Linuxdays 2005, Samba Tutorial

Alain Knaff
alain.knaff@linux.lu

Summary

- 1. Installing
- 2. Basic config (defining shares, ...)
- 3. Operating as a PDC
- 4. Password synchronization
- 5. Access control
- 6. Samba variables
- 7. Advanced printing
- 8. LDAP Backend
- 9. Misc gimmicks

1. Installing (smb.conf)

- Samba 3.0.10-1
  - `apt-get install samba`
  - `apt-get install smbclient`
- Slapd 2.1.30-3
- GQ 1.0beta1
  - `apt-get install gq`

2. Basic config (smb.conf)

- Sections, introduced by [*sectionName*]
- Global section: settings apply to all shares
- Share section: settings apply to one share
- Reserved sections/shares: `printers`, `netlogon`, ...
- User management

Basic config. Global parameters

- workgroup
- printing
  - plp
  - lprng
  - cups
  - ...
- security
  - user
  - domain
  - share

Basic config. Share specific parameters

- comment
- browseable
- public
- read only
- available

Basic config. File Share

- `path`

Basic config. Printer share

- `printable = yes`
- `printer = hp4550`
- `path`

Basic config. General Printers share

- `load printers = yes`
- `[printers]`

Basic config. User management

- `encrypt password = yes`
- `passdb backend = smbpasswd`
- different passwords db for Unix and Windows clients:

  `/etc/samba/smbpasswd` file
- Add a Windows user: `smbpasswd -a`
- `guest user = nobody`
- map Windows users to Unix users:

  `username map = /etc/samba/user.map`
- Username map example:

```
root = admin administrator
tridge = "Andrew Tridgell"
```

