Neste apartado abordaremos os pasos necesarios para instalar o servidor Samba e configuralo para que use como base de datos de usuarios o servidor LDAP. Pero en primeiro lugar, teremos que engadir no LDAP o esquema de samba, que define unha serie de atributos que o servidor samba precisará almacenar para as propiedades dos usuarios no dominio Windows.

Contenido

- 1 Instalación do servidor Samba
- 2 Configurar o servidor LDAP para servir de base de datos de samba
  - 2.1 Incluír o esquema de samba no servidor LDAP
  - 2.2 Engadir os índices necesarios para as buscas de samba
- 3 Configurar o servidor samba
  - 3.1 Parámetros básicos na rede Windows
  - 3.2 Parámetros para actuar como controlador de dominio
  - 3.3 Parámetros para utilizar o servidor LDAP como backend
  - 3.4 Parámetros de rexistro e rendemento
  - 3.5 Parámetros para a compartición de recursos
  - 3.6 Proporcionarlle a samba o contrasinal do LDAP
  - 3.7 Inicializar o dominio samba

Instalación do servidor Samba

Imos instalar tres paquetes: O servidor samba, a documentación e unha serie de utilidades para xestionar os usuarios e grupos de samba no LDAP:

```
sudo apt-get install samba samba-doc smbldap-tools
```

Configurar o servidor LDAP para servir de base de datos de samba

Incluír o esquema de samba no servidor LDAP

- O paquete **samba-doc** inclúe o esquema de samba para o LDAP en formato *schema* e comprimido, así que seguiremos case os mesmos pasos que na instalación de kerberos para introducir o esquema no LDAP.

- Descomprimimos o ficheiro co esquema e transformámolo a formato LDIF para poder engadilo no LDAP:

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

- Creamos o ficheiro *schema_convert.conf* co seguinte contido (**NOTA**: Quitar a liña *include /etc/ldap/schema/kerberos.schema* se non se usa kerberos):

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

- Creamos un directorio temporal para almacenar o ficheiros LDIF:

```
mkdir /tmp/ldif_output
```

- Usamos o comando *slapcat* para converter o ficheiro de esquema a LDIF (**NOTA**: Substituír o 13 por 12 se non se usa kerberos):

```
slapcat -f schema_convert.conf -F /tmp/ldif_output -n0 -s "cn={13}samba,cn=schema,cn=config" > /tmp/cn=samba.ldif
```

- Editamos o ficheiro creado por *slapdcat /tmp/cn\=samba.ldif,* cambiando estes dous atributos:

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

- e borrando as seguintes liñas que se atopan ao final do ficheiro:

```
structuralObjectClass: olcSchemaConfig
entryUUID: b53b75ca-083f-102d-9fff-2f64fd123c95
creatorsName: cn=config
createTimestamp: 20080827045234Z
entryCSN: 20080827045234.341425Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20080827045234Z
```

- Cargamos o esquema en formato LDIF (contrasinal *1234*):

```
```

```
ldapadd -x -D cn=admin,cn=config -W -f /tmp/cn\=samba.ldif
Enter LDAP Password:
adding new entry "cn=samba,cn=schema,cn=config"
```

Engadir os índices necesarios para as buscas de samba

- Neste caso imos engadir un conxunto de campos bastante grande que van ser índices no LDAP, así que os introduciremos nun ficheiro. Introducimos o seguinte contido no ficheiro *samba_indices.ldif*:

```
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: uidNumber eq
olcDbIndex: gidNumber eq
olcDbIndex: loginShell eq
olcDbIndex: memberUid eq,pres,sub
olcDbIndex: uniqueMember eq,pres
olcDbIndex: sambaSID eq
olcDbIndex: sambaPrimaryGroupSID eq
olcDbIndex: sambaGroupType eq
olcDbIndex: sambaSIDList eq
olcDbIndex: sambaDomainName eq
olcDbIndex: default sub
```

- E cargamos os índices no LDAP con *ldapmodify* (de novo contrasinal *1234*):

```
ldapmodify -x -D cn=admin,cn=config -W -f samba_indices.ldif
Enter LDAP Password:
modifying entry "olcDatabase={1}hdb,cn=config"
```

Configurar o servidor samba

Neste apartado imos realizar a configuración básica do servidor samba, para poder utilizalo como un servidor de dominio Windows e que tome os usuarios do servidor LDAP.

