Guía para montar Samba como PDC + autenticación LDAP

Algunas notas introductorias:

- La distro utilizada para estas pruebas fue la **Debian Etch 4.0** (mi preferida). Probablemente se pueda adaptar sin mucho problema a otras distros de Linux.

- Las ubicaciones de los archivos tratados en este documento pueden variar dependiendo de la distro y versión que tenga.

- El procedimiento del montaje descrito en esta guía se hizo con base en mi necesidad específica. De acuerdo con su necesidad particular, puede que necesite llevar a cabo pasos adicionales/diferentes que los citados en este documento. Tome en cuenta que yo no soy experto en LDAP, simplemente pude adecuarlo a lo que yo necesitaba.

- Esta guía se ha elaborado tomando como base diversa documentación obtenida en Internet en conjunto con partes personalizadas a mi gusto.

- **Todos** los comandos ejecutados desde la consola deben llevarse a cabo como usuario **root**.

- Si le gusta el café (como a mí) le aconsejo que se vaya preparando varias tazas antes de comenzar con este procedimiento.

Al final de esta guía tendremos montado un controlador principal de dominio en Samba + perfiles móviles + scripts de inicio y se utilizará la autenticación y organización de usuarios y grupos por medio de openLDAP.

Mucha suerte y paciencia con este montaje.

Ing. Rolando V. (Pish)

ÍNDICE GENERAL

SECCIÓN 1. Instalación del servidor LDAP

Instalar el paquete de openLDAP y algunas utilidades con el comando:

```
# apt-get install slapd ldap-utils
```

Mientras se instala el paquete slapd se le pedirá la siguiente información:

Dato solicitado	Dato a introducir	Notas adicionales
Contraseña del admin	suclave	Contraseña que le asignará a la cuenta admin de LDAP
Confirme la contraseña del admin	suclave	

Cuando se terminen de instalar los paquetes tenemos que reconfigurar a slapd para que nos pida más información:

```
# dpkg-reconfigure slapd
```

Dato solicitado	Dato a introducir	Notas adicionales
Omitir la configuración de OpenLDAP	no	Es para confirmar que desea reconfigurar a OpenLDAP
Nombre de dominio	home	Es el nombre que yo le puse a mi dominio de prueba
Nombre de organización	home	Aquí puede ir un nombre más amigable y descriptivo
Contraseña del admin	suclave	Otra vez volver a digitar la clave del usuario admin de LDAP
Confirme la contraseña del admin	suclave	Otra vez confirmar la clave del usuario admin de LDAP
Motor de base de datos a utilizar	BDB	Formato Berkeley de Base de Datos
Borrar la base de datos al purgar slapd	no	Es para conservar la base de datos de LDAP cuando se purgue
Mover la base de datos antigua	sí	Es para respaldar la base de datos actual de LDAP. (prevención)
Permitir LDAP v2	sí	

Ahora, para probar que el servicio de slapd está arriba y funcionando utilizamos el comando:

```
# ldapsearch -x -b “dc=home”
```

NOTA: Si por ejemplo su dominio se llama sudominio.com entonces el comando debe ser:

```
# ldapsearch -x -b “dc=sudominio,dc=com”
```

Si por ejemplo su dominio se llama sudominio.co.cr entonces el comando debe ser:

```
# ldapsearch -x -b “dc=sudominio,dc=co,dc=cr”
```

Y debe mostrarse una información. Si saliera un mensaje como esto: “ldap_bind: Can't contact LDAP server (-1)”

entonces algo está pasando con el servicio de LDAP.

Si tenemos problemas con el slapd, entonces podemos ejecutarlo en modo debug para ver sus mensajes en tiempo real:

```
# slapd -d 256
```

Si al ejecutar este comando no se despliega ningún error, entonces puede abrir otra consola y pruebe ejecutar allí nuevamente el comando ldapsearch para observar qué mensajes se emiten y cuál puede ser el error.

SECCIÓN 2. Instalación de phpldapadmin

Instalar un administrador gráfico para LDAP nos va ayudar mucho a visualizar nuestro árbol organizativo en LDAP además de que nos permite llevar a cabo funciones muy útiles de una manera muy rápida.
El phpldapadmin es un administrador hecho en PHP que corre encima de un servidor web (por ejemplo: Apache SSL o Apache2) y accesible utilizando cualquier navegador de internet (en mi caso lo usé con Iceweasel que es la versión de firefox que viene con Debian Etch).

NOTA: también existe otro administrador gráfico de LDAP llamado luma que viene entre los paquetes de Debian Etch, pero personalmente prefiero a phpldapadmin y he visto que es el más aceptado.

2.1 Instalación de apache-ssl

Antes de instalar a phpldapadmin vamos a instalar el servidor web Apache-SSL para correr siempre a phpldapadmin desde allí vía páginas seguras.

```
# apt-get install apache-ssl
```

Mientras se instala el paquete apache-ssl se le pedirá la siguiente información:

Dato solicitado	Dato a introducir	Notas adicionales
Nombre del país	CR	Digitar cualquier valor de 2 caracteres
Estado o provincia	HE	Digitar cualquier valor (yo puse HE por Heredia)
Localidad	Heredia	
Nombre de la organización	home	
Nombre de la unidad organizativa	home	
Nombre del host	servidor.home	La computadora se llama servidor y el nombre de dominio es home. Yo también probé digitando solamente el valor localhost y funcionó bien.
Correo electrónico		También puede digitar root@localhost

Para probar si el Apache-SSL está arriba y funcionando, abrimos nuestro navegador de internet y nos vamos a la siguiente dirección:

```
https://localhost
```

Si no nos devuelve ningún error entonces ya tenemos arriba a nuestro servidor web seguro.

2.2 Instalación de smbldap-tools y phpldapadmin

Seguidamente vamos a instalar un paquete llamado smbldap-tools que contiene varias herramientas para Samba y LDAP muy útiles para nuestros intereses:

```
# apt-get install smbldap-tools
```

Ahora sí es momento para instalar el phpldapadmin:

```
# apt-get install phpldapadmin
```

Para probar que el phpldapadmin quedó bien instalado, abrimos el navegador de internet y nos vamos a la siguiente dirección:

```
https://localhost/phpldapadmin
```

Y debe aparecer la página principal de phpldapadmin. Si ocurriera algún error yo recomiendo volver a instalar el phpldapadmin o sino bajar la última versión de la página oficial y montarla en la carpeta /var/www

Al instalar a phpldapadmin también se instalará el servidor apache2 automáticamente (pruebe entrar a `http://localhost` para que revise si tiene el servicio apache2 activo y corriendo). Con respecto a este punto, mencionaré que como gusto personal, NO quiero que phpldapadmin esté hosteado vía apache2, solamente vía apache-ssl para garantizar la utilización del web-seguro en esta herramienta. Para llevar a cabo este objetivo, simplemente habrá que eliminar o mover a otro lugar este enlace simbólico: `/etc/apache2/conf.d/phpldapadmin` y luego reiniciar el servicio apache2 con el comando:

```
# /etc/init.d/apache2 restart
```

Una vez instalado, phpldapadmin requiere de una utilidad llamada mkntpwd para crear los hashes de Samba. Debido a que esta utilidad no ha sido incluida en el paquete smbldap-tools de Debian, habrá que descargar sus archivos fuente de Internet y compilarlos en nuestro sistema para que nos genere el ejecutable de mkntpwd:

La página que aloja los fuentes de mkntpwd es:

```
http://cvs.samba.org/cgi-bin/cvsweb/samba/examples/LDAP/smbldap-tools/mkntpwd/
```

A continuación enumero los 7 archivos de mkntpwd con el fin de que usted corrobore si bajó los correctos:

```
getopt.c
getopt.h
Makefile
md4.c
mkntpwd.c
mkntpwd.h
smbdes.c
```

NOTA: estos archivos yo los tengo en un comprimido llamado mkntpwd.zip que puedo enviar si alguien tiene problemas bajándolos

Para compilarlos en su sistema, vamos a alojar esos 7 archivos en alguna carpeta temporal. Desde la consola nos vamos a dicha carpeta temporal y ejecutamos el comando:

```
# make
```

Esto nos va a generar el archivo ejecutable mkntpwd, el cual vamos a copiar a la carpeta /usr/local/bin:

```
# cp mkntpwd /usr/local/bin
```

Para probar si la utilidad mkntpwd quedó bien instalada simplemente ejecutamos el comando:

```
# mkntpwd
```

y por lo menos debe salir el mensaje de ayuda de mkntpwd. Si se nos muestra que el comando es incorrecto significa que tenemos que revisar los pasos anteriores para ver cuál hicimos mal.

SECCIÓN 3. Instalación de Samba

Vamos a instalar samba y samba-doc con el siguiente comando:

```
# apt-get install samba samba-doc
```

Mientras se instala el paquete samba se le pedirá la siguiente información:

Dato solicitado	Dato a introducir	Notas adicionales
Nombre del dominio	home	Se usa el mismo que se usó para LDAP
Usar passwords encriptados	sí	Puede que NO se le pregunte este dato
Modificar smb.conf para que use la configuración WINS proveniente de DHCP	no	

Por ahora vamos a dejar así a Samba. Más adelante en otra sección lo vamos a configurar como se debe.

