The *Linux* Samba-OpenLDAP Howto
(*Revision* : 20060710)

Jérôme Tournier
Olivier Lemaire

Revision : 20060710

This Howto explains how to set up and maintain a *Linux* Departemental Server with Samba and OpenLDAP in order to provide central authentication services, file and print sharing for Microsoft Windows and Unix clients. It may replace an existing Microsoft Windows Domain Controler server.

The smbldap-tools package is part of the IDEALX OpenTrust software suite (http://IDEALX.com/).

Contents

Listings

1 Introduction

1.1 Softwares used

This howto currently works for:

- release 3.0.22 of Samba,
- Microsoft Windows, Microsoft Windows NT 4.0, Windows 2000 and Windows XP Workstations and Servers,
- *Linux* RedHat 9, albeit it should work with any *Linux* distribution [1]),

[1] some special Debian notes are provided for Woody in section 17 on page 49

- release 2.1.22 of OpenLDAP, albeit it should work with any other release of OpenLDAP and any good LDAP server.

1.2 Using this document

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

An archive file named samba-ldap-howto-((Version)).tar.gz, published on the project page, contains this HOWTO's sourcecode and all the configuration files listed here. Please read this HOWTO along with its sourcecode in order to cut and paste configuration files content from it.

If you find a bug in this document or if you want it 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 sake 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 works (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,

[2] DNS resolution **must** be ok to use Samba without spending hours trying to fix erratic failures)

- 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 consider RedHat/*Linux* 9 as a base and an installation of the involved softwares (Samba, OpenLDAP, smbldap-tools, ...) made through RPM packages.

Of course, this do not mean that Samba only runs on RedHat/*Linux* nor that RedHat/*Linux* is a better *Linux* distribution than Debian GNU/*Linux*. The choice of RedHat/*Linux* offers the advantage to be quickly reproductible by anybody (RedHat *Linux* is very common on the server market nowadays, and supported by many vendors). To help you install and compile the used softwares on your favorite *Linux* (or any other Operating System in fact) the section 17 on page 49 contains all .spec files used to create our specific packages.

2.3 FHS, LSB and High Availability

While installing and compiling the key softwares (Samba and OpenLDAP) we tried to keep in mind 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 that our Primary Domain Controler may be used in a Highly Available configuration (in a futur revision of this Howto).

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

3 Installation

To stick to this Howto[5] you must:

- *FedoraCorerelease*2 install and configure a platform (network and DNS included) [6],
- 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 those packages:

- OpenLDAP,
- Samba,

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

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

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

[6] Thanks to Stefan Schleifer, a special Debian Woody (Samba 2.2 source) section is available in section 17 on page 49

- nss_ldap and pam_ldap,
- smbldap-tools.

The smbldap-tools are available on the project page (http://sourceforge.net/projects/smbldap-tools), others are part of the *FedoraCorerelease*2 distribution. Only OpenLDAP was downloaded separately 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. We use the release of OpenLDAP provided with *FedoraCorerelease*2. Packages that need to be downloaded are (we state below the minimal version numbers):

- 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
```

On a Debian system please use:

```
apt-get install slapd samba samba-doc smbfs ldap-utils ldapscripts
apt-get install libnss-ldap libpam-ldap nscd
apt-get install libnet-ldap-perl libcrypt-smbhash-perl
```

One may also check Webmin (or 'phpldapadmin', 'ldap-account-manager') and 'ultraposs-sum'.

3.2 Samba 3.0.22

Samba 3.0.22 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, there is no need to compile Samba as LDAP is the default backend used with classic RedHat's Samba packages.

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

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

```
rpm -Uvh samba-3.0.22-1.i386.rpm
rpm -Uvh samba-client-3.0.22-1.i386.rpm
rpm -Uvh samba-common-3.0.12-1.i386.rpm
```

You can also use the default RedHat package.

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

3.3 smbldap-tools 0.9.2

smbldap-tools is a package containing some useful scripts to manage users/groups when you store users/groups data (for Unix and for Samba) in a directory (LDAP). In this Howto we use those scripts to add/delete/modify users and groups.

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

For this Howto, just download smbldap-tools release 0.9.2 RPM and install it:

```
rpm -Uvh smbldap-tools-0.9.2-1.i386.rpm
```

On a Debian system please use:

```
apt-get install smbldap-tools
```

smbldap-tools evolves. Read the ChangeLog in the CVS sourcetree to check for interesting enhancements. For our Howto setup we encourage you to use release 0.9.2 as they are sufficient for the limited use covered.

4 Configuration

4.1 OpenLDAP

You'll need to configure your OpenLDAP server for it to act as a SAM (Security Account Manager, a database storing user profiles).

Following our example, we must configure it to:

- accept the Samba 3.0.22 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 (Directory Information Tree):

```
(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)
```

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

[9] and additional needed schemas like core and nis for example

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 (see 5 on page 21).

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 in order to comply with RFC 2307bis, and because we think it's clearer for human comprehension this way.

Using Samba 3.0.22 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.

Under Debian many schemas templates are in file/usr/share/doc/samba-doc/examples/LDAP/.

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, check that your /etc/openldap/slapd.conf includes this line (or the equivalent form):

Listing 1: config/slapd.schema

```
1 include         /etc/openldap/schema/core.schema
2 include         /etc/openldap/schema/cosine.schema
3 include         /etc/openldap/schema/inetorgperson.schema
4 include         /etc/openldap/schema/nis.schema
5 include         /etc/openldap/schema/samba.schema
```

We use the inetOrgPerson to merge organizational with technical data, in order to ease administration. A user account will define:

1. a human user,
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 fits your needs better if this way is not the one you want to follow.

We use the samba.schema shipped with Samba.

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

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:

Listing 2: config/slapd.backend

```
1  database    bdb
2  directory   /var/lib/ldap
3
4  suffix      "dc=IDEALX,dc=ORG"
5  rootdn      "cn=Manager,dc=IDEALX,dc=ORG"
6
7  index       objectClass,uidNumber,gidNumber                    eq
8  index       cn,sn,uid,displayName                              pres,sub,eq
9  index       memberUid,mail,givenname                  eq,subinitial
10 index       sambaSID,sambaPrimaryGroupSID,sambaDomainName      eq
```

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

Listing 3: config/slapd.acl

```
1  access to attrs=userPassword,sambaLMPassword,sambaNTPassword
2         by self write
3         by anonymous auth
4         by * none
5  access to *
6         by * read
```

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

Listing 4: config/slapd.secret

```
1  rootpw              mysecretpwd
```

Don't forget to protect your Root DN password by setting mode 600 on file/etc/openldap/slapd.conf. You can also set a hashed password in that file: use `slappasswd` (program member of the OpenLDAP suite). 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

Listing 5: config/slapd.secret.hashed

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

4.1.3 Clients configuration

Configure default settings for LDAP clients by editing /etc/openldap/ldap.conf. Example:

Listing 6: config/openldap–ldap.conf

```
1 HOST 127.0.0.1
2 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:

- check your configuration files,
- check 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

In this section we will configure our *Linux* box to use LDAP through pam_ldap and nss_ldap.

Then, we will use nscd for a performance gain.

