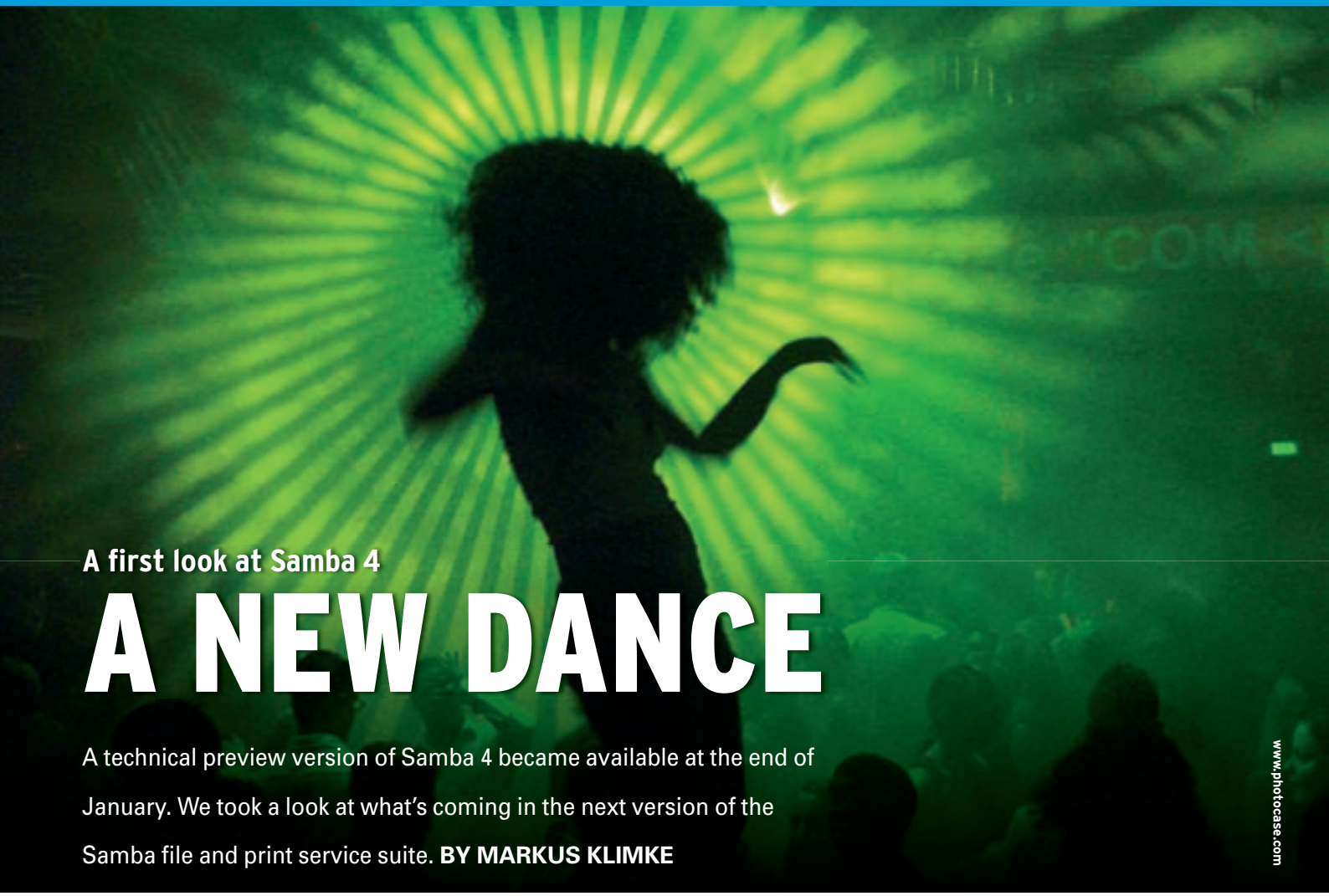

A first look at Samba 4

A NEW DANCE

A technical preview version of Samba 4 became available at the end of January. We took a look at what's coming in the next version of the Samba file and print service suite. **BY MARKUS KLIMKE**

For all versions of Samba, the goal is the same: sharing Windows resources with Unix-style operating systems such as Linux, and sharing Linux resources with Windows systems [1]. Unfortunately, support for Microsoft systems is a moving target: Redmond is not exactly renowned for their willingness to publish specifications, and the software giant keeps extending its SMB/CIFS protocols from one Windows version to the next.

