Smbldap-tools User Manual
(*Release* : 0.8.4)

Jérôme Tournier

Revision : 1.3, generated February 9, 2004

Contents

[1] `http://IDEALX.com/`

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 detailled 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* RedHat 9 (be should work on any *Linux* distribution)
- Samba release 3.0.2pre1,
- OpenLDAP release 2.1.22
- Microsoft Windows NT 4.0, Windows 2000 and Windows XP Workstations and Servers,

This guide applies to smbldap-tools *Release* : 0.8.4.

1.2 Updates of this document

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

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

1.3 Availability of this document

2 Installation

2.1 Requirements

The main requirement for using smbldap-tools is the Net::LDAP Perl module. In most cases, you'll also need the IO-Socket-SSL Perl module to use TLS functionnality. 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://samba.IDEALX.org`). Altought is has been written for Samba2, most of its content still apply to Samba3. The main difference stands in LDAP schema's definitions.

2.2 Installation

An archive of the smbldap-tools scripts can be downloaded on our project page `http://samba.IDEALX.com/`. Archive and RedHat packages are available.

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-0.8.3-1.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-0.8.3.tar.gz`. Uncompress it and copy all of the Perl scripts in `/usr/local/sbin` directory, and the two configuration files in `/etc/smbldap-tools/` directory:

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

The configuration is now based on two differents 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 is 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/`). Just invoke it:

```
/usr/share/doc/smbldap-tools/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. 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 are parameters are defined like this:

```
key="value"
```

Full example configuration files can be found at 9.1.

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 9.1.1.

Let's have a look at all available parameters.

- `UID_START` : minimum user's uid
  Example: `UID_START="1000"`
  Remark: nss_ldap needs to be configured correctly to find the first available value.

- `GID_START` : uid
  Example: `GID_START="1000"`
  Remark: nss_ldap needs to be configured correctly to find the first available value.

- `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).

- `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 severs must be configured to accept TLS connections. See section 6 for more details. 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). See "man Net::LDAP" in start_tls section for more details
  Example: `verify="require"`

- `cafile` : the PEM-format file containing certificates for the CA that slapd will trust
  Example: `cafile="/etc/smbldap-tools/ca.pem"`

- `clientcert` : the file that contains the client certificate
  Example: `clientcert="/etc/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/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"`
  Remark: this branch is relative to the suffix value

- `computersdn` : branch in which computers account can be found or must be added
  Example: `computersdn"ou=Computers"`
  Remark: this branch is relative to the suffix value

- `groupsdn` : branch in which groups account can be found or must be added
  Example: `groupsdn="ou=Groups"`
  Remarks: this branch is 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.

- `userLoginShell` : default shell given to users.
  Example: `userLoginShell="/bin/bash"`
  Remark: This is stored in *loginShell* attribute.

- `userHomePrefix` : default directory where users's home directory are located.
  Example: `userHomePrefix="/home/"`
  Remark: This is stored in `homeDirectory` attribute.

- `userGecos` : gecos 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 a password (in days)
  Example: `defaultMaxPassword="55"`

- `userSmbHome` : samba share used to store user's home directory
  Example: `userSmbHome="\\PDC-SMB3\ homes"`
  Remark: this is stored in *sambaHomePath* attribute.

- `userProfile` : samba share used to store user's profile
  Example: `userProfile="\\PDC-SMB3\ profiles"`
  Remark: this is stored in *sambaProfilePath* attribute.

- `userHomeDrive` : letter used on windows system to map the home directory
  Example: `userHomeDrive="K:"`

- `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"`

- `mk_ntpasswd` : path to the mkntpwd binary
  Example: `mk_ntpasswd="/usr/local/sbin/mkntpwd"`
  Remark: the rpm package of the smbldap-tools will install this utility. If you are using the tarball archive, you have to install it yourself (sources are also in the smbldap-tools archive).

3.2 The smbldap_bind.conf file

This file is only used by *root* to modify the content of the directory. It contains distinguised names and credentials to connect to both the master and slave directories. A full example file is available in section 9.1.2.

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/smbldap-tools/smbldap_bind.conf` to access the master directory **must** 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
-a *user*	administrator login name	Administrator
-b *user*	guest login name	nobody
-e *file*	export a init file	
-i *file*	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: 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 9.2 for more details.

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/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
- 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 -P user_admin
```

4.2.2 Removing a user

To remove a user account, use the `smbldap-userdel` script. One available option is

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 unbackuped data, please be careful.

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 gecos	-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	\\PDC\homes	$userSmbHome
-D	set a letter associated with the home share	H:	$userHomeDrive
-E	set DOS script to execute on login	common.bat	$userScript
-F	set the profile directory	\\PDC\profiles\user)	$userProfile
-H	set the samba account control bits like'[NDHTUMWSLKI]')	[X]	
-N	set the canonical name of the user		
-S	set the surname of the user		

Table 2: Options available to the `smbldap-useradd` script

option	definition
-r	remove home directory

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

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 4.

