Configuración de Samba4 como Controlador de Dominio de Active Directory

Juan Manuel Rodríguez Begines

Junio 2014

Índice de contenido

1. Introducción

En muchas organizaciones, los administradores de sistema se encuentran con la necesidad de integrar sistemas Linux en entornos de dominio de Microsoft Active Directory. Existe mucha documentación disponible para realizar esta labor. Si profundizamos de forma más detallada comprenderemos que hay una gran cantidad de componentes, configuraciones y opciones de integración disponibles.

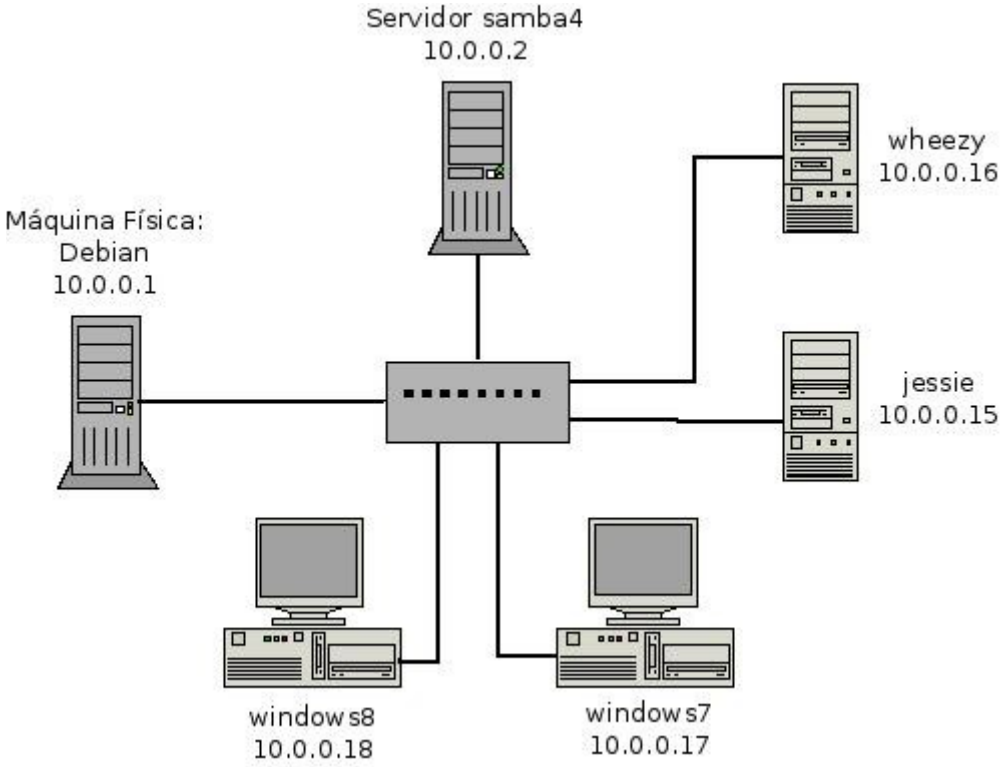
La intención de este proyecto es ayudar a comprender y determinar la mejor solución para implementar en un entorno específico. En este documento se detalla el despliegue e integración de Debian Wheezy en un dominio de Active Directory

2. Características del Proyecto

En este proyecto vamos a configurar un equipo Debian Wheezy con Samba4 como Controlador de Dominio Principal (PDC) compatible con Microsoft Active Directory.

2.1. Escenario

Para realizar esta práctica vamos a utilizar 5 máquinas virtuales: el controlador de dominio (DC), dos clientes Linux y dos clientes Windows.



Las características de los componentes de la red son las siguientes:

Componente	Nombre	IP	Sistema Operativo
Servidor	samba4	10.0.0.2	Debian Wheezy
Cliente1	wheezy	10.0.0.16	Debian Wheezy
Cliente2	jessie	10.0.0.15	Debian Jessie
Cliente3	windows7	10.0.0.17	Windows 7
Cliente4	windows8	10.0.0.18	Windows 8
Red	asir.local	10.0.0.0/24	

3. Componentes

Para llevar a cabo la implementación del proyecto de integración de manera exitosa es esencial comprender cada componente y la función que desempeña. En este apartado vamos a describir de forma más detallada los principales componentes del proyecto.

3.1. Debian Wheezy

Debian Wheezy es la versión 7 de la distribución GNU/Linux Debian. Es el sucesor de Debian Squeeze y antecesor de la versión en pruebas Jessie.

Debian es una de las distribuciones Linux más completas y se caracteriza por:

- La disponibilidad en varias arquitecturas.
- Una amplia colección de software disponible.
- Un grupo de herramientas para facilitar el proceso de instalación y actualización del software (APT, Aptitude, Dpkg, Synaptic, Dselect, etc.)
- Multiarch, que permite instalar paquetes de múltiples arquitecturas en el mismo sistema. Es posible instalar programas de 64 y de 32-bits en el mismo sistema, con la capacidad de resolver las dependencias correctamente de forma automática.
- Servicios en la nube como Xen Nube Plataforma (XCP), Openstack, o nubes públicas como Amazon EC2, Windows Azure, Google Computer Engine.
- Su compromiso con los principios y valores involucrados en el movimiento del Software Libre.
- No tiene marcado ningún entorno gráfico en especial, pudiéndose no instalar ninguno, o instalar GNOME, KDE, Xfce, LXDE, etc.

3.2. Active Directory Domain Services (AD DS)

Servicios de directorio es una base de datos distribuida que permite almacenar información relativa a los recursos de una red con el fin de facilitar su localización y administración.

Active Directory es la implementación de servicios de directorio desarrollados por Microsoft. Utiliza versiones personalizadas de los protocolos estándar como Kerberos, DNS y LDAP. Almacena información de una organización en una base de datos centralizada, organizada y accesible. Los objetos de directorio (usuarios, grupos, equipos, etc) se almacenan de forma jerárquica en nodos, árboles, los bosques y dominios.

3.3. Samba

Samba es una implementación libre de código abierto del protocolo de ficheros compartidos SMB/CIFS para sistemas de tipo UNIX. Samba permite la interoperabilidad entre servidores Linux/Unix y clientes basados en Windows. Samba le ofrece al administrador de red libertad y flexibilidad en términos de ajustes, configuración y elección de sistemas y equipos.
Samba proporciona servicios de archivos e impresión y puede integrarse en un dominio Windows, ya sea como controlador de dominio principal (PDC) o como miembro del dominio.

3.4.SMB/CIFS

Server Message Block (SMB) y Common Internet File System (CIFS) son protocolos de red desarrollados para compartir archivos e impresoras entre nodos de una red. El protocolo SMB fue desarrollado originalmente por IBM y posteriormente ampliado por Microsoft y renombrado como CIFS.

Los términos SMB y CIFS son a menudo intercambiables pero hay características en la implementación de SMB de Microsoft que no son parte del protocolo SMB original. Sin embargo, desde una perspectiva funcional, ambos son protocolos utilizados por Samba.

3.5. Kerberos

Kerberos es un protocolo de seguridad creado por el MIT que usa una criptografía de claves simétricas para validar usuarios con los servicios de red, evitando así tener que enviar contraseñas a través de la red. Al validar los usuarios para los servicios de la red por medio de Kerberos, se frustran los intentos de usuarios no autorizados que intentan interceptar contraseñas en la red.

Kerberos funciona a base de "tickets" que se otorgan por una tercera parte de confianza llamado centro de distribución de claves (KDC) para autenticar los usuarios a un conjunto de servicios de red. Una vez que el usuario se ha autenticado al KDC, se le envía un ticket específico para esa sesión de vuelta a la máquina del usuario. De esta manera cualquier servicio kerberizado buscará el ticket en la máquina del usuario en vez de preguntarle al usuario que se autentique usando una contraseña.

Kerberos tiene su propia terminología para definir varios aspectos del servicio:

- Realm/Reino: red que usa Kerberos, compuesto de uno o varios servidores (también conocidos como KDCs) y un número potencial de clientes.

- Principal: es el nombre único de un usuario o servicio que puede autenticar mediante el uso de Kerberos. Todos los principales de un reino tienen su propia llave, que en el caso de los usuarios se deriva de su contraseña y en le de los servicios se genera aleatoriamente.

- Ticket: son datos cifrados que el servidor Kerberos facilita a los clientes para su autenticación y que estos almacenan durante la sesión. Los principales tipos de tickets son:

  - Ticket Granting Ticket (TGT): ticket de autenticación de un usuario en la red y que se solicita al iniciar la sesión. Normalmente los TGT tienen una validez de 10 horas.

  -Ticket Granting Service (TGS): ticket que solicita un usuario para autenticarse frente a un servidor que también esté en la base de datos de Kerberos.

- KDC (Centro de Distribución de Claves): servidor Kerberos encargado de la autenticación, compuesto por un AS (Servidor de Autenticación) encargado de repartir los TGT y un Ticket Granting Server encargado de distribuir los TGS.

3.6. LDAP

LDAP son las siglas de Lightweight Directory Access Protocol (en español Protocolo Ligero de Acceso a Directorios) que hacen referencia a un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también se considera una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas.

LDAP organiza la información en una jerarquía basada en el uso de directorios. Estos directorios pueden almacenar una variedad de información y se pueden incluso usar de forma similar al Servicio de Información de Red (NIS), permitiendo que cualquiera pueda acceder a su cuenta desde cualquier máquina de la red.

3.7. System Security Services Daemon (SSSD)

El Demonio de servicios de seguridad del sistema (SSSD) proporciona acceso remoto a mecanismos de autenticación e identidad, conocidos como proveedores. Los clientes locales se conectan a SSSD y SSSD contacta con los proveedores externos.

Esto conlleva una serie de ventajas para los administradores:

- Autenticación Offline: SSSD puede guardar opcionalmente una caché de identidades de usuario y credenciales en el equipo local. Esto permite a los usuarios autenticarse a los recursos con éxito, incluso si el servidor de identificación remoto está fuera de línea o el equipo local está desconectado.

- Reducción de la carga en los servidores de autenticación/identificación. En lugar de que cada cliente tenga que conectarse al servidor de autenticación/identificación, todos los clientes locales pueden conectarse a SSSD, el cual puede conectarse al servidor o comprobar su caché.

- Única cuenta de usuario. Dentro de una red, el usuario tiene varias cuentas, por ejemplo la cuenta del dominio y la cuenta local del equipo. Debido a que SSSD soporta autenticación offline y a su caché, los usuarios remotos pueden conectarse a los recursos de la red autenticándose en su equipo local y después SSSD mantiene sus credenciales.

Los dominios son una combinación de un proveedor de identidad y un método de autenticación. SSSD trabaja con proveedores de identidad LDAP (OpenLDAP, Red Hat Directory Server, IdM en RHEL, Microsoft Active Directory) y con autenticación LDAP o Kerberos.