Open source developers try to keep track of the changes to SMB by using tools such as Ethereal to sniff connections, but Microsoft stepped up its game with Windows 2000, introducing the object-based directory system called Active Directory Service (ADS, [2]).

Contrary to previous developments, the Microsoft went for established standards in this case, with the Windows developers welding an LDAP user database onto a Kerberos 5 authentication mechanism and opting for DNS-based name resolution. The fact that Microsoft has mainly kept to genuine standards lets Linux provide a high degree of interoperability, thanks to free implementations such as OpenLDAP and the MIT or Heimdal Kerberos versions.

One major aim of Samba 4 is to provide a Samba directory server that can interoperate with Microsoft Active Directory, and a very early version of this functionality went public late in January. The Samba team opted for a radical approach, re-implementing many routines to free Samba 4 of the workaround legacy that weighed down earlier versions. As a consequence, many options that Samba 3 relies on have now been axed.

Kerberos and LDAP

Samba 3 gave network administrators the option of installing a Linux machine as a domain member server in a Windows 2000/2003 domain. From a technical point of view, the member server uses Kerberos tickets for authentication purposes. Based on this design, both servers and clients (using tools such as *smbmount*) exchange tickets, thus implementing single-sign-on operations between Linux and Windows throughout the domain. The use of Samba 3 as a Primary Domain Controller (PDC) or Backup Domain Controller (BDC) was restricted to Windows NT-style authentication, with Kerberos thrown in.

Now that Samba 4 implements its own Kerberos functionality, Samba can replace a Microsoft-style state-of-the-art

Figure 1: The provision tool initializes the Samba database. You can also run Swat for provisioning.

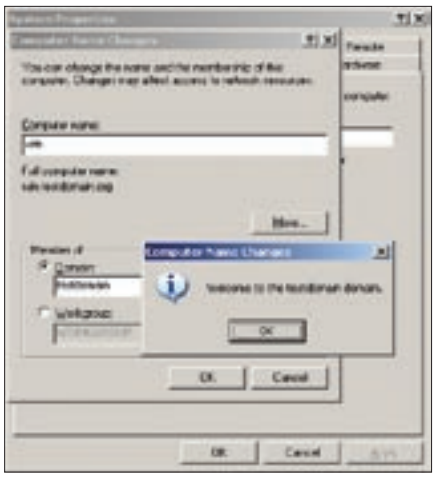

Figure 2: Successfully adding a Windows 2003 Server as a Member Server to a Samba 4 domain.

domain controller (see below). The Kerberos implementation is the Heimdal variant, and it only makes sense that Heimdal developer Love Astrand played a major role in the programing work. In future, it will be possible to use external Kerberos libraries.

One thing that Samba 3 never got round to doing was synchronizing user databases with its own Samba databases (see box titled "Samba4WINS" for more details). As OpenLDAP can replicate its database on other servers of the same type, the Samba 3 developers just dropped the topic. However, configuring an OpenLDAP server is anything but trivial. The Samba 4 team, spearheaded by Andrew Tridgell, sounded the technology charge and implemented its own LDAP back-end known as LDB.

Another important reason for Samba implementing its own LDAP solution is trouble-free replication. For example, the developers wanted to migrate changes across the machines involved to remove any danger of inconsistent replication. It looks very much like Samba 4 will be retaining the ability to bind to OpenLDAP, mainly to support established environments with Samba 3 servers.

CIFS, NTFS, and Posix ACLs

It has never been Samba's aim to restrict support to heterogeneous environments; instead Samba has always played a major role in the NFS domain, supporting the exchange of data between Unix and Linux systems – to the extent of competing with NFS 4, which is not fully developed. This is evidenced by the CIFS kernel modules, where development work has pushed on from version to version. Take the CIFS Experimental Features, for example, which have supported Kerberos since version 2.6.16. This was a big drawback in comparison

Samba4WINS

The Windows Internet Naming Service is a throwback to the days of NT 4. This said, even more recent Windows systems use the WINS protocol to resolve NetBIOS names. When mapping a share, the NetBIOS name can be used after the first backslash or first backslashes. Samba has had NetBIOS support for quite a while now, as this is what enables interoperability between servers. Samba 4 will not be changing this to any great extent.

