Configuració d'un servidor Debian Lenny com a controlador primari de domini amb clients Windows

1. Instal·lem Debian Lenny sense entorn gràfic
2. nano /etc/network/interfaces

```
iface eth0 inet static
address 192.168.1.220
netmask 255.255.255.0
gateway 192.168.1.1
```

3. nano /etc/apt/sources.list

```
# deb cdrom:[Debian GNU/Linux 5.0.1 _Lenny_ - Official i386 CD Binary-
1 20090413-00:10]/ lenny main
```

4. nano /etc/resolv.conf

```
nameserver 192.168.1.1
nameserver 80.58.0.33
```

5. apt-get install apache2
6. apt-get install slapd ldap-utils

Dada sol·licitada	**Dada a introduir**
Administrator password	PASSWORD
Confirm password	PASSWORD

7. dpkg-reconfigure slapd

Dada sol·licitada	**Dada a introduir**
Omit OpenLDAP server configuration?	No
DNS domain name	domini.com
Organization name	domini.com
Administrator password	PASSWORD
Confirm password	PASSWORD
Database backend to use	HDB
Do you want the database to be removed when slapd is purged?	No
Move old database?	Sí
Allow LDAPv2 protocol?	No

8. slapcat > ~/slapd.ldif
9. ldapsearch -x -b "dc=domini,dc=com"
10. apt-get install smbldap-tools phpldapadmin
11. /etc/init.d/apache2 restart
12. apt-get install samba smbclient smbfs samba-doc

Dada sol·licitada	**Dada a introduir**
Nom del domini	DOMINI
Modificar smb.conf perquè utilitzi la configuració WINS del DHCP?	No

13. zcat /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz > /etc/ldap/schema/samba.schema
14. slappasswd -h {MD5}
15. wget http://www.proferamon.com/documents/pdc/slapd.conf
16. cp slapd.conf /etc/ldap/slapd.conf
17. /etc/init.d/slapd stop
18. rm -rf /var/lib/ldap/*
19. slapadd -l ~/slapd.ldif
20. slapindex
21. chown -Rf openldap:openldap /var/lib/ldap
22. /etc/init.d/slapd start
23. slapcat
24. wget http://www.proferamon.com/documents/pdc/smb.conf
25. cp smb.conf /etc/samba/smb.conf
26. smbpasswd -w PASSWORD
27. mkdir -p /var/lib/samba/netlogon /var/lib/samba/profiles
28. chown -Rf root:root /var/lib/samba/netlogon/ /var/lib/samba/profiles/
29. chmod 1777 /var/lib/samba/profiles/
30. /etc/init.d/samba restart
31. testparm
32. zcat /usr/share/doc/smbldap-tools/examples/smbldap.conf.gz > /etc/smbldap-tools/smbldap.conf
33. cp /usr/share/doc/smbldap-tools/examples/smbldap_bind.conf /etc/smbldap-tools/smbldap_bind.conf
34. wget http://www.proferamon.com/documents/pdc/smbldap.conf
35. cp smbldap.conf /etc/smbldap-tools/smbldap.conf
36. net getlocalsid
    copiem el samba SID en un lloc apart
37. nano /etc/smbldap-tools/smbldap.conf
    canviem el samba SID pel que hem copiat anteriorment
38. nano /etc/smbldap-tools/smbldap_bind.conf

```
############################
# 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=domini,dc=com"
slavePw="PASSWORD"
masterDN="cn=admin,dc=domini,dc=com"
masterPw="PASSWORD"
```

39. chmod 0644 /etc/smbldap-tools/smbldap.conf
40. chmod 0600 /etc/smbldap-tools/smbldap_bind.conf
41. smbldap-populate
42. slapcat > ~/smbldap.ldif
43. apt-get install libnss-ldap

Dada sol·licitada	**Dada a introduir**
LDAP server Uniform Resource Identifier	ldap://127.0.0.1
Nom distingit de la base de la cerca	dc=domini,dc=com
Versió d'LDAP a utilitzar	3
LDAP account for root	cn=admin,dc=domini,dc=com
Contrasenya del compte LDAP del superusuari	PASSWORD
Make local root Database admin	Sí
La base de dades d'LDAP requereix d'autenticació d'accés?	No
LDAP account for root	cn=admin,dc=domini,dc=com
Contrasenya del compte LDAP del superusuari	PASSWORD

