Instalación de ldap – Samba.

Ignacio Barrancos Martínez
ignacio@adesx.com

Contenido

1.Introducción..... 1
2.Instalando paquetes..... 2
2.1.Respondiendo a debConf..... 2
3.Configurando los diferentes servicios..... 3
3.1.El demonio de OpenLDAP..... 3
3.1.1.Primera copia de seguridad..... 4
3.1.2.Estructura inicial del árbol..... 4
3.1.3.Explorando nuestro directorio..... 5
3.2.El cliente linux de OpenLDAP..... 6
3.2.1.Instalando y personalizando los comandos de Idealx..... 6
3.3.Configuración de Samba 3..... 8
3.3.1.El fichero de samba: smb.conf..... 9
3.3.2.Encriptando contraseñas..... 12
3.4.Configurando libnss-ldap..... 13
3.5.Configurando pam..... 13
4.Conclusiones y TODO..... 14

1. Introducción

Aquellos Linuxeros que tenemos la suerte o la desgracia de tener que trabajar habitualmente con Windows, nos vemos en la necesidad de configurar prioritariamente Samba. Samba nos ofrece conectividad Linux vs Windows de una manera eficiente.

Si lo que se quiere es montar un pequeño servidor departamental o destinado a una PYME, basado en Linux, y sustituir con él los Windows Servers que hubiera en la red, muchas veces resulta muy molesto andar añadiendo usuarios al sistema (`/etc/passwd`) para cada los usuarios del dominio y los clientes Windows. Para evitar este molesto efecto colateral, la mejor opción de la que disponemos es de OpenLDAP integrado con Samba.

Este documento describe cómo instalar y configurar *OpenLDAP* y *Samba 3*, como servidor de ficheros e impresión (*CPUS*) sobre *Debian Woody 3*.

Los documentos en los que me basé para llevarlo a cabo, fueron los siguientes

- http://www.slag.it/documenti/samba3_ldap_pdc/samba3_ldap_pdc_howto.php. Describe cómo instalar OpenLDAP y Samba 3 en Woody. Si se sigue por completo, no funciona bien: Al final los usuarios no entran bien en el dominio, porque no habla de la configuración de `pam` .

- http://aqua.subnet.at/~max/ldap/ Aunque no habla mucho de la instalación de samba, y *(creo que no termina de funcionar)*, sí que tiene muy bien la parte de `pam`.

- Buscar en Google: *"Ignacio Coupeau"* Lo estuve mirando, y seguirlo es un lío tremendo: Primero la instalación creo que es sobre RedHat y segundo habla de Samba 2.X (últimas versiones). No me interesa.

2. Instalando paquetes

Lo primero, sería añadir a `/etc/apt/sources.list`, como usuario **`root`**:

```
#-Samba 3
deb http://www.backports.org/debian stable samba
```

... y luego ejecutar ...

```
apt-get update
apt-get install samba samba-doc \
                ldap-server ldap-utils \
                libpam-ldap libnss-ldap \
                libnet-ldap-perl nscd
```

darle unos minutillos hasta que descargue todo.

2.1. Respondiendo a debConf

Una vez haya terminado de copiar paquetes, debconf empezará a interrogarnos para que le indiquemos cómo configurar el montón de cosas que ha descargado. Procederemos de la siguiente forma.

- **Samba Server**: Responder a todas las preguntas, con la opción por defecto que proponga debConf. Luego le sustituiremos el archivo de configuración (`/etc/samba/smb.conf`) por completo, con lo que dará un poco igual lo que respondamos.
- **Configuring Libnss-ldap**
  1. **The address of the LDAP server used**: 127.0.0.1 y luego <Ok>.
  2. **The distinguished name of the search base**: *"dc=adesx,dc=com"* y luego <Ok>. Esta será la raíz de nuestro árbol.
  3. **LDAP version to use**: Seleccionar *"3"* y luego <Ok>.
  4. **database requires login**: Pulsar en <No>.
  5. **make configuration readable/writeable by owner only**: Elegir <No>.
  6. **unprivileged database user**: Teclear *"cn=invitado,dc=adesx,dc=com"* y luego <Ok>. Ahora pedirá dos veces la contraseña para este usuario, pondremos una tontorrona como *"qwerty123"* .
  7. **nsswitch.conf is not managed automatically**: Pulsar <Ok>, porque no hay otra opción: Luego lo editaremos.
- **Configuring Libpam-ldap**
  1. **Make local root Database admin**: Pulsar <Yes>.
  2. **Database requires logging in**: Seleccionar <No>.
  3. **Root login account**: *"cn=admin,dc=adesx,dc=com"* y luego <Ok>. Esta es la cuenta del administrador del directorio. Cuando pida la contraseña, le meteremos una contraseña más importante, como puede ser la del root del sistema. Yo en mi caso lo he hecho así, pero no es muy recomendable.