The problem is that Samba-based WINS servers do not support replication. This leaves admins with no alternative but to spend money on running Windows WINS servers. The Samba4WINS [3] cooperation project aims to change this. The companies involved are Sernet, Computacenter, and Fujitsu Siemens Computers, along with the Linux Solutions Group e.V. Samba4WINS will be fully integrated with Samba 4. The functionality can be built into Samba version 3.0.21 or later and run as an independent process.

Listing 1: Testparm Output smb.conf

```
01 # Global parameters
02 [global]
03      server role = pdc
04      workgroup = TESTDOMAIN
05      realm = TESTDOMAIN.ORG
06      netbios name = LINUX
07      log level = 2
08      registry:hkey_users = hku.
   ldb
09      registry:hkey_local_
   machine = hklm.ldb
10      comment =
11      path =
12      ntvfs handler = unixuid,
   default
13      read only = Yes
14      hosts allow =
15      hosts deny =
16      max connections = -1
17      strict sync = No
18      case insensitive
   filesystem = No
19      max print jobs = 1000
20      printable = No
21      printer name =
22      map system = No
23      map hidden = No
24      map archive = Yes
25      browseable = Yes
26      csc policy = manual
27      strict locking = Yes
28      copy =
29      include =
30      available = Yes
31      volume =
32      fstype = NTFS
33      msdfs root = No
34
35 [data]
36      path = /export/data
37      read only = No
38      hosts allow =
39      hosts deny =
40
41 [IPC$]
42      comment = IPC Service
   (Samba 4.0.0tp1)
43      path = /tmp
44      ntvfs handler = default
45      hosts allow =
46      hosts deny =
47      browseable = No
48      fstype = IPC
49
50 [ADMIN$]
51      comment = DISK Service
   (Samba 4.0.0tp1)
52      path = /tmp
53      hosts allow =
54      hosts deny =
55      browseable = No
56      fstype = DISK
```

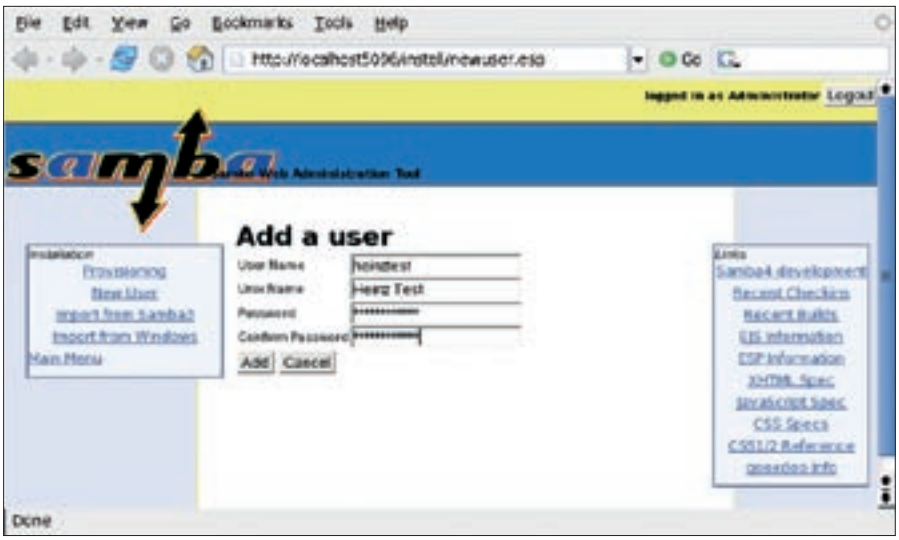

Figure 3: Swat lets you set up a LDIF encoded user; the console tools give you the same ability.

to Windows SMB, which allowed users to mount shares using single sign-on with the *-o krb* option.