44. dpkg-reconfigure libnss-ldap

Dada sol·licitada	**Dada a introduir**
LDAP server Uniform Resource Identifier	ldap://127.0.0.1
Nom distingit de la base de la cerca	dc=domini,dc=com
Versió d'LDAP a utilitzar	3
La base de dades d'LDAP requereix d'autenticació d'accés?	No
Special LDAP privileges for root?	Sí
Make the configuration file readable/writeable by its owner only?	Sí
LDAP account for root	cn=admin,dc=domini,dc=com
Contrasenya del compte LDAP del superusuari	PASSWORD

45. nano /etc/nsswitch.conf canviem les línies

```
passwd: files ldap
group: files ldap
shadow: files ldap
hosts: files mdns4_minimal [NOTFOUND=return] dns mdns4 ldap
```

46. nano /etc/ldap/ldap.conf afegim les següents línies

```
host localhost
base dc=domini,dc=com
binddn cn=admin,dc=domini,dc=com
bindpw PASSWORD

bind_policy soft
pam_password exop
timelimit 15

nss_base_passwd dc=domini,dc=com?sub
nss_base_shadow dc=domini,dc=com?sub
nss_base_group ou=group,dc=domini,dc=com?one
```

47. nano /etc/libnss-ldap.conf canviem les següents línies

```
bind_policy soft
pam_password md5 (ATENCIÓ! Hem de canviar la línia #pam_password
crypt)
nss_base_passwd dc=domini,dc=com?sub
nss_base_shadow dc=domini,dc=com?sub
nss_base_group ou=group,dc=domini,dc=com?one
```

48. cat /etc/libnss-ldap.secret
49. dpkg-reconfigure libpam-ldap

Dada sol·licitada	**Dada a introduir**
Identificador Uniforme de Recurs (URI) del servidor LDAP	ldap://127.0.0.1
Nom distingit de la base de la cerca (DN)	dc=domini,dc=com
Versió d'LDAP a utilitzar	3
Make local root database admin	Sí
La base de dades d'LDAP requereix d'autenticació d'accés?	No
LDAP account for root	cn=admin,dc=domini,dc=com
Contrasenya del compte LDAP del superusuari	PASSWORD
Local crypt to use when changing passwords	md5

50. nano /etc/pam_ldap.conf canviem les següents línies

```
bind_policy soft
nss_base_passwd dc=domini,dc=com?sub
nss_base_shadow dc=domini,dc=com?sub
nss_base_group ou=group,dc=domini,dc=com?one
```

51. cat /etc/pam_ldap.secret
52. reboot
53. smbldap-useradd -a -m nom_usuari
54. smbldap-passwd nom_usuari