4. **Unprivileged database user**: *"cn=invitado,dc=adesx,dc=com"* y luego <Ok>, y le volvemos a poner la contraseña flojita: *"qwerty123"* .

5. **nds - Use Novell Directory Services-style updating, ...**: Pulsar en <Ok>, no hay otra opción.

6. **Local crypt to use when changing passwords**: Seleccionar *"crypt"* y luego <Ok>. Como tendremos que trastear a mano ciertas contraseñas, es preferible de momento, usar crypt para encriptar los passwords.

- **OpenLDAP configuration**

1. **Directory initialization method**: Seleccionar *"auto"* y luego <Ok>. Si ya estamos hartos de crear directorios, podemos elegir la opción *"ldif"* y crear nuestro árbol a mano, a través de archivos ldif. Como esto es una guía rápida, usaremos la primera opción.

2. **Directory suffix style**: Seleccionar *"domain or host"* y luego <Ok>.

3. **Enter the domain name**: Teclear *"adesx.com"* y luego <Ok>. Nos pedirá dos veces la contraseña del administrador del árbol (pusimos la misma que la del root de linux).

4. **Replicate to another LDAP server**: Seleccionar <No>.

5. **LDAP server**: Teclear *"helicon.adesx.com"* y luego <Ok>.

6. **bind DN**: Dejar en blanco y pulsar <Ok>, más adelante se configurará. Después nos pedirá dos veces el password del administrador del árbol (la del root de la máquina): La tecleamos.

3. Configurando los diferentes servicios

Una vez hemos terminado de instalar y configurar los paquetes descargados, empezaremos a configurar uno a uno los diferentes servicios, y siempre como usuario **`root`**.

3.1. El demonio de OpenLDAP

Lo primero que se hará será añadir el *`schema`* de Samba a OpenLDAP. Para ello:

```
su -
cd /etc/ldap/schema
cp /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz .
gunzip samba.schema.gz
```

Una vez hecho esto, se editará el fichero */etc/ldap/slapd.conf* y añadiremos la siguiente línea junto a los otros includes:

```
include     /etc/ldap/schema/samba.schema
```

Dentro de este mismo fichero, ir a la sección *"# Indexing options"* y sustituir la línea similar a la siguiente...

```
 index objectClass eq
```

...por las siguientes ...

```
index objectClass,uid,uidNumber,gidNumber eq
index cn,mail,surname,givenName eq,subinitial
```

con ello estaremos diciendo a *slapd* que genere índices en la base de datos, para los atributos mencionados: ello repercutirá en velocidad en las consultas. Guardamos los cambios y salimos de la edición del fichero.

Se reiniciará el servicio y regenerarán los índices, mediante:

```
/etc/init.d/slapd stop
slapindex
/etc/init.d/slapd start
```

Ahora deberíamos tener abierto el puerto TCP 389, lo cual nos indicará que está arriba el servicio de Ldap. Se puede comprobar mediante `nmap localhost` o el comando `netstat`.

3.1.1. Primera copia de seguridad

En este momento, se supone que ya se tiene configurado el servicio de Directorio. Antes de continuar, convendría tener los archivos que conforman la base de datos del directorio, en una copia de respaldo, para poder volver atrás en cualquier momento, si bien, siempre podremos volver a empezar con `dpkg-reconfigure libnss-ldap`. Si queremos tener copia de seguridad, podremos teclear ...

```
cp -R /var/lib/ldap  ~/var_lib_ldap_incial
```

3.1.2. Estructura inicial del árbol

Dado que el objetivo será configurar el servicio Samba para que se autentique contra el servicio de directorio, se crearán los siguientes contenedores iniciales, por guardar un poco la similitud a como lo hace Active Directory:

- **Grupos**: Contenedor de los Grupos de cuentas de usuario de Samba; En Active Directory sería el conjunto de los grupos globales.
- **Gente**: Contenedor para almacenar las diferentes cuentas de usuarios; En Active Directory serían el conjunto de usuarios del dominio.
- **Equipos**: Contenedor para albergar las cuentas de acceso asociadas a cada una de las estaciones de trabajo clientes, de nuestro futuro dominio Samba; En Active Directory sería equivalente a la colección *Computers*.

