Updates from MIT Kerberos

Benjamin Kaduk
kaduk@mit.edu

27 March, 2014

Features released before EAKC 2012

- krb5 1.9 — December 2010
- krb5 1.10 — January 2012

Particularly notable features in krb5-1.9

- IAKERB
- `kadmin purgekeys`
- password sync pluggable interface
- `KRB5_TRACE`

KRB5_TRACE

What is KRB5_TRACE?

- environment variable
- log from the library at various points to disk or `/dev/sdterr`, etc.
- really useful for tracking down DNS issues, keytab path, ...

KRB5_TRACE example: wrong realm in request

```
kaduk@glossolalia:~$ klist
Ticket cache: FILE:/tmp/krb5cc_zone
Default principal: kaduk@ZONE.MIT.EDU

Valid starting       Expires              Service principal
03/17/2014 13:10:51  03/17/2014 23:10:51  krbtgt/ZONE.MIT.EDU@ZONE.MIT.ED
        renew until 03/18/2014 13:10:51
kaduk@glossolalia:~$ KRB5_TRACE=/tmp/a ssh -k entropy.xvm.mit.edu
kaduk@entropy.xvm.mit.edu's password:
Permission denied, please try again.
```

What's wrong? `ssh -v` helps sometimes, but not always.

KRB5_TRACE example: wrong realm in request

```
kaduk@glossolalia:~$ cut -d '' -f 3- /tmp/a
Convert service host (service with host as instance) on host \
entropy.xvm.mit.edu to principal
Remote host after forward canonicalization: entropy.xvm.mit.edu
Remote host after reverse DNS processing: XVM-SIX-158.MIT.EDU
Got service principal host/xvm-six-158.mit.edu@ATHENA.MIT.EDU
ccselect can't find appropriate cache for server principal \
host/xvm-six-158.mit.edu@ATHENA.MIT.EDU
Getting credentials kaduk@ZONE.MIT.EDU -> \
host/xvm-six-158.mit.edu@ATHENA.MIT.EDU using ccache \
FILE:/tmp/krb5cc_zone
[...]
```

... that's not the right realm for the service principal.
Need to add `domain_realm` mapping for that hostname (and turn off rdns).

KRB5_TRACE example: preauth types

Let's explore a bit of what happens for preauthentication with different principals:

```
kaduk@glossolalia:~$ KRB5_TRACE=/tmp/b kinit kaduk@ATHENA.MIT.EDU
Password for kaduk@ATHENA.MIT.EDU:
kinit: Password incorrect while getting initial credentials
kaduk@glossolalia:~$ KRB5_TRACE=/tmp/c kinit kfwrsa@ATHENA.MIT.EDU
Password for kfwrsa@ATHENA.MIT.EDU:
SAM Authentication
Challenge from authentication server
Duo login: Passcode/option or press return for options:
kinit: Password read interrupted while getting initial credentials
```

KRB5_TRACE example: preauth types

What can KRB5_TRACE tell us?

```
kaduk@glossolalia:~$ grep 'preauth types' /tmp/b /tmp/c | cut -d '' -f 3-
Processing preauth types: 2, 136, 19, 133
Processing preauth types: 2, 136, 19, 133
Processing preauth types: 136, 30, 133
```

From krb5.h:

```
#define KRB5_PADATA_ENC_TIMESTAMP       2 /**< RFC 4120 */
#define KRB5_PADATA_ETYPE_INFO2         19 /**< RFC 4120 */
#define KRB5_PADATA_SAM_CHALLENGE_2     30 /**< draft challenge system, u
#define KRB5_PADATA_FX_COOKIE           133 /**< RFC 6113 */
#define KRB5_PADATA_FX_FAST             136 /**< RFC 6113 */
```

Particularly notable features in krb5-1.10

Particularly notable features in krb5-1.10

- work around glibc bug breaking rdns=false
- GSS acceptors can wildcard hostnames for service principals
- KDC and kadmind network code uses an event loop
- Password changes work over NAT
- localization support (but no translations in-tree)
- DIR: cctype, collection-enabled ccaches, and .k5identity

Collection-enabled credentials caches

What are they good for?

- Users with multiple principals (e.g., `kaduk` and `kaduk/root`)
- Working in multiple realms at the same time

Select a principal to use based on:

- remote realm
- service part of host-based service principal
- host part of host-based service principal (with wildcards)

DIR: type credentials caches

- path to a directory (must already exist) holding credentials
- each TGT and derived service tickets are stored in a FILE: cache format within the directory
- Can refer to an individual FILE cache within the directory with DIR:: (two colons)

What's new?