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): 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:

[11] authconfig is a RedHat utility to configure you PAM and nss modules

Listing 7: config/system–auth

```
1  #%PAM-1.0
2  # This file is auto-generated.
3  # User changes will be destroyed the next time authconfig is run.
4  auth        required      /lib/security/pam_env.so
5  auth        sufficient    /lib/security/pam_unix.so likeauth nullok
6  auth        sufficient    /lib/security/pam_ldap.so use_first_pass
7  auth        required      /lib/security/pam_deny.so
8
9  account     required      /lib/security/pam_unix.so
10 account     sufficient    /lib/security/pam_ldap.so
11
12 password    required      /lib/security/pam_cracklib.so retry=3 type=
13 password    sufficient    /lib/security/pam_unix.so nullok use_authtok
       md5 shadow
14 password    sufficient    /lib/security/pam_ldap.so use_authtok
15 password    required      /lib/security/pam_deny.so
16
17 session     required      /lib/security/pam_limits.so
18 session     required      /lib/security/pam_unix.so
19 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 it).

Moreover please preserve the compatibility of /etc/pam.d/system-auth with 'authconfig' by editing it, keeping a copy, then running authconfig in order to check that invoking it will not inadequately modify your setup.

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:

Listing 8: config/ldap.conf

```
1  # Your LDAP server. Must be resolvable without using LDAP.
2  host 127.0.0.1
3
4  # The distinguished name of the search base.
5  base dc=IDEALX,dc=ORG
6
```

```
7  # The distinguished name to bind to the server with if the effective user
       ID
8  # is root. Password must be stored in /etc/ldap.secret (mode 600)
9  rootbinddn cn=nssldap,ou=DSA,dc=IDEALX,dc=ORG
10
11 # RFC2307bis naming contexts
12 nss_base_passwd          ou=Users,dc=IDEALX,dc=ORG?one
13 nss_base_passwd          ou=Computers,dc=IDEALX,dc=ORG?one
14 nss_base_shadow          ou=Users,dc=IDEALX,dc=ORG?one
15 nss_base_group           ou=Groups,dc=IDEALX,dc=ORG?one
16
17 # Security options
18 ssl no
19 pam_password md5
20
21 # - 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:

Listing 9: config/ldap.secret

```
1  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:

Listing 10: config/nsswitch.conf

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

A complete sample /etc/nsswitch.conf is presented in section 17.1.4 on page 65.

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 on page 62, 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 on page 62 to configure your Samba server. Let make some remarks about this file:

The global section This section allow you to configure the server's global parameters (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 this action.

The option "add machine script" allows 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 eases the administration of machine's account.

Warning: for security reasons, the only account allowed to join a computer to the domain is "Administrator".

For French users, we added a line ("Dos charset") that allows for Samba to map incoming characters in filenames encoded on a DOS code page. This option is very useful if you want to save files and directories names stated, in your profile, with all their accentuated characters. 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. This may, or may not, be convenient to your client machines.

Listing 11: config/smb.conf–global

```
1  [global]
2    workgroup = IDEALX-NT
3    netbios name = PDC-SRV
4    enable privileges = yes
5    server string = SAMBA-LDAP PDC Server
6    ...
7    #unix password sync = Yes
8    #passwd program = /usr/local/sbin/smbldap-passwd -u %u
9    #passwd chat = "Changing password for*\nNew password*" %n\n "*Retype
         new password*" %n\n"
10   ldap passwd sync = Yes
11   ...
12   ; SAMBA-LDAP declarations
13   passdb backend = ldapsam:ldap://127.0.0.1/
14   # ldap filter = (&(objectclass=sambaSamAccount)(uid=%u))
15   ldap admin dn = cn=Manager,dc=IDEALX,dc=ORG
16   ldap suffix = dc=IDEALX,dc=ORG
17   ldap group suffix = ou=Groups
18   ldap user suffix = ou=Users
19   ldap machine suffix = ou=Computers
20   ldap ssl = start_tls
```

```
21
22    add machine script = /usr/local/sbin/smbldap-useradd -w "%u"
23    add user script = /usr/local/sbin/smbldap-useradd -m "%u"
24    ldap delete dn = Yes
25    #delete user script = /usr/local/sbin/smbldap-userdel "%u"
26    add group script = /usr/local/sbin/smbldap-groupadd -p "%g"
27    #delete group script = /usr/local/sbin/smbldap-groupdel "%g"
28    add user to group script = /usr/local/sbin/smbldap-groupmod -m "%u" "%g
          "
29    delete user from group script = /usr/local/sbin/smbldap-groupmod -x "%u
          " "%g"
30    set primary group script = /usr/local/sbin/smbldap-usermod -g "%g" "%u"
31
32    ...
33    Dos charset = 850
34    Unix charset = ISO8859-1
```

The shares sections Here takes place all the share declarations. In particular, we can define in the [homes] section all users home directories:

Listing 12: config/smb.conf–homes

```
1  [homes]
2    comment = Home Directories
3    valid users = %U
4    read only = No
5    create mask = 0664
6    directory mask = 0775
7    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 user. For example if the *sambaProfilePath* is set to \\PDC-SRV\profiles\testuser, than the profile directory for the user *testuser* is /home/samba/profiles/testuser/.

Make sure to have the adequate 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.

Listing 13: config/smb.conf–profiles

```
1  [profiles]
2    path = /home/samba/profiles
3    read only = No
4    create mask = 0600
5    directory mask = 0700
6    browseable = No
7    guest ok = Yes
8    profile acls = Yes
9    csc policy = disable
10   # next line is a great way to secure the profiles
11   force user = %U
12   # next line allows administrator to access all profiles
13   valid users = %U @"Domain Admins"
```

If you want command's file to be downloaded and run when a user successfully logs in from a workstation (client machine), you have to define a *netlogon* section and a *netlogon script*.

Beware: all this stuff is by default devised for MS-Windows clients, not for other platforms.

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.

Listing 14: config/smb.conf–netlogon

```
1  [global]
2    ...
3    logon script = STARTUP.BAT
4    ...
5
6  [netlogon]
7    path = /home/samba/netlogon/
8    browseable = No
9    read only = yes
10
11 [doc]
12   path=/usr/share/doc
13   public=yes
14   writable=no
15   read only=no
16   create mask = 0750
17   guest ok = Yes
```

For example, we could have the STARTUP.BAT script that sets a directory mounted on the "J" volume on Windows clients. Another useful command synchronizes the client clock to the server's one:

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

4.3.2 Preparation

You must create directories referenced in 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 `ldap admin dn` (cn=Manager,dc=IDEALX,dc=ORG) user's password. Note: you specified it in smb.conf. This user is used by Samba to bind to the directory and

it must have enough permissions on the directory (LDAP) service to add/modify accounts stored in it.

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 data in /etc/samba/secrets.tbd.

Note that this "ldap admin dn" can be another account than the Root DN. In a word: use a ldap account who has permissions to write any sambaSAMAccount and some posixAccount attributes (see section 5 on page 21 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 'unknown parameter' message. See man testparm for more info.

4.4 smbldap-tools scripts

You must configure your smbldap-tools to match your system and LDAP service configurations. 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 define now is the "domain secure ID" (`SID`). You can obtain its value by starting samba, waiting a bunch of minutes then use the following command:

  ```
  net getlocalsid
  ```

- 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 'read' requests, and one dedicated to 'write' requests. 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 by 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:
```

[12] if you want to do this manually, a sample LDIF file presented on section 17.2 on page 66 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`

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:
```

[13] see 8.1 on page 28 for more info

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)
```

Then delete this test account:

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

5 Security considerations

5.1 Use an account which is not Root DN

In this HOWTO, we are using the Root DN: the *ldap admin dn* should be another account than Root DN: you should use another ldap account which 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 those accounts were respectivly *samba* and *smbldap-tools* (do NOT use those in a real setup!), 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 accounts
  - `nssldap` also need write access to unix password attribute (for example if a user want to change his password with the `passwd` command).

Here is the corresponding section of slapd.conf:

Listing 15: config/slapdAtts.conf

```
# any users can authenticate and change his 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 accounts
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 accounts
```

