The *Linux* Samba-OpenLDAP Howto (*Revision*: 1.10)

Jérôme Tournier
Olivier Lemaire

***Revision*: 1.10 , generated July 12, 2007**

Release:	
Reference:	
Publication date:	
Print date:	July 12, 2007

This Howto explains how to set up and use an *Linux* Departemental Server with Samba an OpenLDAP to replace an existing Microsoft Windows Domain Controler servers and provide central authentication services, file and print sharing for Microsoft Windows and Unix clients.

Table of Contents

1 Introduction

This smbldap-tools aims on helping to use Open Source softwares *Linux*, Samba and OpenLDAP to replace existing Microsoft Windows Domain Controler servers. It explains how to set up and use a *Linux* Departemental Server with Samba and OpenLDAP to offer central authentication (Domain Controler), file and print sharing for Microsoft Windows and Unix clients.

1.1 Softwares used

This howto currently runs for:

- release 3.0.11*rc*1 of Samba,
- Microsoft Windows, Microsoft Windows NT 4.0, Windows 2000 and Windows XP Workstations and Servers,
- *Linux* RedHat 9 (should work on any *Linux* distribution anyway [1]),
- release 2.1.22 of OpenLDAP (should work anyway on any other releases of OpenLDAP, and any implementation of LDAP servers like iPlanet Directory for example).

1.2 Updates of this document

The most up to date release of this document may be found on the smbldap-tools project page available at `http://`

samba.IDEALX.org/.

If you find any bugs in this document, of if you want this document to integrate some additional infos, please drop us a mail with your bug report and/or change request at samba@IDEALX.org.

1.3 Availability of this document

This document is the property of IDEALX (http://www.IDEALX.com/).

Permission is granted to distribute this document under the terms of the GNU Free Documentation License (See http://www.gnu.org/copyleft/fdl.html).

2 Context of this Howto

This Howto aims at helping to configure an Samba + OpenLDAP Primary Domain Controler for Microsoft Windows Workstations (and, using nss_ldap and pam_ldap, a unique source of authentification for all workstations, including *Linux* and other Unix systems).

For the need of this howto, we took some snakeoils global parameters and default guidelines which are explained hereafter.

2.1 Global parameters

For the need of our example, we settled the following context:

- All workstations and servers are in the same LAN 192.168.1.0/24,
- DNS resolution is okay (using Bind or Djbdns for example), and out of the scope of this Howto [2],
- We want to configure the Microsoft Windows NT Domain named IDEALX-NT,
- We will have a central Primary Domain Controler named PDC-SRV (netbios name) on the host 192.168.1.1/32 ,
- We want this Primary Domain Controller to be the WINS server and the Master Browser Server of the IDEALX-NT domain,
- All authentifications objects (users and groups) will be stored on an OpenLDAP server, using the base DN: dc=idealx,dc=org,
- Users accounts will be stored in ou=Users,dc=idealx,dc=org,
- Computers accounts will be stored in ou=Computers,dc=idealx,dc=org,
- Groups accounts will be stored in ou=Groups,dc=idealx,dc=org.

2.2 RedHat base

In this Howto, we took the RedHat/*Linux* 9 as a base, and made RPM packages for software component involved in this Howto (Samba, OpenLDAP, smbldap-tools, ...) to ease you installing this configuration.

Of course, this do not mean Samba only run on RedHat/*Linux* nor RedHat/*Linux* is a better *Linux* distribution than Debian GNU/*Linux*. The choice of RedHat/*Linux* present the advantage to be quickly reproductible by anybody (RedHat *Linux* is very common on the server market nowadays, and supported by many vendors). However, we presented in section 17 all .spec files used by our packages to help you install and compile the used softwares on your favorite *Linux* (or any other Operating System in fact).

All available RPM (and SRPM) packages are available on the smbldap-tools project home page at http://samba.IDEALX.org/.

2.3 FHS, LSB and High Availability

Installing and compiling the key softwares (Samba and OpenLDAP), we tried to keep in mind two key principles:

1. we must enforce File Hierarchy Standard (FHS[3]) recommandations,
2. we should follow the Linux Standard Base (LSB[4]) recommandations
3. we must think our Primary Domain Controler may be used in a High Available configuration (in a futur revision of

this Howto).

Let us know if you think one of these key principles were not correctly enforced: drop a mail to samba@IDEALX.com.

3 Installation

To stick to this Howto[5], you must have the following requirements prior to download anything:

- *Fedora Core release* 2 installed and operational (network included) [6],
- you must be prepared (if not already done) to use pam_ldap and nss_ldap (we'll see later how to configure them correctly).

Additionnaly, you must download and install packages :

- OpenLDAP,
- Samba,
- nss_ldap and pam_ldap,
- smbldap-tools.

The smbldap-tools are available on the project page (`http://samba.IDEALX.org/dist/`); others are part of the *Fedora Core release* 2 distribution. Only OpenLDAP was downloaded separatly because of the old version available in the distribution.

3.1 OpenLDAP 2.1.29

At the date we wrote this document, release 2.1.29of OpenLDAP was considered stable enough to be used in production environment. We use the release of OpenLDAP provided with *Fedora Core release* 2. Packages that need to be downloaded are :

- core components: openldap-2.1.29-1
- server components: openldap-servers-2.1.29-1,
- clients components: openldap-clients-2.1.29-1

Once downloaded, install the following packages on your system:

```
rpm -Uvh openldap-2.1.29-1.i386.rpm
rpm -Uvh openldap-servers-2.1.29-1.i386.rpm
rpm -Uvh openldap-clients-2.1.29-1.i386.rpm
```

3.2 Samba 3.0.11*rc*1

Samba 3.0.11*rc*1 is the latest release of Samba 3 branch (at the date of this Howto redaction, and used by this Howto). To use Samba with LDAP, ther's no need of compilation options to Samba as LDAP is the default backend used with classic RedHat's Samba packages.

Samba package can be dowloaded on the samba project [7].

Just download the `samba` packages and install them on your system:

```
rpm -Uvh samba-3.0.10-2.i386.rpm
rpm -Uvh samba-client-3.0.10-2.i386.rpm
rpm -Uvh samba-common-3.0.10-2.i386.rpm
```

Of course, you can also use the default RedHat package.

3.3 smbldap-tools 0.8.8

smbldap-tools is a package containing some useful scripts to manage users/groups when you're using LDAP as source of users/groups datas (for Unix and for Samba). We used those scripts in this Howto to add/delete/modify users and groups.

smbldap-tools are included in the Samba source tree scince release 2.2.5 [8], but you will find RPM and SRPMS packages on the smbldap-tools project page.

For this Howto, just download smbldap-tools release 0.8.8 RPM and install it:

```
rpm -Uvh smbldap-tools-0.8.8-1.i386.rpm
```

smbldap-tools will continue to evoluate. Consult the ChangeLog in the CVS source tree to see if changes are interesting for your context. For this Howto setup however, we encourage you to use release 0.8.8 as they are sufficient for the limited use they cover

4 Configuration

4.1 OpenLDAP

You'll need to configure your OpenLDAP server for it to act as a SAM database. Following our context example, we must configure it to :

- accept the Samba 3.0.11*rc*1 LDAP v3 schema[9],
- run on the base DN dc=idealx,dc=org,
- contain the minimal entries needed to start using it.

For the needs of this Howto example, we have used the following LDAP DIT:

```
(using Relative DN notation)

dc=IDEALX,dc=ORG
 |
 `--- ou=Users     : to store user accounts for Unix and Windows systems
 |
 `--- ou=Computers : to store computer accounts for Windows systems
 |
 `--- ou=Groups    : to store system groups for Unix and Windows
 |                   systems (or for any other LDAP-aware systems)
 |
 `--- ou=DSA       : to store special accounts (simpleSecurityObject)
                     systems (or for any other LDAP-aware systems)
```

This DIT is compliant with recommandations from RFC 2307bis. We did not use ou=Host to store computer accounts as there is a difference between TCP/IP hosts and Microsoft Windows computer accounts. We used ou=DSA to store specific security accounts for LDAP Clients, in the context of the smbldap-tools (look at the 5 section for more details and example).

You may choose to use another LDAP tree to store objects: for example, all accounts (shadowAccounts and sambaSAMAccounts) "under" the same DN. We choosed this DIT because of the compliance with RFC 2307bis recommandations, and because we think it's clearer for human comprehension this way.

Using Samba 3.0.11*rc*1 and OpenLDAP, we will store :

- Microsoft Windows user accounts using sambaSAMAccount object class (samba.schema),
- Microsoft Windows computer accounts (ie. workstations) using sambaSAMAccount object class,
- Unix user accounts using posixAccount objectclass and shadowAccount objectclass for the shadow suite password (nis.schema)
- Users groups using posixGroup and sambaGroupMapping object classes [10].

- security accounts used by software clients (Samba and *Linux*) using simpleSecurityObject (core.schema) object class.

4.1.1 Schemas

The Samba schema must be supported by the OpenLDAP server. To do so, and using the smbldap-tools OpenLDAP RedHat packages, just verify that your /etc/openldap/slapd.conf include the lines like the example hereafter:

```
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/nis.schema
include         /etc/openldap/schema/samba.schema
```

As you can see, we use the inetOrgPerson objectclass because we want to merge organizational with technical data. Doing so will ease administration as a user account will be used to define:

1. a human user in your company,
2. a user account for Microsoft Windows and Unix systems,
3. a user account for any LDAP-aware application.

Doing so is not mandatory: feel free to use a context who feet your needs better if this way is not the one you want to follow.

Note that we use the samba.schema shipped with Samba release 3.0.11*rc*1 sources.

4.1.2 Server configuration

Configure the slapd server to be a master server on the following suffix: dc=idealx,dc=org. This will result in the following lines in slapd.conf configuration files:

```
database    bdb
directory   /var/lib/ldap

suffix      "dc=IDEALX,dc=ORG"
rootdn      "cn=Manager,dc=IDEALX,dc=ORG"

index       objectClass,uidNumber,gidNumber                    eq
index       cn,sn,uid,displayName                              pres,sub,eq
index       memberUid,mail,givenname                  eq,subinitial
index       sambaSID,sambaPrimaryGroupSID,sambaDomainName    eq
```

Then, position Access Control Lists to protect your datas. This will result in the following lines in the configuration file:

```
access to attrs=userPassword,sambaLMPassword,sambaNTPassword
      by self write
      by anonymous auth
      by * none
access to *
      by * read
```

Finally, define the Root DN password for your server. This will result in the following lines :

```
rootpw          mysecretpwd
```

Don't forget to place mode 600 on file/etc/openldap/slapd.conf to protect your Root DN password, if not already set. You can also set a hashed password in that file: use the `slappasswd` command. For example, to have the word *mysecretpwd* hashed with the SSHA algorithm, use the command

```
[root@etoile]$ slappasswd -h {SSHA} -s mysecretpwd
{SSHA}X+Qv3lKnVB/oov2uvC6Id1nfEkgYaPrd
```

Available algorithm are CRYPT, MD5, SMD5, SSHA, and SHA. The default is SSHA. The resulting lines in the file/etc/openldap/slapd.conf will then be

```
rootpw      {SSHA}X+Qv3lKnVB/oov2uvC6Id1nfEkgYaPrd
```

4.1.3 Clients configuration

Configure default settings for LDAP clients by editing /etc/openldap/ldap.conf like in the following example:

```
HOST 127.0.0.1
BASE dc=IDEALX,dc=ORG
```

4.1.4 Start the server

Finally, start your OpenLDAP server using the following

```
/etc/init.d/ldap start
```

Everything should work fine. If not:

- verify your configuration files,
- verify that the configuration file `/etc/openldap/slapd.conf` and the directory /var/lib/ldap exist and are owned by the user who run slapd (ldap user for RedHat OpenLDAP packages),
- consult the OpenLDAP documentation.

4.2 *Linux* Operating System

You need to tell you *Linux* box to use LDAP using pam_ldap and nss_ldap. Then, you should run nscd and finish your system LDAP configuration.

4.2.1 pam_ldap, nss_ldap and nscd

Use authconfig [11] to activate pam_ldap :

- Cache Information
- Use LDAP
- dont select 'Use TSL'
- Server: 127.0.0.1
- Base DN: dc=idealx,dc=org
- Use Shadow Passwords
- Use MD5 Passwords
- Use LDAP Authentification
- Server : 127.0.0.1
- Base DN: dc=idealx,dc=org

Cache Information mean you're using nscd (`man nscd` for more info) : if you're going to use pam_ldap and nss_ldap, you should really use it for optimization.

If you don't rely on 'authconfig', you can edit your /etc/pam.d/system-auth by hand, to have something like the following:

```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      /lib/security/pam_env.so
auth        sufficient    /lib/security/pam_unix.so likeauth nullok
auth        sufficient    /lib/security/pam_ldap.so use_first_pass
auth        required      /lib/security/pam_deny.so

account     required      /lib/security/pam_unix.so
account     sufficient    /lib/security/pam_ldap.so

password    required      /lib/security/pam_cracklib.so retry=3 type=
password    sufficient    /lib/security/pam_unix.so nullok use_authtok md5 shadow
password    sufficient    /lib/security/pam_ldap.so use_authtok
password    required      /lib/security/pam_deny.so

session     required      /lib/security/pam_limits.so
session     required      /lib/security/pam_unix.so
session     optional      /lib/security/pam_ldap.so
```

Warning: a special attention must be taken about the account sufficient parameters as it seems RedHat authconfig tools place it as 'required' in any case (which is not the way you'll need).

4.2.2 /etc/ldap.conf

Edit your /etc/ldap.conf to configure your LDAP parameters:

- host: LDAP server host,
- base: distinguished name of the default search base,
- nss_base_passwd: naming context for accounts,
- nss_base_group: naming context for groups,
- rootbinddn and associated password: the distinguished name used to bind if effective ID is root (to allow root to change any user's password for example).

Which should be like the following:

```
# Your LDAP server. Must be resolvable without using LDAP.
host 127.0.0.1

# The distinguished name of the search base.
base dc=IDEALX,dc=ORG

# The distinguished name to bind to the server with if the effective user
ID
# is root. Password must be stored in /etc/ldap.secret (mode 600)
rootbinddn cn=nssldap,ou=DSA,dc=IDEALX,dc=ORG

# RFC2307bis naming contexts
nss_base_passwd         ou=Users,dc=IDEALX,dc=ORG?one
nss_base_passwd         ou=Computers,dc=IDEALX,dc=ORG?one
nss_base_shadow         ou=Users,dc=IDEALX,dc=ORG?one
nss_base_group          ou=Groups,dc=IDEALX,dc=ORG?one

# Security options
ssl no
pam_password md5

# - The End
```

4.2.3 /etc/ldap.secret

You must place in this file, protected by mode 600, the bind password associated with the distinguished name used by nss_ldap to bind to the OpenLDAP directory when the local user is root. In our example, this file must contain the following password:

```
nssldapsecretpwd
```

4.2.4 /etc/nsswitch.conf

Edit your /etc/nswitch.conf to configure your Name Service Switch to use LDAP for users and groups:

```
# significative entries for /etc/nsswitch.conf
using
# Samba and OpenLDAP
passwd:     files ldap
shadow:     files ldap
group:      files ldap
```

A complete sample /etc/nsswitch.conf is presented in section 17.1.4.