In the access management stakes, Samba has been capable of mapping Posix ACLs to NTFS ACLs and vice-versa for quite a while now. Again, version 4 takes a different approach and, instead of storing NT ACLs on the Posix filesystem, introduces a virtual filesystem known as NTVFS, which stores NTFS attributes as is. It is even capable of emulating ACLs in NTFS data streams. Alternate Data Streams (ADS) are a function of the NTFS filesystem, which allows users to store invisible alternate data for a file. Group policies are another important topic of contention; as of this writing, it is uncertain how Samba 4 will handle them.

Primary Domain Controller Trial Run

After unpacking the Samba 4.0.0tp1 source code, which is available at [4], look for the *howto.txt* in the project tree; the file has some useful operating tips. After completing the build, you first need to provision the database. The *provision* tool handles this, creating the LDAP database, the registry, and predefined entries for access to the LDB and Kerberos services DNS server (see Figure 1). You will still need to add manual entries to the zone for the DNS server. The Windows equivalent of the provisioning tool is known as *dcpromo*.

Provision will also create a minimal *smb.conf*. If you pass in the */usr* prefix with the configure script, you will find the configuration file in */usr/lib* when you are done. For more control, you can switch the Samba daemon to interactive mode by entering *smbd -i -M single*; this gives you messages on stdout. Samba 4 supports three process modes: it can be run as a single process, in threaded mode, or as a multiprocess variant. Once the daemon is running and you have set up a trial share, *testparm* should give you something like the lines in Listing 1.

According to the Samba team, version 4.0.0tp1 is capable of replacing a PDC.

Figure 4: The Samba console tool ldbsearch searching for a user.

After adding the DNS entries, there is nothing to stop you adding a Windows machine to the Samba domain. In our lab, we added a Windows 2003 Server as a member server. After specifying the domain and saying that we wanted the machine to join the domain, Windows 2003 seemed quite at home (see Figure 2).

Swat Revisited

System management has been reworked and considerably extended. After adding new features such as Kerberos and LDAP, the Samba team has now taken steps to make life easier for the admin. The well-known, but seldom used, Swat tool has gone through a renaissance in Version 4: the browser-based interface is now an integral part of the Samba suite. As soon as you have launched the Samba daemon, a compact embedded web server by Appweb [5] provides a platform for Swat. This removes the need to set up Swat in contrast to previous versions; you can just surf to the tool in your browser right after starting the Swat daemon.

Swat still lacks a few features to be a complete administrative interface. But it is definitely up to the task of showing you what Samba 4 can do in its PDC

role. The user defaults to Administrator, who is expected to log on using a Windows client. But Swat gives you the ability to add another user.

As an alternative, you might like to try out some of the numerous new console tools: the one you need here is *ldbadd*. Note that *ldbadd* requires an LDIF encoded user. As Swat is not capable of handling this, Figure 3 shows you how to add a user to the domain. The first time this user logs on, the Samba Registry settings require a password change. Swat does not support password policies as of this writing.

Assuming the login works, the user's credentials are now safely stored in Samba's LDB database. If you would like to check or change the database entries, you can launch a console tool such as *ldbedit* or *ldbsearch*. The former opens the database in your favorite editor, where you can search for the user entry and modify the entry if needed. Figure 4 shows you how to use *ldbsearch*.

Samba 3 had the very useful ability of being able to accept a domain you migrated from a Windows NT server and, of course, Samba 4 can do this too. (Additionally, admins can migrate Samba 3 domains to Samba 4 in Swat.) This "Vampire" mode is no longer restricted to Windows NT but also works for Windows 2000/2003 Server. In Figure 5 you can see how we migrated a Windows 2003 domain. If you want to make sure that the logfile wasn't overly optimistic, you can search for a user in the Samba LDB database to make sure the user has survived the migration to the new domain.

Configuration

Editing a configuration file is a tried-and-trusted fine tuning method. In Samba, the number of configuration file options has increased noticeably. At the same time, some Samba 3 options have been dropped. It is still unclear which of these options are missing, as many of them are still hanging on in there as workarounds for problems in interoperability mode operations.

