Integrating NT4 Domains with Samba

The Boss

Microsoft will soon be withdrawing its support for Windows NT4, but Samba for Linux offers a free alternative that provides both users and administrators with a familiar environment. Samba servers are also easily added to existing domains. BY BERNHARD RÖHRIG

Central user management always becomes an issue when users need to access multiple servers on a network. If your network mainly comprises Windows clients, an NT4 type domain is a good choice as it allows your Windows clients to cooperate both with Samba and with Windows servers. There are four major administrative tasks involved:

- Adding Samba servers to existing NT domains
- Setting up Samba as a Primary Domain Controller (PDC) (and possibly as a Backup Domain Controller (BDC)
- Adding Samba servers to the Samba domain
- Adding NT servers and workstations to the Samba domain.

It is quite simple to integrate a Samba host as a member server of an NT domain. The NT domain controller needs an account on the host, that is a machine account, in Microsoft terms this is also known as a trust relationship. You can use normal Microsoft tools to set up the trust relationship. The computer name refers to the NetBIOS name of your Samba server, which is located in the:

```
netbios name =
```

entry in *smb.conf*:

If the entry is missing or blank, you can use the server's DNS hostname, which can be discovered by typing the following command on the server:

```
# hostname -s
```

Three entries in the configuration file need to be added or modified on the member server:

```
security = DOMAIN
workgroup = DWARFKINGDOM
password server = ALBERT
```

DWARFKINGDOM is the name of the NT domain the server will be joining, *ALBERT* the NetBIOS name of the Primary Domain Controller. If the domain comprises Backup Domain Controllers, you can add them after the PDC entry. The names in the list are separated by spaces. A single command allows the Samba server to join the domain:

```
# smbpasswd -j DWARFKINGDOM➥
 -r ALBERT
```

Before issuing the command, you will need to stop the *smbd* and *nmbd* processes on the Samba server. The processes need to be restarted after the server has joined the domain. Scripts are available for both steps.

Listing 1: Samba as a Primary Domain Controller

```
01 [global]
02   workgroup = DWARFKINGDOM
03   security = USER
04   encrypt passwords = yes
05   os level = 65
06   local master = yes
07   preferred master = true
08   domain master = true
09   wins support = yes
10   domain logons = yes
11
12 [netlogon]
13   comment = Domain-Controller
14   path = /home/samba/netlogon
15   public = no
16   read only = yes
17   browseable = no
```

Making Samba the Boss

Of course Samba is a useful supplier of hard disk capacity and printing services, but it can also assume the role of the PDC in an NT domain. In this role, the Samba server will manage both the user accounts and the browsing lists for the domain, which include the IP addresses of the Windows and Samba PCs in the various subnets in a router based infrastructure. The Samba server provides the following features:

- User level security (the server will not request authentication credentials from any other server)
- Encrypted password
- Domain Master Browser (i.e. the server will collate the subnet lists)
- WINS Server (the server will map IP addresses to NetBIOS names)
- the ability to respond to domain logon requests
- a special directory for the domain logon service.

The *smb.conf* entries required for these features are shown in Listing 1.

Otherwise, the Samba server configuration follows the typical pattern. The server can provide shared directories, print queues, and allow network access to mounted CD ROMs – of course, as required. The size of your network and your security requirements will define whether you assign a dedicated machine to handle authentication requests or simply use an existing Samba machine for this task.

Using a Samba server as a Backup Domain Controller is slightly more tricky. As Microsoft has still not pub-

lished the interface required for this task, it should not work at all. Getting it to work despite this fact is complex, and the results may not be completely stable, as the Samba documentation infers [1].

Creating Trust

To allow NT type machines – including any other Samba servers – to talk to a new PDC, you need to set up a machine account for each of these machines on the Samba host. From the viewpoint of the Linux system, a machine account is just a normal user account. However, the task in hand requires a special setup and management.

The most obvious give away is the user name we will be using, as it comprises the NetBIOS name of the member server and a terminating *$* character. You might like to assign UIDs from a special pool to prevent confusion with normal system users. Setting up a machine account for a computer called *winnie* requires three steps:

```
useradd -u 1001 -d /dev/null -s
 /bin/false winnie$
passwd -l winnie$
smbpasswd -am winnie$
```

The *-u* flag of the *useradd* command assigns a UID from a special pool to the machine account. There are no restrictions to where you place the pool, but you will need to avoid duplicate UID assignments. Now let's set up a triple barrier to prevent Linux users from logging on with the machine account:

- no home directory on the filesystem (-d flag)
- no login shell (-s switch)
- account disabled (-l flag in passwd).

