Configuració d'un controlador primari de domini per a clients GNU/Linux i Windows

Configuració del servidor Debian

1. Instal·la Debian 5.0.1 sense entorn gràfic
2. nano /etc/apt/sources.list

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

3. nano /etc/network/interfaces

```
allow-hotplug eth0
iface eth0 inet static
address 192.168.1.2XX
netmask 255.255.255.0
gateway 192.168.1.1
```

4. apt-get update
5. apt-get upgrade
6. apt-get install ssh openssh-server
7. apt-get install ntp
8. nano /etc/ntp.conf

Sota la línia:
```
#server ntp.your-provider.example
```
Afegeix les línies:
```
server pool.ntp.org
server ntp.ubuntu.com
```

9. mkdir /ldaphome /ldapdata
10. apt-get install postfix mailx

```
lloc d'Internet
tallerXX
```

11. apt-get install slapd ldap-utils migrationtools

```
PASSWORD
PASSWORD
```

12. dpkg-reconfigure slapd

```
no
domini.local
domini.local
PASSWORD
PASSWORD
BDB
no
```

```
sí
no
```

13. /etc/init.d/slapd stop
14. nano /etc/ldap/slapd.conf

```
Cerca:           /var/lib/ldap
Canvia la línia: directory        “/var/lib/ldap”
Per:             directory        “/ldapdata”
```

15. cp -R /var/lib/ldap/* /ldapdata
16. chown -R openldap:openldap /ldapdata
17. dpkg-reconfigure slapd

```
no
domini.local
domini.local
PASSWORD
PASSWORD
BDB
no
sí
no
```

18. /etc/init.d/slapd start
19. ldapsearch -x -b dc=domini,dc=local
20. apt-get install samba smbldap-tools smbclient samba-doc

```
DOMINI
no
```

21. cp /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz /etc/ldap/schema
22. gzip -d /etc/ldap/schema/samba.schema.gz
23. nano /etc/ldap/slapd.conf

```
Sota la línia:          include         /etc/ldap/schema/inetorgperson.schema
Afegeix les línies:     include         /etc/ldap/schema/samba.schema
                        include         /etc/ldap/schema/misc.schema

Cerca la línia:         access to attrs=userPassword,shadowLastChange
Canvia-la per:
  access to attrs=userPassword,shadowLastChange,sambaNTPassword,sambaLMPassword
```

24. /etc/init.d/slapd restart
25. cd /etc/samba
26. nano smb.conf

```
Cerca:           security
Canvia la línia: # security = user
Per:             security = user

Cerca:           passdb backend
Canvia la línia: passdb backend = tdbsam
Per:             passdb backend = ldapsam:ldap://localhost/
```

```
Cerca:            obey pam
Canvia la línia:  obey pam restrictions = yes
Per:              obey pam restrictions = no
```

Copia aquestes línies sota la línia que acabes de modificar:

```
ldap admin dn = cn=admin,dc=domini,dc=local
ldap suffix = dc=domini,dc=local
ldap group suffix = ou=Groups
ldap user suffix = ou=Users
ldap machine suffix = ou=Computers
ldap idmap suffix = ou=Users
; Do ldap passwd sync
ldap passwd sync = Yes
passwd program = /usr/sbin/smbldap-passwd %u
passwd chat = *New*password* %n\n *Retype*new*password* %n\n
*all*authentication*tokens*updated*
add user script = /usr/sbin/smbldap-useradd -m "%u"
ldap delete dn = Yes
delete user script = /usr/sbin/smbldap-userdel "%u"
add machine script = /usr/sbin/smbldap-useradd -w "%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"
domain logons = yes
```

```
Cerca:            logon path
Sota la línia:    # logon path = \\%N\%U\profile
Escriu:           logon path =
```

27. /etc/init.d/samba restart
28. smbpasswd -w PASSWORD
29. cd /usr/share/doc/smbldap-tools/examples
30. cp smbldap_bind.conf /etc/smbldap-tools
31. cp smbldap.conf.gz /etc/smbldap-tools
32. gzip -d /etc/smbldap-tools/smbldap.conf.gz
33. cd /etc/smbldap-tools
34. net getlocalsid
    copia el samba SID en un lloc apart
35. nano smbldap.conf
    canvia el samba SID pel que has copiat anteriorment

```
Cerca:            sambaDomain
Canvia:           sambaDomain=”DOMSMB”
Per:              sambaDomain=”DOMINI”

Cerca:            suffix
Canvia:           suffix=”dc=company,dc=com”
Per:              suffix=”dc=domini,dc=local”

Cerca:            sambaUnixIdPooldn
Canvia:           sambaUnixIdPooldn=”sambaDomainName=${sambaDomain},${suffix}”
Per:              sambaUnixIdPooldn=”sambaDomainName=DOMINI,${suffix}”
```

```
Cerca:            userHome
Canvia:           userHome=”/home/%U”
Per:              userHome=”/ldaphome/%U”

Cerca:            userSmbHome
Canvia:           userSmbHome=”\\PDC-SRV\%U”
Per:              userSmbHome=

Cerca:            userProfile
Canvia:           userProfile=”\\PDC-SRV\profiles\%U”
Per:              userProfile=

Cerca:            userHomeDrive
Canvia:           userHomeDrive=”H:”
Per:              userHomeDrive=

Cerca:            userScript
Canvia:           userScript=”logon.bat”
Per:              userScript=

Cerca:            mailDomain
Canvia:           mailDomain=”idealx.com”
Per:              mailDomain=”domini.local”
```

