

Smbldap-tools User Manual

(*Release* : 0.9.3)

Jérôme Tournier

Revision : 1.7, generated July 12, 2007

This document is the property of IDEALX¹. Permission is granted to distribute this document under the terms of the GNU Free Documentation License (<http://www.gnu.org/copyleft/fdl.html>).

Contents

1	Introduction	3
1.1	Software requirements	3
1.2	Updates of this document	3
1.3	Availability of this document	3
2	Installation	4
2.1	Requirements	4
2.2	Installation	4
2.2.1	Installing from rpm	4
2.2.2	Installing from a tarball	4
3	Configuring the smbldap-tools	5
3.1	The smbldap.conf file	5
3.2	The smbldap_bind.conf file	9
4	Using the scripts	10
4.1	Initial directory's population	10
4.2	User management	11
4.2.1	Adding a user	11
4.2.2	Removing a user	13
4.2.3	Modifying a user	13
4.3	Group management	13
4.3.1	Adding a group	13
4.3.2	Removing a group	13
4.4	Adding a interdomain trust account	15

¹<http://IDEALX.com/>

5	Samba and the smbldap-tools scripts	15
5.1	General configuration	15
5.2	Migrating an NT4 PDC to Samba3	16
6	Frequently Asked Questions	16
6.1	How can i use old released uidNumber and gidNumber ?	16
6.2	I always have this error: "Can't locate IO/Socket/SSL.pm"	17
6.3	I can't initialize the directory with smbldap-populate	17
6.4	I can't join the domain with the root account	17
6.5	I have the sambaSamAccount but i can't logged in	17
6.6	I want to create machine account on the fly, but it does not works or I must do it twice	17
6.7	I can't manage the Oracle Internet Database	18
6.8	The directive passwd program = /usr/local/sbin/smbldap-passwd -u %u is not called, or i got a error message when changing the password from windows	18
6.9	New computers account can't be set in ou=computers	18
6.10	I can join the domain, but i can't log on	18
6.11	I can't create a user with smbldap-useradd	18
6.12	smbldap-useradd: Can't call method "get_value" on an undefined value at /usr/local/sbin/smbldap-useradd line 154	19
6.13	Typical errors on creating a new user or a new group	19
7	Thanks	21
8	Annexes	21
8.1	Full configuration files	21
8.1.1	The /etc/opt/IDEALX/smbldap-tools/smbldap.conf file	21
8.1.2	The /etc/opt/IDEALX/smbldap-tools/smbldap_bind.conf file	25
8.1.3	The samba configuration file : /etc/samba/smb.conf	25
8.1.4	The OpenLDAP configuration file : /etc/openldap/slapd.conf	27
8.2	Changing the administrative account (ldap admin dn in smb.conf file)	29
8.3	known bugs	30

1 Introduction

Smbldap-tools is a set of scripts designed to help integrate Samba and a LDAP directory. They target both users and administrators of Linux systems.

Users can change their password in a way similar to the standard “passwd” command.

Administrators can perform user and group management command line actions and synchronise Samba account management consistently.

This document presents:

- a detailed view of the smbldap-tools scripts
- a step by step explanation of how to set up a Samba3 domain controller

1.1 Software requirements

The smbldap-tools have been developped and tested with the following configuration :

- *Linux* CentOS4 (be should work on any *Linux* distribution)
- Samba release 3.0.10,
- OpenLDAP release 2.2.13
- Microsoft Windows NT 4.0, Windows 2000 and Windows XP Workstations and Servers,

This guide applies to smbldap-tools *Release* : 0.9.3.

1.2 Updates of this document

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

If you find any bugs in this document, or if you want this document to integrate some additional infos, please drop me a mail with your bug report and/or change request at jtournier@gmail.com.

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 Installation

2.1 Requirements

The main requirement for using smbldap-tools are the two perl module: Net::LDAP and Crypt::SmbHash. In most cases, you'll also need the IO-Socket-SSL Perl module to use TLS functionality.

If you want samba to call the scripts so that you can use the User Manager (or any other) under MS-Windows (to add, delete modify users and groups), **Samba** must be installed on the same computer. Finally, **OpenLDAP** can be installed on any computer. Please check that it can be contacted by a standard LDAP client software.

Samba and **OpenLDAP** installations will not be discussed here. You can consult the howto also available on the project page (<http://sourceforge.net/projects/smbldap-tools/>).

2.2 Installation

An archive of the smbldap-tools scripts can be downloaded on our project page <http://sourceforge.net/projects/smbldap-tools/>. Archive and RedHat packages are available. If you are upgrading, look at the INSTALL file or read the link 6.13.

2.2.1 Installing from rpm

To install the scripts on a RedHat system, download the RPM package and run the following command:

```
rpm -Uvh smbldap-tools-0.9.3-1.i386.rpm
```

2.2.2 Installing from a tarball

On non RedHat system, download a source archive of the scripts. The current archive is `smbldap-tools-0.9.3.tar.gz`. Uncompress it and copy all of the Perl scripts in `/usr/sbin` directory, and the two configuration files in `/etc/smbldap-tools/` directory:

```
mkdir /etc/smbldap-tools/  
cp *.conf /etc/smbldap-tools/  
cp smbldap-* /usr/sbin/
```

The configuration is now based on two different files:

- `smbldap.conf`: define global parameter
- `smbldap_bind.conf`: define an administrative account to bind to the directory

The second file **must** be readable only for 'root', as it contains credentials allowing modifications on all the directory. Make sure the files are protected by running the following commands:

```
chmod 644 /etc/smbldap-tools/smbldap.conf
chmod 600 /etc/smbldap-tools/smbldap_bind.conf
```

3 Configuring the smbldap-tools

As mentioned in the previous section, you'll have to update two configuration files. The first (`smbldap.conf`) allows you to set global parameter that are readable by everybody, and the second (`smbldap_bind.conf`) defines two administrative accounts to bind to a slave and a master ldap server: this file must thus be readable only by root.