- krb5-1.11 — December 2012
- krb5-1.12 — December 2013

Interesting features new in MIT krb5-1.11

- Complete documentation revamp and consolidation
- Some KDC refactoring
- ASN.1 decoder is now table-driven
- KDC lookaside cache performance improvements
- Programmatic "responder" interface for getting initial credentials
- Client keytab initiation
- Client support for FAST OTP (RFC 6560)
- Build Camellia by default (RFC 6803)
- Store in the ccache how a credential was required (responders can use to reduce the number of user prompts)

New krb5 documentation

- Written in ReStructuredText
- texinfo is no more
- `http://web.mit.edu/kerberos/krb5-latest/doc` for latest stable release
- `http://web.mit.edu/kerberos/krb5-devel/doc` for the current development head
- `http://web.mit.edu/kerberos/krb5-1.11/doc` for the latest krb5-1.11 docs
- Man pages are generated from .rst source, but also checked into the tree
- Retiring DES

New krb5 documentation

Table of contents:

- For users
- For administrators
- For application developers
- For plugin module developers
- Building Kerberos V5
- Kerberos V5 concepts
- MIT Kerberos Features
- How to build this documentation from source
- Contributing to the MIT Kerberos Documentation
- Resources

Interesting features in krb5-1.12

Interesting features in krb5-1.12

- Many more plugin interfaces: aname-to-lname, kuserok, host-realm, default-realm
- Policy information in the KDB is more flexible; no refcounts $\rightarrow$ better performance
- Support principals with no long-term keys (OTP/PKINIT-only)
- KDC support for FAST OTP (RFC 6560)
- KEYRING: ccache type is collection-enabled, other improvements
- AES-NI when available
- Experimental KDC audit pluggable interface

Audit interface

- Still experimental — APIs may change!
- Supplements krb5_klog_syslog for now
- Future work might include a plugin for syslog logging with more standardized formatting
- tickets get a hash value "ticket ID" for tracking requests in the log
- Per-event APIs to get C-struct level detail at various stages of processing
- Sample module which serializes data to JSON and passes to libaudit
- What do you want from an audit system?

Old KfW

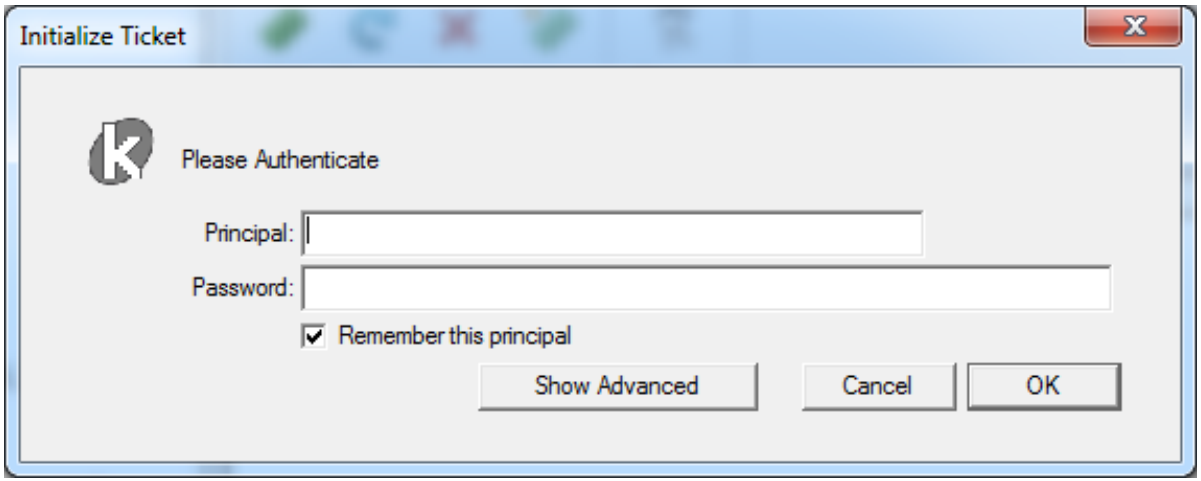
The old state of affairs was pretty bad...