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

Table 4: Options available for the `smbldap-groupadd` script

4.3.2 Removing a group

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

```
smbldap-userdel group1
```

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 31 of the samba howto `http://sambafr.idealx.org/samba/docs/man/NT4Migration.html`.

6 Secure connections: use TLS

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

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

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

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

6.1 Certificates creation

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

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

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

   - Generate pseudo-random bytes

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

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

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

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

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

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

```
1       [ ca ]
2       default_ca              = default_CA
3       [ default_CA ]
4       dir                     = .                     # Where everything is kept
5       certs                   = ./certs               # Where the issued certs are kept
6       new_certs_dir           = ./datas/ca.db.certs   # Where the issued crl are kept
7       database                = ./datas/ca.db.index   # database index file
8       serial                  = ./datas/ca.db.serial  # The current serial number
9       RANDFILE                = ./datas/random-bits   # private random number file
10      certificate             = ./certs/ca.pem        # The CA certificate
11      private_key             = ./private/ca.key      # The private key
12      default_days            = 730
13      default_crl_days        = 30
14      default_md              = md5
15      preserve                = no
16      x509_extensions         = server_cert
17      policy                  = policy_anything
18      [ policy_anything ]
19      countryName             = optional
20      stateOrProvinceName     = optional
21      localityName            = optional
22      organizationName        = optional
```

```
23        organizationalUnitName  = optional
24        commonName              = supplied
25        emailAddress            = optional
26        [ server_cert ]
27        #subjectKeyIdentifier   = hash
28        authorityKeyIdentifier  = keyid:always
29        extendedKeyUsage        = serverAuth,clientAuth,msSGC,nsSGC
30        basicConstraints        = critical,CA:false
```

- initialize the serial database

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

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

   - create the key for the server `ldap.idealx.com`

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

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

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

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

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

6.2 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/smbldap-tools/smbldap.conf` :

- activate the TLS support
  `ldapTLS="1"`
- the file that contains the client certificate
  `clientcert="/etc/smbldap-tools/smbldap-tools.pem"`

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

6.3 OpenLDAP

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

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

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

- TLSVerifyClient demand

6.4 Samba

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

- `ldap ssl = start tls`

6.5 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=com,dc=com`
- 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/smbldap-tools/ca.pem`
- OpenLDAP SSL mechanism
  `ssl start_tls`

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.

7 Frequently Asked Questions

7.1 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.

7.2 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/smbldap-tools/smbldap.conf` file with

  `ldapSSL="0"`

- if you want TLS support, set the `/etc/smbldap-tools/smbldap.conf` file with

  `ldapSSL="1"`

  and check that the directory server is configured to accept TLS connections.

7.3 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"
```

7.4 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) ?

7.5 I have the `sambaSamAccount` but i can't logged in

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

7.6 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 the only add the Posix machine account
- Check that the `add machine script` is present in samba configuration file.

8 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>

9 Annexes

9.1 Full configuration files

9.1.1 The /etc/smbldap-tools/smbldap.conf file

```
1  # $Source: /opt/cvs/samba/smbldap-tools/smbldap.conf,v $
2  # $Id: smbldap.conf,v 1.6 2004/02/07 16:58:52 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 # UID and GID starting at...
36 UID_START="1000"
37 GID_START="1000"
38
39 # Put your own SID
40 # to obtain this number do: net getlocalsid
41 SID="S-1-5-21-3703471949-3718591838-2324585696"
42
43 ##############################################################################
44 #
45 # LDAP Configuration
46 #
47 ##############################################################################
```

