

## Migrating domains from NT4 to Samba

# Moving to a faster beat

Fancy the idea of moving your old server to an open source Samba solution? Many IT people do at present, for various reasons. The conditions have never been so favorable as now. However, you will need to navigate a few obstacles along the way. We show you how to avoid them. **BY BERNHARD RÖHRIG**

**N**o matter whether you need a simple file or print server, or are thinking of replacing a domain controller, a Samba server is easy to deploy, and quickly configured using just a few of the simple standard tools. It is quite simple to integrate a Samba server as a member server with an existing NT4 domain, and using Samba 3.0 with existing Windows 2000, or newer, domains.

Things start to become a little more complicated if you need to port a complete domain hierarchy with users, groups, policies, and login scripts to Samba, and want to avoid entering all that information manually. Again, Samba has a range of tools for the job, but for a perfect migration we need a little more than just that.

## Inventory

A complex job like a migration is something you cannot handle with technology alone, at least not with the kind of tools provided by the software (Windows or Samba). It is just as important for everyone involved to have a clear view of what they want to achieve by the migration, and of those goals that Samba 3.0 will not allow them to achieve, at present.

You also need to think about how to manage the transition process, and about ways of mitigating its impact on production. The aims that most people who are involved want to achieve by migrating from Windows to Samba are as follows:



Peter Glogg, www.sipix.com

- reducing the TCO (Total Cost of Ownership)
- improving user-friendliness
- improving the server response under load
- simplifying network management
- improving stability and availability of services
- removing the dependency on a single software manufacturer

IT staff need to have a clear concept of which of these points apply to their own environment. Only then can they start to

## Windows 2000 Features not supported by Samba

- use as Active Directory Server
- group policy objects in ADS
- computer policies
- login scripts in ADS
- software applications and access controls in ADS

define the milestones for the project and the tasks that need to be completed to achieve these milestones. Of course, you should always look for management buy-in to create a more friendly atmosphere for the whole project.

## Be Realistic

Success can be defined as acceptance by everyone affected by the migration. The best way to get people to accept the changes is to ensure that they have a positive impact, leading to the improvements you were aiming for, but without too much friction along

the way. Again, detailed planning can be critical to your success. The Unix Kiss principle (Keep it simple, stupid) should be right at the top of your list of priorities.

Above all, everyone involved has to know that Samba 3 on Linux offers a lot of things that a Microsoft operating system can not handle, but also that it has a number of limitations (see Box "Windows 2000 Features not supported by Samba", left).

Some straight talk at this stage will save disappointments and potential trouble later. On the other hand, there is an upside to migrating to Samba; things Samba can do, that the legacy product can not, such as:


- extremely cheap licensing
- multiple virtual servers on a single machine
- creating login scripts and policies on the fly

- remote management via OpenSSH
  - flexibility with regards to authentication back-ends (password database)
  - complete single sign-on architecture, even on WANs
- Of course, the best way to communicate these advantages to an end-user is to demonstrate how they will make that user's life much easier. Practical experience shows that this is not always

easy to do. All the more reason to ensure that the migration process is completed with a minimum of friction and that the user experience does not become more complex on account of all the changes that take place.

### Getting Down to Work

In comparison to all that preparatory work, the techni-



Vexira® Antivirus for Mail Servers and File Servers are industry leading, highly scalable virus scanning

is known as the "best of breed" in

**Server :**

- Sendmail
- Postfix
- Qmail
- Exim

**Supported OS:**

- Linux •
- OpenBSD •

Central Command, Inc.  
phone: 330.723.2062 • fax: 330.722.6517  
[www.centralcommand.com](http://www.centralcommand.com)

Central Command, Inc. All rights reserved. Vexira, Vexira logo, and Central Command are trademarks or registered trademarks of Central Command, Inc. All other trademarks are property of their respective owner(s).

cal steps involved in migration your domain are quite harmless. The first step is to set up your designated Samba domain controller under Linux, and configure the server as a Backup Domain Controller (BDC). Listing 1 shows the critical sections in *smb.conf*.