36. nano smbldap_bind.conf

Canvia les quatre últimes línies de l'arxiu per:

```
slaveDN="cn=admin,dc=domini,dc=local"
slavePw="PASSWORD"
masterDN="cn=admin,dc=domini,dc=local"
masterPw="PASSWORD"
```

37. chmod 0644 /etc/smbldap-tools/smbldap.conf
38. chmod 0600 /etc/smbldap-tools/smbldap_bind.conf
39. smbldap-populate -u 30000 -g 30000
40. ldapsearch -x -b dc=domini,dc=local | less
41. smbldap-useradd -a -m -M ncognom -N "Nom" -S "Cognom" ncognom
42. smbldap-passwd ncognom
43. apt-get install libpam-ldap libnss-ldap

```
ldap://127.0.0.1
dc=domini,dc=local
3
cn=admin,dc=domini,dc=local
PASSWORD
Sí
No
cn=admin,dc=domini,dc=local
PASSWORD
```

44. nano /etc/ldap.conf

Afegeix les línies:

```
host 127.0.0.1
base dc=domini,dc=local
```

```
uri ldap://127.0.0.1/
rootbinddn cn=admin,dc=domini,dc=local
bind_policy soft
pam_password md5
```

45. cp /etc/ldap.conf /etc/ldap/ldap.conf
46. nano /etc/nsswitch.conf

Afegeix després de cada aparició de la paraula `compat` la paraula `ldap`

47. cd /etc/pam.d/
48. nano common-auth

```
auth  required    pam_env.so
auth  sufficient  pam_unix.so likeauth nullok
auth  sufficient  pam_ldap.so use_first_pass
auth  required    pam_deny.so
```

49. nano common-account

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

50. nano common-password

```
password    sufficient  pam_unix.so nullok md5 shadow use_authtok
password    sufficient  pam_ldap.so use_first_pass
password    required    pam_deny.so
```

51. nano common-session

```
session     required    pam_limits.so
session     required    pam_mkhomedir.so skel=/etc/skel/ umask=0077
session     required    pam_unix.so
session     optional    pam_ldap.so
```

52. apt-get install nfs-kernel-server nfs-common portmap
53. dpkg-reconfigure portmap

```
no
```

54. /etc/init.d/portmap restart
55. nano /etc/exports

Afegeix la línia: `/ldaphome   *(rw,sync,no_subtree_check)`

56. /etc/init.d/nfs-kernel-server restart
57. nano /etc/resolv.conf

Afegeix al principi de l'arxiu la línia: `search domini.local`

58. apt-get install apache2 php5-ldap

59. apt-get install phpldapadmin
60. nano /etc/apache2/httpd.conf

Escriu la línia: `ServerName tallerXX`

61. /etc/init.d/apache2 restart
62. nano /etc/samba/smb.conf

Afegeix al final de l'arxiu les línies:

```
[ldaphome]
path = /ldaphome
writeable = yes
browseable = yes
security mask = 0777
force security mode = 0
directory security mask = 0777
force directory security mode = 0
```

63. mkdir -p /home/samba/netlogon
64. nano /etc/samba/smb.conf

Descomenta les línies:

```
[netlogon]
   comment = Network Logon Service
   path = /home/samba/netlogon
   guest ok = yes
   read only = yes
   share modes = no
```

65. nano /home/samba/netlogon/script.bat

Escriu les línies

```
@echo off
net time \\192.168.1.2XX /set /y
net use h: /delete
net use h: "\\192.168.1.2XX\ldaphome\%username%"
```

66. apt-get install flip
67. flip -m /home/samba/netlogon/script.bat
68. nano /etc/samba/smb.conf

Cerca: `logon script`
Canvia: `; logon script = logon.cmd`
Per: `logon script = script.bat`

69. reboot

Configuració del client Ubuntu

1. Instal·la Ubuntu
2. sudo -i
3. apt-get install portmap nfs-common
4. /etc/init.d/portmap restart
5. mkdir /ldaphome
6. gedit /etc/fstab

```
192.168.1.2XX:/ldaphome /ldaphome nfs rsize=8192,wsize=8192,timeo=14,intr
```

7. Canvia la configuració de la xarxa. Afegeix com a primer DNS l'adreça IP del servidor
8. apt-get install libpam-ldap libnss-ldap

```
ldap://192.168.1.2XX
dc=domini,dc=local
3
sí
no
cn=admin,dc=domini,dc=local
PASSWORD
```

9. gedit /etc/ldap.conf

```
Cerca:          host
Canvia:         host 127.0.0.1
Per:            host 192.168.1.2XX

Cerca:          bind_policy
Canvia:         #bind_policy hard
Per:            bind_policy soft
```

10. cp /etc/ldap.conf /etc/ldap/ldap.conf
11. cd /etc/pam.d/
12. gedit common-auth

```
Comenta (#) les línies que no ho estan
Afegeix al final les línies:
```

```
auth  required    pam_env.so
auth  sufficient  pam_unix.so likeauth nullok
auth  sufficient  pam_ldap.so use_first_pass
auth  required    pam_deny.so
```

13. gedit common-account

```
Comenta (#) les línies que no ho estan
Afegeix al final les línies:
```

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

14. gedit common-password

Comenta (#) les línies que no ho estan
Afegeix al final les línies:

```
password    sufficient  pam_unix.so nullok md5 shadow use_authtok
password    sufficient  pam_ldap.so use_first_pass
password    required    pam_deny.so
```

15. gedit common-session

Comenta (#) les línies que no ho estan
Afegeix al final les línies:

```
session     required    pam_limits.so
session     required    pam_mkhomedir.so skel=/etc/skel/ umask=0077
session     required    pam_unix.so
session     optional    pam_ldap.so
```

