

Samba Status Update

Linuxkongress Hamburg
October 10, 2008

Volker Lendecke
SerNet
Samba Team



Volker Lendecke

- Co-founder SerNet - Service Network GmbH
 - Free Software as a successful business model
 - Network Security for the industry and the public sector
 - Samba-Support/Development in Germany
- For almost 20 years concerned with Free Software
- First patches to Samba in 1994
- Consultant for industry in IT questions
- Co-founder emlix GmbH (Embedded Systems)



What is Samba?

- Interoperability between Windows and Unix systems
- Most protocols Windows speaks today
 - SMB (File Sharing), Printing, Browsing, Authentication
 - „Samba makes unix machines show up in Network Neighborhood“
- Samba runs on most Unixes these days
 - Main development platform is Linux
 - Solaris, AIX, HP/UX, Stratus V/OS, Tru64, etc...



Samba 3

- Stable version of Samba, production code
- Solid file and print server
- NT and Active Directory domain member
- NT4-compatible Domain Controller
- Security and access control model based on Unix
- Flexible posix-based VFS modules to change file access semantics
- Current version: 3.2.4, 3.3 planned for December



Samba 4

- Started in 2003 by Andrew Tridgell as a new VFS system with the goal to support cluster file systems
- Complete re-write of Samba
- Target: 100% semantics of Windows
- Main feature today: Active Directory Domain controller
- Most useful component for development: smbtoriture, a very comprehensive SMB test suite



Samba 3.2

- License change: GPLv3
 - This caused the naming change from 3.0 to 3.2
- 3.0 will only be maintained for security updates
- 3.2.0 was released on July 1st, 2008
 - The inevitable bugfix releases went in pretty quickly, right now we're at 3.2.4
- The release went surprisingly well, given the number of changes that were put in



IPv6

- NetBIOS over TCP (RFC1001 / 1002) only specifies IPv4
- RFC1002 name resolution naturally embeds IP-addresses
- With AD and CIFS, DNS has become the primary name resolution
 - Nobody is going to change RFC1002
- Samba 3.2 listens on IPv6 interfaces now
 - Main changes: Interface enumeration and name resolution for Samba as a client (getaddrinfo)



Registry configuration

- Parsing and writing smb.conf files with GUI tools is awkward at best
- Samba 3 has to implement a registry, clients expect to find certain keys to determine the server type
- Registry data model matches exactly smb.conf format, it was designed as a .ini file replacement
- HKLM\Software\Samba\smbconf
- Enabled only if „config backend = registry“ is enabled in the smb.conf text file



Cluster support

- Clustering is a very hot topic in the storage industry right now with several solutions
- Several Posix-level cluster file systems available:
 - GFS, OCFS2
 - GPFS, Panasas, CXFS, Isilon etc
- NFS clustering is easily possible on top of those
- SMB clustering puts very heavy demands on the cluster lock manager



CTDB

- None of the existing lock managers provided the semantics needed for CIFS clustering
 - Samba requires locks with associated data, a big share of Samba is just to implement the correct locking
 - Many lock managers are just too slow
- Ctdb is the „clustered tdb“ lock manager
 - ... and also does IP failover, service start/stop, monitoring, TCP tickle acks,
 - So ctdb is more like a complete HA solution



Cluster support

- Samba 3.0 was heavily modified to enable sharing of cluster file systems correctly via CIFS, all patches went upstream into 3.2
- Product shipped by IBM right now based on 3.2 with minor, publically available patches
 - Backports from 3.3, locally necessary small hacks
- Ctdb.samba.org has all Samba-related components
- 3.2 contains all cluster-relevant code



AD LDAP signing

- Policies on W2k3 domain controllers can require that all LDAP access needs to be authenticated and integrity protected
- Cyrus SASL is the standard OpenLDAP way to provide this, but it is hard to configure
- Current OpenLDAP libraries allow to intercept the network traffic
- Samba 3.2 winbind does the SASL integrity wrapping itself



LDB

- Ldb is a lightweight library providing an LDAP-like data model on top of tdb
 - Same idea as SQLite for SQL
 - Main feature: Multi-indexed tdb
- Samba needs to maintain its internal user database
- As a start, group mapping has been converted to ldb
 - In the future, maybe more will be converted



SMB transport encryption

- All SMB authentication variants provide a session key as one result
 - This is used to encrypt the password changes
 - RPC can be encrypted
 - Normal SMB traffic (file content) is plain text
- Samba 3.2 re-uses the RPC encryption routines to encrypt the whole SMB data stream
- Currently only smbclient->smbd
- Now we have to persuade MS to use this :-)



RPC interface generation

- Many important sub-protocols in the SMB world are DCE/RPC based
 - Marshalling of function call arguments has been done with manual code
- „Real“ RPC implementations use IDL
- Samba4 provides the Perl-based IDL compiler IDL
 - Contrary to MIDL (the MS tool), PIDL generates readable code
- Lots of Samba 3.2 code is converted, much ugly code is gone



Samba 3/4

- Samba 3: Good file/print server/domain client, working NT4 PDC
- Samba 4: Starts to become an AD/DC, file server lacks a lot, domain client barely existing
- Libraries shared between 3 and 4 (tdb, talloc, etc)
- New plan: Merge the two projects into one
 - ... in memory of the good old branch-ntdom times when Samba 2.0 was not yet a NT4DC
- We need a good name for it



Samba 3/4 Interfaces

- Samba 4 `smbd` has been renamed to „samba“
- New „master“ branch contains both Samba 3 and 4
- Libraries have been merged, so only one copy of `talloc` and `tdb` exists
- „samba“ listens on all ports, so only one daemon around
- LDAP, Kerberos, CLDAP, `ncacn_ip_tcp` will be handled by Samba4



Samba ¾ SMB handling

- „samba“ listens on all ports including 139 and 445 for SMB
- Client connects to port 139/445 -> Samba 4 forks smbd3 like inetd would
- Smbd3 has no smbpasswd file, when a user authenticates, the local „samba“ can answer. It *is* a DC, and as such can authenticate users.



Samba 3/4 RPC handling

- RPC services are handled in Samba 4
- Several transports: TCP, local sockets, and SMB
- Clients open `\\server\IPC$\SAMR` named pipe
- This is handled inside `smbd3` right now
 - New code will connect back into `smbd4` and just pass back and forth data
- For some pipes, the SMB-level authentication information needs to be passed (e.g. the Session key for SAMR)



Samba 3/4 open questions

- Packaging (lib/smb.conf or etc/smb.conf? :-))
- Compatibility with Samba 3 command line utilities
- /etc/samba/smbpasswd is gone, but how will the smbpasswd utility still work
- Documentation



Questions/comments?

Volker Lendecke, VL@SerNet.DE

SerNet - Service Network GmbH
Bahnhofsallee 1b
37081 Göttingen

Tel: +49 551 370000 0

Fax: +49 551 370000 9

<http://www.SerNet.DE>

<http://Samba.SerNet.DE>

