MIT KDC integration

Andreas Schneider <asn@samba.org>
Günther Deschner <gd@samba.org>

Red Hat

May 21th, 2015

Who we are?

We both

- are Samba Team members
- work for Red Hat on Samba
- love rock climbing
- and love Frankonian beer (an important part of rock climbing)

MIT KDC integration

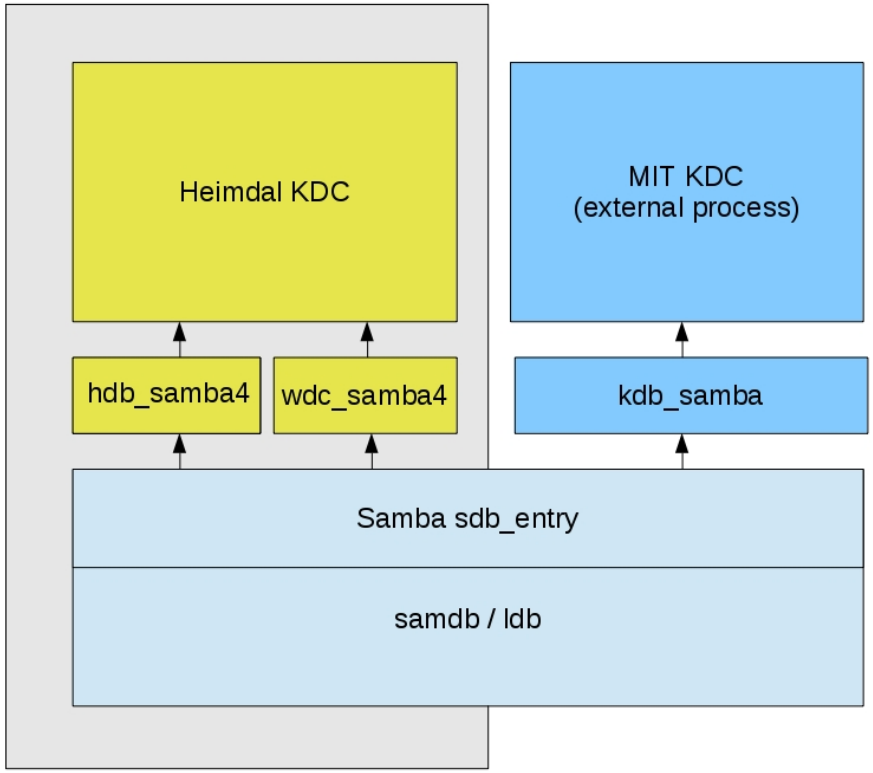
MIT KDC integration

HDB, KDB, SDB

New SDB layer

- simple abstraction of samba_kdc routines into a new sdb layer
- provides conversion routines into HDB and KDB formats (for Heimdal and MIT KDCs)
- Samba builds either MIT or Heimdal plugin, not both
- KDB plugin works for a MIT KDC (version greater 1.10)

New KDC backend layering



MIT KDC integration

Microsoft Kerberos Testsuite

Microsoft Interopability Event September 2014 in Redmond

- MS testsuite testing Samba/MIT KDC with new kdb_samba driver
- Some issues found:
  - kdb_samba driver failed encryption type negotiation
  - ARCFOUR-HMAC-MD5 was the only enctype used
  - Re-ordering enabled AES enctypes
  - Salting issues with salting principals for AES
  - kpasswd support via kadmind

Microsoft Protocol Test Suites

- Publically available: "Kerberos Protocol Test Suite"
- Supports different scenarios
- Report generation
- See "Open Specifications Dev Center" for further details
  `https://msdn.microsoft.com/openspecifications`

MIT KDC integration

The libkrb5 DNS discovery problem

libkrb5 could not find its DC

- We needed support for service discovery via DNS
- We had some DNS faking in the Samba developer build
- BUT: Samba DNS faking did not work with system libraries

resolv_wrapper

- This wraps functions from libresolv.so; res_query(3), res_search(3)
- We have two modes:
  1. Create your own resolv.conf and redirect everything to your DNS server
  2. Fake queries from a simple DNS file
- This is for querying SRV, SOA or CNAME records ...

`https://cwrap.org/resolv_wrapper.html`

resolv_wrapper in Samba Selftest

- resolv_wrapper is preloaded in Selftest
- Currently only supports DNS faking
  - The internal DNS implementation does not correctly handle SOA records, so we can't send DNS queries to it yet
- The system libkrb5 can now do SRV record lookups to discover the KDC

MIT KDC integration

kpasswd support

- "Microsoft Windows 2000 Kerberos Change Password and Set Password Protocols" (RFC3244)
- The 'kpasswd' client from MIT Kerberos did not work
- In MIT Kerberos the kpasswd protocol is implemented in kadmind
- $\Rightarrow$ We needed to start kadmind
- Password Set variant still needs ACL handling

kadmind

- The MIT Kerberos administration server
- Allows administrative tasks via kadmin or kadmin.local tool
- $\Rightarrow$ e.g. modify principals, export keytabs

MIT KDC integration

Netlogon PAC validation

- Netlogon has a logon mode to validate a PAC
- Samba implements an IRPC service to allow that
- Basically the service checks if the signature of the PAC is valid
- When we start the MIT KDC we also set up the IRPC service

MIT KDC integration

What has gone upstream?

- Bugfixes, bugfixes, bugfixes...
- New cwrap components e.g. resolv_wrapper
- Fixes for enabling/disabling parts of the Samba DC for MIT or Heimdal
- Switch to krb5 API calls and structs from private HDB calls and structs
- General migration away from HDB where possible

MIT KDC integration

Under review:

- SDB database abstraction
- KDB samba module
- Automatic MIT KDC detection and/or startup
- selftest and autobuild integration

Under discussion:

- Removal of Heimdal codebase or at least moving it to the "thirdparty" repository
- last Heimdal import was: Mon Jul 25 18:51:53 2011 +0200

TODOs:

- Password set protocol with ACL support
- Full gss_wrap_iov support for Heimdal?
- S4U2SELF/S4U2PROXY support
- Client application (kinit, kpasswd) parameters used in selftest
- Porting new smbtorture krb5 tests to MIT
- samba-tool support for provisioning an MIT KDC with samba backend

How to set it up?

- Fetch git repository from:
  `https://git.samba.org/?p=asn/samba.git;a=shortlog;h=refs/heads/master-mit-kdc`
- Install a MIT Kerberos KDC package
- Compile Samba with –with-system-mitkrb5
- Create kdc.conf and krb5.conf, FIXME: example
- Start samba binary

MIT KDC integration

The problem of Heimdal development

- Core maintainer at Apple
- Project is unactive, no releases
- Maintenance repository on github
- Unclear roadmap (if any)
- Example: gss_wrap_iov

MIT KDC integration

Questions & Answers