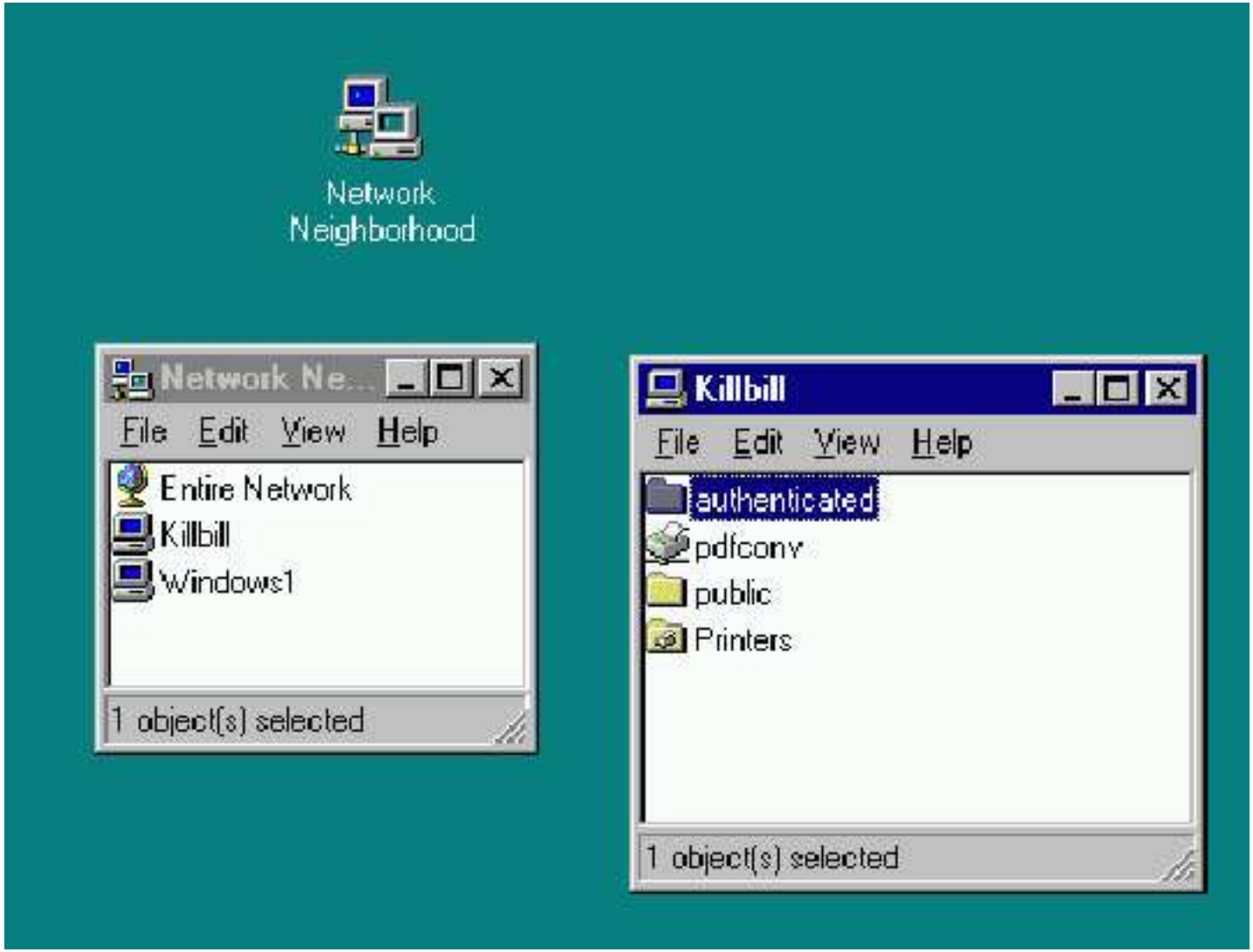
Basic config. Testing

- `testparm`
- `smbclient -L server -U user`
- `smbclient //server/share -U user`
- Log files in `/var/log/samba`

Basic config. Example

```
[global]
        workgroup = samba
        printing = cups
        cups options = "raw,media=a4"
        load printers = yes
        encrypt passwords = yes
        log level = 3
[public]
        comment = A Test Share
        browseable = yes
        public = yes
        read only = yes
        path = /samba/public
[authenticated]
        comment = An authenticated share
        browseable = yes
        read only = no
        path = /samba/auth

[printers]
        comment = Printers share
        printable = yes
```

Basic config. Windows screen shot



3. Primary domain controller

- Global settings
- Netlogon share
- Profile directory

PDC: global settings

- Enable PDC: `domain logons = yes`
- Security: `security = user`
- "Guest" users: `map to guest = Never`
- Workgroup parameter is interpreted as domain
- Set up as wins server: `wins support = yes`
- Script for creating machine accounts:

```
add machine script=/usr/sbin/useradd -d / -G '' -g 100 -s /bin/false -M %u
```

- Drive letter for home directory: `logon drive = "H:"`
- Home directory share:`[homes]`

```
        writable = yes
```

PDC: startup script

- Define a netlogon share
- `logon script = "STARTUP.BAT"`

PDC: profile storage

- Windows 95/98: `logon home`
- Windows NT/2000/XP: `logon path`

Who may add machines to the domain?

- Normally only root (remove `invalid users = root` line, if present)
- You may specify more users using the `IPC$` share:

```
[IPC$]
    admin users = admin root winjoin aknaff
    path = /ipc
```

PDC: Domain administrator

- Domain user
- Has administrative privileges on all clients
- No particular privileges on server
- Set up using the following command:

```
net groupmap modify ntgroup="Domain Administrators" unixgroup=ntadmin
```