3.8 Domain Name System (DNS)

Sistema de Nombres de Dominio (DNS) es un sistema de nomenclatura jerárquica para equipos, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignados a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, con el propósito de poder localizar y direccionar estos equipos mundialmente.

El servidor DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio. En Debian Wheezy, el DNS se configura en el fichero /etc/resolv.conf.

3.9 Network Time Protocol (NTP)

Network Time Protocol (NTP) es un protocolo de Internet que se utiliza para sincronizar los relojes del sistema del ordenador a una fuente de tiempo de referencia. En Debian Wheezy, el demonio ntpd maneja la sincronización. Parámetros de NTP se configura en el archivo /etc/ntp.conf.

3.10. Name Service Switch (NSS)

Name Service Switch (NSS) permite obtener información del usuario y del sistema a partir de diferentes servicios de bases de datos tales como DNS, LDAP, NIS o archivos locales (/etc/passwd, /etc/group,...). En Debian Wheezy, NSS se configuran en el fichero /etc/nsswitch.conf.

3.11. Network File System (NFS)

NFS es un protocolo de nivel de aplicación utilizado para sistemas de archivos distribuido en un entorno de red local. Posibilita que distintos sistemas conectados a una misma red accedan a ficheros remotos como si se tratara de locales. El sistema NFS está dividido al menos en dos partes principales: un servidor y uno o más clientes. Los clientes acceden de forma remota a los datos que se encuentran almacenados en el servidor. En esta práctica utlizaremos la última versión NFSv4.

4. Instalación de Samba4

El primer paso que vamos a llevar a cabo será instalar Samba4 en nuestro servidor al que también hemos llamado *samba4.*

4.1. Requisitos

Antes de instalar Samba, debemos instalar los siguientes paquetes:

```
# aptitude install build-essential libacl1-dev libattr1-dev libblkid-dev \
libgnutls-dev libreadline-dev python-dev python-dnspython gdb pkg-config \
libpopt-dev libldap2-dev dnsutils libbsd-dev attr krb5-user docbook-xsl \
libcups2-dev acl git bind9
```

4.2. Método de instalación

La instalación puede llevarse a cabo desde los repositorios, o bien compilando el código fuente. Según el sistema operativo, hay una versión determinada de Samba4 disponible:

- Debian Wheezy: samba 4.1.7 (desde los repositorios backports)
- Debian Jessie: samba 4.1.7
- Ubuntu 13.10 (Saucy Salamander): samba 4.0.3
- Ubuntu 14.04 LTS (Trusty Tahr): 4.1.6
- CentOS 6: samba 4.0.0

En nuestro caso vamos a optar por compilar la última versión estable Samba 4.1.8. disponible para Debian Wheezy. Mediante *git* descargamos el repositorio samba correspondiente:

```
# git clone -b v4-1-stable git://git.samba.org/samba.git \
/usr/src/samba4.1-stable

# ./configure

# make
# make install
```

La ruta de instalación de Samba es */usr/local/samba/* y contiene los siguientes directorios:

```
root@samba4:~# /usr/local/samba/
bin/     etc/     include/     lib/     private/     sbin/     share/     var/
```

A continuación vamos añadir los directorios /usr/local/samba/bin y /usr/local/samba/sbin al PATH:

```
# echo export PATH=$PATH:/usr/local/samba/bin/:/usr/local/samba/sbin/ >>  \
~/.bashrc
```

Comprobemos qué versión de Samba tenemos instalada:

```
# samba -V
Version 4.1.8
```

4.3. Implementación del nuevo dominio

Utilizaremos el comando *samba-tool domain provision* para implementar nuestro dominio *asir.local* con las opciones que figuran a continuación.

```
# samba-tool domain provision --use-rfc2307 --interactive

Realm: asir.local
Domain [asir]: asir
Server Role (dc, member, standalone) [dc]: dc
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) \
[SAMBA_INTERNAL]: BIND9_DLZ
Administrator password:

Server Role:           active directory domain controller
Hostname:              samba4
NetBIOS Domain:        ASIR
DNS Domain:            asir.local
DOMAIN SID:            S-1-5-21-4289379584-2687096460-2000543676
```

Como servidor DNS hemos preferido elegir Bind9 en lugar del servidor interno de Samba. También debemos asegurarnos de elegir una contraseña de administrador compleja ya que en caso contrario, nos aparecerán una serie de errores.

Comprobaciones
Comprobación de la versión de *smbclient*

```
$ /usr/local/samba/bin/smbclient --version
Version 4.1.8
```

Comprobación de los recursos compartidos.

```
$ /usr/local/samba/bin/smbclient -L localhost -U%
Domain=[ASIR] OS=[Unix] Server=[Samba 4.1.8]

        Sharename       Type      Comment
        ---------       ----      -------
        netlogon        Disk
```

```
        sysvol          Disk
        IPC$            IPC       IPC Service (Samba 4.1.8)
Domain=[ASIR] OS=[Unix] Server=[Samba 4.1.8]

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
```

Comprobación de la autenticación mediante conexión al recurso *netlogon* con la cuenta *administrator* de Samba.

```
$ /usr/local/samba/bin/smbclient //localhost/netlogon -UAdministrator -c 'ls'
Enter Administrator's password:
Domain=[ASIR] OS=[Unix] Server=[Samba 4.1.8]
  .                                   D        0  Thu Jun  5 11:52:22 2014
  ..                                  D        0  Thu Jun  5 11:52:36 2014
```

4.4. Configuración DNS

Por defecto, Samba crea las siguientes dos zonas durante la implementación del nuevo dominio:

- Una zona para nuestro dominio, en nuestro caso **asir.local**
- Y la zona **_msdcs.samdom.asir.local** que contiene los registros SRV para diversos servicios.

Samba no crea la zona de búsqueda inversa, de modo que la creamos de formal manual:

```
# samba-tool dns zonecreate samba4.asir.local 0.0.10.in-addr.arpa
```

Durante la implementación del dominio se creó un fichero *usr/local/samba/private/named.conf* que debemos incluir en el */etc/bind/named.conf* de Bind.

Fichero: /etc/bind/named.conf

```
include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
include "/usr/local/samba/private/named.conf";
```

Comprobación del DNS
Para comprobar que Bind funciona correctamente vamos a realizar las siguientes consultas:

```
$ host -t SRV _ldap._tcp.asir.local
_ldap._tcp.asir.local has SRV record 0 100 389 samba4.asir.local.

$  host -t SRV _kerberos._udp.asir.local
_kerberos._udp.asir.local has SRV record 0 100 88 samba4.asir.local.
```

```
$ host -t A samba4.asir.local
samba4.asir.local has address 10.0.0.2
```

Actualizaciones dinámicas con kerberos
Samba tiene la capacidad de actualizar los ficheros de las zonas de Bind a través de kerberos. Durante la implementación del dominio se creó un fichero keytab que debemos incluir en nuestro *named.conf.options* añadiendo la siguiente línea:

Fichero: etc/bind/named.conf

```
tkey-gssapi-keytab "/usr/local/samba/private/dns.keytab";
```

Las actualizaciones se llevan a cabo al iniciar Samba y luego cada 10 minutos. Podemos ejecutar una actualización de forma manual usando el siguiente comando:

```
 # samba_dnsupdate --verbose --all-names
```

4.5. Kerberos

La configuración de kerberos se encuentra en el fichero */etc/krb5.conf*. Pero cuando configuramos nuestro dominio, se creó otro fichero de configuración de kerberos en */usr/local/samba/private/krb5.conf* que debe reemplazar al que ya existe en el directorio */etc*, y cuyo contenido es el siguiente:

Fichero: /usr/local/samba/private/krb5.conf

```
[libdefaults]
        default_realm = ASIR.LOCAL
        dns_lookup_realm = false
        dns_lookup_kdc = true
```

Para comprobar el funcionamiento de kerberos obtendremos un ticket con el comando *kinit.*

```
$ kinit administrator@ASIR.LOCAL
Password for administrator@ASIR.LOCAL:
Warning: Your password will expire in 41 days on Sat Jul 19 16:41:03 2014

$ klist -5
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: administrator@ASIR.LOCAL

Valid starting     Expires            Service principal
07/06/14 16:52:52  08/06/14 02:52:52  krbtgt/ASIR.LOCAL@ASIR.LOCAL
        renew until 08/06/14 16:52:49
```

4.6. NTP

Active Directory requiere una sincronización de tiempo precisa entre los clientes y el controlador de dominio. Instalaremos un servidor de hora para mantener sincronizados todos los equipos del dominio. Una vez instalado comprobamos la conexión a los servidores de hora públicos.

```
# aptitude install ntp

# ntpq -np
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
+81.19.96.148    192.93.2.20      2 u   29   64    1   43.448   -0.663   0.841
+81.184.154.182  178.17.161.12    3 u   28   64    1   62.217    8.376   2.316
 46.16.60.129    158.227.98.15    2 u    -   64    1   55.712    5.245   1.255
*213.151.108.194 150.214.94.5     2 u    2   64    3   55.330    8.857   0.810
```

Instalamos el mismo paquete en los clientes y modificamos la configuración en */etc/ntp.conf* para usar como servidor de hora a *samba4.asir.local* en lugar de los servidores de hora públicos.

Fichero: /etc/ntp.conf

```
# You do need to talk to an NTP server or two (or three).
#server ntp.your-provider.example
server samba4.asir.local

# pool.ntp.org maps to about 1000 low-stratum NTP servers.  Your server will
# pick a different set every time it starts up.  Please consider joining the
# pool: <http://www.pool.ntp.org/join.html>
#server 0.debian.pool.ntp.org iburst
#server 1.debian.pool.ntp.org iburst
#server 2.debian.pool.ntp.org iburst
#server 3.debian.pool.ntp.org iburst
```

Comprobamos que los clientes obtienen la hora del servidor de hora de la red local.

```
$ ntpq -np
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*10.0.0.2        163.117.202.33   3 u   23   64   17    0.751    9.818   0.147
```

5. Autenticación Kerberos/LDAP/SSSD

En este apartado vamos a configurar la conexión al directorio activo desde los equipos Linux mediante Kerberos, LDAP y SSSD.

5.1. Instalación de SSSD

Vamos a instalar el paquete *sssd* en nuestro servidor *samba4* y en los clientes *wheezy* y *jessie.*

```
# aptitude install sssd
```

SSSD se conectará al directorio activo para obtener la información de las cuentas de usuario usando kerberos. Por lo tanto necesitaremos exportar un fichero *keytab* a los clientes para que SSSD pueda autenticarse frente al servidor.