16. gedit /etc/nsswitch.conf

Afegeix després de cada aparició de la paraula `compat` la paraula `ldap`

17. reboot

Annexos

Arxius de configuració del servidor

Annex 1 - /etc/apt/sources.list

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

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

deb http://ftp.es.debian.org/debian/ lenny main
deb-src http://ftp.es.debian.org/debian/ lenny main

deb http://security.debian.org/ lenny/updates main
deb-src http://security.debian.org/ lenny/updates main

deb http://volatile.debian.org/debian-volatile lenny/volatile main
deb-src http://volatile.debian.org/debian-volatile lenny/volatile main
```

Annex 2 - /etc/network/interfaces

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet static
address 192.168.1.2XX
netmask 255.255.255.0
gateway 192.168.1.1
```

Annex 3 - /etc/ntp.conf

```
# /etc/ntp.conf, configuration for ntpd; see ntp.conf(5) for help
```

```
driftfile /var/lib/ntp/ntp.drift


# Enable this if you want statistics to be logged.
#statsdir /var/log/ntpstats/

statistics loopstats peerstats clockstats
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable


# You do need to talk to an NTP server or two (or three).
#server ntp.your-provider.example
server pool.ntp.org
server ntp.ubuntu.com

# pool.ntp.org maps to about 1000 low-stratum NTP servers.  Your server
will
# pick a different set every time it starts up.  Please consider joining
the
# pool: <http://www.pool.ntp.org/join.html>
server 0.debian.pool.ntp.org iburst dynamic
server 1.debian.pool.ntp.org iburst dynamic
server 2.debian.pool.ntp.org iburst dynamic
server 3.debian.pool.ntp.org iburst dynamic


# Access control configuration; see /usr/share/doc/ntp-doc/html/accopt.html
for
# details.  The web page
<http://support.ntp.org/bin/view/Support/AccessRestrictions>
# might also be helpful.
#
# Note that "restrict" applies to both servers and clients, so a
configuration
# that might be intended to block requests from certain clients could also
end
# up blocking replies from your own upstream servers.

# By default, exchange time with everybody, but don't allow configuration.
restrict -4 default kod notrap nomodify nopeer noquery
restrict -6 default kod notrap nomodify nopeer noquery

# Local users may interrogate the ntp server more closely.
restrict 127.0.0.1
restrict ::1

# Clients from this (example!) subnet have unlimited access, but only if
# cryptographically authenticated.
#restrict 192.168.123.0 mask 255.255.255.0 notrust


# If you want to provide time to your local subnet, change the next line.
# (Again, the address is an example only.)
#broadcast 192.168.123.255

# If you want to listen to time broadcasts on your local subnet, de-comment
the
# next lines.  Please do this only if you trust everybody on the network!
```

```
#disable auth
#broadcastclient
```

Annex 4 - /etc/ldap/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
include         /etc/ldap/schema/misc.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_bdb

# 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 bdb:
# Backend specific directives apply to this backend until another
# 'backend' directive occurs
backend           bdb

########################################################################
# 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 bdb:
# Database specific directives apply to this databasse until another
```

```
# 'database' directive occurs
database        bdb

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

# rootdn directive for specifying a superuser on the database. This is
needed
# for syncrepl.
# rootdn          "cn=admin,dc=domini,dc=local"

# Where the database file are physically stored for database #1
directory       "/ldapdata"

# 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

# Indexing options for database #1
index           objectClass 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

# The userPassword by default can be changed
# by the entry owning it if they are authenticated.
# Others should not be able to see it, except the
# admin entry below
# These access lines apply to database #1 only
access to
attrs=userPassword,shadowLastChange,sambaNTPassword,sambaLMPassword
        by dn="cn=admin,dc=domini,dc=local" write
        by anonymous auth
        by self write
        by * none

# Ensure read access to the base for things like
```

```
# supportedSASLMechanisms.  Without this you may
# have problems with SASL not knowing what
# mechanisms are available and the like.
# Note that this is covered by the 'access to *'
# ACL below too but if you change that as people
# are wont to do you'll still need this if you
# want SASL (and possible other things) to work
# happily.
access to dn.base="" by * read

# The admin dn has full write access, everyone else
# can read everything.
access to *
        by dn="cn=admin,dc=domini,dc=local" write
        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=local" write
#        by dnattr=owner write