ANNEX1 slapd.conf

```
# This is the main slapd configuration file. See slapd.conf(5) for more
# info on the configuration options.

#######################################################################
# Global Directives:

# Features to permit
#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

# Where the pid file is put. The init.d script
# will not stop the server if you change this.
pidfile         /var/run/slapd/slapd.pid

# List of arguments that were passed to the server
argsfile        /var/run/slapd/slapd.args

# Read slapd.conf(5) for possible values
loglevel        none

# Where the dynamically loaded modules are stored
modulepath /usr/lib/ldap
moduleload back_hdb

# The maximum number of entries that is returned for a search operation
sizelimit 500

# The tool-threads parameter sets the actual amount of cpu's that is used
# for indexing.
tool-threads 1

#######################################################################
# Specific Backend Directives for hdb:
# Backend specific directives apply to this backend until another
# 'backend' directive occurs
backend hdb

#######################################################################
# Specific Backend Directives for 'other':
# Backend specific directives apply to this backend until another
# 'backend' directive occurs
#backend <other>

#######################################################################
# Specific Directives for database #1, of type hdb:
# Database specific directives apply to this databasse until another
# 'database' directive occurs
database        hdb

# The base of your directory in database #1
suffix          "dc=domini,dc=com"

# rootdn directive for specifying a superuser on the database. This is needed
# for syncrepl.
rootdn          "cn=admin,dc=domini,dc=com"
rootpw          {MD5}Qhz9FD5FDD9YFKBJVAngcw==

# Where the database file are physically stored for database #1
```

```
directory       "/var/lib/ldap"

# The dbconfig settings are used to generate a DB_CONFIG file the first
# time slapd starts.  They do NOT override existing an existing DB_CONFIG
# file.  You should therefore change these settings in DB_CONFIG directly
# or remove DB_CONFIG and restart slapd for changes to take effect.

# For the Debian package we use 2MB as default but be sure to update this
# value if you have plenty of RAM
dbconfig set_cachesize 0 2097152 0

# Sven Hartge reported that he had to set this value incredibly high
# to get slapd running at all. See http://bugs.debian.org/303057 for more
# information.

# Number of objects that can be locked at the same time.
dbconfig set_lk_max_objects 1500
# Number of locks (both requested and granted)
dbconfig set_lk_max_locks 1500
# Number of lockers
dbconfig set_lk_max_lockers 1500

# Indices to maintain for this database
index objectClass                       eq,pres
index ou,cn,sn,mail,givenname           eq,pres,sub
index uidNumber,gidNumber,memberUid     eq,pres
index loginShell                        eq,pres
## required to support pdb_getsampwnam
index uid                               pres,sub,eq
## required to support pdb_getsambapwrid()
index displayName                       pres,sub,eq
index nisMapName,nisMapEntry            eq,pres,sub
index sambaSID                          eq
index sambaPrimaryGroupSID              eq
index sambaDomainName                   eq
index default                           sub
index uniqueMember                      eq
index sambaGroupType                    eq
index sambaSIDList                      eq

# Save the time that the entry gets modified, for database #1
lastmod         on

# Checkpoint the BerkeleyDB database periodically in case of system
# failure and to speed slapd shutdown.
checkpoint      512 30

# Where to store the replica logs for database #1
# replogfile /var/lib/ldap/replog

# users can authenticate and change their password
access to
attrs=userPassword,sambaNTPassword,sambaLMPassword,sambaPwdMustChange,sambaPwdLastSet
        by self write
        by anonymous auth
        by * none

# those 2 parameters must be world readable for password aging to work correctly
# (or use a priviledge account in /etc/ldap.conf to bind to the directory)
access to attrs=shadowLastChange,shadowMax
        by self write
        by * read

# all others attributes are readable to everybody
access to *
        by * read
```

```
# For Netscape Roaming support, each user gets a roaming
# profile for which they have write access to
#access to dn=".*,ou=Roaming,o=morsnet"
#        by dn="cn=admin,dc=domini,dc=com" write
#        by dnattr=owner write

#######################################################################
# Specific Directives for database #2, of type 'other' (can be hdb too):
# Database specific directives apply to this databasse until another
# 'database' directive occurs
#database        <other>

# The base of your directory for database #2
#suffix "dc=debian,dc=org"
```

ANNEX 2 smb.conf

```
[global]
dos charset = UTF-8
display charset = UTF-8
workgroup = DOMINI
realm = DOMINI.COM
server string = %h server
map to guest = Bad User
passdb backend = ldapsam:ldap://127.0.0.1/
pam password change = Yes
passwd program = /usr/sbin/smbldap-passwd -u %u
passwd chat = *New*password* %n\n *Retype*new*password* %n\n
*all*authentication*tokens*updated*
unix password sync = Yes
syslog = 0
log file = /var/log/samba/log.%m
max log size = 1000
time server = Yes
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
add user script = /usr/sbin/smbldap-useradd -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-usermod -g %g %u
add machine script = /usr/sbin/smbldap-useradd -w %u
logon script = logon.bat
logon path = \\%N\profiles\%U
logon drive = H:
domain logons = Yes
os level = 65
preferred master = Yes
domain master = Yes
dns proxy = No
wins support = Yes
ldap admin dn = cn=admin,dc=domini,dc=com
ldap delete dn = Yes
ldap group suffix = ou=group
ldap idmap suffix = ou=idmap
ldap machine suffix = ou=computer
ldap suffix = dc=domini,dc=com
ldap ssl = no
ldap user suffix = ou=people
panic action = /usr/share/samba/panic-action %d
case sensitive = No

[homes]
```

```
comment = Home Directories
valid users = %S
read only = No
create mask = 0600
directory mask = 0700
browseable = No

[printers]
comment = All Printers
path = /var/spool/samba
create mask = 0700
printable = Yes
browseable = No

[print$]
comment = Printer Drivers
path = /var/lib/samba/printers

[netlogon]
path = /var/lib/samba/netlogon
browseable = No

[profiles]
path = /var/lib/samba/profiles
force user = %U
read only = No
create mask = 0600
directory mask = 0700
guest ok = Yes
profile acls = Yes
browseable = No
csc policy = disable

[public]
path = /tmp
read only = No
guest ok = Yes
```