SECCIÓN 4. Configuración de LDAP

El servidor LDAP necesitará del esquema Samba para trabajar. Para eso vamos a obtener el archivo samba.schema provisto por samba-doc y lo vamos a alojar en la carpeta /etc/ldap/schema. Hacemos lo siguiente desde la consola:

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

Ahora tenemos que editar el archivo de configuración de slapd /etc/ldap/slapd.conf y agregar la siguiente línea después del último "include" que aparezca en ese archivo para que LDAP use el esquema Samba:

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

Además buscaremos la siguiente línea:

```
access to attrs=userPassword
```

y la cambiamos por: (para que los atributos `sambaLMPassword` y `sambaNTPassword` NO sean accesibles a todos)

```
access to attrs=userPassword,shadowLastChange,sambaLMPassword,sambaNTPassword
```

El contenido final y completo del archivo /etc/ldap/slapd.conf se muestra a continuación sin algunas líneas comentadas para no hacerlo tan largo:

```
# Allow LDAPv2 binds
allow bind_v2

# Schema and objectClass definitions
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/inetorgperson.schema
include         /etc/ldap/schema/samba.schema

pidfile         /var/run/slapd/slapd.pid
argsfile        /var/run/slapd/slapd.args
```

```
loglevel        0

modulepath  /usr/lib/ldap
moduleload  back_bdb

sizelimit 500

tool-threads 1

backend           bdb
checkpoint 512 30
database        bdb

suffix          "dc=home"

directory       "/var/lib/ldap"

dbconfig set_cachesize 0 2097152 0
dbconfig set_lk_max_objects 1500
dbconfig set_lk_max_locks 1500
dbconfig set_lk_max_lockers 1500

index           objectClass eq

lastmod         on

access to attrs=userPassword,shadowLastChange,sambaLMPassword,sambaNTPassword
        by dn="cn=admin,dc=home" write
        by anonymous auth
        by self write
        by * none

access to dn.base="" by * read

access to *
        by dn="cn=admin,dc=home" write
        by * read
```

Seguidamente debemos reiniciar a slapd para que estos cambios entren en vigencia:

```
# /etc/init.d/slapd restart
```

SECCIÓN 5. Introducción de los principales contenedores (“Organizational Units”) para el árbol LDAP

(estos pasos pueden variar dependiendo de su necesidad específica)

Para llevar a cabo este objetivo vamos a utilizar a phpldapadmin. Abrimos el navegador de internet y nos vamos a la dirección siguiente:

```
https://localhost/phpldapadmin
```

Para conectarnos digitamos los siguientes datos:

Usuario	cn=admin,dc=home
Contraseña	la contraseña de admin que digitó cuando se configuró el LDAP

NOTA: Si por ejemplo su dominio se llama sudominio.com entonces el usuario debe ser:

```
cn=admin,dc=sudominio,dc=com
```

Si por ejemplo su dominio se llama sudominio.co.cr entonces el usuario debe ser:

```
cn=admin,dc=sudominio,dc=co,dc=cr
```

Procederemos a declarar los contenedores principales. En mi caso particular yo declaré 3 “organizational units”:

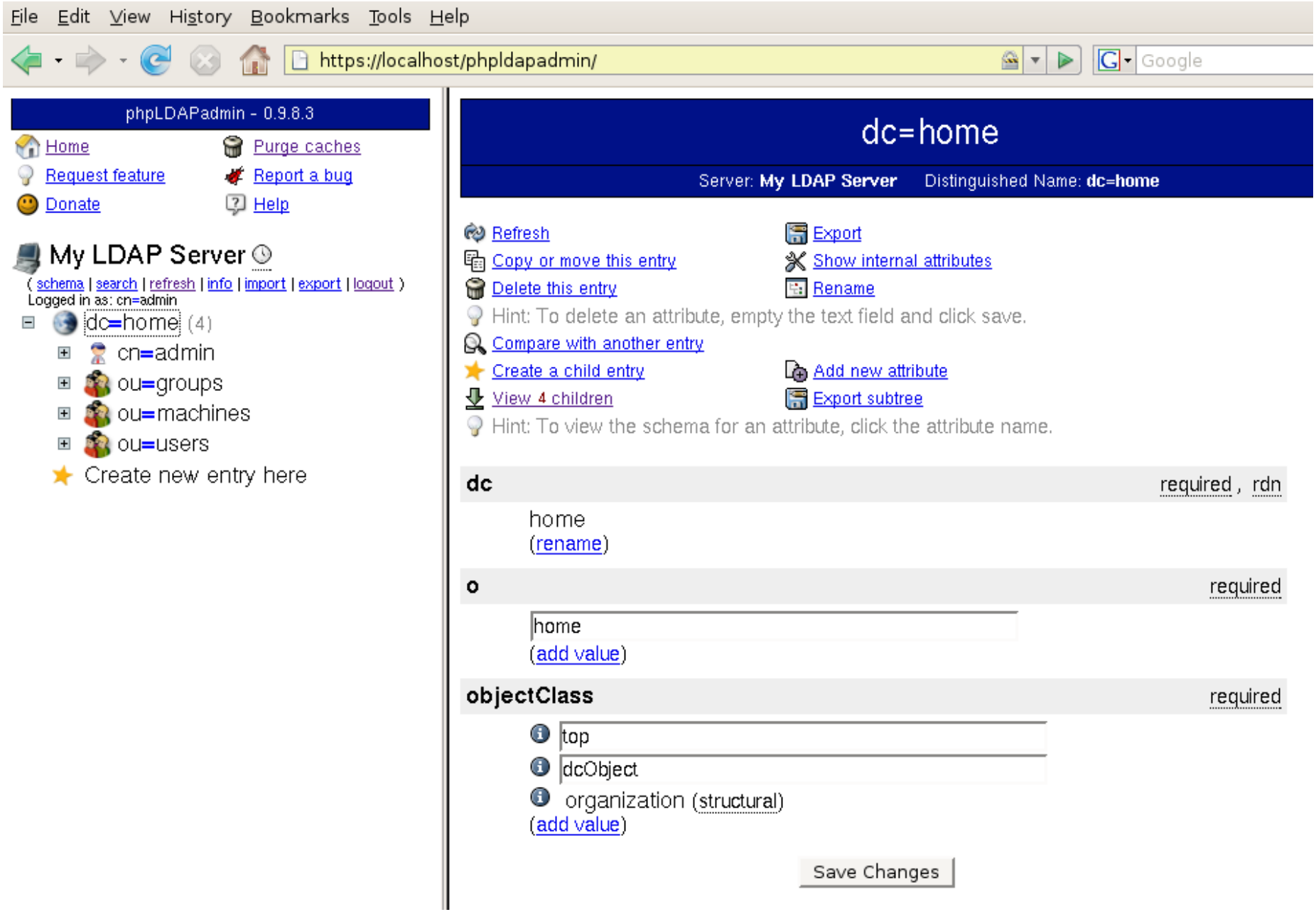
- groups (para manejar las cuentas de grupos)
- machines (para manejar las cuentas de máquinas) y
- users (para manejar las cuentas de los usuarios).

Usando el phpldapadmin expandimos el árbol de dc=home y le damos click a la opción “Create New Entry Here” (para crear un hijo de dc=home), luego seleccionamos “Organizational Unit” (ou), luego digitamos el nombre deseado (en este caso users, por ejemplo) y presionamos la tecla de tabulación para que se habilite el botón para proceder (hasta que no se presione la tecla de tabulación no se habilitará el botón para proceder).

A continuación muestro una imagen de cómo se vería este proceso de creación:

Una vez creada la ou=users, procedemos de la misma forma para crear a ou=machines y a ou=groups. Más adelante crearemos las demás entidades que conformarán nuestro árbol. Por ahora dejémoslo así.

Al final de este paso el árbol de LDAP se vería así:


File Edit View History Bookmarks Tools Help
https://localhost/phpldapadmin/
Google
phpLDAPadmin - 0.9.8.3
Home
Purge caches
Request feature
Report a bug
Donate
Help
My LDAP Server
(schema | search | refresh | info | import | export | logout)
Logged in as: cn=admin
dc=home (4)
cn=admin
ou=groups
ou=machines
ou=users
Create new entry here
dc=home
Server: My LDAP Server Distinguished Name: dc=home
Refresh
Export
Copy or move this entry
Show internal attributes
Delete this entry
Rename
Hint: To delete an attribute, empty the text field and click save.
Compare with another entry
Create a child entry
Add new attribute
View 4 children
Export subtree
Hint: To view the schema for an attribute, click the attribute name.
dc
required , rdn
home
(rename)
o
required
home
(add value)
objectClass
required
top
dcObject
organization (structural)
(add value)
Save Changes

SECCIÓN 6. Configuración de SAMBA

Vamos a configurar a SAMBA para que sea un controlador de dominio principal, para que soporte los scripts de inicio y perfiles móviles (roaming profiles) y para que autentique a los usuarios utilizando LDAP. Además vamos a permitir que el script smbldap-useradd (provisto por smbldap-tools) nos automatice la adición de cuentas de máquina al árbol LDAP cuando éstas se unan al dominio por primera vez.

Antes de tocar el archivo de configuración, primero creamos las carpetas /home/samba/netlogon (para alojar el(los) script(s) de inicio) y /home/samba/profiles (para alojar los perfiles móviles de los usuarios). Asignamos todos los permisos (777) a dicha carpeta profiles, para que cualquiera ya sea de sambaadmins o sambausers pueda grabar su perfil móvil en el servidor.