```
37  access to dn="ou=Groups,dc=idealx,dc=org"
38          by dn="cn=samba,ou=DSA,dc=idealx,dc=org" write
39          by dn="cn=smbldap-tools,ou=DSA,dc=idealx,dc=org" write
40          by * none
41  # samba need to be able to create new computers accounts
42  access to dn="ou=Computers,dc=idealx,dc=org"
43          by dn="cn=samba,ou=DSA,dc=idealx,dc=org" write
44          by dn="cn=smbldap-tools,ou=DSA,dc=idealx,dc=org" write
45          by * none
46  # this can be omitted but we let it stay because there could be other
47  # branches in the directory
48  access to *
49          by self read
50          by * none
```

5.2 Secure connections: use TLS !

In this HOWTO, whe are using a cleartext (non-cyphered) LDAP transport between Samba and OpenLDAP. As both servers implement SSL, you should use TLS transport instead, in to protect informations and passwords from eavesdropping.

If you want to use TLS, you have to create a certificate for each server. Certificates can be self-signed but it is preferable to have certificates signed by the same certification 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).

One may also use a PKI in order to ease certificate management. Hint: use IDX-PKI from the IDEALX OpenTrust suite (http://IDEALX.com/).

Remember one important thing: a certificates is created with its "common name" hard-coded in it. Each time you want to connect to the server in secure mode, you **must** contact it using this name (and not an alias or 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 then 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  data keys  private data/ca.db.certs
     ln -s data datas
     touch private/ca.key data/ca.db.serial
     cp /dev/null data/ca.db.index
     ```

   - Generate pseudo-random bytes

     ```
     openssl rand 1024 > data/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 data/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

```
[ ca ]
default_ca              = default_CA
[ default_CA ]
dir                     = .                      # Where everything is kep
certs                   = ./certs                # Where the issued certs
new_certs_dir           = ./data/ca.db.certs     # Where the issued crl are
database                = ./data/ca.db.index     # database index file
serial                  = ./data/ca.db.serial    # The current serial numbe
RANDFILE                = ./data/random-bits     # private random number fi
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' > data/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.ideal
  ```

- extract the ldap.idealx.com certificate

  ```
  perl -n -e 'm/BEGIN CERTIFICATE/ && do {$$seen=1}; $$seen && print;' < certs/ldap
  ```

- 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 sessions:

- 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 data

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 Starting and stopping the LDAP and Samba 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-group` to help you migrating users and groups defined in `/etc/passwd` (and/or `/etc/shadow`) and `/etc/group`.

You can find his scripts in 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 follows:

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
   ```

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 follows:

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 profile
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:

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

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 sambaBadPasswordCount sambaBadPasswordTime	samba samba samba	specify the type of the samba account Bad password attempt count 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

authentification, and the smbldap-tools may offer you a good base to manage user accounts data.

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.

[14] http://sourceforge.net/projects/smbldap-tools

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 Idealx Management Console (IMC)

Have a look on the project site (https://sourceforge.net/projects/imc/) for more information.

8.1.4 idxldapaccounts webmin module

If you prefer a nice GUI on a Web browser you should have a look on the idxldapaccounts Webmin module. This module is not maintained anymore!

8.1.5 Microsoft Windows NT Domain management tools

You can manage users account using the Microsoft Windows NT Domain management tools. This can be launch using the `usrmgr.exe` command in a MS-DOS 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 manage 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 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 data.

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 data (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 http://sourceforge.net/projects/smbldap-tools.

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: This is a work in progress!

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?

You may 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
```

Beware: remember to establish adequate passwords before going into production.

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 SomeServerName
[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 '$' character appended to its name (meaning: "this is a 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 (uid=0) must exist and be used.

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 on page 28. Then you can add the computer in the domain, following those 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:

- log into Windows using the administrator account.
- click on the "start" menu, "Parameters" and "Configuration".
- double click on "System", select the "Network identification" tab, 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

This can also be directly done from Microsoft Windows NT, using the administrator account. This procedure will create automatically an account for the computer, and will also join it to the domain.

To do so, follow the steps described in section 10.2.1 on the previous page. When asked for the 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 pressing 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 something changed.

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 data,
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 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 fails**, 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:

```
[netlogon]
        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:\WINNT\sysem32\repl\import\) 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 checklist presented in this section is 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 operation of your samba-ldap system. We assume a system running all the needed services, you can check 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 check this using the following command:

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

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, you 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 on page 28. If interested in a graphical user interface to manager user and group accounts, please have a look on the idxldapaccounts Webmin module (see "idxldapaccounts" 32).

To test it:

- create an user account for 'testsmbuser' (8.1.2 on page 31)
- check this user account:

```
$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 a ldapbrowser, you should see the new uid=testsmbuser,ou=Users,dc=IDEAL 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[15]
- Domain: IDEALX-NT

You should then log on fine. When you log in the domain with your username testsmbuser, check 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, check that you can save it
- check 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 think that you are the culprit :-)

To tackle this pleasant world, you should have a look on the following considerations.

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, and the O'Reilly books).

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).

[15] in fact, the one you gave in the section: 8.1.2 on page 31

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.

TODO: indexing the serializing back-end

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:

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. Check 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 correctly set privileges 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 embedded cache).

If you did 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),
- Neil Darlow
- 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

Listing 16: config/slapd.conf

```
1  include         /etc/openldap/schema/core.schema
2  include         /etc/openldap/schema/cosine.schema
3  include         /etc/openldap/schema/inetorgperson.schema
4  include         /etc/openldap/schema/nis.schema
5  include         /etc/openldap/schema/samba.schema
6
7  schemacheck     on
8  lastmod         on
9
10 TLSCertificateFile /etc/openldap/ldap.idealx.com.pem
11 TLSCertificateKeyFile /etc/openldap/ldap.idealx.com.key
12 TLSCACertificateFile /etc/openldap/ca.pem
13 TLSCipherSuite :SSLv3
14 #TLSVerifyClient demand
15
16 ########################################################################
17 # bdb database definitions
18 ########################################################################
19 database        bdb
20 suffix          dc=idealx,dc=org
21 rootdn          "cn=Manager,dc=idealx,dc=org"
22 rootpw          secret
23 directory       /var/lib/ldap
24 index       objectClass,uidNumber,gidNumber                    eq
25 index       cn,sn,uid,displayName                              pres,sub,eq
26 index       memberUid,mail,givenname                  eq,subinitial
27 index       sambaSID,sambaPrimaryGroupSID,sambaDomainName      eq
28
29 # users can authenticate and change their password
30 access to attrs=userPassword,sambaNTPassword,sambaLMPassword
31       by self write
32       by anonymous auth
33       by * none
```

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

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

Listing 17: config/samba.schema

```
1  ##
2  ## schema file for OpenLDAP 2.x
3  ## Schema for storing Samba user accounts and group maps in LDAP
4  ## OIDs are owned by the Samba Team
5  ##
6  ## Prerequisite schemas - uid         (cosine.schema)
7  ##                      - displayName (inetorgperson.schema)
8  ##                      - gidNumber   (nis.schema)
9  ##
10 ## 1.3.6.1.4.1.7165.2.1.x - attributetypes
11 ## 1.3.6.1.4.1.7165.2.2.x - objectclasses
12 ##
13
14 ##########################################################################
15 ##                                HISTORICAL                            ##
16 ##########################################################################
17
18 ##
19 ## Password hashes
20 ##
21 #attributetype ( 1.3.6.1.4.1.7165.2.1.1 NAME 'lmPassword'
22 #       DESC 'LanManager Passwd'
23 #       EQUALITY caseIgnoreIA5Match
24 #       SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{32} SINGLE-VALUE )
25
26 #attributetype ( 1.3.6.1.4.1.7165.2.1.2 NAME 'ntPassword'
27 #       DESC 'NT Passwd'
28 #       EQUALITY caseIgnoreIA5Match
29 #       SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{32} SINGLE-VALUE )
30
31 ##
32 ## Account flags in string format ([UWDX      ])
33 ##
34 #attributetype ( 1.3.6.1.4.1.7165.2.1.4 NAME 'acctFlags'
35 #       DESC 'Account Flags'
36 #       EQUALITY caseIgnoreIA5Match
37 #       SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{16} SINGLE-VALUE )
38
39 ##
40 ## Password timestamps & policies
41 ##
42 #attributetype ( 1.3.6.1.4.1.7165.2.1.3 NAME 'pwdLastSet'
43 #       DESC 'NT pwdLastSet'
```

