Configure Samba with ACL and Active Directory integration

Robert LeBlanc (leblanc@byu.edu)
BioAg Computer Support, Brigham Young University

This document uses Debain Linux 3.1 (Sarge) on x86 hardware. Your mileage may very. This document is intended to help others wanting to set-up a Linux server to participate in an Active Directory environment as a Samba file server. I am not responsible for any damage done to your computer or network due to following this document. It has worked well in our environment. I suggest testing on a non-production machine before putting into production.

Enough of that, lets get into the good stuff. The document is pretty bare without a lot of explanation. If you wish to add some explanations to the document, please send me the comments and I will add them in for others.

Install needed packages:

```
apt-get update
apt-get install samba krb5-config krb5-user winbind acl ntp-server ntpdate \
                    xfsprogs attr quota
```

Edit Samba config (/etc/samba/smb.conf):

```
----------------Start /etc/samba/smb.conf---------------------
#
# Sample configuration file for the Samba suite for Debian GNU/Linux.
#
#
# This is the main Samba configuration file. You should read the
# smb.conf(5) manual page in order to understand the options listed
# here. Samba has a huge number of configurable options most of which
# are not shown in this example
#
# Any line which starts with a ; (semi-colon) or a # (hash)
# is a comment and is ignored. In this example we will use a #
# for commentary and a ; for parts of the config file that you
# may wish to enable
#
# NOTE: Whenever you modify this file you should run the command
# "testparm" to check that you have not many any basic syntactic
# errors.
#

#======================= Global Settings =======================

[global]

## Browsing/Identification ###

# Change this to the workgroup/NT-domain name your Samba server will part of
   workgroup = BA
   realm = BA.BYU.EDU
   password server = alfred.ba.byu.edu

# server string is the equivalent of the NT Description field
   server string = %h server (Samba %v)

# Windows Internet Name Serving Support Section:
```

```
# WINS Support - Tells the NMBD component of Samba to enable its WINS Server
;   wins support = no

# WINS Server - Tells the NMBD components of Samba to be a WINS Client
# Note: Samba can be either a WINS Server, or a WINS Client, but NOT both
;   wins server = w.x.y.z

# This will prevent nmbd to search for NetBIOS names through DNS.
   dns proxy = no

# What naming service and in what order should we use to resolve host names
# to IP addresses
;   name resolve order = lmhosts host wins bcast


#### Debugging/Accounting ####

# This tells Samba to use a separate log file for each machine
# that connects
   log file = /var/log/samba/log.%m

# Put a capping on the size of the log files (in Kb).
   max log size = 1000

# If you want Samba to only log through syslog then set the following
# parameter to 'yes'.
;   syslog only = no

# We want Samba to log a minimum amount of information to syslog. Everything
# should go to /var/log/samba/log.{smbd,nmbd} instead. If you want to log
# through syslog you should set the following parameter to something higher.
   syslog = 0

# Do something sensible when Samba crashes: mail the admin a backtrace
   panic action = /usr/share/samba/panic-action %d


####### Authentication #######

# "security = user" is always a good idea. This will require a Unix account
# in this server for every user accessing the server. See
# /usr/share/doc/samba-doc/htmldocs/ServerType.html in the samba-doc
# package for details.
;   security = user
   security = ADS

# You may wish to use password encryption.  See the section on
# 'encrypt passwords' in the smb.conf(5) manpage before enabling.
   encrypt passwords = true

# If you are using encrypted passwords, Samba will need to know what
# password database type you are using.
   passdb backend = tdbsam guest

;   obey pam restrictions = yes

;   guest account = nobody
   invalid users = root

# This boolean parameter controls whether Samba attempts to sync the Unix
# password with the SMB password when the encrypted SMB password in the
# passdb is changed.
;   unix password sync = no

# For Unix password sync to work on a Debian GNU/Linux system, the following
# parameters must be set (thanks to Augustin Luton <aluton@hybrigenics.fr> for
# sending the correct chat script for the passwd program in Debian Potato).
   passwd program = /usr/bin/passwd %u
   passwd chat = *Enter\snew\sUNIX\spassword:* %n\n *Retype\snew\sUNIX\spassword:* %n\n .
```

```
# This boolean controls whether PAM will be used for password changes
# when requested by an SMB client instead of the program listed in
# 'passwd program'. The default is 'no'.
;   pam password change = no


########## Printing ##########

# If you want to automatically load your printer list rather
# than setting them up individually then you'll need this
;   load printers = yes

# lpr(ng) printing. You may wish to override the location of the
# printcap file
;   printing = bsd
;   printcap name = /etc/printcap

# CUPS printing.  See also the cupsaddsmb(8) manpage in the
# cupsys-client package.
;   printing = cups
;   printcap name = cups

# When using [print$], root is implicitly a 'printer admin', but you can
# also give this right to other users to add drivers and set printer
# properties
;   printer admin = @ntadmin


######## File sharing ########

# Name mangling options
;   preserve case = yes
;   short preserve case = yes


############ Misc ############

# Using the following line enables you to customise your configuration
# on a per machine basis. The %m gets replaced with the netbios name
# of the machine that is connecting
;   include = /home/samba/etc/smb.conf.%m

# Most people will find that this option gives better performance.
# See smb.conf(5) and /usr/share/doc/samba-doc/htmldocs/speed.html
# for details
# You may want to add the following on a Linux system:
#         SO_RCVBUF=8192 SO_SNDBUF=8192
   socket options = TCP_NODELAY

# The following parameter is useful only if you have the linpopup package
# installed. The samba maintainer and the linpopup maintainer are
# working to ease installation and configuration of linpopup and samba.
;   message command = /bin/sh -c '/usr/bin/linpopup "%f" "%m" %s; rm %s' &

# Domain Master specifies Samba to be the Domain Master Browser. If this
# machine will be configured as a BDC (a secondary logon server), you
# must set this to 'no'; otherwise, the default behavior is recommended.
;   domain master = auto
   domain master = no

# Some defaults for winbind (make sure you're not using the ranges
# for something else.)
;   idmap uid = 10000-20000
;   idmap gid = 10000-20000
;   template shell = /bin/bash
   winbind uid = 10000-20000
   winbind gid = 10000-20000
   winbind enum groups = yes
   winbind enum users = yes
   winbind use default domain = yes
   winbind separator = +

#======================= Share Definitions =======================

#[homes]
#   comment = Home Directories
#   browseable = no

[shared folder]
   comment = My Shared Folder
   browseable = yes
   guest ok = no
   writeable = yes
   create mask = 0700
   directory mask = 0700
   path = /ifolder
   admin users = BA\domain admins


# By default, the home directories are exported read-only. Change next
# parameter to 'yes' if you want to be able to write to them.
#   writable = no

# File creation mask is set to 0700 for security reasons. If you want to
# create files with group=rw permissions, set next parameter to 0775.
;   create mask = 0700

# Directory creation mask is set to 0700 for security reasons. If you want to
# create dirs. with group=rw permissions, set next parameter to 0775.
;   directory mask = 0700

# Un-comment the following and create the netlogon directory for Domain Logons
# (you need to configure Samba to act as a domain controller too.)
;[netlogon]
;   comment = Network Logon Service
;   path = /home/samba/netlogon
;   guest ok = yes
;   writable = no
;   share modes = no

;[printers]
;   comment = All Printers
;   browseable = no
;   path = /tmp
;   printable = yes
;   public = no
;   writable = no
;   create mode = 0700

# Windows clients look for this share name as a source of downloadable
# printer drivers
;[print$]
;  comment = Printer Drivers
;  path = /var/lib/samba/printers
;  browseable = yes
;  read only = yes
;  guest ok = no
# Uncomment to allow remote administration of Windows print drivers.
# Replace 'ntadmin' with the name of the group your admin users are
# members of.
;   write list = root, @ntadmin

# A sample share for sharing your CD-ROM with others.
;[cdrom]
;   comment = Samba server's CD-ROM
;   writable = no
;   locking = no
;   path = /cdrom
;   public = yes
```

```
# The next two parameters show how to auto-mount a CD-ROM when the
#           cdrom share is accesed. For this to work /etc/fstab must contain
#           an entry like this:
#
#      /dev/scd0   /cdrom  iso9660 defaults,noauto,ro,user   0 0
#
# The CD-ROM gets unmounted automatically after the connection to the
#
# If you don't want to use auto-mounting/unmounting make sure the CD
#           is mounted on /cdrom
#
;   preexec = /bin/mount /cdrom
;   postexec = /bin/umount /cdrom


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

testparm

Edit the /etc/pam.d/samba file to allow samba authentication. Order is important!