Todos os parámetros de configuración do servidor samba residen no ficheiro **smb.conf**, que en Ubuntu Server podemos atopar na ruta **/etc/samba/smb.conf**. Este ficheiro contén un montón de parámetros (cada un nunha liña coa sintaxe *parámetro = valor*) agrupados en **seccións**. O comezo de cada sección indícase por unha liña que contén o nome da sección entre corchetes (por exemplo *[global]*, *[homes]*, *[comun]*, etc.), e a continuación todos os parámetros que se inclúan nas seguintes liñas pertencen a esa sección. O fin dunha sección márcase co comezo da seguinte sección, ou co final do ficheiro.

Cada sección describe os parámetros de configuración dun recurso compartido, e o nome da sección será o nome do recurso compartido. Así, a sección *[comun]* define o recurso compartido *comun*, e dentro dela definiremos os parámetros do recurso: que carpeta se comparte, con que permisos, etc.

Hai tres seccións especiais:

- **[global]**: Esta é a sección que engloba os parámetros de configuración globais do servidor samba, e polo tanto é a única que non se corresponde con un recurso compartido.

- **[homes]**: É un recurso compartido especial que comparte todas as carpetas persoais dos usuarios, de forma que cando un usuario inicia sesión no servidor samba, verá a súa carpeta persoal.
- **[printers]**: É un recurso compartido especial que comparte todas as impresoras do equipo.

Podemos contar por centos o número de parámetros que pode conter o ficheiro de configuración de samba, así que o que se presenta aquí é un exemplo de configuración cos parámetros de configuración máis relevantes explicados con comentarios (as liñas que comezan por # son comentarios), pero por suposto dependendo das circunstancias concretas pode ser necesario axustar outros parámetros que no exemplo non aparecen. Remítese ao lector ao manual do ficheiro *smb.conf* (http://us1.samba.org/samba/docs/man/manpages-3/smb.conf.5.html) para obter información dos parámetros que se poden usar.

No noso caso, o paquete do servidor samba inclúe un ficheiro *smb.conf* con unha serie de información de exemplo e moitos comentarios; pero nós imos completar o noso ficheiro de configuración dende cero. Así que borramos o ficheiro */etc/samba/smb.conf* e comezamos a editar un novo ficheiro baleiro con este mesmo nome. Introducimos a liña que marca o comezo da sección *global*:

```
[global]
```

Parámetros básicos na rede Windows

A continuación introducimos os parámetros básicos para o servidor de samba na rede Windows, como é o nome do equipo, descrición, etc:

```
#
# PARAMETROS BASICOS DA REDE WINDOWS
#
# Nome do dominio
workgroup = IESCALQUERA
# Nome do equipo na rede Windows
netbios name = server00
# Descricion do equipo na rede Windows
server string = Servidor de dominio do IES Calquera
# O servidor actua como servidor WINS (Resolucion de nomes na rede Windows)
wins support = yes
# O parametro security e un dos mais importantes, xa que determina o modo en que samba controla o acceso
# aos recursos compartidos. Os valores posibles son:
# share: Establecese unha autenticacion por recurso compartido. Non se recomenda
# user: Opcion por defecto. O usuario autentificase ao acceder ao servidor
# domain: Usaremola cando o equipo estea integrado nun dominio Windows NT e samba valida os usuarios contra o PDC
# server: Samba valida os usuarios contra outro servidor samba
# ads: Usaremola cando o equipo estea integrado nun dominio con Active Directory. Samba usara kerberos para autentic
security = user
```

Parámetros para actuar como controlador de dominio

Os seguintes parámetros configuran o servidor samba como un controlador dun dominio Windows:

```
#
# PARAMETROS DE CONTROLADOR DE DOMINIO WINDOWS
#
# Para activar a autentificación de clientes do dominio
domain logons = yes
# Este número indica na rede Windows o tipo de sistema operativo do equipo. Desta maneira, estamoslle
# dicindo ao resto dos equipos da rede Windows que este equipo e un servidor
os level = 65
# Para que actúe como servidor do dominio
domain master = yes
# Conecta a carpeta persoal do usuario na unidade Z: do cliente
logon drive = Z:
# Indica onde se atopa a carpeta persoal do usuario (\\Servidor\NomeUsuario)
# Teremos que compartir con samba os directorios home dos usuarios para que esa comparticion exista
logon home = \\%N\%U
# Indica onde se almacena a configuracion persoal do usuario (o seu perfil)
# Por defecto gardase dentro do directorio persoal, pero poderia interesarnos gardalos nunha carpeta
# particion aparte, poñendo por exemplo o valor \\%N\perfis\%U
logon path = \\%N\%U\profile
```