Para ello, creamos un archivo `~/mi-active-base.ldif` con el siguiente contenido.

```
dn: ou=Grupos,dc=adesx,dc=com
objectClass: top
objectClass: organizationalUnit
ou: Grupos

dn: ou=Gente,dc=adesx,dc=com
objectClass: top
objectClass: organizationalUnit
ou: Gente

dn: ou=Equipos,dc=adesx,dc=com
objectClass: top
objectClass: organizationalUnit
ou: Equipos
```

No estaría demás que se dejara una copia de este archivo en `/etc/ldap`, con el fín de tener por duplicado y centralizada esta configuración *post-inicial*. Estando arrancado el servicio de de ldap, ejecutamos...

```
ldapadd -x -h localhost -D "cn=admin,dc=adesx,dc=com" -f base.ldif -W
Enter LDAP Password:
adding new entry "ou=Grupos,dc=adesx,dc=com"
adding new entry "ou=Gente,dc=adesx,dc=com"
adding new entry "ou=Equipos,dc=adesx,dc=com"
```

3.1.3. Explorando nuestro directorio

Llegado este momento ya estaríamos en condiciones de poder curiosear entre los objetos de nuestro directorio. Para ello, necesitaremos de un explorador de LDAP. Aunque no he ahondado mucho en Google, encontré 2 herramientas:

- http://www.maxware.com/download/?code=1083491880, cliente para Windows que se integra con el escritorio, de la misma manera que el entorno de red. Se puede descargar la versión de evaluación para 30 días: cuando nos solicite la dirección de correo, indicaremos `ibarrancos@exagroup.com`
- Ldap Viewer, cliente para java para Linux, que no recuerdo la Url, ni la tengo localizada.

Para ilustrar este documento usaremos el cliente de Maxware, desde una estación Windows. Si accedemos en el explorador de Windows a la pestaña de arriba (barra de direcciones) y le pinchamos al combo, veremos como más abajo del *escritorio*, y del *entorno de red*, aparece una entrada llamada `maxware`. Pinchamos en ella, y luego en *"add directory server"* . Los parámetros serán los siguientes:

- En la pestaña de `Server`:
  - **Server name**: helicon *(sólo es el nombre que queremos darle a esta configuración)*
  - **Server addres**: 192.168.1.20 *(la dirección IP del servidor donde hemos montado LDAP)*
  - **LDAP version**: 3 *(está claro, así lo dejamos configurado con debconf)*
  - **Port number**: Default *(para que use el puerto por defecto, el 389)*
- En la pestaña de `Login`, marcar la opción **Explicit**, y luego en el resto de campos poner...
  - **Login user name**: `cn=admin,dc=adesx,dc=com` *(será la cadena que identifique la cuenta del administrador del árbol)*
  - **Login passowrd**: Teclearemos la contraseña del administrador del árbol, presumiblemente la del root.
  - **Security options**: Simple
- En la pestaña de `Directory`...
  - **Start node (DN)**: `dc=adesx,dc=com` *(será el raíz de nuestro árbol)*
  - **Search filter**: `(objectclass=*)`.
  - **Max. entries to return, Timeout, Entries per page**: Dejar todos con el valor de `50`.
- En la pestaña de `Advanced` dejar las opciones por defecto.

Luego pulsar los botones de *"Aplicar"* y *"Aceptar"* . Una vez se cierre la ventana, si hacemos doble click sobre helicon (el servidor de ldap que se ha instalado y configurado, veremos cómo ya aparecen los objetos que se acaban de crear).

Aquellos objetos que no creamos y que aparecen (*People*, y *Roaming*), será porque le dijimos a *debconf* que creara el árbol **auto**máticamente y no mediante *ldif* de manera manual.

3.2. El cliente linux de OpenLDAP

En este punto de la instalación se debe configurar el cliente OpenLDAP para que acceda al directorio LDAP que se acaba de crear: Esto se necesitará cuando debamos configurar libpam más tarde.