The *-m* option tells the *smbpasswd* program that the account is a machine account. This ensures that a password is automatically created and encrypted without any intervention by the admin user. To allow Windows 2000/XP clients to perform a domain logon on the Samba server, the system administrator *root* must be added to the Samba password file:

```
#  smbpasswd -a root
```

For security reasons *root* should be assigned different passwords for Linux and Samba. The password is required when an XP/2000 client joins the domain, and plays no other role on the network apart from this.

Come together

The other Samba servers on the network can now become member servers of the domain. The *[global]* section of their configuration files contains the following entries:

```
workgroup = DWARFKINGDOM
security = DOMAIN
encrypt passwords = yes
password server = PINOCCHIO
```

The PDC just set up on Linux/Samba will be called *pinocchio* and is in charge of the *DWARFKINGDOM* domain. The commands required to add the member server to the domain after completing the configuration steps are shown in Listing 2; the example is based on SuSE Linux. The *smbpasswd* command is identical no matter what Linux system you are using.

After the re-launch, the member server will request authentication information from the domain controller *pinocchio*. All that remains to do now, is to ensure that the users of the client systems log on to the *DWARFKINGDOM* domain log, and not to local systems or stand-alone servers. This will allow them to access the resources provided by the member servers within the constraints of their user accounts without needing to re-authenticate.

If the workstations involved are NT/2000/XP type machines, you will need to repeat the steps described above to create machine accounts for them on the Samba PDC. Windows 9x/Me clients do not need a machine account. A client running Windows XP Professional requires an additional setting *Domain-Member:Digitally encrypt or sign secure channel data (always) = Disabled* in the *Control Panel/Administrative Tools/Local Security Policy/Local Policies/Security Options*.

A member server will normally attempt to change its machine account password on the PDC at regular intervals. The default period for a Samba server is one week, or 604800 seconds, just like for an NT machine. You can use the following *smb.conf* entry:

```
machine password timeout = 86400
```

to shorten the interval to one day.

Welcome Friends

The final task is adding existing NT servers to your Samba domain. After creating machine accounts for these computers on the Samba PDC, the required steps are performed on the individual NT servers. Right click on the *Network Neighborhood* icon on the Windows desktop to open the applet. The *Identification* tab shows the NetBIOS name of the server and the name of the workgroup or domain the server currently belongs to.

Click on the *Change* button to open the *Identification Changes* dialog box. Now select the *domain* radio button and type *DWARFKINGDOM* in the *domain* text box (see Figure 1). Do not check the *Create Computer Account* checkbox, as a machine account for the server has already been set up on the Samba PDC. Click on *OK* to confirm and after a short

Listing 2: Joining a Samba Domain

```
01 #  /etc/init.d/smb stop
02 Shutting down SAMBA nmbd                          done
03 Shutting down SAMBA smbd                          done
04 #  smbpasswd -j dwarfkingdom -r pinocchio
05 2002/12/31 16:48 : change:trust_account_password:
Changed password for
06 domain DWARFKINGDOM.
07 Joined domain DWARFKINGDOM.
08 #  /etc/init.d/smb start
09 Starting SAMBA nmbd                               done
10 Starting SAMBA smbd                               done
11 #
```

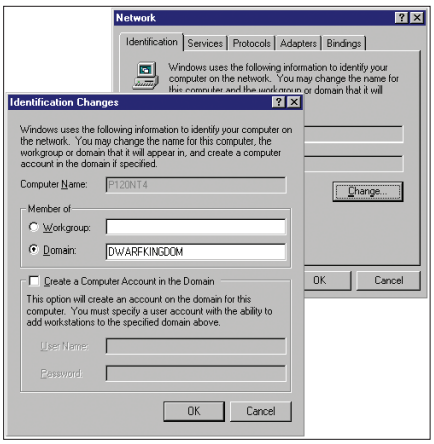

Figure 1: Connecting an MS Windows NT server to a Samba domain is easy

wait a message will appear to welcome the new member server to the domain. You will now need to restart your Windows NT server to apply the changes permanently.

