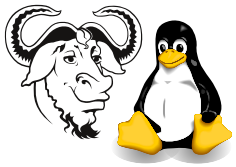

Implementing a Primary Domain Controller for Windows 2000 Clients using Samba

1 Aim

After completing this exercise, you will be able to install and perform basic configuration of a Samba server as a primary domain controller (PDC) for Windows 2000 clients. You will test it as a primary domain controller for Windows 2000 clients.

2 Background

Samba is an implementation of the networking used by Microsoft Windows. The core protocol is SMB (Symmetric Message Block), hence the name of the software. It has been achieved through reverse engineering Microsoft's proprietary protocols. Samba has a good reputation for stability and performance `http://www.pcmag.com/article/0,2997,s%253D1474%2526a%253D16554,00.asp`

2.1 Limitations of Samba

- Samba 2.2 works as an NT 4 compatible PDC; it does not support Active Directory in the way that a Windows 2000 server does
- Samba 2.2 can neither be a Backup Domain Controller (BDC) nor use one
- User information stored on a Samba PDC is not as complete as that stored on a Windows PDC
- Samba obeys Linux group file access permissions on the PDC, but it does not tell the client machine about it properly. Group file permissions are hard to set from a client.
- Full support for ACLs (access control lists) depends on applying a patch to the Linux kernel and recompiling the kernel.

Note that Samba 3 (now in alpha release) can be a member of an Active Directory domain.

2.2 An Overview

Samba's operation is managed through a configuration file, `/etc/samba/smb.cfg`. There is a comprehensive manual page for this: do `man smb.conf`. This file is either edited with a text editor, or edited using a program such as `swat`.

The process of a computer joining a Samba domain requires that the new domain member have an account created on the Samba machine; this account usually goes into the `/etc/passwd` file. The account name is the NetBIOS name of the new member, with a dollar "$" at the end. This account is created automatically by this statement in the Samba configuration file:

```
add user script = /usr/sbin/useradd \
          -n            \
          -g machines   \
          -c 'Samba Machine PDC member' \
          -d /dev/null  \
          -s /bin/false \
          -M            \
           %m$
```

Shares are also created in the Samba configuration file. The one provided contains a number of examples.

3 Procedure

1. Choose a partner so that at least one of you has Windows 2000 Prefessional or Advanced Server, that is *not* either a primary or backup domain controller.

2. Make sure that samba is installed on your machine:

   ```
   $ rpm -qa | grep samba
   samba-swat-2.2.7-5.8.0
   samba-2.2.7-5.8.0
   samba-client-2.2.7-5.8.0
   samba-common-2.2.7-5.8.0
   ```

3. If not, install the required packages, using the (Tab) key to reduce typing mistakes:

   ```
   $ cd /home/nfs/rh-8.0-updated/RedHat/RPMS
   $ sudo rpm -Uhv samba-*.rpm
   ```

4. Back up the original `smb.conf` configuration file for Samba:

   ```
   $ cd /etc/samba
   $ sudo cp -p smb.conf smb.conf-orig
   ```

5. Copy the new configuration file from the same directory on `ictlab`:

   ```
   $ sudo cp -p /home/nfs/samba/smb.conf-pdc-example /etc/samba/smb.conf
   ```

6. Edit the Samba configuration file using emacs:

   ```
   $ xhost +localhost
   $ sudo -v
   $ sudo emacs /etc/samba/smb.conf &
   ```

   > I *strongly* suggest that you open this file, and *keep it open.* It wastes time to continually open and close the configuration file.

7. Any time you modify this file, before using the server, tell samba to read your changes with:

```
$ sudo service smb reload
```

8. Set the NetBIOS name to a *unique* name:

```
netbios name = sammy
```

Instead of ***sammy***, put a name for your computer that will be different from the NetBIOS names of all the other computers in your class. Avoid spaces; stay with letters (the first character of the computer name should be a letter), digits and the hyphen character "-".

9. Change the "`workgroup`" to a *unique* name of your choice, with a letter or digit appended. Note: this is the NetBIOS *domain name* for your computer.

You should understand that NetBIOS domain names are different from DNS domain names. DNS domain names form a hierarchy, whereas NetBIOS domain names are all in one big flat name space.

10. Create two groups: `machines` and `smbadm`. Make the user `root` a member of `smbadm`.

```
$ sudo groupadd machines
$ sudo groupadd smbadm
$ sudo gpasswd -a root smbadm
```

11. Verify that the configuration file has no syntax errors using the `testparm` program:

```
$ testparm
Load smb config files from /etc/samba/smb.conf
Processing section "[homes]"
Processing section "[netlogon]"
Processing section "[printers]"
Loaded services file OK.
Press enter to see a dump of your service definitions
```

12. Start the two servers with:

```
$ sudo service smb start
```

Then check to see that it is running with:

```
$ sudo service smb status
smbd (pid 2696) is running...
nmbd (pid 2701) is running...
```

13. Make sure that samba runs next time you boot by making the correct symbolic links in the `/etc/rc.d/rc[345].d` directories:

```
$ sudo chkconfig smb on
```

14. Create a number of samba account passwords. Each of them must have an entry in the `/etc/passwd` file (i.e., perhaps you added the account earlier using `useradd`. Note that today, we will use separate passwords for samba and for logging into Linux.

Example of adding a user that is not in your password file already:

```
$ sudo useradd -c 'Nick Urbanik (local)' nickl
$ sudo smbpasswd -a nickl
```

Example of adding a user that is already in your password file:

```
$ sudo smbpasswd -a nickl
```

15. Add a password for root:

```
$ sudo smbpasswd -a root
```

Note that this password should be different from the Linux login password for root, for security reasons. You will need to give your partner this password.