El contenido final y completo del archivo /etc/samba/smb.conf con todo el soporte citado con anterioridad se muestra a continuación sin algunas líneas comentadas para no hacerlo tan largo:

```
[global]
### Configuracion basica del servidor ###
workgroup = home
netbios name = servidor
server string = Samba PDC Version %v
socket options = TCP_NODELAY IPTOS_LOWDELAY SO_SNDBUF=8192 SO_RCVBUF=8192

### Configuracion para que la maquina sea el PDC master ###
os level = 65
preferred master = yes
local master = yes
domain master = yes
domain logons = yes

### Configuracion de seguridad y conexion ###
security = user
guest ok = no
encrypt passwords = yes
null passwords = no
hosts allow = 127.0.0.1 192.168.0.0/255.255.255.0
wins support = yes
name resolve order = wins lmhosts host bcast
dns proxy = no
time server = yes
```

```
### Otras configuraciones varias para SAMBA ###
log file = /var/log/samba/log.%m
log level = 2
max log size = 50
hide unreadable = yes
hide dot files = yes
panic action = /usr/share/samba/panic-action %d
unix charset = ISO8859-1

### Parametros para el soporte de LDAP ###
passdb backend = ldapsam:ldap://127.0.0.1
ldap suffix = dc=home
ldap machine suffix = ou=machines
ldap user suffix = ou=users
ldap group suffix = ou=groups
ldap admin dn = cn=admin,dc=home
ldap delete dn = no
enable privileges = yes
; Para permitir a los usuarios cambiar su clave desde Windows
ldap password sync = yes

### Perfiles moviles de usuario, carpeta home y script de inicio ###
logon home = \\%L\%U\.profile
logon drive = H:
logon path = \\%L\profiles\%U
logon script = %U.bat OR netlogon.bat

### Script para automatizar la adicion de cuentas de maquinas     ###
### al arbol LDAP cuando estas se unan por primera vez al dominio ###
add machine script = /usr/sbin/smbldap-useradd -w "%u"

### Impresion ###

load printers = yes
printcap name = /etc/printcap
printing = cups
printcap name = cups
; Si quiero que el grupo sambaadmins pueda administrar las impresoras
; printer admin = @sambaadmins
```

```
### Recursos SAMBA ###

# Ruta en donde se alojaran el(los) script(s) de inicio
[netlogon]
  comment = Network Logon Service
  path = /home/samba/netlogon
  guest ok = no
  writable = no
  browseable = no
  share modes = no

# Carpeta en donde se guardan los perfiles moviles de los usuarios
[profiles]
  comment = Perfiles de Usuarios
  path = /home/samba/profiles
  writeable = yes
  browseable = no
  guest ok = no
  hide files = /desktop.ini/ntuser.ini/NTUSER.*/
  create mask = 0600
  directory mask = 0700
  csc policy = disable

# Impresoras
[printers]
  comment = Impresoras
  browseable = no
  path = /var/spool/samba
  printable = yes
  public = no
  writable = no
  create mode = 0700

# Los clientes Windows buscan este recurso como fuente de drivers
[print$]
  comment = Drivers de Impresoras
  path = /var/lib/samba/printers
  browseable = yes
  read only = yes
  guest ok = no

# carpetas home de los usuarios
```

```
[homes]
  path = /home/users/%U
  comment = Carpetas HOME
  browseable = no
  writeable = yes
  valid users = %S
  read only = no
  guest ok = no
  inherit permissions = yes

# Este es un recurso que solo debe ser accesible
# para un grupo POSIX especial llamado sysfox
[sysfox]
  comment = Directorio de Sistemas en Fox
  path = /home/posix/sysfox
  writeable = yes
  delete readonly = yes
  valid users = @sysfox
  write list = @sysfox
  force group = sysfox
  browseable = yes
  create mask = 0770
  directory mask = 0770

# Este recurso es por si quiero compartir la unidad de CD
;[cdrom]
;   comment = Samba server CD
;   writable = no
;   locking = no
;   path = /media/cdrom0
;   public = yes

; Lo siguiente es para auto-montar el CD cada vez que es accesado y desmontarlo
; cuando se termina la conexión al servidor.
; Para que esto trabaje, el archivo /etc/fstab debe contener una
; entrada así: /dev/hdc0   /media/cdrom  iso9660 defaults,noauto,ro,user   0 0
;
;   preexec = /bin/mount /cdrom
;   postexec = /bin/umount /cdrom
```

Una vez que ya tenemos listo a /etc/samba/smb.conf podemos ejecutar el comando testparm para asegurarnos que la configuración Samba no tenga ningún error:

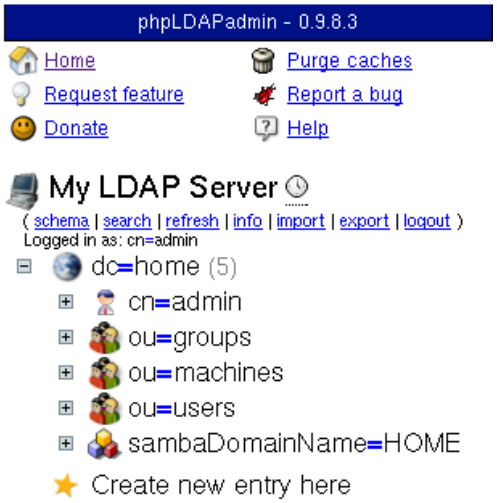
```
# testparm
```

Antes de reiniciar el servicio Samba, le proveemos a Samba la contraseña de root(admin) para LDAP:

```
# smbpasswd -w suclave
# /etc/init.d/samba restart
```

NOTA: para no hacerme enredos con diferentes contraseñas, yo utilizo la misma contraseña tanto para el superusuario de Linux (**root**) como para el **admin** de LDAP.

Ahora podemos irnos al phpldapadmin y refrescar su información para corroborar que tenemos una entrada más que se llama: sambaDomainName=HOME. Muestro a continuación la imagen correspondiente:



Si damos click en la entrada sambaDomainName podremos observar sus propiedades en la ventana de la derecha. Aprovechemos este momento para copiar en algún lugar el valor sambaSID (por ejemplo, el mío es: S-1-5-21-125945932-740595490-3132273231) ya que lo ocuparemos más adelante.

SID: abreviatura de ***S**ecure **ID**entifier*. Es un identificador único utilizado para identificar un objeto específico, que puede ser un usuario o un grupo en una red, por ejemplo.

SECCIÓN 7. Mapeos de grupos con Samba

Primero definiré brevemente algunos términos a usar en esta sección:

RID: abreviatura de ***R****elative* ***ID****entifier*. Es un identificador por medio del cual un grupo corriente se convierte en un grupo **especial** con ciertas características especiales en nuestro dominio.

GID: abreviatura de ***G****roup* ***ID****entifier*. Es el identificador único de un grupo.

A partir de Samba-3 tenemos la disponibilidad de crear mapeos o asociaciones entre los grupos de Windows y los grupos de UNIX. Esto es algo necesario debido a que existen grupos especiales propios de los dominios Windows que tienen características y privilegios específicos (Domain Admins, Domain Controllers, Builtin Print Operators, etc.) y vamos a querer que existan en nuestro dominio Samba ya que nos van a ser muy útiles.

En esencia lo que se hace para mapear un grupo en Samba, es asignarle el **RID** específico a dicho grupo para que adquiera las características específicas y especiales del grupo Windows correspondiente.
La siguiente tabla muestra los grupos Windows y sus correspondientes **RIDs**, así como su tipo y si es esencial en el directorio LDAP o no: (los RIDs **no** son declarados por mí, son valores ya establecidos)

Nombre del Grupo Windows	RID	Tipo	Esencial
Domain Administrator	500	Usuario	No
Domain Guest	501	Usuario	No
Domain KRBTGT	502	Usuario	No
Domain Admins	512	Grupo	Yes
Domain Users	513	Grupo	Yes
Domain Guests	514	Grupo	Yes
Domain Computers	515	Grupo	No
Domain Controllers	516	Grupo	No
Domain Certificate Admins	517	Grupo	No
Domain Schema Admins	518	Grupo	No
Domain Enterprise Admins	519	Grupo	No