4.3 Samba

Here, we'll configure Samba as a Primary Domain Controler for the Microsoft Windows NT Domain named IDEALX-NT with the SAM database stored in our OpenLDAP server.

4.3.1 Configuration

We need to configure /etc/samba/smb.conf like in the example of 17.1.3, assuming that :

- Our Microsoft Windows NT Domain Name will be : IDEALX-NT
- Our server Netbios Name will be : PDC-SRV
- Our server will allow roving/roaming profiles
- All samba share will rely on /home/samba/* excepted for home directories (always on /home/USERNAME).
- We really want our Samba-LDAP PDC server to be the domain browser on the LAN.

Edit your /etc/samba/smb.conf like in the example of 17.1.3 to configure your Samba server. Let make some remarques about this file:

The global section

This section allow you to configure the global parameter of the server. Here takes places all the parameters we defined in the previous paragraph. We also have defined the program used for a user to change his password (*passwd program*) and the dialog used between the server and the user during the change.

The option "add machine script" allow smbd to add, as root, a new machine account in the doamin. When a machine contact the domain, this script is called and the new machine's account is created in the domain. This makes easily the administration of machine's account. For security reason, the only account allowed to join computer in the domain is the "Administrator" which is a privilege account.

For french users, we added a line that allow smbd to map incoming filenames from a DOS code page. This option is very useful if you want that files and directories in your profiles are saved with all the accents they have. Don't forget to read the man page for more detail: this option is a Western European UNIX character set. The parameter client code page MUST be set to code page 850 in order for the conversion to the UNIX character set to be done correctly.

```
  workgroup = IDEALX-NT
  netbios name = PDC-SRV
  enable privileges = yes
  server string = SAMBA-LDAP PDC Server
  ...
  #unix password sync = Yes
  #passwd program = /usr/local/sbin/smbldap-passwd -u %u
  #passwd chat = "Changing password for*\nNew password*" %n\n "*Retype new
password*" %n\n"
  ldap passwd sync = Yes
  ...
  ; SAMBA-LDAP declarations
  passdb backend = ldapsam:ldap://127.0.0.1/
  # ldap filter = (&(objectclass=sambaSamAccount)(uid=%u))
  ldap admin dn = cn=Manager,dc=IDEALX,dc=ORG
  ldap suffix = dc=IDEALX,dc=ORG
  ldap group suffix = ou=Groups
  ldap user suffix = ou=Users
  ldap machine suffix = ou=Computers
  ldap ssl = start_tls

  add machine script = /usr/local/sbin/smbldap-useradd -w "%u"
  add user script = /usr/local/sbin/smbldap-useradd -m "%u"
  ldap delete dn = Yes
  #delete user script = /usr/local/sbin/smbldap-userdel "%u"
  add group script = /usr/local/sbin/smbldap-groupadd -p "%g"
  #delete group script = /usr/local/sbin/smbldap-groupdel "%g"
  add user to group script = /usr/local/sbin/smbldap-groupmod -m "%u" "%g"
  delete user from group script = /usr/local/sbin/smbldap-groupmod -x "%u" "%g"
  set primary group script = /usr/local/sbin/smbldap-usermod -g "%g" "%u"

  ...
  Dos charset = 850
  Unix charset = ISO8859-1
```

The shares sections

Here takes place all the share sections. In particular, we can define all the user's home directories which are defined by the [homes] section:

```
  comment = Home Directories
  valid users = %U
  read only = No
  create mask = 0664
  directory mask = 0775
  browseable = No
```

Users' profile will be stored in the share named `[profiles]`. This is the root directory for profiles and the ldap variable *sambaProfilePath* specify exactly the path for each users. For example if the *sambaProfilePath* is set to PDC-SRVprofilestestuser, than the profile directory for user *testuser* is /home/samba/profiles/testuser/. Make sure to have the right permissions for this directory. The sticky bit must be set. Make a simple chmod 1777 /home/samba/profiles and it will be ok. Don't forget that the system doesn't take this change immediately. You should wait several minutes before any profile takes place.

```
  path = /home/samba/profiles
  read only = No
  create mask = 0600
  directory mask = 0700
  browseable = No
  guest ok = Yes
  profile acls = Yes
  csc policy = disable
  # next line is a great way to secure the profiles
  force user = %U
  # next line allows administrator to access all
profiles
  valid users = %U @"Domain Admins"
```

If you want command's file to be downloaded and ran when a user successfully logged in the windows workstation, you have to define a *netlogon* section and a *netlogon script*. The *netlogon script* must take place in the *global* section and the script must be a relative path to the [netlogon] service. For example, if the [netlogon] service specifies a path of */home/samba/netlogon* (like in our example), then if the script is defined as *logon script = STARTUP.BAT*, the file that will be downloaded is */home/samba/netlogon/STARTUP.BAT*. Finally, we defined a *doc* section that authorized everybody to browse the */usr/share/doc* documentation directory.

```
  ...
  logon script = STARTUP.BAT
  ...

[netlogon]
  path = /home/samba/netlogon/
  browseable = No
  read only = yes

[doc]
  path=/usr/share/doc
  public=yes
  writable=no
  read only=no
  create mask = 0750
  guest ok = Yes
```

For example, we could have the STARTUP.BAT script that set the documentation directory mounted on the "J" volume on windows clients. Another useful command set windows time synchronized to the server's one:

```
NET USE J: \\PDC-SRV\doc
NET TIME \\PDC-SRV /SET /YES
```

4.3.2 Preparation

You must create some directories, according to your /etc/samba/smb.conf :

```
mkdir /home/samba
mkdir /home/samba/netlogon
mkdir /home/samba/profiles
chmod 1777 /home/samba/profiles
```

4.3.3 Initial entries

Samba must know the passwd of the `ldap admin dn` (cn=Manager,dc=IDEALX,dc=ORG) user you've specified in smb.conf. This user is used by samba to bind to the directory and must have enough permissions to add/modify accounts stored in the ldap directory.

To do so, use the following command (assuming 'mysecretpwd' is the ldap admin dn password, see your /etc/openldap/slapd.conf configuration file to be sure) :

```
[root@pdc-srv samba]# smbpasswd -w mysecretpwd
Setting stored password for "cn=Manager,dc=IDEALX,dc=ORG" in secrets.tdb
```

Samba will store this datas in /etc/samba/secrets.tbd.

Note that this "ldap admin dn" can be another account than the Root DN : you should use another ldap account who should have permissions to write any sambaSAMAccount and some posixAccount attrs (see section 5 for security considerations).

4.3.4 Testing

To validate your Samba configuration, use testparm who should return 'Loaded services file OK.' without any warnings nor unknow parameter. See man testparm for more info.

4.4 smbldap-tools scripts

Finally, you must configure your smbldap-tools to match your system and LDAP configuration. This can be done in the two files */etc/opt/IDEALX/smbldap-tools/smbldap.conf* and */etc/opt/IDEALX/smbldap-tools/smbldap_bind.conf*.

4.4.1 Configuration

- the */etc/opt/IDEALX/smbldap-tools/smbldap.conf* file You'll find some other configuration options in this configuration file: those are the default values used by smbldap-tools when creating an account (user or computer). Feel free to change those values if desired. Consult the smbldap-tools documentation for more information about configuration parameters. The main option that you need to defined now is the domain secure ID (`SID`). You can obtain its value using the following command

  ```
  net getlocalsid
  ```

  Note that you need to start samba for several minutes for this command to successfull finished)
- the */etc/opt/IDEALX/smbldap-tools/smbldap_bind.conf* file and configure them according to your LDAP configuration (RootDN password and LDAP server @IP address). You'll find two confusing entries: slaveLDAP and masterLDAP. For our first example, those two LDAP servers will be the same one, but in a real life configuration, you may want to have a slave server to serve all your read request, and one dedicated to write request. Anyway, in the current example, as we build the PDC using Samba and OpenLDAP on the same host, you should specify 127.0.0.1 for the two LDAP servers.
  Note that you can't put hashed password here ! This configuration file must then be readable only for root.

4.4.2 Initial entries

We need to add some initial entries on the new configured OpenLDAP server:

1. base entries:
   - base DN: dc=idealx,dc=org
   - base organizational categories (ou=Users,dc=idealx,dc=org, ou=Groups,dc=idealx,dc=org and, ou=Computers, dc=idealx,dc=org)
2. security accounts later used by software clients (Samba and *Linux*):
   - Samba server DN: cn=samba,ou=DSA,dc=idealx,dc=org
   - *Linux* DN: cn=nssldap,ou=DSA,dc=idealx,dc=org
   - smbldap-tools DN: cn=smbldap-tools,ou=DSA,dc=idealx,dc=org

The easiest way to set up your directory and add the default base entries can be done using the `smbldap-populate` script [12]:

```
[root@etoile root]# smbldap-populate
Populating LDAP directory for domain IDEALX-NT (S-1-5-21-4205727931-
4131263253-1851132061)
(using builtin directory structure)

adding new entry: dc=idealx,dc=org
adding new entry: ou=Users,dc=idealx,dc=org
adding new entry: ou=Groups,dc=idealx,dc=org
adding new entry: ou=Computers,dc=idealx,dc=org
adding new entry: uid=root,ou=Users,dc=idealx,dc=org
adding new entry: uid=nobody,ou=Users,dc=idealx,dc=org
adding new entry: cn=Domain Admins,ou=Groups,dc=idealx,dc=org
adding new entry: cn=Domain Users,ou=Groups,dc=idealx,dc=org
adding new entry: cn=Domain Guests,ou=Groups,dc=idealx,dc=org
adding new entry: cn=Domain Computers,ou=Groups,dc=idealx,dc=org
adding new entry: cn=Administrators,ou=Groups,dc=idealx,dc=org
adding new entry: cn=Account Operators,ou=Groups,dc=idealx,dc=org
adding new entry: cn=Print Operators,ou=Groups,dc=idealx,dc=org
adding new entry: cn=Backup Operators,ou=Groups,dc=idealx,dc=org
adding new entry: cn=Replicators,ou=Groups,dc=idealx,dc=org
adding new entry: sambaDomainName=IDEALX-NT,dc=idealx,dc=org

Please provide a password for the domain root:
Changing password for root
New password :
Retype new password :
```

The `sambaDomainName=IDEALX-NT,dc=idealx,dc=org` entry define the samba domain and specially it's domain SID. We also use it to defined the next uidNumber and gidNumber available for creating new users and groups. The default values for those numbers are 1000. You can change it with the `-u` and `-g` option. For example, if you want the first available value for uidNumber and gidNumber to be set to 1500, you can use the following command :

```
smbldap-populate -u 1550 -g 1500
```

The 'Administrator' user's password, ie the root account password is immediatly defined. In fact, any user placed in the "Domain Admins" group will be granted Windows admin rights for the domain, but only the *Administrator* account is allowed to join computers to the domain.

Once added, you should add the security accounts for Samba and *Linux*. To proceed, copy/paste the accounts defined in section 17.3 and add them in the directory with the following command:

```
ldapadd -x -h localhost -D "cn=Manager,dc=IDEALX,dc=ORG" -f smbldap-dsa.ldif -W
```

Finally, set the default password to those accounts:

- the Samba security account, using 'sambasecretpwd' password:

```
 ldappasswd -x -h localhost -D "cn=Manager,dc=IDEALX,dc=ORG" -s sambasecretpwd \
-W cn=samba,ou=DSA,dc=IDEALX,dc=ORG
```

- the *Linux* (nss_ldap) security account, using 'nssldapsecretpwd' password:

```
 ldappasswd -x -h localhost -D "cn=Manager,dc=IDEALX,dc=ORG" -s nssldapsecretpwd \
 -W cn=nssldap,ou=DSA,dc=IDEALX,dc=ORG
```

- the smbldap-tools security account, using 'smbldapsecretpwd' password:

```
 ldappasswd -x -h localhost -D "cn=Manager,dc=IDEALX,dc=ORG" -s smbldapsecretpwd \
-W cn=smbldap-tools,ou=DSA,dc=IDEALX,dc=ORG
```

(type your admin DN password, 'mysecretpwd' to complete the command when prompted).

4.5 Test your system

To test your system, we'll create a system account in LDAP (say 'testuser'), and will try login as this new user.

To create a system account in LDAP, use the smbldap-useradd[13] script (assuming you have already configured your smbldap-tools):

```
[root@pdc-srv tmp]# smbldap-useradd -m testuser1
[root@pdc-srv tmp]# smbldap-passwd testuser1
Changing password for testuser1
New password :
Retype new password :
```

Then, try to login on your system (Unix login) as testuser1 (using another console, or using ssh). Everything should work fine :

```
[user@host-one:~]$ ssh testuser1@pdc-srv
testuser1@pdc-srv's password:
Last login: Sun Dec 23 15:49:40 2004 from host-one

[testuser1@pdc-srv testuser1]$ id
uid=1000(testuser1) gid=100(users) groupes=100(users)
```

Dont forget to delete this testuser1 after having completed your tests :

```
[root@pdc-srv]# smbldap-userdel -r testuser1
```

5 Security considerations

5.1 Use an account which is not Root DN

In this HOWTO, we're using the Root DN : the *ldap admin dn* should be another account than Root DN : you should use another ldap account who should have permissions to write any sambaSAMAccount and some posixAccount attributes.

