Samba4 and Directory Backends

Andrew Bartlett
Samba Team
Red Hat Inc

A year on

- Last year, I presented some vapor ware
- Looked at ideas of directory intergration
- But it is the code that really counts...

Samba4 and LDAP backends

- First hacked up in June
  - But relied on no schema checking
- Martin Kuehl
  - Summer of Code student
  - Fixed up Jelmer's ldb_map
- 'make test' Passed against OpenLDAP in September

ldb_map

- Generic mapping for LDAP
- Rename attributes/objectClasses
  - Work around conflicts with vendor/standard LDAP classes
  - Use LDAP server for GUID/modifyTime etc
  - Possibly a different backend schema...
- Add 'extensibleObject' to all entries
- Re-filters results

ad2OLschema

- Conversion binary to create schema for backends
- Reads a mapping file of 'horrors'
  - Standard OpenLDAP attributes
- These conflict with OpenLDAP builtins
  - objectClasses
  - subSchema
  - ModifyTimestamp

More horrors

- Conflicting OIDs
  - MiddleName
  - defaultGroup
- A large integer format is unimplemented in OpenLDAP 2.3
- A case insensitive string isn't available
- A DN syntax isn't in OpenLDAP
- Treat Security Descriptors as binary

Why OpenLDAP first?

- Started on OpenLDAP when experimenting with Apple
- Initially easier to manage
  - Ldapi:// support
  - Easily scripted start

Fedora DS

- I work for Red Hat's directory services and security group
- Fedora DS is 'our' product
  - GPL + additional permissions
- Useful features:
  - Multi-master replication
- Idea:
  - Multi-master replicated Samba4?

Challenges

- OpenLDAP and bitwise operations
  - Bugs in handling of MAX_INT values
- Fedora DS and bitwise operations
  - Initially unsupported
  - Now a plugin
- Fedora DS didn't support ldapi://
  - OpenLDAP specific 'standard'
  - Darn useful...

Schema Challenges

- First did this work against OpenLDAP 2.1
  - Schema checking off
- Builtin Schema in OpenLDAP
  - Can't override certain definitions
- Fedora DS schema
  - 00core.ldif wasn't the real core
  - Needed to cut it down to the real core

More Challenges

- Not part of the standard testsuite
  - Jelmer kept breaking my 'magic' TEST_LDAP
- Untested code is broken code
  - Build farm host 'node1' runs OpenLDAP
- One day, I hope it is a standard part of 'make test'
  - enable these tests with OpenLDAP or FDS installed

Demonstration

- One Samba4 domain
- Two Domain Controllers
- Both backed onto a Fedora DS replica
  - Each DC talking to localhost:2389
- No manual configuration of PDC/BDC
  - This configuration is in the directory

HOWTO

- Setup replication agreement
- Provision both servers
  - This actually fills and wipes the DB...
- 'net join' BDC to PDC
- Add “NTDS Setting” object for BDC
  - Metze's new join code would do this

Demo

- Join WinXP to Samba4 domain
- Show both DCs are available
- Shut down other DC
  - Ie, the one not joined to
  - Show that we can still log in

Shortcomings

- Not sure of interactions with DRSUAPI
  - Probably for 'pure samba4' domains only
- No mapping support for existing servers
  - Project to have this work against a Samba3 schema never really went anywhere
  - More practical to have Samba4 against an alternate extended schema

Possibilities

- Replace AD sync tool for Fedora DS with 'native' replication?
  - Use Fedora DS schema as the mapping backend

Smart Card Login

- The vaporware half of the talk..
- Samba4 smart card status:
  - Built on Heimdal's PKINIT
  - PKINIT is kerberos login with a public key
  - PKINIT demonstrated in 'make test'
  - No demonstration with windows clients yet

The market is in the middle

- Most smart-card middle ware is proprietary
- Drivers, card OS, enrollment
  - This controls many of the 'interesting' parts of Smart Card
- RedHat has CoolKey and ESC
  - But it requires Certificate System as a backend
  - CS is big, and currently proprietary
    - I'm assured they are working hard to make it Open Source
  - Demo of smart-card insertion

Useful ways to start with smart-cards

- Be able to load a key and certificate onto a CoolKey
- Run a micro-CA for easy, scripted testing
- Virtual (QEMU) smartcards would be **very** handy