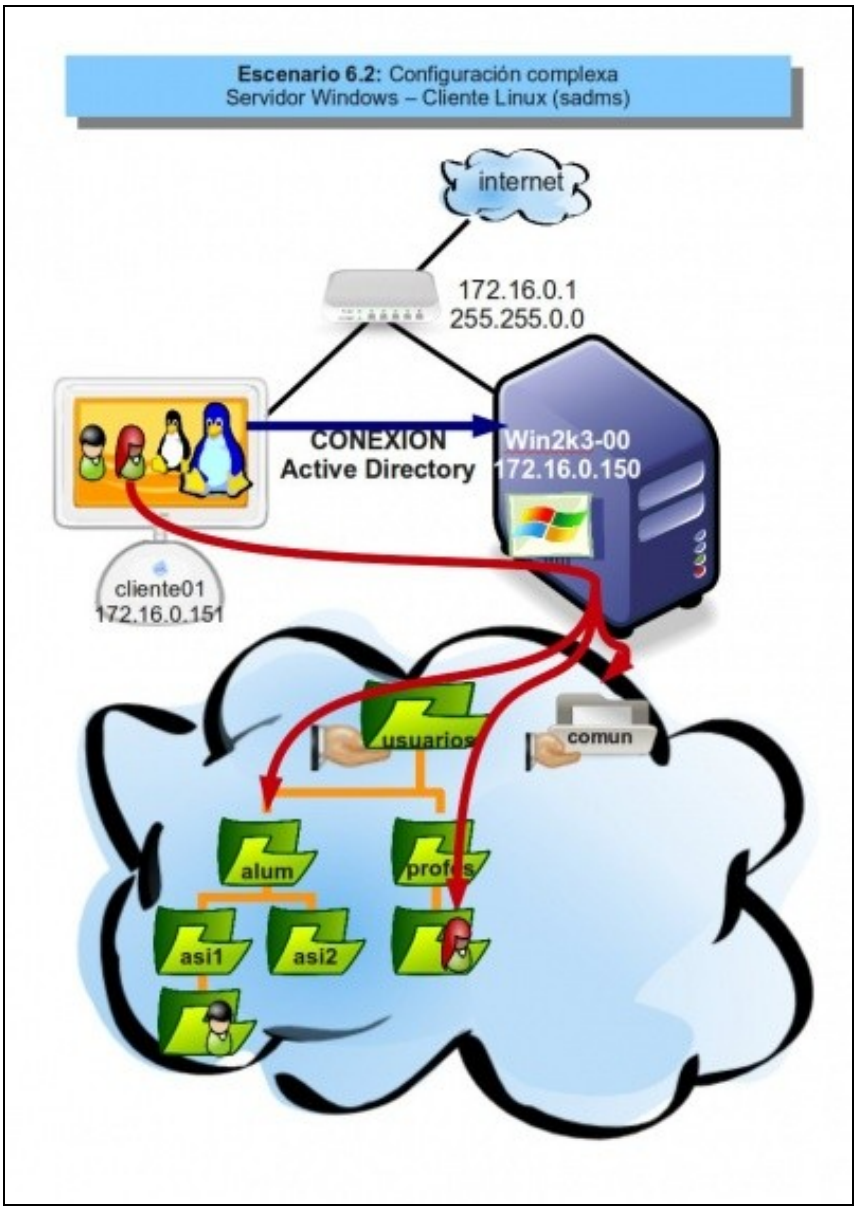
- No anterior escenario pódense observar unha serie de limitacións:
    - O cliente só se pode conectar a un só recurso compartido do servidor.
    - A codificación de caracteres pode que non sexa a correcta.
    - Que pasaría se as carpetas persoais dos usuarios do directorio activo están en distintas ubicacións e non todas xuntas nunha mesma carpeta.

- Como no escenario anterior vaise operar co Directorio Activo e crear novas carpetas no servidor **win2k3-00** . Posto que o obxectivo deste apartado é conectar un equipo Ubuntu ó dominio de Windows, non se axustarán os permisos das carpetas dos usuarios. Ademais vanse crear varios grupos, ós cales van pertencer os usuarios. O ideal sería elevar o nivel funcional do dominio, para que permitise aniñamento de grupos e así só habería que preocuparse que un usuario pertencese ó grupo máis abaixo na xeraquía de aniñamento. Todo isto recoméndase que si se faga nun sistema real, para iso seguir o punto 10 do curso de Windows e Active Directory.