```
44 #         EQUALITY integerMatch
45 #         SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
46
47 #attributetype ( 1.3.6.1.4.1.7165.2.1.5 NAME 'logonTime'
48 #         DESC 'NT logonTime'
49 #         EQUALITY integerMatch
50 #         SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
51
52 #attributetype ( 1.3.6.1.4.1.7165.2.1.6 NAME 'logoffTime'
53 #         DESC 'NT logoffTime'
54 #         EQUALITY integerMatch
55 #         SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
56
57 #attributetype ( 1.3.6.1.4.1.7165.2.1.7 NAME 'kickoffTime'
58 #         DESC 'NT kickoffTime'
59 #         EQUALITY integerMatch
60 #         SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
61
62 #attributetype ( 1.3.6.1.4.1.7165.2.1.8 NAME 'pwdCanChange'
63 #         DESC 'NT pwdCanChange'
64 #         EQUALITY integerMatch
65 #         SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
66
67 #attributetype ( 1.3.6.1.4.1.7165.2.1.9 NAME 'pwdMustChange'
68 #         DESC 'NT pwdMustChange'
69 #         EQUALITY integerMatch
70 #         SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
71
72 ##
73 ## string settings
74 ##
75 #attributetype ( 1.3.6.1.4.1.7165.2.1.10 NAME 'homeDrive'
76 #         DESC 'NT homeDrive'
77 #         EQUALITY caseIgnoreIA5Match
78 #         SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{4} SINGLE-VALUE )
79
80 #attributetype ( 1.3.6.1.4.1.7165.2.1.11 NAME 'scriptPath'
81 #         DESC 'NT scriptPath'
82 #         EQUALITY caseIgnoreIA5Match
83 #         SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{255} SINGLE-VALUE )
84
85 #attributetype ( 1.3.6.1.4.1.7165.2.1.12 NAME 'profilePath'
86 #         DESC 'NT profilePath'
87 #         EQUALITY caseIgnoreIA5Match
88 #         SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{255} SINGLE-VALUE )
89
90 #attributetype ( 1.3.6.1.4.1.7165.2.1.13 NAME 'userWorkstations'
91 #         DESC 'userWorkstations'
92 #         EQUALITY caseIgnoreIA5Match
93 #         SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{255} SINGLE-VALUE )
94
95 #attributetype ( 1.3.6.1.4.1.7165.2.1.17 NAME 'smbHome'
96 #         DESC 'smbHome'
```

```
97  #       EQUALITY caseIgnoreIA5Match
98  #       SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{128} )
99
100 #attributetype ( 1.3.6.1.4.1.7165.2.1.18 NAME 'domain'
101 #       DESC 'Windows NT domain to which the user belongs'
102 #       EQUALITY caseIgnoreIA5Match
103 #       SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{128} )
104
105 ##
106 ## user and group RID
107 ##
108 #attributetype ( 1.3.6.1.4.1.7165.2.1.14 NAME 'rid'
109 #       DESC 'NT rid'
110 #       EQUALITY integerMatch
111 #       SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
112
113 #attributetype ( 1.3.6.1.4.1.7165.2.1.15 NAME 'primaryGroupID'
114 #       DESC 'NT Group RID'
115 #       EQUALITY integerMatch
116 #       SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
117
118 ##
119 ## The smbPasswordEntry objectclass has been depreciated in favor of the
120 ## sambaAccount objectclass
121 ##
122 #objectclass ( 1.3.6.1.4.1.7165.2.2.1 NAME 'smbPasswordEntry' SUP top
        AUXILIARY
123 #        DESC 'Samba smbpasswd entry'
124 #        MUST ( uid $ uidNumber )
125 #        MAY  ( lmPassword $ ntPassword $ pwdLastSet $ acctFlags ))
126
127 #objectclass ( 1.3.6.1.4.1.7165.2.2.2 NAME 'sambaAccount' SUP top
        STRUCTURAL
128 #       DESC 'Samba Account'
129 #       MUST ( uid $ rid )
130 #       MAY  ( cn $ lmPassword $ ntPassword $ pwdLastSet $ logonTime $
131 #                logoffTime $ kickoffTime $ pwdCanChange $ pwdMustChange $
         acctFlags $
132 #                displayName $ smbHome $ homeDrive $ scriptPath $
        profilePath $
133 #                description $ userWorkstations $ primaryGroupID $ domain
        ))
134
135 #objectclass ( 1.3.6.1.4.1.7165.2.2.3 NAME 'sambaAccount' SUP top
        AUXILIARY
136 #       DESC 'Samba Auxiliary Account'
137 #       MUST ( uid $ rid )
138 #       MAY  ( cn $ lmPassword $ ntPassword $ pwdLastSet $ logonTime $
139 #                logoffTime $ kickoffTime $ pwdCanChange $ pwdMustChange $
        acctFlags $
140 #                displayName $ smbHome $ homeDrive $ scriptPath $
        profilePath $
```

```
141 #              description $ userWorkstations $ primaryGroupID $ domain )
    )
142
143 ###############################################################################
144 ##                                END OF HISTORICAL                          ##
145 ###############################################################################
146
147 ###############################################################################
148 ##                    Attributes used by Samba 3.0 schema                    ##
149 ###############################################################################
150
151 ##
152 ## Password hashes
153 ##
154 attributetype ( 1.3.6.1.4.1.7165.2.1.24 NAME 'sambaLMPassword'
155         DESC 'LanManager Password'
156         EQUALITY caseIgnoreIA5Match
157         SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{32} SINGLE-VALUE )
158
159 attributetype ( 1.3.6.1.4.1.7165.2.1.25 NAME 'sambaNTPassword'
160         DESC 'MD4 hash of the unicode password'
161         EQUALITY caseIgnoreIA5Match
162         SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{32} SINGLE-VALUE )
163
164 ##
165 ## Account flags in string format ([UWDX      ])
166 ##
167 attributetype ( 1.3.6.1.4.1.7165.2.1.26 NAME 'sambaAcctFlags'
168         DESC 'Account Flags'
169         EQUALITY caseIgnoreIA5Match
170         SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{16} SINGLE-VALUE )
171
172 ##
173 ## Password timestamps & policies
174 ##
175 attributetype ( 1.3.6.1.4.1.7165.2.1.27 NAME 'sambaPwdLastSet'
176         DESC 'Timestamp of the last password update'
177         EQUALITY integerMatch
178         SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
179
180 attributetype ( 1.3.6.1.4.1.7165.2.1.28 NAME 'sambaPwdCanChange'
181         DESC 'Timestamp of when the user is allowed to update the
              password'
182         EQUALITY integerMatch
183         SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
184
185 attributetype ( 1.3.6.1.4.1.7165.2.1.29 NAME 'sambaPwdMustChange'
186         DESC 'Timestamp of when the password will expire'
187         EQUALITY integerMatch
188         SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
189
190 attributetype ( 1.3.6.1.4.1.7165.2.1.30 NAME 'sambaLogonTime'
191         DESC 'Timestamp of last logon'
```

```
192         EQUALITY integerMatch
193         SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
194
195 attributetype ( 1.3.6.1.4.1.7165.2.1.31 NAME 'sambaLogoffTime'
196         DESC 'Timestamp of last logoff'
197         EQUALITY integerMatch
198         SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
199
200 attributetype ( 1.3.6.1.4.1.7165.2.1.32 NAME 'sambaKickoffTime'
201         DESC 'Timestamp of when the user will be logged off automatically
                '
202         EQUALITY integerMatch
203         SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
204
205
206 ##
207 ## string settings
208 ##
209 attributetype ( 1.3.6.1.4.1.7165.2.1.33 NAME 'sambaHomeDrive'
210         DESC 'Driver letter of home directory mapping'
211         EQUALITY caseIgnoreIA5Match
212         SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{4} SINGLE-VALUE )
213
214 attributetype ( 1.3.6.1.4.1.7165.2.1.34 NAME 'sambaLogonScript'
215         DESC 'Logon script path'
216         EQUALITY caseIgnoreMatch
217         SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{255} SINGLE-VALUE )
218
219 attributetype ( 1.3.6.1.4.1.7165.2.1.35 NAME 'sambaProfilePath'
220         DESC 'Roaming profile path'
221         EQUALITY caseIgnoreMatch
222         SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{255} SINGLE-VALUE )
223
224 attributetype ( 1.3.6.1.4.1.7165.2.1.36 NAME 'sambaUserWorkstations'
225         DESC 'List of user workstations the user is allowed to logon to'
226         EQUALITY caseIgnoreMatch
227         SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{255} SINGLE-VALUE )
228
229 attributetype ( 1.3.6.1.4.1.7165.2.1.37 NAME 'sambaHomePath'
230         DESC 'Home directory UNC path'
231         EQUALITY caseIgnoreMatch
232         SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{128} )
233
234 attributetype ( 1.3.6.1.4.1.7165.2.1.38 NAME 'sambaDomainName'
235         DESC 'Windows NT domain to which the user belongs'
236         EQUALITY caseIgnoreMatch
237         SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{128} )
238
239 ##
240 ## SID, of any type
241 ##
242
243 attributetype ( 1.3.6.1.4.1.7165.2.1.20 NAME 'sambaSID'
```