- ==> All users in ntadmin group have admin privileges

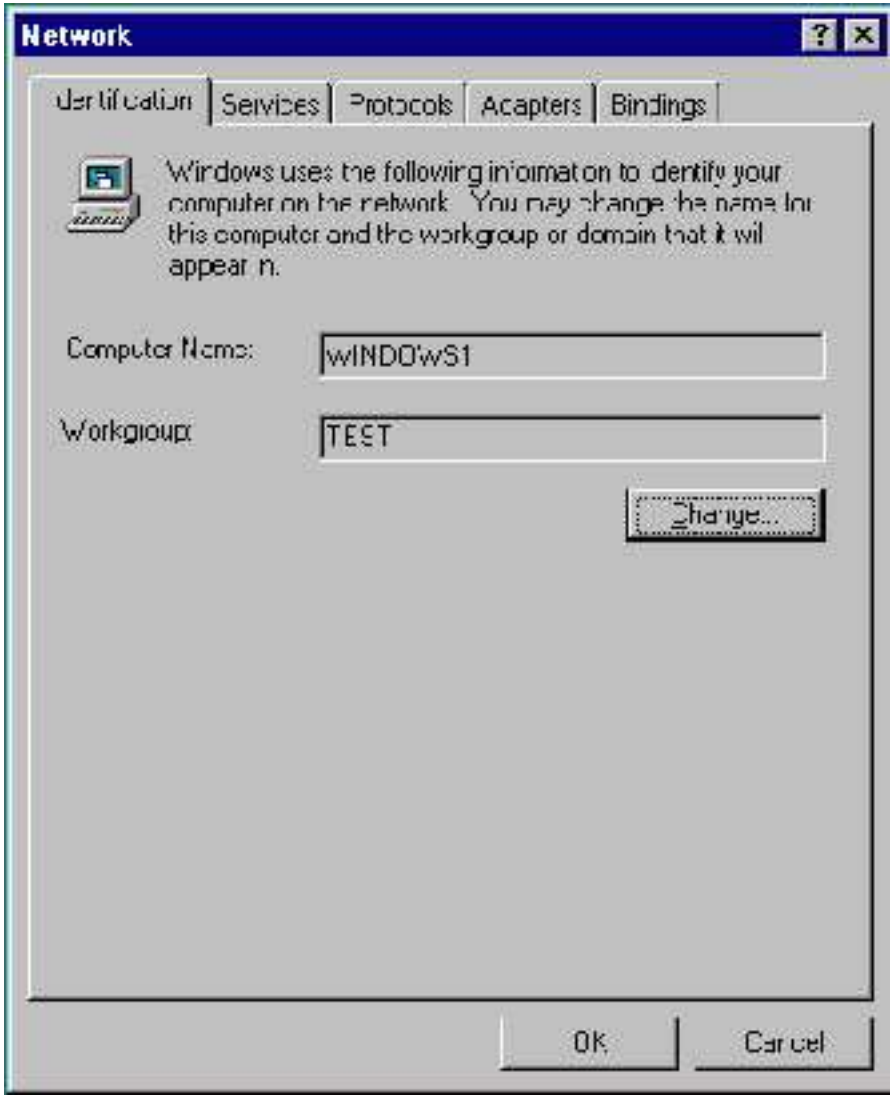
PDC: example

```
[global]
## Browsing/Identification ###

# Change this to the workgroup/NT-domain name your Samba server will part of
   workgroup = belgium
   domain logons = yes
   security = user
   encrypt passwords = yes
   add machine script = /usr/sbin/useradd -d / -G '' -g 100 -s /bin/false %u

   printing = cups
   cups options = "raw,media=a4"
   load printers = yes
   username map = /etc/samba/user.map
...
# Windows Internet Name Serving Support Section:
# WINS Support - Tells the NMBD component of Samba to enable its WINS Server
   wins support = yes
```

