

Samba

Samba is an open source program which allows file sharing between Linux and Windows. Samba can also be setup as a Domain Controller, providing services that a windows active directory server could provide. This document covers setup procedures for samba as a PDC with and without ldap, a domain member and shows how to mount windows shares on a linux box using smb tools.

Contents

Samba for PDC without LDAP	1
Join Samba server to Windows domain.....	4
Integrate to AD 2003.....	5
Samba integrated with LDAP	Error! Bookmark not defined.
Mount Windows share on Linux	6

Samba for PDC without LDAP

```
[global]
    workgroup = ANANDHACORP
    netbios name = NAUSICAA
    server string = Nausicaa Samba Server
    passdb backend = tdbsam
    security = user
    pam password change = yes
    password level = 2
    username level = 2
    log level = 2
    log file = /var/log/samba/samba.log
    max log size = 100
    logon path = \\%L\profiles\%u\%m
    logon script = %U.bat
    logon drive = M:
    domain logons = yes
    os level = 33
    preferred master = yes
    domain master = yes
    hosts allow = 192.168.1., 127.
```

```
[homes]
    comment = Home Directories
    read only = No
    browseable = No
```

```
[user_acc]
    comment = User Account Only Admin
    path = /home/users
    read only = No
    create mask = 03777
    directory mask = 02777
    browseable = No
```

```
[netlogon]
    comment = Network Logon Service
    path = /usr/local/samba/lib/netlogon
    write list = @domadm
    guest ok = Yes
    share modes = No
```

```
[profiles]
  path = /profiles
  read only = No
  create mask = 0600
  directory mask = 0700
  profile acls = Yes
  browseable = No
```

You must first add the root user – this is the administrator

```
smbpasswd root
Password: *****
```

Join to domain as PDC

```
net join
Password: ****
Welcome to domain
```

Global policy settings

Changes settings such as password expiry date, length and logon attempts much be changed before users are added to the samba database

Using the pbedit command the following polices can be created

```
pbedit -P "min password length" -C 8
pbedit -P "minimum password age" -C 3888000
pbedit -P "bad lockout attempt" -C 3
```

Group configuration

net groupmap list – to see which groups are predefined.

Before users and groups are added to samba they must exist in /etc/passwd and /etc/passwd.

```
groupadd nausadmin
useradd -gnausadmin -c"ananth anandhakrishnan" -d/home/ananth ananth
```

Then in samba you can assign user groups a group role

Adding groups:

```
net groupmap modify ntgroup="Domain Admins" unixgroup=nausadmin
```

This will assign the group a RID: eg. 512

Adding users:

```
smbpasswd -a ananth
```

pbedit -Lv ananth to check to ensure the RID is 512

also add all computers as domain machines

```
net groupmap add ntgroup="Domain Computers" unixgroup=workstation rid=515
type=d
```

add root as domain controller

```
net groupmap add ntgroup="Domain Controllers" unixgroup=root rid=516 type=d
```

- net groupmap modify might need to be used for certain groups.

after adding worstations to unix group add machines in the following way

```
useradd -gworkstations serfina$
smbpasswd -ma serfina$
```

Table 11.1. Well-Known User Default RIDs

Well-Known Entity	RID	Type	Essential
Domain Administrator	500	User	No
Domain Guest	501	User	No
Domain KRBTGT	502	User	No
Domain Admins	512	Group	Yes
Domain Users	513	Group	Yes
Domain Guests	514	Group	Yes
Domain Computers	515	Group	No
Domain Controllers	516	Group	No
Domain Certificate Admins	517	Group	No
Domain Schema Admins	518	Group	No
Domain Enterprise Admins	519	Group	No
Domain Policy Admins	520	Group	No
Builtin Admins	544	Alias	No
Builtin users	545	Alias	No
Builtin Guests	546	Alias	No
Builtin Power Users	547	Alias	No
Builtin Account Operators	548	Alias	No
Builtin System Operators	549	Alias	No
Builtin Print Operators	550	Alias	No
Builtin Backup Operators	551	Alias	No
Builtin Replicator	552	Alias	No
Builtin RAS Servers	553	Alias	No

To ensure the user gets the correct login script
 logon script = %U.bat where U = username or groupname – depending on how many people you have on your network. Group would be the better choice.
 BDC

Smb.conf for backup PDC

```
[global]
  workgroup = ANANDHACORP
  server string = serfina
  security = domain
  password server = 192.168.1.101
  passdb backend = tdbsam
  pam password change = yes
  password level = 8
  username level = 8
  log file = /var/log/samba/smbd.log
  max log size = 500
  logon script = %G.bat
  logon path = \\%N%\%u
  domain logons = Yes
  os level = 33
  preferred master = No
  local master = No
  domain master = No
```

```
dns proxy = No
```

You should also setup all the same shares as the PDC

Set the SID of the BDC as the same as the PDC

```
nausicaa –
```

```
net rpc getsid
```

Storing SID S-1-5-21-2160242107-1482373154-96390633 for Domain ANANDHACORP in secrets.tdb

```
net rpc setsid S-1-5-21-2160242107-1482373154-96390633
```

Join Samba server to Windows domain

Referencing to: http://www.linux-sxs.org/networking/nt4dom_samba.html
http://www.richard-york.com/blog/linux/ad_integration.html

NT4 Domain

To join a samba client built in Linux to a windows domain, the following changes must be made.