```
244         DESC 'Security ID'
245         EQUALITY caseIgnoreIA5Match
246         SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{64} SINGLE-VALUE )
247
248
249 ##
250 ## Primary group SID, compatible with ntSid
251 ##
252
253 attributetype ( 1.3.6.1.4.1.7165.2.1.23 NAME 'sambaPrimaryGroupSID'
254         DESC 'Primary Group Security ID'
255         EQUALITY caseIgnoreIA5Match
256         SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{64} SINGLE-VALUE )
257
258 ##
259 ## group mapping attributes
260 ##
261 attributetype ( 1.3.6.1.4.1.7165.2.1.19 NAME 'sambaGroupType'
262         DESC 'NT Group Type'
263         EQUALITY integerMatch
264         SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
265
266 ##
267 ## Store info on the domain
268 ##
269
270 attributetype ( 1.3.6.1.4.1.7165.2.1.21 NAME 'sambaNextUserRid'
271         DESC 'Next NT rid to give our for users'
272         EQUALITY integerMatch
273         SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
274
275 attributetype ( 1.3.6.1.4.1.7165.2.1.22 NAME 'sambaNextGroupRid'
276         DESC 'Next NT rid to give out for groups'
277         EQUALITY integerMatch
278         SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
279
280 attributetype ( 1.3.6.1.4.1.7165.2.1.39 NAME 'sambaNextRid'
281         DESC 'Next NT rid to give out for anything'
282         EQUALITY integerMatch
283         SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
284
285 attributetype ( 1.3.6.1.4.1.7165.2.1.40 NAME 'sambaAlgorithmicRidBase'
286         DESC 'Base at which the samba RID generation algorithm should
              operate'
287         EQUALITY integerMatch
288         SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
289
290
291 ########################################################################
292 ##              objectClasses used by Samba 3.0 schema                ##
293 ########################################################################
294
295 ## The X.500 data model (and therefore LDAPv3) says that each entry can
```

```
296 ## only have one structural objectclass.  OpenLDAP 2.0 does not enforce
297 ## this currently but will in v2.1
298
299 ##
300 ## added new objectclass (and OID) for 3.0 to help us deal with backwards
301 ## compatibility with 2.2 installations (e.g. ldapsam_compat)  --jerry
302 ##
303 objectclass ( 1.3.6.1.4.1.7165.2.2.6 NAME 'sambaSamAccount' SUP top
    AUXILIARY
304         DESC 'Samba 3.0 Auxilary SAM Account'
305         MUST ( uid $ sambaSID )
306         MAY  ( cn $ sambaLMPassword $ sambaNTPassword $ sambaPwdLastSet $
307                sambaLogonTime $ sambaLogoffTime $ sambaKickoffTime $
308                sambaPwdCanChange $ sambaPwdMustChange $ sambaAcctFlags $
309                displayName $ sambaHomePath $ sambaHomeDrive $
                       sambaLogonScript $
310                sambaProfilePath $ description $ sambaUserWorkstations $
311                sambaPrimaryGroupSID $ sambaDomainName ))
312
313 ##
314 ## Group mapping info
315 ##
316 objectclass ( 1.3.6.1.4.1.7165.2.2.4 NAME 'sambaGroupMapping' SUP top
    AUXILIARY
317         DESC 'Samba Group Mapping'
318         MUST ( gidNumber $ sambaSID $ sambaGroupType )
319         MAY  ( displayName $ description ))
320
321 ##
322 ## Whole-of-domain info
323 ##
324 objectclass ( 1.3.6.1.4.1.7165.2.2.5 NAME 'sambaDomain' SUP top
    STRUCTURAL
325         DESC 'Samba Domain Information'
326         MUST ( sambaDomainName $
327                sambaSID )
328         MAY ( sambaNextRid $ sambaNextGroupRid $ sambaNextUserRid $
329               sambaAlgorithmicRidBase ) )
330
331 ## used for idmap_ldap module
332 objectclass ( 1.3.6.1.4.1.7165.1.2.2.7 NAME 'sambaUnixIdPool' SUP top
    AUXILIARY
333         DESC 'Pool for allocating UNIX uids/gids'
334         MUST ( uidNumber $ gidNumber ) )
335
336
337 objectclass ( 1.3.6.1.4.1.7165.1.2.2.8 NAME 'sambaIdmapEntry' SUP top
    AUXILIARY
338         DESC 'Mapping from a SID to an ID'
339         MUST ( sambaSID )
340         MAY ( uidNumber $ gidNumber ) )
341
```

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

17.1.2 smbldap-tools

Listing 18: config/smbldap.conf

```
1  # $Source: //samba/samba-ldap-howto/config/smbldap.conf,v $
2  # $Id: smbldap.conf,v 1.5 2005/10/31 15:32:57 jtournier Exp $
3  #
4  # smbldap-tools.conf : Q & D configuration file for smbldap-tools
5
6  #  This code was developped by IDEALX (http://IDEALX.org/) and
7  #  contributors (their names can be found in the CONTRIBUTORS file).
8  #
9  #                 Copyright (C) 2001-2002 IDEALX
10 #
11 #  This program is free software; you can redistribute it and/or
12 #  modify it under the terms of the GNU General Public License
13 #  as published by the Free Software Foundation; either version 2
14 #  of the License, or (at your option) any later version.
15 #
16 #  This program is distributed in the hope that it will be useful,
17 #  but WITHOUT ANY WARRANTY; without even the implied warranty of
18 #  MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
19 #  GNU General Public License for more details.
20 #
21 #  You should have received a copy of the GNU General Public License
22 #  along with this program; if not, write to the Free Software
23 #  Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307,
24 #  USA.
25
26 #  Purpose :
27 #       . be the configuration file for all smbldap-tools scripts
28
29 ##############################################################################

30 #
31 # General Configuration
32 #
33 ##############################################################################

34
35 # Put your own SID. To obtain this number do: "net getlocalsid".
36 # If not defined, parameter is taking from "net getlocalsid" return
37 SID="S-1-5-21-4205727931-4131263253-1851132061"
38
39 # Domain name the Samba server is in charged.
40 # If not defined, parameter is taking from smb.conf configuration file
41 # Ex: sambaDomain="IDEALX-NT"
```