Sumario

Escenario de partida

Partindo do escenario 6.2 deste apartado VI, vaise configurar o servidor windows **win2k3-00** e o equipo Ubutu Desktop **cliente01**, tocando uns ficheiros de configuración que permitan resolver os problemas presentados.


Escenario 6.2: Configuración complexa
Servidor Windows – Cliente Linux (sadms)
internet
172.16.0.1
255.255.0.0
CONEXION
Active Directory
Win2k3-00
172.16.0.150
cliente01
172.16.0.151
usuarios
comun
alum
asi1
asi2

Crear e compartir carpetas

- No equipo **win2k3-00** eliminar as carpetas dos usuarios **pol** e **paz** do escenario anterior. Crear novas carpetas:
    - Para as carpetas persoais do profesorado e alumnado de 1º e 2º do ciclo de Administración de Sistemas Informáticos: **c:\usuarios\profes**, **c:\usuarios\alum\asi1** e **c:\usuarios\alum\asi2**. A carpeta usuarios segue compartida como no escenario 1.
    - Unha carpeta comun: **c:\comun** para que os usuarios poidan compartir documentos. Compartir a carpeta **comun** co nome de **comun** dándolle en permisos de compartir ó grupo **Todos:Control Total**.

- As ACLs de seguridade déixanse como as configura MS Windows 2003, pero o ideal sería axustar os permisos.

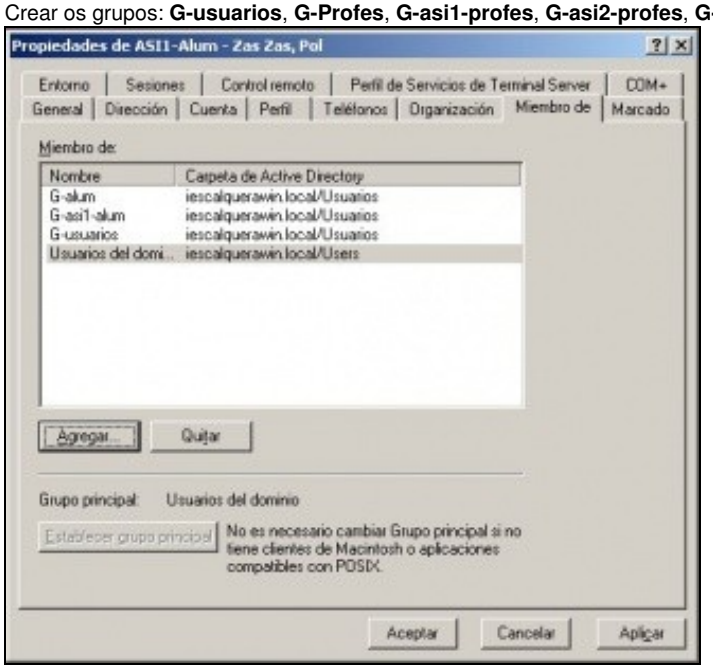
- O resultado de crear as carpetas anteriores e compartir **comun**.

Alta de grupos e modificación de perfiles dos usuarios en Active Directory

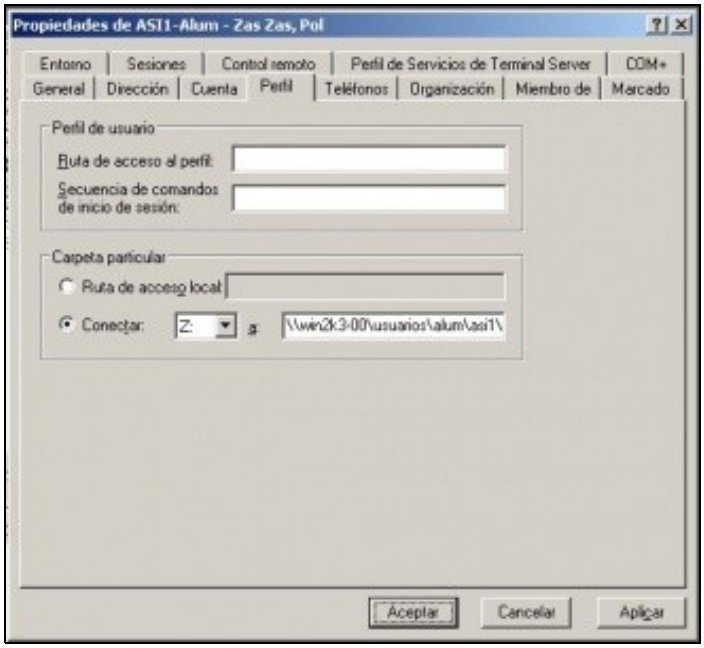
Vanse crear unha serie de grupos ós cales van pertencer os distintos usuarios do dominio. Estes grupos usaríanse para axustar os permisos das carpetas anteriores, pero algúns deles vanse usar no **cliente01** para que cando entre un usuario, saber se se trata dun alumno ou dun profesor, e conectarlle á súa carpeta persoal, así como outras cousas.

