<Samba status report>

<Volker Lendecke>
<Samba Team / SerNet GmbH>
<Bahnhofsallee 1b>
<37081 Göttingen>
<Germany>
<vl@samba.org / vl@sernet.de>

1 Abstract

Samba 3.2 has been released on July, 1st, 2008. This talk will give an overview of the current status of Samba development and what can be expected in the near future.

Major new developments in Samba 3.2 are:

IPv6 support Samba can now listen on IPv6 interfaces

Registry configuration To make configuration for OEMs easier, Samba now provides a registry based configuration method. This makes parsing and writing smb.conf files unnecessary and also enables remote configuration via the Windows regedit.exe possible.

Cluster support Based on a posix cluster file system like GFS, OCFS or GPFS Samba can now share the same file space via different nodes of the cluster and still maintain consistent CIFS semantics.

SMB transport encryption NFSv4 has it, so we have to have it, too :-). smbclient to smbd can now encrypt the bulk data, cifsfs is being extended to also do so.

Future development

Samba 4 Samba 4 is making progress being an active directory domain controller, although it is still incomplete.

Samba 3/4 merge A new merge project has been started: Merge the best parts of Samba 3 and Samba 4 into one build and thus provide an AD controller as well as a solid file and print server. This talk will show where the interfaces are and how we plan to cope with them.

2 Registry configuration

Samba has internally provided a registry database for quite a while now. Windows workstations remotely access the registry via the WINREG RPC interface to figure out certain properties of a file server or domain controller. If Samba failed to provide those values, Workstations would not function properly against a Samba server. The other big user of the WINREG interface is the printing subsystem. Although the SPOOLS interface provides all necessary calls to query printer information, many printer drivers query the registry directly, accessing the keys where Windows happens to store the printer information.

Samba 3.2 optionally makes much more use of the registry now: You can put the smb.conf file into the registry. Why would you want that? The most compelling reason is that OEMs packaging Samba can now much more easily manipulate the Samba configuration using scripts. Samba provides the net conf

command with subcommands to set parameters, create shares and so on. Samba also exports a registry key with the configuration, available to admins remotely accessing the Samba box via regedit or custom tools. The registry configuration is part of another talk in this conference.

3 Cluster support

At a former Linuxkongress I have given a talk about the upcoming cluster support in Samba, why it is difficult to cluster CIFS and what Samba would do to solve these difficulties.

Here I can say that the experimental cluster support has been merged into Samba 3.2 and is successfully used in production in a number of large installations on top of GPFS. It seems that RedHat right now is interested in getting this to run on top of GFS. I do not expect any Samba/GFS specific difficulties. The only thing is that Windows clients tend to play very nasty games with file systems, and I would expect some tuning by the GFS team to play those games well.

4 SMB transport encryption

SMB historically has had very weak support for protecting the data transferred back and forth. Quite early user passwords could be sent encrypted over the wire using a challenge response scheme. The crypographic details of the authentication have seen many revisions, the last one being NTLMv2. With Windows 2000 and Active Directory Kerberos was added as an authentication mechanism to SMB.

The data itself for a while could not be protected, until Windows NT implemented SMB signing. Based on a session key that is calculated during authentication, clients and servers cryptographically sign the SMB messages, so that nobody in between can mess with the data that travels unencrypted.

Samba 3.2 has added code that encrypts the data stream based on the same session key used for signing. Just add -e to smbclient, and the data is encrypted. This encryption support will be added to the Linux cifsfs, and who knows, maybe at some time in the future even in Windows clients.

5 Merge project aka Franky

The Samba project right now is split up into two sub-projects: Samba 3 and Samba 4. Samba 3 is the stable file and print server and NT4 compatible domain controller that is running at many sites. Samba 3 is the direct descendant of the code that Andrew Tridgell started in 1991. A few years ago, Tridge wanted to extend Samba to enable a more flexible, NTFS-Style virtual file system interface. It turned out that the code base had acquired too much history to be easily adapted to the new needs. So he started a completely new code base which turned into the Samba 4 project.

On its way, the focus of Samba 4 has changed significantly: From a new implementation of the VFS its main target now to implement an Active Directory (AD) compatible Domain Controller (DC). The AD DC is the one big missing feature that Samba 3 lacks. Many sites are running Samba 3 as a NT4 compatible DC, but modern Windows environments depend on features available only in real AD domains, such as domain local groups and group policy objects.

The AD support in Samba 4 is partly complete. Workstations and Servers can join a domain hosted by a Samba 4 DC, fully believing that they are member of an Active Directory domain. Among other things this means that logon to the workstation happens using Kerberos tickets, and that during startup and logon they will start to download and apply group policy objects. This applies to a single DC only at the moment, to enable replication you have to rely on a replicating LDAP database for the domain objects. Also, right now trusts are not fully functional yet, although that is being worked on right now (Sept. 2008).

While the AD functionality is actively developed, other big parts are less functional in Samba 4 right now:

- Domain membership: Samba 4 right now is not a very good member in existing domains. An initial implementation of winbind has been developed, but this is far from being finished.
- Posix ACL interoperability: Samba 4 has an implementation of NTFS Access Control Lists, which are stored as extended attributes. Many existing sites use the Posix permissions or ACLs to control access to the file space. Samba 4 does not map those very well.
- Print support: Samba 4 does not yet have any support for exporting printers.
- Cluster support: Samba 4 has rudimentary support for a cluster environment, but the Samba 3 implemenation of a clustered CIFS server is more mature.