A script named `configure.pl` can help you to set their contents up. It is located in the tarball downloaded or in the documentation directory if you got the RPM archive (see `/usr/share/doc/smbldap-tools-0.9.3/`). Just invoke it:

```
/usr/share/doc/smbldap-tools-0.9.3/configure.pl
```

It will ask for the default values defined in your `smb.conf` file, and will update the two configuration files used by the scripts. Samba configuration file should then be already configured. Note that you can stop the script at any moment with the `Crtl-C` keys.

Before using this script :

- the two configuration files **must** be present in the `/etc/smbldap-tools/` directory
- check that samba is configured and running, as the script will try to get your workgroup's domain secure id (SID).

In those files, parameters are defined like this:

```
key="value"
```

Full example configuration files can be found at 8.1.

3.1 The smbldap.conf file

This file is used to define parameters that can be readable by everybody. A full example file is available in section 8.1.1.

Let's have a look at all available parameters.

- `UID_START` and `GID_START` : parameters deprecated
 - Those parameters must be removed or commented.
 - Available uid and gid are now defined in the default new entry `sambaUnixIdPool` `dn=sambaDomain`. See later for `${sambaDomain}` and `${suffix}` definitions.
- `SID` : Secure Identifier Domain
 - Example: `SID="S-1-5-21-3703471949-3718591838-2324585696"`
 - Remark: you can get the SID for your domain using the `"net getlocalsid"` command. Samba must be up and running for this to work (it can take **several** minutes for a Samba server to correctly negotiate its status with other network servers).
- `sambaDomain` : Samba Domain the Samba server is in charge
 - Example: `sambaDomain="DOMSMB"`
 - Remark: if not defined, parameter is taking from `smb.conf` configuration file
- `slaveLDAP` : slave LDAP server
 - Example: `slaveLDAP="127.0.0.1"`
 - Remark: must be a resolvable DNS name or it's IP address
- `slavePort` : port to contact the slave server
 - Example: `slavePort="389"`
- `masterLDAP` : master LDAP server
 - Example: `masterLDAP="127.0.0.1"`
- `masterPort` : port to contact the master server
 - Example: `masterPort="389"`
- `ldapTLS` : should we use TLS connection to contact the ldap servers ?
 - Example: `ldapTLS="1"`
 - Remark: the LDAP servers must be configured to accept TLS connections. See section the Samba-LDAP Howto for more details (<http://samba.idealx.org/smbldap-howto.fr.html>). If you are using TLS support, select port 389 to connect to the master and slave directories.
- `verify` : How to verify the server's certificate (none, optional or require).
 - Example: `verify="require"`
 - Remark: See "man Net::LDAP" in `start_tls` section for more details
- `cafile` : the PEM-format file containing certificates for the CA that slapd will trust
 - Example: `cafile="/etc/opt/IDEALX/smbldap-tools/ca.pem"`

- `clientcert` : the file that contains the client certificate
 - Example: `clientcert="/etc/opt/IDEALX/smbldap-tools/smbldap-tools.iallanis.com.pem"`
- `clientkey` : the file that contains the private key that matches the certificate stored in the `clientcert` file
 - Example: `clientkey="/etc/opt/IDEALX/smbldap-tools/smbldap-tools.iallanis.com.key"`
- `suffix` : The distinguished name of the search base
 - Example: `suffix="dc=idealx,dc=com"`
- `usersdn` : branch in which users account can be found or must be added
 - Example: `usersdn="ou=Users,${suffix}"`
 - Remark: this branch is **not** relative to the suffix value
- `computersdn` : branch in which computers account can be found or must be added
 - Example: `computersdn="ou=Computers,${suffix}"`
 - Remark: this branch is **not** relative to the suffix value
- `groupsdn` : branch in which groups account can be found or must be added
 - Example: `groupsdn="ou=Groups,${suffix}"`
 - Remarks: this branch is **not** relative to the suffix value
- `idmapdn` : where are stored Idmap entries (used if samba is a domain member server)
 - Example: `idmapdn="ou=Idmap,${suffix}"`
 - Remarks: this branch is **not** relative to the suffix value
- `sambaUnixIdPool` : object in which next uidNumber and gidNumber available are stored
 - Example: `sambaUnixIdPool="cn=NextFreeUnixId,${suffix}"`
 - Remarks: this branch is **not** relative to the suffix value
- `scope` : the search scope.
 - Example: `scope="sub"`
- `hash_encrypt` : hash to be used when generating a user password.
 - Example: `hash_encrypt="SSHA"`
 - Remark: This is used for the unix password stored in *userPassword* attribute.
- `crypt_salt_format="%s"` : if `hash_encrypt` is set to CRYPT, you may set a salt format. Default is "%s", but many systems will generate MD5 hashed passwords if you use "\$1\$%.8s". This parameter is optional.
- `userLoginShell` : default shell given to users.

- Example: `userLoginShell="/bin/bash"`
- Remark: This is stored in *loginShell* attribute.
- **userHome** : default directory where users's home directory are located.
 - Example: `userHome="/home/%U"`
 - Remark: This is stored in *homeDirectory* attribute.
- **userGecos** : geccos used for users
 - Example: `userGecos="System User"`
- **defaultUserGid** : default primary group set to users accounts
 - Example: `defaultUserGid="513"`
 - Remark: this is stored in *gidNumber* attribute.
- **defaultComputerGid** : default primary group set to computers accounts
 - Example: `defaultComputerGid="550"`
 - Remark: this is stored in *gidNumber* attribute.
- **skeletonDir** : skeleton directory used for users accounts
 - Example: `skeletonDir="/etc/skel"`
 - Remark: this option is used only if you ask for home directory creation when adding a new user.
- **defaultMaxPasswordAge** : default validation time for Samba password (in days)
 - Example: `defaultMaxPassword="55"`
- **userSmbHome** : samba share used to store user's home directory
 - Example: `userSmbHome="//PDC-SMB3/home/%U"`
 - Remark: this is stored in *sambaHomePath* attribute.
- **userProfile** : samba share used to store user's profile
 - Example: `userProfile="//PDC-SMB3/profiles/%U"`
 - Remark: this is stored in *sambaProfilePath* attribute.
- **userHomeDrive** : letter used on windows system to map the home directory
 - Example: `userHomeDrive="K:"`
- **userScript** : default user netlogon script name. If not used, will be automatically *username.cmd*
 - Example: `userScript="%U"`
 - Remark: this is stored in *sambaProfilePath* attribute.

