

# SAMBA AD for the Enterprise

May 4th, 2017

Andreas Schneider

Red Hat Inc.



## Who am l?

#### ABOUT ME

Free and Open Source Software developer working on:

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

### WHAT IS THIS TALK ABOUT?

e we there yet? Samba - Rolling Release

#### SAMBA AD AND MIT KERBEROS

The talk will answer the following questions:

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

### SAMBA AD FOR THE ENTERPRISE

#### SAMBA ON RHEL/SLE

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

What is this talk about? O	Samba AD for the Enterprise	History 000000000000000000000000000000000000	Samba - Rolling Release 00000
SAMBA AD P	ORTING		

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

## HISTORY

What is this talk about? O	Samba AD for the Enterprise	History ••••••••••••••••••••••••••••••••••••	/	Samba - Rolling Release 00000
HISTORY X				

2013-2017

 What is this talk about?
 Samba AD for the Enterprise
 History
 Are we there yet?
 Samba - Rolling Release

 o
 o
 o
 o
 o
 o

#### HOW TO GET STARTED?

#### 2013: If we port to MIT Kerberos how do we run the tests?

#### THE CWRAP PROJECT

cwrap(socket\_wrapper): 2013-02-07 Andreas Schneider Initial commit

#### WHAT IS CWRAP?

### cwrap is..

a set of tools to create a fully isolated network environment to test client/server components on a single host, complete with synthetic account information, hostname resolution and privilege separation support. The heart of cwrap consists of four libraries you can preload to any executable.



Think of cwrap like it is

"The Matrix"

where reality is simulated and everything is a lie.

https://cwrap.org/

What is this talk about? O	Samba AD for the Enterprise	History 000000000000000000000000000000000000	/	Samba - Rolling Release 00000
CWRAP IN SA	AMBA			

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

History Are we

Are we there yet? Samba - Rolling Release

#### CWRAP IN SAMBA

#### Samba Testsuite with MIT Kerberos

ALL OK (14658 tests in 2030 testsuites) Test time 3h30min

#### CWRAP IN SAMBA

February 2014: We started to use cwrap in Samba 2014-02-13 Andreas Schneider selftest: Preload socket\_wrapper History Are v

we there yet? Samba - Rolling Release

#### SAMBA AND THE MIT KDC

At the same time Günther and I worked on the possibility to start the KDC and use it.

Günther Deschner and myself worked on the code together, till Günther changed teams. Stefan Metzmacher also participated from time to time.



April 2014: We introduced the sdb shim layer

- $\rightarrow$  Simple abstraction of Samba KDC routines
- $\rightarrow~{\rm Provides~conversion~between~Heimdal~HDB}$  and MIT KDB (KDC database plugins)
- $\rightarrow$  Günther Deschner wrote the SDB shim layer

#### MIT KDB PLUGIN

May 2014: We also added the MIT KDB module upstream

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

#### SAMBA AND CWRAP

May - August 2014

- $\rightarrow~{\rm cwrap}:$  We found missing features and impelmented them
- $\rightarrow~$  Samba: Changes for the gensec GSSAPI module to work with MIT
- $\rightarrow~$  Samba: Added more tests so we do not regress e.g. for kpasswd
- $\rightarrow$  MIT KRB5: Discovered bugs and reported them upstream
- $\rightarrow$  Started to work on resolv\_wrapper (August)

History Are we

re we there yet? Samba - Rolling Release 000 00000

#### SERVICE DISCOVERY

May 2014: We a discovered a new problem:

- $\rightarrow$  Service discovery in the Samba testsuite is not working
- $\rightarrow$  Started to work on resolv\_wrapper (August)

What is this talk about?	Samba AD for the Enterprise	History	Are we there yet?	Samba - Rolling Release
0		○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○	0000	00000
RESOLV_WR	ADDER			