The procedure for adding Windows 2000 and XP workstations that share their hard disk and printers on the network to the domain follows a similar pattern; the main difference being that you access the configuration options via the *My Computer* icon on the desktop (instead of the *Network Neighborhood*). Right click the icon and select *Properties* in the drop-down menu to open the *System Properties* dialog box. The *Identification* tab displays two buttons. The lower button, *Properties*, opens the *Identification Changes* dialog box, which additionally provides the *More* button.

Windows Pages

You can click on this button to open the *DNS Suffix and NetBIOS Computer Name* dialog box. The *Change primary DNS suffix when domain membership changes* checkbox is checked by default. As Samba environments currently do not use Active Directory, you will need to remove the checkmark. When you close the dialog box, ensure that you toggle from workgroup to domain mode in the lower part of the *Identification Changes* dialog box. Enter the *DWARFKINGDOM* domain just like on your NT servers.

Click on *OK* to access the Samba PDC which will prompt you for authentication credentials. Type *root* as the username, supply the Samba password, and again click on *OK* to add the machine to the domain. Again, you will need to restart the Windows machine.

Enhanced Service

Using a Samba server as your PDC allows you to use scripts to simplify the logon procedure for your users. In this case the scripts will be a sequence of DOS or Windows commands that are stored centrally, but run locally on the individual desktops when the client logs on. They are useful for tasks such as adjusting the click to the Windows time server, assigning local drive letters for shares on the Samba servers, and the ilk.

As these scripts are parsed by Microsoft systems, you must ensure that they contain the correct end-of-line character – so pay attention when using UNIX editors. To use a script add an entry such as *logon script = %U.bat* to the *smb .conf* on the PDC to run a logon script for each individual user (macro *%U*). You can stipulate *%m* to run machine specific scripts. The admin user will need to opt for one of these approaches.

Samba expects the scripts to be located in the netlogon share, which is set by the *path* statement in the *[netlogon]* section of the configuration file. User profiles are another useful feature. They are comprised of a mass of information that defines the appearance and behavior of the individual user environments, such as the desktop scheme and the contents of the Start menu.

Managing Roaming Profiles

Windows NT and its successors create a profile for each user, and profiles can optionally be defined for Windows 9x/Me systems. In contrast to local profiles, which are stored on the individual workstations, server-based (roaming) profiles are stored and managed independently of any workstations.

From the user's viewpoint this means logging on to a familiar environment no matter where. Profile information is automatically copied back and forth, and more or less transparently for the user. The Samba configuration file requires a statement in the *[global]* section and a special *[profile]* for this purpose. Listing 3 shows the additional entries.

Do not make the mistake of confusing the *logon path* with the *path* in the *[netlogon]* share. The latter is used for logon processes, is owned by *root*, and contains logon scripts for all users. In contrast, the directories below */home/samba/profiles* are owned by individual users, can only be read and written to by these users, and they are used for storing profile information.

An overview such as this article cannot give a product such as Samba true justice, so let us conclude by mentioning a few additional configuration options.

Reduce Administrative Effort

The different approaches to user management on Windows NT and Linux have always proved challenging. The *winbindd* server process introduced in Samba 2.2.2, and the associated statements in *smb.conf* (*Winbind options* section in Swat's *Advanced View*) provide more or less painless integration of these two realms. The *domain admin group* and *domain guest group* options in*smb.conf* also help.

Manually creating Linux user accounts on all your servers can cause headaches, but the winbind daemon can prove useful in this situation. The configuration statements required are *add user script* and *delete user script*. The (default) *allow trusted domains = yes* entry allows trust relationships between domains.

Samba version 3.0 sees the introduction of the Net tool, which can perform one particularly neat trick (amongst other things); typing *net rpc vampire* will migrate an entire NT security database to a Samba PDC. ■

Listing 3: Centrally Managed User Profiles

```
01 [global]
02   logon path =
\\pinocchio\profile\%U
11 [profile]
12   path = /home/samba/profiles
13   read only = no
14   browseable = no
15   create mode = 0600
16   directory mode = 0700
```

INFO

[1] "How to Act as a Backup Domain Controller in a Purely Samba Controlled Domain." Samba documentation ("Samba-BDC-HOWTO.html")