New keywords describe the state and behavior of the KDC – *kpasswd port* or *krb5 port*, for example. The *paranoid server security* option defines a security level, whereas *ntvfs handler* specifies how the NTVFS Layer should behave.

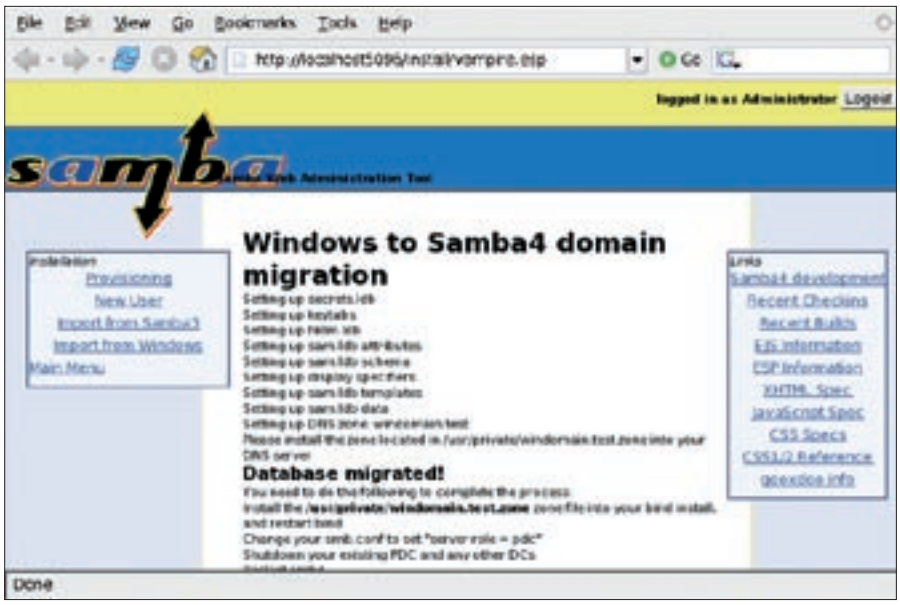

Figure 5: Swat following the successful migration of a Windows 2003 domain.

The default here is *ntvfs handler = unixuid*, which syncs file operations with the underlying Posix filesystem.

The *ntvfs handler = cifs* option lets you run a Samba server as a CIFS gateway, which forwards file requests to another CIFS server. If the gateway is a domain member server, it can forward requesting user or service tickets:

```
[extdata]
  ntvfs handler = cifs
  cifs:server = nextserver
  cifs:share = shared
```

There are not many back-ends for NTVFS at this time of writing. Besides the one I just mentioned, the source code has a *simple* option, however, the option entails performing file operations with root privileges, which makes it less than useful. If you need more information on the *samba.conf* options, check out *source/param/loadparm.c* in the source code.

Leave Well Alone

All in all, it looks as though Samba 4 is about to break free from its legacy tethers. Besides LDAP and Kerberos, the software can handle ACLs beyond Posix, and it has its own Active Directory Server emulation. Samba4WINS provides replication services for WINS servers. There are three models for improved scalability, single process, multiple process as in Samba 3, or a threaded variant.

The "Technical Preview" we looked at is intended as a platform for reviewing new technologies. It does not have the full range of features you would need in production operations, for example, printer support is missing. The developers advise against deploying Samba 4 in production environments until they have completed their work. A press release indicates that this will not happen before summer. The word from some developers is to look out for backports from version 4 in Samba 3.

Version 4 is not the only thing keeping the Samba developers on their toes; there is the small matter of the undocumented Windows Vista SMB 2 version, which has a completely new design. If the EU monopolies case against Microsoft fails to force the company to publish interfaces, the Samba team look forward to revisiting its early practice, sniffing file transfers with Ethereal. ■

INFO

[1] Samba: *http://samba.org*

[2] Active Directory: *http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirectory/default.mspx*

[3] Samba4WINS: *http://EnterpriseSamba.org/index.php?id=88*

[4] Samba 4.0.0tp1: *http://devel.samba.org/samba/ftp/samba4/*

[5] Appweb Embedded Webserver: *http://www.appwebserver.org*