```
42 sambaDomain="IDEALX-NT"
43
44 ##############################################################################
45 #
46 # LDAP Configuration
47 #
48 ##############################################################################
49
50 # Notes: to use to dual ldap servers backend for Samba, you must patch
51 # Samba with the dual-head patch from IDEALX. If not using this patch
52 # just use the same server for slaveLDAP and masterLDAP.
53 # Those two servers declarations can also be used when you have
54 # . one master LDAP server where all writing operations must be done
55 # . one slave LDAP server where all reading operations must be done
56 #   (typically a replication directory)
57
58 # Slave LDAP server
59 # Ex: slaveLDAP=127.0.0.1
60 # If not defined, parameter is set to "127.0.0.1"
61 slaveLDAP="127.0.0.1"
62
63 # Slave LDAP port
64 # If not defined, parameter is set to "389"
65 slavePort="389"
66
67 # Master LDAP server: needed for write operations
68 # Ex: masterLDAP=127.0.0.1
69 # If not defined, parameter is set to "127.0.0.1"
70 masterLDAP="127.0.0.1"
71
72 # Master LDAP port
73 # If not defined, parameter is set to "389"
74 masterPort="389"
75
76 # Use TLS for LDAP
77 # If set to 1, this option will use start_tls for connection
78 # (you should also used the port 389)
79 # If not defined, parameter is set to "1"
80 ldapTLS="0"
81
82 # How to verify the server's certificate (none, optional or require)
83 # see "man Net::LDAP" in start_tls section for more details
84 verify="require"
85
86 # CA certificate
87 # see "man Net::LDAP" in start_tls section for more details
88 cafile=""
89
90 # certificate to use to connect to the ldap server
91 # see "man Net::LDAP" in start_tls section for more details
92 clientcert=""
```

```
93
94  # key certificate to use to connect to the ldap server
95  # see "man Net::LDAP" in start_tls section for more details
96  clientkey=""
97
98  # LDAP Suffix
99  # Ex: suffix=dc=IDEALX,dc=ORG
100 suffix="dc=idealx,dc=org"
101
102 # Where are stored Users
103 # Ex: usersdn="ou=Users,dc=IDEALX,dc=ORG"
104 # Warning: if 'suffix' is not set here, you must set the full dn for
        usersdn
105 usersdn="ou=Users,${suffix}"
106
107 # Where are stored Computers
108 # Ex: computersdn="ou=Computers,dc=IDEALX,dc=ORG"
109 # Warning: if 'suffix' is not set here, you must set the full dn for
        computersdn
110 computersdn="ou=Computers,${suffix}"
111
112 # Where are stored Groups
113 # Ex: groupsdn="ou=Groups,dc=IDEALX,dc=ORG"
114 # Warning: if 'suffix' is not set here, you must set the full dn for
        groupsdn
115 groupsdn="ou=Groups,${suffix}"
116
117 # Where are stored Idmap entries (used if samba is a domain member server
        )
118 # Ex: groupsdn="ou=Idmap,dc=IDEALX,dc=ORG"
119 # Warning: if 'suffix' is not set here, you must set the full dn for
        idmapdn
120 idmapdn="ou=Idmap,${suffix}"
121
122 # Where to store next uidNumber and gidNumber available for new users and
        groups
123 # If not defined, entries are stored in sambaDomainName object.
124 # Ex: sambaUnixIdPooldn="sambaDomainName=${sambaDomain},${suffix}"
125 # Ex: sambaUnixIdPooldn="cn=NextFreeUnixId,${suffix}"
126 sambaUnixIdPooldn="sambaDomainName=IDEALX-NT,${suffix}"
127
128 # Default scope Used
129 scope="sub"
130
131 # Unix password encryption (CRYPT, MD5, SMD5, SSHA, SHA, CLEARTEXT)
132 hash_encrypt="SSHA"
133
134 # if hash_encrypt is set to CRYPT, you may set a salt format.
135 # default is "%s", but many systems will generate MD5 hashed
136 # passwords if you use "$1$%.8s". This parameter is optional!
137 crypt_salt_format="%s"
138
```

```
139 ##############################################################################

140 #
141 # Unix Accounts Configuration
142 #
143 ##############################################################################

144
145 # Login defs
146 # Default Login Shell
147 # Ex: userLoginShell="/bin/bash"
148 userLoginShell="/bin/bash"
149
150 # Home directory
151 # Ex: userHome="/home/%U"
152 userHome="/home/%U"
153
154 # Default mode used for user homeDirectory
155 userHomeDirectoryMode="700"
156
157 # Gecos
158 userGecos="System User"
159
160 # Default User (POSIX and Samba) GID
161 defaultUserGid="513"
162
163 # Default Computer (Samba) GID
164 defaultComputerGid="515"
165
166 # Skel dir
167 skeletonDir="/etc/skel"
168
169 # Default password validation time (time in days) Comment the next line
      if
170 # you don't want password to be enable for defaultMaxPasswordAge days (be
171 # careful to the sambaPwdMustChange attribute's value)
172 defaultMaxPasswordAge="45"
173
174 ##############################################################################

175 #
176 # SAMBA Configuration
177 #
178 ##############################################################################

179
180 # The UNC path to home drives location (%U username substitution)
181 # Just set it to a null string if you want to use the smb.conf 'logon
      home'
182 # directive and/or disable roaming profiles
183 # Ex: userSmbHome="\\PDC-SMB3\%U"
184 userSmbHome="\\PDC-SRV\%U"
185
```

```
186 # The UNC path to profiles locations (%U username substitution)
187 # Just set it to a null string if you want to use the smb.conf 'logon
      path'
188 # directive and/or disable roaming profiles
189 # Ex: userProfile="\\PDC-SMB3\profiles\%U"
190 userProfile="\\PDC-SRV\profiles\%U"
191
192 # The default Home Drive Letter mapping
193 # (will be automatically mapped at logon time if home directory exist)
194 # Ex: userHomeDrive="H:"
195 userHomeDrive="H:"
196
197 # The default user netlogon script name (%U username substitution)
198 # if not used, will be automatically username.cmd
199 # make sure script file is edited under dos
200 # Ex: userScript="startup.cmd" # make sure script file is edited under
      dos
201 userScript="logon.bat"
202
203 # Domain appended to the users "mail"-attribute
204 # when smbldap-useradd -M is used
205 # Ex: mailDomain="idealx.com"
206 mailDomain="idealx.com"
207
208 ##############################################################################################

209 #
210 # SMBLDAP-TOOLS Configuration (default are ok for a RedHat)
211 #
212 ##############################################################################################

213
214 # Allows not to use smbpasswd (if with_smbpasswd == 0 in smbldap_conf.pm)
      but
215 # prefer Crypt::SmbHash library
216 with_smbpasswd="0"
217 smbpasswd="/usr/bin/smbpasswd"
218
219 # Allows not to use slappasswd (if with_slappasswd == 0 in smbldap_conf.
      pm)
220 # but prefer Crypt:: libraries
221 with_slappasswd="0"
222 slappasswd="/usr/sbin/slappasswd"
223
224 # comment out the following line to get rid of the default banner
225 # no_banner="1"
```

Listing 19: config/smbldap_bind.conf

```
1 ##############################
2 # Credential Configuration #
```

```
3 ##############################
4 # Notes: you can specify two differents configuration if you use a
5 # master ldap for writing access and a slave ldap server for reading
      access
6 # By default, we will use the same DN (so it will work for standard Samba
7 # release)
8 slaveDN="cn=Manager,dc=idealx,dc=org"
9 slavePw="secret"
10 masterDN="cn=Manager,dc=idealx,dc=org"
11 masterPw="secret"
```

17.1.3 Samba

Listing 20: config/smb.conf

```
1 # Global parameters
2 [global]
3         workgroup = IDEALX-NT
4         netbios name = PDC-SRV
5         enable privileges = yes
6         interfaces = 192.168.5.11
7         username map = /etc/samba/smbusers
8         server string = Samba Server %v
9         security = user
10        encrypt passwords = Yes
11        min passwd length = 3
12        obey pam restrictions = No
13        #unix password sync = Yes
14        #passwd program = /usr/local/sbin/smbldap-passwd -u %u
15        #passwd chat = "Changing password for*\nNew password*" %n\n "*
              Retype new password*" %n\n"
16        ldap passwd sync = Yes
17        log level = 0
18        syslog = 0
19        log file = /var/log/samba/log.%m
20        max log size = 100000
21        time server = Yes
22        socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
23        mangling method = hash2
24        Dos charset = 850
25        Unix charset = ISO8859-1
26
27        logon script = logon.bat
28        logon drive = H:
29        logon home =
30        logon path =
31
32        domain logons = Yes
33        os level = 65
34        preferred master = Yes
```