- 

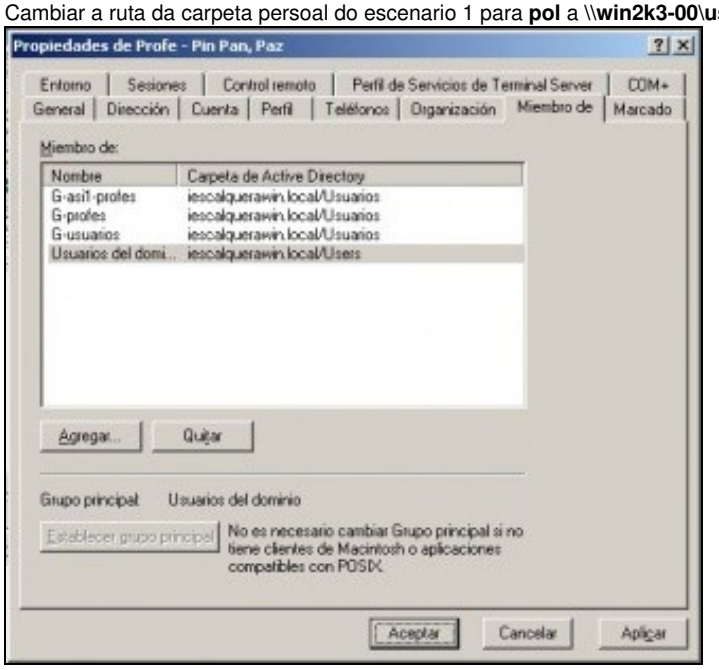
Crear os grupos: **G-usuarios**, **G-Profes**, **G-asi1-profes**, **G-asi2-profes**, **G-alum**, **G-asi1-alum** e **G-asi2-alum**.

- 

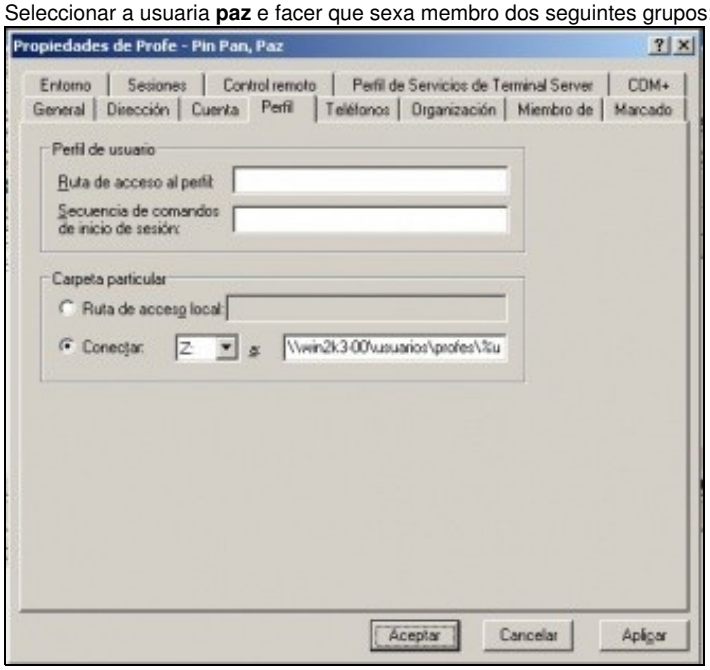
Seleccionar o usuario **pol** e facer que sexa membro dos seguintes grupos: G-usuarios, G-alum e G-asi1-alum. Se se tivera elevado o nivel funcional do dominio, os grupos poderían estar aniñados e **pol** portencería directamente a G-asi1-alum e transitivamente a G-alum e G-usuarios.

- 

Cambiar a ruta da carpeta persoal do escenario 1 para **pol** a **win2k3-00\usuarios\alum\asi1\%username%**.