- KfW 3.2.x is based on krb5 1.6
- Installers have no digital signature
- How to rebuild from source is not documented
- Supporting 64-bit systems was "exciting"

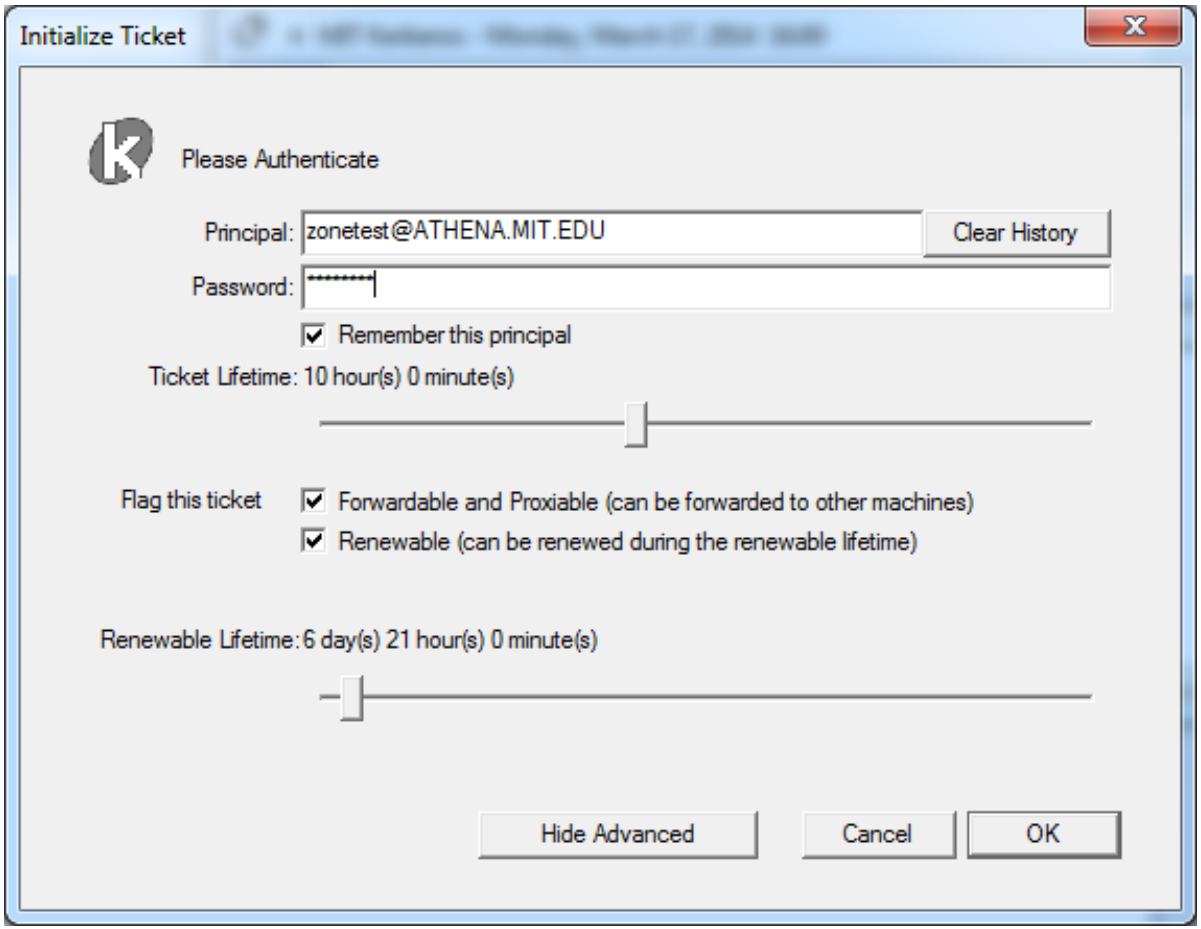
KfW 4.0.x

- KfW 4.0.1 released on 7 December 2012
- MSI installers, signed with an MIT code-signing certificate
- Based on krb5 1.10
- Yes, that means you get `KRB5_TRACE`!
- New Ticket Manager UI; uses windows ribbon
- Well-documented procedure to build from source
- (the only non-MSFT build dependency is perl)
- No more kerbsrc.zip; use git or git archive or similar
- Native 64-bit support; 64-bit installers also provide 32-bit libraries
- more minimal krb5.ini (in new location)

