



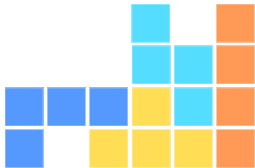
SAMBA AD

for the Enterprise

May 4th, 2017

Andreas Schneider

Red Hat Inc.



Who am I?

ABOUT ME

Free and Open Source Software developer working on:

- Samba - The domain controller and file server
- libssh - The SSH Library
- cwrap - Client/Server testing made easy
- cmocka - a unit testing framework for C

WHAT IS THIS TALK ABOUT?



SAMBA AD AND MIT KERBEROS

The talk will answer the following questions:

- What is Samba AD for the Enterprise?
- Are we there yet?
- How can I get my hands dirty?

SAMBA AD FOR THE ENTERPRISE



SAMBA ON RHEL/SLE

- RHEL/SLE only package Samba FS (File Server)
- Enterprise distributions are required to ship with MIT Kerberos



SAMBA AD PORTING

→ We need to port Samba AD to MIT Kerberos to get it into RHEL

HISTORY



CWRAP IN SAMBA

cwrap powers the Samba test environment and allows us to do complicated tests in a simple to use environment.



MIT KDB PLUGIN

May 2014: We also added the MIT KDB module upstream

- This way we were able to start the MIT KDC manually
- Started to find and fix bugs in Samba so it will work with MIT Kerberos



PATCHES PUSHED UPSTREAM

April 2015

- The MIT Kerberos patchset for Samba AD had more than 140 patches
- We pushed half of the patches upstream
- We had still 69 testsuites failing in Samba

FIXING TESTS

May - June 2015

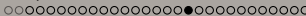
- We implemented missing features (exporting keytabs)
- We fixed a lot of tests (special MIT tests)



MISSING FEATURES IN MIT KERBEROS

July 2015

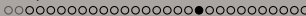
- Started to write missing features in MIT Kerberos
- Added support to deal with TLS encrypted connections



KADMIND

August 2015

- Added code to start kadmind from MIT Kerberos
- This is needed for password changing using the Kerberos protocol
- Then we realised that it doesn't support ACLs



SAMBA-TOOL

September 2015

- Started to implement DC provisioning using 'samba-tool'
- This means create a kdc.conf for MIT Kerberos

BACKUPKEY

November - December 2015

- Started to port backupkey to GnuTLS
- Encrypted secret storage [MS-BKRP]
- Found issues in GnuTLS
- Implemented missing RC4 stuff with Nikos in GnuTLS

KINIT AND KDC TESTS

January 2016

- More tests for MIT Kerberos
- Simple kinit tests



BUGS IN MIT KERBEROS

February 2016

- We found bugs in MIT Kerberos and fixed them
- Added more missing features in MIT Kerberos (`kinit --request-pac`)

TESTING WITH MIT KERBEROS

February - April 2016

- Started to implement special MIT KDC tests
- These already exists for Heimdal
- Important hooks for testing for pre-send/post-receive missing in MIT
- First step was implmenting those and getting them into MIT Kerberos

+ BADLOCK

KADMIND REVISTED

June - July 2016

- Do you remember the kadmind ACL issue?
- To fix this I've started to implement the kadmind in Samba itself
- GOAL: Share as much as possible between Heimdal and MIT Kerberos
- This involved porting the gensec_krb5 module

THE TRUST BUGS

August - September 2016

- I found the first bugs which showed issues with trusts
- We did not correctly pass credentials through winbind
- We ended up e.g. using the wrong realm requesting tickets
- Metze and I started a major rewrite of the client creds passed around in libsmb



STORING CREDENTIALS

December 2016

- Worked on storing the correct credentials in the right caches for trusted domains
- Some function of MIT behaved differently than Heimdal
- Some nicher GSSAPI functions are not available with Heimdal



MIT 1.15 NOT USEABLE

December 2016

- MIT Kerberos released version 1.15
- This version had a major issue
- They removed function which allowed memory management in KDB modules

ARE WE THERE YET?



MIT KERBEROS SUPPORT UPSTREAMED

2017-04-30 The code hit master!



WHEN?

When will we get Samba AD with MIT Kerberos?

???



WHEN?

When will we get Samba AD with MIT Kerberos?

September 2017



WHEN?

When will we get it in Fedora?

Fedora 27

SAMBA - ROLLING RELEASE



DEPENDENCIES

You need:

- MIT Kerberos $\geq 1.15.1$ (krb5-devel, krb5-server)
- GnuTLS $\geq 3.4.7$



BUILDING

```
./configure --with-system-mitkrb5  
make -j
```



WHAT WORKS?

All of the really important stuff!

- Single DC
- Forest trusts
- External trusts



WHAT IS MISSING?

- PKINIT support (should work, tests missing)
- Smartcard support
- Kerberos impersonation support (S4U2SELF/S4U2PROXY)
- RODC support (We need a libkdc from MIT Kerberos for that)

Questions & Answers

If you like this project tweet and blog about it!

<https://samba.org/>

<https://cwrap.org/>

<https://cmocka.org/>