```
48
49  # Notes: to use to dual ldap servers backend for Samba, you must patch
50  # Samba with the dual-head patch from IDEALX. If not using this patch
51  # just use the same server for slaveLDAP and masterLDAP.
52  # Those two servers declarations can also be used when you have
53  # . one master LDAP server where all writing operations must be done
54  # . one slave LDAP server where all reading operations must be done
55  #   (typically a replication directory)
56
57  # Ex: slaveLDAP=127.0.0.1
58  slaveLDAP="127.0.0.1"
59  slavePort="389"
60
61  # Master LDAP : needed for write operations
62  # Ex: masterLDAP=127.0.0.1
63  masterLDAP="127.0.0.1"
64  masterPort="389"
65
66  # Use TLS for LDAP
67  # If set to 1, this option will use start_tls for connection
68  # (you should also used the port 389)
69  ldapTLS="1"
70
71  # How to verify the server's certificate (none, optional or require)
72  # see "man Net::LDAP" in start_tls section for more details
73  verify="require"
74
75  # CA certificate
76  # see "man Net::LDAP" in start_tls section for more details
77  cafile="/etc/smbldap-tools/ca.pem"
78
79  # certificate to use to connect to the ldap server
80  # see "man Net::LDAP" in start_tls section for more details
81  clientcert="/etc/smbldap-tools/smbldap-tools.pem"
82
83  # key certificate to use to connect to the ldap server
84  # see "man Net::LDAP" in start_tls section for more details
85  clientkey="/etc/smbldap-tools/smbldap-tools.key"
86
87  # LDAP Suffix
88  # Ex: suffix=dc=IDEALX,dc=ORG
89  suffix="dc=idealx,dc=com"
90
91  # Where are stored Users
92  # Ex: usersdn="ou=Users,dc=IDEALX,dc=ORG"
93  usersdn="ou=Users,dc=idealx,dc=com"
94
95  # Where are stored Computers
96  # Ex: computersdn="ou=Computers,dc=IDEALX,dc=ORG"
97  computersdn="ou=Computers,dc=idealx,dc=com"
98
99  # Where are stored Groups
100 # Ex groupsdn="ou=Groups,dc=IDEALX,dc=ORG"
101 groupsdn="ou=Groups,dc=idealx,dc=com"
102
103 # Default scope Used
104 scope="sub"
105
106 # Unix password encryption (CRYPT, MD5, SMD5, SSHA, SHA)
107 hash_encrypt="SSHA"
108
109 ##############################################################################
110 #
111 # Unix Accounts Configuration
112 #
113 ##############################################################################
```

```
114
115 # Login defs
116 # Default Login Shell
117 # Ex: userLoginShell="/bin/bash"
118 userLoginShell="/bin/bash"
119
120 # Home directory prefix (without username)
121 # Ex: userHomePrefix="/home/"
122 userHomePrefix="/home/"
123
124 # Gecos
125 userGecos="System User"
126
127 # Default User (POSIX and Samba) GID
128 defaultUserGid="513"
129
130 # Default Computer (Samba) GID
131 defaultComputerGid="553"
132
133 # Skel dir
134 skeletonDir="/etc/skel"
135
136 # Default password validation time (time in days) Comment the next line if
137 # you don't want password to be enable for defaultMaxPasswordAge days (be
138 # careful to the sambaPwdMustChange attribute's value)
139 defaultMaxPasswordAge="55"
140
141 ##############################################################################
142 #
143 # SAMBA Configuration
144 #
145 ##############################################################################
146
147 # The UNC path to home drives location without the username last extension
148 # (will be dynamically prepended)
149 # Ex: \\My-PDC-netbios-name\homes
150 # Just set it to a null string if you want to use the smb.conf 'logon home'
151 # directive and/or desabling roaming profiles
152 userSmbHome=""
153
154 # The UNC path to profiles locations without the username last extension
155 # (will be dynamically prepended)
156 # Ex: \\My-PDC-netbios-name\profiles\
157 # Just set it to a null string if you want to use the smb.conf 'logon path'
158 # directive and/or desabling roaming profiles
159 userProfile=""
160
161 # The default Home Drive Letter mapping
162 # (will be automatically mapped at logon time if home directory exist)
163 # Ex: q(U:) for U:
164 userHomeDrive="H:"
165
166 # The default user netlogon script name
167 # if not used, will be automatically username.cmd
168 # make sure script file is edited under dos
169 userScript=""
170
171
172 ##############################################################################
173 #
174 # SMBLDAP-TOOLS Configuration (default are ok for a RedHat)
175 #
176 ##############################################################################
177
178 # Allows not to use smbpasswd (if with_smbpasswd == 0 in smbldap_conf.pm) but
179 # prefer mkntpwd... most of the time, it's a wise choice :-)
```

```
180 with_smbpasswd="0"
181 smbpasswd="/usr/bin/smbpasswd"
182 mk_ntpasswd="/usr/local/sbin/mkntpwd"
183
```

9.1.2 The /etc/smbldap-tools/smbldap_bind.conf file

```
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=com"
9  slavePw="secret"
10 masterDN="cn=Manager,dc=idealx,dc=com"
11 masterPw="secret"
12
```

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