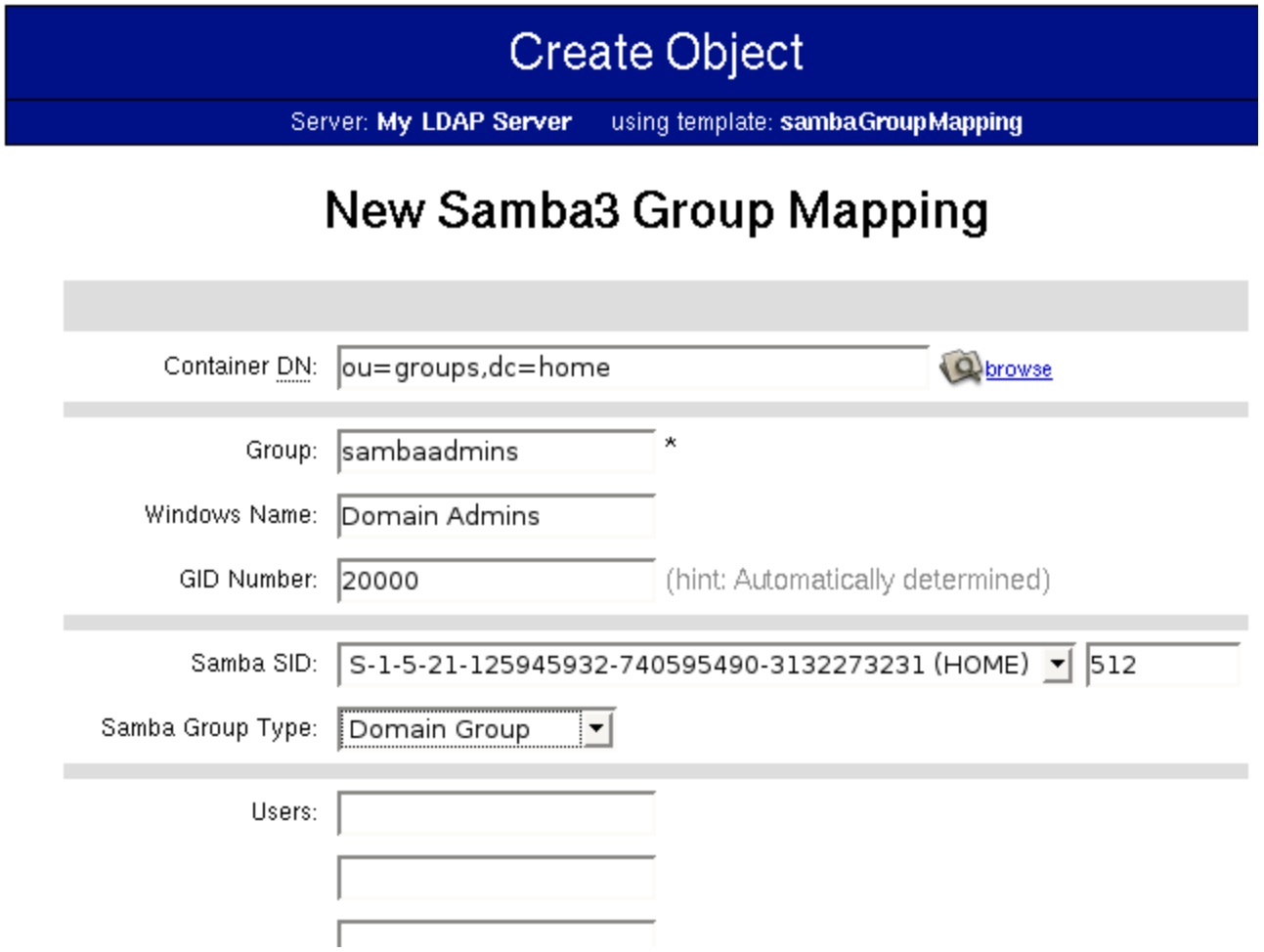
Domain Policy Admins	520	Grupo	No
Builtin Admins	544	Alias	No
Builtin users	545	Alias	No
Builtin Guests	546	Alias	No
Builtin Power Users	547	Alias	No
Builtin Account Operators	548	Alias	No
Builtin System Operators	549	Alias	No
Builtin Print Operators	550	Alias	No
Builtin Backup Operators	551	Alias	No
Builtin Replicator	552	Alias	No
Builtin RAS Servers	553	Alias	No

Como pudimos ver, son muchos los grupos Windows que se pueden mapear en Samba. Sin embargo, para mi necesidad específica únicamente mapearé a los siguientes 4 grupos:

Nombre Windows	**Nombre UNIX**	**Notas adicionales**
Domain Admins	sambaadmins	Este grupo de usuarios tendrán privilegios de administrador **localmente** en sus computadoras. Es decir, podrán instalar programas, si corren alguna aplicación que necesite modificar algo en las carpetas de sistema no tendrán problema, etc.
Domain Users	sambausers	Usuarios limitados **localmente** en sus computadoras.
Domain Guests	sambaguests	Quiero tener este grupo pero no pienso usarlo por el momento
Domain Computers	sambamachines	Aquí se alojarán las cuentas de máquinas del dominio

Para agregar nuestros grupos mapeados Samba, nos vamos al phpldapadmin y dentro de nuestra ou=groups (nuestra “Organizational Unit” llamada groups) vamos a crear nuestros 4 “Samba 3 Group Mappings”.

La siguiente imagen muestra cómo se ve el proceso de creación de Domain Admins: (cuyo RID es 512)
NOTA: por gusto personal los GIDs de mis grupos los comencé a partir de 20000.


Create Object
Server: My LDAP Server using template: sambaGroupMapping
New Samba3 Group Mapping
Container DN:
ou=groups,dc=home
browse
Group:
sambaadmins
*
Windows Name:
Domain Admins
GID Number:
20000
(hint: Automatically determined)
Samba SID:
S-1-5-21-125945932-740595490-3132273231 (HOME)
512
Samba Group Type:
Domain Group
Users:

SECCIÓN 8. Configuración de la autenticación UNIX

Ahora vamos a configurar a nuestro sistema para que vea a los usuarios LDAP como usuarios “normales” de UNIX.

8.1 Instalación de libnss-ldap

Primero vamos a instalar el paquete libnss-ldap:

```
# apt-get install libnss-ldap
```

Mientras se instala el paquete libnss-ldap se le pedirá alguna información. Sin embargo, al finalizar la instalación de este paquete, tendremos que reconfigurarlo para que nos pida más información. Recordemos que para reconfigurarlo debemos ejecutar el siguiente comando:

```
# dpkg-reconfigure libnss-ldap
```

La siguiente tabla muestra la información que se nos puede pedir (ya sea en la instalación o en la reconfiguración) y lo que debemos digitar:

Dato solicitado	Dato a introducir	Notas adicionales
Servidor de LDAP	127.0.0.1	
Nombre distintivo (DN)	dc=home	
Versión de LDAP	3	
Se requiere usuario para la base de datos LDAP	no	
Privilegios especiales de LDAP para root	sí	
Configuración leíble y escribible sólo para el propietario	sí	
Cuenta LDAP para root	cn=admin,dc=home	
Contraseña para la cuenta LDAP de root	suclave	La misma del admin de LDAP

Ahora vamos a editar el archivo de configuración /etc/nsswitch.conf.
Buscamos las siguientes 3 líneas:

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

y las reemplazamos para que queden así:

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

El contenido final y completo de este archivo se muestra a continuación:

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

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

hosts:          files dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

En este momento podemos usar la utilidad getent para confirmar que se muestren los grupos mapeados que creamos con anterioridad:

```
# getent group
```

y el resultado puede contener lo siguiente:

```
...
sambaadmins:*:20000:
sambausers:*:20001:
sambaguests:*:20002:
sambamachines:x:20003:
...
```

8.2 Instalación de libpam-ldap

Seguidamente vamos a instalar el paquete libpam-ldap:

```
# apt-get install libpam-ldap
```

Mientras se instala el paquete libpam-ldap se le pedirá alguna información. Sin embargo, al finalizar la instalación de este paquete, tendremos que reconfigurarlo para que nos pida más información. Recordemos que para reconfigurarlo debemos ejecutar el siguiente comando:

```
# dpkg-reconfigure libpam-ldap
```

La siguiente tabla muestra la información que se nos puede pedir (ya sea en la instalación o en la reconfiguración) y lo que debemos digitar:

Dato solicitado	Dato a introducir	Notas adicionales
Servidor de LDAP	127.0.0.1	
Nombre distintivo (DN)	dc=home	
Versión de LDAP	3	
Make local root Database admin	sí	La pregunta venía en Inglés
Se requiere usuario para la base de datos LDAP	no	
LDAP account for root	cn=admin,dc=home	La pregunta venía en Inglés
Contraseña para la cuenta LDAP de root	suclave	La misma del admin de LDAP
Local crypt to use when changing passwords	md5	

Como se pudo observar, algunos datos solicitados fueron los mismos que pidió el paquete libnss-ldap.

Ahora vamos a editar los archivos de correspondientes para configurar PAM para LDAP:

Primero vamos con el archivo /etc/pam.d/common-account. Buscamos la siguiente línea:

```
account        required        pam_unix.so
```

la comentamos y agregamos estas dos líneas:

```
account         sufficient      pam_ldap.so
account         required        pam_unix.so try_first_pass
```

Así, el contenido final y completo del archivo /etc/pam.d/common-account se muestra a continuación:

```
#
# /etc/pam.d/common-account - authorization settings common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authorization modules that define
# the central access policy for use on the system.  The default is to
# only deny service to users whose accounts are expired in /etc/shadow.
#
#account    required    pam_unix.so

account           sufficient  pam_ldap.so
account           required    pam_unix.so try_first_pass
```

En el archivo /etc/pam.d/common-auth buscamos la siguiente línea:

```
auth   required        pam_unix.so nullok_secure
```

la comentamos y agregamos estas dos líneas:

```
auth    sufficient      pam_ldap.so
auth    required        pam_unix.so nullok_secure use_first_pass
```

Así, el contenido final y completo del archivo /etc/pam.d/common-auth se muestra a continuación:

```
#
# /etc/pam.d/common-auth - authentication settings common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authentication modules that define
# the central authentication scheme for use on the system
# (e.g., /etc/shadow, LDAP, Kerberos, etc.).  The default is to use the
# traditional Unix authentication mechanisms.
#
#auth required    pam_unix.so nullok_secure
auth    sufficient      pam_ldap.so
auth    required        pam_unix.so nullok_secure use_first_pass
```

