The road to MIT KRB5 support

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

Red Hat

May 14th, 2014

The road to MIT KRB5 support

The road to MIT KRB5 support

Why Heimdal Kerberos KDC?

Heimdal and Samba4 AD development

- Kerberos implementation of choice during Samba4 development
- most advanced in AD support at the time
- close relationship with Heimdal community

Why Heimdal Kerberos KDC?

Heimdal KDC technical features

- plugin APIs for implementing Active Directory KDC features
- KDC can be built as a library
- KDC runs in the one-process model of the Samba binary
- KDC can be fully controlled in automated testing (buildfarm)

Heimdal plugin APIs

HDB

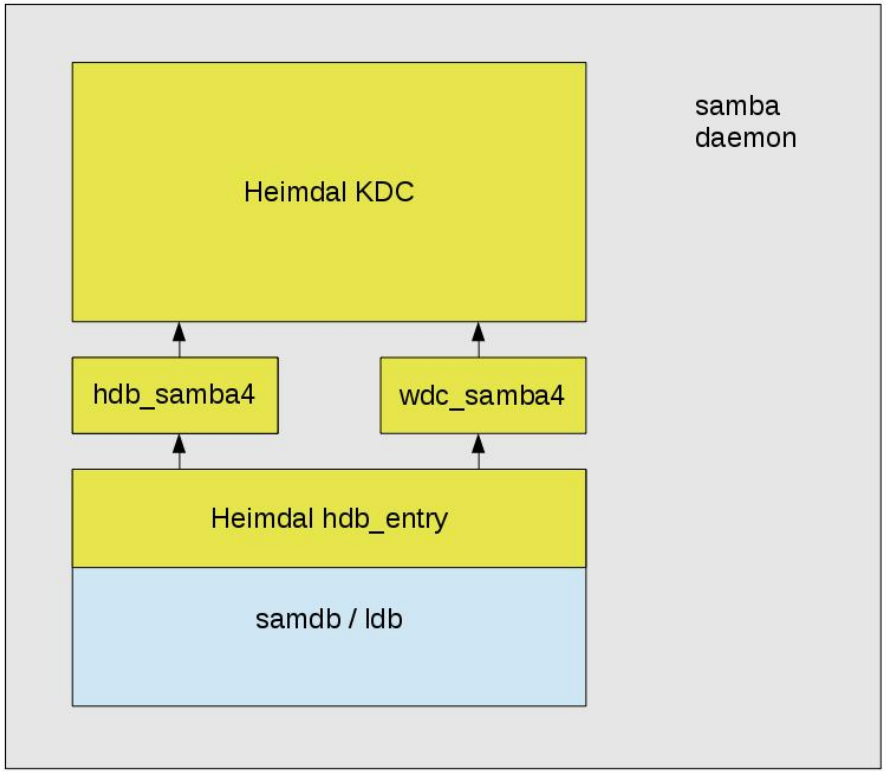
- HDB is database backend for principals and their properties
- provides hdb_entry object representation
- checks if S4U2SELF or S4U2PROXY is allowed for account
- update bad password counters, etc.
- Samba provides HDB_SAMBA4 module

Heimdal plugin APIs

WINDC

- layer to process Kerberos PACs
- krb5plugin_windc_pac_generate
- krb5plugin_windc_pac_verify
- krb5plugin_windc_client_access
- Samba provides WDC_SAMBA4 module

Current KDC backend layering



Why MIT Kerberos KDC?