So if you don't want to use the `cn=Manager,dc=idealx,dc=org` account anymore, you can use a dedicated account for Samba and another one for the smbldap-tools scripts. The two users were created in section 4.4.2 in the `DSA` branch : `cn=samba,ou=DSA,dc=idealx,dc=org` and `cn=smbldap-tools,ou=DSA,dc=idealx,dc=org`. If the password set for thoses account were respectivly *samba* and *smbldap-tools*, you can modify the configuration files as follow (of course, you can use the same account for both samba and smbldap-tools) :

- file */etc/opt/IDEALX/smbldap-tools/smbldap_bind.conf*

```
slaveDN="cn=smbldap-tools,ou=DSA,dc=idealx,dc=org"
slavePw="smbldapsecretpwd"
masterDN="cn=smbldap-tools,ou=DSA,dc=idealx,dc=org"
masterPw="smbldapsecretpwd"
```

- file `/etc/samba/smb.conf`

```
ldap admin dn = cn=samba,ou=DSA,dc=idealx,dc=org
```

  don't forget to also set the samba account password in `secrets.tdb` file :

```
smbpasswd -w sambasecretpwd
```

- file `/etc/openldap/slapd.conf`: many access control list must be set :
  - *samba* user need write access to all samba attributes and some others (uidNumber, gidNumber ...).
  - `smbldap-tools` must have write access to add or delete new users, groups or computers account
  - `nssldap` also need write access to unix password attribute (for example if a user want to change his password with the `passwd` command).

```
# users can authenticate and change their password
access to attrs=userPassword,sambaNTPassword,sambaLMPassword,sambaPwdLastSet,
sambaPwdMustChange
      by dn="cn=samba,ou=DSA,dc=idealx,dc=org" write
      by dn="cn=smbldap-tools,ou=DSA,dc=idealx,dc=org" write
      by dn="cn=nssldap,ou=DSA,dc=idealx,dc=org" write
      by self write
      by anonymous auth
      by * none
# some attributes need to be readable anonymously so that 'id user' can answer
correctly
access to attrs=objectClass,entry,homeDirectory,uid,uidNumber,gidNumber,memberUid
      by dn="cn=samba,ou=DSA,dc=idealx,dc=org" write
      by dn="cn=smbldap-tools,ou=DSA,dc=idealx,dc=org" write
      by * read
# somme attributes can be writable by users themselves
access to attrs=description,telephoneNumber,roomNumber,homePhone,loginShell,gecos,cn,
sn,givenname
      by dn="cn=samba,ou=DSA,dc=idealx,dc=org" write
      by dn="cn=smbldap-tools,ou=DSA,dc=idealx,dc=org" write
      by self write
      by * read
# some attributes need to be writable for samba
access to attrs=cn,sambaLMPassword,sambaNTPassword,sambaPwdLastSet,sambaLogonTime,
sambaLogoffTime,sambaKickoffTime,sambaPwdCanChange,sambaPwdMustChange,sambaAcctFlags,
displayName,sambaHomePath,sambaHomeDrive,sambaLogonScript,sambaProfilePath,
description,sambaUserWorkstations,sambaPrimaryGroupSID,sambaDomainName,
sambaMungedDial,sambaBadPasswordCount,sambaBadPasswordTime,sambaPasswordHistory,
sambaLogonHours,sambaSID,sambaSIDList,sambaTrustFlags,sambaGroupType,sambaNextRid,
sambaNextGroupRid,sambaNextUserRid,sambaAlgorithmicRidBase,sambaShareName,
sambaOptionName,sambaBoolOption,sambaIntegerOption,sambaStringOption,
sambaStringListoption,sambaPrivilegeList
      by dn="cn=samba,ou=DSA,dc=idealx,dc=org" write
      by dn="cn=smbldap-tools,ou=DSA,dc=idealx,dc=org" write
      by self read
      by * none
# samba need to be able to create the samba domain account
access to dn.base="dc=idealx,dc=org"
      by dn="cn=samba,ou=DSA,dc=idealx,dc=org" write
      by dn="cn=smbldap-tools,ou=DSA,dc=idealx,dc=org" write
      by * none
# samba need to be able to create new users account
access to dn="ou=Users,dc=idealx,dc=org"
      by dn="cn=samba,ou=DSA,dc=idealx,dc=org" write
      by dn="cn=smbldap-tools,ou=DSA,dc=idealx,dc=org" write
      by * none
# samba need to be able to create new groups account
access to dn="ou=Groups,dc=idealx,dc=org"
      by dn="cn=samba,ou=DSA,dc=idealx,dc=org" write
      by dn="cn=smbldap-tools,ou=DSA,dc=idealx,dc=org" write
      by * none
# samba need to be able to create new computers account
```

```
access to dn="ou=Computers,dc=idealx,dc=org"
      by dn="cn=samba,ou=DSA,dc=idealx,dc=org" write
      by dn="cn=smbldap-tools,ou=DSA,dc=idealx,dc=org" write
      by * none
# this can be omitted but we leave it: there could be other branch
# in the directory
access to *
      by self read
      by * none
```

5.2 Secure connections: use TLS !

In this HOWTO, whe are using clear LDAP transport between Samba and OpenLDAP. As both servers implement SSL, you should use TLS transport instead.

If you want to use TLS, you have to create a certificate for each servers. Certificates can be self-signed but it is preferable to have certificates signed by the same authority (CA) if OpenLDAP is configured so that client are requested (`TLSVerifyClient demand` in *slapd.conf* file).

The next paragraphs illustrate the few steps needed to set up an example CA and how to create a server's certificate signed by the CA. Refer to the appropriate documentations for more informations (for example `http://www.openldap.org/pub/ksoper/OpenLDAP_TLS_howto.html`).

You may also want to take a look at IDX-PKI for installing the real thing. See `http://www.idealx.com/solutions/idxpki/` for more informations.

Remember one important thing: certificates are created with their common name hardcoded in the certificate. Each time you want to connect to the server in secure mode, you **must** contact it using this name (and not it's IP address, unless you set it's common name to the IP address)!

Certificates creation

For this example, we'll create a CA authority. Next, we'll create a certificate for the server `ldap.idealx.com` wich will be signed by the CA.

1. create the CA key and certificate
   - create directory structure

     ```
     mkdir certs  csr  datas  keys  private datas/ca.db.certs
     touch private/ca.key datas/ca.db.serial
     cp /dev/null datas/ca.db.index
     ```

   - Generate pseudo-random bytes

     ```
     openssl rand 1024 > datas/random-bits
     ```

   - create the key for the CA: a pass phrase will be asked to you. Don't forget it: it will be asked to you each time you want to create a new certificate's server.

     ```
     openssl genrsa -des3 -out private/ca.key 1024 -rand datas/random-bits
     chmod 600 private/ca.key
     ```

     Warning: key the `ca.key` private !
   - Self-sign the root CA

     ```
     openssl req -new -x509 -days 3650 -key private/ca.key -out certs/ca.pem
     ```

- create a configuration `ca.conf` file for the CA

```
      default_ca              = default_CA
      [ default_CA ]
      dir                     = .                       # Where everything is kept
      certs                   = ./certs                 # Where the issued certs are
kept
      new_certs_dir           = ./datas/ca.db.certs     # Where the issued crl are
kept
      database                = ./datas/ca.db.index     # database index file
      serial                  = ./datas/ca.db.serial    # The current serial number
      RANDFILE                = ./datas/random-bits     # private random number file
      certificate             = ./certs/ca.pem          # The CA certificate
      private_key             = ./private/ca.key        # The private key
      default_days            = 730
      default_crl_days        = 30
      default_md              = md5
      preserve                = no
      x509_extensions         = server_cert
      policy                  = policy_anything
      [ policy_anything ]
      countryName             = optional
      stateOrProvinceName     = optional
      localityName            = optional
      organizationName        = optional
      organizationalUnitName  = optional
      commonName              = supplied
      emailAddress            = optional
      [ server_cert ]
      #subjectKeyIdentifier   = hash
      authorityKeyIdentifier  = keyid:always
      extendedKeyUsage        = serverAuth,clientAuth,msSGC,nsSGC
      basicConstraints        = critical,CA:false
```

- initialize the serial database

```
echo '01' > datas/ca.db.serial
```

2. create the server key and certificate for `ldap.idealx.com` server
   - create the key for the server `ldap.idealx.com`

```
openssl genrsa -out keys/ldap.idealx.com.key 1024
```

   - create certificate data for ldap.idealx.com: when asking you for the *Common Name*, you **must** set the full qualified name of the server, ie `ldap.idealx.com`

```
openssl req -new -key keys/ldap.idealx.com.key -out csr/ldap.idealx.com.csr
```

   - sign the ldap.idealx.com certificate with the CA one

```
openssl ca -config ca.conf -out certs/ldap.idealx.com.txt -infiles csr/ldap.
idealx.com.csr
```

   - extract the ldap.idealx.com certificate

```
perl -n -e 'm/BEGIN CERTIFICATE/ && do {$$seen=1}; $$seen && print;' < certs/
ldap.idealx.com.txt > certs/ldap.idealx.com.pem
```

- you can also verify the certificate

```
openssl verify -CAfile certs/ca.pem certs/ldap.idealx.com.pem
```

3. you then have the three files you need for setting up properly the configuration's server :
   - `./certs/ca.pem` : the CA certificate
   - `./certs/ldap.idealx.com.pem` : the ldap server certificate
   - `./keys/ldap.idealx.com.key` : and it's associated key

Configure the smbldap-tools scripts

The smbldap-tools scripts will connect to the secure directory. We'll then need to create a certificate for this client : use `smbldap-tools` as common name.
Update the configuration file */etc/opt/IDEALX/smbldap-tools/smbldap.conf* :

- activate the TLS support
  `ldapTLS="1"`
- the file that contains the client certificate
  `clientcert="`*`/etc/opt/IDEALX/smbldap-tools/smbldap-tools.pem`*`"`
- the file that contains the private key that matches the certificate stored in the *clientcert* file
  `clientkey="`*`/etc/opt/IDEALX/smbldap-tools/smbldap-tools.key`*`"`
- the PEM-format file containing certificates for the CA's that slapd will trust.
  `cafile="`*`/etc/opt/IDEALX/smbldap-tools/ca.pem`*`"`

Configure OpenLDAP

Create a certificate for the OpenLDAP server with common name `ldap.idealx.com`.
Update the configuration file `/etc/openldap/slapd.conf` and set :

- the file that contains the server certificate
  `TLSCertificateFile ldap.idealx.com.pem`
- the file that contains the private key that matches the certificate stored in the *TLSCertificateFile* file
  `TLSCertificateKeyFile ldap.idealx.com.key`
- the PEM-format file containing certificates for the CA's that slapd will trust
  `TLSCACertificateFile ca.idealx.com.pem`

You can also request a valid certificate to all incoming TLS session :

- TLSVerifyClient demand

Configure Samba

Simply add one line in the configuration file `/etc/samba/smb.conf` :

- `ldap ssl = start tls`

Configure the linux operating system

Check that the `/etc/ldap.conf` contains the following informations :

- the OpenLDAP server
  `host ldap.idealx.com`
- the distinguished name of the search base
  `base dc=idealx,dc=org`
- require and verify server certificate
  `tls_checkpeer yes`

- the PEM-format file containing certificates for the CA's that slapd will trust.
  `tls_cacertfile /etc/opt/IDEALX/smbldap-tools/ca.pem`
- OpenLDAP SSL mechanism
  `ssl start_tls`
- if you also configured OpenLDAP to request a valid certificate to all incoming TLS session (with the "TLSVerifyClient demand" directive), you have to create a certificate for nss. Then you can add the two following lines :
  `tls_cert /etc/nss/nss.idealx.org.pem`
  `tls_key /etc/nss/nss.idealx.org.key`

Be careful to set a proper name for the *host* directive: it must match the exact name that what given to the OpenLDAP server certificate. It must also be a resolvable name.

5.3 Backup your datas

TODO: how to backup and restore your PDC !

Crucial ! Some scripts may help do the job (even if not used, the will explain what to backup exactly, and how to restore). In fact, those scripts just have to backup: config files (ldap, nss, ldap, samba and tbds..) and the 'SAM' (so a LDIF may do the job). An smbldap-backup and smbldap-restore?

6 Start-Stop servers

To :

- start/stop the OpenLDAP server : `/etc/init.d/ldap start/stop`
- start/stop the Samba server : `/etc/init.d/smb start/stop`

7 Migrating posix accounts and groups

Pawel Wielaba has written two scripts `smbldap-migrate-unix-accounts` and `smbldap-migrate-unix-groups` to help you migrating users and groups defined in `/etc/passwd` (and/or `/etc/shadow`) and `/etc/group`.

You can find his scripts with the smbldap-tools package (in documentation directory for rpm package). They can also be found on his site : http://www.iem.pw.edu.pl/~wielebap/ldap/smbldap-tools/2/

7.1 users migration (from `/etc/shadow`)

We suppose that you use the shadow password. We'll then also use the shadow file to migrate password's account.
Users migration should be done as follow :

1. copy `/etc/passwd` and `/etc/shadow` in a temporary directory :

   ```
   cp /etc/passwd /etc/shadow /tmp/
   ```

2. remove all accounts on both file that you not want to be in the directory :

   ```
   for user in root nobody bin daemon
   do
    export user
    perl -i -pe's@^$ENV{user}:(.*)\n@@' /tmp/passwd
    perl -i -pe's@^$ENV{user}:(.*)\n@@' /tmp/shadow
   done
   ```

   don't forget to remove the user *nobody* as it is created when initializing the directory with `smbldap-populate`.
3. migrate accounts :

```
/usr/share/doc/smbldap-tools-*/smbldap-migrate-unix-accounts -a -P /tmp/passwd -
S /tmp/shadow
```

4. remove migrated users from `/etc/passwd` and `/etc/shadow`

Note : with the `-a` option on `smbldap-migrate-unix-accounts`, the *sambaSAMAccount* will be added to users. All users having previously a shell defined in `/etc/passwd` will then be able to connect to the server and update their "windows" password using `/opt/IDEALX/sbin/smbldap-passwd` script.

7.2 groups migration (from `/etc/group`)

We'll now migrate all groups defined in `/etc/group` file. Migration process should be done as follow :

1. copy `/etc/group` in a temporary directory :

```
cp /etc/group /tmp/
```

2. remove all groups that you not want to be in the directory :

```
for group in root bin daemon
do
        export group
        perl -i -pe's@^$ENV{group}:(.*)\n@@' /tmp/group
done
```

3. migrate groups :

```
/usr/share/doc/smbldap-tools-*/smbldap-migrate-unix-groups -a -G /tmp/group
```

4. remove migrated groups from `/etc/group`

Note : with the `-a` option on `smbldap-migrate-unix-groups`, the *sambaGroupMapping* will be added to groups so that they can be used as "windows" groups (samba will than mapped unix groups to windows groups). You should remove this option if you don't want this.

8 Exploitation

8.1 User management

To manager user accounts, you can use:

1. smbldap-tools, using the following scripts:
   - smbldap-useradd : to add a new user
   - smbldap-userdel : to delete an existing user
   - smbldap-usermod : to modify an existing user data
2. idxldapaccounts (webmin module) if you are looking for a nice Graphical User Interface.
3. Microsoft Windows NT Domain management tools

The first method will be presented hereafter.