- `mailDomain` : Domain appended to the users "mail" attribute.
 - Example: `mailDomain="idealx.org"`
- `with_smbpasswd` : should we use the `smbpasswd` command to set the user's password (instead of the `mkntpwd` utility) ?
 - Example: `with_smbpasswd="0"`
 - Remark: must be a boolean value (0 or 1).
- `smbpasswd` : path to the `smbpasswd` binary
 - Example: `smbpasswd="/usr/bin/smbpasswd"`
- `with_slappasswd` : should we use the `slappasswd` command to set the Unix user's password (instead of the `Crypt::` librairies) ?
 - Example: `with_smbpasswd="0"`
 - Remark: must be a boolean value (0 or 1).
- `slappasswd` : path to the `slappasswd` binary
 - Example: `smbpasswd="/usr/sbin/slappasswd"`

3.2 The `smbldap_bind.conf` file

This file is only used by `root` to give bind parameters to the directory when modifications are asked. It contains distinguished names and credentials to connect to both the master and slave directories. A full example file is available in section 8.1.2.

Let's have a look at all available parameters.

- `slaveDN` : distinguished name used to bind to the slave server
 - Example 1: `slaveDN="cn=Manager,dc=idealx,dc=com"`
 - Example 2: `slaveDN=""`
 - Remark: this can be the manager account of the directory or any LDAP account that has sufficient permissions to read the full directory (Slave directory is only used for reading). Anonymous connections uses the second example form.
- `slavePw` : the credentials to bind to the slave server
 - Example 1: `slavePw="secret"`
 - Example 2: `slavePw=""`
 - Remark: the password must be stored here in clear form. This file must then be readable only by root! All anonymous connections use the second form provided in our example.
- `masterDN` : the distinguished name used to bind to the master server

- Example: `masterDN="cn=Manager,dc=idealx,dc=com"`
- Remark: this can be the manager account of the directory or any LDAP account that has enough permissions to modify the content of the directory. Anonymous access does not make any sense here.
- `masterPw` : the credentials to bind to the master server
 - Example: `masterPw="secret"`
 - Remark: the password must be in clear text. Be sure to protect this file against unauthorized readers!

4 Using the scripts

4.1 Initial directory's population

You can initialize the LDAP directory using the `smbldap-populate` script. To do that, the account defined in the `/etc/opt/IDEALX/smbldap-tools/smbldap_bind.conf` to access the master directory **must** be the manager account defined in the directory configuration. On RedHat system, this file is `/etc/openldap/slapd.conf` and the account is defined with

```
1 rootdn      "cn=Manager,dc=idealx,dc=com"
2 rootpw      secret
```

The `smbldap_bind.conf` file must then be configured so that the parameters to connect to the master LDAP server match the previous ones:

```
1 masterDN="cn=Manager,dc=idealx,dc=com"
2 masterPw="secret"
```

Available options for this script are summarized in the table 1:

option	definition	default value
<code>-u uidNumber</code>	first uidNumber to allocate	1000
<code>-g gidNumber</code>	first uidNumber to allocate	1000
<code>-a user</code>	administrator login name	Administrator
<code>-b user</code>	guest login name	nobody
<code>-e file</code>	export a init file	
<code>-i file</code>	import a init file	

Table 1: Options available for the `smbldap-populate` script

In the more general case, to set up your directory, simply use the following command:

```
[root@etoile root]# smbldap-populate
Using builtin directory structure
```

```
adding new entry: dc=idealx,dc=com
adding new entry: ou=Users,dc=idealx,dc=com
adding new entry: ou=Groups,dc=idealx,dc=com
adding new entry: ou=Computers,dc=idealx,dc=com
adding new entry: ou=Idmap,dc=idealx,dc=org
adding new entry: cn=NextFreeUnixId,dc=idealx,dc=org
adding new entry: uid=Administrator,ou=Users,dc=idealx,dc=com
adding new entry: uid=nobody,ou=Users,dc=idealx,dc=com
adding new entry: cn=Domain Admins,ou=Groups,dc=idealx,dc=com
adding new entry: cn=Domain Users,ou=Groups,dc=idealx,dc=com
adding new entry: cn=Domain Guests,ou=Groups,dc=idealx,dc=com
adding new entry: cn=Print Operators,ou=Groups,dc=idealx,dc=com
adding new entry: cn=Backup Operators,ou=Groups,dc=idealx,dc=com
adding new entry: cn=Replicator,ou=Groups,dc=idealx,dc=com
adding new entry: cn=Domain Computers,ou=Groups,dc=idealx,dc=com
```

After this step, if you don't want to use the `cn=Manager,dc=idealx,dc=com` account anymore, you can create a dedicated account for Samba and the smbldap-tools. See section 8.2 for more details.

