Samba4 and Directory Services

Andrew Bartlett
Samba Team

Who Am I

- Samba Developer
- Authentication Systems
  - I care about who you are
- Directory Services
  - I've enjoyed the more painful parts of actually using them
- Real World Experience
  - Samba at Hawker College

Identity Management

- Key part of any large organisation
  - HR
  - E-mail
  - Login details
  - Organisation structure
- Typical use for a Directory Server

Directory Servers

- A number of Free and Proprietary vendors:
  - OpenLDAP
  - eDirectory
  - Apple Open Directory
  - Fedora/RedHat directory
- All have particular challenges
  - Particularly in password management

Windows Client Support: Missing

- Poor LDAP vendor support for windows clients
- Some use Samba3
- Some sync with AD
- Some ignore the problem
- Can Samba4 provide that AD Client support?

Samba3 as a Directory Client

- Samba3 is a directory client only
  - Mostly this is a pain
    - It forces users to fight OpenLDAP
    - Many aspects become 'not our problem'
  - Sometimes a benifit
    - Well administered centralised networks
    - Good sharing of attributes with traditional schema
  - Products
    - Traditional OpenLDAP/Samba setup
    - Samba3 backed by Novell's eDirectory
    - Apple's Open Directory uses Samba3

Samba4 as a Directory Server

- Directory service interfaces are required by clients
- Could become a general purpose directory?
  - Integrated KDC/PDC/LDAP already attracted interest
  - Perhaps an LDAP server for Samba3?
- Should it?
  - What is the development cost of general purpose LDAP?

Samba4 as a Directory Client

- Could Samba4 be a client to another directory?
  - Already works Samba4 -> Samba4 LDAP
- Would this make Samba4 attractive to directories vendors?
- Could this avoid 'sync with AD' cludges?
  - Assuming Samba4 provides the 'bits' of AD a site requires
- Can we back Samba4 by Microsoft's LDAP, for testing?

Advantages

- Replication
  - We can get internal replication 'for free'
  - Even multi-master replication with Fedora DS
- Scalability
  - Backend already tweaked etc
- Vendor Interest
  - AD support should be a great way to sell your directory product

Challenges

- Back in Samba3's land with configuration
  - At least it is now optional
- Schema translation
  - We have a start, but there is along way to go

Infrastructure to be built

- We need to finish SASL support:
  - GSSAPI bulk encryption buffer size issues
- Digest-MD5
  - An Internet standard shared-secret mechanism
- TLS/SSL and 'EXTERNAL'
  - Identify to the LDAP server with an SSL cert
- LDB modules for partitions
  - We will not want to outsource all parts of the directory

Schema

- Samba's schema is a mess:
  - Partly Microsoft's schema
  - ...with our own extensions
- We need to either:
  - Write valid schema for our extensions or
  - Drop them or
  - Hide/fake them (make the backend not seem them)
- We need to convert schema into OpenLDAP/FedoraDS/etc format

Who holds the passwords?

- The LDAP server is a good 'store'
  - Ensures passwords are deleted with the user
  - Keeps password and password-related attributes close
  - But won't understand most of the passwords

Password abstraction

- Apple's Password Server
  - Apple runs Samba3 without showing Samba the passwords
- NSS Crypto abstraction
  - RedHat directory folks maintain NSS
  - This has an 'at arms length' crypto abstraction
- AD won't expose the passwords over LDAP
- Probably not worth running a KDC 'at arms length'

What should LDAP look like?

- How smart should the backend LDAP server be?
- Two extremes:
  - Just a key-value pair database
    - Racy, unless it supports transactions
  - Complete backend
    - Re-implement/port most of our modules into arbitrary LDAP servers
    - Fully manage authentication
    - Clients talk to this LDAP server

Likely LDAP solution

- Backend (LDAP Server)
  - Password management
  - Group membership (update memberOf)
- Frontend (Samba)
  - Authentication
  - Non-standard features

Complications

- Two LDAP ports?
- Multiple IPs?
- Windows Clients -> Samba4
- Other Clients -> Direct?

Is it worth it?

- Using an external LDAP server may simply be too high a cost
- Perhaps we end up back at synchronization