Para ello, editar el archivo `/etc/ldap/ldap.conf` y añadir las siguientes líneas:

```
HOST 127.0.0.1
BASE dc=adesx,dc=com
```

Se podrá testear la conexion mediante

```
ldapsearch  -x
```

Ahora se editará el fichero `/etc/nsswitch.conf`, y nos aseguraremos de añadir a las líneas `passwd`,`group` y `shadow` la entrada para ldap, quedando algo similar a lo siguiente:

```
passwd: ldap compat
group: ldap compat
shadow: ldap compat
```

3.2.1. Instalando y personalizando los comandos de Idealx

Idealx es una empresa francesa destinada a la venta servicios basados en Open Source, que cuenta entre sus principales clientes a varios ministerios del gobierno francés, Leroy-Merlyn, Alcatel o Canal Plus Francia. Entre otras aportaciones a la comunidad, se encuentra el SMB-LDAP PDC Howto que describe cómo configurar Samba2 con Ldap para convertirlo en un PDC.

Con el fín de facilitar la administración del conjunto, implementaron un conjunto de scripts perl que interactuaban con Ldap, para crear los objetos del dominio Samba. La persona que mantiene el backport de Samba3 para Woody, tuvo la genial idea de incluirlos en el mismo, con lo que no tendremos que descargarlos de manera separada. Para ello...

```
cd /usr/local/sbin
cp /usr/share/doc/samba-doc/examples/LDAP/smbldap-tools/*.p*.gz .
cp /usr/share/doc/samba-doc/examples/LDAP/smbldap-tools/*.pl .
gunzip *.gz
chmod u+x smbldap*pl
```

Ahora necesitaremos compilamos el comando `mkntpwd`.

```
cd /usr/share/doc/samba-doc/examples/LDAP/smbldap-tools/mkntpwd
gunzip *.gz
make
cp mkntpwd /usr/local/sbin
chmod u+x /usr/local/sbin/mkntpwd
```

Cuando una persona trabaja en la administración de Windows (*la verdad es que no hay mucho que administrar, lo más complicado suele ser pulsar el botón de reset, que nunca terminas de atreverte porque dudas si arrancará el equipo o no*), termina acostumbrándose a la jerga: La palabra SID aparece hasta la infinidad cuando se habla de dominios, Active Directory y relaciones de confianza. **SID** es el abrevio de *Security IDentifier* y es un pedazo de chorizo que los productos *Microsoft (TM)* utilizan para identificar objetos de manera única. Cuando se están configurando redes *Microsoft (TM)*, cada equipo de la red, cada cuenta de usuario, cada grupo, etc, etc... tiene asociado un SID diferente, sobre el que se definen el resto de permisos, privilegios, etc, etc... en los registros de los controladores de dominio, PDCs, e incluso en los de los equipos clientes. Es por ello, que nuestro propio servidor Samba tendrá un SID asociado, y necesitamos conocerlo para configurar los scripts perl de Idealx. Para ello, ejecute como root:

```
helicon:~# net getlocalsid
SID for domain HELICON is: S-1-5-21-1583388958-2540867174-1836719564
```

No teclear la segunda línea: Esta será el resultado de ejecutar la primera, y nos mostrará el SID de nuestro servidor: Tomaremos nota de él.

Ahora editaremos el archivo `/usr/local/sbin/smbldap_conf.pm`, e iremos buscando cada una de las líneas donde se definen las siguientes variables, y sustituyéndolas por su valor, o por el valor que se propone a continuación.

```
$SID = "S-1-5-21-1583388958-2540867174-1836719564";
```

Está claro que aquí pondremos el SID resultante de haber ejecutado `net getlocalsid`. Seguimos sustituyendo valores de variables...

```
$suffix = "dc=adesx,dc=com"
$usersou = q(Gente);
$computersou = q(Equipos);
$groupsou = q(Grupos);
$hash_encrypt="CRYPT";
$binddn = "cn=admin,$suffix";
$bindpasswd = "XXXXX";
```

En vez de XXXXX habrá que poner la contraseña del administrador de Openldap en claro (la del root). Seguimos cambiando valores de variables:

```
$_userLoginShell = q(/bin/bash);
$_userHomePrefix = q(/home/samba);
```

Le pongo este directorio, porque como enseguida veremos, colgaré todo lo referente a samba (perfiles, buzones compartidos, directorios personales, drivers para impresoras, netlogon, etc...) a partir del directorio `/home/samba`. Seguimos actualizando las variables del fichero `/usr/local/sbin/smbldap_conf.pm` ...

```
$_defaultUserGid = 221;
$_defaultComputerGid = 300;
```

No lo tengo nada claro la relevancia de estos IDs. En principio los he dejado así, y no he tenido ningún problema.

