HOWTO: LDAP + SAMBA

Instalando los paquetes

apt-get install slapd ldap-utils samba samba-doc libpam-smbpass smbclient smbldap-tools

Vamos a usar dc=tuxnetworks,dc=com

Llenar el servidor con lo más básico
***Acordarse de cambiar dc=tuxnetworks,dc=com con la configuración deseada

ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/cosine.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/nis.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/inetorgperson.ldif

Creamos el archivo LDIF. Crearemos estos archivos dentro de /home/usuarioquetengas

cd /home/usuarioquequieras
gedit backend.ldif

Con el siguiente contenido:

```
dn: cn=module,cn=config
objectClass: olcModuleList
cn: module
olcModulepath: /usr/lib/ldap
olcModuleload: back_hdb


dn: olcDatabase=hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {1}hdb
olcSuffix: dc=tuxnetworks,dc=com
olcDbDirectory: /var/lib/ldap
olcRootDN: cn=admin,dc=tuxnetworks,dc=com
olcRootPW: mypassword
olcDbConfig: set_cachesize 0 2097152 0
olcDbConfig: set_lk_max_objects 1500
olcDbConfig: set_lk_max_locks 1500
olcDbConfig: set_lk_max_lockers 1500
olcDbIndex: objectClass eq
olcLastMod: TRUE
```

olcDbCheckpoint: 512 30
olcAccess: to attrs=userPassword by dn="cn=admin,dc=tuxnetworks,dc=com" write by anonymous auth by self write by * none
olcAccess: to attrs=shadowLastChange by self write by * read
olcAccess: to dn.base="" by * read
olcAccess: to * by dn="cn=admin,dc=tuxnetworks,dc=com" write by * read

***** Acordarse de cambiar dc=tuxnetworks,dc=com y olcrootPW con lo que tengas que usar.

Ahora añadimos esa configuración al servidor:

sudo ldapadd -Y EXTERNAL -H ldapi:/// -f backend.ldif

Descarga esta configuración de samba:

wget http://www.tuxnetworks.com/configs/smb.conf

Editala con tus datos y la reemplazas con el smb.conf antiguo

cp smb.conf /etc/samba/

Le ponemos la contraseña, yo recomiendo que sea la misma que ldap:

smbpasswd -W

Reiniciamos samba:

service smbd restart

Para comprobar que funciona bien usamos: samba-client (Cuando nos pregunte por la contraseña, le damos al INTRO):

sudo smbclient -L localhost

Verás algo asi;

usuario@pc:~$ sudo smbclient -L localhost
Enter root's password:
Anonymous login successful
Domain=[SAMBA] OS=[Unix] Server=[Samba 3.4.7]

Sharename Type Comment
--------- ---- -------
print$ Disk Printer Drivers Share

shared Disk
archive Disk
IPC$ IPC IPC Service (Samba 3.4.7)
Anonymous login successful
Domain=[SAMBA] OS=[Unix] Server=[Samba 3.4.7]

Server Comment
--------- -------
CALLISTO Samba 3.4.7

Workgroup Master
--------- -------
SAMBA CALLISTO

Creamos los directorios netlogon para los usuarios

mkdir -v -m 777 /var/lib/samba/profiles
mkdir -v -p -m 777 /var/lib/samba/netlogon

Necesitamos instalar las estructuras para el servidor LDAP. Estas estructuras son parte del paquete samba-docs que hemos instalado anteriormente.

cp /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz /etc/ldap/schema/
gzip -d /etc/ldap/schema/samba.schema.gz

Necesitamos transformar estas estructuras a LDIF para poder usarlas.

Crear un archivo llamado schema_convert.conf

gedit schema_convert.conf

Y pegar estas lineas:

include /etc/ldap/schema/core.schema
include /etc/ldap/schema/collective.schema
include /etc/ldap/schema/corba.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/duaconf.schema
include /etc/ldap/schema/dyngroup.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/java.schema
include /etc/ldap/schema/misc.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/openldap.schema

include /etc/ldap/schema/ppolicy.schema
include /etc/ldap/schema/samba.schema

Ahora usamos slapcat para convertirlo a LDIF:

slapcat -f schema_convert.conf -F ~ -n0 -s "cn={12}samba,cn=schema,cn=config" > cn=samba.ldif

slapcat generará el archivo "cn\=samba.ldif". Edita este archivo:

gedit cn\=samba.ldif

Y cambia los siguientes atributos:

dn: cn={12}samba,cn=schema,cn=config
...
cn: {12}samba

a

dn: cn=samba,cn=schema,cn=config
...
cn: samba

También, elimina estas lineas del final del archivo:

structuralObjectClass: olcSchemaConfig
entryUUID: 99e797a8-07cb-102f-8c5c-739a8467e607
creatorsName: cn=config
createTimestamp: 20100609043122Z
entryCSN: 20100609043122.188753Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20100609043122Z

Añadir la estructuctura al servidor;

sudo ldapadd -Y EXTERNAL -H ldapi:/// -f cn\=samba.ldif

Debería devolver este mensaje sin errore:.

adding new entry "cn=samba,cn=schema,cn=config"

Comprobemos como van las cosas con:

sudo ldapsearch -Y EXTERNAL -H ldapi:/// -D cn=admin,cn=config -b cn=config -W olcDatabase={1}hdb

Al final deberíam

search result
search: 2
result: 0 Success

numResponses: 2
numEntries: 1

Si ves una salida como esta, es que el servidor LDAP funciona, pero tenemos que configurar un poco a samba

Descomprimir samba-ldap-tools:

gzip -d /usr/share/doc/smbldap-tools/configure.pl.gz

Vamos a ejecutar un script en perl. Para casi todas las opciones le daremos a INTRO. Pero hay unas excepciones. Cuando nos pregunten por "logon home" and "logon path" escribir un "." (punto) y nada mas. Cuando nos pregunten por una contraseña (ldap master/slave bind password) Usar la contraseña para admin que hemos usado antes. Recuerda dejar por defecto los demás parámetros.

ejecutamos el script;

perl /usr/share/doc/smbldap-tools/configure.pl

Ahora que el script nos ha creado la configuración, podemos rellenar el servidor;

smbldap-populate

Últimos retoques;

/etc/init.d/slapd stop
slapindex
chown openldap:openldap /var/lib/ldap/*
/etc/init.d/slapd start

Hacer a “root” el administrador del dominio:

smbldap-groupmod -m 'root' 'Administrators'

Si al añadir el usuario no nos da ningún mensaje de error, es que todo está bien.

Ahora, necesitamos que los clientes se autentifiquen con el servidor. Para esto, instalaremos un paquete.

apt-get --yes install ldap-auth-client

Le decimos a PAM que use LDAP para autentificarse:

auth-client-config -t nss -p lac_ldap
pam-auth-update ldap

Si todo está bien, podremos añadir un usuario al servidor

smbldap-useradd -a -m -P juan

Puedes comprobar el nuevo usuario usando:

ldapsearch -xLLL -b "dc=tuxnetworks,dc=com" uid=juan

Para los clientes, instalar:

apt-get install libpam-ldap libnss-ldap nss-updatedb libnss-db