# Samba/LDAP How-To using Samba v. 3

**By**
**David Trask**
**Technology Coordinator/Computer Teacher**
**Vassalboro Community School**
**Vassalboro, Maine USA**

What this document is: This is a how-to for setting up a simple Samba/LDAP server for your network as a means of providing centralized authentication and home directories. If it is done correctly you can provide one common logon for all platforms...Windows, Linux, and Mac OS X. This is exactly what I do in my own school. You can also host a common home directory for all users and export via NFS as necessary. This method does not incorporate the many security features that can be employed to better enhance network security. If you'd like more information on that please take a look at the how-to's located in the Samba Projects section at http://www.idealx.org/prj/samba/index.en.html .

My test environment: I chose Fedora Core 2 as my base OS for the server install. I chose to install "everything" in terms of packages to make sure I got what I needed....this can obviously be tweaked greatly. My Windows network is made up of WinXP Pro machines....I have not been able to test on anything else, but there's no reason it should not work. The packages I used for configuring Samba/LDAP can be downloaded from http://www.idealx.org/prj/samba/dist/ . I downloaded the latest RedHat 9 rpm....version 0.8.4 I believe.

Ok...let's get started!

**(NOTE: the next couple steps MAY not be necessary for your setup. In some cases it may be prudent, but I have found recently with Fedora Core 2...if you install "everything" you'll have what you need with regard to LDAP stuff...you can skip to Step 3 if you wish)**

**Step 1: Installing Apt (make sure you're connected to the Internet)**

(assuming you have loaded your server and set it up) Let's take care of a few housekeeping items to get our server ready for any updates and stuff we may need in the future....not all of this is necessary but it is prudent. Let's set up apt. Go to http://www.fedora.us/wiki/FedoraHOWTO and download the latest apt rpm package. Get the version for Fedora 2 if you're using that. Here's the link: http://download.fedora.us/fedora/fedora/2/i386/RPMS.stable/apt-0.5.15cnc6-0.fdr.11.2.i386.rpm

Using the terminal...let's install the rpm (go to the directory you downloaded it to...I usually work as root..so that's where it is... /root)

rpm -Uhv apt-0.5.15cnc6-0.fdr.11.2.i386.rpm

Good! Now that we have that installed...let's stay in terminal and get apt configured.

apt-get update

follow the prompts and set it up....I chose everything.

This will take a few minutes....so relax. Once this part finishes we should make sure it's all set by running

apt-get -f install

this will make sure the newest packages are in place. Answer “yes” and let it go. Once it's done we can move on.

**Step 2: Installing CPAN bundles**

Now we need to make sure our perl modules are all there and up to date. We can do this easily by running

perl -MCPAN -e -shell

Let it run. Answer “no” when it asks about Manual configuration.

Once it stops you'll be at the cpan prompt....type

install Bundle::CPAN

this will install many perl modules for you. Answer “yes” to any dependency questions. When you get to the question about “libnet”....answer “no”. Once you are finished...hit “enter” to exit....it'll run for a few seconds more and then bring you back to the cpan prompt. For good measure let's type

install Net::LDAP it should be up to date

now let's type

install Unicode::MapUTF8

Answer “yes” to any dependency questions. This module will be necessary if you ever choose to use the idxldapaccounts webmin module.

Now let's check a couple other things to be safe.

Type

install Crypt::SmbHash and install it

then type

install Convert::BER

Once that's done we're ready to move on!  Type exit to quit from the cpan prompt.

**Step 3:  Installing the smbldap-tools**

Now we need to install the smbldap-tools.  If you have not already done so....download the tools from idealx.