8.1.1 A LDAP view

First, let's have a look on what is really a user accounts for LDAP. In fact, there is two kinds of user accounts :

- Posix Accounts, for use with LDAP-aware systems like Unix (*Linux* using pam_ldap and nss_ldap, in this HOWTO).

Those kind of accounts use the posixAccount, or shadowAccount if you are using shadow passwords.

- Samba Accounts, for the use of Samba Windows user accounts (and computer accounts too). Those kind of accounts use the sambaSAMAccount LDAP object class (according to the Samba samba.schema).

Here's a LDAP view of an Unix Account (posixAccount in fact, for this HOWTO) :

```
dn: uid=testuser1,ou=Users,dc=IDEALX,dc=ORG
objectClass: top
objectClass: account
objectClass: posixAccount
cn: testuser1
uid: testuser1
uidNumber: 1000
gidNumber: 100
homeDirectory: /home/testuser1
loginShell: /bin/bash
gecos: User
description: User
userPassword: {SSHA}ZSPozTWYsy3addr9yRbqx8q5K+J24pKz
```

Here's a LDAP view of a Samba user account (sambaSAMAccount) :

```
dn: uid=testsmbusers2,ou=Users,dc=idealx,dc=org
objectClass: top,inetOrgPerson,posixAccount,shadowAccount,sambaSAMAccount
cn: testsmbusers2
sn: testsmbusers2
uid: testsmbusers2
uidNumber: 1000
gidNumber: 513
homeDirectory: /home/testsmbusers2
loginShell: /bin/bash
gecos: System User
description: System User
sambaLogonTime: 0
sambaLogoffTime: 2147483647
sambaKickoffTime: 2147483647
sambaPwdCanChange: 0
displayName: System User
sambaSID: S-1-5-21-4231626423-2410014848-2360679739-3000
sambaPrimaryGroupSID: S-1-5-21-4231626423-2410014848-2360679739-513
sambaLogonScript: testsmbusers2.cmd
sambaProfilePath: \\PDC-SRV\profiles\testsmbusers2
sambaHomePath: \\PDC-SRV\home\testsmbusers2
sambaHomeDrive: H:
sambaLMPassword: 7584248B8D2C9F9EAAD3B435B51404EE
sambaAcctFlags: [U]
sambaNTPassword: 186CB09181E2C2ECAAC768C47C729904
sambaPwdLastSet: 1081281346
sambaPwdMustChange: 1085169346
userPassword: {SSHA}jg1v0WaeBkymhWasjeiprxzHxdmTAHd+
```

Here follow a quick explanation about the attributes used:

Attribute	from schema	Usage
cn	core	usually, the username
uid	core	username
description	core	TODO
userPassword	core	password for Unix systems using NSS/PAM LDAP

displayName	inetorgperson	TODO
uidNumber	nis	the numeric user number (Unix and Samba)
gidNumber	nis	the primary group number of the user (Unix)
loginShell	nis	the logon shell used on Unix systems
gecos	nis	the long form of the username
homeDirectory	nis	home directory path for Unix systems
sambaPwdLastSet	samba	The integer time in seconds since 1970 when
		the lm and ntpasswd were last set.
sambaLogonTime	samba	timestamp of last logon
sambaLogoffTime	samba	timestamp of last logoff
sambaKickoffTime	samba	timestamp of when the user will be logged off automatically
sambaPwdCanChange	samba	timestamp of when the user is allowed to update the password
sambaPwdMustChange	samba	timestamp of when the password will expire
sambaPwdLastSet	samba	timestamp of the last password update
sambaAcctFlags	samba	specify the type of the samba account
sambaBadPasswordCount	samba	Bad password attempt count
sambaBadPasswordTime	samba	Time of the last bad password attempt
		(W=workstation, U=user, D=disabled,
		X=no password expiration,...)
sambaSID	samba	the secure identifier (SID) of the user
sambaPrimaryGroupID	samba	the relative identifier (SID) of the primary group
		of the user
sambaHomePath	samba	specifies the path of the home directory for the
		user. The string can be null. If homeDrive is set and
		specifies a drive letter, homeDirectory should be a
		UNC path. The path must be a network UNC path.
		This value can be a null string
sambaLogonScript	samba	The scriptPath property specifies the path of
		the user's logon script, .CMD, .EXE, or .BAT file.
		The string can be null. The path is relative to the
		netlogon share
sambaLMmPassword	samba	the LANMAN password
sambaNTPassword	samba	the NT password (md4 hash)
sambaHomeDrive	samba	specifies the drive letter to which to map the UNC
		path specified by homeDirectory. The drive letter
		must be specified in the form "driveletter:" where
		driveletter is the letter of the drive to map.
		For example: "Z:"
sambaProfilePath	samba	specifies a path to the user's profile. This value
		can be a null string, a local absolute path, or
		a UNC path

Table 1: Attributes used for a user Account

8.1.2 Using the smbldap-tools scripts

To manipulate user accounts, we've developped a collection of PERL scripts named smbldap-tools : they provide all the tools you need to manage user and groups accounts, in a LDAP directory.

Because we've merged posixAccount, shadowAccount and sambaAccount, those scripts may be used to manage Unix and Windows (Samba) accounts. As most of existing software are LDAP aware, you can use your SAMBA-LDAP PDC to be an unique source of authentification, and the smbldap-tools may offer you a good base to manage user accounts datas.

In this Howto, we have used the following tools to manage user accounts :

- smbldap-useradd : to add an user account (by default a posixAccount. Using '-a' option for a sambaSAMAccount, '-w' option for a machine sambaAccount),
- smbldap-userdel : to delete an existing user account
- smbldap-usermod : to modify an user account.
- smbldap-userinfo : to allow users to modify some informations themselves

For a detail used of those scripts, consult the smbldap-tools's documentation on the project homepage[14].

Create a Unix (Posix) user account

To create a new posixAccount (only usefull for Unix) named testposixuser (we'll use 'coucou' as the password when asked):

```
[root@pdc-srv testsmbuser2]# smbldap-useradd -m testposixuser
[root@pdc-srv testsmbuser2]# smbldap-passwd testposixuser
Changing password for testposixuser
New password for user testposixuser:
Retype new password for user testposixuser:
```

Create an Samba user account

To create a new sambaSAMAccount (for use under Unix and Samba) named jdoo (we'll use 'coucou' as the password when asked) :

```
[root@pdc-srv testsmbuser2]# smbldap-useradd -a -m -c "John Doo" jdoo
[root@pdc-srv testsmbuser2]# smbldap-passwd jdoo
Changing password for jdoo
New password for user jdoo:
Retype new password for user jdoo:
```

Setup an user password

You can use smbldap-passwd as a replacement for the system command passwd and the Samba command smbpasswd:

```
[root@pdc-srv testsmbuser2]# smbldap-passwd jdoo
Changing password for jdoo
New password for user jdoo:
Retype new password for user jdoo:
```

Delete a Posix user account

Just use the following smbldap-tools command:

```
[root@pdc-srv testsmbuser2]# smbldap-userdel -r jdoo
```

In this example, we wanted to remove the user named 'jdoo' and his home directory.

Delete a Samba user account

Exactly like for the deletion of an Unix account, just use smbldap-userdel.

Modify an user account

Use the smbldap-usermod to modify a user's account. Options available with the smbldap-useradd script are also available here.

Another script smbldap-userinfo can be used by users so that they can update their own informations (such as telephoneNumber, rootNumber, shell, ...) themselves. Note that this implies that correct ACL must be defined on the directory configuration.

8.1.3 Using Idealx Management Console (IMC)

Have a look on the project site (http://www.idealx.org/prj/imc/) for more informations on installation procedure.

8.1.4 Using idxldapaccounts webmin module

If you prefer nice GUI to shell, you should have a look on the idxldapaccounts Webmin module. See `http://webmin.idealx.org/`. This module is available for both samba2 and samba3. Note that idxldapaccounts is not maintained anymore !

8.1.5 Using the Microsoft Windows NT Domain management tools

You can manager users account using the Microsoft Windows NT Domain management tools. This can be launch using the `usrmgr.exe` command in a msdos console

8.2 Group management

A unix group need to be mapped to a windows group if you want it to be seen and used from Microsoft Windows environment. This can be done automatically.

To manager group accounts, you can use:

1. smbldap-tools using the following scripts:
   - smbldap-groupadd : to add a new group
   - smbldap-groupdel : to delete an existing group
   - smbldap-groupmod : to modify an existing group
2. idxldapaccounts if you are looking for a nice Graphical User Interface.
3. Microsoft Windows NT Domain management tools

The first method will be presented hereafter.

8.2.1 A LDAP view

First, let's have a look on what is really a posix group account for LDAP. Here's a LDAP view of a group named unixGroup:

```
dn: cn=unixGroup,ou=Groups,dc=idealx,dc=org
objectClass: posixGroup
cn: unixGroup
gidNumber: 1000
memberUid: usertest1
memberUid: usertest2
```

Here's a LDAP view of a Samba group named sambaGroup:

```
dn: cn=sambaGroup,ou=Groups,dc=idealx,dc=org
objectClass: posixGroup,sambaGroupMapping
gidNumber: 512
cn: sambaGroup
description: Samba Group
sambaSID: S-1-5-21-4231626423-2410014848-2360679739-3001
sambaGroupType: 2
displayName: sambaGroup
memberUid: testsmbuser2
memberUid: testsmbuser1
```

8.2.2 Windows specials groups

The Windows world come with some built-ins users groups :

Group name	rid	Group SID	Description
Domain Admins	512	$SID-512	
Domain Users	513	$SID-513	
Domain Guests	514	$SID-514	
Print Operators	550	S-1-5-32-550	
Backup Operators	551	S-1-5-32-551	
Replicator	552	S-1-5-32-552	

Table 2: Well known rid and corresponding SID of windows administrative groups. $SID refer to the domain secure ID

8.2.3 Using the smbldap-tools scripts

To manipulate groups, we've developped a collection of PERL scripts named smbldap-tools : they provide all the tools you need to manage user and groups accounts, in a LDAP directory.

Because Samba use posixGroup, those scripts may be used to manage Unix and Windows (Samba) accounts. As most of existing software are LDAP aware, you can use your SAMBA-LDAP PDC to be an unique source of authentification, and the smbldap-tools may offer you a good base to manage user accounts datas.

In this Howto, we have used the following tools to manage groups :

- smbldap-groupadd : to add a new group,
- smbldap-userdel : to delete an existing group,
- smbldap-usermod : to modify any group datas (mostly to add or remove an user from a given group).

For a detail used of those scripts, consult the smbldap-tools's documentation on the project homepage[15].

8.2.4 Using Idealx Management Console (IMC)

Have a look on the project site (http://www.idealx.org/prj/imc/) for more informations on installation procedure.

8.2.5 Using idxldapaccounts webmin module

If you prefer nice GUI to shell, you should have a look on the idxldapaccounts Webmin module. See `http://webmin.idealx.org/`. Note that idxldapaccounts is not maintained anymore !

8.2.6 Using the Microsoft Windows NT Domain management tools

You can manager users account using the Microsoft Windows NT Domain management tools. This can be launch using the `usrmgr.exe` command in a msdos console

8.3 Computer management

To manage computer accounts, we'll use the following scripts (from smbldap-tools) :

- smbldap-useradd : to add a new computer
- smbldap-userdel : to delete an existing computer
- smbldap-usermod : to modify an existing computer data

Computer accounts are sambaSAMAccounts objects, just like Samba user accounts are.

8.3.1 A LDAP view

Here's a LDAP view of a Samba computer account :

```
dn: uid=testhost3$,ou=Computers,dc=IDEALX,dc=ORG
objectClass: top
objectClass: posixAccount
objectClass: sambaSAMAccount
cn: testhost3$
gidNumber: 553
homeDirectory: /dev/null
loginShell: /bin/false
uid: testhost3$
uidNumber: 1005
sambaPwdLastSet: 0
sambaLogonTime: 0
sambaLogoffTime: 2147483647
sambaKickoffTime: 2147483647
sambaPwdCanChange: 0
sambaPwdMustChange: 2147483647
description: Computer Account
rid: 0
primaryGroupID: 0
lmPassword: 7582BF7F733351347D485E46C8E6306E
ntPassword: 7582BF7F733351347D485E46C8E6306E
acctFlags: [W          ]
```

TODO: explain the LDIF, present attribute types (from schema) and explain them.

8.3.2 Using the smbldap-tools scripts

To manipulate computer accounts, we've developped a collection of PERL scripts named smbldap-tools: they provide all the tools you need to manage user and groups accounts, in a LDAP directory.

In this Howto, we have used the following tools to manage user accounts :

- smbldap-useradd : to add a computer account, using -w option,
- smbldap-userdel : to delete an existing computer account ,
- smbldap-usermod : to modify an existing computer account.

Create a Computer account

To create a computer account, you can use smbldap-tools to manually add accounts :

```
[root@pdc-srv root]# smbldap-useradd -w testcomputer1
```

You can also use the automatic procedure within your Microsoft Windows client (see your client chapter: Microsoft Windows NT, w2k...) for more information.

Delete a Computer account

To delete a computer account, just use smbldap-tools :

```
[root@pdc-srv root]# smbldap-userdel testcomputer1$
```

Instead of removing the computer account, you may want to de-activate the Samba Account. The easyest way is to use the `smbldap-usermod` script as follow :

- to disable the computer account : `smbldap-usermod -I testcomputer1$`
- enable the computer account : `smbldap-usermod -I testcomputer1$`

You can also use an LDAP browser and modify the 'acctFlags' from [W] to [WD] ('D' indicating 'Disabled'). To re-activate the computer account, just modifiy [WD] to [W]. Sometimes, de/re-activation is a better mean to temporary disable the workstation for some times.

8.4 Profile management

WARNING : Under writing !

TODO: Howto manage profiles (NT profiles, as Unix do the job since... AT&T time...)

8.4.1 Roaming/Roving profiles

When a Microsoft Windows NT user joined the IDEALX-NT domain, his profile is stored in the directory defined in the *profile* section of the samba configuration file. He has to log out for the profile to be saved. This is a roaming profile : he can use this profile from any computer he want. If his personal configuration changed, it will be integrated in his roaming profile.

In this Howto, we used roaming profiles: the LDAP sambaProfilePath attribute indicate to Samba where to look for those roaming profile (

PDC-SRV
profiles
testsmbuser2 for example), and the [profiles] section of the /etc/samba/smb.conf indicate to samba how to deal with those profiles.