- Heimdal Kerberos is not a supported component in Fedora and RedHat
- Most Linux vendors don't ship Heimdal Kerberos
- MIT Kerberos is industry standard Kerberos implementation
- Samba should be able to integrate into external components

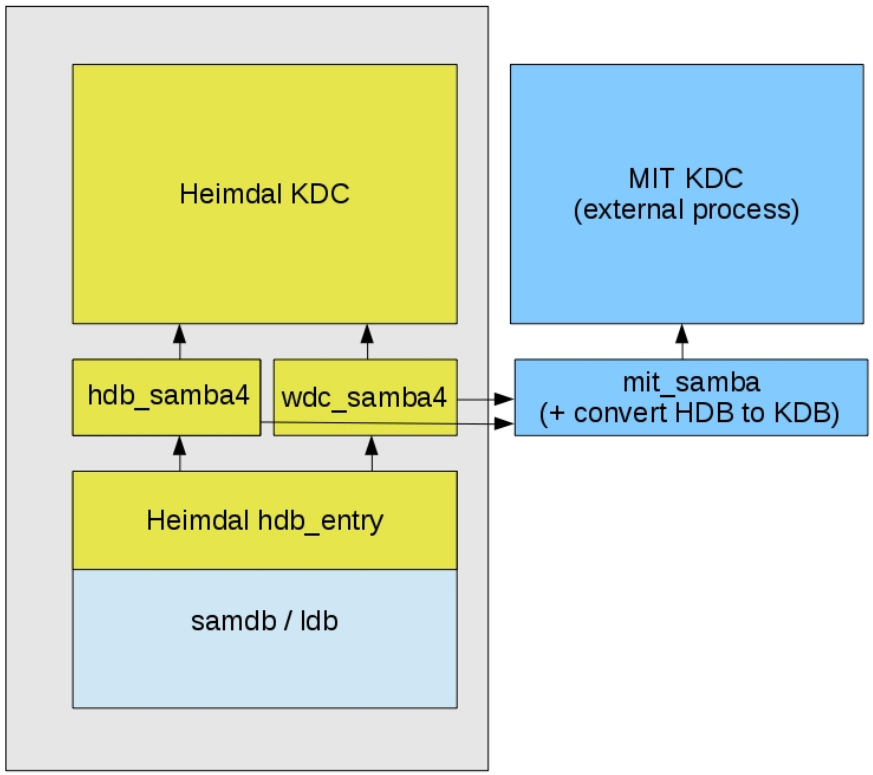
The road to MIT KRB5 support

mit_samba

plugin (2010) mit_samba.so

- written in 2010 by Simo Sorce
- wrapped around HDB_SAMBA4 and WDC_SAMBA4 code
- plugin needs to convert from Heimdal HDB format into MIT KDB format
- used and linked against native Heimdal codebase
- Heimdal code in MIT code

initial mit_samba plugin



mit_samba.so revamped

Building blocks for the mit_samba.so revamp

- new version needs to be testable from early on
- cwrap was a requirement
- krb5 wrap layer needs to able to compile all of the samba_kdc code
- hdb_entry needs to be abstracted

krb5_wrap

krb5_wrap

- abstraction layer to provide krb5 C functions that work with MIT **and** Heimdal
- initially created in the Samba 3 krb5 client code
- extended for the release of Samba 4 (Alexander Bokovoy et al)
- shim but very important layer, needs documentation btw.