Parámetros para utilizar o servidor LDAP como *backend*

Para configurar samba para que use o LDAP como *backend*, introducimos a seguinte configuración:

```
#
# PARAMETROS PARA OBTER OS USUARIOS DO LDAP
#
# Indicamos que use o servidor LDAP para obter os usuarios. Non e necesaria a conexion segura xa
# que o servidor LDAP esta na mesma maquina. Tamen poderiamos poñer ldapi:///
passdb backend = ldapsam:"ldap://localhost"

# Parametros para a conexion co LDAP e localizar os distintos elementos
ldap suffix = dc=iescalquera,dc=local
ldap user suffix = ou=usuarios
ldap group suffix = ou=grupos
ldap machine suffix = ou=maquinas
ldap idmap suffix = ou=idmap
ldap admin dn = cn=admin,dc=iescalquera,dc=local
ldap ssl = no
ldap passwd sync = yes

# Con estes parametros samba usara o servidor LDAP para obter a asignacion
# entre UIDs e GIDs cos identificadores dos usuarios en Windows:
idmap backend = ldap:ldap://localhost
idmap uid = 10000-20000
idmap gid = 10000-20000

# Estes scripts permiten que o servidor de samba poida dar de alta maquinas no LDAP (por exemplo,
# cando se agrega un equipo no dominio) e xestionar os usuarios e grupos, de forma que se poden
# manipular con ferramentas de xestión de Windows:
add user script = /usr/sbin/smbldap-useradd -a -m '%u'
delete user script = /usr/sbin/smbldap-userdel '%u'
add group script = /usr/sbin/smbldap-groupadd -p '%g'
delete group script = /usr/sbin/smbldap-groupdel '%g'
add user to group script = /usr/sbin/smbldap-groupmod -m '%u'  '%g'
delete user from group script = /usr/sbin/smbldap-groupmod -x '%u'  '%g'
set primary group script = /usr/sbin/smbldap-groupmod -g '%g'  '%u'
add machine script = /usr/sbin/smbldap-useradd -w '%u'
```

Parámetros de rexistro e rendemento

Os seguintes parámetros axustan os ficheiros e nivel de rexistro (log) do servidor samba e

axustes para obter un mellor rendemento:

```
#
# PARAMETROS DE REXISTRO E RENDEMENTO
#
# Desta forma o servidor samba manten un ficheiro de rexistro por cada cliente que se conecta
log file = /var/log/samba/log.%m
# Tamano maximo dos ficheiros de rexisto (en KB)
max log size = 1000
# O servidor mostrase como un servidor de tempo para os clientes Windows
time server = yes
# Opcions de rendemento recomendadas para Linux
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
# Evita que busque por dns nomes de equipo de NetBIOS
dns proxy = no
```

Parámetros para a compartición de recursos

Os seguintes parámetros poden ser interesantes na compartición de carpetas por samba:

```
#
# PARAMETROS DE COMPARTICION DE RECURSOS
#
# Oculta para os clientes ficheiros especiais como sockets e dispositivos
hide special files = yes
# Comparte como ocultos os ficheiros que comezan por punto (os ocultos de Linux)
hide dot files = yes
# Oculta para os clientes os ficheiros e directorios para os que o usuario non ten permiso de lectura
hide unreadable = yes
```

Proporcionarlle a samba o contrasinal do LDAP

- Para rematar a configuración do servidor samba, temos que proporcionarlle o contrasinal do administrador do LDAP (indicado no parámetro *ldap admin dn*) para que poida acceder a este servizo con privilexios administrativos. Este contrasinal non se almacena como un parámetro máis do servidor de samba porque o ficheiro de configuración de samba pode ser lido por todos os usuarios, e é conveniente gardalo nun ficheiro máis seguro (ficheiro *secrets.tdb*).