The `cn=NextFreeUnixId,dc=idealx,dc=org` entry is only used 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
```

4.2 User management

4.2.1 Adding a user

To add a user, use the `smbldap-useradd` script. Available options are summarized in the table 2. If applicable, default values are mentionned in the third column. Any string beginning with a `$` symbol refers to a parameter defined in the `/etc/opt/IDEALX/smbldap-tools/smbldap.conf` configuration file.

For example, if you want to add a user named `user_admin` and who :

- is a windows user
- must belong to the group of `gid=512` ('Domain Admins' group)
- has a home directory
- does not have a login shell
- has a `homeDirectory` set to `/dev/null`

option	definition	example	default value
-a	create a Windows account. Otherwise, only a Posix account is created		
-w	create a Windows Workstation account		
-i	create an interdomain trust account. See section 4.4 for more details		
-u	set a uid value	-u 1003	first uid available
-g	set a gid value	-g 1003	first gid available
-G	add the new account to one or several supplementary groups (comma-separated)	-G 512,550	
-d	set the home directory	-d /var/user	\$userHomePrefix/user
-s	set the login shell	-s /bin/ksh	\$userLoginShell
-c	set the user geccos	-c "admin user"	\$userGecos
-m	creates user's home directory and copies /etc/skel into it		
-k	set the skeleton dir (with -m)	-k /etc/skel2	\$skeletonDir
-P	ends by invoking smbldap-passwd to set the user's password		
-A	user can change password ? 0 if no, 1 if yes	-A 1	
-B	user must change password at first session ? 0 if no, 1 if yes	-B 1	
-C	set the samba home share	-C \\PDC\homes	\$userSmbHome
-D	set a letter associated with the home share	-D H:	\$userHomeDrive
-E	set DOS script to execute on login	-E common.bat	\$userScript
-F	set the profile directory	-F \\PDC\profiles\user	\$userProfile
-H	set the samba account control bits like '[NDHTUMWSLKI]'	-H [X]	
-N	set the canonical name of the user		
-S	set the surname of the user		
-M	local mailAddress (comma separated)	-M testuser,aliasuser	
-T	forward mail address (comma separated)	-T testuser@domain.org	

Table 2: Options available to the smbldap-useradd script

- does not have a roaming profile
- and for whom we want to set a first login password

you must invoke:

```
smbldap-useradd -a -G 512 -m -s /bin/false -d /dev/null -F "" -P user_admin
```

4.2.2 Removing a user

To remove a user account, use the `smbldap-userdel` script. Available options are

option	definition
-r	remove home directory
-R	remove home directory interactively

Table 3: Option available to the `smbldap-userdel` script

For example, if you want to remove the `user1` account from the LDAP directory, and if you also want to delete his home directory, use the following command :

```
smbldap-userdel -r user1
```

Note: '-r' is dangerous as it may delete precious and unbackupid data, please be careful.

4.2.3 Modifying a user

To modify a user account, use the `smbldap-usermod` script. Availables options are listed in the table 4. You can also use the `smbldap-userinfo` script to update user's information. This script can also be used by users themselves to update their own informations listed in the tables 5 (adequats ACL must be set in the directory server). Available options are :

4.3 Group management

4.3.1 Adding a group

To add a new group in the LDAP directory, use the `smbldap-groupadd` script. Available options are listed in the table 6.

4.3.2 Removing a group

To remove the group named `group1`, just use the following command :

```
smbldap-userdel group1
```

option	definition	example
-c	set the user geccos	-c "admin user"
-d	set the home directory	-d /var/user
-u	set a uid value	-u 1003
-g	set a gid value	-g 1003
-G	add the new account to one or several supplementary groups (comma-separated)	-G 512,550
		-G -512,550
		-G +512,550
-s	set the login shell	-s /bin/ksh
-N	set the canonical name of the user	
-S	set the surname of the user	
-P	ends by invoking smbldap-passwd to set the user's password	
-a	add sambaSAMAccount objectclass	
-e	set an expiration date for the password (format: YYYY-MM-DD HH:MM:SS)	
-A	user can change password ? 0 if no, 1 if yes	-A 1
-B	user must change password at first session ? 0 if no, 1 if yes	-B 1
-C	set the samba home share	-C \\PDC\homes
		-C ""
-D	set a letter associated with the home share	-D H:
		-D ""
-E	set DOS script to execute on login	-E common.bat
		-E ""
-F	set the profile directory	-F \\PDC\profiles\user
		-F ""
-H	set the samba account control bits like '[NDHTUMWSLKI]'	-H [X]
-I	disable a user account	-I 1
-J	enable a user	-J 1
-M	local mailAddress (comma seperated)	-M testuser,aliasuser
-T	forward mail address (comma seperated)	-T testuser@domain.org

Table 4: Options available to the smbldap-usermod script

option	definition	example
-f	set the full name's user	-f MyName
-r	set the room number	-r 99
-w	set the work phone number	-w 111111111
-h	set the home phone number	-h 222222222
-o	set other information (in gecost definition)	-o "second stage"
-s	set the default bash	-s /bin/ksh

Table 5: Options available to the smbldap-userinfo script

option	definition	example
-a	add automatic group mapping entry	
-g <i>gid</i>	set the <i>gidNumber</i> for this group to <i>gid</i>	-g 1002
-o	gidNumber is not unique	
-r <i>group-rid</i>	set the rid of the group to <i>group-rid</i>	-r 1002
-s <i>group-sid</i>	set the sid of the group to <i>group-sid</i>	-s S-1-5-21-3703471949-3718591838-2324585696-1002
-t <i>group-type</i>	set the <i>sambaGroupType</i> to <i>group-type</i>	-t 2
-p	print the gidNumber to stdout	

Table 6: Options available for the smbldap-groupadd script

4.4 Adding a interdomain trust account

To add an interdomain trust account to the primary controller *trust-pdc*, use the **-i** option of `smbldap-useradd` as follows :

```
[root@etoile root]# smbldap-useradd -i trust-pdc
New password : *****
Retype new password : *****
```

The script will terminate asking for a password for this trust account. The account will be created in the directory branch where all computer accounts are stored (**ou=Computers** by default). The only two particularities of this account are that you are setting a password for this account, and the flags of this account are [I].

5 Samba and the smbldap-tools scripts

5.1 General configuration

Samba can 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 this utility, samba needs to be configured correctly. The `smb.conf` configuration file must contain the following directives :