Eventually, Samba 4 will close all these gaps, but until then, users are faced with the situation that neither Samba 3 nor Samba 4 have all features they need: A fully functional file and print server and an Active Directory Domain Controller.

If this situation sounds familiar to people running Samba for a long time already, they are right. Before Samba 2.2 was released, the NTDOM branch of Samba was a much more functional NT4 domain controller than Samba 2.0 was. Many people were running both side by side on a single box, Samba NTDOM providing the DC functionality and Samba 2 doing the file and print services.

A new development effort has started to repeat this and unite Samba 3 and 4. Samba 4 will do the LDAP, Kerberos and most RPC services, while Samba 3 will do the file and print services. The initial naming idea for this merged project by Kai Blin was to call it Frankenstein, but this was seen as too scary for the general audience. So we settled on **Franky** as a nice nickname for the merged project.

When finished, Franky will provide a single Makefile that builds all necessary parts from a single source tree.

5.1 services

There are several services that need distributing across the two deamons:

5.1.1 SMB

SMB is the basic file and print service listening on ports 139 and 445. Samba 4 will listen on these ports, but not provide the services itself. Instead, it will fork a subprocess and immediately start a smbd from Samba 3 the same way inetd does. This is done so that the number of daemons stays small. Samba 4 has to run anyway for LDAP, Kerberos and other services, but it should notact as a file server itself.

5.1.2 RPC

MSRPC or rather DCE/RPC services come in many different flavors. They can be offered via many different transports and they fulfil a huge number of different services. It will mainly be the Samba4's task to offer RPCs, although there are exceptions.

The most important RPC services a DC offers are Netlogon, LSA and SAMR. The Netlogon Service is responsible for user authentication and calculation of the user's group memberships at logon time. Netlogon does the cryptographic calculations behind NTLM and related protocols. Netlogon is also reponsible for querying the name of a trusted DC, or for changing a workstation account password.

5.1.3 Print services

Print services are one exception where Samba 3 will provide an RPC service, just because Samba 4 does not do this service yet. Fortunately, print services are only used via the named pipe transport (see below), so no backdoor from Samba 4 into Samba 3 is necessary.

SAMR offers an RPC-based access to the domain user and group database. In AD environments many uses of SAMR have been replaced by LDAP calls, but for example the creation of a workstation account when a machine joins a domain is still done via RPC.

5.1.4 LDAP and Kerberos

Both these services are handled by Samba 4, currently there are no plans to extend Samba 3 by a LDAP server or by a KDC.

5.2 Necessary glue

If it all was so simple, no development would be necessary. Just compile Samba 3 and Samba 4, install and configure them properly, and you are done. Unfortunately, there are some interfaces necessary that need to be developed.

5.2.1 SMB authentication

As Samba 4 holds the user database, but Samba 3 performs the file service, authentication for CIFS needs to be passed on from S3 to S4. This turns out to be pretty simple: Samba 4 acts as a Domain Controller anyway, and Samba 3 has solid support as a domain member. So we need to join the Samba 3 daemon as a member into the Samba 4 domain and use the existing Netlogon RPC interfaces. As both daemons run on the same box, the transport to be used will be a Unix domain socket to avoid real network traffic and problems with potentially non-existing or mis-configured network interfaces.

5.2.2 RPC over named pipes

By far the most-used transport for MSRPC traffic is the named pipe transport ncacn_np. A named pipe is a virtual file on the IPC$ share of a domain controller, named for example `\\PIPE\samr`. A client requesting access to the SAMR RPC service opens this virtual file, writing to and reading from it issues the RPC requests.

As said above, Samba 4 provides the RPC service, but Samba 3 controls the SMB service. Samba 3 right now performs all RPC services in-process, but this will have to change with Franky. Fortunately the RPC data stream is a pretty clean interface: Bytes coming in on a named pipe virtual file can directly be passed into a unix domain socket that Samba 4 listens on.

There is one problem left with this approach: The named pipe RPC transport mechanism assumes that the daemon providing the RPC service must have access to the authentication information the client used to access the IPC$ share. For example a user can change his password via the SAMR interface, and the passwords are encrypted with the session key that was calculated during the SMB-level authentiation. This will be solved by a custom packet passed from Samba 3, the SMB server, to Samba 4, the RPC server, before the real RPC traffic starts.

5.3 Current status

In September 2008 both source trees have been merged into a single one. Whereas the former Samba 3 and Samba 4 branches both had their own source/ subdirectories, the new merged branch has a source3/ and source4/ subdirectories. This was the first necessary step to merge development efforts. As a second step, some common libraries such as talloc, tdb and libreplace have been moved into a common place, so that a manual merge between the Samba3 and Samba4 copies is no longer necessary.

Jelmer Vernooij has put a lot of effort into a shared build system that compiles the relevant parts of Samba4 when compiling Samba3, given that the necessary components like for example python are available at build time.

Most of the necessary glue code exists in a git repository on git://git.samba.org/vl/samba.git. The Samba 3 parts were mostly developed by the author of this paper, Stefan Metzmacher helped implementing the necessary glue in Samba 4. This code is some months old and needs to be merged into the merged franky tree.

5.4 TODO

When the shared build is done, and the necessary glue code is merged into the tree, we still have to solve a lot of issues. For example the smb.conf configuration file has diverged between the two Samba branches. Options valid for Samba 3 do not exist in Samba 4 anymore and are replaced by different options.