The packages I used for configuring Samba/LDAP can be downloaded from http://www.idealx.org/prj/samba/dist .  I downloaded the latest RedHat 9 rpm....version 0.8.4 I believe. (get the i386 version)

Install it by typing in terminal....

rpm -Uhv smbldap-tools-0.8.4-1.i386.rpm  (substitute any newer version #'s)

*Note:  if you skipped the steps above (naughty you!) then this may not work as it depends on Net::LDAP.  **In my experience in using Fedora Core 2 you should be all set if you paid attention to what was installed.**

**Step 4:  Edit the file /etc/ldap.conf to reflect your own search base...see below....**

```
# The distinguished name of the search base.
base dc=vcs,dc=org
```

**Step 5:  Copying the samba.schema file**

(helpful step:  If you have not done it yet you may want to run  updatedb  so you can locate files more quickly...this command takes a few minutes to run so be patient....once it's done you can locate files by typing  locate filename  ex:  locate samba.schema )

On your system you'll need to locate the samba.schema file.  On my system it is located at

/usr/share/doc/samba-3.0.3/LDAP/samba.schema

so let's go to that directory and copy the samba.schema file to /etc/openldap/schema

cd /usr/share/doc/samba-3.0.3/LDAP/

and then copy the file

cp samba.schema /etc/openldap/schema

**Step 6: Editing the Openldap files**

Now we need to edit the files located in /etc/openldap

Let's go there

cd /etc/openldap

Now type ls and let's see what's in there.

Type

gedit slapd.conf

there are many things to change in here...see my sample below for more...

Sample /etc/openldap/slapd.conf file

```
# $OpenLDAP: pkg/ldap/servers/slapd/slapd.conf,v 1.23.2.8 2003/05/24 23:19:14 kurt Exp $
#
# See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.
#
include                 /etc/openldap/schema/core.schema
include                 /etc/openldap/schema/cosine.schema
include                 /etc/openldap/schema/inetorgperson.schema
include                 /etc/openldap/schema/nis.schema
include                 /etc/openldap/schema/samba.schema

# Allow LDAPv2 client connections.  This is NOT the default.
#allow bind_v2

# Do not enable referrals until AFTER you have a working directory
# service AND an understanding of referrals.
#referral       ldap://root.openldap.org

pidfile         /var/run/slapd.pid
#argsfile       //var/run/slapd.args



########################################################################
# ldbm and/or bdb database definitions
########################################################################

database        ldbm
```

```
suffix                  "dc=vcs,dc=org"
rootdn                  "cn=Manager,dc=vcs,dc=org"
# Cleartext passwords, especially for the rootdn, should
# be avoided.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw                  secret
# rootpw                {crypt}ijFYNcSNctBYg

# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd and slap tools.
# Mode 700 recommended.
directory       /var/lib/ldap

# Indices to maintain for this database
#index objectClass                      eq,pres
#index ou,cn,mail,surname,givenname      eq,pres,sub
#index uidNumber,gidNumber,loginShell    eq,pres
#index uid,memberUid                    eq,pres,sub
#index nisMapName,nisMapEntry           eq,pres,sub
index objectClass           eq
index cn                    pres,sub,eq
index sn                    pres,sub,eq
index uid                   pres,sub,eq
index displayName           pres,sub,eq
index uidNumber             eq
index gidNumber             eq
index memberUID             eq
index sambaSID              eq
index sambaPrimaryGroupSID  eq
index sambaDomainName       eq
index default               sub
```

I've highlighted most of what needs to be changed....the default file has a lot more in it....feel free to cut and paste with your own values....in the end it should look almost exactly like mine.  Pay particular attention to the password....remember that you need to substitute 'secret' with the password you entered earlier in the smbldap_bind.conf file.  Remember?  I told you that you'd need to remember it.

Now we need to edit the other file....ldap.conf

type

gedit ldap.conf

This one is easy....just put in your values....see my example below.

Sample /etc/openldap/ldap.conf

```
# $OpenLDAP: pkg/ldap/libraries/libldap/ldap.conf,v 1.9 2000/09/04 19:57:01 kurt Exp $
#
# LDAP Defaults
#

# See ldap.conf(5) for details
# This file should be world readable but not world writable.

#BASE       dc=example, dc=com
#URI        ldap://ldap.example.com ldap://ldap-master.example.com:606

#SIZELIMIT              12
#TIMELIMIT              15
#DEREF                  never
HOST 127.0.0.1
BASE dc=vcs,dc=org
```

**Step 7: Starting the LDAP service**

If everything is done correctly we can now start the LDAP server. Simply type

service ldap start

If everything works....you're ready to move on...if not...you need to recheck your steps.