- 

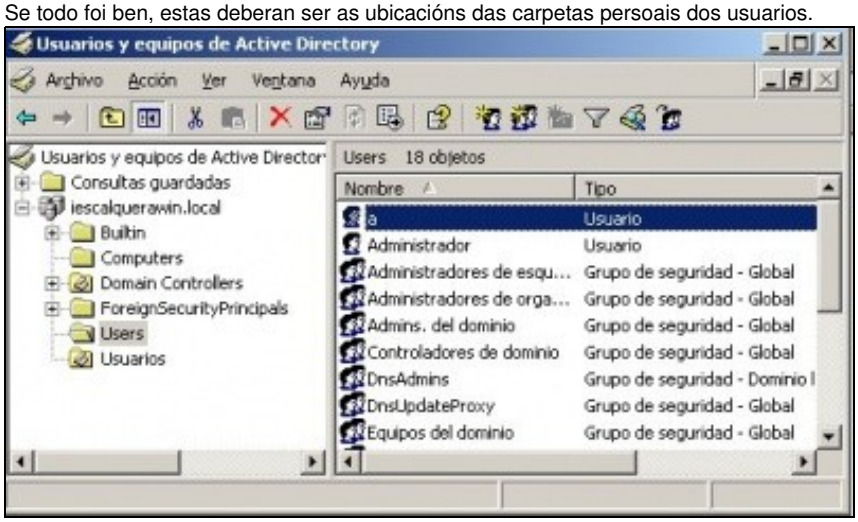
Seleccionar a usuaria **paz** e facer que sexa membro dos seguintes grupos: G-usuarios, G-profes e G-asi1-profes.

- 

Cambiar a ruta da carpeta persoal do escenario 1 para **paz** a **win2k3-00\usuarios\profes\%username%**.

- 

Se todo foi ben, estas deberan ser as ubicacións das carpetas persoais dos usuarios.

- 

Crear o usuario **a** do usuario **administrador** da unidade organizativa **users**. Este usuario usarase para introducir estacións de traballo no dominio. Realmente habería que facelo delegando o control sobre a unidade organizativa **computers** ós usuarios que sin ser administradores tiveran permisos para meter estacións no dominio, tal e como se explica nos apuntes antes sinalados. Neste caso para continuar non se fará así e simplemente se copiará o usuario **a** do **administrador**. Este usuario habilitarase e deshabilitarase segundo proceda, antes e despois de comezar o proceso de alta de estacións no dominio. Tamén se lle cambiará o contrasinal cada vez que se use.

Parar servizos en SADMS en equipo cliente01

Como o equipo vén do escenario 1, antes de facer cambios na configuración dos arquivos de SADMS, pararanse tódolos servizos.

- Parar os servizos de PAM: premer en **Unistall PAM**.

- Parar os demais servizos. Precísase que a solapa de datos estea cuberta, pode ser con datos reais ou ficticios, pero deben estar cubertos. Premer en **Uninstall**.

- Os servizos parados:

Recoméndase borrar as carpetas persoais dos usuarios do dominio que se crearon no cliente01, cando se entrou nese equipo con eses usuarios.

```
sudo rm /home/pol -r
sudo rm /home/paz -r
```

Configuración de sadms

Sadms, usa unha serie de ficheiros de configuración que se usan no momento no que se activan os distintos servizos. No caso de PAM úsanse hai que facer modificacións en dous arquivos:

Puntos de montaxe ós recursos compartidos

No ficheiro **/usr/local/lib/sadms-2.0.14/conf/_pam_mout.conf.xml** especifícanse os volumes a montar por PAM MOUNT cando un usuario inicia sesión. Este arquivo é procesado por SADMS para crear ós puntos de montaxe en **/etc/security/pam_mount.conf.xml**. Deste xeito, cando un usuario do dominio entra no equipo, cóllese o nome do servidor, o usuario, o recurso compartido, etc. e créase un punto de montaxe na carpeta persoal do usuario en **$HOME/.cifsmount** ó recurso compartido.

- O seguinte ficheiro **/usr/local/lib/sadms-2.0.14/conf/_pam_mout.conf.xml** recolle a configuración antiga e a nova, para contemplar que se conecten varios recursos compartidos e non só un.

```
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE pam_mount SYSTEM "pam_mount.conf.xml.dtd">


<pam_mount>
```

```
<volume user="*" fstype="cifs" server="win2k3-00" path="usuarios" mountpoint="~/.usuarios" options="iocharset=utf8"/>
<volume user="*" fstype="cifs" server="win2k3-00" path="comun" mountpoint="~/.comun" options="iocharset=utf8"/>




<debug enable="0" />



<mntoptions allow="nosuid,nodev,loop,encryption,fsck,nonempty,allow_root,allow_other" />

<mntoptions require="nosuid,nodev" />

<path>/sbin:/bin:/usr/sbin:/usr/bin:/usr/local/sbin:/usr/local/bin</path>

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



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

</pam_mount>
```