En el archivo /etc/pam.d/common-password buscamos la siguiente línea:

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

la comentamos y agregamos estas dos líneas:

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

Así, el contenido final y completo del archivo /etc/pam.d/common-password se muestra a continuación:

```
# /etc/pam.d/common-password - password-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define  the services to be
#used to change user passwords.  The default is pam_unix

# The "nullok" option allows users to change an empty password, else
# empty passwords are treated as locked accounts.
#
# (Add `md5' after the module name to enable MD5 passwords)
#
# The "obscure" option replaces the old `OBSCURE_CHECKS_ENAB' option in
# login.defs. Also the "min" and "max" options enforce the length of the
# new password.

#password   required   pam_unix.so nullok obscure min=4 max=8 md5

# Alternate strength checking for password. Note that this
# requires the libpam-cracklib package to be installed.
# You will need to comment out the password line above and
# uncomment the next two in order to use this.
# (Replaces the `OBSCURE_CHECKS_ENAB', `CRACKLIB_DICTPATH')
#
# password required       pam_cracklib.so retry=3 minlen=6 difok=3
# password required       pam_unix.so use_authtok nullok md5

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

Ahora, debido a que nuestro servidor LDAP va a ser consultado de una manera muy constante, es una buena práctica configurar un servicio de caché para algunos datos de usuario. Mientras los datos que residan en la caché sean lo suficientemente recientes, se utilizarán estos en vez de preguntar al servidor LDAP otra vez. El servicio de cacheo de nombres (nscd) o “name service caching daemon” cumple exactamente esta tarea.

Instalamos el paquete nscd con el siguiente comando:

```
# apt-get install nscd
```

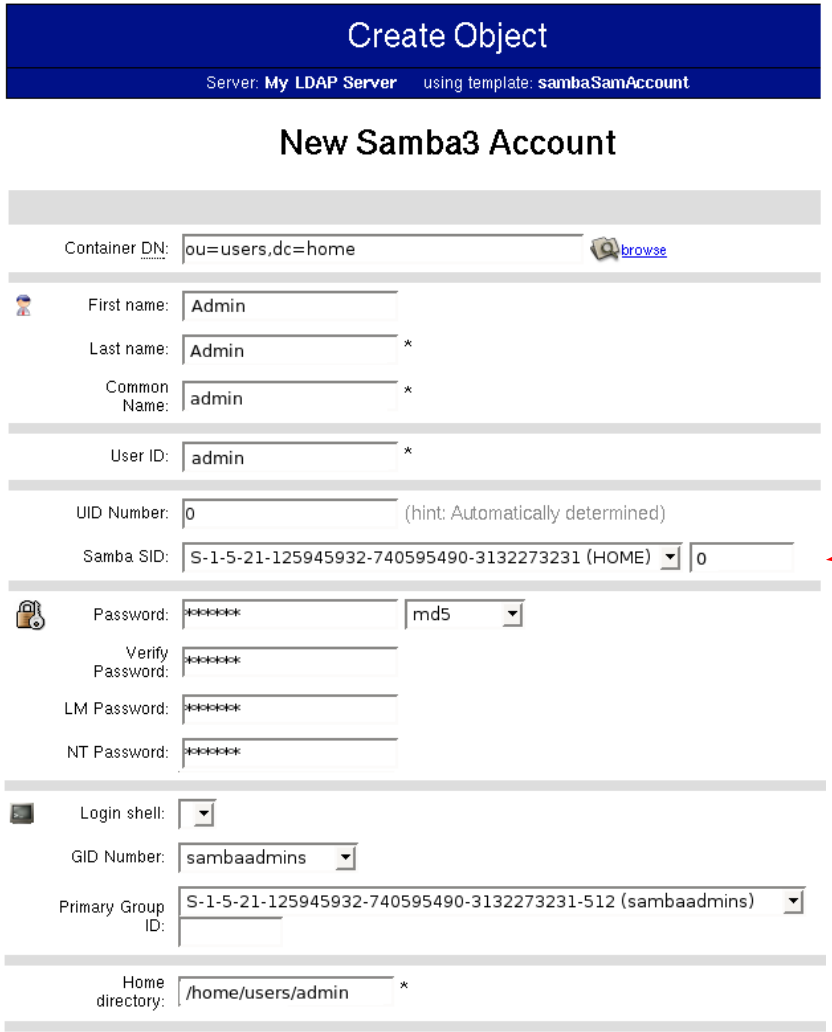
Este sería un muy buen momento para reiniciar el servicio Samba:

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

SECCIÓN 9. Agregando usuarios a nuestro directorio LDAP

Aquí, vamos a agregar algunos usuarios (“Samba 3 Accounts”). Lo primero que vamos a hacer es agregar a LDAP el usuario que va a ser el administrador (como el root) del dominio y será el **único** con permisos para unir las máquinas al dominio. Para darle esa característica de administrador/root del dominio su identificador deberá ser 0 (uid=0). El nombre de usuario que escogí fue **admin** para que fuera el mismo nombre de la cuenta root de LDAP. De paso voy a hacerlo miembro del grupo sambaadmins (“Domain Admins”). Recordar que debemos agregar a los usuarios en la **ou=users** de nuestro directorio LDAP.

En la siguiente imagen se muestra el proceso de creación de este usuario:



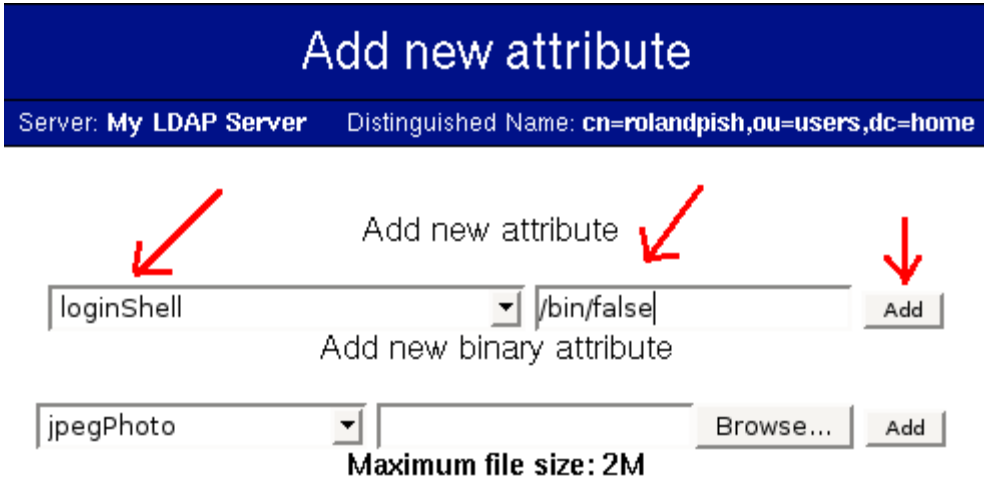
Tome en cuenta que el número UID que vaya a utilizar para el usuario también debe ser escrito al final del SAMBA SID.

Esto aplica para TODOS los usuarios que vaya a crear en LDAP

En este punto me es muy importante mencionar que por un gusto muy personal **no** quiero permitir a ninguno de los usuarios "corrientes" del directorio LDAP "loggearse" físicamente en el servidor. Si usted pudo darse cuenta, cuando agregamos al usuario **admin** de LDAP no habían opciones disponibles para escoger en el atributo `loginShell`.
Como el siguiente paso es agregar a los usuarios "corrientes" de LDAP, necesito que `phpldapadmin` **me permita** asignarle `/bin/false` al atributo `loginShell` para evitar el "loggeo" físico de esos usuarios en el servidor.
Ok, no nos preocupemos por eso en este momento. Lo haremos **inmediatamente después** de agregar la **primera cuenta** de usuario "corriente".

De esta forma, vamos a agregar un usuario corriente (roland) que lo haremos miembro de sambaadmins (privilegios de administrador localmente). Básicamente, este proceso es el mismo que ya hicimos para agregar la cuenta de usuario admin de LDAP.
NOTA: por gusto personal los UIDs de mis usuarios "corrientes" los comencé a partir de 10000.

Ahora sí, este es el momento para habilitar la opción de `/bin/false` para el atributo `loginShell` que automáticamente quedará disponible para todas las siguientes cuentas de usuarios "corrientes" que agreguemos. En la ventana de la izquierda dar click en el usuario roland: "cn=roland", en la ventana de mano derecha dar click al link que dice "Add new attribute". En la página que se carga, escoger **loginShell** en la lista desplegable y escribir **/bin/false** en la caja de texto. Luego le damos click al botón "Add" y listo! como lo muestran las flechas rojas de la imagen que se muestra a continuación:
NOTA: no digitar nada en los campos para "Add new binary attribute", no se necesitan



Por último vamos a agregar otro usuario de prueba (spiderman) que sea miembro de sambausers (limitado localmente). Observe que ahora sí es posible escoger la opción `/bin/false` en el atributo `loginShell`.

Una vez que hemos creado los usuarios, **no olvidar** crear las correspondientes carpetas home de cada uno en la ruta /home/users/<usuario> además de asignarle los permisos correspondientes del usuario y grupo al que pertenece. Si desea, puede copiar en cada una de esas carpetas los archivos ocultos ubicados en /etc/skel para que todos los usuarios tengan las mismas configuraciones iniciales para cosas como PATH, procesos de teclado y variables de entorno (esto lo hago simplemente por orden a pesar de que yo escogí que ningún usuario "corriente" va a poder loggearse físicamente al servidor). Por ejemplo, para crear la carpeta para el usuario roland y asignarle los permisos de su usuario y el grupo al que pertenece ejecutamos:

```
# mkdir /home/users/roland
# cp /etc/skel/.* /home/users/roland/
# chown -R roland /home/users/roland
# chgrp -R sambaadmins /home/users/roland
```

En este momento, podemos usar el comando getent para verificar que el nss esté trabajando correctamente en Linux:

```
# getent passwd
```

y el resultado puede contener lo siguiente:

```
...
admin:*:0:20000:admin:/home/users/admin:
roland:*:10000:20000:roland:/home/users/roland:/bin/false
spiderman:*:10001:20001:spiderman:/home/users/spiderman:/bin/false
...
```

Como se puede ver, tanto admin y roland pertenecen al grupo sambaadmins ("Domain Admins") cuyo GID es el 20000, mientras que el usuario spiderman pertenece al grupo sambausers ("Domain Users") cuyo GID es el 20001.

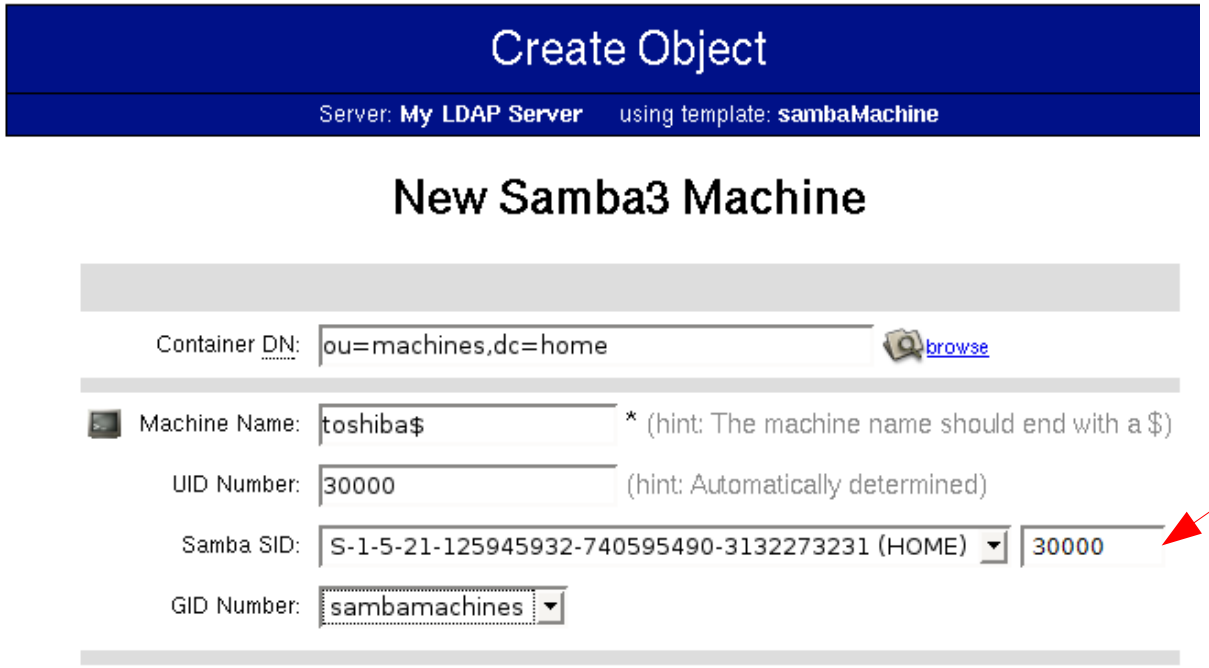
SECCIÓN 10. Uniendo máquinas a nuestro dominio Samba

Para que una máquina pueda unirse a un dominio se le solicitará el usuario y contraseña del usuario con uid=0 (en nuestro caso: admin), además es necesario crear la "cuenta de máquina" correspondiente en el directorio LDAP; si no se crea la cuenta de máquina, entonces el dominio rechaza la conexión. Ahora bien, para crear las cuentas de máquina existen dos formas de hacerlo: la forma manual y la automática.

NOTA: nuestro archivo de configuración Samba está hecho para que las cuentas de máquina sean agregadas de manera automática. Más adelante en esta sección ofreceré la explicación correspondiente.

10.1 Método manual para agregar cuentas de máquina a LDAP

Usando el phpldapadmin creamos una entrada tipo "Samba 3 Machine" bajo ou=machines y perteneciente al grupo sambamachines. A continuación muestro una imagen con el proceso:
NOTA: por gusto personal los UIDs de las máquinas los comencé a partir de 30000.



Aquí también debe escribir el UID de la máquina al final del SAMBASID.

Aplica también para TODAS las máquinas

Recuerde que tendrá que hacer esto para cada máquina que se quiera unir al dominio.

10.2 Método automático para agregar cuentas de máquina a LDAP

Recordemos por un momento la siguiente línea de configuración Samba en el archivo /etc/samba/smb.conf:

```
# script para automatizar la adicion de cuentas de maquinas
# al arbol LDAP cuando estas se unan por primera vez al dominio
add machine script = /usr/sbin/smbldap-useradd -w "%u"
```

Esto significa que vamos a usar un script hecho en Perl llamado smbldap-useradd (ubicado en /usr/sbin) provisto por el paquete smbldap-tools para automatizar el proceso de creación de cuentas de máquina en LDAP. Sin embargo, este script necesita de 2 archivos de configuración para poder trabajar: smbldap.conf y smbldap_bind.conf que tendremos que alojarlos en la carpeta /etc/smbldap-tools para que el script los pueda utilizar.

La ubicación original de estos 2 archivos es /usr/share/doc/smbldap-tools/examples. El archivo smbldap.conf se encuentra dentro de un archivo comprimido llamado smbldap.conf.gz, mientras que el archivo smbldap_bind.conf se encuentra allí directamente en la carpeta mencionada.

MUY IMPORTANTE: una vez que hemos alojado estos archivos en la carpeta /etc/smbldap-tools, cambiaremos sus permisos para que **sólo el root** pueda leerlos y modificarlos. Más adelante explico el porqué de esto.
Para alojar en /etc/smbldap-tools a los 2 archivos que necesitamos y cambiar sus permisos, vamos a ejecutar los siguientes comandos:

```
# cd /usr/share/doc/smbldap-tools/examples
# cp smbldap.conf.gz smbldap_bind.conf /etc/smbldap-tools
# cd /etc/smbldap-tools
# gunzip smbldap.conf.gz
# chown root:root *
# chmod 600 *
```

Primero vamos a configurar el archivo /etc/smbldap-tools/smbldap_bind.conf y le indicamos nuestro dominio y la contraseña del admin de LDAP. El contenido final y completo de este archivo se muestra a continuación:

```
############################
# Credential Configuration #
############################
# Notes: you can specify two differents configuration if you use a
# master ldap for writing access and a slave ldap server for reading access
# By default, we will use the same DN (so it will work for standard Samba
# release)
slaveDN="cn=admin,dc=home"
slavePw="suclave"
masterDN="cn=admin,dc=home"
masterPw="suclave"
```

Como se puede observar, la contraseña tuvo que ser escrita **directamente** y en **texto plano**. Por esta razón es que sólo el root puede acceder a leer este archivo y es por eso que le hemos cambiado los permisos a estos 2 archivos.

Ahora procedemos a configurar el archivo /etc/smbldap_tools/smbldap.conf. Como hay que cambiar diversas opciones, he preferido mostrar acá el contenido final y completo del archivo. Usted puede compararlo con el archivo original para que pueda notar las diferencias: (he eliminado algunas líneas comentadas para que no se haga tan largo)
NOTA: prepare el sambaSID que copió en la SECCIÓN 6 (Configuración de Samba) y escríbalo aquí en este archivo de configuración.