#######################################################################
# Specific Directives for database #2, of type 'other' (can be bdb 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 5 - /etc/samba/smb.conf

```
#
# Sample configuration file for the Samba suite for Debian GNU/Linux.
#
#
# This is the main Samba configuration file. You should read the
# smb.conf(5) manual page in order to understand the options listed
# here. Samba has a huge number of configurable options most of which
# are not shown in this example
#
# Some options that are often worth tuning have been included as
# commented-out examples in this file.
#  - When such options are commented with ";", the proposed setting
#    differs from the default Samba behaviour
#  - When commented with "#", the proposed setting is the default
#    behaviour of Samba but the option is considered important
#    enough to be mentioned here
#
# NOTE: Whenever you modify this file you should run the command
# "testparm" to check that you have not made any basic syntactic
# errors.
# A well-established practice is to name the original file
# "smb.conf.master" and create the "real" config file with
# testparm -s smb.conf.master >smb.conf
# This minimizes the size of the really used smb.conf file
# which, according to the Samba Team, impacts performance
```

```
# However, use this with caution if your smb.conf file contains nested
# "include" statements. See Debian bug #483187 for a case
# where using a master file is not a good idea.
#

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

[global]

## Browsing/Identification ###

# Change this to the workgroup/NT-domain name your Samba server will part
of
   workgroup = DOMINI

# server string is the equivalent of the NT Description field
   server string = %h server

# Windows Internet Name Serving Support Section:
# WINS Support - Tells the NMBD component of Samba to enable its WINS
Server
#   wins support = no

# WINS Server - Tells the NMBD components of Samba to be a WINS Client
# Note: Samba can be either a WINS Server, or a WINS Client, but NOT both
;   wins server = w.x.y.z

# This will prevent nmbd to search for NetBIOS names through DNS.
   dns proxy = no

# What naming service and in what order should we use to resolve host names
# to IP addresses
;   name resolve order = lmhosts host wins bcast

#### Networking ####

# The specific set of interfaces / networks to bind to
# This can be either the interface name or an IP address/netmask;
# interface names are normally preferred
;   interfaces = 127.0.0.0/8 eth0

# Only bind to the named interfaces and/or networks; you must use the
# 'interfaces' option above to use this.
# It is recommended that you enable this feature if your Samba machine is
# not protected by a firewall or is a firewall itself.  However, this
# option cannot handle dynamic or non-broadcast interfaces correctly.
;   bind interfaces only = yes



#### Debugging/Accounting ####

# This tells Samba to use a separate log file for each machine
# that connects
   log file = /var/log/samba/log.%m

# Cap the size of the individual log files (in KiB).
   max log size = 1000

# If you want Samba to only log through syslog then set the following
```

```
# parameter to 'yes'.
#   syslog only = no

# We want Samba to log a minimum amount of information to syslog.
Everything
# should go to /var/log/samba/log.{smbd,nmbd} instead. If you want to log
# through syslog you should set the following parameter to something
higher.
   syslog = 0

# Do something sensible when Samba crashes: mail the admin a backtrace
   panic action = /usr/share/samba/panic-action %d


####### Authentication #######

# "security = user" is always a good idea. This will require a Unix account
# in this server for every user accessing the server. See
# /usr/share/doc/samba-doc/htmldocs/Samba3-HOWTO/ServerType.html
# in the samba-doc package for details.
   security = user

# You may wish to use password encryption.  See the section on
# 'encrypt passwords' in the smb.conf(5) manpage before enabling.
   encrypt passwords = true

# If you are using encrypted passwords, Samba will need to know what
# password database type you are using.
   passdb backend = ldapsam:ldap://localhost/

   obey pam restrictions = no

ldap admin dn = cn=admin,dc=domini,dc=local
ldap suffix = dc=domini,dc=local
ldap group suffix = ou=Groups
ldap user suffix = ou=Users
ldap machine suffix = ou=Computers
ldap idmap suffix = ou=Users
; Do ldap passwd sync
ldap passwd sync = Yes
passwd program = /usr/sbin/smbldap-passwd %u
passwd chat = *New*password* %n\n *Retype*new*password* %n\n
*all*authentication*tokens*updated*
add user script = /usr/sbin/smbldap-useradd -m "%u"
ldap delete dn = Yes
delete user script = /usr/sbin/smbldap-userdel "%u"
add machine script = /usr/sbin/smbldap-useradd -w "%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"
domain logons = yes

# This boolean parameter controls whether Samba attempts to sync the Unix
# password with the SMB password when the encrypted SMB password in the
# passdb is changed.
#   unix password sync = yes

# For Unix password sync to work on a Debian GNU/Linux system, the
```

```
following
# parameters must be set (thanks to Ian Kahan <<kahan@informatik.tu-
muenchen.de> for
# sending the correct chat script for the passwd program in Debian Sarge).
   passwd program = /usr/bin/passwd %u
   passwd chat = *Enter\snew\s*\spassword:* %n\n
*Retype\snew\s*\spassword:* %n\n *password\supdated\ssuccessfully* .

# This boolean controls whether PAM will be used for password changes
# when requested by an SMB client instead of the program listed in
# 'passwd program'. The default is 'no'.
#   pam password change = yes

########## Domains ###########

# Is this machine able to authenticate users. Both PDC and BDC
# must have this setting enabled. If you are the BDC you must
# change the 'domain master' setting to no
#
;   domain logons = yes
#
# The following setting only takes effect if 'domain logons' is set
# It specifies the location of the user's profile directory
# from the client point of view)
# The following required a [profiles] share to be setup on the
# samba server (see below)
;   logon path = \\%N\profiles\%U
# Another common choice is storing the profile in the user's home directory
# (this is Samba's default)
#   logon path = \\%N\%U\profile
logon path =

# The following setting only takes effect if 'domain logons' is set
# It specifies the location of a user's home directory (from the client
# point of view)
;   logon drive = H:
#   logon home = \\%N\%U

# The following setting only takes effect if 'domain logons' is set
# It specifies the script to run during logon. The script must be stored
# in the [netlogon] share
# NOTE: Must be store in 'DOS' file format convention
   logon script = script.bat

# This allows Unix users to be created on the domain controller via the
SAMR
# RPC pipe.  The example command creates a user account with a disabled
Unix
# password; please adapt to your needs
; add user script = /usr/sbin/adduser --quiet --disabled-password --gecos
"" %u

# This allows machine accounts to be created on the domain controller via
the
# SAMR RPC pipe.
# The following assumes a "machines" group exists on the system
; add machine script  = /usr/sbin/useradd -g machines -c "%u machine
account" -d /var/lib/samba -s /bin/false %u

# This allows Unix groups to be created on the domain controller via the
```

```
SAMR
# RPC pipe.
; add group script = /usr/sbin/addgroup --force-badname %g

########## Printing ##########

# If you want to automatically load your printer list rather
# than setting them up individually then you'll need this
#   load printers = yes

# lpr(ng) printing. You may wish to override the location of the
# printcap file
;   printing = bsd
;   printcap name = /etc/printcap

# CUPS printing.  See also the cupsaddsmb(8) manpage in the
# cupsys-client package.
;   printing = cups
;   printcap name = cups

############ Misc ############

# Using the following line enables you to customise your configuration
# on a per machine basis. The %m gets replaced with the netbios name
# of the machine that is connecting
;   include = /home/samba/etc/smb.conf.%m

# Most people will find that this option gives better performance.
# See smb.conf(5) and /usr/share/doc/samba-doc/htmldocs/Samba3-
HOWTO/speed.html
# for details
# You may want to add the following on a Linux system:
#         SO_RCVBUF=8192 SO_SNDBUF=8192
   socket options = TCP_NODELAY

# The following parameter is useful only if you have the linpopup package
# installed. The samba maintainer and the linpopup maintainer are
# working to ease installation and configuration of linpopup and samba.
;   message command = /bin/sh -c '/usr/bin/linpopup "%f" "%m" %s; rm %s' &

# Domain Master specifies Samba to be the Domain Master Browser. If this
# machine will be configured as a BDC (a secondary logon server), you
# must set this to 'no'; otherwise, the default behavior is recommended.
#   domain master = auto

# Some defaults for winbind (make sure you're not using the ranges
# for something else.)
;   idmap uid = 10000-20000
;   idmap gid = 10000-20000
;   template shell = /bin/bash

# The following was the default behaviour in sarge,
# but samba upstream reverted the default because it might induce
# performance issues in large organizations.
# See Debian bug #368251 for some of the consequences of *not*
# having this setting and smb.conf(5) for details.
;   winbind enum groups = yes
;   winbind enum users = yes

# Setup usershare options to enable non-root users to share folders
```

```
# with the net usershare command.

# Maximum number of usershare. 0 (default) means that usershare is
disabled.
;   usershare max shares = 100

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

#[homes]
#   comment = Home Directories
#   browseable = no

# By default, the home directories are exported read-only. Change the
# next parameter to 'no' if you want to be able to write to them.
#   read only = yes

# File creation mask is set to 0700 for security reasons. If you want to
# create files with group=rw permissions, set next parameter to 0775.
#   create mask = 0700

# Directory creation mask is set to 0700 for security reasons. If you want
to
# create dirs. with group=rw permissions, set next parameter to 0775.
#   directory mask = 0700

# By default, \\server\username shares can be connected to by anyone
# with access to the samba server.
# The following parameter makes sure that only "username" can connect
# to \\server\username
# This might need tweaking when using external authentication schemes
#   valid users = %S

# Un-comment the following and create the netlogon directory for Domain
Logons
# (you need to configure Samba to act as a domain controller too.)
[netlogon]
   comment = Network Logon Service
   path = /home/samba/netlogon
   guest ok = yes
   read only = yes
   share modes = no

# Un-comment the following and create the profiles directory to store
# users profiles (see the "logon path" option above)
# (you need to configure Samba to act as a domain controller too.)
# The path below should be writable by all users so that their
# profile directory may be created the first time they log on
;[profiles]
;   comment = Users profiles
;   path = /home/samba/profiles
;   guest ok = no
;   browseable = no
;   create mask = 0600
;   directory mask = 0700

[printers]
   comment = All Printers
   browseable = no
   path = /var/spool/samba
   printable = yes
```

```
   guest ok = no
   read only = yes
   create mask = 0700

# Windows clients look for this share name as a source of downloadable
# printer drivers
[print$]
   comment = Printer Drivers
   path = /var/lib/samba/printers
   browseable = yes
   read only = yes
   guest ok = no
# Uncomment to allow remote administration of Windows print drivers.
# You may need to replace 'lpadmin' with the name of the group your
# admin users are members of.
# Please note that you also need to set appropriate Unix permissions
# to the drivers directory for these users to have write rights in it
;   write list = root, @lpadmin

# A sample share for sharing your CD-ROM with others.
;[cdrom]
;   comment = Samba server's CD-ROM
;   read only = yes
;   locking = no
;   path = /cdrom
;   guest ok = yes

# The next two parameters show how to auto-mount a CD-ROM when the
#     cdrom share is accesed. For this to work /etc/fstab must contain
#     an entry like this:
#
#       /dev/scd0   /cdrom  iso9660 defaults,noauto,ro,user   0 0
#
# The CD-ROM gets unmounted automatically after the connection to the
#
# If you don't want to use auto-mounting/unmounting make sure the CD
#     is mounted on /cdrom
#
;   preexec = /bin/mount /cdrom
;   postexec = /bin/umount /cdrom

[ldaphome]
path = /ldaphome
writeable = yes
browseable = yes
security mask = 0777
force security mode = 0
directory security mask = 0777
force directory security mode = 0
```