3.3. Configuración de Samba 3

Ya estamos casi terminando. Ahora crearemos los directorios donde dejaremos todo los directorios que formarán parte de nuestro dominio. Como ya se adelantó, se dejarán todos a partir de `/home/samba`. Para ello,

```
mkdir -p -m 777 /home/samba/var
cd /home/samba/var
mkdir -p -m 777 comun netlogon perfiles print-drivers
```

El objetivo de cada directorio es ...

- `/home/samba`: En él se irán creando un directorio para cada uno de los usuarios de nuestro dominio, directorio que se supone que será privado, y sólo tendrá permisos de lectura/escritura en red, el propio usuario. *(Unidad de Red personal)*.

- `/home/samba/var/comun`: Buzón común a todos los usuarios del sistema: Todos van a poder leer y escribir en él.

- `/home/samba/var/netlogon`: Unidad de red donde se dejarán los scripts de Logon. Ya hablaremos mucho más de esto en futuras versiones de este documento. Un script de Logon típico para nuestro dominio podría ser un fichero .BAT con el siguiente contenido:

  ```
  @echo off
  net use M: \\Helicon\comun
  net use U: \\Helicon\personal
  ```

  Aunque mi predilección por kix32 para este fin, es muy superior a cualquier otra alternativa.

- `/home/samba/var/perfiles`: Cada usuario deberá tener una carpeta para albergar su perfil de Windows. Debo repasar el fichero de configuración, pero yo he conseguido con Samba3, que para cada usuario se almacene en directorio diferentes su perfil de Windows 9x, el 2000 y el de XP.

- `/home/samba/var/print-drivers`: Almacenará los drivers para Windows de las diferentes impresoras exportadas por Samba. Cada que lo he intentado, he terminado con principio de locura, pero lo conseguiré algún día.

Ahora se crearán los grupos iniciales de nuestro dominio, en plan Windows 2000. No tenemos porqué usar los nombres en inglés, pero deberíamos ser consecuentes con UID y GID que configuramos en `/usr/local/sbin/smbldap_conf.pm`,

```
smbldap-groupadd.pl -a -g 200 "Domain Admins"
smbldap-groupadd.pl -a -g 201 "Domain Users"
smbldap-groupadd.pl -a -g 202 "Domain Guests"
smbldap-groupadd.pl -a -g 220 "Administrators"
smbldap-groupadd.pl -a -g 221 "NT Users"
smbldap-groupadd.pl -a -g 222 "Guests"
smbldap-groupadd.pl -a -g 223 "Power Users"
smbldap-groupadd.pl -a -g 224 "Account operators"
smbldap-groupadd.pl -a -g 225 "Server operators"
smbldap-groupadd.pl -a -g 226 "Print operators"
smbldap-groupadd.pl -a -g 227 "Backup operators"
smbldap-groupadd.pl -a -g 228 "Replicator"
smbldap-groupadd.pl -a -g 300 "Hosts"
```

Como se puede ver, la ejecución de los comandos anteriores no ha modificado para nada el fichero `/etc/group`. También podemos echarle un vistazo al explorador del directorio (maxware) y observar cómo ha metido los grupos en el contenedor de Grupos. *Se nos va a quedar una cosa guapa, guapa, guapa.*

3.3.1. El fichero de samba: smb.conf

Ahora se debe editar el fichero de configuración de samba. Antes de hacer nada, deberíamos sacarle copia de seguridad al original, no vaya a ser que ...

```
cp /etc/samba/smb.conf  /etc/samba/smb.conf-original
```