```
#
#  Purpose :
#       . be the configuration file for all smbldap-tools scripts

##############################################################################
#
# General Configuration
#
##############################################################################

# Put your own SID. To obtain this number do: "net getlocalsid".
# If not defined, parameter is taking from "net getlocalsid" return
SID="S-1-5-21-125945932-740595490-3132273231"

# Domain name the Samba server is in charged.
# If not defined, parameter is taking from smb.conf configuration file
sambaDomain="home"
```

```
##############################################################################
#
# LDAP Configuration
#
##############################################################################

# Slave LDAP server
# If not defined, parameter is set to "127.0.0.1"
slaveLDAP="127.0.0.1"

# Slave LDAP port
# If not defined, parameter is set to "389"
slavePort="389"

# Master LDAP server: needed for write operations
# If not defined, parameter is set to "127.0.0.1"
masterLDAP="127.0.0.1"

# Master LDAP port
# If not defined, parameter is set to "389"
masterPort="389"

# Use TLS for LDAP
# If set to 1, this option will use start_tls for connection
# (you should also used the port 389)
# If not defined, parameter is set to "1"
ldapTLS="0"

# How to verify the server's certificate (none, optional or require)
# see "man Net::LDAP" in start_tls section for more details
verify="none"

# CA certificate
# see "man Net::LDAP" in start_tls section for more details
#cafile="/etc/opt/IDEALX/smbldap-tools/ca.pem"

# certificate to use to connect to the ldap server
# see "man Net::LDAP" in start_tls section for more details
#clientcert="/etc/opt/IDEALX/smbldap-tools/smbldap-tools.pem"
```

```
# key certificate to use to connect to the ldap server
# see "man Net::LDAP" in start_tls section for more details
#clientkey="/etc/opt/IDEALX/smbldap-tools/smbldap-tools.key"

# LDAP Suffix
suffix="dc=home"

# Where are stored Users
# Warning: if 'suffix' is not set here, you must set the full dn for usersdn
usersdn="ou=users,${suffix}"

# Where are stored Computers
# Warning: if 'suffix' is not set here, you must set the full dn for computersdn
computersdn="ou=machines,${suffix}"

# Where are stored Groups
# Warning: if 'suffix' is not set here, you must set the full dn for groupsdn
groupsdn="ou=groups,${suffix}"

# Where are stored Idmap entries (used if samba is a domain member server)
# Warning: if 'suffix' is not set here, you must set the full dn for idmapdn
#idmapdn="ou=Idmap,${suffix}"

# Where to store next uidNumber and gidNumber available for new users and groups
# If not defined, entries are stored in sambaDomainName object.
sambaUnixIdPooldn="sambaDomainName=home,${suffix}"

# Default scope Used
scope="sub"

# Unix password encryption (CRYPT, MD5, SMD5, SSHA, SHA, CLEARTEXT)
hash_encrypt="MD5"

# if hash_encrypt is set to CRYPT, you may set a salt format.
# default is "%s", but many systems will generate MD5 hashed
# passwords if you use "$1$%.8s". This parameter is optional!
crypt_salt_format="%s"

##############################################################################
#
# Unix Accounts Configuration
#
```

```
##############################################################################

# Login defs
# Default Login Shell
userLoginShell="/bin/false"

# Home directory
userHome="/home/users/%U"

# Default mode used for user homeDirectory
userHomeDirectoryMode="700"

# Gecos
userGecos="System Computer"

# Default User (POSIX and Samba) GID
defaultUserGid="515"

# Default Computer (Samba) GID
defaultComputerGid="20003"

# Skel dir
skeletonDir="/etc/skel"

# Default password validation time (time in days) Comment the next line if
# you don't want password to be enable for defaultMaxPasswordAge days (be
# careful to the sambaPwdMustChange attribute's value)
#defaultMaxPasswordAge="45"

##############################################################################
#
# SAMBA Configuration
#
##############################################################################

# The UNC path to home drives location (%U username substitution)
# Just set it to a null string if you want to use the smb.conf 'logon home'
# directive and/or disable roaming profiles
userSmbHome=""

# The UNC path to profiles locations (%U username substitution)
# Just set it to a null string if you want to use the smb.conf 'logon path'
```

```
# directive and/or disable roaming profiles
userProfile=""

# The default Home Drive Letter mapping
# (will be automatically mapped at logon time if home directory exist)
userHomeDrive="H:"

# The default user netlogon script name (%U username substitution)
# if not used, will be automatically username.cmd
# make sure script file is edited under dos
#userScript="logon.bat"

# Domain appended to the users "mail"-attribute
# when smbldap-useradd -M is used
#mailDomain="idealx.com"

##############################################################################
#
# SMBLDAP-TOOLS Configuration
#
##############################################################################

# Allows not to use smbpasswd (if with_smbpasswd == 0 in smbldap_conf.pm) but
# prefer Crypt::SmbHash library
with_smbpasswd="0"
smbpasswd="/usr/bin/smbpasswd"

# Allows not to use slappasswd (if with_slappasswd == 0 in smbldap_conf.pm)
# but prefer Crypt:: libraries
with_slappasswd="0"
slappasswd="/usr/sbin/slappasswd"
```

Listo!

Ahora, pongámole atención por un momento a la línea de configuración que acabamos de poner en el archivo smbldap.conf:

```
# Where to store next uidNumber and gidNumber available for new users and groups
# If not defined, entries are stored in sambaDomainName object.
sambaUnixIdPooldn="sambaDomainName=home,${suffix}"
```

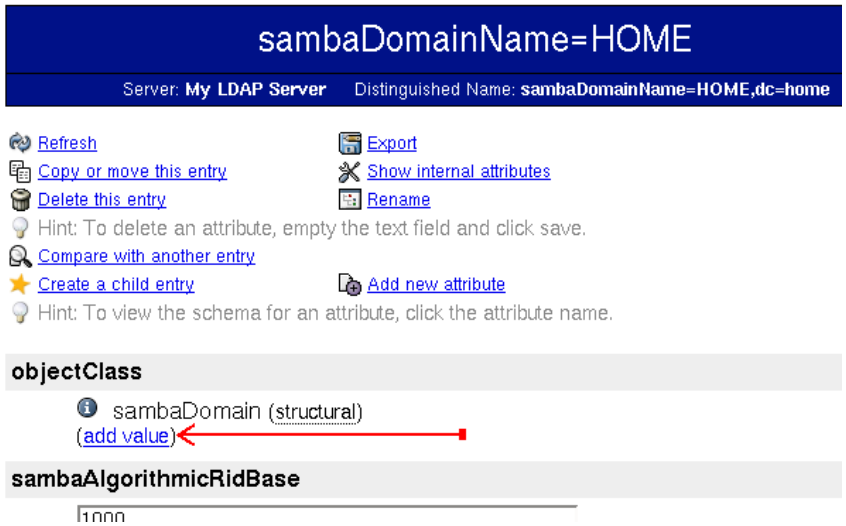
Cuando Samba llama al script smbldap-useradd para agregar automáticamente una cuenta de máquina, lo llama así: smbldap-useradd -w “%u” (tal y como lo especificamos en nuestra configuración de Samba). Podemos observar que en esa llamada **no** estamos especificando el UID ni el GID que llevará cada cuenta de máquina cuando se agregue.
Entonces es aquí donde la línea de configuración que acabamos de mostrar, nos indica que guardaremos en un atributo llamado sambaUnixIdPool los valores de UID y GID a usar en la siguiente cuenta de usuario/máquina que agreguemos en el directorio de LDAP si no especificamos directamente dichos valores.

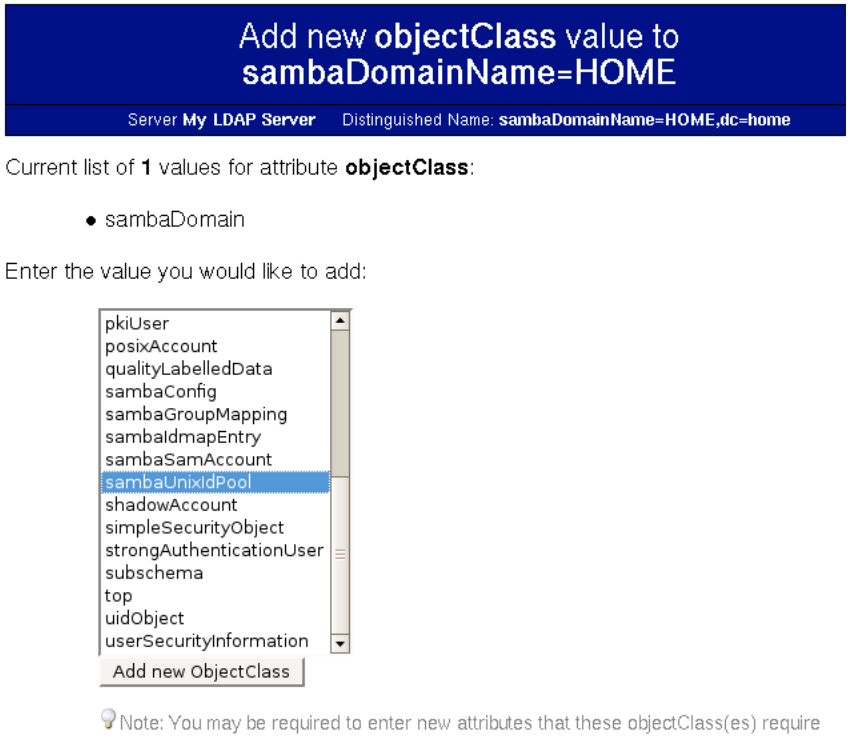
MUY IMPORTANTE: el valor del UID irá incrementando automáticamente de 1 en 1 con cada cuenta que se vaya agregando, mientras que el GID **no se incrementará** sino que se mantendrá siempre **fijo** (y de hecho es exactamente lo que ocupamos).

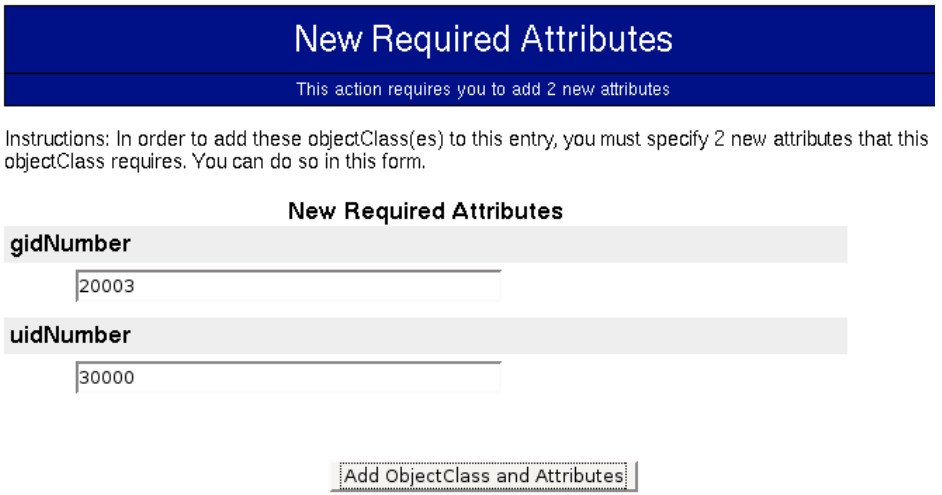
Ahora, tenemos que ir al phpldapadmin a declarar dicho atributo sambaUnixIdPool para el dominio Samba ya que por defecto no lo trae. Así que le damos click a la entrada sambaDomainName=HOME y en el espacio de la derecha vamos a buscar donde está el o los atributos tipo **objectClass**, le damos click en donde dice **add value**, escogemos **sambaUnixIdPool** y en la siguiente página digitamos los valores de UID y GID iniciales con los que vamos a arrancar para nuestros efectos.

Las siguientes imágenes muestran el proceso: (considerando los valores de UID y GID que personalmente he escogido en este documento)

NOTA: el GID 20003 corresponde a mi grupo sambamachines y el UID 30000 es el número inicial que yo quise utilizar para las cuentas de máquinas.


sambaDomainName=HOME
Server: My LDAP Server Distinguished Name: sambaDomainName=HOME,dc=home
Refresh
Export
Copy or move this entry
Show internal attributes
Delete this entry
Rename
Hint: To delete an attribute, empty the text field and click save.
Compare with another entry
Create a child entry
Add new attribute
Hint: To view the schema for an attribute, click the attribute name.
objectClass
sambaDomain (structural)
(add value)
sambaAlgorithmicRidBase
1000

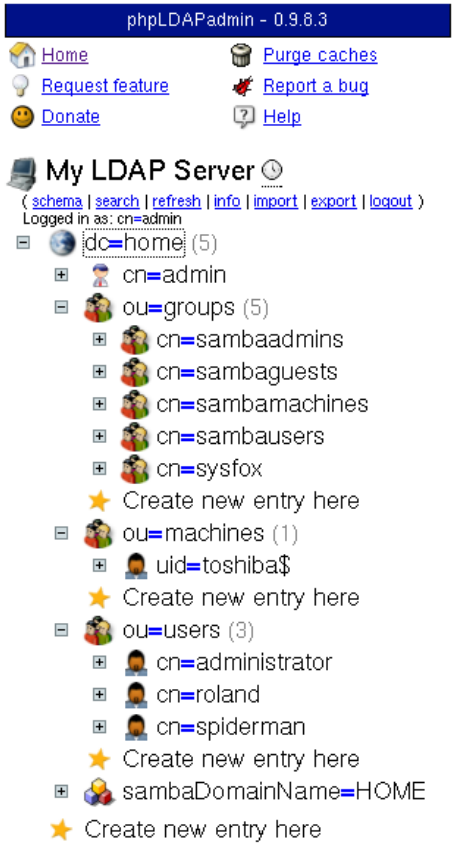

Add new objectClass value to sambaDomainName=HOME
Server My LDAP Server Distinguished Name: sambaDomainName=HOME,dc=home
Current list of 1 values for attribute objectClass:
• sambaDomain
Enter the value you would like to add:
pkiUser
posixAccount
qualityLabelledData
sambaConfig
sambaGroupMapping
sambaIdmapEntry
sambaSamAccount
sambaUnixIdPool
shadowAccount
simpleSecurityObject
strongAuthenticationUser
subschema
top
uidObject
userSecurityInformation
Add new ObjectClass
Note: You may be required to enter new attributes that these objectClass(es) require


New Required Attributes
This action requires you to add 2 new attributes
Instructions: In order to add these objectClass(es) to this entry, you must specify 2 new attributes that this objectClass requires. You can do so in this form.
New Required Attributes
gidNumber
20003
uidNumber
30000
Add ObjectClass and Attributes

SECCIÓN 11. Agregando un grupo Posix

¿Qué son los grupos Posix?
Son grupos "normales" de usuarios. ¿Qué quiero decir con "normales"? Que **no** son grupos **mapeados** especiales.
En mi caso particular yo quise tener un recurso compartido llamado **sysfox** que contiene unos sistemas en fox los cuáles **sólo** deberán ser accesibles por ciertos usuarios. Para este propósito yo creé un grupo "normal" (Posix) de usuarios llamado **sysfox** (creado en ou=groups). Una vez que usted cree el primer grupo Posix deberá agregarle un atributo llamado **memberUid** (usando el mismo proceso que hicimos para agregar el atributo loginShell al usuario roland) que le va a servir para ir agregando miembros a este y a cualquier grupo Posix. Con este tema de los atributos usted ya se va dando cuenta la infinidad de atributos que pueden usarse con los diferentes objetos de LDAP. Allí es donde usted podrá personalizarlo a su gusto y necesidad específica.

La siguiente imagen muestra cómo está organizado mi directorio de LDAP hasta el momento:



Hasta este momento tenemos un directorio LDAP sumamente sencillo. A partir de aquí existen muchísimas opciones y directivas que se pueden utilizar según su necesidad específica.

NOTA: también existen comandos de consola para llevar a cabo las operaciones en el directorio LDAP pero no están en el alcance de este documento. En cuanto me sea posible las incluiré en una nueva versión de esta guía.

APÉNDICE A. Unir clientes de Windows XP al dominio.

Si desea unir al dominio una computadora con el sistema operativo Windows XP Profesional, deberá hacer un pequeño ajuste. Ejecutar el regedit e ir a la siguiente clave:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters`

y en el valor de "`requiresignorseal`" que es de tipo dword asignarle 0
también al valor de "`requirestrongkey`" que es de tipo dword asignarle 0

Deberá reiniciar la computadora para que los cambios surtan efecto.

APÉNDICE B. Respaldo y restauración de la base de datos LDAP.

Esta es una información muy valiosa suministrada por Novell que habla acerca del respaldo y restauración de la base de datos de nuestro directorio LDAP en un sistema Novel Suse.

NOTA: no he probado ninguno de estos procedimientos pero adjunto dicha información para que pueda ser probada y revisada

B.1 Backup and Restore

All system information (system structure, the configuration and deployment method for each Branch Server and Point of Service terminal, image information, and so forth) is stored in an LDAP directory on the Administration Server. This information must be backed up regularly to protect against data loss in case of storage failure and administration errors.
It is recommended that, at a minimum, you do an online logical backup to a local file before any complex reconfiguration of the system.
The following sections discuss methods you can use to backup and restore your Service LDAP directory.

Offline Physical Backup

An offline backup must be executed on the Administration Server and does not put any load on the LDAP server. The drawback is that the LDAP server is not available during the time of the backup.
To perform a physical file backup of the LDAP directory:

1. Stop the LDAP server using the /usr/sbin/rcldap stop command.
2. Copy all the files in the /var/lib/ldap/ directory to an archive directory.
3. After the copy completes, start the LDAP server using the /usr/sbin/rcldap start command.

Offline Logical Backup

To perform a logical backup of the LDAP directory (database dump):

1. Stop the LDAP server using the /usr/sbin/rcldap stop command.
2. Run the slapcat >ldap.\$(date +'\%Y\%m\%d-\%T') command.

This generates an LDIF file named ldap.datetime where datetime is the current date and time. The output file can be archived, backed up on offline media, and restored with the slapadd command. The LDIF file is a structured ASCII file that can be viewed, for example, with the less command.

3. After the backup completes, start the LDAP server by using the /usr/sbin/rcldap start command.

Online Backup

An online backup uses the LDAP server to extract all data. This has the advantage that the server is available at all times and the backup can be taken from a remote machine that has an LDAP client.

Run the following command:

ldapsearch -h LDAPServer -x -b baseDN > ldap.\$(date +'\%Y\%m\%d-\%T')

where:

LDAPServer is the LDAP server name or IP address.
baseDN is the base DN (distinguished name) of the LDAP structure (for example, o=mycorp,c=us).

This creates an LDIF file like the slapcat command used for offline backup.

This file must be added to the LDAP server with the ldapadd command. Do not use slapadd with this file.
If access controls are implemented on the LDAP server, an authenticated LDAP bind must be used. In this case, the previous command should be extended with the following arguments:

ldapsearch -x -D adminDN -w adminPassword

where:

adminDN is the DN of the administrator user (for example, cn=admin,o=mycorp,c=us).
adminPassword is this user's password (for example, secret).

Restore

To restore an offline backup:

1. Stop the LDAP server using the /usr/sbin/rcldap stop command.
2. If you did a physical file backup, restore the files in /var/lib/ldap.

or
If you did a logical backup, run the slapadd command to restore the logical database dump:

slapadd -l backupfile

where backupfile is the file created by slapcat.

3. Start the LDAP server using the /usr/sbin/rcldap start command.

To restore an online backup, the LDAP server must be running. The LDAP server is able to run with an empty database. If the database has been corrupted, the database files in /var/lib/ldap/ must be removed before restoring the online backup.

1. To restore a backup file taken with ldapsearch, run the following command:

ldapadd -D adminDN -x -w adminPassword -h LDAPServer -x -f backupfile