```
35          domain master = Yes
36          wins support = Yes
37          passdb backend = ldapsam:ldap://127.0.0.1/
38          # passdb backend = ldapsam:"ldap://127.0.0.1/ ldap://slave.idealx
                .com"
39          # ldap filter = (&(objectclass=sambaSamAccount)(uid=%u))
40          ldap admin dn = cn=samba,ou=Users,dc=idealx,dc=org
41          ldap suffix = dc=idealx,dc=org
42          ldap group suffix = ou=Groups
43          ldap user suffix = ou=Users
44          ldap machine suffix = ou=Computers
45          ldap idmap suffix = ou=Users
46          ldap ssl = start tls
47          add user script = /usr/local/sbin/smbldap-useradd -m "%u"
48          ldap delete dn = Yes
49          #delete user script = /usr/local/sbin/smbldap-userdel "%u"
50          add machine script = /usr/local/sbin/smbldap-useradd -w "%u"
51          add group script = /usr/local/sbin/smbldap-groupadd -p "%g"
52          #delete group script = /usr/local/sbin/smbldap-groupdel "%g"
53          add user to group script = /usr/local/sbin/smbldap-groupmod -m "%
                u" "%g"
54          delete user from group script = /usr/local/sbin/smbldap-groupmod
                -x "%u" "%g"
55          set primary group script = /usr/local/sbin/smbldap-usermod -g "%g
                " "%u"
56
57          # printers configuration
58          printer admin = @"Print Operators"
59          load printers = Yes
60          create mask = 0640
61          directory mask = 0750
62          nt acl support = No
63          printing = cups
64          printcap name = cups
65          deadtime = 10
66          guest account = nobody
67          map to guest = Bad User
68          dont descend = /proc,/dev,/etc,/lib,/lost+found,/initrd
69          show add printer wizard = yes
70          ; to maintain capital letters in shortcuts in any of the profile
                folders:
71          preserve case = yes
72          short preserve case = yes
73          case sensitive = no
74
75  [homes]
76          comment = repertoire de %U, %u
77          read only = No
78          create mask = 0644
79          directory mask = 0775
80          browseable = No
81
82  [netlogon]
```

```
83          path = /home/samba/netlogon/
84          browseable = No
85          read only = yes
86
87  [profiles]
88          path = /home/samba/profiles
89          read only = no
90          create mask = 0600
91          directory mask = 0700
92          browseable = No
93          guest ok = Yes
94          profile acls = yes
95          csc policy = disable
96          # next line is a great way to secure the profiles
97          force user = %U
98          # next line allows administrator to access all profiles
99          valid users = %U @"Domain Admins"
100
101 [printers]
102         comment = Network Printers
103         printer admin = @"Print Operators"
104         guest ok = yes
105         printable = yes
106         path = /home/samba/spool/
107         browseable = No
108         read only  = Yes
109         printable = Yes
110         print command = /usr/bin/lpr -P%p -r %s
111         lpq command = /usr/bin/lpq -P%p
112         lprm command = /usr/bin/lprm -P%p %j
113
114 [print$]
115         path = /home/samba/printers
116         guest ok = No
117         browseable = Yes
118         read only = Yes
119         valid users = @"Print Operators"
120         write list = @"Print Operators"
121         create mask = 0664
122         directory mask = 0775
123
124 [public]
125         comment = Repertoire public
126         path = /home/samba/public
127         browseable = Yes
128         guest ok = Yes
129         read only = No
130         directory mask = 0775
131         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.

Listing 21: config/ldap.conf

```
1  # Your LDAP server. Must be resolvable without using LDAP.
2  host 127.0.0.1
3
4  # The distinguished name of the search base.
5  base dc=IDEALX,dc=ORG
6
7  # The distinguished name to bind to the server with if the effective user
       ID
8  # is root. Password must be stored in /etc/ldap.secret (mode 600)
9  rootbinddn cn=nssldap,ou=DSA,dc=IDEALX,dc=ORG
10
11 # RFC2307bis naming contexts
12 nss_base_passwd          ou=Users,dc=IDEALX,dc=ORG?one
13 nss_base_passwd          ou=Computers,dc=IDEALX,dc=ORG?one
14 nss_base_shadow          ou=Users,dc=IDEALX,dc=ORG?one
15 nss_base_group           ou=Groups,dc=IDEALX,dc=ORG?one
16
17 # Security options
18 ssl no
19 pam_password md5
20
21 # - The End
```

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

Listing 22: config/ldap.secret

```
1  nssldapsecretpwd
```

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

Listing 23: config/etc–nsswitch.conf

```
1  #
2  # /etc/nsswitch.conf
3  #
4  # An example Name Service Switch config file. This file should be
5  # sorted with the most-used services at the beginning.
6  #
7  # The entry '[NOTFOUND=return]' means that the search for an
8  # entry should stop if the search in the previous entry turned
9  # up nothing. Note that if the search failed due to some other reason
10 # (like no NIS server responding) then the search continues with the
11 # next entry.
12 #
13 # Legal entries are:
14 #
15 #       nisplus or nis+         Use NIS+ (NIS version 3)
```

```
16 #       nis or yp                Use NIS (NIS version 2), also called YP
17 #       dns                      Use DNS (Domain Name Service)
18 #       files                    Use the local files
19 #       db                       Use the local database (.db) files
20 #       compat                   Use NIS on compat mode
21 #       hesiod                   Use Hesiod for user lookups
22 #       [NOTFOUND=return]        Stop searching if not found so far
23 #
24
25 # To use db, put the "db" in front of "files" for entries you want to be
26 # looked up first in the databases
27 #
28 # Example:
29
30 passwd:      files ldap
31 shadow:      files ldap
32 group:       files ldap
33
34 hosts:       files dns
35
36 # Example - obey only what nisplus tells us...
37 #services:    nisplus [NOTFOUND=return] files
38 #networks:    nisplus [NOTFOUND=return] files
39 #protocols:   nisplus [NOTFOUND=return] files
40 #rpc:         nisplus [NOTFOUND=return] files
41 #ethers:      nisplus [NOTFOUND=return] files
42 #netmasks:    nisplus [NOTFOUND=return] files
43
44 bootparams: nisplus [NOTFOUND=return] files
45
46 ethers:      files
47 netmasks:    files
48 networks:    files
49 protocols:   files
50 rpc:         files
51 services:    files
52
53 netgroup:    files
54
55 publickey:   nisplus
56
57 automount:   files
58 aliases:     files nisplus
```

