

Samba Status Update

Linuxkongress

Oktober 2009

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)



SerNet

- SLA based support for more than 650 customers
- network security for industrial and public customers
 - firewalls, VPN, certificates, audits
 - based on open standards wherever possible
- Support for many OS: Linux, Cisco IOS, Windows etc.
- Compliant with BSI Grundschutz and ISO 27001 and other international regulations



SerNet and Samba

- technological leadership of SerNet worldwide
 - involved in almost every big European Samba project
 - 5 out of 6 European developers work for SerNet
 - SerNet distributes up-to-date Samba packages
- samba eXPerience
 - *The* international Samba conference
 - > 150 developers & users from > 15 countries



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: 3.3.5 very soon



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



Release model

- 3.2 was released in July 2008
- Every 6 months we release a new 3.x
- 3.x.y released as necessary
- A release is put into maintenance once the successor is out
- After next successor: No fixes except severe security fixes
- 3.0 completely end of life since July 2009



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 relatively easy 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 to implement the correct locking
 - Many lock managers are much 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 component
- Installations on top of GFS exist, RedHat will ship it



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



NTFS ACL support

- Samba 3 is a „good“ Unix process
 - Access Controls are done by the kernel, Samba does „su - <authenticated user>“
- Posix ACLs are very limited
 - Only rwx, NFSv4 modeled after the 13 NTFS rights
 - Posix can't delegate right to set ACLs
- Samba 3.3 contains `acl_xattr` and `acl_tdb` modules
 - Optional full NTFS Acls in user space



Async libsmbclient

- A blog entry by Felix von Leitner (fefe) stating Samba's performance sucks made me think...
- Serial read performance using SMB is limited by the 64k request limit
 - Larger requests work, but that's Samba only
 - SMB can be multiplexed: More than one request on the fly: 3.2 smbclient is heavily tuned
- Using 10GigE, „smbclient get“ I've seen >700MBytes/sec against a Samba server reading from ramdisk



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 :-)



SMB2

- New protocol introduced with Windows Vista
- Mostly done because SMB1 implementations carry too much historical code
- Basic SMB2 is semantically very similar to SMB1
 - Main call CreateFile is almost the same
- New protocol features added only to SMB2
- Durable File handles: Open files survive a network reconnect



SMB2 in Samba

- First prototype implementation in Samba4
 - No docs available yet, so the client library and torture suite was done first to discover the protocol
- Microsoft now has opened the specs for SMB2
- Stefan Metzmacher has implemented SMB2 in S3
- Microsoft has tested Samba with their own test tools
 - This accidentally ran against the S3 SMB2 code, worked fine...
- Durable file handles to be developed



AD Protocol Mix

- Active Directory: A big mix of protocols
- LDAP: User database held in a directory
 - Lots of other stuff moved there
- Kerberos: Authentication protocol
 - Extensions for authorization
- Tons of RPC services
 - NETLOGON, SAMR, LSA, DRSUAPI, etc
- DNS, NTP, CLDAP, etc



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
- 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
- Subsystems shared between 3 and 4 (tdb, talloc, etc)



Active Directory Domain Controller

- The main services beyond NT4: LDAP and Kerberos
 - RPC services have been extended as well
- Kerberos is almost standard, Samba4 ships heimdal
- LDAP has been extended extensively for AD
 - DRSUAPI for multi-master replication
 - Many improvements for scalability and consistency
- Samba4's LDAP/DRSUAPI server is right now under heavy development
 - Corporate interests by many vendors



RPC services

- RPC services: SAMR, LSA, NETLOGON, DRSUAPI
 - SAMR: User/Group Management
 - LSA: Misc security stuff, SID<->Name translation
 - NETLOGON: NTLM authentication
 - DRSUAPI: Directory Replication
- SAMR and LSA required by normal file servers
- NETLOGON required on DCs
- DRSUAPI required on Active Directory DCs



RPC services

- SAMR, LSA and NETLOGON exist in Samba 3 now
 - Smbpasswd, tdbsam and ldap as databases
- Samba 4 has its own directory as backend
 - SAMR, LSA and NETLOGON connect only there
- pdb_ads was added to Samba 3
 - Contact the local Samba4 directory
 - „smbpasswd -a“ creates an AD user now



Current work in Samba4

- Andrew Tridgell and Andrew Bartlett are heavily working on AD replication
 - First success: A W2k8 DC joined a S4 domain and replicated
- People from Postpath (Cisco) are working on ACLs on directory objects
- Many other people are working on minor things
 - S4 seems to attract more developers than S3. For some weird reason developing new things is more attractive than fixing old bugs....



Naming things: What will Samba4 be?

- Samba-FS
 - Samba3 SMB server with NT PDC support
- Samba-AuthD
 - Samba3 winbind
 - Domain membership, trust handling on Dcs
- Samba-HD (HyperDirectory ;-)
 - Not trademarked...
 - Samba4 AD server



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>



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>