```
---------------Start /etc/pam.d/samba----------------------------
@include common-auth
auth          required   pam_winbind.so
@include common-account
account    required   pam_winbind.so
@include common-session

---------------End /etc/pam.d/samba-----------------------------
```

Edit the /etc/nsswitch.conf file to get information from winbind that gets the information from Active Directory

```
---------------Start /etc/nsswitch.conf----------------------------
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:         compat winbind
group:          compat winbind
shadow:         compat winbind

hosts:          files dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis

---------------End /etc/nsswitch.conf-----------------------------
```

Edit the Kerberos settings in /etc/krb5.conf

```
---------------Start /etc/krb5.conf---------------------------------
[libdefaults]
        default_realm = BA.BYU.EDU

[realms]
BA.BYU.EDU = {
        default_domain = ba.byu.edu
         kdc = alfred.ba.byu.edu
         kdc = gordon.ba.byu.edu
         kdc = maridian.ba.byu.edu
         kdc = robin.ba.byu.edu
        admin_server = alfred.ba.byu.edu
}

[domain_realm]
        .ba.byu.edu=BA.BYU.EDU
        ba.byu.edu=BA.BYU.EDU

-------------------End /etc/krb5.conf------------------------------
```

Configure ntp so that time drift between Linux and Windows Domain controllers stays less then 5 minutes apart. Add ntp server entries into /etc/ntp.conf and run ntpdate to get the clock synchronized now (apt-get may already have done this), then run the ntp daemon to keep it there.

```
/etc/init.d/ntp-server stop
ntpdate pool.ntp.org
/etc/init.d/ntp-server start
```

Now that all the files are edited create a Kerberos ticket:

```
kinit robert
```

And enter password

You should see that the ticket has been created. Join the Linux machine to the domain

```
net ads join –U robert
```

The machine should become a member of the domain. Start up the winbind and samba daemons.

```
/etc/init.d/winbind force-reload && /etc/init.d/samba force-reload
```

Check to see that you can see all the domain users and groups and that the environment is being mapped correctly. **It may take a half hour or more for changes to replicate in domains that have sites!**

```
wbinfo –u
wbinfo –g
getent passwd
getent group
```

Set-up the directory to have as the shared space with ACL enabled.

```
cfdisk /dev/sdb
mkfs.xfs /dev/sdb1
```

Add the mount point to /etc/fstab and mount. Use setfacl to configure the permissions for the directories.

```
setfacl –m g:domain\ admins:rwx shared_folder
setfacl –m default:g:domain\ admins:rwx shared_folder
setfacl –m default:g:domain\ users:rx shared_folder
getfacl test_folder
```

Add additional permissions as necessary. Most other permissions can be added by a Windows workstation and don't require command line interaction. Windows needs the default ACLs to work properly. This document does not show the use of quotas even though quota was installed at the start of the document.