17.2 Sample data: 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 ;-)

Listing 24: config/smbldap–base.ldif

```
1 dn: dc=idealx,dc=org
2 objectClass: dcObject
```

```
3  objectclass: organization
4  o: idealx
5  dc: idealx
6
7  dn: ou=Users,dc=idealx,dc=org
8  objectClass: organizationalUnit
9  ou: Users
10
11 dn: ou=Groups,dc=idealx,dc=org
12 objectClass: organizationalUnit
13 ou: Groups
14
15 dn: ou=Computers,dc=idealx,dc=org
16 objectClass: organizationalUnit
17 ou: Computers
18 dn: uid=Administrator,ou=Users,dc=idealx,dc=org
19 cn: Administrator
20 sn: Administrator
21 objectClass: inetOrgPerson
22 objectClass: sambaSAMAccount
23 objectClass: posixAccount
24 objectClass: shadowAccount
25 gidNumber: 512
26 uid: Administrator
27 uidNumber: 0
28 homeDirectory: /home/%U
29 sambaPwdLastSet: 0
30 sambaLogonTime: 0
31 sambaLogoffTime: 2147483647
32 sambaKickoffTime: 2147483647
33 sambaPwdCanChange: 0
34 sambaPwdMustChange: 2147483647
35 sambaHomePath: \\PDC-SMB3\home\%U
36 sambaHomeDrive: H:
37 sambaProfilePath: \\PDC-SMB3\profiles\%U\Administrator
38 sambaPrimaryGroupSID: S-1-5-21-4231626423-2410014848-2360679739-512
39 sambaLMPassword: XXX
40 sambaNTPassword: XXX
41 sambaAcctFlags: [U          ]
42 sambaSID: S-1-5-21-4231626423-2410014848-2360679739-2996
43 loginShell: /bin/false
44 gecos: Netbios Domain Administrator
45
46 dn: uid=nobody,ou=Users,dc=idealx,dc=org
47 cn: nobody
48 sn: nobody
49 objectClass: inetOrgPerson
50 objectClass: sambaSAMAccount
51 objectClass: posixAccount
52 objectClass: shadowAccount
53 gidNumber: 514
54 uid: nobody
55 uidNumber: 999
```

```
56 homeDirectory: /dev/null
57 sambaPwdLastSet: 0
58 sambaLogonTime: 0
59 sambaLogoffTime: 2147483647
60 sambaKickoffTime: 2147483647
61 sambaPwdCanChange: 0
62 sambaPwdMustChange: 2147483647
63 sambaHomePath: \\PDC-SMB3\home\%U
64 sambaHomeDrive: H:
65 sambaProfilePath: \\PDC-SMB3\profiles\%U\nobody
66 sambaPrimaryGroupSID: S-1-5-21-4231626423-2410014848-2360679739-514
67 sambaLMPassword: NO PASSWORDXXXXXXXXXXXXXXXXXXXXX
68 sambaNTPassword: NO PASSWORDXXXXXXXXXXXXXXXXXXXXX
69 sambaAcctFlags: [NU          ]
70 sambaSID: S-1-5-21-4231626423-2410014848-2360679739-2998
71 loginShell: /bin/false
72
73 dn: cn=Domain Admins,ou=Groups,dc=idealx,dc=org
74 objectClass: posixGroup
75 objectClass: sambaGroupMapping
76 gidNumber: 512
77 cn: Domain Admins
78 memberUid: Administrator
79 description: Netbios Domain Administrators
80 sambaSID: S-1-5-21-4231626423-2410014848-2360679739-512
81 sambaGroupType: 2
82 displayName: Domain Admins
83
84 dn: cn=Domain Users,ou=Groups,dc=idealx,dc=org
85 objectClass: posixGroup
86 objectClass: sambaGroupMapping
87 gidNumber: 513
88 cn: Domain Users
89 description: Netbios Domain Users
90 sambaSID: S-1-5-21-4231626423-2410014848-2360679739-513
91 sambaGroupType: 2
92 displayName: Domain Users
93
94 dn: cn=Domain Guests,ou=Groups,dc=idealx,dc=org
95 objectClass: posixGroup
96 objectClass: sambaGroupMapping
97 gidNumber: 514
98 cn: Domain Guests
99 description: Netbios Domain Guests Users
100 sambaSID: S-1-5-21-4231626423-2410014848-2360679739-514
101 sambaGroupType: 2
102 displayName: Domain Guests
103
104 dn: cn=Print Operators,ou=Groups,dc=idealx,dc=org
105 objectClass: posixGroup
106 objectClass: sambaGroupMapping
107 gidNumber: 550
108 cn: Print Operators
```

```
109 description: Netbios Domain Print Operators
110 sambaSID: S-1-5-21-4231626423-2410014848-2360679739-550
111 sambaGroupType: 2
112 displayName: Print Operators
113
114 dn: cn=Backup Operators,ou=Groups,dc=idealx,dc=org
115 objectClass: posixGroup
116 objectClass: sambaGroupMapping
117 gidNumber: 551
118 cn: Backup Operators
119 description: Netbios Domain Members can bypass file security to back up
        files
120 sambaSID: S-1-5-21-4231626423-2410014848-2360679739-551
121 sambaGroupType: 2
122 displayName: Backup Operators
123
124 dn: cn=Replicator,ou=Groups,dc=idealx,dc=org
125 objectClass: posixGroup
126 objectClass: sambaGroupMapping
127 gidNumber: 552
128 cn: Replicator
129 description: Netbios Domain Supports file replication in a
        sambaDomainName
130 sambaSID: S-1-5-21-4231626423-2410014848-2360679739-552
131 sambaGroupType: 2
132 displayName: Replicator
133
134 dn: cn=Domain Computers,ou=Groups,dc=idealx,dc=org
135 objectClass: posixGroup
136 objectClass: sambaGroupMapping
137 gidNumber: 553
138 cn: Domain Computers
139 description: Netbios Domain Computers accounts
140 sambaSID: S-1-5-21-4231626423-2410014848-2360679739-553
141 sambaGroupType: 2
142 displayName: Domain Computers
143
144 #dn: cn=Administrators,ou=Groups,dc=idealx,dc=org
145 #objectClass: posixGroup
146 #objectClass: sambaGroupMapping
147 #gidNumber: 544
148 #cn: Administrators
149 #description: Netbios Domain Members can fully administer the computer/
        sambaDomainName
150 #sambaSID: S-1-5-21-4231626423-2410014848-2360679739-544
151 #sambaGroupType: 2
152 #displayName: Administrators
153
154 #dn: cn=Users,ou=Groups,dc=idealx,dc=org
155 #objectClass: posixGroup
156 #objectClass: sambaGroupMapping
157 #gidNumber: 545
158 #cn: Users
```

```
159 #description: Netbios Domain Ordinary users
160 #sambaSID: S-1-5-21-4231626423-2410014848-2360679739-545
161 #sambaGroupType: 2
162 #displayName: users
163
164 #dn: cn=Guests,ou=Groups,dc=idealx,dc=org
165 #objectClass: posixGroup
166 #objectClass: sambaGroupMapping
167 #gidNumber: 546
168 #cn: Guests
169 #memberUid: nobody
170 #description: Netbios Domain Users granted guest access to the computer/
        sambaDomainName
171 #sambaSID: S-1-5-21-4231626423-2410014848-2360679739-546
172 #sambaGroupType: 2
173 #displayName: Guests
174
175 #dn: cn=Power Users,ou=Groups,dc=idealx,dc=org
176 #objectClass: posixGroup
177 #objectClass: sambaGroupMapping
178 #gidNumber: 547
179 #cn: Power Users
180 #description: Netbios Domain Members can share directories and printers
181 #sambaSID: S-1-5-21-4231626423-2410014848-2360679739-547
182 #sambaGroupType: 2
183 #displayName: Power Users
184
185 #dn: cn=Account Operators,ou=Groups,dc=idealx,dc=org
186 #objectClass: posixGroup
187 #objectClass: sambaGroupMapping
188 #gidNumber: 548
189 #cn: Account Operators
190 #description: Netbios Domain Users to manipulate users accounts
191 #sambaSID: S-1-5-21-4231626423-2410014848-2360679739-548
192 #sambaGroupType: 2
193 #displayName: Account Operators
194
195 #dn: cn=Server Operators,ou=Groups,dc=idealx,dc=org
196 #objectClass: posixGroup
197 #objectClass: sambaGroupMapping
198 #gidNumber: 549
199 #cn: Server Operators
200 #description: Netbios Domain Server Operators
201 #sambaSID: S-1-5-21-4231626423-2410014848-2360679739-549
202 #sambaGroupType: 2
203 #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.

Listing 25: config/smbldap–dsa.ldif

```
1  dn: ou=DSA,dc=IDEALX,dc=ORG
2  objectClass: top
3  objectClass: organizationalUnit
4  ou: DSA
5  description: security accounts for LDAP clients
6
7  dn: cn=samba,ou=DSA,dc=IDEALX,dc=ORG
8  objectclass: organizationalRole
9  objectClass: top
10 objectClass: simpleSecurityObject
11 userPassword: sambasecretpwd
12 cn: samba
13
14 dn: cn=nssldap,ou=DSA,dc=IDEALX,dc=ORG
15 objectclass: organizationalRole
16 objectClass: top
17 objectClass: simpleSecurityObject
18 userPassword: nssldapsecretpwd
19 cn: nssldap
20
21 dn: cn=smbldap-tools,ou=DSA,dc=IDEALX,dc=ORG
22 objectclass: organizationalRole
23 objectClass: top
24 objectClass: simpleSecurityObject
25 userPassword: smbldapsecretpwd
26 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
```