Samba4 Status Update

Against the odds: Challenges and successes building Samba4

Jelmer Vernooij
Andrew Bartlett
Samba Team

Samba Domains: Who would have thought?

- First Samba Domain work back in 1996
- Samba ntdom, TNG, 2.0
- Samba 2.2 makes domain logons production
- Samba 3.0 takes it seriously
  - But massive changes still take place
- Samba4: The Active Directory challenge

Samba 4: A new start

- Why not just Samba 3.0?
    - 'Active Directory'
    - Kerberos logins
    - Chance to ditch NTLM
    - Hoping for group policy
    - Provide a way 'out' when NT4 compatibility vanishes
    - New infrastructure for multiple protocols

Samba4: Where are we at?

- Past the 'rigged demo'
  - But real networks are more complex
- Domain logons work
  - Clients can join
  - KDC issues ticket with PACs
  - Clients login to a Kerberos environment
  - Similar 'user experience' to Samba3
  - No trusted domains, forests, poor group manipulations, etc...

samba

A year's progress

- Major changes
  - Lots of work on LDB and the LDAP server
  - EJS and SWAT2
  - Kerberos logons on Windows, PAC
  - Vampire
  - WINS replication
  - More asynchronous interfaces
  - NTVFS POSIX backend
  - File notification
  - ... and lots and lots of bugfixes

New infrastructure: But less implementation

- PIDL
- New talloc()
- LDB
- New client libraries
- New ejs-based SWAT
- Event sub-system
- Multi-protocol
- Shared libraries
  - Internal subsystems
  - Externally available libraries
  - Driven by OpenChange

First technology Previews

- First technology preview out
  - Not complete enough for any production use
    - TP1 released during Linux.Conf.Au
    - TP3 due out during this conference
- First alphas will have a basic feature set
  - Technology previews will be released until then

sam‍ba

Work in progress

- Documentation (manpages, howto)
- Upgrade from Samba3
- Support for scripting in Python
- Winbind
    - Architecture in place
- Printing
    - Skeleton in place
- Lanman Browsing
- Watching changes in info levels
- Other work across the suite

Early dividends

- Samba3 is better because of Samba4 research:
  - Transactional TDB
  - NTLMSSP code in 3.0.21
  - readdir() changes
  - Testsuite
  - PIDL
- Near-future backporting
  - PIDL on all pipes
  - RPC client infrastructure
  - inotify()

samba

Samba4 Alpha features

- Before we release an alpha, we will have:
  - Primitive AD Domain Logon
    - Just doing the join/logon enough for some workgroups
    - Similar to what Samba 2.2 was with NT4
  - Platform for future Group Policy implemention
    - We think it's easy, but not sure yet
  - MMC support
  - Command line tools
  - Samba3 client support

samba

The ideal first Samba4 site

- Experienced Sysadmin
  - Samba, Kerberos and LDAP experience
- Needs Kerberos integration at the domain logon stage
- Not yet running AD
  - Needs only a subset of AD Features and compatibility
- Small network (single DC)
- Multi-platform clients environment
  - Mac, windows, Linux

Why do developers want this

- A basis for research
- A vision for how we could do things
- A prototype for what we need
- Allow features to grow
  - Kindergarten for very different features

samba

Longer odds

- Some things are still a longer way off
  - Exchange support?
    - As soon as you say 'AD', folks want exchange to work...
  - Full Schema
  - Replication against Windows
  - Trust Relationships
  - DHCP extensions
  - DDNS
  - Microsoft's File System replication
  - etc
- User expectations are another can of worms

Against the quality odds

- Focus on testing
  - Both for Samba3 and Samba4
  - Trying to increase coverage
- Focus on autogenerated code
  - Fix the bug once in the generator
- Over 160 torture tests
- Build farm
  - Valgrind
  - IBM Checker

samba

Against the political odds

- Writing your 'own' KDC and LDAP server
  - Scares people
  - Upsets established players
  - Was essential to current progress
- Making development releases
  - Needs careful expectation management
  - 'Should I wait for Samba4?'
  - How to describe early development releases?
    - Technology Preview currently
    - High expectations on 'alpha' and 'beta'
  - How to describe lack of functionality

Against the research odds

- Writing and testing unknown protocols is hard
- SMB2
    – Introduced in Vista
    – Primitive client implementation
    – Even more primitive server implementation
    – Testsuite
- Kerberos error codes
    – Mapping and including NTSTATUS codes
- PAC signatures

Cans of worms

- DSUSAPI Cracknames
  - A 'simple' translation call
  - Any to any translation of names
    - 12 Name types
    - 8 direct meaningful errors
    - Not all combinations defined
  - Flags
    - Syntactic only
    - Eval at DC
    - Global Catalog Verify
- Samba4 has a partial, local only implementation

More worms

- How many different ways can you evaluate a password login?
    - RPC-SAMSYNC test tries:
        - 36 function and level combinations
        - 22 different NTLM variations
        - 14 different username types
        - Including when your previous password is still accepted!
    - NTLMSSP flags are in addition to this