En este caso hemos usado la cuenta del equipo *samba4* para generar el keytab. Es importante asignar bien los permisos al keytab para evitar errores con SSSD.

```
# samba-tool domain exportkeytab /etc/krb5.keytab --principal=SAMBA4$
# chmod 600 /etc/krb5.keytab
```

5.2. Configuración de SSSD

Al instalar SSSD se crea un fichero de configuración por defecto */etc/sssd/sssd.conf.* Debemos editarlo de la siguiente manera:

Fichero: /etc/sssd/sssd.conf.

```
[sssd]
config_file_version = 2
reconnection_retries = 3
sbus_timeout = 30
services = nss, pam
domains = asir.local
debug_level = 6


[nss]


[pam]


[domain/asir.local]
cache_credentials = true

id_provider = ldap
ldap_schema = rfc2307bis
ldap_referrals = false
ldap_uri = ldap://samba4.asir.local
ldap_search_base = dc=asir,dc=local
ldap_force_upper_case_realm = true

access_provider = simple

auth_provider = krb5
chpass_provider = krb5
ldap_sasl_mech = gssapi
ldap_sasl_authid = SAMBA4$@ASIR.LOCAL
krb5_realm = ASIR.LOCAL
krb5_server = samba4.asir.local
krb5_kpasswd = samba4.asir.local
ldap_krb5_keytab = /etc/krb5.keytab
ldap_user_object_class = user
ldap_user_name = samAccountName
ldap_user_home_directory = homeDirectory
ldap_user_principal = userPrincipalName
ldap_user_shell = loginShell
ldap_group_object_class = group
```

Mediante este fichero estamos configurando la conexión de SSSD al servidor, indicándole el dominio, los datos de conexión al servidor LDAP, la información que debe recuperar y el método de conexión mediante kerberos.

5.3. Configuración de NSS

Por defecto el sistema obtiene la información del usuario (uid-nombre de usuario) y del grupo (gid-nombre del grupo) consultando los ficheros *passwd* y *group.* Entonces vamos a configurar NSS para que además de consultar estos ficheros, obtenga la correspondencia entre UID/GID y nombres a través de SSSD.

Para ello instalamos la biblioteca *libnss-sss* (en este caso se instaló cuando isntalamos SSSD) y editamos el fichero */etc/nsswitch.conf* añadiendo *sss* a las entradas *passwd* y *group.*

Fichero: /etc/nsswitch.conf

```
passwd:         compat sss
group:          compat sss
```

5.4. Configuración PAM

Para configurar PAM para que use SSSD debemos instalar la biblioteca *libpam-sss* (ya instalada cuando instalamos SSSD) y editar los ficheros *common-** ubicados en */etc/pam.d.*

Fichero: /etc/pam.d/common-auth

```
auth    [success=2 default=ignore]      pam_unix.so nullok_secure
auth    [success=1 default=ignore]      pam_sss.so use_first_pass
auth    requisite                       pam_deny.so
auth    required                        pam_permit.so
```

Fichero: /etc/pam.d/common-account

```
account [success=1 new_authtok_reqd=done default=ignore]  pam_unix.so
account requisite                                         pam_deny.so
account required                        pam_permit.so
account sufficient                                        pam_localuser.so
account [default=bad success=ok user_unknown=ignore]      pam_sss.so
```

Fichero: /etc/pam.d/common-password

```
password        [success=2 default=ignore]      pam_unix.so obscure sha512
password        sufficient                                      pam_sss.so
password        requisite                       pam_deny.so
password        required                        pam_permit.so
```

Fichero: /etc/pam.d/common-session

```
session [default=1]         pam_permit.so
session requisite           pam_deny.so
session required            pam_permit.so
session required            pam_unix.so
```

```
session optional            pam_sss.so
```

Una vez terminada la configuración, iniciamos el demonio SSSD:

```
# service sssd start
```

Ahora ya podemos iniciar sesión en el equipo con un usuario del dominio.

5.5. Comprobaciones

Para hacer las comprobaciones vamos a crear el usuario *prueba1* mediante el siguiente comando:

```
# samba-tool user add prueba1 --uid-number=2001 --gid-number=2000 \
--login-shell=/bin/bash --home-directory=/home/prueba1
```

El directorio */home/prueba1* aún no existe. Lo creamos y le asignamos el propietario y grupo correspondiente:

```
# mkdir /home/prueba1
# cp /etc/skel/.* /home/prueba1
# chown -R 2001:2000 /home/prueba1
```

También modificamos el grupo *Domain Users* del directorio activo para poder utilizarlo tanto en Windows como Linux. Para ello lo editamos y le añadimos los siguientes atributos:

```
# ldbmodify -H /usr/local/samba/private/sam.ldb
dn: CN=Domain Users,CN=Users,DC=asir,DC=local
changetype: modify
add: objectClass
objectClass: posixGroup
-
add: gidNumber
gidNumber: 2000
Modified 1 records successfully
```

Para comprobar el correcto funcionamiento de *nss* con *sss* utilizaremos el comando *getent:*

```
# getent passwd prueba1
prueba1:*:2001:2000:prueba1:/home/prueba1:/bin/bash

getent group Domain\ Users
Domain Users:*:2000:
```

También podemos loguearnos con el usuario *prueba1* y crear un directorio o fichero para comprobar el propietario y grupo.

```
# su prueba1
$ cd /tmp/
$ mkdir pruebadir
$ touch prueba.txt
$ ls -l
total 4
drwxr-xr-x 2 prueba1 Domain Users 4096 jun 10 12:07 pruebadir
-rw-r--r-- 1 prueba1 Domain Users    0 jun 10 12:07 prueba.txt
```

Por útlimo nos conectamos por ssh desde *whezzy* a *samba4* usando el usuario *prueba1:*

```
root@wheezy:~# ssh prueba1@samba4.asir.local
prueba1@samba4.asir.local's password:

prueba1@samba4:~$
```

6. Unión del equipo al Dominio

En este apartado vamos a unir los equipos Windows y Linux al dominio de Active Directory. En el caso de Windows, el proceso es idéntico a como lo haríamos si el controlador de dominio fuese Windows Server. En el caso de los clientes Linux, explicaremos de forma más detallada cómo hacerlo.

6.1. Uniendo un cliente Linux al dominio

La configuración será la misma para *wheezy* y *jessie.* Empecemos por configurar correctamente el FQDN del equipo y el DNS. En el fichero */etc/resolv.conf* indicamos el dominio de búsqueda y el DNS apuntando al servidor *samba4.*

Fichero: /etc/resolv.conf

```
domain asir.local
search asir.local
nameserver 10.0.0.2
```

A continuación instalamos los siguientes paquetes para configurar el cliente de kerberos y marcamos como Reino predeterminado *ASIR.LOCAL*

```
# aptitude search krb5-user krb5-config
```

El siguiente paso es instalar el paquete *smbclient.* En Debian Wheezy la versión de *smbclient* es la 3.6.6 mientras que en Debian Jessie es la 4.1.7. En la versión 3.6.6 se produce un error de actualización del DNS, por lo que tendremos que crear los registros A y PTR de forma manual.

Instalamos *smbclient, samba-common y samba-common-bin* en nuestro cliente Debian Wheezy:

```
# aptitude install smbclient samba-common samba-common-bin
```

Editamos el fichero *smb.conf* de la siguiente manera:

Fichero: /etc/samba/smb.conf

```
[global]
   workgroup = PROYECTO
   client signing = yes
   client use spnego = yes
   kerberos method = secrets and keytab
   log file = /var/log/samba/%m.log
   realm = ASIR.LOCAL
   security = ADS
   password server =*
```

Para unir el equipo al dominio utilizaremos el comando *net ads* pero antes debemos crear el directorio */var/lib/samba/private/* donde se almacenará la base de datos *secrets.tdb.* En caso contrario se produciría un error al unir el equipo.

```
# mkdir /var/lib/samba/private/

# net ads join -U administrator
Enter administrator's password:
Using short domain name -- ASIR
Joined 'WHEEZY' to dns domain 'asir.local'
```

Podemos realizar comprobaciones utilizando el mismo comando:

```
# net ads testjoin
Join is OK

# net ads info
LDAP server: 10.0.0.2
LDAP server name: samba4.asir.local
Realm: ASIR.LOCAL
Bind Path: dc=ASIR,dc=LOCAL
LDAP port: 389
Server time: mar, 10 jun 2014 19:24:38 CEST
KDC server: 10.0.0.2
Server time offset: 0
```

Comprobamos que en *jessie* sí se han actualizado los registros DNS de forma automática:

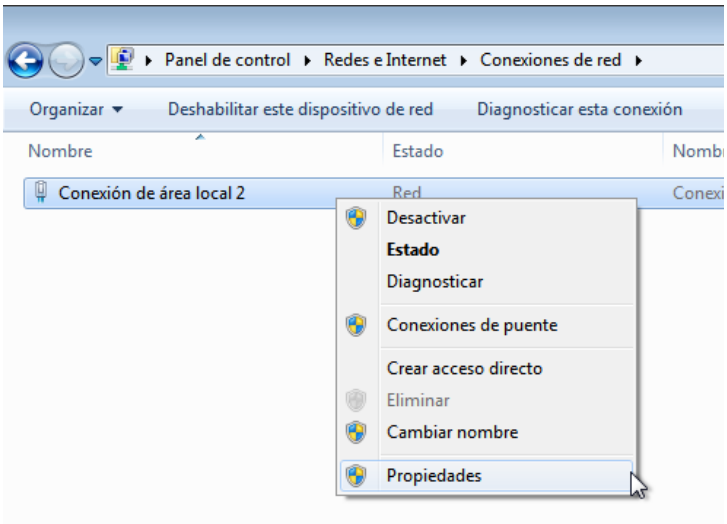
```
# dig jessie.asir.local

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> wheezy.asir.local
```

```
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31506
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;wheezy.asir.local.             IN      A

;; ANSWER SECTION:
wheezy.asir.local.      3600    IN      A       10.0.0.15

;; AUTHORITY SECTION:
asir.local.             900     IN      NS      samba4.asir.local.

;; ADDITIONAL SECTION:
samba4.asir.local.      900     IN      A       10.0.0.2

;; Query time: 4 msec
;; SERVER: 10.0.0.2#53(10.0.0.2)
;; MSG SIZE  rcvd: 88
```