Keep in mind that a 'regular' roaming profile is about 186 Kb of data (even more if users uses big GIF or BMP image as background picture ...): don't forget impact on load/traffic...

8.4.2 Mandatory profiles

The mandatory profile is created by the same way of the roaming profile. The difference is that his profile is made read only by the administrator so that the user can have only one fixed profile on the domain.

To do so, rename the file NTuser.dat to NTuser.man (for MANdatory profile), and remove the right access bit. For our *testsmbuser1* user, you'll have to do:

```
mv /opt/samba/profiles/testsmbuser1/NTUSER.DAT /opt/samba/profiles/
testsmbuser1/NTUSER.MAN
chmod -w /opt/samba/profiles/testsmbuser1/NTUSER.MAN
```

This way, you may want to set up a common user profile for every user on the Domain.

8.4.3 Logon Scripts

To use Logon Scripts (.BAT or .CMD), just specify the relative path from the netlogon share to the command script desired in the **sambaScriptPath** attribute for the user.

Variable substitutions (the logon script smb.conf directive when you're using LDAP.

8.4.4 LDAP or not LDAP?

Perhaps, you'll want to use an alternative system policy concerning profiles : granting some user the roaming profile privilege across the domain, while some other may have only roaming profile on one PDC server, and some other won't use roaming profile at all. This alternative way is possible thanks to Samba who will search in the LDAP sambaSAMAccount for the profile location if no information is given by the 'logon drive', 'logon script' and 'logon path' directives of smb.conf.

We'll discuss this alternative in a future revision of this document.

9 Interdomain Trust Relationships

We'll have a look on how making interdomain trust relationships so that

- Samba-3 trusts NT4 (NT4 is the trusted domain, Samba-3 is the trusting domain)
- NT4 trusts Samba-3 (samba-3 is the trusted domain, NT4 is the trusting domain)

Domain properties for each domain are :

- NT4 domain : domain `NT4`, netbios name `PDC-NT4`
- Samba-3 domain: domain `IDEALX-NT`, netbios name `PDC-SRV`

9.1 Samba-3 trusts NT4

On the Windows NT Server, open "User Manager", "Policies" menu, and "Trust Relationship". Now create an account for the samba-3 domain :

```
domaine: IDEALX-NT
mot de passe: secret
```

Let's establish the trust from the Samba-3 server :

```
net rpc trustdom establish NT4
```

Note that this command may fail with major release of samba with the following error message:

```
[root@etoile root]# net rpc trustdom establish IDEALX
Password:
Could not connect to server POMEROL
[2005/06/23 16:52:36, 0] rpc_parse/parse_prs.c:prs_mem_get(537)
  prs_mem_get: reading data of size 4 would overrun buffer.
[2005/06/23 16:52:36, 0] utils/net_rpc.c:rpc_trustdom_establish(4686)
  WksQueryInfo call failed.
```

This is caused by the security *restrictanonymous* parameter set on the Windows NT4 server :

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous
```

If so, set it to `0` and restart the NT4 server.

9.2 NT4 trusts Samba-3

On the Samba-3 domain controler, create an account for the `NT4` domain :

```
smbldap-useradd -i NT4
```

The created account will have a '$' caracter appended to its name (as workstation account), the sambaSAMAccount objectclass and the 'I' flag. A password will also be asked for this account.

Let's establish the trust from Windows NT Server : open the "User Manager", "Policies" menu, and "Trust Relationship". Now join the trusting domain : enter IDEALX-NT and the password defined in the previous command.

10 Integration

10.1 Fake user root

To allow workstations to be joined to the domain, a root user must exist and used (uid=0).

Such a user is created when initializing the directory whith the `smbldap-populate` script.

From Samba 3.0.12, it is now possible for admin users to join computers to the domain without using the "root" account.
For example, to allow members of the "Domain Admins" group to join computers to the domain, you need to

- add the admin user to the "Domain Admin" group

```
smbldap-usermod -G +512 adminuser
```

- add the following directive to samba configuration file ([global] section in smb.conf)

```
enable privileges = yes
```

- execute the following command (replace XXX with the root's password)

```
net -U root%XXX rpc rights grant 'IDEALX-NT\Domain Admins' SeMachineAccountPrivilege
```

In fact, the 'root' account is needed in the first place so that the SeXXX privileges can be set.

10.2 Workstations integration

10.2.1 Adding a new computer in the domain by creating an account manually

If you want the computer named "testmachine" to be added to the domain IDEALX-NT, you must create a account for it.
This can be manually done using the script smbldap-useradd previously described in the section 8.1. Then you can add
the computer in the domain, following this steps :

for Microsoft Windows NT 4 (SP1, SP6):

- logged into Microsoft Windows NT using the administrator account
- click on the "start" menu, "Parameters" and "Configuration"
- double click on "Network" and the "modify" button
- you must now see the machine's name and the domain's name. You have to change the default parameters, or modifie a previous configuration. Then select the "domain" option and add the name of the domain you want to join.
- click on the "ok" button
- the computer is already registered so that you normally have the welcome message "welcome to domain IDEALX-NT"
- restart your windows system.

for Microsoft Windows NT, Windows XP and Microsoft Windows 2000 :

- logged into windows using the administrator account.
- click on the "start" menu, "Parameters" and "Configuration".
- double click on "System", select the onglet "Network identification" and then "properties".
- you must now see the machine's name. You have to change the default parameters, or to modifie a previous configuration by indicating the domaine name.
- the computer is already registered so that you normally have the welcome message "welcome to domain IDEALX-NT"
- restart your windows system.

10.2.2 Adding a new computer in the domain automatically

A second way to do this can be directly done from Microsoft Windows NT environnement, using the administrator priviledged account. This procedure will create automatically an account for the comuter, and will also join it to the domain.

To do so, follow the same steps as the previous section described in section 10.2.1. When informing the domain name, ask for creating a new computer account, and add the administrator account For Microsoft Windows NT 2000, the account is asked when prssing the "ok" button.

- Login : administrator
- Password : coucou

10.3 Servers integration

10.3.1 Samba Member Server

TODO: explain configuration

The smb.conf of this Samba member server should indicate:

```
; Samba Domain Member server
; like the Samba-LDAP PDC but without security user and LDAP directives, but
; the followin lines:
security = domain
password server = hostname.fqdn (or IP address) of the Samba-LDAP PDC
; note: this samba server does not need to be compiled with
; --with-ldapsam option
```

Once configured and started, you should add the machine account on the PDC, using the following commands:

```
root@on-the-PDC# smbldap-useradd -w short-hostname-of-the-samba-member-server
```

and then, on the Samba member server itself:

```
root@on-the-member-server# smbpasswd -j "IDEALX-NT"
```

10.3.2 Samba BDC Server

TOD0: explain. explain alternatives

10.3.3 Microsoft Windows NT Member Server

TODO: explain

10.3.4 Microsoft Windows NT BDC Server

TODO: explain why not :-)

10.3.5 Windows 2000 Member Server

TODO: explian

10.3.6 Windows 2000 BDC Server

TODO: explain why not :-)

11 Migration

In this section, we'll describe how to migrate from a Microsoft Windows NT PDC Server to a Samba+LDAP Domain Controler, in two different user cases:

- migration from a given Domain (the old one) to another (the new one),
- the same Domain is used

In both cases, emphasis must be placed on transparency of migration: movement to the new system (Samba+LDAP) should be accomplished with the absolute minimum of interference to the working habits of users, and preferably without those users even noticing that is has happened, if feasible.

In both cases, migration concern the following informations:

1. users accounts (humans and machines),
2. groups and group members,
3. users logon scripts,
4. users profiles (NTUSER.DAT),
5. all datas,
6. all shares and shares permissions informations,
7. all NTFS ACLs used by users on shares.

11.1 General issues

In this example, we'll suppose that we want to migrate a NT4 domain defined with :

- workgroup: NT4_DOMAIN
- netbios name : NT4_PDC

11.1.1 Users, Groups and machines accounts

Let's have a look on the different steps needed to migrate all the accounts...

- Initial entries
  before migrating the directory, you have to create the organizatioal unit to store accounts. These are *ou=Users*, *ou=Groups* and *ou=Computers*. You will also need to create the well knows administrative groups (*cn=Domain Admins*, *cn=Domain Users* and *cn=Domain Computers*). The first step is to find the SID of the NT4 domain you want to migrate.

  ```
  net rpc getsid -S NT4_PDC -W NT4_DOMAIN
  ```

  And we can now configure the smbldap-tools correctly in the */etc/opt/IDEALX/smbldap-tools/smbldap.conf* configuration file :

  ```
  SID="S-1-5-21-191762950-446452569-929701000"
  ```

  Then we can create our directory structure :

  ```
  smbldap-populate
  ```

- configure samba
  You have to configure samba as a BDC to allow accounts and groups migrations to the samba server. The `smb.conf` configuration file must have :

  ```
  Workgroup = NT4_DOMAIN
  domain master = No
  ```

  Where `NT4_DOMAIN` is the domain that the Windows NT4 PDC control.

  Next, Samba must be configured to use the smbldap-tools scripts. This allows administrators to add, delete or modify user and group accounts for Microsoft Windows operating systems using, for example, User Manager utility under MS-Windows. To enable the use of those scripts, samba needs to be configured correctly. The `smb.conf` configuration file

must contain the following directives :

```
ldap delete dn = Yes
add user script = /usr/local/sbin/smbldap-useradd -m "%u"
add machine script = /usr/local/sbin/smbldap-useradd -w "%u"
add group script = /usr/local/sbin/smbldap-groupadd -p "%g"
add user to group script = /usr/local/sbin/smbldap-groupmod -m "%u" "%g"
delete user from group script = /usr/local/sbin/smbldap-groupmod -x "%u" "%g"
set primary group script = /usr/local/sbin/smbldap-usermod -g "%g" "%u"
```

Finally, you have to restart samba :

```
/etc/init.d/smb restart
```

Remark: the two directives `delete user script` et `delete group script` can also be used. However, an error message can appear in User Manager even if the operations actually succeed. If you want to enable this behaviour, you need to add

```
delete user script = /usr/local/sbin/smbldap-userdel "%u"
delete group script = /usr/local/sbin/smbldap-groupdel "%g"
```

- join the samba server to the domain managed by the Windows NT4 domain controller.
  For this to be done, you need to know an administrative account for the domain. We'll suppose that this account is `Administrator` with password `password` :

  ```
  net rpc join -Uadministrator%passsword
  ```

  This will create a DBC server account for the samba server on the NT4 Windows PDC. **If this step fail**, you certainly have a netbios resolution problem. The best way is to update the */etc/samba/lmhosts* to set the internet adress of the primary domain controler. For example, you can have :

  ```
  192.168.0.1   NT4_PDC
  192.168.0.1   NT4_DOMAIN
  ```

  where `NT4_DOMAIN` is the domain managed by the `NT4_PDC` domain controller.

- migrate accounts and groups to the LDAP directory.

  ```
  net rpc vampire -S NT4_PDC
  ```

  Note that there is no need to give a user/password for vampire, the procedure is done anonymously using server password (set when joining the domain).

- stop the Windows NT4 domain controller

- configure samba to be the primary domain controller (PDC).
  the configuration file */etc/samba/smb.conf* must contain :

  ```
  domain master = Yes
  ```

- restart samba :

  ```
  /etc/init.d/smb restart
  ```

11.1.2 Logon scripts

Logon scripts are DOS scripts that are run every time someone logs on. They must be placed on the **[netlogon]** special share, and you can specify, for each user, the location of this script in the *sambaScriptPath* LDAP attribute.

For example, if your special netlogon share is defined like the following example in your /etc/samba/smb.conf configuration file:

```
        comment = Network Logon Service
        path = /data/samba/netlogon
        guest ok = Yes
```

And you want the user **myuser** to execute the script named myuser.cmd, just complete the following operations:

- copy the myuser.cmd from the old PDC to the new *Linux* server on /opt/samba/netlogon/myuser.cmd,
- modify the LDAP user definition by placing myuser.cmd on the *sambaScriptPath* attribute,
- logon as **myuser** on a Microsoft Windows NT (or Windows 2000) workstation connected to the domain, just to test the logon script activation on login.

So, to migrate all logons scripts from the old Microsoft Windows NT PDC to the new *Linux* server, just copy all logon scripts (placed in C:WINNTsysem32replimport) to /opt/samba/netlogon/, and modify the *sambaScriptPath* users definitions in the LDAP directory to record the name of the user's logon scripts.

Note that if both `logon scripts` directive of smb.conf and *sambaScriptPath* users definitions are used, the ldap definition will be used. This also mean that if you don't want any logon script for a user, the *sambaScriptPath* attribute for the user must not have any value defined, and also the general `logon scripts` directive in smb.conf file.

11.1.3 Users profiles

To be written.

11.1.4 Datas

To be written. Use Rsync !

11.1.5 Shares and permissions

To be written.

11.1.6 NTFS ACLs

To be written. use chacl !

11.2 Same domain

To be written.

11.3 Changing domain

To be written.

12 Troubleshooting

The test-list presented in this section are common to all windows system's versions. If one version may cause problem, or if the procedure is different, we'll make a special note.

12.1 Global configuration

This section help you to test the good configuration and the good operation of your samba-ldap system. We suppose that your system is running all the needed services. You can verify this using the following steps :

- If you have problems starting samba, you can use the testparm command to see if the configuration's file syntax is right :

```
Load smb config files from /etc/samba/smb.conf
Processing section "[netlogon]"
Processing section "[profiles]"
Processing section "[printers]"
Processing section "[print$]"
Processing section "[homes]"
Loaded services file OK.
```

- Check if processes are present

```
[root@PDC-SRV root]# ps afuxw | grep smb
0        17049  0.0  0.7  5524 1888 ?        S    11:45   0:00 smbd -D
1002     17146  0.0  1.3  7184 3408 ?        S    11:50   0:00  \_ smbd -D
0        17223  0.1  1.2  7060 3140 ?        S    12:00   0:00  \_ smbd -D
[root@PDC-SERV root]# ps afuxw | grep nmb
0        17054  0.0  0.7  4636 1856 ?        S    11:45   0:00 nmbd -D
0        17057  0.0  0.6  4584 1552 ?        S    11:45   0:00  \_ nmbd -D
```

- is your ldap server up ? You can verify using the following command line :

```
[root@PDC-SRV root]# ps afuxw | grep ldap
ldap     12358  0.0  5.0 16004 12972 ?       S    Nov14   0:03 /usr/sbin/slapd -
u ldap
```

or