**Step 8: Configuring Samba**

Now we need to configure Samba. More specifically the file /etc/samba/smb.conf You may need to refer back to some of the values you entered in the Samba section of the file /etc/smbldap-tools/smbldap.conf . I have include my own smb.conf file for you to follow and or copy.

Sample /etc/samba/smb.conf

```
# Global parameters
[global]
        workgroup = MIDNIGHT
        netbios name = MIDNIGHT-PDC
       #(make sure this next line reflects the NIC connected to the Samba network!)
        interfaces = eth0, lo
        username map = /etc/samba/smbusers
        #admin users= @"Domain Admins"
        server string = Samba Server %v
        security = user
```

```
        encrypt passwords = Yes
        min passwd length = 3
        obey pam restrictions = No
        unix password sync = Yes
        #passwd program = /usr/local/sbin/smbldap-passwd -u %u
#passwd chat = "Changing password for*\nNew password*" %n\n "*Retype new password*" %n\n"
        ldap passwd sync = Yes
        log level = 0
        syslog = 0
        log file = /var/log/samba/log.%m
        max log size = 100000
        time server = Yes
        socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
        mangling method = hash2
        Dos charset = 850
        Unix charset = ISO8859-1

        logon script = startup.bat
        logon drive = F:
        logon home =
        logon path =

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

```
[homes]
        comment = Home Directories
        valid users = %S
        writeable = yes
        create mask = 0664
        directory mask = 0775
        browseable = Yes

[netlogon]
        comment = Network Logon Service
        path = /opt/samba/netlogon

[profiles]
        path = /opt/samba/profiles
        writeable = yes
        writeable = yes
        browseable = yes
        create mode = 0644
        directory mode = 0755

[printers]
        comment = All Printers
        path = /var/spool/samba
        printable = Yes
        browseable = No

#[tmp]
#       comment = Temporary file sadd user script=/usr/local/sbin/smbldap-useradd.plpace
#       path = /tmp
#       writeable = yes
#       guest ok = Yes


[whole_linux_server]
        comment = whole_linux_box
        path = /
        valid users = admin root dtrask
        admin users = admin root dtrask
        write list = admin root dtrask
        public = no
        writable = yes
```

(this last share is not wise unless you are in a secure situation and know your users!  Otherwise share only what you need to)

I highlighted in yellow the things that you'll need to change according to the values you put into smbldap.conf earlier. The stuff in green is some stuff you should pay attention to as you'll need it to be functional. *Note: the profiles share is only if you are going to be using roaming profiles in a Windows environment....(I do hence the reason it's there). Again...feel free to cut and paste.

(Don't start Samba yet...we'll do that in a few minutes)

**Step 9: Setting the Manager password**

Now we need to set the password for the Manager account that we specified in many of our configuration files. To do this....type

smbpasswd -w secret (where 'secret' is the password you specified in the config files earlier)

You'll see:

Setting stored password for "cn=Manager,dc=vcs,dc=org" in secrets.tdb (with your values of course)

**Step 10: Get the local SID...**

First we need to get the local SID from the system....so in the terminal type

net getlocalsid

then copy the SID (copy command in terminal....so you can paste in a few mins)

**Step 11: Configuring the smbldap-tools**

Now we need to configure the smbldap-tools you installed earlier. Smbldap-tools does come bundled with Samba, but the newest version we just downloaded is much easier to use....so....

Now we need to edit the files in /etc/smbldap-tools...so type

cd /etc/smbldap-tools

type

ls

to see what's in there

Now type

gedit smbldap.conf

this will open up the file in a nice GUI based text editor that we can edit the file as well as do search and replace.  (if you are a veteran Linux user...feel free to use your favorite text editor)

Edit the values for your system....I have included my own file below for your reference....feel free to simply cut and paste and insert your own information.

My sample /etc/smbldap-tools/smbldap.conf