```

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

```

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

```

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

```

5.2 Migrating an NT4 PDC to Samba3

The account migration procedure becomes really simple when samba is configured to use the smbldap-tools. Samba configuration (`smb.conf` file) must contain the directive defined above to properly call the script for managing users, groups and computer accounts. The migration process is outlined in the chapter 30 of the samba howto <http://sambafr.idealx.org/samba/docs/man/Samba-HOWTO-Collection/NT4Migration.html>.

6 Frequently Asked Questions

6.1 How can i use old released uidNumber and gidNumber ?

There are two way to do this :

- modify the `cn=NextFreeUnixId,dc=idealx,dc=org` and change the `uidNumber` and/or `gidNumber` value. This must be done manually. For example, if you want to use all available `uidNumber` and `gidNumber` higher then 1500, you need to create a `update-NextFreeUnixId.ldif` file containing :

```

1 dn: cn=NextFreeUnixId,dc=idealx,dc=org
2 changetype: modify
3 uidNumber: 1500
4 gidNumber: 1500

```

and then update the directory :

```
ldapmodify -x -D "cn=Manager,dc=idealx,dc=org" -w secret -f update-NextFreeUnixId.ldi
```

- use the `-u` or `-g` option to the script you need to set the value you want to use

6.2 I always have this error: "Can't locate IO/Socket/SSL.pm"

This happens when you want to use a certificate. In this case, you need to install the IO-Socket-SSL Perl module.

6.3 I can't initialize the directory with smbldap-populate

When I want to initialize the directory using the `smbldap-populate` script, I get

```
[root@slave sbin]# smbldap-populate.pl
Using builtin directory structure
adding new entry: dc=IDEALX,dc=COM
Can't call method "code" without a package or object reference at
/usr/local/sbin/smbldap-populate.pl line 270, <GEN1> line 2.
```

Answer: check the TLS configuration

- if you don't want to use TLS support, set the `/etc/opt/IDEALX/smbldap-tools/smbldap.conf` file with
`ldapSSL="0"`
- if you want TLS support, set the `/etc/opt/IDEALX/smbldap-tools/smbldap.conf` file with
`ldapSSL="1"`
and check that the directory server is configured to accept TLS connections.

6.4 I can't join the domain with the root account

- check that the root account has the `sambaSamAccount` objectclass
- check that the directive `add machine script` is present and configured

6.5 I have the sambaSamAccount but i can't logged in

Check that the `sambaPwdLastSet` attribute is not null (equal to 0)

6.6 I want to create machine account on the fly, but it does not works or I must do it twice

- The script defined with the `add machine script` must not add the `sambaSAMAccount` objectclass of the machine account. The script must only add the Posix machine account. Samba will add the `sambaSAMAccount` when joining the domain.
- Check that the `add machine script` is present in samba configuration file.

6.7 I can't manage the Oracle Internet Database

If you have an error message like :

```
1 Function Not Implemented at /usr/local/sbin/smbldap_tools.pm line 187.  
2 Function Not Implemented at /usr/local/sbin/smbldap_tools.pm line 627.
```

For Oracle Database, all attributes that will be requested to the directory must be indexed. Add a new index for samba attributes and make sure that the following attributes are also indexed : uidNumber, gidNumber, memberUid, homedirectory, description, userPassword ...

6.8 The directive passwd program = /usr/local/sbin/smbldap-passwd -u %u is not called, or i got a error message when changing the password from windows

The directive is called if you also set `unix password sync = Yes`. Notes:

- if you use OpenLDAP, none of those two options are needed. You just need `ldap passwd sync = Yes`.
- the script called here must only update the `userPassword` attribute. This is the reason of the `-u` option. Samba passwords will be updated by samba itself.
- the `passwd chat` directive must match what is prompted when using the `smbldap-passwd` command

6.9 New computers account can't be set in ou=computers

This is a known samba bug. There's a workarround: look at <http://marc.theaimsgroup.com/?l=samba&m=108439612826440&w=2>

6.10 I can join the domain, but i can't log on

look at section 6.9

6.11 I can't create a user with smbldap-useradd

When creating a new user account I get the following error message:

```
/usr/local/sbin/smbldap-useradd.pl: unknown group SID not set for unix group 513
```

Answer:

- is `nss_ldap` correctly configured ?

- is the default group's users mapped to the 'Domain Users' NT group ?

```
net groupmap add rid=513 unixgroup="Domain Users" ntgroup="Domain Users"
```

6.12 smbldap-useradd: Can't call method "get_value" on an undefined value at /usr/local/sbin/smbldap-useradd line 154

- does the default group defined in smbldap.conf exist (defaultUserGid="513") ?
- does the NT "Domain Users" group mapped to a unix group of rid 513 (see option *-r* of smbldap-groupadd and smbldap-groupmod to set a rid) ?

6.13 Typical errors on creating a new user or a new group

- i've got the following error:

```
Could not find base dn, to get next uidNumber at /usr/local/sbin//smbldap_tools.pm li
```

1. you do not have created the object to defined the next uidNumber and gidNumber available.

- for version 0.8.7 : you can just run the `smbldap-populate` script that will update the `sambaDomain` entry to store those informations
- for version before 0.8.7 : You have updated the `smbldap-tools` to version 0.8.5 or newer. You have to do this manually. Create an file called `add.ldif` and containing

```
dn: cn=NextFreeUnixId,dc=idealx,dc=org
objectClass: inetOrgPerson
objectClass: sambaUnixIdPool
uidNumber: 1000
gidNumber: 1000
cn: NextFreeUnixId
sn: NextFreeUnixId
```

and then add the object with the `ldapadd` utility:

```
$ ldapadd -x -D "cn=Manager,dc=idealx,dc=org" -w secret -f add.ldif
```

Here, 1000 is the first available value for uidNumber and gidNumber (of course, if this value is already used by a user or a group, the first available after 1000 will be used).

2. The error also appear when there is a need for TLS (`ldapTLS=1` in `smbldap.conf`) and something is wrong with certificate naming or path settings.

- i've got the following error:

```
Use of uninitialized value in string at
/usr/local/sbin//smbldap\_tools.pm line 914.
```

```
Error: No DN specified at /usr/local/sbin//smbldap\_tools.pm line 919
```

You have not updated the configuration file to defined the object where are sotred the next uidNumber and gidNumber available. In our example, you have to add a nex entry in */etc/opt/IDEALX/smbldap-tools/smbldap.conf* containing :

```
# Where to store next uidNumber and gidNumber available
sambaUnixIdPoolDn="cn=NextFreeUnixId,${suffix}"
```

btw, a new option is now available too: the domain to append to users. You can add to the configuration file the following lines:

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

- i've got the following error:

```
Use of uninitialized value in concatenation (.) or string at /usr/local/sbin/smbldap-
Use of uninitialized value in substitution (s///) at /usr/local/sbin/smbldap-useradd
Use of uninitialized value in string at /usr/local/sbin/smbldap-useradd line 264.
failed to add entry: homedirectory: value #0 invalid per syntax at /usr/local/sbin/sm
userHomeDirectory=User "jto" already member of the group "513".
failed to add entry: No such object at /usr/local/sbin/smbldap-useradd line 382.
```

you have to change the variable name *userHomePrefix* to *userHome* in */etc/opt/IDEALX/smbldap-tools/smbldap.conf*

- i've got the following error:

```
failed to add entry: referral missing at /usr/local/sbin/smbldap-useradd line 279, <D
```

you have to update the configuration file that defined users, groups and computers dn. Those parameters must not be relative to the *suffix* parameter. A typical configuration look like this :

```
usersdn="ou=Users,${suffix}"
computersdn="ou=Computers,${suffix}"
groupsdn="ou=Groups,${suffix}"
```

- i've got the following error:

```
erreur LDAP: Can't contact master ldap server (IO::Socket::INET: Bad protocol 'tcp')
at /usr/local/sbin//smbldap_tools.pm line 153.
```

remove *ldap* from */etc/nsswitch.conf* for *services* list of possible check. For example, if your ldap directory is not configured to give services information, you must have

```
services    files
```

and not

```
services:   ldap [NOTFOUND=return] files
```

7 Thanks

People who have worked on this document are

- Jérôme Tournier <jerome.tournier@IDEALX.com>
- David Barth <david.barth@IDEALX.com>
- Nat Makarevitch <nat@IDEALX.com>

The authors 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 :

- IDEALX team :
 - Roméo Adekambi <romeo.adekambi@IDEALX.com>
 - Aurelien Degremont <adegremont@IDEALX.com>
 - Renaud Renard <rrenard@IDEALX.com>
- John H Terpstra <jht@samba.org>

8 Annexes

8.1 Full configuration files

8.1.1 The /etc/opt/IDEALX/smbldap-tools/smbldap.conf file

```
1 # $Source: $
2 # $Id: smbldap.conf,v 1.18 2005/05/27 14:28:47 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-1-5-21-2252255531-4061614174-2474224977"
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="DOMSMB"
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="/etc/smbldap-tools/ca.pem"
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="/etc/smbldap-tools/smbldap-tools.pem"
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="/etc/smbldap-tools/smbldap-tools.key"
97
98 # LDAP Suffix
99 # Ex: suffix=dc=IDEALX,dc=ORG
100 suffix="dc=company,dc=com"
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,${suffix}"
126 sambaUnixIdPooldn="sambaDomainName=${sambaDomain},${suffix}"
127
128 # Default scope Used
129 scope="sub"
130
131 # Unix password encryption (CRYPT, MD5, SMD5, SSHA, SHA, CLEARTXT)
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 # SMLDAP-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"
226

```

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

```

1 #####
2 # Credential Configuration #
3 #####
4 # Notes: you can specify two different 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=company,dc=com"
9 slavePw="secret"
10 masterDN="cn=Manager,dc=company,dc=com"
11 masterPw="secret"
12

```

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

```

1 # Global parameters
2 [global]
3     workgroup = DOMSMB
4     netbios name = PDC-SRV
5     security = user
6     enable privileges = yes
7     #interfaces = 192.168.5.11
8     #username map = /etc/samba/smbusers
9     server string = Samba Server %v
10    #security = ads
11    encrypt passwords = Yes
12    min passwd length = 3
13    #pam password change = no
14    #obey pam restrictions = No
15
16    # method 1:
17    #unix password sync = no
18    #ldap passwd sync = yes
19
20    # method 2:
21    unix password sync = yes
22    ldap passwd sync = no
23    passwd program = /usr/sbin/smbldap-passwd -u "%u"
24    passwd chat = "Changing *\nNew password*" %n\n "*Retype new password*" %n\n"
25
26    log level = 0
27    syslog = 0
28    log file = /var/log/samba/log.%U
29    max log size = 100000
30    time server = Yes
31    socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
32    mangling method = hash2
33    Dos charset = 850
34    Unix charset = ISO8859-1
35
36    logon script = logon.bat
37    logon drive = H:
38    logon home =
39    logon path =

```

