Samba

OpenLDAP Developer’s Day
Tübingen

Volker Lendecke, Günther Deschner

Samba Team

VL@samba.org, GD@samba.org
http://samba.org

Overview

- OpenLDAP/Samba in the past
- Samba3 directions
- Samba4
- Samba4/AD
- Wishes by the Samba3 people

Volker Lendecke

- Samba Team Member
- Co-Founder SerNet GmbH
- SerNet: Open Source and Network Security services
- 30 employees, 5 exclusively for Samba

Samba3

- Based on first code from 1991
- Stable production branch
- NT4-style Domain Controller
- Can use LDAP as password database
- Can contact AD for user information
- Gerald Carter, Jeremy Allison, Günther Deschner, Volker Lendecke

Samba4

- New from Scratch, originally for cluster development
- Lots of research for 100% CIFS procotol support
- Internally most databases are based on ldb, a simple on-disk library with LDAP-like data model and API
- Main target nowadays: AD domain controller
  - AD used to be largely an unknown, thus for research we needed a familiar code base for research
- Andrew Tridgell, Andrew Bartlett, Stefan Metzmacher, Jelmer Vernooji, Simo Sorce (did I forget anyone?)

Samba3/LDAP

- Samba uses LDAP as a pure database
- Historically little more than NT/LM style password store
- More and more info is put into LDAP
  - Windows-style Group information (Aliases/Local groups)
  - Account policies
  - SID⇔Unix ID mappings

Samba/LDAP pitfalls

- German Parliament most prominent failure
- Samba historically used to rely *only* on nss for user/group info
- Glibc 2.3.2 crashed on `getgrouplist()`: Enumerating posixGroup for member information was necessary
- For Samba 3.0.14 a lot of work was done to streamline the LDAP queries

Samba/LDAP annoyances

- Windows provides remote user management via SAMR pipe (usrmgr.exe)
- Changes need to be reflected in LDAP
- Normally shell/perl scripts called from Samba are used
  - Inefficient, tricky configuration
  - Lots of policy (Tree layout etc) put into config files
- Newer Samba versions can edit the tree without external scripts, with only very little policy configuration possible.

Samba3 directions

- Better SMB file serving, extensions to integrate Linux clients, transport Posix semantics via SMB
- Cluster SMB file servers
- More complete NT4 compatibility as domain controller
- Improving Linux client integration into Windows environments
- Exec summary: Business as usual, fix bugs, tiny steps

Samba4

- Started out as a new Virtual File System layer in Samba3
- Tridge wanted to make Samba3 cluster-aware
- Samba3 file server code in bad shape at that time, at the time the code was written we did not *really* know what's going on
- He started Samba4 from scratch with the 10 years of CIFS experience

Samba4

- For 1.5 years this was a one-man show with very little public results
- A lot of work has been put into good infrastructure
- talloc, transactional tdb, ldb, async architecture
- In Samba4 it is a lot easier to implement prototype protocol implementations, Samba4 does not need to support the > 330 parameters Samba3 has

Samba4 directions

- Samba as a project is competing with Microsoft, as Jerry said: We have no shame in doing everything Windows does.
- Samba has lost one of the selling points: W2k3 is a stable, mature product
- Samba3 is 10 years behind on important features, Samba *has* to be an Active Directory Domain Controller
- Andrew Bartlett: ’Almost, but not entirely unlike LDAP’

Options for Samba/AD

- Who listens on 389?
- Clients expect AD, not LDAP on port 389.
- Extend OpenLDAP?
  - Main obstacle for us: Unknown code base
- Current approach: Proxy to standard Directory
  - Quite a few translations necessary, see Andrew's talk on http://samba.org/ abartlet/samba-war-stories-notemplate.pdf

Wish for Samba3

- Access to the data stream before it hits the net
- This would enable us to implement async operations, we could weave libldap into our events model
  - The inability to get real async client operations with libldap was the main reason for me to do my own libs.
- We could implement SASL sign/seal
  - Yes, Cyrus SASL exists, but this is yet another unknown code base. . .

Cooperation, yesterdays dinner

- Cooperation on authentication
- Using Samba as an auth source for OpenLDAP
  - What do you need? We have MD5 of the user's password
- Using OpenLDAP for more than a DB (passwords not readable)
  - MS protocols allow for some authentication forwarding (Domain member / trusted domains)
  - OpenLDAP would have to be a full"DC protocol-wise