Annex 6 - /etc/smbldap-tools/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-1-5-21-840900740-4195848015-3315765215"

# 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=local"

# 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=Users,${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=Computers,${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=Groups,${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,${suffix}"
sambaUnixIdPooldn="sambaDomainName=DOMINI,${suffix}"

# Default scope Used
scope="sub"

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

# 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="/ldaphome/%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="\\PDC-SRV\%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="\\PDC-SRV\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:"
userHomeDrive=

# 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"
userScript=

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

##############################################################################
#
# 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"
```

Annex 7 - /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=local"
slavePw="PASSWORD"
masterDN="cn=admin,dc=domini,dc=local"
masterPw="PASSWORD"
```

Annex 8 - /etc/ldap.conf

```
host 127.0.0.1
base dc=domini,dc=local
uri ldap://127.0.0.1/
rootbinddn cn=admin,dc=domini,dc=local
bind_policy soft
pam_password md5
```

Annex 9 - /etc/nsswitch.conf

```
# /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
```

Annex 10 - /etc/pam.d/common-auth

```
#
# /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  required    pam_env.so
auth  sufficient  pam_unix.so likeauth nullok
auth  sufficient  pam_ldap.so use_first_pass
auth  required    pam_deny.so
```

Annex 11 - /etc/pam.d/common-account

```
#
# /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_unix.so
account     sufficient  pam_ldap.so
account     required    pam_deny.so
```

Annex 12 - /etc/pam.d/common-password

```
#
# /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.

# Explanation of pam_unix options:
#
# The "nullok" option allows users to change an empty password, else
# empty passwords are treated as locked accounts.
#
# The "md5" option enables MD5 passwords.  Without this option, the
# default is Unix crypt.
#
# The "obscure" option replaces the old `OBSCURE_CHECKS_ENAB' option in
# login.defs.
#
# You can also use the "min" option to enforce the length of the new
# password.
#
# See the pam_unix manpage for other options.

# password   required   pam_unix.so nullok obscure 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_unix.so nullok md5 shadow use_authtok
password    sufficient  pam_ldap.so use_first_pass
password    required    pam_deny.so
```

Annex 13 - /etc/pam.d/common-session

```
#
# /etc/pam.d/common-session - session-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 tasks to be performed
# at the start and end of sessions of *any* kind (both interactive and
# non-interactive).  The default is pam_unix.
#
# session   required    pam_unix.so

session     required    pam_limits.so
session     required    pam_mkhomedir.so skel=/etc/skel/ umask=0077
session     required    pam_unix.so
session     optional    pam_ldap.so
```

Annex 14 - /etc/exports

```
# /etc/exports: the access control list for filesystems which may be
exported
#           to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes       hostname1(rw,sync,no_subtree_check)
hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes  gss/krb5i(rw,sync,no_subtree_check)
#

/ldaphome   *(rw,sync,no_subtree_check)
```

Annex 15 - /etc/resolv.conf

```
search domini.local
nameserver 192.168.1.1
nameserver 80.58.0.33
nameserver 80.58.61.250
```

Annex 16 - /etc/apache2/httpd.conf

```
ServerName tallerXX
```

Annex 17 - /home/samba/netlogon/script.bat

```
@echo off
net time \\192.168.1.2XX /set /y
net use h: /delete
```

```
net use h: "\\192.168.1.2XX\ldaphome\%username%"
```

Arxius de configuració del client

Annex 18 - /etc/fstab

```
# /etc/fstab: static file system information.
#
# Use 'blkid -o value -s UUID' to print the universally unique identifier
# for a device; this may be used with UUID= as a more robust way to name
# devices that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
proc            /proc           proc    defaults        0       0
# / was on /dev/sda1 during installation
UUID=2d47fcb9-e88e-4cc4-a96f-bd524fa3d5f9 /               ext4    errors=remount-ro
0       1
# swap was on /dev/sda5 during installation
UUID=a245b98c-88db-482f-a992-3a78f4e9cd0a none            swap    sw              0
0
/dev/scd0       /media/cdrom0   udf,iso9660 user,noauto,exec,utf8 0       0
/dev/fd0        /media/floppy0  auto    rw,user,noauto,exec,utf8 0       0
192.168.1.2XX:/ldaphome   /ldaphome    nfs    rsize=8192,wsize=8192,timeo=14,intr
```

