Henry Hotz (JPL)

JPL's kaserver to Kerberos 5 Upgrade

As this presentation is given JPL will be in the middle of upgrading from the traditional AFS kaserver to the Heimdal Kerberos 5 KDC. The process is basically very simple, but there are a host of details to be handled in order to minimize service interruptions. We have a good set of requirements, which shows that neither Heimdal, nor MIT provide all the capabilities we will need. We also have a comprehensive list of all the details that have to be taken care of including: converting administration scripts from kas to kadmin, operational procedures that need to be available, Firewall exceptions and database replication.
JPL’s Kerberos 5 Upgrade

Henry B. Hotz
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
  - 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

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

* Implemented history checking does not match JPL requirement
** Requires patch and custom code.
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.
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 principals.
- 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
Deferred Implementation

- Multi-Factor Authentication
- Web support
- Password History