```
[root@PDC-SRV root]# netstat -tan | grep LISTEN | grep 389
tcp        0      0 0.0.0.0:389             0.0.0.0:*               LISTEN
```

12.2 Creating an user account

With samba3, cou can create user accounts with Microsoft Windows NT Domain management tools (launch `usrmgr.exe` in a msdos console). You can of course also use the smbldap-tools (or any other LDAP manipulation tools). To do so, see section 8.1. If interested in a graphical user interface to manager user and group accounts, please have a look on the idxldapaccounts Webmin module available at http://webmin.idealx.org/

To test:

- create an user account for 'testsmbuser' (8.1.2)
- verify this user account is ok :

```
$id testsmbuser
```

should return something like that:

```
[root@speed3 samba]# id testsmbuser
uid=1008(testsmbuser) gid=100(users) groups=100(users),501(Domain Users)
```

- additionnaly, if you're using an ldapbrowser, you should see the new uid=testsmbuser,ou=Users,dc=IDEALX,dc=org in the directory.

12.3 Logging in the domain as testsmbuser

You need to use an already Domain added workstation to proceed this test. This is previously explained is section 10.2.1 or 10.2.2.

Call the Winlogon (CTRL-ALT-SUPPR), and enter:

- Login : testsmbuser
- Password : coucou[16]
- Domain : IDEALX-NT

You should then log on fine. When you log in the domain with your username testsmbuser, verify that those differents points are ok:

- browse your personal folder and all shared folders, and read a file
- create a new file in your home directory, verify that you can save it
- verify that all permissions seems right: you can't browse a directory you don't have the permissions to, you can't edit or/ and modify a file you don't have permissions to.

13 Performance and real life considerations

Now we've detail how to set up your brand new PDC-Killer prototype, we're ready to go further: the real life, the one where users don't care about looking for solutions to a given problem, but will first consider they've got one and you're the guilty :-)

To struggle in this pleasant world, you should have a look on the following considerations : they may help you.

First, if this HOWTO was your fist approach with Samba and OpenLDAP, you should have a look on:

- a very good OpenLDAP brief by Adam Williams available at `ftp://kalamazoolinux.org/pub/pdf/ldapv3.pdf`: an excellent presentation/briefing on OpenLDAP on the *Linux* Platform.
- the OpenLDAP project website,
- the Samba project website,
- numerous documentation (printed or not) done on these two topics (Teach Yourself Samba in 24 hours for example).

13.1 Lower Log Level in production

When everything is okay with you configuration, you are **strongly encouraged** to lower log levels for better performance.

Best practices are to activate debuging logs only when you want to investigate a potential problem, and stay with low log level (or no log at all if you're seeking maximum performance) during exploitation time (most of the time as Samba really a robust implementation, thank's to the Samba Team).

Here's is an example of a standard exploitation mode log management parameters for a Samba server :

```
log file = /var/log/samba/%m.log
log level = 0
max log size = 5000
```

13.2 OpenLDAP tunning

You should consider indices on your directory server. For OpenLDAP, the following should be ok for a PDC like the one we described in this HOWTO :

```
# index
index       objectClass,uidNumber,gidNumber                    eq
index       cn,sn,uid,displayName                              pres,sub,eq
index       memberUid,mail,givenname                    eq,subinitial
index       sambaSID,sambaPrimaryGroupSID,sambaDomainName    eq
```

Of course, indices depends on you directory usage. Consult the OpenLDAP documentation for more info.

Have a look on the following slapd.conf directives too:

- loglevel: lower to '0' for production purpose
- lastmod: set it to 'off' if you really don't need it
- cachesize: set a confortable cache size (say 1000 for a mid-level production site for 1000 users),
- dbcachesize: set a confortable db cache size (say 10000 for a mid-level production site for 1000 users)
- dbnosync: in case you're fool enough to think nothing will never crash :-)

13.3 Start NSCD

Start the nscd server : `/etc/init.d/nscd start`

14 Heavy loads and high availability

TODO: indicate some load params, and present a redundant and HA solution.

TODO: describe test-plateform.

14.1 OpenLDAP Load

As we're storing users and groups in a LDAP directory, we will have a closer look on the OpenLDAP capacity to store numerous account, and systems (Samba and pam_ldap) to interact with this LDAP database.

For testing purpose, we're going to test bind/read/write operations on LDAP, with a population of 50.000 users, 50.000 computers. and 1000 groups.

14.2 Samba Load

As we're storing the SAM database in a LDAP directory, we will have a closer look on the Samba-LDAP capacity to interact under heavy stress.

For testing purpose, we're going to compare Samba with and without the LDAP stored SAM.

We'll have to show stress test results (smbtorture?) using 20, 50, 100, 150 and 200 clients.

14.3 High Availability

TODO: Present an HA configuration: what to do, how to do it (using Kimberlite/Mon or Hearbeat/Mon).

15 Frequently Asked Questions

15.1 User/Group/Profile management

15.1.1 Is there a way to manage users and group *via* a graphical interface?

If interested in a Graphical User Interface to manage user and groups, have a look on the idxldapaccounts Webmin module. You'll find this module at http://webmin.IDEALX.org/.

15.1.2 my profiles are not saved on the server

Make sure that the profile directory on the server has the right permissions. You must do a `chmod 1757 /opt/samba/profiles` for example.

Additionaly, you may want to use the *group = +<groupname>*, *create mask* and related options.

Note that Windows 2000 check for the profile's owner which may fail if ACL are not supported. Try then to add `nt acl support = yes` in profile section.

15.2 Joining domain

15.2.1 I can't join a Microsoft Windows NT 4 to the domain on the fly:

There's two solutions :

- try adding it manually, using the script *smbldap-useradd* (you must be root on the PDC server). If your machine's name is VMNT, then the command line is:

  ```
  smbldap-useradd -w VMNT$
  pdbedit -a -m -u VMNT$
  ```

  Then, try again to join the NT4 server to the domain
- for NT4, server's account belong to the Domain User group. Try to use the 513 number for computer's account: in smbldap.conf, set the following parameter:

  ```
  defaultComputerGid="513"
  ```

15.2.2 I can't join the domain

many reason can cause this problem. verify the following points:

- in the samba configuration file (smb.conf), put the *interface* parameter to the interface which is listening the network on. We originally put "interfaces = 192.168.2.0/24 127.0.0.1/32" which caused the "can't join the domain" problem.
- if you found this error message in samba's log: `Error: modifications require authentication at /opt/IDEALX/sbin//smbldap_tools.pm line 1008`, this certainly mean that you haven't set correctly priviledge for machine account. See chapter 10.1

15.2.3 I deleted my computer from the domain, and I can't connect to it anymore

When you leave the domain IDEALX-NT, you have to reboot your machine (workstation). If you don't, you will not be able to join any more the domain (because of the workstation embeded cache).

If you done this and it still doesn't work, remove the machine's account from the OpenLDAP directory and recreate it. For this, use the command `smbldap-userdel myworstation-nebiosname$` .

16 Thanks

This document is a collective work which aims at:

- quickly discover the LDAP PDC functionnalities of Samba branch 3,
- quickly have a working configuration to help you discover this kind of Samba configuration,

This Howto is an updated document of the Samba2 Howto initiated by Olivier Lemaire. Peoples who directly worked on the last release are :

- Olivier Lemaire,
- David Le Corfec,
- Jérôme Tournier (jtournier@IDEALX.com),
- Michael Weisbach (mwei@tuts.nu),
- Stefan Schleifer (stefan.schleifer@linbit.com).

The author would like to thank the following people for providing help with some of the more complicated subjects, for clarifying some of the internal workings of Samba or OpenLDAP, for pointing out errors or mistakes in previous versions of this document, or generally for making suggestions (in alphabetical order):

- Gerald Carter (jerry@samba.org),
- Ignacio Coupeau (icoupeau@unav.es),
- Michael Cunningham (archive@xpedite.com),
- Adam Williams (awilliam@whitemice.org),
- Some people on **irc.openproject.org #samba-technical**
- Samba and Samba-TNG Teams of course !

17 Annexes

Here you'll find some sample documentations and config files, used in this HOWTO.

17.1 Configuration files

17.1.1 OpenLDAP

The OpenLDAP configuration file : `/etc/openldap/slapd.conf`

```
include  /etc/openldap/schema/core.schema
include  /etc/openldap/schema/cosine.schema
include  /etc/openldap/schema/inetorgperson.schema
include  /etc/openldap/schema/nis.schema
include  /etc/openldap/schema/samba.schema

schemacheck on

TLSCertificateFile /etc/openldap/ldap.idealx.com.pem
TLSCertificateKeyFile /etc/openldap/ldap.idealx.com.key
TLSCACertificateFile /etc/openldap/ca.pem
TLSCipherSuite :SSLv3
#TLSVerifyClient demand

########################################################################
# bdb database definitions
########################################################################
database bdb
suffix  dc=idealx,dc=org
rootdn  "cn=Manager,dc=idealx,dc=org"
rootpw  secret
directory /var/lib/ldap
lastmod  on
index      objectClass,uidNumber,gidNumber                  eq
index      cn,sn,uid,displayName                            pres,sub,eq
index      memberUid,mail,givenname                 eq,subinitial
index      sambaSID,sambaPrimaryGroupSID,sambaDomainName    eq

# users can authenticate and change their password
access to attrs=userPassword,sambaNTPassword,sambaLMPassword
      by self write
```

```
      by anonymous auth
      by * none
# all others attributes are readable to everybody
access to *
      by * read
```

The `/etc/openldap/schema/samba.schema` file

The Samba schema is shipped with Samba-3.0.2 source code (in example/LDAP/).

```
##
## schema file for OpenLDAP 2.x
## Schema for storing Samba user accounts and group maps in LDAP
## OIDs are owned by the Samba Team
##
## Prerequisite schemas - uid         (cosine.schema)
##                      - displayName (inetorgperson.schema)
##                      - gidNumber   (nis.schema)
##
## 1.3.6.1.4.1.7165.2.1.x - attributetypes
## 1.3.6.1.4.1.7165.2.2.x - objectclasses
##

################################################################################
##                                HISTORICAL                                  ##
################################################################################

##
## Password hashes
##
#attributetype ( 1.3.6.1.4.1.7165.2.1.1 NAME 'lmPassword'
# DESC 'LanManager Passwd'
# EQUALITY caseIgnoreIA5Match
# SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{32} SINGLE-VALUE )

#attributetype ( 1.3.6.1.4.1.7165.2.1.2 NAME 'ntPassword'
# DESC 'NT Passwd'
# EQUALITY caseIgnoreIA5Match
# SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{32} SINGLE-VALUE )

##
## Account flags in string format ([UWDX     ])
##
#attributetype ( 1.3.6.1.4.1.7165.2.1.4 NAME 'acctFlags'
# DESC 'Account Flags'
# EQUALITY caseIgnoreIA5Match
# SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{16} SINGLE-VALUE )

##
## Password timestamps & policies
##
#attributetype ( 1.3.6.1.4.1.7165.2.1.3 NAME 'pwdLastSet'
# DESC 'NT pwdLastSet'
# EQUALITY integerMatch
# SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )

#attributetype ( 1.3.6.1.4.1.7165.2.1.5 NAME 'logonTime'
# DESC 'NT logonTime'
# EQUALITY integerMatch
# SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
```

```
#attributetype ( 1.3.6.1.4.1.7165.2.1.6 NAME 'logoffTime'
# DESC 'NT logoffTime'
# EQUALITY integerMatch
# SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )

#attributetype ( 1.3.6.1.4.1.7165.2.1.7 NAME 'kickoffTime'
# DESC 'NT kickoffTime'
# EQUALITY integerMatch
# SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )

#attributetype ( 1.3.6.1.4.1.7165.2.1.8 NAME 'pwdCanChange'
# DESC 'NT pwdCanChange'
# EQUALITY integerMatch
# SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )

#attributetype ( 1.3.6.1.4.1.7165.2.1.9 NAME 'pwdMustChange'
# DESC 'NT pwdMustChange'
# EQUALITY integerMatch
# SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )

##
## string settings
##
#attributetype ( 1.3.6.1.4.1.7165.2.1.10 NAME 'homeDrive'
# DESC 'NT homeDrive'
# EQUALITY caseIgnoreIA5Match
# SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{4} SINGLE-VALUE )

#attributetype ( 1.3.6.1.4.1.7165.2.1.11 NAME 'scriptPath'
# DESC 'NT scriptPath'
# EQUALITY caseIgnoreIA5Match
# SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{255} SINGLE-VALUE )

#attributetype ( 1.3.6.1.4.1.7165.2.1.12 NAME 'profilePath'
# DESC 'NT profilePath'
# EQUALITY caseIgnoreIA5Match
# SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{255} SINGLE-VALUE )

#attributetype ( 1.3.6.1.4.1.7165.2.1.13 NAME 'userWorkstations'
# DESC 'userWorkstations'
# EQUALITY caseIgnoreIA5Match
# SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{255} SINGLE-VALUE )

#attributetype ( 1.3.6.1.4.1.7165.2.1.17 NAME 'smbHome'
# DESC 'smbHome'
# EQUALITY caseIgnoreIA5Match
# SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{128} )

#attributetype ( 1.3.6.1.4.1.7165.2.1.18 NAME 'domain'
# DESC 'Windows NT domain to which the user belongs'
# EQUALITY caseIgnoreIA5Match
# SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{128} )

##
## user and group RID
##
#attributetype ( 1.3.6.1.4.1.7165.2.1.14 NAME 'rid'
# DESC 'NT rid'
# EQUALITY integerMatch
# SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
```

```
#attributetype ( 1.3.6.1.4.1.7165.2.1.15 NAME 'primaryGroupID'
# DESC 'NT Group RID'
# EQUALITY integerMatch
# SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )

##
## The smbPasswordEntry objectclass has been depreciated in favor of the
## sambaAccount objectclass
##
#objectclass ( 1.3.6.1.4.1.7165.2.2.1 NAME 'smbPasswordEntry' SUP top AUXILIARY
#        DESC 'Samba smbpasswd entry'
#        MUST ( uid $ uidNumber )
#        MAY  ( lmPassword $ ntPassword $ pwdLastSet $ acctFlags ))

#objectclass ( 1.3.6.1.4.1.7165.2.2.2 NAME 'sambaAccount' SUP top STRUCTURAL
# DESC 'Samba Account'
# MUST ( uid $ rid )
# MAY  ( cn $ lmPassword $ ntPassword $ pwdLastSet $ logonTime $
#               logoffTime $ kickoffTime $ pwdCanChange $ pwdMustChange $ acctFlags $
#               displayName $ smbHome $ homeDrive $ scriptPath $ profilePath $
#               description $ userWorkstations $ primaryGroupID $ domain ))