Annex 19 - /etc/ldap.conf

```
###DEBCONF###
##
## Configuration of this file will be managed by debconf as long as the
## first line of the file says '###DEBCONF###'
##
## You should use dpkg-reconfigure to configure this file via debconf
##

#
# @(#)$Id: ldap.conf,v 1.38 2006/05/15 08:13:31 lukeh Exp $
#
# This is the configuration file for the LDAP nameservice
# switch library and the LDAP PAM module.
#
# PADL Software
# http://www.padl.com
#

# Your LDAP server. Must be resolvable without using LDAP.
# Multiple hosts may be specified, each separated by a
# space. How long nss_ldap takes to failover depends on
# whether your LDAP client library supports configurable
# network or connect timeouts (see bind_timelimit).
```

```
host 192.168.1.2XX

# The distinguished name of the search base.
base dc=domini,dc=local

# Another way to specify your LDAP server is to provide an
uri ldap://192.168.1.2XX
# Unix Domain Sockets to connect to a local LDAP Server.
#uri ldap://127.0.0.1/
#uri ldaps://127.0.0.1/
#uri ldapi://%2fvar%2frun%2fldapi_sock/
# Note: %2f encodes the '/' used as directory separator

# The LDAP version to use (defaults to 3
# if supported by client library)
ldap_version 3

# The distinguished name to bind to the server with.
# Optional: default is to bind anonymously.
# binddn cn=admin,dc=padl,dc=com

# The credentials to bind with.
# Optional: default is no credential.
# bindpw

# The distinguished name to bind to the server with
# if the effective user ID is root. Password is
# stored in /etc/ldap.secret (mode 600)
rootbinddn cn=admin,dc=domini,dc=local

# The port.
# Optional: default is 389.
#port 389

# The search scope.
#scope sub
#scope one
#scope base

# Search timelimit
#timelimit 30

# Bind/connect timelimit
#bind_timelimit 30

# Reconnect policy: hard (default) will retry connecting to
# the software with exponential backoff, soft will fail
# immediately.
bind_policy soft

# Idle timelimit; client will close connections
# (nss_ldap only) if the server has not been contacted
# for the number of seconds specified below.
#idle_timelimit 3600

# Filter to AND with uid=%s
#pam_filter objectclass=account

# The user ID attribute (defaults to uid)
#pam_login_attribute uid
```

```
# Search the root DSE for the password policy (works
# with Netscape Directory Server)
#pam_lookup_policy yes

# Check the 'host' attribute for access control
# Default is no; if set to yes, and user has no
# value for the host attribute, and pam_ldap is
# configured for account management (authorization)
# then the user will not be allowed to login.
#pam_check_host_attr yes

# Check the 'authorizedService' attribute for access
# control
# Default is no; if set to yes, and the user has no
# value for the authorizedService attribute, and
# pam_ldap is configured for account management
# (authorization) then the user will not be allowed
# to login.
#pam_check_service_attr yes

# Group to enforce membership of
#pam_groupdn cn=PAM,ou=Groups,dc=padl,dc=com

# Group member attribute
#pam_member_attribute uniquemember

# Specify a minium or maximum UID number allowed
#pam_min_uid 0
#pam_max_uid 0

# Template login attribute, default template user
# (can be overriden by value of former attribute
# in user's entry)
#pam_login_attribute userPrincipalName
#pam_template_login_attribute uid
#pam_template_login nobody

# HEADS UP: the pam_crypt, pam_nds_passwd,
# and pam_ad_passwd options are no
# longer supported.
#
# Do not hash the password at all; presume
# the directory server will do it, if
# necessary. This is the default.
pam_password md5

# Hash password locally; required for University of
# Michigan LDAP server, and works with Netscape
# Directory Server if you're using the UNIX-Crypt
# hash mechanism and not using the NT Synchronization
# service.
#pam_password crypt

# Remove old password first, then update in
# cleartext. Necessary for use with Novell
# Directory Services (NDS)
#pam_password clear_remove_old
#pam_password nds
```

```
# RACF is an alias for the above. For use with
# IBM RACF
#pam_password racf

# Update Active Directory password, by
# creating Unicode password and updating
# unicodePwd attribute.
#pam_password ad

# Use the OpenLDAP password change
# extended operation to update the password.
#pam_password exop

# Redirect users to a URL or somesuch on password
# changes.
#pam_password_prohibit_message Please visit http://internal to change your
password.

# RFC2307bis naming contexts
# Syntax:
# nss_base_XXX          base?scope?filter
# where scope is {base,one,sub}
# and filter is a filter to be &'d with the
# default filter.
# You can omit the suffix eg:
# nss_base_passwd ou=People,
# to append the default base DN but this
# may incur a small performance impact.
#nss_base_passwd  ou=People,dc=padl,dc=com?one
#nss_base_shadow  ou=People,dc=padl,dc=com?one
#nss_base_group         ou=Group,dc=padl,dc=com?one
#nss_base_hosts         ou=Hosts,dc=padl,dc=com?one
#nss_base_services      ou=Services,dc=padl,dc=com?one
#nss_base_networks      ou=Networks,dc=padl,dc=com?one
#nss_base_protocols     ou=Protocols,dc=padl,dc=com?one
#nss_base_rpc           ou=Rpc,dc=padl,dc=com?one
#nss_base_ethers  ou=Ethers,dc=padl,dc=com?one
#nss_base_netmasks      ou=Networks,dc=padl,dc=com?ne
#nss_base_bootparams    ou=Ethers,dc=padl,dc=com?one
#nss_base_aliases ou=Aliases,dc=padl,dc=com?one
#nss_base_netgroup      ou=Netgroup,dc=padl,dc=com?one

# attribute/objectclass mapping
# Syntax:
#nss_map_attribute      rfc2307attribute  mapped_attribute
#nss_map_objectclass    rfc2307objectclass      mapped_objectclass

# configure --enable-nds is no longer supported.
# NDS mappings
#nss_map_attribute uniqueMember member

# Services for UNIX 3.5 mappings
#nss_map_objectclass posixAccount User
#nss_map_objectclass shadowAccount User
#nss_map_attribute uid msSFU30Name
#nss_map_attribute uniqueMember msSFU30PosixMember
#nss_map_attribute userPassword msSFU30Password
#nss_map_attribute homeDirectory msSFU30HomeDirectory
#nss_map_attribute homeDirectory msSFUHomeDirectory
#nss_map_objectclass posixGroup Group
```

```
#pam_login_attribute msSFU30Name
#pam_filter objectclass=User
#pam_password ad

# configure --enable-mssfu-schema is no longer supported.
# Services for UNIX 2.0 mappings
#nss_map_objectclass posixAccount User
#nss_map_objectclass shadowAccount user
#nss_map_attribute uid msSFUName
#nss_map_attribute uniqueMember posixMember
#nss_map_attribute userPassword msSFUPassword
#nss_map_attribute homeDirectory msSFUHomeDirectory
#nss_map_attribute shadowLastChange pwdLastSet
#nss_map_objectclass posixGroup Group
#nss_map_attribute cn msSFUName
#pam_login_attribute msSFUName
#pam_filter objectclass=User
#pam_password ad

# RFC 2307 (AD) mappings
#nss_map_objectclass posixAccount user
#nss_map_objectclass shadowAccount user
#nss_map_attribute uid sAMAccountName
#nss_map_attribute homeDirectory unixHomeDirectory
#nss_map_attribute shadowLastChange pwdLastSet
#nss_map_objectclass posixGroup group
#nss_map_attribute uniqueMember member
#pam_login_attribute sAMAccountName
#pam_filter objectclass=User
#pam_password ad

# configure --enable-authpassword is no longer supported
# AuthPassword mappings
#nss_map_attribute userPassword authPassword

# AIX SecureWay mappings
#nss_map_objectclass posixAccount aixAccount
#nss_base_passwd ou=aixaccount,?one
#nss_map_attribute uid userName
#nss_map_attribute gidNumber gid
#nss_map_attribute uidNumber uid
#nss_map_attribute userPassword passwordChar
#nss_map_objectclass posixGroup aixAccessGroup
#nss_base_group ou=aixgroup,?one
#nss_map_attribute cn groupName
#nss_map_attribute uniqueMember member
#pam_login_attribute userName
#pam_filter objectclass=aixAccount
#pam_password clear

# Netscape SDK LDAPS
#ssl on

# Netscape SDK SSL options
#sslpath /etc/ssl/certs

# OpenLDAP SSL mechanism
# start_tls mechanism uses the normal LDAP port, LDAPS typically 636
#ssl start_tls
#ssl on
```

```
# OpenLDAP SSL options
# Require and verify server certificate (yes/no)
# Default is to use libldap's default behavior, which can be configured in
# /etc/openldap/ldap.conf using the TLS_REQCERT setting.  The default for
# OpenLDAP 2.0 and earlier is "no", for 2.1 and later is "yes".
#tls_checkpeer yes

# CA certificates for server certificate verification
# At least one of these are required if tls_checkpeer is "yes"
#tls_cacertfile /etc/ssl/ca.cert
#tls_cacertdir /etc/ssl/certs

# Seed the PRNG if /dev/urandom is not provided
#tls_randfile /var/run/egd-pool

# SSL cipher suite
# See man ciphers for syntax
#tls_ciphers TLSv1

# Client certificate and key
# Use these, if your server requires client authentication.
#tls_cert
#tls_key

# Disable SASL security layers. This is needed for AD.
#sasl_secprops maxssf=0

# Override the default Kerberos ticket cache location.
#krb5_ccname FILE:/etc/.ldapcache

# SASL mechanism for PAM authentication - use is experimental
# at present and does not support password policy control
#pam_sasl_mech DIGEST-MD5
nss_initgroups_ignoreusers avahi,avahi-
autoipd,backup,bin,couchdb,daemon,games,gdm,gnats,haldaemon,hplip,irc,kerno
ops,libuuid,list,lp,mail,man,messagebus,news,proxy,pulse,root,saned,speech-
dispatcher,statd,sync,sys,syslog,uucp,www-data
```