Crear enlaces ós puntos de montaxe

No ficheiro **usr/local/lib/sadms-2.0.14/conf/_bash_profile-ext** está o contido co que se van configurar os arquivos **/etc/skel/.bash_profile** e **/etc/X11/Xsession.d/99cifsmount** cando se instala PAM en SADMS. Cando un usuario inicie sesión crearanse unha serie de enlaces ós puntos de montaxe.

- O seguinte arquivo **usr/local/lib/sadms-2.0.14/conf/_bash_profile-ext**, amosa a configuración orixinal e as modificacións que se lle fixeron para adaptarse á nova situación. Este ficheiro é tido en conta cando se instala PAM en SADMS.

```
# ORIXINAL INICIO
## network links
# if [ -d ${netmountpoint} ];then
#       u=${USER##*/}
#       [ -L $HOME/net-home ] || ln -s ${netmountpoint} $HOME/net-home
#       if [ ! -z "${haveperusersubdir}" -o -d "${netmountpoint}/${u}" ]; then
#               [ -L $HOME/net-home-${u} ] || ln -s ${netmountpoint}/${u} $HOME/net-home-${u}
#       fi
#else
#       echo mountpoint ${netmountpoint} does not exist
#fi
# ORIXINAL FIN

#Neste script comentado, a variable netmountpoint, toma por defecto o valor de .cifsmount
u=${USER##*/}

####### Nome do servidor Windows.
SERVIDOR=Win2k3-00


######### Para todos os usuarios
# Comprobar se non existe o enlace simbólico na carpeta do usuario Comun-en-$SERVIDOR
# Se non existe creáse apuntado ó punto de montaxe que se crea na carpeta do usuario cando
# este entra. Neste caso o punto de montaxe está oculto en $HOME/.comun.
[ -L $HOME/Comun-en-$SERVIDOR ] || ln -s ~/.comun $HOME/Comun-en-$SERVIDOR


########### Para os usuarios profesores
if (groups ${u} | grep profes);then
        [ -L $HOME/${u}-en-$SERVIDOR ] || ln -s ~/.usuarios/Profes/${u} $HOME/${u}-en-$SERVIDOR
```

```
# Fixarse que se é un profesor facilítaselle a vida creándolle un enlace ás carpetas persoais dos
# alumnos para que poida acceder ó contido dos alumnos ós que lle imparte clase.
        [ -L $HOME/Alumnos-en-$SERVIDOR ] || ln -s ~/.usuarios/Alum $HOME/Alumnos-en-$SERVIDOR

# Imaxinar que en Comun do servidor hai unha carpeta Avisos, e ahí hai avisos para os profes
# nun documento html. Esta liña lanzaría ese aviso para os profesores.
        firefox $HOME/Comun-en-$SERVIDOR/Avisos/Aviso_profes.htm &
fi


########## Para os usuarios alumnos
#Dependendo do grupo do alumno, este terá a carpeta persoal nunha ubicación ou en outra.
curso=
if (groups ${u} | grep asi1-alum);then
        curso=asi1
fi

if (groups ${u} | grep asi2-alum);then
        curso=asi2
fi


if [ $curso ];then
        [ -L $HOME/${u}-en-$SERVIDOR ] || ln -s ~/.usuarios/alum/${curso}/${u} $HOME/${u}-en-$SERVIDOR

# Avisos: a mesma explicación que no caso dos profesores.
        firefox $HOME/Comun-en-$SERVIDOR/Avisos/Aviso_alumnos.htm &
fi
```

Datos de configuración

Como se viu no escenario 1, despois de detectar os datos, había que poñer o nome NETBIOS, o usuario administrador, o seu contrasinal e eliminar da OU a entrada **computers**.

Pois ben, pódese ter un ficheiro de configuración, que se cargue xa cos datos que non varían para cada equipo.

Crear un ficheiro de configuracion en: /**usr**/**local**/**lib**/**sadms-2.0.14**/**settings**/ con nome **A_iescalquerawin.sadms** . A letra **A** inicial, é para que cando se busque ese arquivo na carpeta apareza de primeiro.