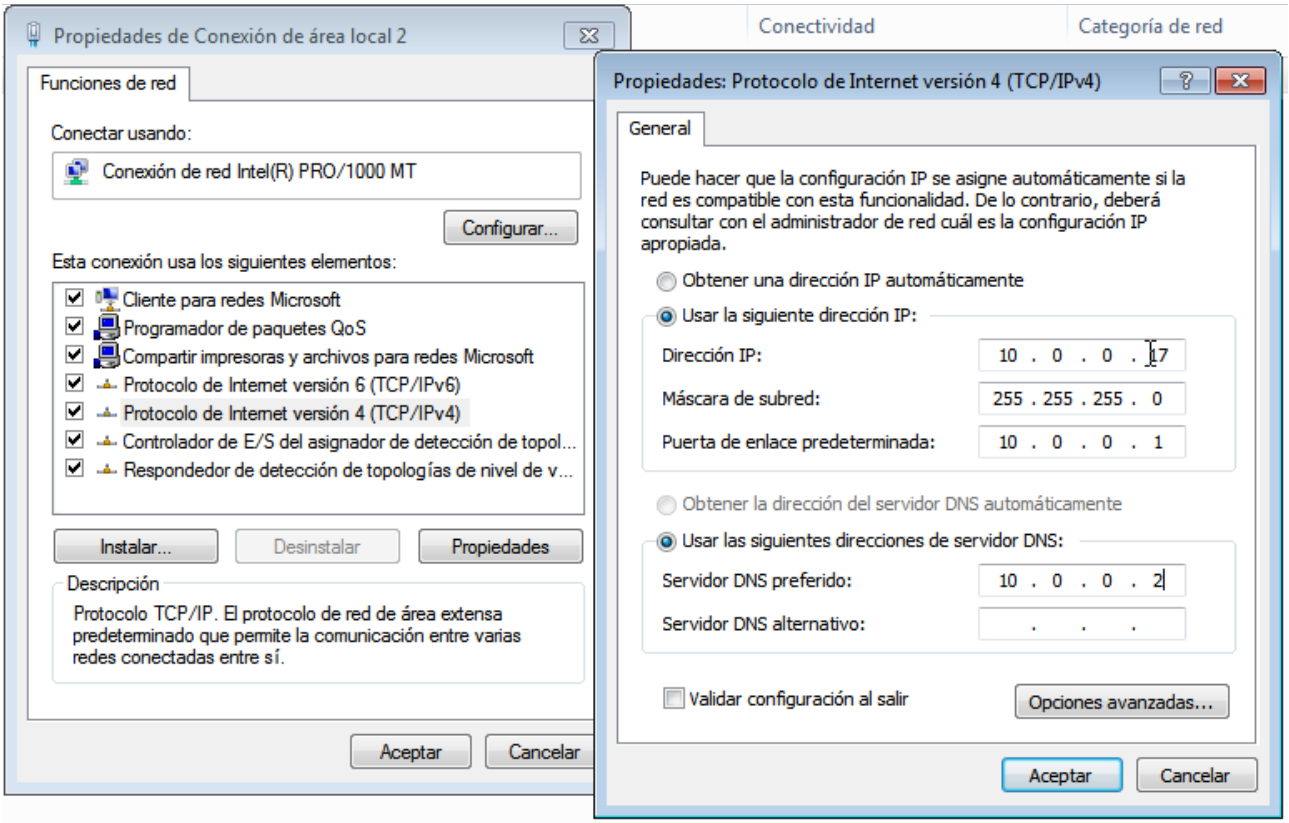
6.2. Uniendo un cliente Windows al dominio

Tenemos un cliente Windows7 y otro Windows8. La forma de proceder es la misma en ambos, de modo que vamos a explicarlo sólo para windows7.

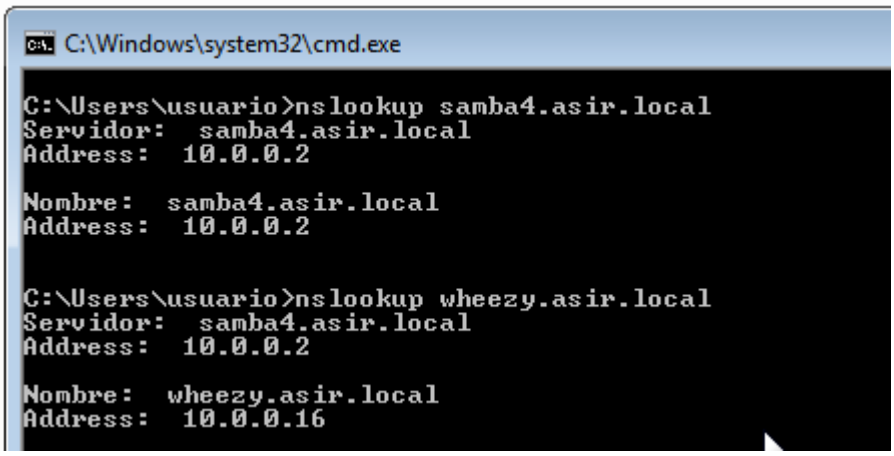
Para configurar el DNS nos vamos a *Inicio* > *Panel de control* > *Redes e Internet* > *Conexiones de red,* hacemos clic derecho sobre la conexión de red y seleccionamos *Propiedades.*



Seleccionamos *Protocolo de Internet versión 4* y marcamos la dirección del servidor DNS de nuestra red, en este caso 10.0.0.2.

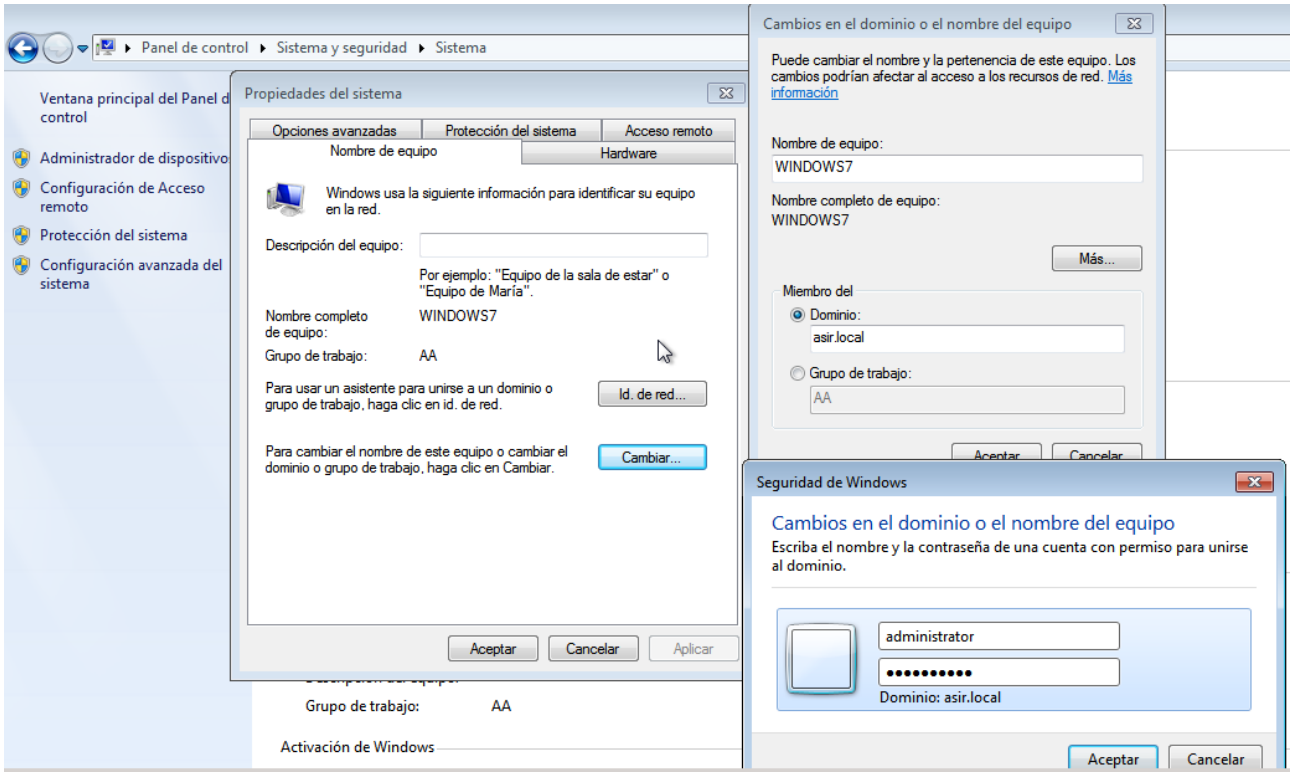


Aceptamos y comprobamos mediante la consola de comandos de Windows haciendo una consulta DNS:



A continuación comprobamos que tenemos bien configurado el nombre de equipo (en nuestro caso WINDOWS7) y procedemos a unir el equipo al dominio.

Accedemos a *Panel de control* > *Sistema y seguridad* > *Sistema,* abrimos *Configuración avanzada del sistema* y dentro de la nueva ventana seleccionamos la pestaña *Nombre de equipo.*
Comprobamos que el nombre del equipo está correcto. Hacemos clic en *Cambiar...* y seleccionamos el dominio al que queremos unirnos (asir.local). Aceptamos y nos pedirá el nombre del usuario administrador del dominio y la contraseña.



Aceptamos de nuevo, nos pedirá reiniciar el equipo y ya tendremos el equipo unido al dominio *asir.local.* Ahora podemos iniciar sesión con el usuario *prueba1.*

7. NFS4

En este apartado vamos a configurar nuestro equipo *samba4* como servidor NFS para exportar los directorios de cada usuario del dominio. De esta manera, el usuario podrá loguearse en cualquier equipo de la red y disponer de su directorio HOME.

7.1. Configuración NFSv4 del servidor

En el servidor instalaremos los paquetes *nfs-kernel-server* y *nfs-common.* En los clientes solo se instala *nfs-common.*

```
# aptitude install nfs-kernel-server nfs-common
```

Debemos editar los ficheros de configuración para que utilicen kerberos a través de GSSAPI.