- Para subministrar a clave usaremos o comando **smbpasswd**:

```
sudo smbpasswd -w admin
```

- E reiniciamos o servidor samba para activar a configuración:

```
sudo service smbd restart
sudo service nmbd restart
```

Inicializar o dominio samba

Para que o noso dominio samba funcione correctamente, é necesario inicializar o dominio cos usuarios, grupos e obxectos LDAP necesarios para almacenar toda a información do mesmo. O paquete *smbldap-tools* inclúe un comando que xa nos solicitará os datos necesarios para inicializar o dominio samba, pero antes de poder utilizalo debemos configurar o paquete con todos os datos do noso dominio, para o cal usaremos un script que tamén inclúe o paquete *smbldap-tools*.

En primeiro lugar realizaremos dúas comprobacións que se recomendan no inicio do propio script e nos permitirán comprobar que o servidor samba está en execución e que a conexión co servidor LDAP é correcta:

- Comprobamos que o servidor samba está efectivamente correndo:

```
sudo service smbd status
smbd start/running, process xxxxx
sudo service nmbd status
nmbd start/running, process xxxxx
```

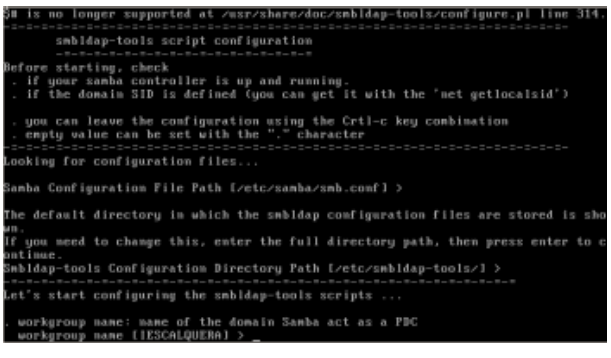
- E que o equipo xa ten un SID (*Identificador de seguridade* de Windows):

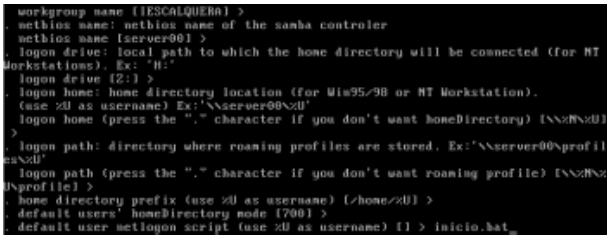
```
sudo net getlocalsid
SID for domain SERVER00 is: S-1-5-21-517027167-838517763-176716501
```

Se as comprobacións dan un resultado correcto, podemos executar o script de configuración de *smbldap-tools*:

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

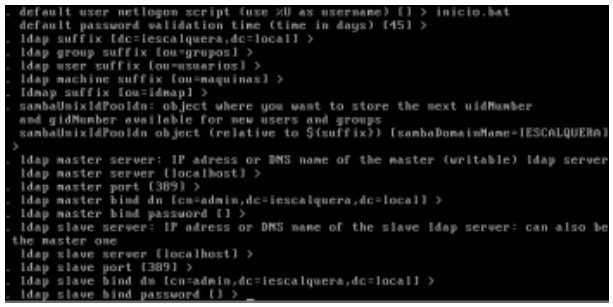
Script de configuración de smbldap-tools

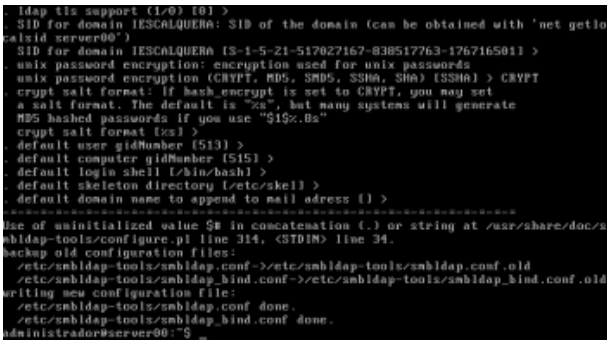




Inicio do script. Veremos que na maioría dos parámetros a opcións que nos propón por defecto xa é a que debemos poñer, xa que a obtén do ficheiro *smb.conf*; só teremos que premer *Enter*