ANNEX 3 smbldap.conf

```
# $Source: $
# $Id: smbldap.conf,v 1.18 2005/05/27 14:28:47 jtournier Exp $
#
# smbldap-tools.conf : Q & D configuration file for smbldap-tools

#  This code was developped by IDEALX (http://IDEALX.org/) and
#  contributors (their names can be found in the CONTRIBUTORS file).
#
#                 Copyright (C) 2001-2002 IDEALX
#
#  This program is free software; you can redistribute it and/or
#  modify it under the terms of the GNU General Public License
#  as published by the Free Software Foundation; either version 2
#  of the License, or (at your option) any later version.
#
#  This program is distributed in the hope that it will be useful,
#  but WITHOUT ANY WARRANTY; without even the implied warranty of
#  MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
#  GNU General Public License for more details.
#
#  You should have received a copy of the GNU General Public License
#  along with this program; if not, write to the Free Software
#  Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307,
#  USA.
```

```
#  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-1-5-21-1169193956-4199179787-2206793627"

# Domain name the Samba server is in charged.
# If not defined, parameter is taking from smb.conf configuration file
# Ex: sambaDomain="IDEALX-NT"
sambaDomain="DOMINI"

##############################################################
#
# LDAP Configuration
#
##############################################################

# Notes: to use to dual ldap servers backend for Samba, you must patch
# Samba with the dual-head patch from IDEALX. If not using this patch
# just use the same server for slaveLDAP and masterLDAP.
# Those two servers declarations can also be used when you have
# . one master LDAP server where all writing operations must be done
# . one slave LDAP server where all reading operations must be done
#   (typically a replication directory)

# Slave LDAP server
# Ex: slaveLDAP=127.0.0.1
# 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
# Ex: masterLDAP=127.0.0.1
# 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="require"

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

# LDAP Suffix
# Ex: suffix=dc=IDEALX,dc=ORG
suffix="dc=domini,dc=com"

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

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

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

# Where are stored Idmap entries (used if samba is a domain member server)
# Ex: groupsdn="ou=Idmap,dc=IDEALX,dc=ORG"
# 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.
# Ex: sambaUnixIdPooldn="sambaDomainName=${sambaDomain},${suffix}"
# Ex: sambaUnixIdPooldn="cn=NextFreeUnixId,${suffix}"
sambaUnixIdPooldn="sambaDomainName=${sambaDomain},${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
# Ex: userLoginShell="/bin/bash"
userLoginShell="/bin/bash"

# Home directory
# Ex: userHome="/home/%U"
userHome="/home/%U"

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

# Gecos
userGecos="System User"
```

```
# Default User (POSIX and Samba) GID
defaultUserGid="513"

# Default Computer (Samba) GID
defaultComputerGid="515"

# 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
# Ex: userSmbHome="\\PDC-SMB3\%U"
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
# Ex: userProfile="\\PDC-SMB3\profiles\%U"
userProfile=""

# The default Home Drive Letter mapping
# (will be automatically mapped at logon time if home directory exist)
# Ex: userHomeDrive="H:"
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
# Ex: userScript="startup.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
# Ex: mailDomain="idealx.com"
mailDomain="domini.com"

################################################################
#
# SMBLDAP-TOOLS Configuration (default are ok for a RedHat)
#
################################################################

# 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"

# comment out the following line to get rid of the default banner
# no_banner="1"
```