16. Create a directory to hold the policy files, and another to hold the logon scripts:

```
$ sudo mkdir -p  /var/samba/netlogon/scripts
```

17. Examine the log files while you do the following steps. The log files are in `/var/log/samba`.

Give yourself permission to change into and read the samba log files by:

```
$ sudo chgrp ⟨yourStudentID⟩ /var/log/samba
$ sudo chmod g+rx /var/log/samba
```

You can then change into and read files in that directory. Open some windows and run `tail -f` on the log files. A new log file is created for each machine you connect to. Start with `smbd.log` if no machine specific file is created yet:

```
$ cd /var/log/samba
$ ls -ltr
$ tail -f smbd.log
```

18. Test that your Windows 2000 machine can share out your home directory; you can do this by right-clicking on the w2k equivalent of network neighbourhood, selecting map network drive, and choose "`Log in as a different user`" and enter your user name and your Samba password for your own account. For the share, type:

*sammy**nickl*

where, instead of ***sammy***, you enter the NetBIOS name of your samba server, and instead of ***nickl***, you enter your user name for your own account. Do not proceed with the remaining steps until this is successful.

19. Log into a Windows 2000 machine *locally* as `administrator`. Note: this Windows machine must not already be a primary domain controller, since a PDC cannot be made a member of another domain. You can use Windows 2000 Advanced Server, as long as it is not a PDC or BDC. If you have no Windows 2000 Professional for which you have administrator access, you can use Windows 98, but this will reduce what you can test.

(a) In Windows 2000, if `ipconfig /all` shows the WINS server is different from 192.168.68.240, then from TCP/IP settings, add 192.168.68.240 as the WINS server address. Select the radio button Enable NetBIOS over TCP/IP.

(b) In Windows 2000, right-click Network Places and select `Properties`; from the `Advanced` menu, select `Network Identification`. Press `Properties`.

(c) Choose `Domain`, enter the domain name of your samba server. Click (OK).

(d) Enter the user name `administrator` and enter the Samba password for `root` on your Samba server.

(e) Wait for confirmation and reboot when prompted.

Two problems may arise:

- Your Windows computer may have a NetBIOS name that starts with a digit, or
- You may have a connection to a share on your samba server from the Windows machine already. Solving that is simple: just "disconnect the drive".

If the name of your Windows machine starts with a digit, then `useradd` will not create a machine account for it. You could either rename the Windows machine with a name that begins with a letter, and contains only letters, digits and hyphens (rebooting when prompted), or add the machine account to your `/etc/passwd` file manually by:

(a) manually enter a command like this:

```
$ sudo useradd -n -g machines -c 'Samba Machine PDC member' \
  -d /dev/null -s /bin/false -M ⟨machineName⟩$
```

where ⟨*machineName*⟩ is the computer name of your Windows machine with leading digits removed.

(b) Add the digit(s) manually with the `vipw` command. First edit the password file:

```
$ sudo vipw
```

then add the digit(s) to the username for your Windows computer.

20. Now test this as a primary domain controller. Note that it is an NT4 compatible PDC, not a Windows 2000 PDC .

Read the documentation in `/usr/share/doc/samba-2.2.7/docs/Samba-HOWTO-Collection.pdf`.

Being a *primary domain controller* means allowing other machines to join the domain so that when any user logs into the domain, then:

- the user can access any resources (e.g., shares, printers) that are
  - provided by any of the machines that are members of the domain and that
  - they have the rights to access

- without entering a password again.

21. Login in to the domain as `administrator` from your Windows 2000 box. Browse to the `netlogon` share, and create some logon scripts using notepad. For the user `nickl`, the script is the file `/var/samba/netlogon/scripts/nickl.bat`. The logon script is run by the client when it logs in. Here is an example of a logon script:

```
@echo off

net time \\nicksbox /set /yes
if %OS%.==Windows_NT. goto WinNT

:Win9x
net use y: \\nicksbox\nickl
net use p: \\nicksbox\ossi
net use q: \\nicksbox\notlinux
net use r: \\nicksbox\linux
goto end
:WinNT
net use y: \\nicksbox\nickl /persistent:no
net use p: \\nicksbox\ossi /persistent:no
net use q: \\nicksbox\notlinux /persistent:no
net use r: \\nicksbox\linux /persistent:no
:end
```

Note that each line must be terminated by a carriage return/linefeed pair. Each share is a share section in `smb.conf`.

22. Documentation for the new features of Samba 2.2 is in `/usr/share/doc/samba-2.2.7/docs/Samba-HOWTO-Collection.pdf`. Open this up:

```
$ cd /usr/share/doc/samba-2.2.7/docs
$ acroread Samba-HOWTO-Collection.pdf &
```

and move to page 48 (by page numbering in the document itself), or page 53 if count pages starting from beginning as page 1. This section is about *System Policies and Profiles*.

23. I have extracted the policy editor `poledit.exe` from the NT4 Service pack 6a, and put it, together with the files `common.adm` and `winnt.adm` into the directory `profile-editor-from-service-pack-6a` in the `samba` NFS directory from `ictlab`. Test editing policies on your samba server from the Windows 2000 machine.

24. I have also downloaded the server manager for NT 4. You will find it in the `samba` NFS directory from `Ictlab`. Test the server manager.

25. Samba 2.2 supports downloadable printer drivers. This is described in the `Samba-HOWTO-Collection.pdf` file on page 27(32). Test it.

26. Samba 2.2 supports DFS . Read the documentation about it on page 20(25) in the `Samba-HOWTO-Collection.pdf` file. Also see `/usr/share/doc/samba-2.2.7/docs/htmldocs/msdfs_setup.html`.

27. Test your domain controller as much as you can.