Introducir no arquivo o seguinte contido:

```
realm=IESCALQUERAWIN.LOCAL
dns=iescalquerawin.local
kdc=win2k3-00
domain=IESCALQUERAWIN
hostOu=
administrator=a
hostsAllow=172.
winsServer=
```

Fixarse como en hostOU, non se pon información, e como usuario administrador xa carga por defecto o usuario **a** creado anteriormente no Active Directory.

Crear marcadores

Isto xa non ten nada que ver con SADMS, pero xa postos, vaise facilitar que os usuarios cando inicien sesión, teñan xa uns marcadores creados en **Lugares**, que apunten ós recursos compartidos que máis van usar. Incluso se creará un enlace no escritorio á carpeta de rede do usuario.

Engadir ó final do arquivo /**etc**/**profile** o seguinte:

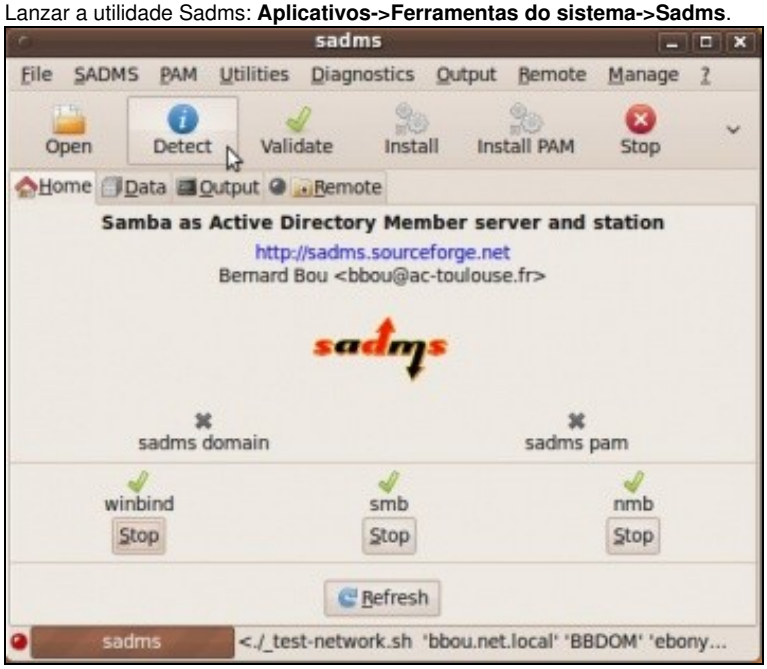
```
SERVIDOR=Win2k3-00

echo file://$HOME/$USER-en-$SERVIDOR>$HOME/.gtk-bookmarks
echo file://$HOME/Comun-en-$SERVIDOR>>$HOME/.gtk-bookmarks
echo file://$HOME/Alumnos-en-$SERVIDOR>>$HOME/.gtk-bookmarks
ln -s $HOME/$USER-en-$SERVIDOR $HOME/Escritorio/$USER-en-$SERVIDOR
```

Iniciar servizos con SADMS

Agora toca iniciar SADMS e volver a lanzar os servizos coas modificacións que se fixeron anteriormente.