#### September 2014: I've added resolv\_wrapper to Samba

History Are we

Are we there yet? Samba - Rolling Release 0000 00000

#### PATCHES PUSHED UPSTREAM

April 2015

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

#### **FIXING TESTS**

#### May - June 2015

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

HISTORY Are we

re we there yet? Samba - Rolling Release

#### MISSING FEATURES IN MIT KERBEROS

#### July 2015

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



### August 2015

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

#### September 2015

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

#### BACKUPKEY

November - December 2015

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

#### KINIT AND KDC TESTS

#### January 2016

- $\rightarrow$  More tests for MIT Kerberos
- $\rightarrow$  Simple kinit tests

History Are we

re we there yet? Samba - Rolling Release

#### **BUGS IN MIT KERBEROS**

#### Febuary 2016

- $\rightarrow~$  We found bugs in MIT Kerberos and fixed them
- → Added more missing features in MIT Kerberos (kinit --request-pac)

History Are we

Are we there yet? Samba - Rolling Release 0000 00000

#### TESTING WITH MIT KERBEROS

#### February - April 2016

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

#### KADMIND REVISTED

June - July 2016

- ightarrow Do you remember the kadmind ACL issue?
- ightarrow To fix this I've started to implement the kadmind in Samba itself
- $\rightarrow~$  GOAL: Share as much as possible between Heimdal and MIT Kerberos
- ightarrow This involved porting the gensec\_krb5 module

#### THE TRUST BUGS

August - September 2016

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

History Are we

re we there yet? Samba - Rolling Release

#### STORING CREDENTIALS

December 2016

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

#### MIT 1.15 NOT USEABLE

December 2016

- $\rightarrow$  MIT Kerberos released version 1.15
- $\rightarrow$  This version had a major issue
- $\rightarrow~{\rm They~removed}$  function which allowed memory management in KDB modules

#### **GENSEC FUN**

January 2017

- → I discovered gensec requests tickets with the principal: cifs/HOSTNAME@(null)
- → With metze I debugged the issue and we starting figuring how what magic in Heimdal make this work
- $\rightarrow\,$  We correctly implemented passing credentials around here and fixed more issues in libsmb

#### THE LAST TRUST BUG

January - March 2017

- ightarrow The last test failing was about external trusts
- ightarrow One issue was in the MIT KDB module for Samba
- $\rightarrow~$  The second issue was a bug in gensec redirecting requests to the correct KDC

# ARE WE THERE YET?

What is this talk about? Samba AD for the Enterprise Hist 0

History Are we

Are we there yet? Samba - Rolling Relea

#### MIT KERBEROS SUPPORT UPSTREAMED

2017-04-30 The code hit master!

What is this talk about? O	Samba AD for the Enterprise	History 000000000000000000000000000000000000	,	Samba - Rolling Release 00000
WHEN?				

#### When will we get Samba AD with MIT Kerberos?

???

What is this talk about? O	Samba AD for the Enterprise	History 000000000000000000000000000000000000	,	Samba - Rolling Release 00000
WHEN?				

#### When will we get Samba AD with MIT Kerberos?

September 2017

What is this talk about? O	Samba AD for the Enterprise	History 000000000000000000000000000000000000	,	Samba - Rolling Release 00000
WHEN?				

### When will we get it in Fedora?

Fedora 27

What is this talk about? O	Samba AD for the Enterprise	History 000000000000000000000000000000000000	,	Samba - Rolling Release 00000
WHEN?				

#### When will we get it in RHEL?

RHEL 7.5 as a Tech Preview

# SAMBA – ROLLING RELEASE

#### DEPENDENCIES

You need:

- → MIT Kerberos >= 1.15.1 (krb5-devel, krb5-server)
- $\rightarrow$  GnuTLS >= 3.4.7

What is this talk about? O	Samba AD for the Enterprise	History 000000000000000000000000000000000000	/	Samba - Rolling Release ○●○○○
BUILDING				

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



#### All of the really important stuff!

- $\rightarrow$  Single DC
- $\rightarrow$  Forest trusts
- $\rightarrow$  External trusts

#### WHAT IS MISSING?

- → PKINIT support (should work, tests missing)
- $\rightarrow$  Smartcard support
- $\rightarrow$  Kerberos impersonation support (S4U2SELF/S4U2PROXY)
- $\rightarrow~$  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/