Fichero: /etc/default/nfs-kernel-server

```
NEED_SVCGSSD=yes
```

Fichero: /etc/default/nfs-common

```
# Do you want to start the idmapd daemon? It is only needed for NFSv4.
NEED_IDMAPD=yes

# Do you want to start the gssd daemon? It is required for Kerberos mounts.
NEED_GSSD=yes
```

Fichero: /etc/idmapd.conf

```
Domain = asir.local
```

A continuación debemos añadir el principal kerberos para el servicio NFS en el servidor y los clientes.

```
root@samba4:/etc# net ads keytab add nfs -k
Processing principals to add...

root@samba4:/etc# klist -k krb5.keytab
Keytab name: FILE:krb5.keytab
KVNO Principal
----
--------------------------------------------------------------------------
   1 SAMBA4$@ASIR.LOCAL
   1 SAMBA4$@ASIR.LOCAL
   1 SAMBA4$@ASIR.LOCAL
   1 nfs/samba4.asir.local@ASIR.LOCAL
   1 nfs/samba4.asir.local@ASIR.LOCAL
   1 nfs/samba4.asir.local@ASIR.LOCAL
   1 nfs/samba4.asir.local@ASIR.LOCAL
   1 nfs/samba4.asir.local@ASIR.LOCAL
   1 nfs/SAMBA4@ASIR.LOCAL
   1 nfs/SAMBA4@ASIR.LOCAL
   1 nfs/SAMBA4@ASIR.LOCAL
   1 nfs/SAMBA4@ASIR.LOCAL
   1 nfs/SAMBA4@ASIR.LOCAL
```

En los clientes:

```
root@wheezy:/etc# net ads keytab add nfs -U administrator
Processing principals to add...
Enter administrator's password:

root@wheezy:/etc# klist -k krb5.keytab
Keytab name: FILE:krb5.keytab
KVNO Principal
----
--------------------------------------------------------------------------
   1 SAMBA4$@ASIR.LOCAL
   1 SAMBA4$@ASIR.LOCAL
   1 SAMBA4$@ASIR.LOCAL
   1 host/wheezy.asir.local@ASIR.LOCAL
   1 host/wheezy.asir.local@ASIR.LOCAL
   1 host/wheezy.asir.local@ASIR.LOCAL
   1 host/wheezy.asir.local@ASIR.LOCAL
   1 host/wheezy.asir.local@ASIR.LOCAL
   1 host/wheezy@ASIR.LOCAL
   1 host/wheezy@ASIR.LOCAL
   1 host/wheezy@ASIR.LOCAL
   1 host/wheezy@ASIR.LOCAL
   1 host/wheezy@ASIR.LOCAL
   1 WHEEZY$@ASIR.LOCAL
   1 WHEEZY$@ASIR.LOCAL
   1 WHEEZY$@ASIR.LOCAL
   1 WHEEZY$@ASIR.LOCAL
   1 WHEEZY$@ASIR.LOCAL
   1 nfs/wheezy.asir.local@ASIR.LOCAL
   1 nfs/wheezy.asir.local@ASIR.LOCAL
   1 nfs/wheezy.asir.local@ASIR.LOCAL
   1 nfs/wheezy.asir.local@ASIR.LOCAL
   1 nfs/wheezy.asir.local@ASIR.LOCAL
   1 nfs/wheezy@ASIR.LOCAL
   1 nfs/wheezy@ASIR.LOCAL
   1 nfs/wheezy@ASIR.LOCAL
   1 nfs/wheezy@ASIR.LOCAL
   1 nfs/wheezy@ASIR.LOCAL
```

El siguiente paso será exportar el directorio */etc/home* del servidor. Para ello creamos el directorio base */nfs4* a partir del cual vamos a exportar el resto de directorios. Dentro de éste crearemos el directorio *home* sobre el que vamos a montar el */etc/home/* que contiene los directorios de cada usuario.

```
# mkdir -p /nfs4/home
# mount --bind /home /nfs4/home
```

Editamos el fichero */etc/fstab/* para que este cambio sea permanente.

```
/home           /nfs4/home      none    rw,bind         0       0
```

Definimos los directorios que se van a exportar en el fichero */etc/exports:*

Fichero: /etc/exports

```
/nfs4          10.0.0.0/24(rw,sync,fsid=0,crossmnt,no_subtree_check,sec=krb5i)
/nfs4/home     10.0.0.0/24(rw,sync,no_subtree_check,sec=krb5i)
```

Por último reiniciamos los demonios y comprobamos los directorios que se exportarán:

```
# service nfs-kernel-server restart
# service nfs-common restart
# showmount -e
Export list for samba4:
/nfs4            10.0.0.0/24
/nfs4/home       10.0.0.0/24
```

7.2. Cliente NFSv4 en Linux

En el cliente tenemos instalado y configurado *nfs-common* y tenemos el fichero keytab con el principal de kerberos para el servicio NFS.

De nuevo utilizamos *showmount* para ver qué directorios del servidor podemos montar.

```
# showmount -e samba4.asir.local
Export list for samba4.asir.local:
/nfs4/home       10.0.0.0/24
/nfs4            10.0.0.0/24
```

Vamos a montar el *home* que exporta el servidor en el directorio */home* del cliente.

```
# mount -t nfs4 -o sec=krb5i samba4.asir.local:/home /home/

# mount | grep nfs4
samba4.asir.local:/home on /home type nfs4
(rw,relatime,vers=4,rsize=32768,wsize=32768,namlen=255,hard,proto=tcp,port=0,t
imeo=600,retrans=2,sec=krb5i,clientaddr=10.0.0.16,minorversion=0,local_lock=no
ne,addr=10.0.0.2)
```

Para que el cambio sea permanente editamos el */etc/fstab* del cliente:

Fichero: /etc/fstab

```
samba4.asir.local:/home        /home    nfs4    rw,sec=krb5i    0       0
```

Reiniciamos el cliente para comprobar que el directorio se monta correctamente e iniciamos sesión con el usuario *prueba1.*

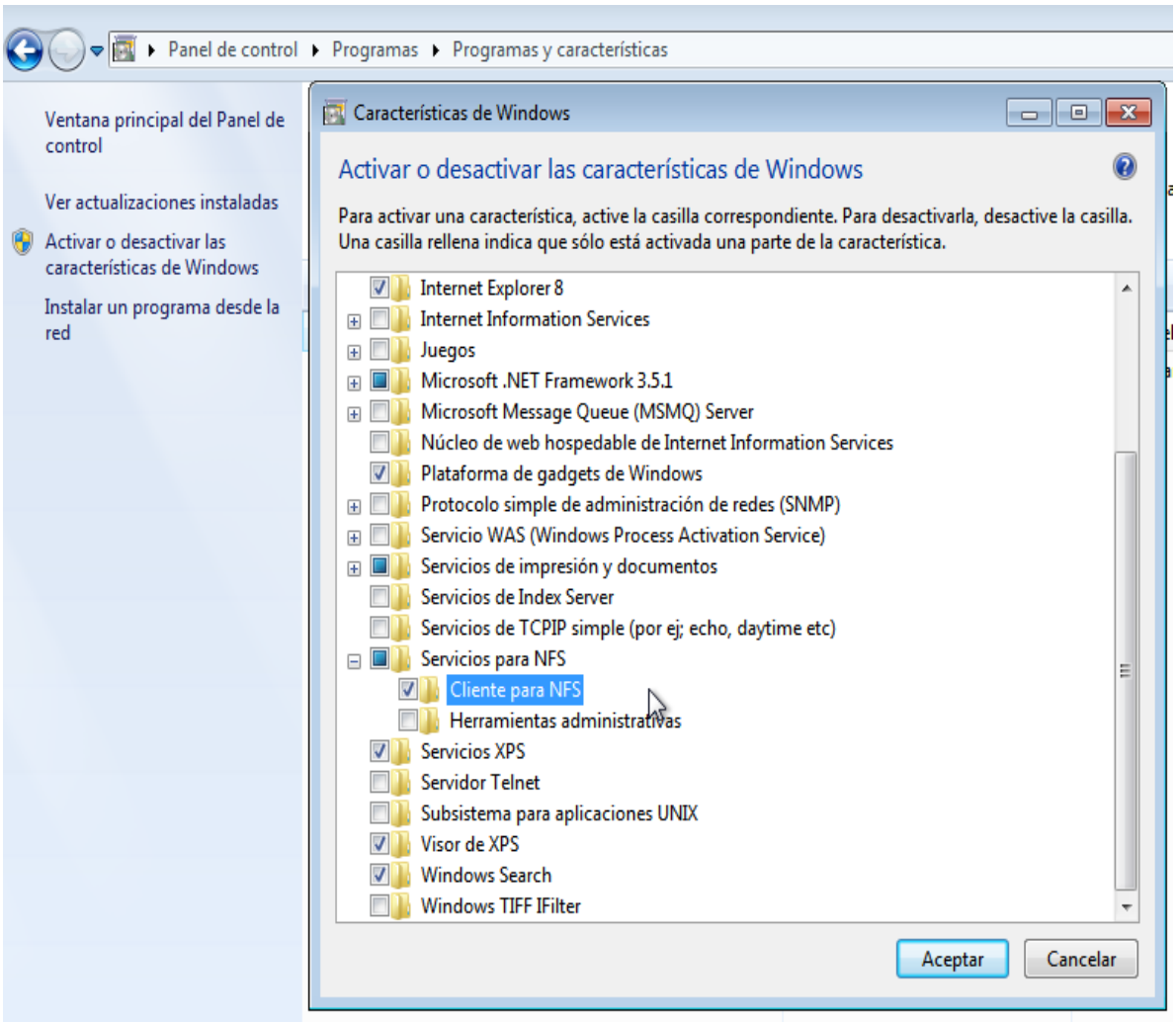
```
wheezy login: prueba1
Password:
prueba1@wheezy:~$ pwd
/home/prueba1
prueba1@wheezy:~$ mkdir pruebadir
prueba1@wheezy:~$ touch prueba.txt
prueba1@wheezy:~$ ls -l
total 4
drwxr-xr-x 2 prueba1 Domain Users 4096 jun 12 11:54 pruebadir
-rw-r--r-- 1 prueba1 Domain Users    0 jun 12  2014 prueba.txt
```

Hemos creado un directorio y un fichero para comprobar que tenemos permiso de escritura en */home/prueba1* y que se crean con los permisos, propietario y grupo correspondientes.

7.3. Cliente NFSv4 en Windows7

Vamos a instalar el cliente para NFS de Windows para tener acceso a los directorios exportados por el servidor NFS configurado en *samba4.* El cliente para NFS de Windows7 solo está disponible en las versiones Ultimate y Enterprise.

Para instalar el Cliente para NFS debemos acceder a *Panel de control* > *Programas* > *Programas y características* y seleccionamos la opción *Activar o desactivar las características de Windows.* En la nueva ventana nos desplazamos hasta la casilla *Servicios para NFS* y dentro de ésta seleccionamos la casilla *Cliente para NFS.* Aceptamos y esperamos hasta que finalice.



Para iniciar el servicio NFS desde la línea de comandos abrimos un símbolo del sistema con privilegios de Administrador y escribimos:

```
C:\Windows\system32>nfsadmin client localhost start
```

Podemos ver la configuración por defecto del cliente NFS mediante el siguiente comando:

```
C:\Windows\system32>nfsadmin client localhost config

Los siguientes forman la configuración en localhost

Protocolo                                   : TCP+UDP
Tipo de montaje                             : SOFT
Distingue mayúsculas de minúsculas          : No
Reintentos                                  : 1
Tiempo de espera                            : 8 segundos
Tamaño de búfer de lectura                  : 32 KiloBytes
Tamaño de búfer de escritura                : 32 KiloBytes
Usar puertos reservados                     : sí
Tipos de seguridad          : sys,krb5,krb5i

Configuración de archivo
               Usuario                      : rwx
               Grupo                        : r-x
               Otros                        : r-x
```

De esta configuración vamos a modificar el *Tipo de seguridad* para permitir solo el montaje con seguridad kerberos *krb5i.* Para ello deshabilitamos *sys* y *krb5.*

```
C:\Windows\system32>nfsadmin client localhost config SecFlavors=-sys -krb5
```

El acceso a los servidores de archivos de Network File System (NFS) requieren identidades de usuario y grupo de estilo UNIX, que no son iguales a las identidades de usuario y grupo de Windows. Para permitir a los usuarios el acceso a los recursos compartidos de NFS, Cliente para NFS de Windows puede recuperar datos de identidad de estilo UNIX de Active Directory (si el esquema incluye los atributos adecuados) o de un servidor de Asignación de nombres de usuario. Si ninguna de estas dos opciones está configurada, el Cliente para NFS intentará obtener acceso a los recursos de NFS de forma anónima.