```
# $Source: /opt/cvs/samba/smbldap-tools/smbldap.conf,v $
# $Id: smbldap.conf,v 1.6 2004/02/07 16:58:52 jtournier Exp $
#
# smbldap-tools.conf : Q & D configuration file for smbldap-tools

#  This code was developped by IDEALX (http://IDEALX.org/) and
#  contributors (their names can be found in the CONTRIBUTORS file).
#
#               Copyright (C) 2001-2002 IDEALX
#
#  This program is free software; you can redistribute it and/or
#  modify it under the terms of the GNU General Public License
#  as published by the Free Software Foundation; either version 2
#  of the License, or (at your option) any later version.
#
#  This program is distributed in the hope that it will be useful,
#  but WITHOUT ANY WARRANTY; without even the implied warranty of
#  MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
#  GNU General Public License for more details.
#
#  You should have received a copy of the GNU General Public License
#  along with this program; if not, write to the Free Software
#  Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307,
#  USA.

#  Purpose :
#       . be the configuration file for all smbldap-tools scripts

##############################################################################
#
# General Configuration
#
##############################################################################

# UID and GID starting at...
UID_START="1000"
GID_START="1000"
```

```
# Put your own SID
# to obtain this number do: net getlocalsid  see Step 10
SID="S-1-5-21-272829073-2839789003-218174137"

########################################################################
#
# LDAP Configuration
#
########################################################################

# Notes: to use to dual ldap servers backend for Samba, you must patch
# Samba with the dual-head patch from IDEALX. If not using this patch
# just use the same server for slaveLDAP and masterLDAP.
# Those two servers declarations can also be used when you have
# . one master LDAP server where all writing operations must be done
# . one slave LDAP server where all reading operations must be done
#   (typically a replication directory)

# Ex: slaveLDAP=127.0.0.1
slaveLDAP="127.0.0.1"
slavePort="389"

# Master LDAP : needed for write operations
# Ex: masterLDAP=127.0.0.1
masterLDAP="127.0.0.1"
masterPort="389"

ldapTLS="0"

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

# Where are stored Users
# Ex: usersdn="ou=Users,dc=IDEALX,dc=ORG"
usersdn="ou=Users,dc=vcs,dc=org"

# Where are stored Computers
# Ex: computersdn="ou=Computers,dc=IDEALX,dc=ORG"
computersdn="ou=Computers,dc=vcs,dc=org"

# Where are stored Groups
# Ex groupsdn="ou=Groups,dc=IDEALX,dc=ORG"
groupsdn="ou=Groups,dc=vcs,dc=org"

# Default scope Used
```

```
scope="sub"

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

#######################################################################
#
# Unix Accounts Configuration
#
#######################################################################

# Login defs
# Default Login Shell
# Ex: userLoginShell="/bin/bash"
userLoginShell="/bin/bash"

# Home directory prefix (without username)
# Ex: userHomePrefix="/home/"
userHomePrefix="/home/"

# Gecos
userGecos="System User"

# Default User (POSIX and Samba) GID
defaultUserGid="513"

# Default Computer (Samba) GID
defaultComputerGid="553"

# Skel dir
skeletonDir="/etc/skel"

# Default password validation time (time in days) Comment the next line if
# you don't want password to be enable for defaultMaxPasswordAge days (be
# careful to the sambaPwdMustChange attribute's value)
#defaultMaxPasswordAge="55"

#######################################################################
#
# SAMBA Configuration
#
#######################################################################

# The UNC path to home drives location without the username last extension
# (will be dynamically prepended)
# Ex: \\My-PDC-netbios-name\homes
```

```
# Just set it to a null string if you want to use the smb.conf 'logon home'
# directive and/or desabling roaming profiles
userSmbHome="\\MIDNIGHT-PDC\homes"