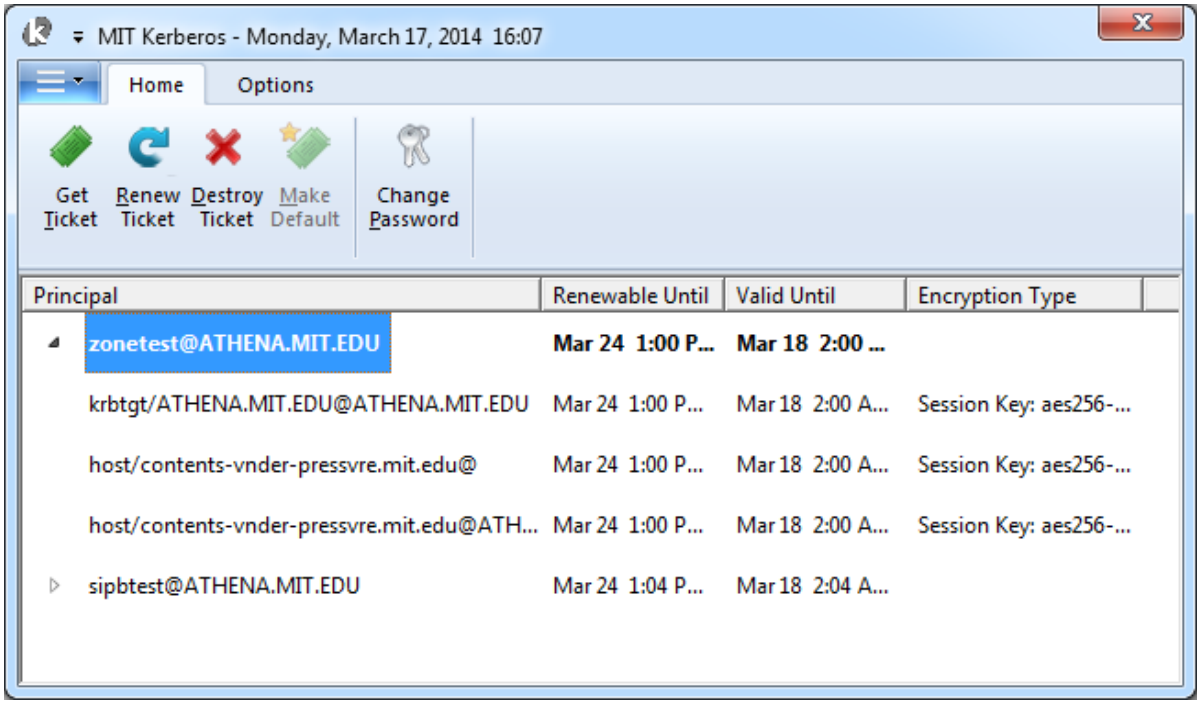
KfW Screenshots



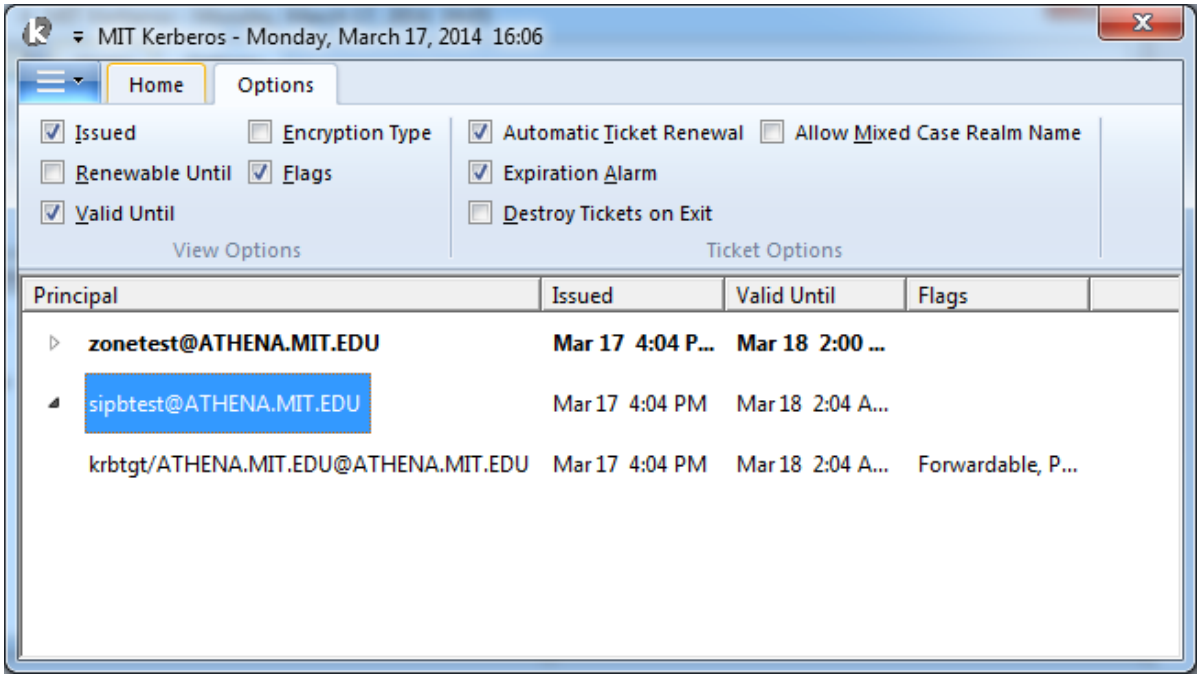
KfW Screenshots



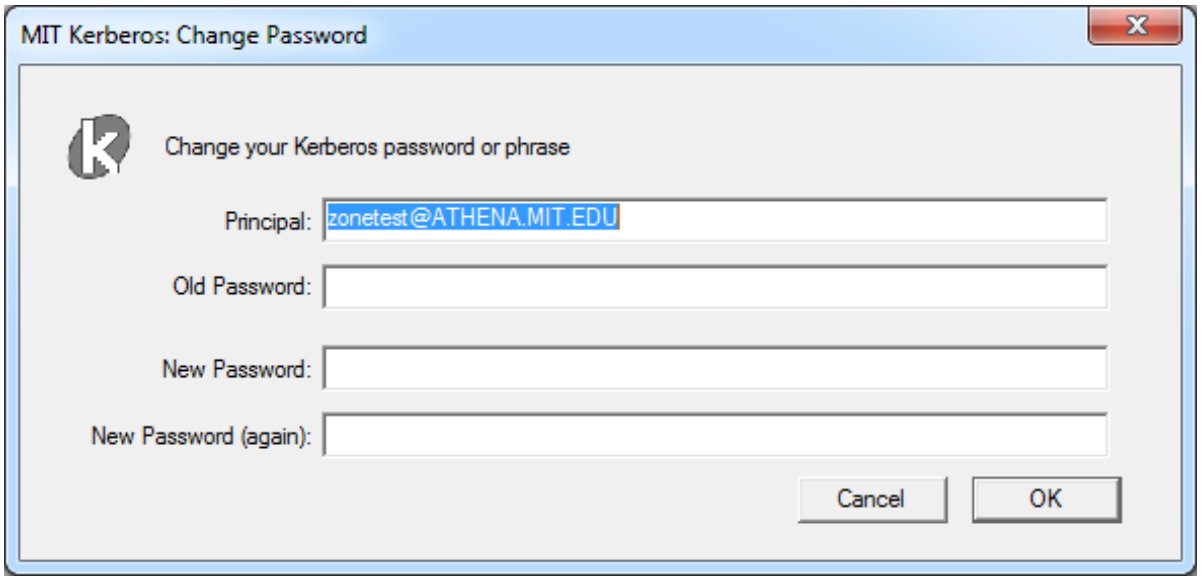
KfW Screenshots



KfW Screenshots



KfW Screenshots



What's new for developers

- Main repo is now in git
- Public repo is `https://github.com/krb5/krb5`, with the authoritative repo for committers hosted at MIT
- Since the 1.11 release, documentation sources are ReStructuredText
- Bug reports still go to `krb5-bugs@mit.edu`
- Security issues PGP encrypted to `krbcore-security@mit.edu`
- Code submissions as github pull requests
- Code style, submission guidelines/requirements, etc., at `http://k5wiki.kerberos.org`

Upcoming items from MIT Kerberos

- KfW 4.1 expected this summer
- krb5-1.13 expected in early October
- Shortened 10-month release cycle for 1.13 to better align with downstream release schedules
- Should be back to 1-year releases for 1.14

Expected krb5-1.13 features

- HTTP(S) transport — MS-KKDCP HTTP proxy
- Hierarchical iprop
- more (but we're not sure exactly what, yet)

Long-term goals

- Stop relying on the DNS!
- Let the KDC do name resolution; it can have a copy of the zone, or a secure path to the nameserver, or similar
- CAMMAC and PAD, akin to the MSFT PAC
- Pluggable interface for kadmin ACLs
- API or KCM-like credentials cache
- Python krb5 implementation for flexible testing
- much more

Thanks!