Só imos cubrir o nome do ficheiro de inicio de sesión (*netlogon script*), xa que aínda non o configuramos en *smb.conf*, pero será *inicio.bat*





Todo está ok, introducimos cando se nos pide o contrasinal do administrador do LDAP(*admin*)

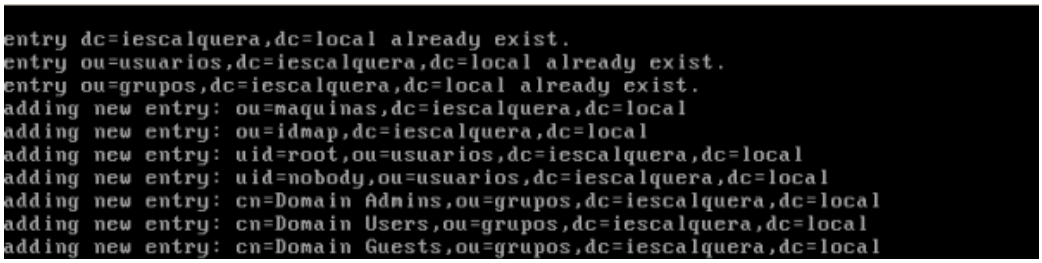
Só indicamos que o formato dos contrasinais e *crypt*, xa que é o formato usado en Linux

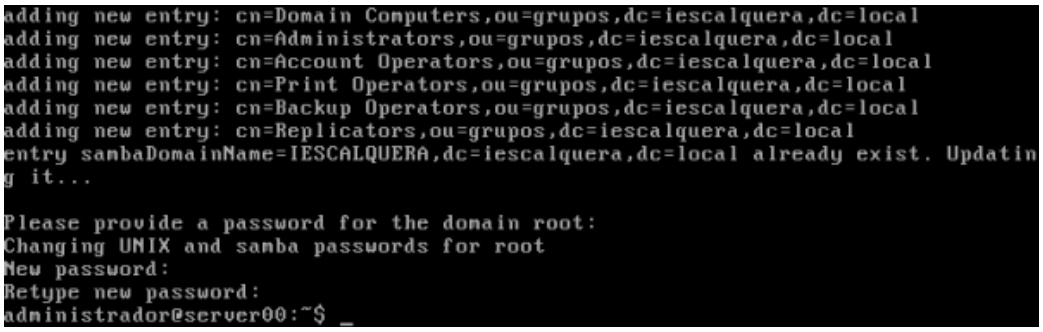
Como podemos ver no remate do script, crea a partir dos valores indicados os ficheiros */etc/smbldap-tools/smbldap.conf* e */etc/smbldap-tools/smbldap_bind.conf*, que podemos modificar posteriormente en caso de que tivésemos introducido algún valor erróneo.

Agora xa podemos executar o comando **smbldap-populate** para crear os usuarios, grupos e obxectos LDAP necesarios para o dominio samba. Antes de facelo, é conveniente facer unha copia de todo o contido do LDAP, para o que podemos usar o comando **slapcat**:

```
sudo slapcat -l backup.ldif
sudo smbldap-populate
```

Como se pode ver na imaxe, o comando crea as unidades organizativas no LDAP necesarias para almacenar toda a información de samba e os grupos propios dun dominio Windows (Administradores do dominio, Usuarios do dominio, etc.). Tamén crea o usuario root no LDAP e como usuario samba, e teremos que asignarlle un contrasinal:




adding new entry: cn=Domain Computers,ou=grupos,dc=iescalquera,dc=local
adding new entry: cn=Administrators,ou=grupos,dc=iescalquera,dc=local
adding new entry: cn=Account Operators,ou=grupos,dc=iescalquera,dc=local
adding new entry: cn=Print Operators,ou=grupos,dc=iescalquera,dc=local
adding new entry: cn=Backup Operators,ou=grupos,dc=iescalquera,dc=local
adding new entry: cn=Replicators,ou=grupos,dc=iescalquera,dc=local
entry sambaDomainName=IESCALQUERA,dc=iescalquera,dc=local already exist. Updatin
g it...
Please provide a password for the domain root:
Changing UNIX and samba passwords for root
New password:
Retype new password:
administrador@server00:~$ _