Heimdal Status Update

by Nicolas Williams for Heimdal developers

Heimdal 1.6 is dead

- OS distributions shipped broken pre-1.6 releases as 1.6 sowing confusion
- 1.6 took too long, too many commits have hit master since the last rc
- We're going to skip to release 1.7 instead

Changes Since 1.6rc2

- Bug fixes
- Contributions from Samba team for interop
- Feature removals
- Features

Bug Fixes Since 1.6rc2

- kadmin/kadmind key management
- Referrals (client) fixes
- GSS fixes for functions like gss_store_cred() and gss_acquire_cred_with_password()
  - Needed by ssh
- Samba interop bugs
- Bugs found by coverity

Features Removed

- kx, kf, and friends now removed from the tree
- use ssh instead

Notable New Features

- Improved daemonization functionality
- Added ext_keytab --random-key option
- Improved error messages from ccache
- Added (fixed and documented) name canonicalization rules

Other Notable Changes

- ktutil and kadmin moved to bindir from sbindir

STATUS, TODO

- Code review and merge outstanding PRs
- Make Heimdal’s use of OpenSSL RAND_bytes() thread safe
- Finish large iprop bugfix wad, but if it takes too long we can leave this for 1.8
    - Race conditions between master and slaves related to renames
    - Safety in general

STATUS, TODO for iprop

- New scheme is a two-phase commit with roll-forward. iprop log and HDB locks taken, tx appended to iprop log, tx written to HDB, on success a header entry in the iprop log is updated to point to the tx just completed

- Roll-forward at next write transaction

- Unconfirmed transactions are not replicated

STATUS, TODO for iprop

- iproplog command improved
  - can view log forward, backward, with and without locking, can truncate and keep N records
- SQLite and LMDB HDB backend fixes
- (regression tests implement)

What Comes After 1.7

- 1.8, natch
- No plans at this time, but as usual things will come up
- Many ideas
  - Improved logging in kdc
  - Tracing in libraries

What Comes After 1.7

- New gss additions
- Kerberos extensions
    - New enctypes
    - Multiple round trips for gss mech, for error recovery, user-to-user, and so on
    - PKCROSS would be nice...