```

40
41     domain logons = Yes
42     domain master = Yes
43     os level = 65
44     preferred master = Yes
45     wins support = yes
46     passdb backend = ldapsam:ldap://127.0.0.1/
47     ldap admin dn = cn=Manager,dc=company,dc=com
48     #ldap admin dn = cn=samba,ou=DSA,dc=company,dc=com
49     ldap suffix = dc=company,dc=com
50     ldap group suffix = ou=Groups
51     ldap user suffix = ou=Users
52     ldap machine suffix = ou=Computers
53     #ldap idmap suffix = ou=Idmap
54     add user script = /usr/sbin/smbldap-useradd -m "%u"
55     #ldap delete dn = Yes
56     delete user script = /usr/sbin/smbldap-userdel "%u"
57     add machine script = /usr/sbin/smbldap-useradd -t 0 -w "%u"
58     add group script = /usr/sbin/smbldap-groupadd -p "%g"
59     #delete group script = /usr/sbin/smbldap-groupdel "%g"
60     add user to group script = /usr/sbin/smbldap-groupmod -m "%u" "%g"
61     delete user from group script = /usr/sbin/smbldap-groupmod -x "%u" "%g"
62     set primary group script = /usr/sbin/smbldap-usermod -g '%g' '%u'
63
64     # printers configuration
65     #printer admin = @"Print Operators"
66     load printers = Yes
67     create mask = 0640
68     directory mask = 0750
69     #force create mode = 0640
70     #force directory mode = 0750
71     nt acl support = No
72     printing = cups
73     printcap name = cups
74     deadtime = 10
75     guest account = nobody
76     map to guest = Bad User
77     dont descend = /proc,/dev,/etc,/lib,/lost+found,/initrd
78     show add printer wizard = yes
79     ; to maintain capital letters in shortcuts in any of the profile folders:
80     preserve case = yes
81     short preserve case = yes
82     case sensitive = no
83
84 [netlogon]
85     path = /home/netlogon/
86     browseable = No
87     read only = yes
88
89 [profiles]
90     path = /home/profiles
91     read only = no
92     create mask = 0600
93     directory mask = 0700
94     browseable = No
95     guest ok = Yes
96     profile acls = yes
97     csc policy = disable
98     # next line is a great way to secure the profiles
99     #force user = %U
100    # next line allows administrator to access all profiles
101    #valid users = %U "Domain Admins"
102
103 [printers]
104     comment = Network Printers
105     #printer admin = @"Print Operators"

```

```

106     guest ok = yes
107     printable = yes
108     path = /home/spool/
109     browseable = No
110     read only = Yes
111     printable = Yes
112     print command = /usr/bin/lpr -P%p -r %s
113     lpq command = /usr/bin/lpq -P%p
114     lprm command = /usr/bin/lprm -P%p %j
115     # print command = /usr/bin/lpr -U%U%M -P%p -r %s
116     # lpq command = /usr/bin/lpq -U%U%M -P%p
117     # lprm command = /usr/bin/lprm -U%U%M -P%p %j
118     # lppause command = /usr/sbin/lpc -U%U%M hold %p %j
119     # lpresume command = /usr/sbin/lpc -U%U%M release %p %j
120     # queuepause command = /usr/sbin/lpc -U%U%M stop %p
121     # queueresume command = /usr/sbin/lpc -U%U%M start %p
122
123 [print$]
124     path = /home/printers
125     guest ok = No
126     browseable = Yes
127     read only = Yes
128     valid users = @"Print Operators"
129     write list = @"Print Operators"
130     create mask = 0664
131     directory mask = 0775
132
133 [public]
134     path = /tmp
135     guest ok = yes
136     browseable = Yes
137     writable = yes

```

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

```

1  #
2  # See slapd.conf(5) for details on configuration options.
3  # This file should NOT be world readable.
4  #
5  include          /etc/openldap/schema/core.schema
6  include          /etc/openldap/schema/cosine.schema
7  include          /etc/openldap/schema/inetorgperson.schema
8  include          /etc/openldap/schema/nis.schema
9  include          /etc/openldap/schema/samba.schema
10
11 schemacheck      on
12
13 # Allow LDAPv2 client connections.  This is NOT the default.
14 allow bind_v2
15
16 # Do not enable referrals until AFTER you have a working directory
17 # service AND an understanding of referrals.
18 #referral         ldap://root.openldap.org
19
20 pidfile          /var/run/slapd.pid
21 argsfile         /var/run/slapd.args
22
23 # Load dynamic backend modules:
24 # modulepath      /usr/sbin/openldap
25 # moduleload      back_bdb.la
26 # moduleload      back_ldap.la
27 # moduleload      back_ldbm.la
28 # moduleload      back_passwd.la
29 # moduleload      back_shell.la

```

```

30
31 # The next three lines allow use of TLS for encrypting connections using a
32 # dummy test certificate which you can generate by changing to
33 # /usr/share/ssl/certs, running "make slapd.pem", and fixing permissions on
34 # slapd.pem so that the ldap user or group can read it. Your client software
35 # may balk at self-signed certificates, however.
36 #TLSCertificateFile /etc/openldap/ldap.company.com.pem
37 #TLSCertificateKeyFile /etc/openldap/ldap.company.com.key
38 #TLSCACertificateFile /etc/openldap/ca.pem
39 #TLSCipherSuite :SSLv3
40
41 # Sample security restrictions
42 #     Require integrity protection (prevent hijacking)
43 #     Require 112-bit (3DES or better) encryption for updates
44 #     Require 63-bit encryption for simple bind
45 # security ssf=1 update_ssf=112 simple_bind=64
46
47 # Sample access control policy:
48 #     Root DSE: allow anyone to read it
49 #     Subschema (sub)entry DSE: allow anyone to read it
50 #     Other DSEs:
51 #         Allow self write access
52 #         Allow authenticated users read access
53 #         Allow anonymous users to authenticate
54 #     Directives needed to implement policy:
55 # access to dn.base="" by * read
56 # access to dn.base="cn=Subschema" by * read
57 # access to *
58 #     by self write
59 #     by users read
60 #     by anonymous auth
61 #
62 # if no access controls are present, the default policy
63 # allows anyone and everyone to read anything but restricts
64 # updates to rootdn. (e.g., "access to * by * read")
65 #
66 # rootdn can always read and write EVERYTHING!
67
68 #####
69 # ldbm and/or bdb database definitions
70 #####
71
72 database            bdb
73 suffix              "dc=company,dc=com"
74 rootdn              "cn=Manager,dc=company,dc=com"
75 # Cleartext passwords, especially for the rootdn, should
76 # be avoided. See slapd.conf(5) and slapd.conf(5) for details.
77 # Use of strong authentication encouraged.
78 rootpw              secret
79 # rootpw            {crypt}ijFYNcSNctBYg
80
81 # The database directory MUST exist prior to running slapd AND
82 # should only be accessible by the slapd and slap tools.
83 # Mode 700 recommended.
84 directory            /var/lib/ldap
85 lastmod              on
86
87 # Indices to maintain for this database
88 index objectClass    eq,pres
89 index ou,cn,sn,mail,givenname    eq,pres,sub
90 index uidNumber,gidNumber,memberUid    eq,pres
91 index loginShell     eq,pres
92 ## required to support pdb_getsampwnam
93 index uid            pres,sub,eq
94 ## required to support pdb_getsambapwrid()
95 index displayName    pres,sub,eq

```