# The UNC path to profiles locations without the username last extension
# (will be dynamically prepended)
# Ex: \\My-PDC-netbios-name\profiles\
# Just set it to a null string if you want to use the smb.conf 'logon path'
# directive and/or desabling roaming profiles
userProfile="\\MIDNIGHT-PDC\profiles\"

# The default Home Drive Letter mapping
# (will be automatically mapped at logon time if home directory exist)
# Ex: q(U:) for U:
userHomeDrive="F:"

# The default user netlogon script name
# if not used, will be automatically username.cmd
# make sure script file is edited under dos
userScript="startup.bat"


##############################################################################
#
# SMBLDAP-TOOLS Configuration (default are ok for a RedHat)
#
##############################################################################

# Allows not to use smbpasswd (if with_smbpasswd == 0 in smbldap_conf.pm) but
# prefer mkntpwd... most of the time, it's a wise choice :-)
with_smbpasswd="0"
smbpasswd="/usr/bin/smbpasswd"
mk_ntpasswd="/usr/local/sbin/mkntpwd"
```

Now we need to configure smbldap_bind.conf

so type

gedit smbldap_bind.conf

Edit the information for your site.  My example is below...

Sample /etc/smbldap-tools/smbldap_bind.conf

```
############################
# Credential Configuration #
############################
# Notes: you can specify two differents configuration if you use a
# master ldap for writing access and a slave ldap server for reading access
# By default, we will use the same DN (so it will work for standard Samba
# release)
slaveDN="cn=Manager,dc=vcs,dc=org"
slavePw="secret"
masterDN="cn=Manager,dc=vcs,dc=org"
masterPw="secret"
```

*Note: "secret" is where you put your own password....remember it as you'll be using it again.

**Step 12: Populating the database**

Now we need to populate the data (ldif). This is easy to do....simply type

smbldap-populate

this will run a script that will populate the database with a built-in directory structure. It should just run....any errors and something is amiss.....check your stuff from previous steps.

**Step 13: Setting the Administrator password...**

We also need to set a password and make a tweak for a "special" account... Administrator This account was created when you ran smbldap-populate. It is vital as it is the account that will be used to join Windows machines to the Samba Domain. It must have a uid of "0". One very important thing we need to do is comment out a line in the /etc/samba/smbusers file. To do this let's go to the directory...

cd /etc/samba

and then edit the file

gedit smbusers

find the line that shows ....

root=administrator admin

and comment it out by adding the # symbol

#root=administrator admin
then save and exit.

**Now let's set the password.** To set the password for the Administrator account type...

smbpasswd -a Administrator

and enter a password of your choosing. Don't forget it as you'll need it when you start adding Windows machines to your domain.

### Step 14: Starting Samba

First let's test the samba configs by running...

testparm

if there are no errors (except maybe one where the name is too long for old Win95 and DOS clients...if you don't have any....ignore it) then let's proceed

type:

service smb start

(You may wish to restart ldap too...do that with...)

service ldap restart

### Step 15: Running authconfig to set up authentication of our server

We now need to tell our server to authenticate to the LDAP portion of our server. This can be easily done by running authconfig. There are two versions of authconfig....a GUI version which can be invoked by typing authconfig-gtk or the plain version which is called by typing authconfig

They are very similar....the only difference being that the GUI version is prettier (but less geeky) ;-)

The following pieces need to be selected (checked)

(*) Cache Information

(*) Use LDAP configure LDAP to show Server: 127.0.0.1
Base DN: dc=vcs,dc=org (use your own values)
*Note: Do not select Use TLS!

On the Authentication side (tab) you need to select:

(*) Use Shadow Passwords

(*) Use MD5 Passwords
(*) Enable LDAP  and configure (just check should be all filled in) as above

that's it!  Once you click OK....the service “nscd” should now start.

**Step 16:  Setting up Netlogon and Profiles shares**

Now we need to set up our netlogon and profiles shares.  To do so run the following commands in sequence.

mkdir /opt/samba
mkdir /opt/samba/netlogon
mkdir /opt/samba/profiles
chmod 1777 /opt/samba/profiles

*Note....I am in a public school and the thought of putting the profiles directory in the students home folder give me the chills...especially when kids might figure out how to delete those profiles “by accident”.  Hence the reason I put them in /opt/samba/profiles  But....if you wish you can change this to something like /home/samba/profiles....or whatever...just be sure to change the values in the smbldap.conf, smb.conf, and so forth.  The set up above works very well for us.

Netlogon is where we put the login script that we'll use for when the user logs in to map a directory...set the time or whatever.  This file MUST BE CREATED IN DOS!  The easiest way to do it is to use “notepad” on a windows box....create a file called startup.bat and save it to the floppy.  Then you can take the floppy over to your Samba/LDAP server.....mount it by typing:

mount /dev/fd0 /mnt/floppy

then simply go the the directory and copy it over to /opt/samba/netlogon

cd /mnt/floppy
cp startup.bat /opt/samba/netlogon

Below is a sample of my simple startup.bat file

REM To set the time when the clients logon to the domain:
net time \\10.0.0.234 /set /yes
REM
REM To map a home directory to drive f:
net use f: /home

to unmount the floppy type:

umount /dev/fd0

**Step 17: Setting the services to start when the server starts**

This is being written based on a RedHat or Fedora model. This step may be different for other distributions. Nonetheless....the easy GUI method for making sure the ldap, smb, and nscd services all start when the server is booted....simply go to the GUI....click on the RedHat....find the System Settings menu item....then Server Settings....then Services. On the left find ldap....check the box....and then find smb and check the box....nscd should already be checked. Then click "save". That's it!

OR...from the command line in Terminal....type

chkconfig smb on
chkconfig ldap on

Helpful hint:

Since you need to restart the ldap server when you make config changes...same for samba....I made a quick batch script to restart all my services when I make changes.....it's a lot faster...to do it copy the text below into a file named something like restartservices Make the file executable by typing

chmod a+x restartservices

Here's the script:

```
service ldap restart
service smb restart
service nscd restart
```

**Step 18: Let's create some accounts and do some testing!**

Let's type in this command:

slapcat

You should get a lengthy file of output. If you did....great!

Let's move on...we need to prove the server is really running

ldapsearch -x -b "dc=vcs,dc=org" "(ObjectClass=*)"

More stuff? Should be lots of info there....look it over....you may start to see a little about how the LDAP database works.

Try this command:

getent passwd | grep Administrator

You should see something similar to this:

Administrator:x:998:512:Netbios Domain Administrator:/home:/bin/false

OK!  We're ready to add a user!

Let's run the following commands.....

smbldap-useradd -m -a username

smbldap-passwd username

You'll see:

Changing password for username
New password : XXXXXXXX
Retype new password : XXXXXXXX

now run:

smbpasswd username

You'll see:

New SMB password: XXXXXXXX
Retype new SMB password: XXXXXXXX

*Note:  Put in your own username where it says 'username'...and make up your own password.  Make the password the same in all cases.

Add a couple more users using the same steps if you wish....don't worry..there are faster ways to do this when we get this up and running.

Now let's verify that the Unix (Posix) user can be resolved via NSS.  Try this command:

getent passwd

something similar to this should be the result:

Administrator:x:998:512:Netbios Domain Administrator:/home:/bin/false
nobody:x:999:514:nobody:/dev/null:/bin/false
bobj:x:1000:513:System User:/home/bobj:/bin/bash
stans:x:1001:513:System User:/home/stans:/bin/bash
chrisr:x:1002:513:System User:/home/chrisr:/bin/bash

maryv:x:1003:513:System User:/home/maryv:/bin/bash

Now try:

id username  (username is one of the users you entered)

something like this should result:

uid=1002(chrisr) gid=513(Domain Users) groups=513(Domain Users)

Now let's make certain that a home directory has been created for every user by listing the directories in /home as follows:

Type:

ls -al /home

which should show something similar to this:

```
drwxr-xr-x   8 root   root         176 Dec 17 18:50 ./
drwxr-xr-x  21 root   root         560 Dec 15 22:19 ../
drwx------   7 bobj   Domain Users     568 Dec 17 01:16 bobj/
drwx------   7 chrisr Domain Users     568 Dec 17 01:19 chrisr/
drwx------   7 maryv  Domain Users     568 Dec 17 01:27 maryv/
drwx------   7 stans  Domain Users     568 Dec 17 01:43 stans/
```

The final validation step involves making certain that Samba-3 can obtain the user accounts from the LDAP ldapsam passwd backend.

Type:

pdbedit -Lv username  (where username is one of the accounts you created)

something similar to this should result:

```
Unix username:        chrisr
NT username:          chrisr
Account Flags:        [U          ]
User SID:             S-1-5-21-3504140859-1010554828-2431957765-3004
Primary Group SID:    S-1-5-21-3504140859-1010554828-2431957765-513
Full Name:            System User
Home Directory:       \\MASSIVE\homes
HomeDir Drive:        H:
Logon Script:         chrisr.cmd
Profile Path:         \\MASSIVE\profiles\chrisr
```

Domain: MEGANET2
Account desc: System User
Workstations:
Munged dial:
Logon time: 0
Logoff time: Mon, 18 Jan 2038 20:14:07 GMT
Kickoff time: Mon, 18 Jan 2038 20:14:07 GMT
Password last set: Wed, 17 Dec 2003 17:17:40 GMT
Password can change: Wed, 17 Dec 2003 17:17:40 GMT
Password must change: Mon, 18 Jan 2038 20:14:07 GMT

Now we really do want to confirm that UNIX group resolution from LDAP is functioning as it should.

Type:

getent group

Which should show a long list (cut here) similar to this

Domain Admins:x:512:Administrator
Domain Users:x:513:bobj,stans,chrisr,maryv
Domain Guests:x:514:

The final step we need to validate is that Samba can see all the Windows Domain Groups and that they are correctly mapped to the respective UNIX group account. To do this, type:

net groupmap list

something similar to this should result

Domain Admins (S-1-5-21-3504140859-...-2431957765-512) -> Domain Admins
Domain Users (S-1-5-21-3504140859-...-2431957765-513) -> Domain Users
Domain Guests (S-1-5-21-3504140859-...-2431957765-514) -> Domain Guests

Ok! We're ready!

**Step 19: Adding a Machine account**

Ok, before we move to a Windows machine to try this out...we need to add those machines to the database. To add a machine to LDAP....type the following:

smbldap-useradd -w machinename (where machinename is the name of the computer you wish to add)
Example: smbldap-useradd -w MYPC1

Add more if you wish.

**Step 20: Ok....let's test this puppy out!**

Go to a windows machine and try to join the machine to the domain. Don't forget the username is Administrator and the password you assigned for that account. Once you've joined the machine to the domain you'll need to restart...and then try to log in! If it works you're all set!

# Additional Notes about setting up clients and so forth

**Roaming/Roving profiles**

When a Microsoft Windows NT/2K/XP user joins the SAMPLE-NT domain, his profile is stored in the directory defined in the profile section of the samba configuration file. He has to log out for this to be saved. This is a roaming profile: he can use this profile from any computer he wants, hence the name "roaming profiles". Roaming profiles are very useful as they consist of user data such as "Favorites", "History", desktop wallpaper, "My Documents", and more. If a users personal configuration changes, it will be integrated in his roaming profile.

In this Howto, we used roaming profiles: the LDAP ProfilePath indicate to Samba where to look for those roaming profiles…example: (SAMPLE-PDC\profiles\testsmbuser2) and the [profiles] section of the /etc/samba/smb.conf indicates to samba how to deal with profiles.

**Mandatory profiles**

The mandatory profile is created the same way as the roaming profile. The difference is

that this profile is made 'read only' by the administrator so that the user can have only one fixed profile on the domain.

## My favorite way to do this:

First, on the Samba/LDAP server create a directory

mkdir /opt/samba/profiles/default user

