JPL

JPL's Kerberos 5 Upgrade

Henry B. Hotz

Jet Propulsion Laboratory

California Institute of Technology

JPL

Overview

- Preparation
- Requirements and Testing
- MIT/KTH (Heimdal) Tradeoff
- Doing the upgrade
- Follow-on
  - Migrating clients
  - New/Additional capabilities

Preparation

- Download and read the AFS to Krb5 migration kit
  - ftp://ftp.cmf.nrl.navy.mil/pub/kerberos5/afs-krb5-2
  - This package includes really good descriptions of all the technical issues (in addition to patches and utilities you need to use MIT Kerberos).
- Ensure you have about 600MB disk space for KTH-Krb, Heimdal, and your database.
- Ensure you are not competing with a Windows Domain for your realm name.
  - Both Windows and Kerberos will use the same DNS SRV records to locate their servers.
  - Kerberos 5 will use DNS entries for anything not spelled out in the krb5.conf.

Requirements and Testing

- When a job is big enough some formality is a good idea.
  - Given good requirements you can do a test for each of the requirements and then check off the requirements that have been tested prior to deployment.
- Requirements types
  - Basic — realm name, ticket handling, password change
  - Strength — encryption types, password strength and reuse
  - Legacy — existing interfaces that have to keep working
  - Compatibility — client OS's to support
  - Support — performance and availability monitoring and alarms
  - Operations — administrative and client procedures
  - Backup — (don't backup the master key with the database)
  - Evolution — future requirements and legacy capabilities to phase out

MIT/KTH (Heimdal) Tradeoff

Feature	MIT	KTH/Heimdal	Requirement
Cracklib	Patch available	Yes	1.1.4
Kerb 5 to 4 translation	Non-MIT daemon	Yes	1.1.8, and 4.3
kaserver emulation	Non-MIT daemon	Yes	1.1.8, and 4.4
Replay cache	Yes	No	None (but 1.1.9 says we Òshould Ó)
V4 addressless	No	Configurable	1.2.1 (need it both ways, req. missing)
Password history	Yes, but. . .*	No	1.2.4
SecureID	Patch available	No	1.2.7
NASA password reqÕs	No**	No	1.2.8, and 1.2.9
AFS string-to-key	Supported	Supported	4.1
Microsoft compatible	Yes	Yes	4.3
Updatable master key	No	Yes	None
Incremental propagation	No	Yes	None
PKINIT	No	Yes	None

* Implemented history checking does not match JPL requirement

** Requires patch and custom code.

JPL

Server Upgrade Procedure Outline

- Download/install berkeley db3, KTH-Krb4, Heimdal, cracklib, and cracklib shim routine
  - Cracklib shim needs customizing for site policy
  - Install krb5.conf and master key file on all db servers
- Convert kaserver database to Heimdal database with hprop | hpropd
  - Add principals needed for kdc/kpasswdd/kadmin operation
  - Create /var/heimdal/kadmind.acl file with list of AFS admin principals.
- Shut down kaserver, and startup kdc, kpasswdd, and kadmind
  - Add stuff to /etc/rc* and /etc/inetd.conf to do this automatically
  - Update /etc/services
- Repeat for slave servers
  - Create hprop service principals and keytab files for all slaves
  - Start hpropd (or ipropd) instead of kpasswdd and kadmind.

JPL

ToDo List

- Some requirements take more work than others.
  - Sometimes you discover requirements late.
- JPL-unique wordlist for cracklib.
- Expiring password notification process.
- Procedure for reverting to the kaserver if the upgrade fails.
- KDC log rotation and backup
- Extra security for admin prinicipals.
- Password expiration and ticket renewal limit not set by kaserver import.

Client migration

- All existing interfaces continue to work
  - Except password change
- Need K5 initial authorization
  - Unix

    SSH - in flux, but progressing (3.8 has some support)

    PAM - pam_krb5afs

    Other - ak[5]log or gssklog command line
  - MacOS X

    Current: aklog plugin

    Future: need PAG in terms of Mach Security Context
    - Would allow kernel module to get the afs token itself
  - Windows
    - WolfCall http://www.eos.ncsu.edu/wolfcall/
    - Wake http://www.rose-hulman.edu/TSC/software/wake/
    - KfW http://web.mit.edu/kerberos/
      - Unlike the base MIT package AFS integration is included

JPL

Deferred Implementation

- Multi-Factor Authentication
- Web support
- Password History