En nuestro caso vamos a recuperar los datos de identidad de estilo Unix usando Active Directory. Desde línea de comandos escribimos:

```
C:\Windows\system32>nfsadmin mapping localhost config adlookup=yes
addomain=asir.local
```

La configuración del cliente NFS queda de la siguiente manera:

```
C:\Windows\system32>nfsadmin mapping localhost
Los siguientes forman la configuración en localhost
```

```
Búsqueda de servidor de asignaciones        : Deshabilitado
Servidor de asignaciones                    :
Búsqueda de AD                              : Habilitado
Dominio AD                                  : asir.local
```

Una vez configurado el Cliente para NFS, ya podemos montar los recursos compartidos ofrecidos por el servidor NFS.

```
C:\Users\prueba1>showmount -e samba4.asir.local
Lista de exportaciones en samba4.asir.local:
/nfs4                          10.0.0.0/24
/nfs4/home                     10.0.0.0/24
```

Lo que nos interesa es tener acceso al directorio del usuario que inicia sesión en el cliente Windows7. En este caso hemos iniciado sesión con el usuario *prueba1* y vamos a montar su directorio particular */nfs4/home/prueba1*. Podemos asignarle una letra de unidad, o indicar un asterisco (*) para que el sistema lo monte en la primera letra disponible, en este caso la unidad Z.

```
C:\Users\prueba1>mount -o sec=krb5i samba4.asir.local:/srv/nfs4/homes/prueba1
*
Z: está conectado ahora correctamente a
samba4.asir.local:/srv/nfs4/homes/prueba
1
El comando se completó correctamente.

C:\Users\prueba1>mount

Local    Remoto                                          Propiedades
-------------------------------------------------------------------------------
-
Z:       \\samba4.asir.local\nfs4\home\prueba1      UID=2001, GID=2000
                                                    rsize=32768, wsize=32768
                                                    mount=soft, timeout=0.8
                                                    retry=1, locking=yes
                                                    fileaccess=755, lang=ANSI
                                                    casesensitive=no
                                                    seg.=krb5i
```

Ejecutando *mount* podemos ver las características del montaje. Observamos que el UID y GID corresponden al usuario *prueba1* y que el tipo de seguridad es *krb5i.*

En el apartado *Directivas de grupo* crearemos una política de grupo para que cada usuario monte su directorio HOME al inicio de sesión y le asigne la unidad Z.

8. Administración remota del dominio con RSAT (Remote Server Administration Tools)

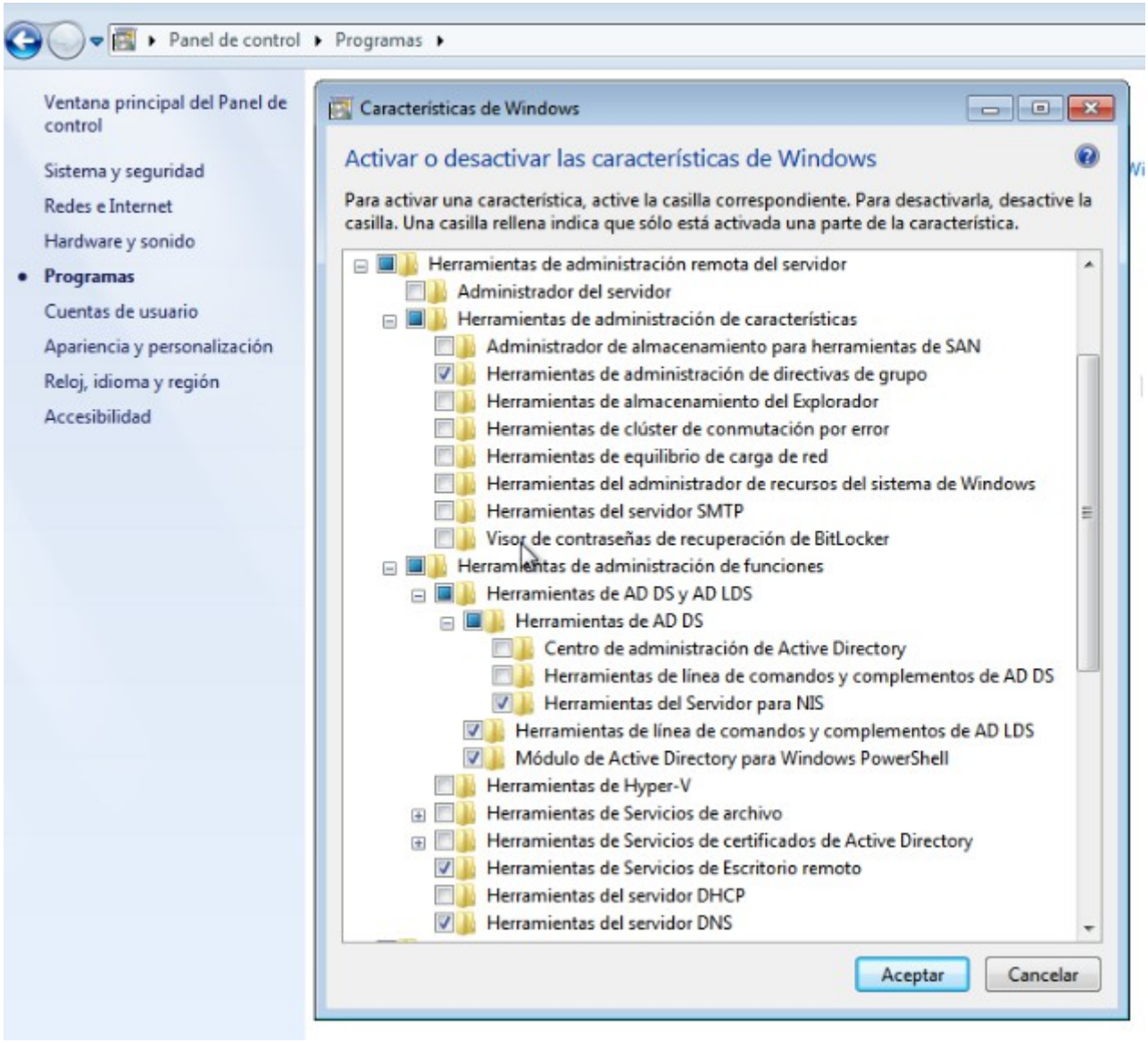
Una manera más gráfica de administrar un Dominio Samba y el Directorio Activo es usando las Herramientas de Administración Remota del Servidor en un equipo con Windows. RSAT es un paquete gratuito disponible para Windows7 y Windows8 que permite administrar el controlador de dominio de la misma manera que lo haríamos en Windows 2008 Server.

Anteriormente, en nuestro AD DC *samba4* hemos utilizado el comando *samba-tool* para realizar muchas labores de administración del servidor. Pero hay otras funciones como la administración de las directivas de grupo (GPO) para las que necesitamos de RSAT.

8.1. Instalación de RSAT

En un equipo con Windows 7 descargamos el paquete de Herramientas de administración remota del servidor para Windows 7 desde el Centro de descarga de Microsoft http://www.microsoft.com/es-ES/download/details.aspx?id=7887

Una vez instalado nos dirigimos a *Panel de control* > *Programas* > *Activar o desactivar las características de Windows* y expandimos las *Herramientas de administración remota del servidor.* Seleccionamos las características que necesitemos, en nuestro caso hemos activado las siguientes:

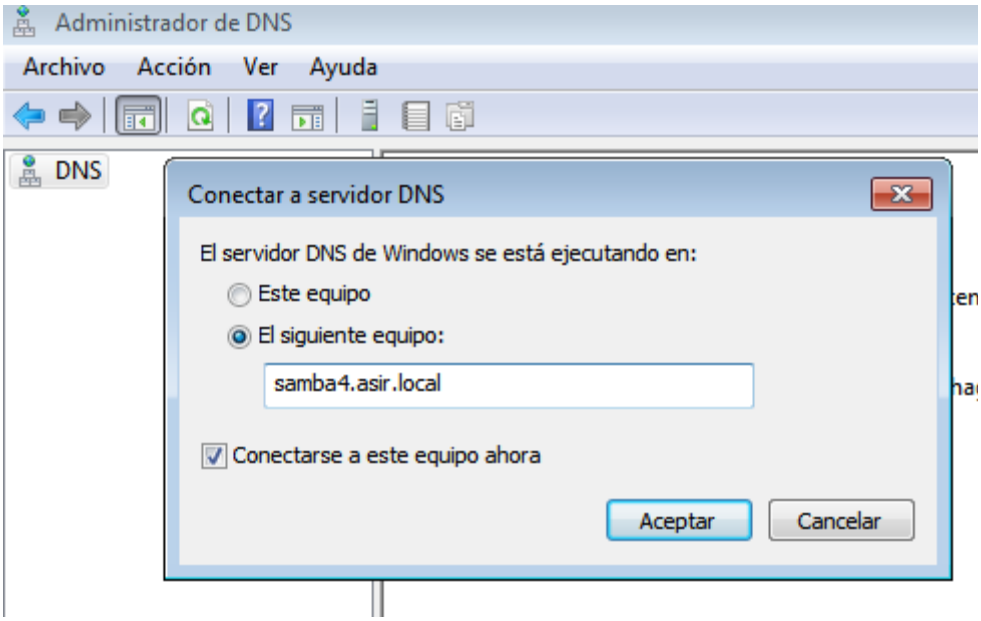


Una vez finalizada la instalación, podemos acceder a las nuevas herramientas de administración desde *Panel de control* > *Sistema y seguridad* > *Herramientas administrativas.*