#objectclass ( 1.3.6.1.4.1.7165.2.2.3 NAME 'sambaAccount' SUP top AUXILIARY
# DESC 'Samba Auxiliary Account'
# MUST ( uid $ rid )
# MAY  ( cn $ lmPassword $ ntPassword $ pwdLastSet $ logonTime $
#              logoffTime $ kickoffTime $ pwdCanChange $ pwdMustChange $ acctFlags $
#              displayName $ smbHome $ homeDrive $ scriptPath $ profilePath $
#              description $ userWorkstations $ primaryGroupID $ domain ))

########################################################################
##                        END OF HISTORICAL                           ##
########################################################################

########################################################################
##                Attributes used by Samba 3.0 schema                 ##
########################################################################

##
## Password hashes
##
attributetype ( 1.3.6.1.4.1.7165.2.1.24 NAME 'sambaLMPassword'
 DESC 'LanManager Password'
 EQUALITY caseIgnoreIA5Match
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{32} SINGLE-VALUE )

attributetype ( 1.3.6.1.4.1.7165.2.1.25 NAME 'sambaNTPassword'
 DESC 'MD4 hash of the unicode password'
 EQUALITY caseIgnoreIA5Match
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{32} SINGLE-VALUE )

##
## Account flags in string format ([UWDX     ])
##
attributetype ( 1.3.6.1.4.1.7165.2.1.26 NAME 'sambaAcctFlags'
 DESC 'Account Flags'
 EQUALITY caseIgnoreIA5Match
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{16} SINGLE-VALUE )

##
```

```
## Password timestamps & policies
##
attributetype ( 1.3.6.1.4.1.7165.2.1.27 NAME 'sambaPwdLastSet'
 DESC 'Timestamp of the last password update'
 EQUALITY integerMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )

attributetype ( 1.3.6.1.4.1.7165.2.1.28 NAME 'sambaPwdCanChange'
 DESC 'Timestamp of when the user is allowed to update the password'
 EQUALITY integerMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )

attributetype ( 1.3.6.1.4.1.7165.2.1.29 NAME 'sambaPwdMustChange'
 DESC 'Timestamp of when the password will expire'
 EQUALITY integerMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )

attributetype ( 1.3.6.1.4.1.7165.2.1.30 NAME 'sambaLogonTime'
 DESC 'Timestamp of last logon'
 EQUALITY integerMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )

attributetype ( 1.3.6.1.4.1.7165.2.1.31 NAME 'sambaLogoffTime'
 DESC 'Timestamp of last logoff'
 EQUALITY integerMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )

attributetype ( 1.3.6.1.4.1.7165.2.1.32 NAME 'sambaKickoffTime'
 DESC 'Timestamp of when the user will be logged off automatically'
 EQUALITY integerMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )


##
## string settings
##
attributetype ( 1.3.6.1.4.1.7165.2.1.33 NAME 'sambaHomeDrive'
 DESC 'Driver letter of home directory mapping'
 EQUALITY caseIgnoreIA5Match
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{4} SINGLE-VALUE )

attributetype ( 1.3.6.1.4.1.7165.2.1.34 NAME 'sambaLogonScript'
 DESC 'Logon script path'
 EQUALITY caseIgnoreMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{255} SINGLE-VALUE )

attributetype ( 1.3.6.1.4.1.7165.2.1.35 NAME 'sambaProfilePath'
 DESC 'Roaming profile path'
 EQUALITY caseIgnoreMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{255} SINGLE-VALUE )

attributetype ( 1.3.6.1.4.1.7165.2.1.36 NAME 'sambaUserWorkstations'
 DESC 'List of user workstations the user is allowed to logon to'
 EQUALITY caseIgnoreMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{255} SINGLE-VALUE )

attributetype ( 1.3.6.1.4.1.7165.2.1.37 NAME 'sambaHomePath'
 DESC 'Home directory UNC path'
 EQUALITY caseIgnoreMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{128} )
```

```
attributetype ( 1.3.6.1.4.1.7165.2.1.38 NAME 'sambaDomainName'
 DESC 'Windows NT domain to which the user belongs'
 EQUALITY caseIgnoreMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{128} )

##
## SID, of any type
##

attributetype ( 1.3.6.1.4.1.7165.2.1.20 NAME 'sambaSID'
 DESC 'Security ID'
 EQUALITY caseIgnoreIA5Match
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{64} SINGLE-VALUE )


##
## Primary group SID, compatible with ntSid
##

attributetype ( 1.3.6.1.4.1.7165.2.1.23 NAME 'sambaPrimaryGroupSID'
 DESC 'Primary Group Security ID'
 EQUALITY caseIgnoreIA5Match
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{64} SINGLE-VALUE )

##
## group mapping attributes
##
attributetype ( 1.3.6.1.4.1.7165.2.1.19 NAME 'sambaGroupType'
 DESC 'NT Group Type'
 EQUALITY integerMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )

##
## Store info on the domain
##

attributetype ( 1.3.6.1.4.1.7165.2.1.21 NAME 'sambaNextUserRid'
 DESC 'Next NT rid to give our for users'
 EQUALITY integerMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )

attributetype ( 1.3.6.1.4.1.7165.2.1.22 NAME 'sambaNextGroupRid'
 DESC 'Next NT rid to give out for groups'
 EQUALITY integerMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )

attributetype ( 1.3.6.1.4.1.7165.2.1.39 NAME 'sambaNextRid'
 DESC 'Next NT rid to give out for anything'
 EQUALITY integerMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )

attributetype ( 1.3.6.1.4.1.7165.2.1.40 NAME 'sambaAlgorithmicRidBase'
 DESC 'Base at which the samba RID generation algorithm should operate'
 EQUALITY integerMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )


########################################################################
##              objectClasses used by Samba 3.0 schema                ##
########################################################################
```

```
## The X.500 data model (and therefore LDAPv3) says that each entry can
## only have one structural objectclass.  OpenLDAP 2.0 does not enforce
## this currently but will in v2.1

##
## added new objectclass (and OID) for 3.0 to help us deal with backwards
## compatibility with 2.2 installations (e.g. ldapsam_compat)  --jerry
##
objectclass ( 1.3.6.1.4.1.7165.2.2.6 NAME 'sambaSamAccount' SUP top AUXILIARY
 DESC 'Samba 3.0 Auxilary SAM Account'
 MUST ( uid $ sambaSID )
 MAY  ( cn $ sambaLMPassword $ sambaNTPassword $ sambaPwdLastSet $
        sambaLogonTime $ sambaLogoffTime $ sambaKickoffTime $
        sambaPwdCanChange $ sambaPwdMustChange $ sambaAcctFlags $
               displayName $ sambaHomePath $ sambaHomeDrive $ sambaLogonScript $
        sambaProfilePath $ description $ sambaUserWorkstations $
        sambaPrimaryGroupSID $ sambaDomainName ))

##
## Group mapping info
##
objectclass ( 1.3.6.1.4.1.7165.2.2.4 NAME 'sambaGroupMapping' SUP top AUXILIARY
 DESC 'Samba Group Mapping'
 MUST ( gidNumber $ sambaSID $ sambaGroupType )
 MAY  ( displayName $ description ))

##
## Whole-of-domain info
##
objectclass ( 1.3.6.1.4.1.7165.2.2.5 NAME 'sambaDomain' SUP top STRUCTURAL
 DESC 'Samba Domain Information'
 MUST ( sambaDomainName $
        sambaSID )
 MAY ( sambaNextRid $ sambaNextGroupRid $ sambaNextUserRid $
       sambaAlgorithmicRidBase ) )

## used for idmap_ldap module
objectclass ( 1.3.6.1.4.1.7165.1.2.2.7 NAME 'sambaUnixIdPool' SUP top AUXILIARY
        DESC 'Pool for allocating UNIX uids/gids'
        MUST ( uidNumber $ gidNumber ) )


objectclass ( 1.3.6.1.4.1.7165.1.2.2.8 NAME 'sambaIdmapEntry' SUP top AUXILIARY
        DESC 'Mapping from a SID to an ID'
        MUST ( sambaSID )
 MAY ( uidNumber $ gidNumber ) )

objectclass ( 1.3.6.1.4.1.7165.1.2.2.9 NAME 'sambaSidEntry' SUP top STRUCTURAL
        DESC 'Structural Class for a SID'
        MUST ( sambaSID ) )
```

17.1.2 smbldap-tools

The *`/etc/opt/IDEALX/smbldap-tools/smbldap.conf`* file

```
# $Source: /opt/cvs/samba/samba-ldap-howto/config/smbldap.conf,v $
# $Id: smbldap.conf,v 1.5 2005/10/31 15:32:57 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-1-5-21-4205727931-4131263253-1851132061"

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

##############################################################################
#
# 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=""

# certificate to use to connect to the ldap server
# see "man Net::LDAP" in start_tls section for more details
clientcert=""

# key certificate to use to connect to the ldap server
# see "man Net::LDAP" in start_tls section for more details
clientkey=""

# LDAP Suffix
# Ex: suffix=dc=IDEALX,dc=ORG
suffix="dc=idealx,dc=org"

# 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,${suffix}"
sambaUnixIdPooldn="sambaDomainName=IDEALX-NT,${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="/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="\\PDC-SRV\%U"

# 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"

# 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="idealx.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"
```

The *`/etc/opt/IDEALX/smbldap-tools/smbldap_bind.conf`* file

```
############################
# 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=Manager,dc=idealx,dc=org"
slavePw="secret"
masterDN="cn=Manager,dc=idealx,dc=org"
masterPw="secret"
```

17.1.3 Samba

The samba configuration file : `/etc/samba/smb.conf`

```
# Global parameters
[global]
        workgroup = IDEALX-NT
        netbios name = PDC-SRV
 enable privileges = yes
        interfaces = 192.168.5.11
        username map = /etc/samba/smbusers
        server string = Samba Server %v
        security = user
        encrypt passwords = Yes
        min passwd length = 3
        obey pam restrictions = No
        #unix password sync = Yes
        #passwd program = /usr/local/sbin/smbldap-passwd -u %u
 #passwd chat = "Changing password for*\nNew password*" %n\n "*Retype new password*"
%n\n"
        ldap passwd sync = Yes
        log level = 0
        syslog = 0
        log file = /var/log/samba/log.%m
        max log size = 100000
        time server = Yes
        socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
        mangling method = hash2
        Dos charset = 850
        Unix charset = ISO8859-1

        logon script = logon.bat
        logon drive = H:
        logon home =
        logon path =

        domain logons = Yes
        os level = 65
        preferred master = Yes
        domain master = Yes
        wins support = Yes
        passdb backend = ldapsam:ldap://127.0.0.1/
        # passdb backend = ldapsam:"ldap://127.0.0.1/ ldap://slave.idealx.com"
 # ldap filter = (&(objectclass=sambaSamAccount)(uid=%u))
        ldap admin dn = cn=samba,ou=Users,dc=idealx,dc=org
        ldap suffix = dc=idealx,dc=org
        ldap group suffix = ou=Groups
        ldap user suffix = ou=Users
        ldap machine suffix = ou=Computers
        ldap idmap suffix = ou=Users
        ldap ssl = start tls
        add user script = /usr/local/sbin/smbldap-useradd -m "%u"
        ldap delete dn = Yes
        #delete user script = /usr/local/sbin/smbldap-userdel "%u"
        add machine script = /usr/local/sbin/smbldap-useradd -w "%u"
        add group script = /usr/local/sbin/smbldap-groupadd -p "%g"
        #delete group script = /usr/local/sbin/smbldap-groupdel "%g"
        add user to group script = /usr/local/sbin/smbldap-groupmod -m "%u" "%g"
        delete user from group script = /usr/local/sbin/smbldap-groupmod -x "%u" "%g"
```

```
        set primary group script = /usr/local/sbin/smbldap-usermod -g "%g" "%u"

        # printers configuration
        printer admin = @"Print Operators"
        load printers = Yes
        create mask = 0640
        directory mask = 0750
        nt acl support = No
        printing = cups
        printcap name = cups
        deadtime = 10
        guest account = nobody
        map to guest = Bad User
        dont descend = /proc,/dev,/etc,/lib,/lost+found,/initrd
        show add printer wizard = yes
        ; to maintain capital letters in shortcuts in any of the profile folders:
        preserve case = yes
        short preserve case = yes
        case sensitive = no

[homes]
        comment = repertoire de %U, %u
        read only = No
        create mask = 0644
        directory mask = 0775
        browseable = No

[netlogon]
        path = /home/samba/netlogon/
 browseable = No
        read only = yes

[profiles]
        path = /home/samba/profiles
        read only = no
        create mask = 0600
        directory mask = 0700
        browseable = No
        guest ok = Yes
        profile acls = yes
        csc policy = disable
        # next line is a great way to secure the profiles
        force user = %U
        # next line allows administrator to access all profiles
        valid users = %U @"Domain Admins"

[printers]
        comment = Network Printers
        printer admin = @"Print Operators"
        guest ok = yes
        printable = yes
        path = /home/samba/spool/
        browseable = No
        read only  = Yes
        printable = Yes
        print command = /usr/bin/lpr -P%p -r %s
        lpq command = /usr/bin/lpq -P%p
        lprm command = /usr/bin/lprm -P%p %j

[print$]
        path = /home/samba/printers
```

```
        guest ok = No
        browseable = Yes
        read only = Yes
        valid users = @"Print Operators"
        write list = @"Print Operators"
        create mask = 0664
        directory mask = 0775

[public]
        comment = Repertoire public
        path = /home/samba/public
 browseable = Yes
        guest ok = Yes
        read only = No
        directory mask = 0775
        create mask = 0664
```

/etc/openldap/ldap.conf

17.1.4 nss_ldap & pam_ldap

/etc/ldap.conf

Here's an complete sample /etc/ldap.conf used in this smbldap-tools.

```
# Your LDAP server. Must be resolvable without using LDAP.
host 127.0.0.1

# The distinguished name of the search base.
base dc=IDEALX,dc=ORG

# The distinguished name to bind to the server with if the effective user
ID
# is root. Password must be stored in /etc/ldap.secret (mode 600)
rootbinddn cn=nssldap,ou=DSA,dc=IDEALX,dc=ORG

# RFC2307bis naming contexts
nss_base_passwd         ou=Users,dc=IDEALX,dc=ORG?one
nss_base_passwd         ou=Computers,dc=IDEALX,dc=ORG?one
nss_base_shadow         ou=Users,dc=IDEALX,dc=ORG?one
nss_base_group          ou=Groups,dc=IDEALX,dc=ORG?one

# Security options
ssl no
pam_password md5

# - The End
```

/etc/ldap.secret

Here's a sample /etc/ldap.secret used in this smbldap-tools.

```
nssldapsecretpwd
```

/etc/nsswitch.conf

Here's a complete sample /etc/nsswitch.conf use in this smbldap-tools.