The important thing here is a combination *domain logons = yes/domain master = no*, which prevents your new domain controller from barging in and assuming the PDC role, which it can not do at the moment as it does not have the user database with the required information. The Samba server needs to query the Windows PDC for this information first.

To allow this to happen, you need to create a BDC computer account for your new Samba server on your existing NT4 PDC. The tool for doing this is the NT Server Manager. To complete the actual migration process (that is the transfer of the all important user database) you first need to disable the *smbd* and *nmbd* daemons that are running on your Linux machine.

The next step is to enter the commands shown in Listing 2, below. Lines 1 and 2 add the Samba machine as a

Backup Domain Controller to the *DWARFKINGDOM* domain. Line 3, using *rpcvampire*, tells the new BDC to poll the current PDC *ALBERT* to pick up, and so copy, the user database.

### Script-Controlled Migration

Line 4 outputs the whole user list, just to make sure. You need to supply the NT server administrator password for *ALBERT* in lines 1 and 3. The script called in line 6 maps the domain groups to corresponding Unix groups on the Samba server. Line 7 checks the results. Listing 3 shows an example of a script for automating group mappings. You can modify the script to reflect your own requirements, and then copy the *initGroups.sh* file to the */etc/samba* directory.

Before you run the script, you first need to create the Unix groups you need on your Samba machine. Note that Linux does not support capitals or space characters in group names, and that must be 16 characters or less (Listing 3 takes this into account).

Following this, the login scripts, user profiles, and policy files need to be transferred from the NT4 PDC to your Samba

server. The login scripts need to be stored in the *netlogon* directory, as specified by the *path* statement in the *[netlogon]* section of the configuration file (see Listing 1).

You need a separate directory for the user profiles (*NTuser.DAT* on Windows NT)

```
/home/samba/profiles
```

on the Samba server.

Profile files include the SID (security identifier) for the domain in a format intended for the Windows software running on the NT PDC. Unfortunately, Samba 3 does not understand this format. After transferring all the files, you need to convert the SIDs with the *profiles* tool (see the *man profiles* manpage and the notes in the "Tools" box, previous page). The Samba team recommends the use of the MS policy editor [1] to migrate the security policies over to your new system.

### Switch over

Finally, you need to add the following statement to the *smb.conf* file on your future Samba PDC,

```
domain master = yes
```

and then shut down the current domain controller.

You can now launch both the *smbd* and *nmbd* daemons on your Linux machine to fire up your newly migrated Primary Domain Controller, the definitive machine for any remaining (Windows) servers and clients that reside on your network. ■

#### Listing 2: Migration procedure

```
01 # net rpc join -S ALBERT -w DWARFKINGDOM -U Administrator%Password
02 Joined domain DWARFKINGDOM.
03 # net rpc vampire -S ALBERT -U Administrator%Password
04 # pdbedit -L
05 ...
06 # /etc/samba/initGroups.sh
07 # net groupmap list
```

#### Listing 3: /etc/samba/initGroups.sh

```
01 #!/bin/bash
02 # Default domain global groups
03     net groupmap modify ntgroup="Domain Admins" unixgroup=root
    rid=512
04     net groupmap modify ntgroup="Domain Users" unixgroup=users
    rid=513
05     net groupmap modify ntgroup="Domain Guests" unixgroup=nobody
    rid=514
06
07 # Special groups within the enterprise
08     net groupmap add ntgroup="Purchasing" unixgroup=purchasing
    type=d rid=3200
09     net groupmap add ntgroup="Sales" unixgroup=sales type=d rid=3210
10     net groupmap add ntgroup="Service and Hot line"
    unixgroup=service type=d rid=3220
```

#### INFO

[1] Migration from NT4 PDC to Samba-3 PDC:  
<http://samba.mirror.ac.uk/samba/docs/man/Samba-HOWTO-Collection/NT4Migration.html>

#### THE AUTHOR

Bernhard Röhrig is an IT consultant and has written several books on Linux/Unix and databases.

You can reach him on the Internet at:  
<http://www.roehrig.com>.