```
1  # Global parameters
2  [global]
3          workgroup = SMB3
4          netbios name = PDC-SMB3
5          interfaces = 192.168.5.11
6          username map = /etc/samba/smbusers
7          #admin users= @"Domain Admins"
8          server string = Samba Server %v
9          security = user
10         encrypt passwords = Yes
11         min passwd length = 3
12         obey pam restrictions = No
13         passwd chat = *New*password* %n\n *Retype*new*password* %n\n *all*authentication*tokens*updated*
14         passwd program = /usr/local/sbin/smbldap-passwd %u
15         ldap passwd sync = Yes
16         log level = 0
17         syslog = 0
18         log file = /var/log/samba/log.%m
19         max log size = 100000
20         time server = Yes
21         socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
22         mangling method = hash2
23         Dos charset = 850
24         Unix charset = ISO8859-1
25
26         logon script = logon.bat
27         logon drive = H:
28         logon home =
29         logon path =
30
31         domain logons = Yes
32         os level = 65
33         preferred master = Yes
34         domain master = Yes
35         wins support = Yes
36         passdb backend = ldapsam:ldap://127.0.0.1/
37         # passdb backend = ldapsam:"ldap://127.0.0.1/ ldap://slave.idealx.com"
38         ldap admin dn = uid=samba,ou=Users,dc=idealx,dc=com
39         ldap suffix = dc=idealx,dc=com
40         ldap group suffix = ou=Groups
```

```
41          ldap user suffix = ou=Users
42          ldap machine suffix = ou=Computers
43          ldap idmap suffix = ou=Users
44          ldap ssl = start tls
45          add user script = /usr/local/sbin/smbldap-useradd -m "%u"
46          ldap delete dn = Yes
47          #delete user script = /usr/local/sbin/smbldap-userdel "%u"
48          add machine script = /usr/local/sbin/smbldap-useradd -w "%u"
49          add group script = /usr/local/sbin/smbldap-groupadd -p "%g"
50          #delete group script = /usr/local/sbin/smbldap-groupdel "%g"
51          add user to group script = /usr/local/sbin/smbldap-groupmod -m "%u" "%g"
52          delete user from group script = /usr/local/sbin/smbldap-groupmod -x "%u" "%g"
53          set primary group script = /usr/local/sbin/smbldap-usermod -g "%g" "%u"
54
55          # printers configuration
56          printer admin = @"Print Operators"
57          load printers = Yes
58          create mask = 0640
59          directory mask = 0750
60          nt acl support = No
61          printing = cups
62          printcap name = cups
63          deadtime = 10
64          guest account = nobody
65          map to guest = Bad User
66          dont descend = /proc,/dev,/etc,/lib,/lost+found,/initrd
67          show add printer wizard = yes
68          ; to maintain capital letters in shortcuts in any of the profile folders:
69          preserve case = yes
70          short preserve case = yes
71          case sensitive = no
72
73  [homes]
74          comment = repertoire de %U, %u
75          read only = No
76          create mask = 0644
77          directory mask = 0775
78          browseable = No
79
80  [netlogon]
81          path = /home/netlogon/
82          read only = yes
83          write list = admin
84          force user = admin
85
86  [profiles]
87          path = /home/profiles
88          read only = no
89          create mask = 0600
90          directory mask = 0700
91          browseable = No
92          guest ok = Yes
93          profile acls = yes
94          csc policy = disable
95          # next line is a great way to secure the profiles
96          force user = %U
97          # next line allows administrator to access all profiles
98          valid users = %U "Domain Admins"
99
100 [printers]
101         comment = Network Printers
102         printer admin = @"Print Operators"
103         guest ok = yes
104         printable = yes
105         path = /home/spool/
106         browseable = No
```

```
107         read only  = Yes
108         printable = Yes
109         print command = /usr/bin/lpr -P%p -r %s
110         lpq command = /usr/bin/lpq -P%p
111         lprm command = /usr/bin/lprm -P%p %j
112
113 [print$]
114         path = /home/printers
115         guest ok = No
116         browseable = Yes
117         read only = Yes
118         valid users = @"Print Operators"
119         write list = @"Print Operators"
120         create mask = 0664
121         directory mask = 0775
122
123 [public]
124         comment = Repertoire public
125         path = /home/public
126         guest ok = Yes
127         read only = No
128         directory mask = 0775
129         create mask = 0664
130
```

9.1.4 The OpenLDAP configuration file : `/etc/openldap/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 # ldbm database definitions
18 ########################################################################
19 database        ldbm
20 suffix                dc=idealx,dc=com
21 rootdn                "cn=Manager,dc=idealx,dc=com"
22 rootpw                secret
23 directory        /var/lib/ldap
24 index    sambaSID    eq
25 index    sambaPrimaryGroupSID    eq
26 index    sambaDomainName    eq
27 index        objectClass,uid,uidNumber,gidNumber,memberUid        eq
28 index        cn,mail,surname,givenname                       eq,subinitial
29
30 # users can authenticate and change their password
31 access to attrs=userPassword,sambaNTPassword,sambaLMPassword
32       by dn="cn=Manager,dc=idealx,dc=com" write
33       by self write
34       by anonymous auth
35       by * none
36 # all others attributes are readable to everybody
37 access to *
```

```
38        by * read
```

9.2 Changing the administrative account

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/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  # somme 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
```

9.3 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.
- it is not possible to remove a user profile (*sambaProfilePath* attribute) using `smbldap-usermod -F '' user`.