* backup all files before continuing.

To allow unified login under the windows domain Winbind needs to be enabled.

Winbind is the unix implementation of Microsoft RPC protocol which uses Name service switch for identity resolution and pluggable authentication modules for user authentication. Winbind maintains a database which has mappings between UNIX SID GID's and NT SID AND GID's.

NSS /etc/nsswitch.conf serves as a lookup for services such as DNS, email and SID/GID. In this file a function can be tied down to a service, for example passwd can be managed by winbindd or nis, or hostname can be managed by dns. The C library looks in this file to see which service to use.

Make changes /etc/nsswitch.conf

```
passwd:          files    winbind
shadow:         files    winbind
group:          files    winbind
```

Through PAM winbind allows user passwords to be kept at a central location – Active directory. No need for synchronisation.

make changes to /etc/pam.d/login

```
##PAM-1.0
auth      required      pam_securetty.so
auth      sufficient    pam_winbind.so
auth      required      pam_stack.so service=system-auth
auth      required      pam_nologin.so
account   sufficient    pam_winbind.so
account   required      pam_stack.so service=system-auth
password  required      pam_stack.so service=system-auth
# pam_selinux.so close should be the first session rule
session   required      pam_selinux.so close
session   required      pam_stack.so service=system-auth
session   required      pam_loginuid.so
session   optional     pam_console.so
# pam_selinux.so open should be the last session rule
session   required      pam_selinux.so multiple open
```

make changes to the `smd.conf` file so it includes the Windows domain information

```
wins server = 192.168.1.10
  workgroup = TEMASEK # domain name

winbind separator = +
  winbind uid = 10000-20000
  winbind gid = 10000-20000
  winbind enum users = yes
  winbind enum groups = yes
  winbind use default domain = yes
  template homedir = /home/winnt/%D/%U
  template shell = /bin/bash

  idmap uid = 16777216-33554431
  idmap gid = 16777216-33554431
```

start services

```
/sbin/service smb start
/sbin/service winbind start
```

Attempt to join the machine to the domain.

```
net rpc join -W TEMASEK -U - where the user is an administrator of the domain.
```

If you have a large domain and a large number of account, it may take quite a long time to get the password prompt to come up.

Once joined to the domain you can try accessing shares on the Linux machine of a windows client by browsing the host name or ip address `//192.168.1.101` or `//nausicaa`

By using `wbinfo` tools you can check to make sure you have joined the domain successfully.

Integrate to AD 2003

Active Directory uses LDAP and Kerberos for authentication. Linux also has LDAP and Kerberos support to integrate machines into a windows domain and also to act as a primary domain controller with windows machines attached.

From command line run: `authconfig-tui`

On the first screen tick use Kerberos password under authentication.

On the next screen enter Kerberos realm, KDC and admin servers

```
REALM= DOMAIN.LOCAL
KDC=pcd.domain.local:88
ADMIN_SERVER=pcd.domain.local:749
```

This will add entries in `/etc/krb5.conf` and `/etc/krb.conf`

Smb.conf settings

```

[global]
#--authconfig--start-line--

# Generated by authconfig on 2008/06/26 21:18:47
# DO NOT EDIT THIS SECTION (delimited by --start-line--/--end-line--)
# Any modification may be deleted or altered by authconfig in future

    workgroup = DOMAIN
    password server = pdc.domain.local:88
    realm = DOMAIN.LOCAL
    security = ADS
    idmap uid = 16777216-33554431
    idmap gid = 16777216-33554431
    winbind separator = _
    template shell = /bin/ksh
    winbind use default domain = true
    winbind offline logon = false

#--authconfig--end-line--
    server string = Linux Samba Server %v
    passdb backend = tdbsam
    winbind enum users = Yes
    winbind enum groups = Yes
    winbind normalize names = Yes
    cups options = raw
    # disable master browser
    domain master = No

[homes]
    comment = Home Directories
    read only = No
    browseable = No
    # Expose these for Subversion access
    hide dot files = No

```

to join: start smb services then type the following command
net ads join -Uadministrator - enter the windows ADS password for authentication
ensure the time on this server is sync'd with the domain server otherwise connection will fail.

Mount Windows share on Linux

To test to see if the Linux machine sees the shares on the Windows box:
smbclient -L andromida-U ananth

Make a directory for the mountpoint:
mkdir /mnt/windows

Mount the share:
mount -t smbfs //andromida/downloads /mnt/windows

Try cifs if smbfs doesnt work - FC5 is not shipped with smbfs

Create a symbolic link to the mounted drive:
ln -s /mnt/<name-of-mount-point> /<path-of-symlink>