y editamos el archivo `/etc/samba/smb.conf` para dejar todo este contenido. (He añadido comentarios para que quede más entendible:

```
#- Creado el 2/Mayo/2004, para ver como pitaba con OpenLadap.

#======================= Global Settings =====================

[global]

   # Nombre del dominio NT
   workgroup = adesx

   # Descripcion del equipo. Este se ve cuando estamos en el
   # entorno de red de Windows, con la vista de carpeta en
   # detalles.
   #  Los parametros son:
   #    %h = Nombre del host
   #    %v = La version instalada de samba.
   server string = Servidor %h (Samba %v)

   # Hace que el demonio NMBD haga de servidor Wins.
   wins support = yes

   # Lo dejamos comentado, porque esto es para decirle a Samba que
   # su servidor Wins esta en otro equipo. Se supone que aqui se le
   # mete la IP del servidor Wins. Pasamos, porque al ser propio
   # servidor, el que haga las veces de Wins, no se tiene que poner.
;   wins server = w.x.y.z

   # Esto es por si se recibiera el servidor Wins por el DHCP. Se deja
   # comentado porque no lo vamos a recibir por DHCP... Si somos nosotros!!
;   include = /etc/samba/dhcp.conf

   # Esto se supone que es para decirle al demonio nmdb que busque los
   # los nombres NetBIOS en DNS. De momento nos olvidamos de ello, que
   # los busque escuchando los broadcast de los Windows.
   dns proxy = no

   # Esto le dice a samba en que orden debe resolver la IP de los nombres
   # de los equipos. Por defecto viene comentado, yo lo descomento.
   name resolve order = lmhosts host wins bcast

#### Depurando problemas   ####

   # Le decimos que use logs diferentes para cada Cliente. Esto es
   # preferible cuando no se sabe muy bien, que va a pasar... asi
   # se puede ver lo que hace una maquina Windows 95 y una XP.
   log file = /var/log/samba/log.%m

   # Maxima capacidad (en Kb) del archivo de Log.
   max log size = 1000

   # Si queremos que samba solo tire logs en /var/log/messages. Lo dejo
   # como viene por defecto en la instalacion de Debian.
;   syslog only = no

   # Cuanta informacion en log quieres. Cuanto mayor sea el numero mas
   # informacion sacara en el log.
   syslog = 10

   # Para cuando pete samba. Lo dejo como viene por defecto para Debian.
   panic action = /usr/share/samba/panic-action %d
```

```
####### Autenticacion #######

   # Hay diferentes tipos de niveles de seguridad. Esta es la que de
   # momento usaremos.
   security = user

# You may wish to use password encryption.  See the section on
# 'encrypt passwords' in the smb.conf(5) manpage before enabling.
   # Lo dejo como viene por defecto. Creo que esto da problemas con
   # Windows 95, 98 y NT Service Pack 3 (y anteriores). El resto por
   # defecto envian las contraseñas encriptadas, pero se les puede
   # tocar en el registro para que las envien en claro.
   # Si hubiera estaciones Windows 95/98 habria que plantearse esto.
   encrypt passwords = true

   # Esto es para que busque en LDAP.
   passdb backend = ldapsam:ldap://127.0.0.1

   # No tengo ni idea de lo que hace, pero lo dejo a no, porque lo
   # vi en un tutorial para configurar LDAP y Samba.
   obey pam restrictions = no

   # Lo dejo por defecto como viene en Debian. No me complico.
;   guest account = nobody
   invalid users = root

   # Esto es para el sincronismo de contraseña. Lo dejo tal cual lo vi en
   # un tutorial de SAMBA y LDAP.
;   unix password sync = yes
   passwd program = /usr/local/sbin/smbldap-passwd.pl -o %u
   passwd chat = *new*password* %n\n *new*password* %n\n *successfully*


   # Lo dejo por defecto como viene en Debian. No me complico.
;   pam password change = no

########## Opciones para LDAP  ##########

   # Parametros para LDAP
   ldap suffix = dc=adesx,dc=com
   ldap admin dn = cn=admin,dc=adesx,dc=com
   ldap ssl = no
   ldap user suffix = ou=Gente
   ldap group suffix = ou=Grupos
   ldap machine suffix = ou=Equipos

########## Opciones para convertir Samba en PDC  ##########

   # Esto lo dice a los Windows que es un PDC, que se anden con
   # cuidao.
   os level = 33