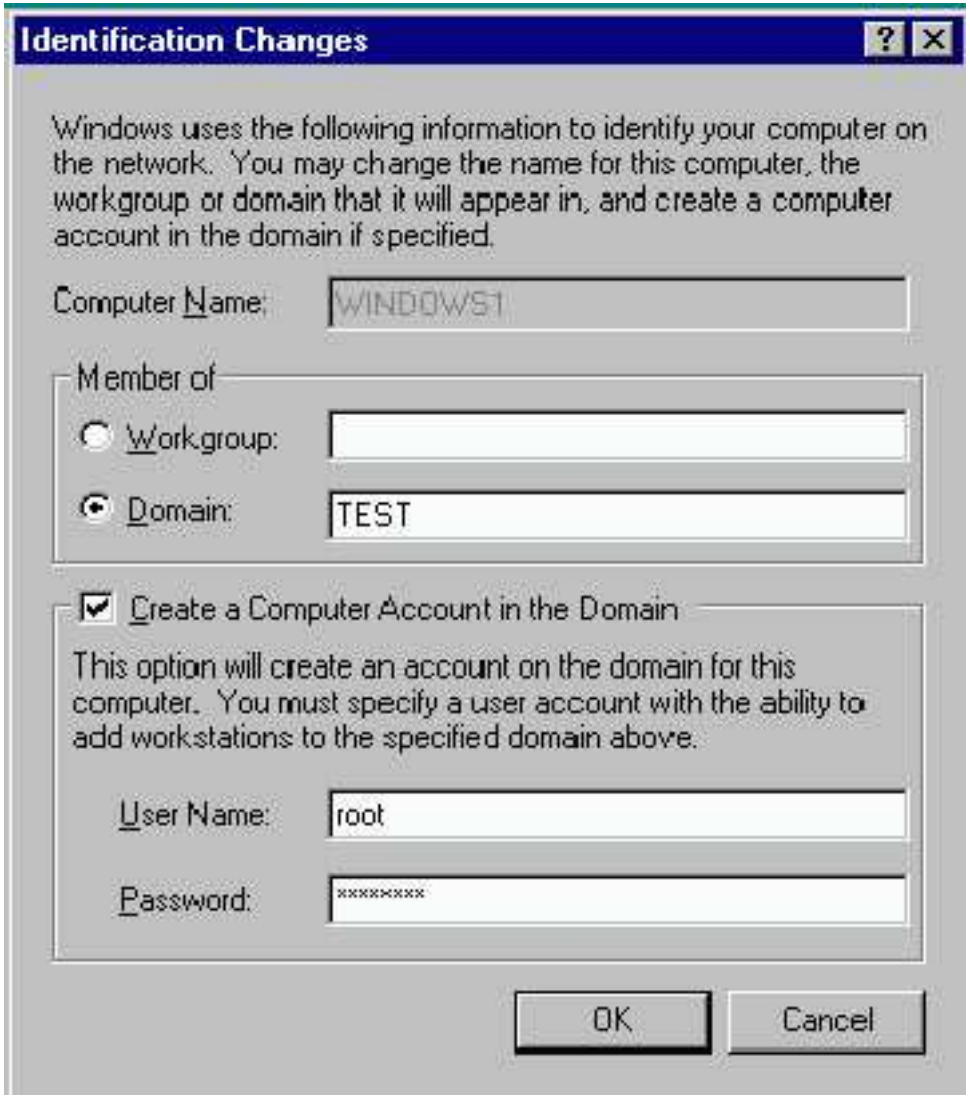
PDC: example (cont’d)

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

# 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 = yes
...
```

PDC: setting up the client



PDC: setting up the client



4. Password synchronization

- Global settings
- Unix pass follows windows: `/etc/pam.d/samba`
- Windows pass follows Unix: `/etc/pam.d/passwd`

Password synchro: global settings

- `unix password sync = Yes`
- `pam password change = Yes`

- N.B. You need to (temporarily) disable LDAP in `/etc/pam.d/common-password` to have this work

Password synchro: /etc/pam.d/samba

```
@include common-auth
@include common-account
@include common-session
@include common-password
```

- Test with `smbpasswd -r localhost -U tata`

Password synchro: /etc/pam.d/passwd

(Not supported in Debian, SuSE example):

```
auth     required  pam_unix2.so    nullok
account  required  pam_unix2.so
password required  pam_pwcheck.so  nullok
password required  pam_unix2.so    nullok use_first_pass use_authtok
password required  pam_smbpass.so  nullok try_first_pass use_authtok
session  required  pam_unix2.so
```

Debian solutions:

- Compile samba yourself
- Symlink /usr/bin/passwd to smbpasswd

5. Access control

- By user
- By IP
- Controlling Unix rights once access is granted

Access control: by user

- Users who can/cannot access:
  - `valid users`
  - `invalid users`
  - invalid users takes precedence
- Users who can/cannot write:
  - `write list`
  - `read list`
  - write list takes precedence
- All-mighty users:
  - `admin users`

Access control: by IP

- `hosts deny`
- `hosts allow`
- allow takes precedence

Access control: Unix rights

- User/group
  - `force user`
  - `force group`
- Permission bits on creation
  - maximal [AND]: `(directory|create) mask`
  - minimal [OR]: `force (directory|create) mode`
- Permission bits for chmod
  - `[directory] security mask`
  - `force [directory] security mode`
- Write access implies chmod access:
  - `dos filemode = yes`

6. Samba variables

- `%U` user name requested
- `%u` user name granted (after force)
- `%G` primary group of `%U`
- `%g` primary group of `%u`
- `%H` home directory of `%u`
- `%m` NetBIOS name of client machine
- `%I` IP of client
- `%a` Win variant of client (WfWg, Win95, WinNT, Win2k, ...)
- `%L` name of the server

- Example:

```
logon path = \\\\%L\\%U\\profile.%a
```

7. Advanced printer support

- `add printer command`: script to add a printer to printcap
- `enumports command`: script listing all current printers
- `printer admin = joe`: adds joe as administrator for printer share
- `show add printer wizard = yes`

8. LDAP backend

- Goal: Store user information in LDAP
- Useful for if user database
  - is huge
  - changes frequently
  - must be distributed across several hosts
- Allows to specify some settings per user, which would normally be global:
  - profile path
  - startup script

LDAP backend: openldap config

- Install samba.schema and call it from slapd.conf
- `http://samba.org/~jerry/patches/post-3.0.6/samba.schema`
- `include /etc/ldap/schema/samba.schema`
- Create a samba-specific object tree:

```
com---tux-industries---belgium----Group
                                  |
                                  |--Samba---Group
                                  |
                                  |--Samba---Idmap
                                  |
                                  |--Samba---Machine
```

LDAP backend: openldap config

- Security:

```
access to attribute=sambaLMPassword
        by dn="cn=admin,dc=belgium,dc=tux-industries,dc=com" write
        by self write
        by * none

access to attribute=sambaNTPassword
        by dn="cn=admin,dc=belgium,dc=tux-industries,dc=com" write
        by self write
        by * none
```

LDAP backend: samba config

- Enter the following into `/etc/samba/smb.conf` :

```
passdb backend = ldapsam:ldap://localhost
idmap backend = ldap:ldap://localhost
ldap admin dn = cn=admin,dc=belgium,dc=tux-industries,dc=com
ldap ssl = on
ldap filter = (cn=%u)
ldap suffix = dc=belgium,dc=tux-industries,dc=com
ldap user suffix = ou=People
ldap group suffix = ou=Group
ldap idmap suffix = ou=Idmap,ou=Samba
ldap machine suffix = ou=Machine,ou=Samba
ldap passwd sync = yes
unix passwd sync = no
```

N.B. Remember to remove the old `passdb backend` line!

- Set ldap password using `smbpasswd -w lxd2005`

LDAP backend: user-specific attributes

- `objectClass sambaSamAccount account`
- `uid` user name
- `sambaSID` Samba Sid of user (use `net getlocalsid` to find SID base, and add Unix uid to end)
- `sambaLMPassword` and `sambaNTPassword` hashed LM and passwords (use `smbpasswd` to set)
- `sambaLogonScript` script to be invoked at logon time (equiv. to `logon script` in `smb.conf`)
- `sambaHomeDrive` drive letter of home share (`logon drive`)
- `sambaProfilePath` Windows Path where 95/98 profile is stored (`logon home`)
- `sambaHomePath` Windows Path where NT/2000/XP profile is stored (`logon path`)
- `sambaUserWorkstations` comma-separated list of workstations from where use may log on

LDAP backend: groupmap-specific attributes

- `objectClass top posixGroup sambaGroupMapping`
- `cn` group name
- `sambaSID` Samba Sid of user. Must end with `512`
- `gidNumber` Unix Gid
- `sambaGroupType` `2`

9. Other gimmicks

- User monitoring
- Time service
- Veto/hide files
- Include/override config files

Others: User monitoring/logging

- `smbstatus` displays currently active sessions
- Account samba sessions in wtmp (last): Define following on share
  - `root preexec = /usr/X11R6/bin/sessreg -l %m -h %M -a %u`
  - `root postexec = /usr/X11R6/bin/sessreg -l %m -h %M -d %u`

Others: time service

- In global config: `time server = yes`
- On client (or startup script): `net time \\server /set`

Others: hiding files

- In share config
- Hides files (by setting hidden bit): `hide files = *.exe/*.scr`
- Hides files completely: `veto files = *.exe/*.scr`

Others: include/override config

- Override:
  - `config file = /etc/samba/lib/smb.conf.%m`
  - replaces current config
  - ignored if file does not exist
- Include:
  - `include = /etc/samba/lib/smb.conf.%m`
  - supplements current config
  - ignored if file does not exist (TBC)

URL of this presentation

- This presentation will be placed at the following address

`http://www.lll.lu/Presentations/LinuxDay2005/samba.pdf`