Samba4 status report

Andrew Tridgell
Samba Team

Technology Preview Release

- We have just released Samba 4.0.0-tp1
  - supports being an active directory domain controller
  - supports true NT ACLs and file streams
  - includes a replicating WINS server
  - builtin LDAP and Kerberos servers
- What is a technology preview?
  - not a production release!
  - a way to encourage more people to get involved
  - many core features are still missing

Integrated Heimdal

- Kerberos is central to ADS support
  - needs to be closely integrated with LDAP and RPC
  - needs to support Microsoft kerberos extensions
- Integrated Heimdal
  - worked closely with Heimdal developer Love Astrand
  - developed an embeddable version of Heimdal
  - integrated into Samba4 source tree

External Kerberos?

- Why not an external kerberos lib?
  - The need for a common storage backend for all Samba components
  - We need bleeding edge kerberos features, and updating the system kerberos lib is notoriously tricky
- Common KDC backend
  - Embedded Heimdal can provide this via pluggable storage backends
  - In the future we hope that it will be possible to use external MIT or Heimdal kerberos in a similar way

Web Management

- Poor management tools
  - Samba has historically suffered from poor management tools
  - hope to fix this with a new web management system
- based on embedded javascript engine
  - makes for easier web interface development
  - allows for scripting objects to be passed from browser to server
- Usability and security features
  - automatic TLS/SSL setup and certificate generation
  - automatic https discovery

LDAP and ldb

- LDAP schema
  - now support a ADS compatible schema
  - much more detailed schema records than traditional OpenLDAP schema
  - schema holds information on management layout, and default class ACLs
- LDAP controls
  - ldb now supports a number of LDAP controls
  - server_sort, notification, paged_results, asq, extended_dn, dirsync
- Other new features
  - support for operational (computed) attributes
  - integrated rootDSE module
  - more sophisticated SAM module

ejs engine

- Scripting for Samba
  - Samba4 includes an embedded scripting engine called 'ejs', a mini-JavaScript implementation
  - Used both for command line tools and web management
  - Integrated with the Samba library of C code
- Code generation
  - New pidl backend to auto-generate ejs bindings for RPC calls
  - allows for easy scripting of windows management calls
- talloc integration
  - needed auto-cleaned of embedded C objects when js variables went out of scope
  - used talloc destructors and wrapper objects in js

Vampire Demo

- Take over a domain
  - start with a win2003 PDC, and member servers
  - use Samba4 SWAT to 'upgrade' to Samba
  - pull all accounts, passwords and attributes from Windows domain
  - shutdown the old PDC
  - Samba4 starts up as new PDC

Whats next

- Management Interface
  - The new SWAT is a good start, but lots more work needed!
- Printing
  - Currently Samba4 does not support printing at all
  - port Samba3 print backend to Samba4, re-worked to use Samba4 RPC infrastructure
- Re-add lots of missing features
  - Many Samba3 features have been lost in the development of Samba4
- Lots more ldap work
  - more schema work, full MMC support, ACLs on ldb records

SMB2 Network Analysis

- SMB2 is a new variant of SMB
  - first seen in Vista preview releases
  - Samba4 includes an initial implementation
  - totally different packet structure from old SMB
  - reported to have support for database style transactions?
- The challenge!
  - no documentation on SMB2 at all
  - can we implement both client and server SMB2 using the same network analysis techniques we used for SMB ?

Decoding SMB2

- Basic steps
  - work out how to break protocol into separate requests
  - work out header/body structure
  - decipher header fields
  - find possible opcodes
  - decode each opcode payload

Modifying proxy

- sockspy-smb2
  - setup as proxy between two Vista boxes
  - modify fields and watch effect
- Field properties
  - Can add some bits to a value? Probably a flags field
  - Can invert all bits in a value? Probably an opaque token
  - Only accepts a small range of values? Probably an opcode or enumerated type

Opcode Scanning

- SMB2-SCAN
  - try all possible opcodes
  - look for error code change
  - don't need to actually get a NT_STATUS_OK, just looking for a change, any change, from a unknown opcode
- Once found
  - When an opcode is found, next step is to produce a successful call
  - try randomised data, biased to small values