   preferred master = yes
   domain master = yes
   local master = yes
   domain logons = yes

   # Para que los PCS se añadan automaticamente
   add machine script = /usr/local/sbin/smbldap-useradd.pl -w -d /dev/null -s /
bin/false %u

   # Donde se almacenan los perfiles
   #--- Propuesto por el tutorial
;   logon path = \\%N\Profiles\%u
   #--- Hecho para el Pelluz %U= Usuario que hace logon, %a=Tipo de Windows
   logon path = \\%L\Profiles\%U\%a

   # Unidad mapeada temporalmente por los usuarios mientras ejecutan
   # el script de logon
   logon drive = Y:

   # Script de Logon que ejecutara el usuario: El script se llamará igual que
   # el usuario.
   logon home = %u.bat

########## Impresion (servida por CUPS)  ##########

   # Le decimos a samba que si, que vamos a imprimir.
   load printers = yes
```

```
   # Que lo vamos hacer con CUPS.
   printing = cups
   printcap name = cups

   # Como consultar el estado de las impresoras e imprimir.
   lpq command = lpstat.cups -o %p
   lprm command = lprm.cups  %p-%j

   # No tengo ni idea. Lo dejo tal cual lo pone el debconf
;   printer admin = @ntadmin


########  Opciones para los nombres de ficheros  ########

   # Esto me dio problemas con Windows 95/98 y Samba 3 en
   # el Pelluz: Los nombres de los archivos quedaban hechos
   # una patata.
;   dos charset = ANSI
   unix charset = ISO-8859-1

   # Lo dejo como lo deja debconf.
;   preserve case = yes
;   short preserve case = yes


############ Miscelanea ############

   # Se supone que esto es para que cada cliente Windows tenga una
   # configuracion# personalizada. Paso de esto.
;   include = /home/samba/etc/smb.conf.%m

   # Opciones para los sockets. Lo dejo como viene por defecto
   # con debconf.
   socket options = TCP_NODELAY
   #--- En el Pelluz tenia...
;   socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192

   # Esto es para que funcionen los mensajitos de WindowsPopup. Necesita
   # el paquete linpopup, pero de momento paso de el. Lo tengo que
   # probar, porque algun vez me ha hecho falta, sobre todo para avisar
   # a los usuarios antes de reinciar el servidor.
;   message command = /bin/sh -c '/usr/bin/linpopup "%f" "%m" %s; rm %s' &

   # Opciones de Winbind. No tengo ni idea de lo que es. No lo toco, y
   # lo dejo como lo pone debconf.
;   idmap uid = 10000-20000
;   idmap gid = 10000-20000
;   template shell = /bin/bash

#======================= Share Definitions =======================

[homes]
   # Comentario de lo que aparecera en el entorno de red de Windows.
   comment = Carpeta personal de %U
   path = /home/samba/%U

   browseable = yes
   writable = yes
   create mask = 0700
   directory mask = 0700

[netlogon]
   # Donde se ponen los scripts de Logon.
   comment = Servicio de Logon
   path = /home/samba/var/netlogon

   guest ok = yes
   writable = no
   locking = no
   public = no
   browseable = yes
   share modes = no
   public=no

[printers]
   # Carpeta de las impresoras del servidor.
   comment = Servidor de Impresion
   path = /tmp
```

```
   browseable = no
   guest ok = yes
   writable = no
   printable = yes
;   print ok = yes
;   use client drivers = yes
;   create mode = 0700

[print$]
   # Recurso con los drivers de las impresoras. No he conseguido
   # que funcione bien con Windows 95/98, con XP si, pero añadiendo
   # los drivers desde XP, no desde el Linux. Era un rollazo fuerte.
   comment = Drivers de Impresion
   path = /home/samba/var/print-drivers
   browseable = yes
   read only = no
   guest ok = yes

;   write list = root, @ntadmin

[Profiles]
   comment = Unidad con los perfiles de red
   path=/home/samba/var/perfiles
   create mode = 0600
   csc policy = disable
   directory mode = 0700
   profile acls = yes
   read only = no

[comun]
   comment = Unidad de red comun a todos
   path=/home/samba/var/comun
   browseable = yes
   writable = yes
   readonly = no
   force create mode = 0777
   create mode = 0777
   force directory mode = 0777
   directory mode = 0777
```