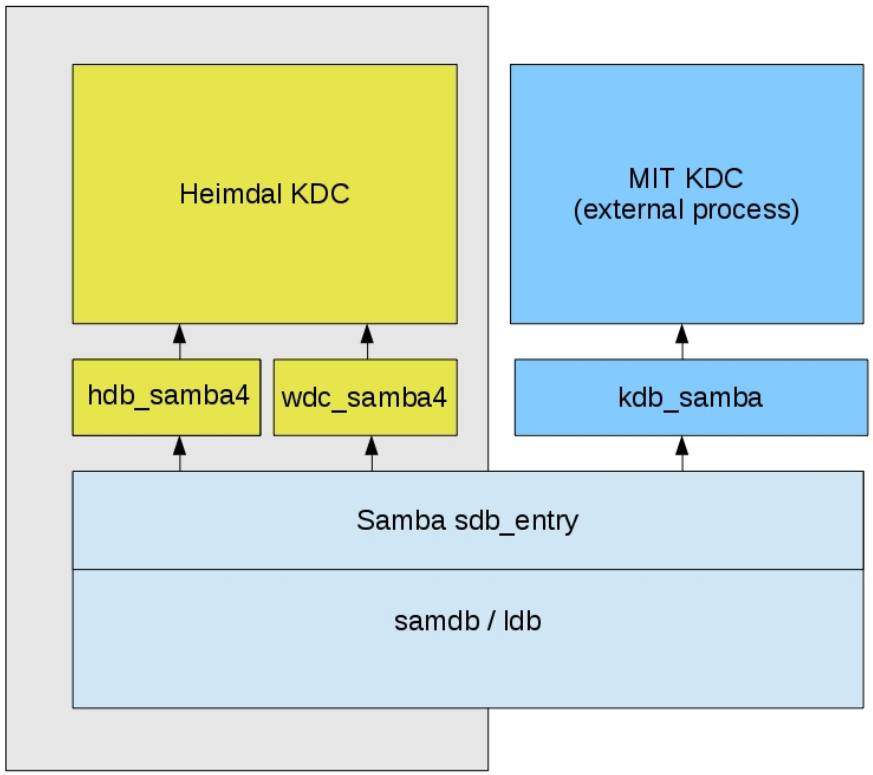
The road to MIT KRB5 support

HDB, KDB, SDB

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)
- future plan: avoid conversion, provide accessor functions

New KDC backend layering



The road to MIT KRB5 support

How do we get the Samba DC working with MIT Kerberos?

- We discussed this last year before and at SambaXP
- We came to the conclusion it isn't hard to do it
- **But how do we test it?**

The road to MIT KRB5 support

The cwrap project

- Samba has an huge and amazing testsuite.
- But we were only able to test code inside the Samba source tree
- So running and external process like the 'krb5kdc' was not possible
- The cwrap project has been created for this

The cwrap project

- The cwrap project has been created for this
- Makes it possible to test external processes
- Now we can integrate every compiled binary in our test environment
- The work on cwrap started at last SambaXP and finished at FOSDEM

The cwrap project

Consists of three wrapper libraries.

- socket_wrapper: Creates a fully isolated client/server network environment
- nss_wrapper: Artificial users and groups; dns name resolution
- uid_wrapper: Fakes privilege separation
- **More about cwrap in my talk tomorrow**

Latest socket_wrapper changes

socket_wrapper and krb5kdc

- Nalin Dahyabhai from Red Hat started to use it to test MIT Kerberos
- We fixed rebinding information on connect()
- Added support for IP_PKTINFO for UDP

The road to MIT KRB5 support

Tasks in Samba4

- We have services which are organized as tasks
- These tasks are e.g. rpc ldap s3fs dns kdc
- smb services = -kdc +mitkdc

The MIT KDC task

- Created a task to start the MIT 'krb5kdc' binary
- It is started like the smbd (s3fs) as a child of the samba daemon (DC)
- You configure it via the standard kdc.conf

The MIT KDC detection

- The 'krb5kdc' binary is detected during configure
- You can specify is with `--with-system-mitkdc`
- It can be overwritten in smb.conf with 'mit kdc command'
- `mit kdc command = /my/very/special/krb5kdc`

The testsuite

Testing system 'krb5kdc' in 'make test'

- We create a kdc.conf in our test env
- We load a special Samba KDB driver

The road to MIT KRB5 support

The KDB driver

This is the way the KDC gets access to information of the DC

- Rebased Simo Sorce his KDB driver on latest MIT KRB5
- Next step was to build the KDB plugin in the Samba tree
- This simplified some code

The road to MIT KRB5 support

MIT KDC branch

MIT KDC branch

- samba.git: http://tinyurl.com/m6gjrw8
- currently approx. 140 patches
- 75 files changed, 4284 insertions(+), 568 deletions(-)
- needs to pass all PAC and Kerberos testsuites we have
- move away from krb5 C functions to GSSAPI where possible
- revalidate "kerberos-porting-to-mit-notes.txt" document

The road to MIT KRB5 support

Questions & Answers

- Slides `http://www.samba.org/~asn/`