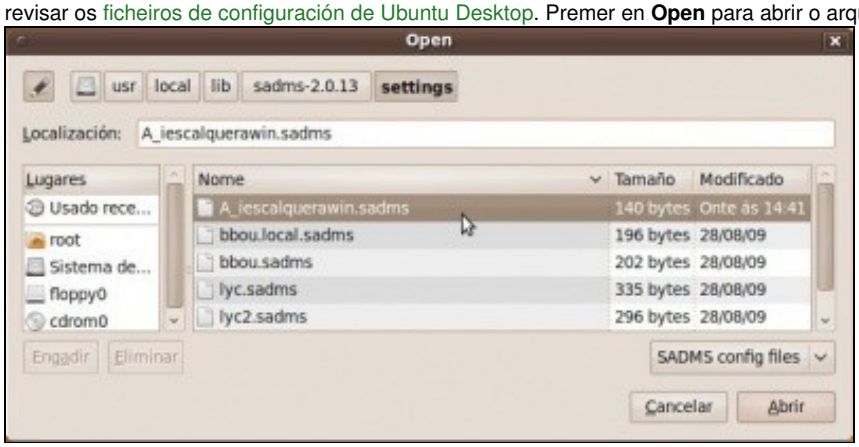
- 

Lanzar a utilidade Sadms: **Aplicativos->Ferramentas do sistema->Sadms**.
- 

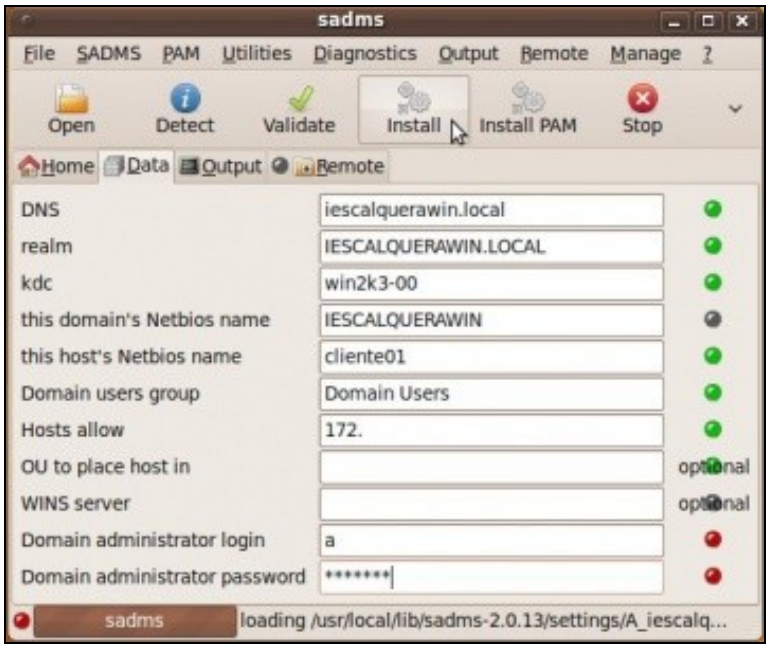
Premer sobre o botón **Detect**, deste xeito detectáse...

- 

... o servidor DNS, de dominio, nome de equipo, etc. Se ó premer en **DETECT** non se cumprimentar os campos da imaxe, entón débense revisar os ficheiros de configuración de Ubuntu Desktop. Premer en **Open** para abrir o arquivo de configuración anteriormente creado ...

- 

... seleccionalo.

- 

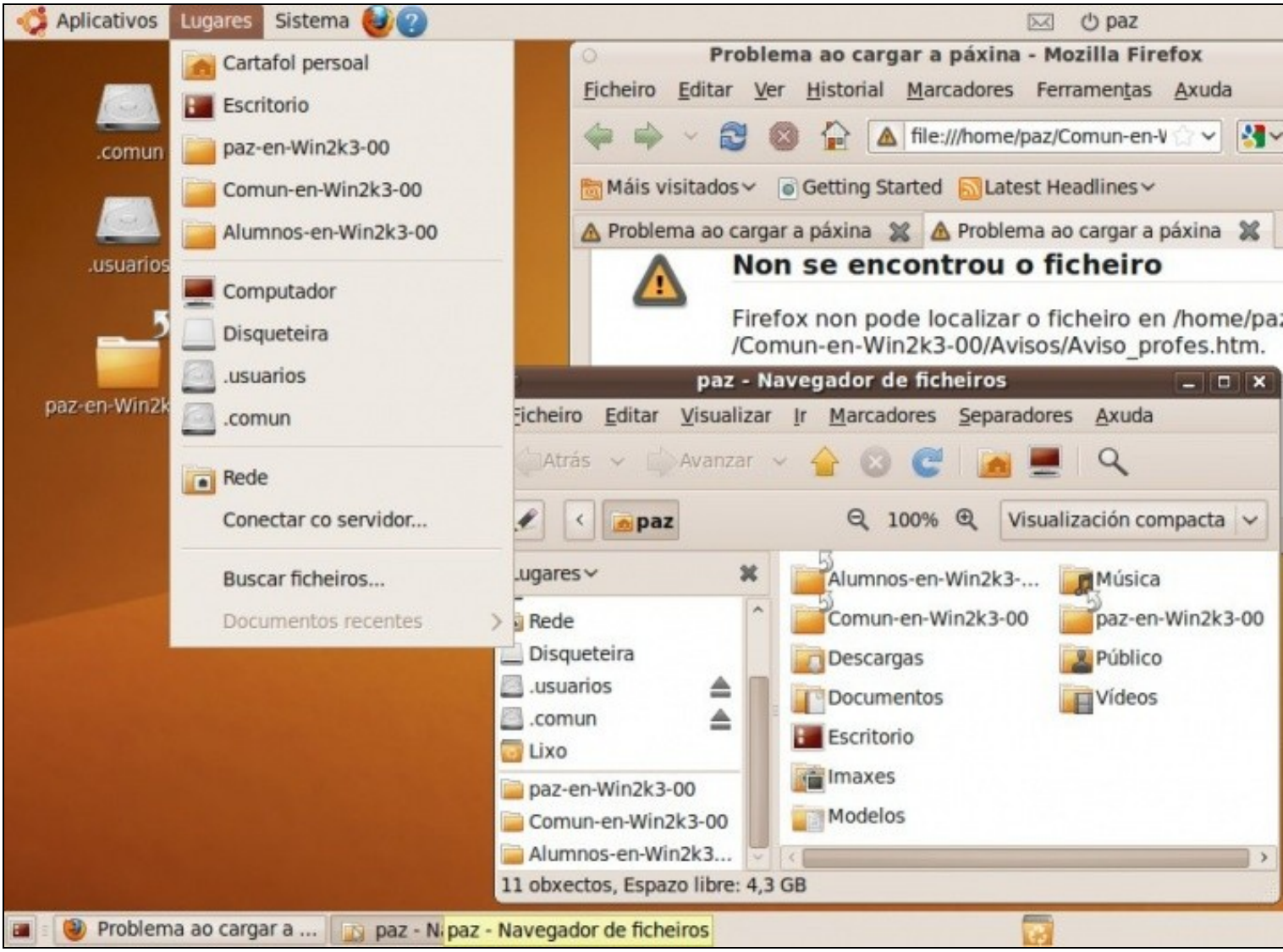
Agora xa están os daots necesarios cubertos, e eliminado computers de OU. Só resta introducir o contrasinal dos usuario do dominio **a'.** ***Premer en*** *Install*.