Annex 20 - /etc/pam.d/common-auth

```
#
# /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.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
#auth [success=2 default=ignore]    pam_unix.so nullok_secure
```

```
#auth [success=1 default=ignore]    pam_ldap.so use_first_pass
# here's the fallback if no module succeeds
#auth requisite              pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success
code
# since the modules above will each just jump around
#auth required               pam_permit.so
# and here are more per-package modules (the "Additional" block)
# end of pam-auth-update config

auth  required    pam_env.so
auth  sufficient  pam_unix.so likeauth nullok
auth  sufficient  pam_ldap.so use_first_pass
auth  required    pam_deny.so
```

Annex 21 - /etc/pam.d/common-account

```
#
# /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.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.
#

# here are the per-package modules (the "Primary" block)
#account    [success=2 new_authtok_reqd=done default=ignore]
      pam_unix.so
#account    [success=1 default=ignore]    pam_ldap.so
# here's the fallback if no module succeeds
#account    requisite              pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success
code
# since the modules above will each just jump around
#account    required               pam_permit.so
# and here are more per-package modules (the "Additional" block)
# end of pam-auth-update config

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

Annex 22 - /etc/pam.d/common-password

```
#
# /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.

# Explanation of pam_unix options:
#
# The "sha512" option enables salted SHA512 passwords.  Without this
option,
# the default is Unix crypt.  Prior releases used the option "md5".
#
# The "obscure" option replaces the old `OBSCURE_CHECKS_ENAB' option in
# login.defs.
#
# See the pam_unix manpage for other options.

# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
#password   [success=2 default=ignore]   pam_unix.so obscure sha512
#password   [success=1 user_unknown=ignore default=die]    pam_ldap.so
use_authtok try_first_pass
# here's the fallback if no module succeeds
#password   requisite              pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success
code
# since the modules above will each just jump around
#password   required               pam_permit.so
# and here are more per-package modules (the "Additional" block)
#password   optional    pam_gnome_keyring.so
# end of pam-auth-update config

password    sufficient  pam_unix.so nullok md5 shadow use_authtok
password    sufficient  pam_ldap.so use_first_pass
password    required    pam_deny.so
```

Annex 23 - /etc/pam.d/common-session

```
#
# /etc/pam.d/common-session - session-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 tasks to be performed
# at the start and end of sessions of *any* kind (both interactive and
# non-interactive).
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.
```

```
# here are the per-package modules (the "Primary" block)
#session    [default=1]             pam_permit.so
# here's the fallback if no module succeeds
#session    requisite               pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success
code
# since the modules above will each just jump around
#session    required                pam_permit.so
# and here are more per-package modules (the "Additional" block)
#session    required    pam_unix.so
#session    optional                pam_ldap.so
#session    optional                pam_ck_connector.so nox11
# end of pam-auth-update config

session     required    pam_limits.so
session     required    pam_mkhomedir.so skel=/etc/skel/ umask=0077
session     required    pam_unix.so
session     optional    pam_ldap.so
```

Annex 24 - /etc/nsswitch.conf

```
# /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 mdns4_minimal [NOTFOUND=return] dns mdns4
networks:       files

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

netgroup:       nis
```