Se podrán comprobar los parámetros del archivo de configuración de samba, mediante:

```
testparm -v
```

Ahora se debe fijar a Samba la contraseña del administrador del LDAP :

```
smbpasswd -w XXXXX
```

donde XXXXX se sustituirá por la contraseña del Admin del LDAP. Ahora se creará la cuenta del administrador del dominio...

```
smbldap-useradd.pl -a -m administrador
smbldap-usermod.pl -u 0 administrador
smbldap-passwd.pl administrador
```

Como contraseña he puesto *“pokemon”* . Puede ser que para añadir equipos al dominio haga falta poner la clave del administrador del dominio, por eso no pongo la del administrador del LDAP.

3.3.2. Encriptando contraseñas

Para codificar claves en forma {CRYPT}, podemos usar el suiguiente programita en perl:

```
#!/usr/bin/perl
$a= crypt("pokemon","gq");
print "Clave : $a \n";
```

donde *"pokemon"* es la contraseña a encriptar.

3.4. Configurando libnss-ldap

Esta librería permite decirle a Linux cómo encontrar cuentas de acceso en LDAP, *algo parecido a nsloo-kup en dns, pero con cuentas usuarios en ldap*. Para ello, necesitaremos de una cuenta especial en el directorio, que llamaremos nss. Lo primero será crearnos el archivo `/etc/ldap/nss.ldif` con el siguiente contenido ...

```
dn: cn=nss,dc=adesx,dc=com
objectClass: organizationalRole
objectClass: simpleSecurityObject
cn: nss
description: Cuenta de usuario para user-lookups
userPassword: {CRYPT}gq9a.KazGGQkI
```

La clave que aparece ahí es *"pokemon"* , (resultado de haber ejecutado el script perl que se ha descrito líneas más arriba). Ahora importamos la cuenta en el directorio...

```
ldapadd -x -h localhost -D "cn=admin,dc=adesx,dc=com" -f nss.ldif -W
```

y ponemos la clave del administrador del Directorio. Después, nos aseguramos de que el archivo `/etc/libnss-ldap.conf` tenga estas líneas :

```
host 127.0.0.1
base ou=Gente,dc=adesx,dc=com
uri ldap://127.0.0.1/
ldap_version 3

binddn cn=nss,dc=adesx,dc=com
bindpw pokemon

nss_base_passwd ou=Gente,dc=adesx,dc=com
nss_base_group ou=Grupos,dc=adesx,dc=com

pam_password crypt
```

3.5. Configurando pam

Ahora toca la hora de configurar pam, que es el módulo que gestiona de manera centralizada la autenticación de los diferentes servicios que se ejecutan en nuestro Linux. Para ello, editaremos el fichero `/etc/pam_ldap.conf` y nos aseguramos de que tenga:

```
host 127.0.0.1
base dc=adesx,dc=com
uri ldap://127.0.0.1/
ldap_version 3
binddn cn=nss,dc=adesx,dc=com
bindpw pokemon
rootbinddn cn=admin,dc=adesx,dc=com
pam_password crypt
```

y en el fichero `/etc/ldap.secret` pondremos la contraseña del administrador del directorio (en claro). Asegurarse que el archivo tiene sólo permisos 600.

Ahora se editará el archivo `/etc/pam.d/samba`, y se añadirá en todas secciones el módulo ldap (líneas donde aparece pam_ldap.so). Al final quedará algo así (*el orden es importante, respetarlo*):

```
auth sufficient pam_ldap.so
auth required pam_unix.so nullok

account sufficient pam_ldap.so
account required pam_unix.so

session sufficient pam_ldap.so
session required pam_unix.so

password sufficient pam_ldap.so
password required pam_unix.so
```

También editaremos el fichero `/etc/pam.d/password` y dejaremos algo así:

```
password sufficient pam_ldap.so
password required pam_unix.so nullok obscure min=4 max=8 md5
```

Sólo nos quedará reiniciar el servicio de samba, y empezar a probar ...

```
/etc/init.d/samba restart
```

4. Conclusiones y TODO

Este mini-howto está aún inacabado, porque aún me queda cómo documentar:

- Como se configuran los clientes Windows 9x, 2000 y XP para que sean clientes de nuestro dominio,, así cómo las modificaciones en los registros que se deben realizar.
- Problemas típicos con los perfiles errantes, perfiles por defecto, y tipos: habituales y obligatorios.
- Scripts de logon guapos, guapos en Kix32 que mapean unidades dependiendo de la pertenencia del usuario a determinados grupos, realizan el inventario Software/Hardware del Windows cliente en el Logon, modifican el registro de manera remota, conexión de impresoras en el Logon, etc, etc...
- Políticas de seguridad para las cuentas de usuarios, y estaciones de trabajo, en los Windows.
- Compartición de unidades con automount. *Caso típico: En una empresa sólo hay una grabadora de CD y un lector, y todos los usuarios quieren poder quemar CDs.*
- Kerberos + LDAP + Samba3 = Active Directory.

La mayoría de cosas las tengo hechas (excepto la última), pero no tengo mucho tiempo de documentar. Ahorá sólo quedará recordar cómo manejarse básicamente con las cuentas de usuario y cuentas para las estaciones de trabajo

- **Agregar una estación NT/2K/XP** al dominio, donde `SOLARIA` es el nombre del equipo. Ojo esto sólo es necesario, para que el Windows Cliente ejecute los scripts de Logon.

```
smbldap-useradd.pl -w -d /dev/null -s /bin/false SOLARIA
```

- **Añadir usuarios ...**

```
smbldap-useradd.pl -a -m LOGIN
```

- **Cambiar el password a los usuarios...**

```
smbldap-passwd.pl LOGIN
```

- **Cualquier otra cosa ....** teclear `smbldap-` y pulsar varias veces el tabulador ... :)