```

96 index nisMapName,nisMapEntry          eq,pres,sub
97 index sambaSID                        eq,sub
98 index sambaPrimaryGroupSID            eq
99 index sambaDomainName                  eq
100 index default                          sub
101
102
103 # users can authenticate and change their password
104 access to attrs=userPassword,sambaNTPassword,sambaLMPassword,sambaPwdMustChange,sambaPwdLastSet
105     by dn="cn=Manager,dc=company,dc=com" write
106     by self write
107     by anonymous auth
108     by * none
109
110 # those 2 parameters must be world readable for password aging to work correctly
111 # (or use a privileged account in /etc/ldap.conf to bind to the directory)
112 access to attrs=shadowLastChange,shadowMax
113     by dn="cn=Manager,dc=company,dc=com" write
114     by self write
115     by * read
116
117
118 # all others attributes are readable to everybody
119 access to *
120     by * read
121
122 # Replicas of this database
123 #repllogfile /var/lib/ldap/openldap-master-replog
124 #replica host=ldap-1.example.com:389 starttls=critical
125 # bindmethod=sasl saslmech=GSSAPI
126 # authcId=host/ldap-master.example.com@EXAMPLE.COM

```

8.2 Changing the administrative account (ldap admin dn in smb.conf file)

If you don't want to use the `cn=Manager,dc=idealx,dc=com` account anymore, you can create a dedicated account for Samba and the smbldap-tools scripts. To do this, create an account named *samba* as follows (see section 4.2.1 for a more detailed syntax) :

```
smbldap-useradd -s /bin/false -d /dev/null -P samba
```

This command will ask you to set a password for this account. Let's set it to *samba* for this example. You then need to modify configuration files:

- file `/etc/opt/IDEALX/smbldap-tools/smbldap.bind.conf`

```

1 slaveDN="uid=samba,ou=Users,dc=idealx,dc=com"
2 slavePw="samba"
3 masterDN="uid=samba,ou=Users,dc=idealx,dc=com"
4 masterPw="samba"

```

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

```
1 ldap admin dn = uid=samba,ou=Users,dc=idealx,dc=com
```

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

```
smbpasswd -w samba
```

- file `/etc/openldap/slapd.conf`: give to the *samba* user permissions to modify some attributes: this user needs to be able to modify all the samba attributes and some others (uidNumber, gidNumber ...) :

```

1  # users can authenticate and change their password
2  access to attrs=userPassword,sambaNTPassword,sambaLMPassword,sambaPwdLastSet,sambaPwdMustChange
3      by dn="uid=samba,ou=Users,dc=idealx,dc=com" write
4      by self write
5      by anonymous auth
6      by * none
7  # some attributes need to be readable anonymously so that 'id user' can answer correctly
8  access to attrs=objectClass,entry,gecos,homeDirectory,uid,uidNumber,gidNumber,cn,memberUid
9      by dn="uid=samba,ou=Users,dc=idealx,dc=com" write
10     by * read
11  # some attributes can be writable by users themselves
12  access to attrs=description,telephoneNumber
13      by dn="uid=samba,ou=Users,dc=idealx,dc=com" write
14      by self write
15      by * read
16  # some attributes need to be writable for samba
17  access to attrs=cn,sambaLMPassword,sambaNTPassword,sambaPwdLastSet,sambaLogonTime,sambaLogoffTime,sambaKickoffTime,
18      by dn="uid=samba,ou=Users,dc=idealx,dc=com" write
19      by self read
20      by * none
21  # samba need to be able to create the samba domain account
22  access to dn.base="dc=idealx,dc=com"
23      by dn="uid=samba,ou=Users,dc=idealx,dc=com" write
24      by * none
25  # samba need to be able to create new users account
26  access to dn="ou=Users,dc=idealx,dc=com"
27      by dn="uid=samba,ou=Users,dc=idealx,dc=com" write
28      by * none
29  # samba need to be able to create new groups account
30  access to dn="ou=Groups,dc=idealx,dc=com"
31      by dn="uid=samba,ou=Users,dc=idealx,dc=com" write
32      by * none
33  # samba need to be able to create new computers account
34  access to dn="ou=Computers,dc=idealx,dc=com"
35      by dn="uid=samba,ou=Users,dc=idealx,dc=com" write
36      by * none
37  # this can be omitted but we leave it: there could be other branch
38  # in the directory
39  access to *
40      by self read
41      by * none

```

8.3 known bugs

- Option `-B` (user must change password) of `smbldap-useradd` does not have effect: when `smbldap-passwd` script is called, *sambaPwdMustChange* attribute is rewrite.