On a Windows machine....log in as a user you created. Spend some time and create the perfect base profile with all the appropriate icons, bookmarks, wallpaper...etc. Then log out. Then log back in...and back out again...we want some files to be generated. Now log back in as the local machine Administrator. Browse to "Documents and Settings" and find the local profile for that user you were just working with. Search for and destroy any instances within that folder of desktop.ini (very annoying). Now using Network neighborhood....copy the contents of the profile on the local machine to the default user folder on the server. (If you can't access this folder via Network Neighborhood you may need to create a share in smb.conf.....hence my share called "whole-linux-server"...see my sample smb.conf above) Make the directory read only to the average user....this will now be the base profile

that everyone starts out with.

You can also do.....

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

mv /opt/samba/profiles/testsmbuser1/NTUSER.DAT

/opt/samba/profiles/testsmbuser1/NTUSER.MAN

chmod -w /opt/samba/profiles/testsmbuser1/NTUSER.MAN

A Mandatory profile allows you to set up a common user profile for every user on the Domain…useful to give everyone a common starting point or for specifying specific settings without having to do so for each user.

**Logon Scripts**

To use Logon Scripts (.BAT or .CMD), just specify the relative path from the netlogon share to the command script desired in the scriptPathattribute for the user. This is done easily in the program Directory Administrator or other GUI LDAP Manager.

**NFS Exports**

We will set up NFS to export the home directories so Linux users will access the same home directories as Windows/Samba users.

1. Add the following line to /etc/exports

/home 192.168.0.0/24(rw) use your own IP addresses on this line

2. Restart the NFS services

service nfs restart

**Another method:**

On your file/ldap server, add the following lines to /etc/exports

/home 10.1.2.3/255.255.255.255(rw)

Replace "10.1.2.3" with the IP address of the "client" server. You can

spec a whole range of course, such as "10.0.0.0/255.0.0.0" for all of

the 10.x.x.x addresses.

Now run "exportfs -a".

Also double-check that you are not firewalling off access to NFS & portmap

(UDP ports 111 & 2049).

**Client Set-Up**

***Linux Client (local hard drive…NOT an LTSP or K12LTSP terminal)***

To set up a linux client to use the primary domain controller for authentication and home directory, do the following:

**Automounter**

Configure the automounter to mount the home directories as needed.

1. Edit /etc/auto.master add:
2. /home /etc/auto.homes --timeout=60
3. Edit /etc/auto.homes
4. * 192.168.0.1:/home/& you should use your own IP addresses
5. Restart the automounter:

service autofs restart

***Windows 98***

Adding a windows 98 box to the domain is exactly the same as adding a windows 98 box to a NT/2000/XP domain.

1. Open the network control panel
2. Select ``client for Microsoft networks" and click ``properties."
3. Select ``log on to windows NT domain"
4. Enter domain name (SAMPLE-NT)
5. Restart the computer

LDAP or not LDAP?

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

**RequireSignOrSeal (this may be fixed in Samba 3, but I'm not sure....it doesn't hurt)**

This registry key (gathered from the Samba-tng lists) is needed for Windows 2000 and XP clients to join and logon to a Samba domain

It is suggested that you check the following registry entries which should be set to (0). This is the default under W2K (but check to confirm) however under XP the default is (1) and definitely needs changing:

**[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Netlogon\Parameters]**
**"requirestrongkey"=dword:00000000**
**"requiresignorseal"=dword:00000000**
**[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services\Netlogon\Parameters]**
**"requirestrongkey"=dword:00000000**
**"requiresignorseal"=dword:00000000**
**[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters]**
**"requirestrongkey"=dword:00000000**
**"requiresignorseal"=dword:00000000**

You can change this in the Local or Domain policy editor in Windows 2000/XP. (regedit)