```
#
# /etc/nsswitch.conf
#
# An example Name Service Switch config file. This file should be
# sorted with the most-used services at the beginning.
#
# The entry '[NOTFOUND=return]' means that the search for an
# entry should stop if the search in the previous entry turned
# up nothing. Note that if the search failed due to some other reason
# (like no NIS server responding) then the search continues with the
# next entry.
#
# Legal entries are:
#
# nisplus or nis+  Use NIS+ (NIS version 3)
# nis or yp  Use NIS (NIS version 2), also called YP
# dns   Use DNS (Domain Name Service)
# files   Use the local files
# db   Use the local database (.db) files
# compat   Use NIS on compat mode
# hesiod   Use Hesiod for user lookups
# [NOTFOUND=return] Stop searching if not found so far
#

# To use db, put the "db" in front of "files" for entries you want to be
# looked up first in the databases
#
# Example:

passwd:     files ldap
shadow:     files ldap
group:      files ldap

hosts:      files dns

# Example - obey only what nisplus tells us...
#services:   nisplus [NOTFOUND=return] files
#networks:   nisplus [NOTFOUND=return] files
#protocols:  nisplus [NOTFOUND=return] files
#rpc:        nisplus [NOTFOUND=return] files
#ethers:     nisplus [NOTFOUND=return] files
#netmasks:   nisplus [NOTFOUND=return] files

bootparams: nisplus [NOTFOUND=return] files

ethers:     files
netmasks:   files
networks:   files
protocols:  files
rpc:        files
services:   files

netgroup:   files

publickey:  nisplus

automount:  files
aliases:    files nisplus
```

17.2 Sample datas: smbldap-base.ldif

Here is a LDIF output of initial entries for the OpenLDAP server. Most of the groups are still not implementing in samba: that's why they are commented ;-)

```
dn: dc=idealx,dc=org
objectClass: dcObject
objectclass: organization
o: idealx
dc: idealx

dn: ou=Users,dc=idealx,dc=org
objectClass: organizationalUnit
ou: Users

dn: ou=Groups,dc=idealx,dc=org
objectClass: organizationalUnit
ou: Groups

dn: ou=Computers,dc=idealx,dc=org
objectClass: organizationalUnit
ou: Computers
dn: uid=Administrator,ou=Users,dc=idealx,dc=org
cn: Administrator
sn: Administrator
objectClass: inetOrgPerson
objectClass: sambaSAMAccount
objectClass: posixAccount
objectClass: shadowAccount
gidNumber: 512
uid: Administrator
uidNumber: 0
homeDirectory: /home/%U
sambaPwdLastSet: 0
sambaLogonTime: 0
sambaLogoffTime: 2147483647
sambaKickoffTime: 2147483647
sambaPwdCanChange: 0
sambaPwdMustChange: 2147483647
sambaHomePath: \\PDC-SMB3\home\%U
sambaHomeDrive: H:
sambaProfilePath: \\PDC-SMB3\profiles\%U\Administrator
sambaPrimaryGroupSID: S-1-5-21-4231626423-2410014848-2360679739-512
sambaLMPassword: XXX
sambaNTPassword: XXX
sambaAcctFlags: [U          ]
sambaSID: S-1-5-21-4231626423-2410014848-2360679739-2996
loginShell: /bin/false
gecos: Netbios Domain Administrator

dn: uid=nobody,ou=Users,dc=idealx,dc=org
cn: nobody
sn: nobody
objectClass: inetOrgPerson
objectClass: sambaSAMAccount
objectClass: posixAccount
objectClass: shadowAccount
gidNumber: 514
uid: nobody
uidNumber: 999
```

```
homeDirectory: /dev/null
sambaPwdLastSet: 0
sambaLogonTime: 0
sambaLogoffTime: 2147483647
sambaKickoffTime: 2147483647
sambaPwdCanChange: 0
sambaPwdMustChange: 2147483647
sambaHomePath: \\PDC-SMB3\home\%U
sambaHomeDrive: H:
sambaProfilePath: \\PDC-SMB3\profiles\%U\nobody
sambaPrimaryGroupSID: S-1-5-21-4231626423-2410014848-2360679739-514
sambaLMPassword: NO PASSWORDXXXXXXXXXXXXXXXXXXXX
sambaNTPassword: NO PASSWORDXXXXXXXXXXXXXXXXXXXX
sambaAcctFlags: [NU         ]
sambaSID: S-1-5-21-4231626423-2410014848-2360679739-2998
loginShell: /bin/false

dn: cn=Domain Admins,ou=Groups,dc=idealx,dc=org
objectClass: posixGroup
objectClass: sambaGroupMapping
gidNumber: 512
cn: Domain Admins
memberUid: Administrator
description: Netbios Domain Administrators
sambaSID: S-1-5-21-4231626423-2410014848-2360679739-512
sambaGroupType: 2
displayName: Domain Admins

dn: cn=Domain Users,ou=Groups,dc=idealx,dc=org
objectClass: posixGroup
objectClass: sambaGroupMapping
gidNumber: 513
cn: Domain Users
description: Netbios Domain Users
sambaSID: S-1-5-21-4231626423-2410014848-2360679739-513
sambaGroupType: 2
displayName: Domain Users

dn: cn=Domain Guests,ou=Groups,dc=idealx,dc=org
objectClass: posixGroup
objectClass: sambaGroupMapping
gidNumber: 514
cn: Domain Guests
description: Netbios Domain Guests Users
sambaSID: S-1-5-21-4231626423-2410014848-2360679739-514
sambaGroupType: 2
displayName: Domain Guests

dn: cn=Print Operators,ou=Groups,dc=idealx,dc=org
objectClass: posixGroup
objectClass: sambaGroupMapping
gidNumber: 550
cn: Print Operators
description: Netbios Domain Print Operators
sambaSID: S-1-5-21-4231626423-2410014848-2360679739-550
sambaGroupType: 2
displayName: Print Operators

dn: cn=Backup Operators,ou=Groups,dc=idealx,dc=org
objectClass: posixGroup
objectClass: sambaGroupMapping
```

```
gidNumber: 551
cn: Backup Operators
description: Netbios Domain Members can bypass file security to back up files
sambaSID: S-1-5-21-4231626423-2410014848-2360679739-551
sambaGroupType: 2
displayName: Backup Operators

dn: cn=Replicator,ou=Groups,dc=idealx,dc=org
objectClass: posixGroup
objectClass: sambaGroupMapping
gidNumber: 552
cn: Replicator
description: Netbios Domain Supports file replication in a sambaDomainName
sambaSID: S-1-5-21-4231626423-2410014848-2360679739-552
sambaGroupType: 2
displayName: Replicator

dn: cn=Domain Computers,ou=Groups,dc=idealx,dc=org
objectClass: posixGroup
objectClass: sambaGroupMapping
gidNumber: 553
cn: Domain Computers
description: Netbios Domain Computers accounts
sambaSID: S-1-5-21-4231626423-2410014848-2360679739-553
sambaGroupType: 2
displayName: Domain Computers

#dn: cn=Administrators,ou=Groups,dc=idealx,dc=org
#objectClass: posixGroup
#objectClass: sambaGroupMapping
#gidNumber: 544
#cn: Administrators
#description: Netbios Domain Members can fully administer the computer/
sambaDomainName
#sambaSID: S-1-5-21-4231626423-2410014848-2360679739-544
#sambaGroupType: 2
#displayName: Administrators

#dn: cn=Users,ou=Groups,dc=idealx,dc=org
#objectClass: posixGroup
#objectClass: sambaGroupMapping
#gidNumber: 545
#cn: Users
#description: Netbios Domain Ordinary users
#sambaSID: S-1-5-21-4231626423-2410014848-2360679739-545
#sambaGroupType: 2
#displayName: users

#dn: cn=Guests,ou=Groups,dc=idealx,dc=org
#objectClass: posixGroup
#objectClass: sambaGroupMapping
#gidNumber: 546
#cn: Guests
#memberUid: nobody
#description: Netbios Domain Users granted guest access to the computer/
sambaDomainName
#sambaSID: S-1-5-21-4231626423-2410014848-2360679739-546
#sambaGroupType: 2
#displayName: Guests

#dn: cn=Power Users,ou=Groups,dc=idealx,dc=org
```

```
#objectClass: posixGroup
#objectClass: sambaGroupMapping
#gidNumber: 547
#cn: Power Users
#description: Netbios Domain Members can share directories and printers
#sambaSID: S-1-5-21-4231626423-2410014848-2360679739-547
#sambaGroupType: 2
#displayName: Power Users

#dn: cn=Account Operators,ou=Groups,dc=idealx,dc=org
#objectClass: posixGroup
#objectClass: sambaGroupMapping
#gidNumber: 548
#cn: Account Operators
#description: Netbios Domain Users to manipulate users accounts
#sambaSID: S-1-5-21-4231626423-2410014848-2360679739-548
#sambaGroupType: 2
#displayName: Account Operators

#dn: cn=Server Operators,ou=Groups,dc=idealx,dc=org
#objectClass: posixGroup
#objectClass: sambaGroupMapping
#gidNumber: 549
#cn: Server Operators
#description: Netbios Domain Server Operators
#sambaSID: S-1-5-21-4231626423-2410014848-2360679739-549
#sambaGroupType: 2
#displayName: Server Operators
```

17.3 DSA accounts: smbldap-dsa.ldif

Here is a LDIF output of DSA accounts that may be used for administrative purpose.

```
dn: ou=DSA,dc=IDEALX,dc=ORG
objectClass: top
objectClass: organizationalUnit
ou: DSA
description: security accounts for LDAP clients

dn: cn=samba,ou=DSA,dc=IDEALX,dc=ORG
objectclass: organizationalRole
objectClass: top
objectClass: simpleSecurityObject
userPassword: sambasecretpwd
cn: samba

dn: cn=nssldap,ou=DSA,dc=IDEALX,dc=ORG
objectclass: organizationalRole
objectClass: top
objectClass: simpleSecurityObject
userPassword: nssldapsecretpwd
cn: nssldap

dn: cn=smbldap-tools,ou=DSA,dc=IDEALX,dc=ORG
objectclass: organizationalRole
objectClass: top
objectClass: simpleSecurityObject
userPassword: smbldapsecretpwd
cn: smbldap-tools
```

17.4 Implementation details

17.4.1 RedHat packages

TODO: present spec files for redhat packages we've made.

OpenLDAP

TODO: describe quicly what's new with this package, and present the spec file.

Samba

TODO: describe quickly what's new with this package, and present the spec file.

17.4.2 Samba-OpenLDAP on Debian Woody

The standard Samba Debian package is compiled with PAM Support. So you have to get the samba source and recompile it yourself.

For this howto, I used Samba version 2.2.4-1:

```
# apt-get source samba
```

Then, in the samba-2.2.4/debian edit the following files:

- rules: get rid of any pam compile options. I have added any missing options mentioned in this redhat howto. Also comment some files which are not created (so don't install or move them):

```
 61         [ -f source/Makefile ] || (cd source && ./configure \
 62                 --host=$(DEB_HOST_GNU_TYPE) \
 63                 --build=$(DEB_BUILD_GNU_TYPE) \
 64                 --with-fhs \
 65                 --prefix=/usr \
 66                 --sysconfdir=/etc \
 67                 --with-privatedir=/etc/samba \
 68                 --localstatedir=/var \
 69                 --with-netatalk \
 70                 --with-smbmount \
 71                 --with-syslog \
 72                 --with-sambabook \
 73                 --with-utmp \
 74                 --with-readline \
 75                 --with-libsmbclient \
 76                 --with-winbind \
 77                 --with-msdfs \
 78                 --with-automount \
 79                 --with-acl-support \
 80                 --with-profile \
 81                 --disable-static \
 82                 --with-ldapsam)


131         #install -m 0644 source/nsswitch/pam_winbind.so \
132                 #$(DESTDIR)/lib/security/

142         #mv $(DESTDIR)/usr/bin/pam_smbpass.so $(DESTDIR)/lib/security/
```

```
182         #cp debian/samba.pamd $(DESTDIR)/etc/pam.d/samba
```

- libpam-smbpass.files: get rid of the lib/security/pam_smbpass.so entry (yes the file is then empty),
- samba-common.conffiles: get rid of the /etc/pam.d/samba entry (yes the file is then empty)
- winbind.files: get rid of the lib/security/pam_winbind.so

Afterwards make a dpkg-buildpackage from the main directory level. when finished you have the .deb files ready to be installed:

```
# dpkg -i samba-common_2.2.4-1_i386.deb libsmbclient_2.2.4-1_i386.deb
samba_2.2.4-1_i386.deb smbclient_2.2.4-1_i386.deb smbfs_2.2.4-1_i386.deb
swat_2.2.4-1_i386.deb winbind_2.2.4-1_i386.deb
```

1
some special Debian notes are provided for Woody in section 17

2
DNS resolution **must** be ok to use Samba without spending hours trying to understand why that think is supposed to work and don't !

3
See http://www.pathname.com/fhs/

4
See http://www.freestandards.org/

5
remember: feel free to test under other distros and OS, and please report: we'll update this Howto

6
Thanks to Stefan Schleifer, a special Debian Woody section is available in section 17

7
binary package can be found on http://us1.samba.org/samba/ftp/Binary_Packages/RedHat/RPMS/i386/9.0/

8
consult path-to-samba-sources/examples/LDAP/smbldap-tools/

9
and additional needed schemas like core and nis for example

10
for Windows groups, both object class are needed. For unix group, the sambaGroupMapping is not needed

11
authconfig is a RedHat utility to configure you pam and nss modules

12
if you want to do this manually, a sample LDIF file presented on section 17.2 give you more details on what objects you are going to add to the OpenLDAP database. Copy/paste it on a file named smbldap-base.ldif and add it using the following command (type your admin DN password, 'mysecretpw' to complete the command when prompted): `ldapadd -x -h localhost -D "cn=Manager,dc=IDEALX,dc=ORG" -f smbldap-base.ldif -W`

13
see 8.1 for more info

14
http://samba.idealx.org and specially http://samba.idealx.org/smbldap-tools.fr.html

15
http://samba.idealx.org and specially http://samba.idealx.org/smbldap-tools.fr.html

16

in fact, the one you gave in the section : 8.1.2

This document was translated from $LaTeX$ by HEVEA.