- 

Premer en **PAM Install**. Pero nesta ocasión non fai falla indicar nin servidor nin recurso compartido, porque están postos explicitamente no ficheiro de configuración: /**usr**/**local**/**lib**/**sadms-2.0.14**/**conf**/**_pam_mout.conf.xml**.

Iniciar sesión cun usuario do dominio

- Reiniciar o equipo
- Entrar co usuario **paz**. Crearase a carpeta persoal de **paz** en /**home** e dentro hai enlaces a determinadas carpetas do servidor **win2k3-00**.


Aplicativos
Lugares
Sistema
paz
Cartafol persoal
Escritorio
paz-en-Win2k3-00
Comun-en-Win2k3-00
Alumnos-en-Win2k3-00
Computador
Disqueteira
.usuarios
.comun
Rede
Conectar co servidor...
Buscar ficheiros...
Documentos recentes
.comun
.usuarios
paz-en-Win2k
Problema ao cargar a páxina - Mozilla Firefox
Ficheiro Editar Ver Historial Marcadores Ferramentas Axuda
file:///home/paz/Comun-en-W
Máis visitados
Getting Started
Latest Headlines
Problema ao cargar a páxina
Problema ao cargar a páxina
Non se encontrou o ficheiro
Firefox non pode localizar o ficheiro en /home/paz
/Comun-en-Win2k3-00/Avisos/Aviso_profes.htm.
paz - Navegador de ficheiros
Ficheiro Editar Visualizar Ir Marcadores Separadores Axuda
Atrás
Avanzar
paz
100%
Visualización compacta
Lugares
Rede
Disqueteira
.usuarios
.comun
Lixo
paz-en-Win2k3-00
Comun-en-Win2k3-00
Alumnos-en-Win2k3...
Alumnos-en-Win2k3-...
Comun-en-Win2k3-00
Descargas
Documentos
Escritorio
Imaxes
Modelos
Música
paz-en-Win2k3-00
Público
Vídeos
11 obxectos, Espazo libre: 4,3 GB
Problema ao cargar a ...
paz - N
paz - Navegador de ficheiros

- Observar:
    - como se trataba de cargar no navegador o ficheiro de aviso dos profesores, pero ... é que non estaba creado.
    - Como no escritorio está o enlace de /etc/profile
    - Como no menú lugares están os marcadores que se crearon dende o arquivo /etc/profile.
    - Como na carpeta persoal están os enlaces creados por /etc/X11/Xsession.d/99cifsmount.
    - E na carpeta persoal hai puntos de montaxe ocultos, creados por /etc/security/pam_mount.conf.xml no momento de iniciar sesión o usuario.

Se nalgún caso anterior houbera problemas coas tiles e as eñes (**ñ**) entre o cliente e o servidor agora non debería habelas.

-- Antonio de Andrés Lema e Carlos Carrión Álvarez -- (28 feb 2010).