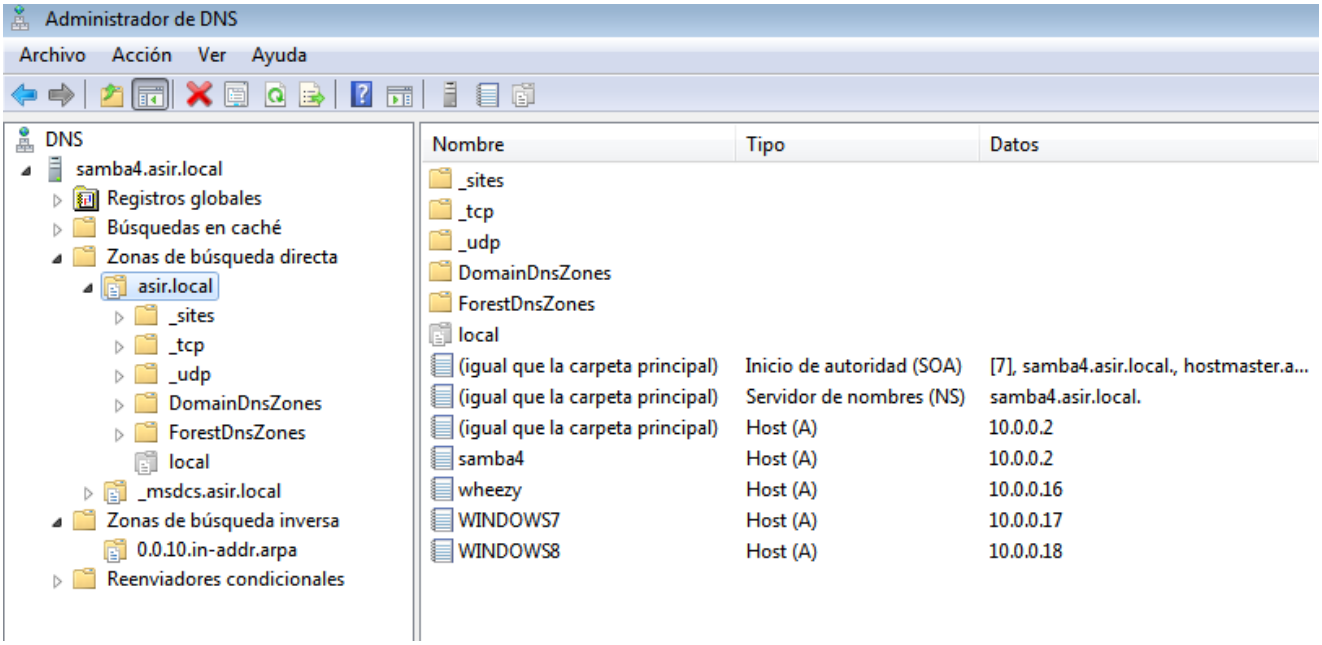
9. Administración del dominio

9.1. Administración DNS en Windows

Con RSAT instalado nuestro equipo Windows7 ya podemos conectarnos al servidor DNS de nuestra red y realizar las tareas de gestión y configuración del DNS. Para ello accedemos a *Panel de control* > *Sistema y seguridad* > *Herramientas administrativas* > *DNS.* Dentro del administrador de DNS hacemos clic en el menú *Acción* > *Conectar a servidor DNS...* y escribimos el nombre o IP del servidor DNS de la red.



Una vez conectados al servidor DNS, podemos administrarlo de la misma forma que haríamos en un equipo Windows Server.



En la imagen podemos ver la zona de búsqueda directa *asir.local* y la zona de búsqueda inversa *0.0.10.in-addr.arpa* de nuestro dominio.

9.2. Administración DNS en Linux

Para gestionar el DNS en nuestro servidor *samba4* contamos con la herramienta *samba-tool.*

Crear una nueva zona

```
samba-tool dns zonecreate <server> <zone> [options]

# samba-tool dns zonecreate samba4.asir.local asir.local
```

Eliminar una zona

```
samba-tool dns zonedelete <server> <zone> [options]

# samba-tool dns zonedelete samba4.asir.local 1.168.192.in-addr.arpa
```

Crea un registro

```
samba-tool dns add <server> <zone> <name> <A|PTR|CNAME|NS|MX|SRV|TXT> <data>

# samba-tool dns add samba4.asir.local asir.local nuevo A 10.0.0.30
```

Eliminar un registro

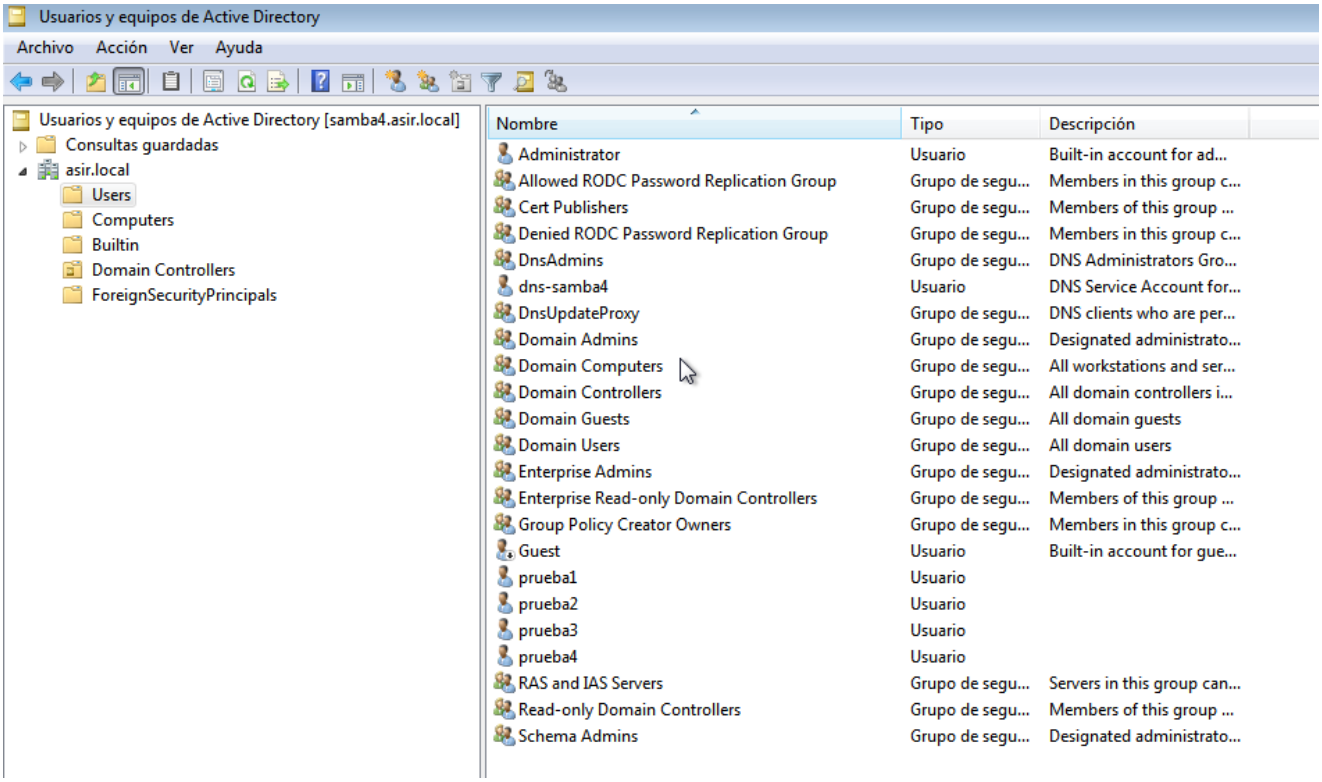
```
samba-tool dns delete <server> <zone> <name> <A|AAAA|PTR|CNAME|NS|MX|SRV|TXT>
<data>

# samba-tool dns delete samba4.asir.local asir.local nuevo A 10.0.0.30
```

Actualizar un registro

```
samba-tool dns update <server> <zone> <name> <A|PTR|CNAME|NS|MX|SOA|SRV|TXT>
<olddata> <newdata>

# samba-tool dns update samba4.asir.local asir.local nuevo A 10.0.0.30
10.0.0.31
```

9.3. Gestión de usuarios y equipos del Directorio Activo

Podemos gestionar el directorio activo con RSAT a través de *Panel de control > Sistema y seguridad > Herramientas administrativas > Usuarios y equipos de Active Directory.* Al igual que en Windows Server, podremos crear y modificar usuarios, equipos, unidades organizativas,etc.



9.4. Gestión de usuarios y grupos en Linux/Unix

En uno de los apartados anteriores ya usamos el comando *samba-tool* para crear un usuario de prueba. Vamos a mostrar alguno de los subcomandos más utilizados para la administración de usuarios y grupos.

Crear un usuario

```
# samba-tool user add prueba5 --uid-number=2005 --gid-number=2000 –login-shell=/bin/bash  \
--home-directory=/home/prueba5
New Password:
```

Eliminar un usuario

```
# samba-tool user delete prueba5
```

Cambiar contraseña del usuario

```
# samba-tool user setpassword prueba5
New Password:
```

Listar todos los usuarios

```
# samba-tool user list
Administrator
dns-samba4
prueba1
prueba2
prueba3
```

```
prueba4
prueba5
krbtgt
Guest
```

Crear un grupo

```
# samba-tool group add grupoA
```

Añadir miembros a un grupo

```
# samba-tool group addmembers grupoA prueba4,prueba5
```

Listar miembros de un grupo

```
# samba-tool group listmembers grupoA
prueba4
prueba5
```

10. Perfiles móviles

Los perfiles móviles contienen los entornos de trabajo de los usuarios, que incluyen la configuración y los elementos del escritorio. Algunos ejemplos de lo que contienen estos entornos son el fondo de escritorio, la configuración del ratón, el tamaño y posición de las ventanas, y las conexiones de impresora y de red.

10.1. Compartir el directorio *perfiles*

En el servidor *samba4* creamos un directorio donde almacenar los perfiles de cada usuario y le asignamos permisos de escritura para los usuarios del dominio.

```
# mkdir /usr/local/samba/var/perfiles
# chown :Domain\ Users /usr/local/samba/var/perfiles
# chmod 770 /usr/local/samba/var/perfiles
```

Para compartir el directorio *perfiles* con permiso de escritura editamos el fichero de configuración de samba añadiendo las siguientes líneas:

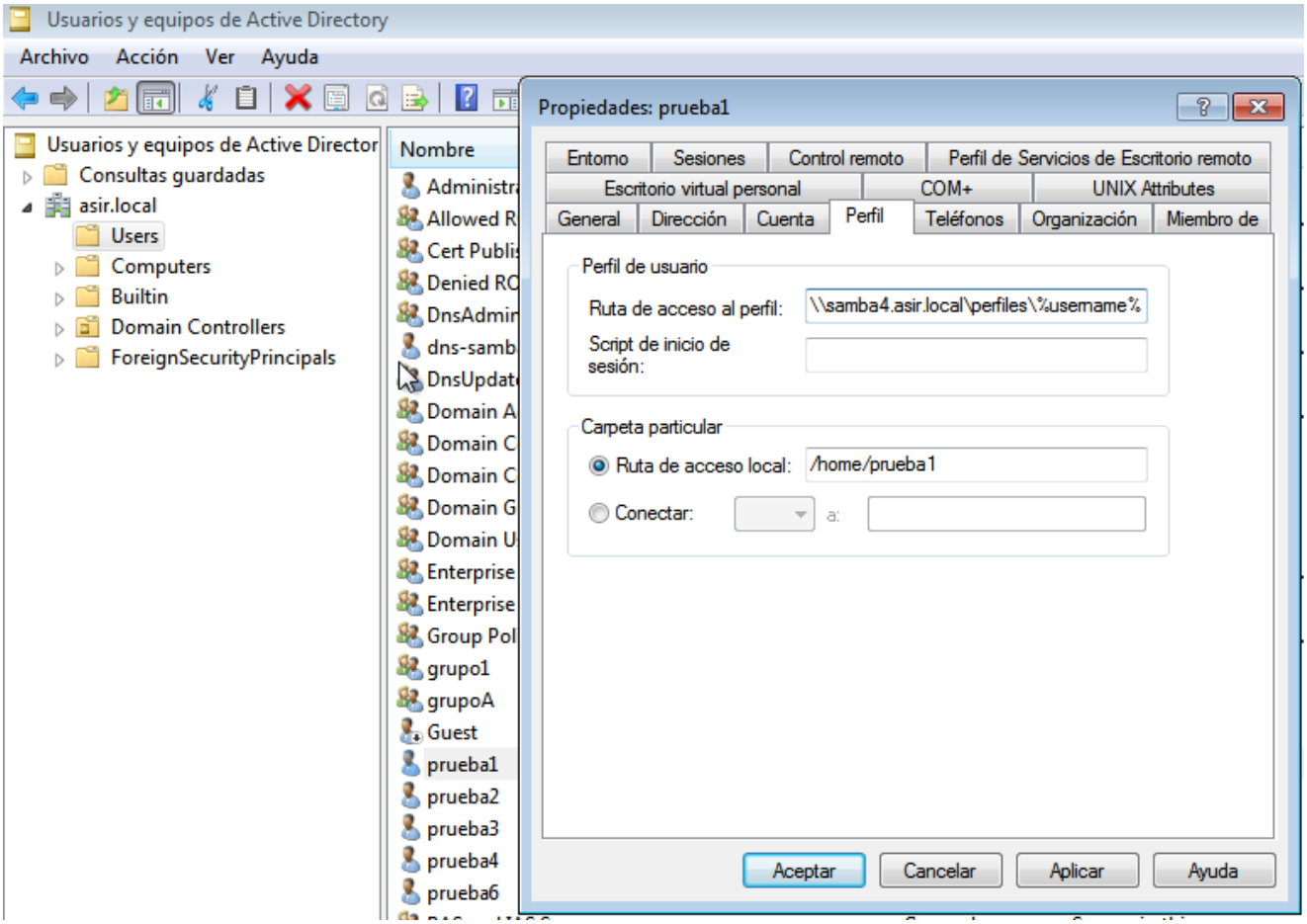
Fichero: /usr/local/samba/etc/smb.conf

```
[perfiles]
        path = /usr/local/samba/var/perfiles
        read only = No
```

10.2. Configuración del perfil móvil

Podemos configurar la ruta de acceso al perfil de cada usuario del dominio desde Windows usando la herramienta administrativa *Usuarios y equipos de Active Directory.*

Accedemos a las *Propiedades* del usuario, a la pestaña *Perfil* y escribimos la ruta en la casilla *Ruta de acceso al perfil:* \\samba4.asir.local\perfiles\%username%



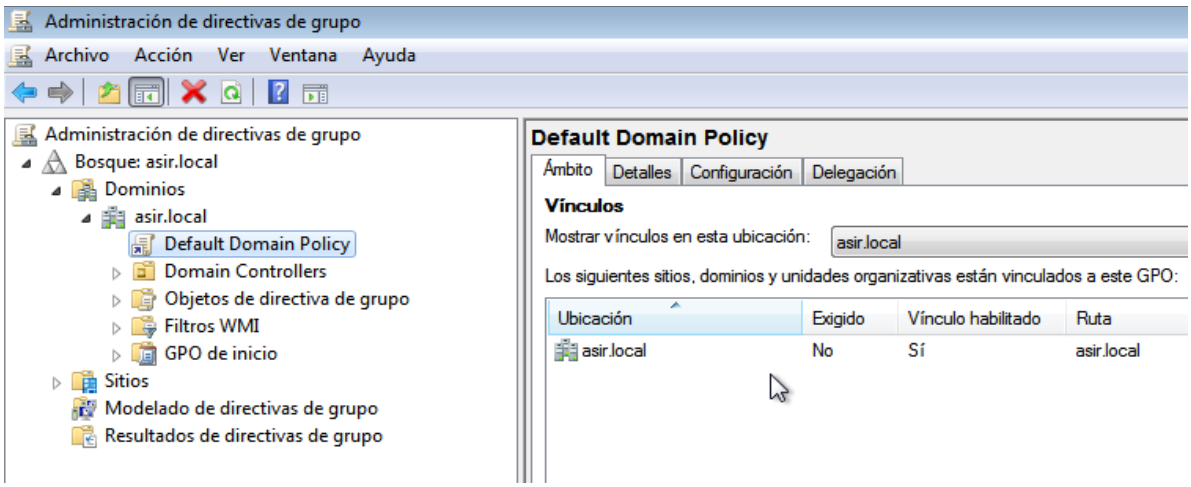
También tenemos la posibilidad de configurar la ruta de acceso al perfil desde el servidor cuando creamos un nuevo usuario, indicándolo mediante el atributo *profilePath.*

```
# samba-tool user add prueba1 --uid-number=2001 –gid-number=2000 \
--login-shell=/bin/bash –home-directory=/home/prueba1 \
--profile-path="\\\samba4.asir.local\perfiles\prueba1"
```

11. Directivas de grupo

La directiva de grupo es una de las principales razones para implementar Active Directory, ya que permite administrar objetos de usuarios y equipos. Las Directivas de Grupo permiten definir diversas configuraciones del usuario que accede al sistema o del equipo desde el cual se accede, de modo que podemos determinar cuales le serán aplicadas a cada usuario y/o equipo de un Sitio, Dominio o Unidad Organizativa.

Vamos a administrar las directivas de grupo desde nuestro equipo Windows7 con RSAT. Accedemos a *Panel de control > Sistema y seguridad > Herramientas administrativas > Administración de directivas de grupo.*



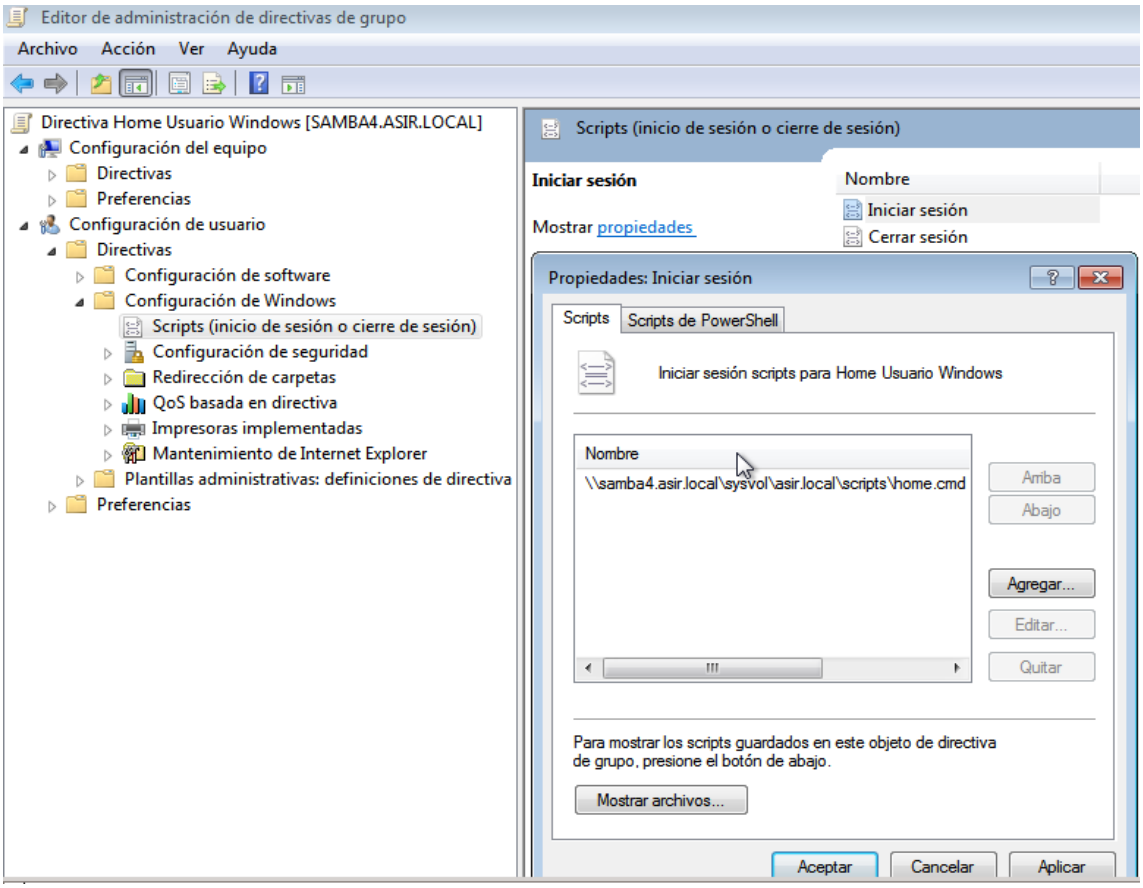
Por defecto tenemos la directiva *Default Domain Policy* que afecta a todo el dominio *asir.local.*

11.1. Configuración del HOME del usuario en Windows

Vamos a crear un GPO para que cada usuario que inicie sesión en un equipo Windows monte su directorio HOME y le asigne la unidad Z.

Para crear el GPO hacemos clic derecho sobre el dominio *asir.local* y seleccionamos *Crear un GPO en este dominio y vincularlo aquí...* En la nueva ventana le asignamos un nombre, por ejemplo *Home Usuario Windows.*

Una vez creado, hacemos clic derecho sobre el nuevo GPO y seleccionamos *Editar...* para acceder al *Editor de administración de directivas de grupo.*En esta nueva ventana navegamos hasta *Configuración de usuario > Directivas > Configuración de Windows > Scripts (inicio de sesión o cierre de sesión)* y elegimos el elemento *Iniciar sesión.*



En las propiedades del elemento *Iniciar sesión* agregamos el script correspondiente ubicado en la ruta \\samba4.asir.local\sysvol\asir.local\scripts\home.cmd siendo el contenido de este script el siguiente:

Fichero: home.cmd

```
mount -o sec=krb5i samba4.asir.local:/srv/nfs4/homes/%username% Z:
```

12. Referencias

Wiki Samba

https://wiki.samba.org/index.php/Main_Page

Wiki Samba – Samba4/LDBIntro

https://wiki.samba.org/index.php/Samba4/LDBIntro

Ubuntu Manuals – SSSD

http://manpages.ubuntu.com/manpages/natty/man8/sssd.8.html

Wiki Debian – NFS4/Kerberos

https://wiki.debian.org/NFS/Kerberos

Microsoft Technet – Administración de Cliente NFS para NFS

http://technet.microsoft.com/es-es/library/cc771698.aspx