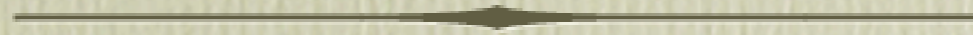


MacOS X and AFS



AFS Flavors

- OpenAFS
 - Used widely here
 - Built to work with the kerberos on board (MIT's version)
- Arla
 - Swedish group, not so widely used here
 - Can be build with MIT kerberos, or other
 - Generally good laptop support

Installing AFS

- Download the OS X binary from www.openafs.org (not the darwin package, although that should work)
- This package is just a client!
- It's a normal mac package, just run the installer
- The default package uses the “newer” paths for config files
`/var/db/openafs/etc` (instead of `/usr/vice/etc`)
- Edit the ThisCell file with your home cell, and add the afs server data to CellServDB if it's not already there

ThisCell

- Just a one liner to tell AFS what cell you normally live in
- It defines the default for where to authenticate you via afs programs
- Does not limit you to a single cell

CellServDB

- A list of AFS cell names and the servers comprising them
- By default, AFS uses this file to find cells

```
>isis.unc.edu # University of North Carolina
Project Isis
152.2.1.5 #db0.isis.unc.edu
152.2.1.6 #db1.isis.unc.edu
152.2.1.7 #db2.isis.unc.edu
>cs.unc.edu # University of North
Carolina at Chapel Hill
152.2.128.1 #crow.cs.unc.edu
152.2.128.2 #falcon.cs.unc.edu
152.2.128.8 #thrush.cs.unc.edu
```

How AFS starts

- Uses a script in `/Library/StartupItems/OpenAFS`
- Script checks out startup conditions and then starts `afsd` with appropriate flags
- Part of that startup checks for an `afsd.options` file in `/var/db/openafs/etc/config`, if that file exists, the startup script uses its settings, not its own

Sample afsd.options file

```
-stat 2000 -dcache 800 -daemons 3 -volumes 70 -rootvol root.afs
```

- This is ok for desktop machines, but not for laptops that may not be on the network
- Definitely want to add `-fakestat` or `-fakestate-all` (laptops!)
 - Fakestat prevents finder from hanging when it cannot access a directory
 - Fakestat-all applies this setting to all afs directories
- Consider adding `-dynroot` (laptops)
 - Lets the system mount afs cells as needed

UIDs

- By default, the first user created on a mac has UID 501. That's most certainly not your AFS UID
- It's helpful to match your local Unix UID to your AFS UID
 - Use the instructions at <http://help.unc.edu/?id=3748#doe170> (but don't use `cp -pR`, use `CpMac -pr` instead, that will preserve resource forks!)
 - OR, use instructions under the Matching UIDs section of <http://www.ibiblio.org/macsupport/arla.html> (but keep a couple of terminal windows open--this method chowns files on the fly)

Integrating Login

- We want to integrate 3 logins with AFS
 - Main GUI login
 - Screensaver
 - Remote Login
- The first two are done with Kerberos and /etc/authorization
- The third is done with a pam module and sshd
- See <http://www.ibiblio.org/macsupport/kerberos/>

Kerberos/AFS

- Install MIT's kerberos extras (optional: put the kerberos.app in the dock and startup items for login)
- Edit `/Library/Preferences/edu.mit.Kerberos` (or in your library preferences, if you prefer)
 - Add Kerberos realm data
 - Add notification for aklog
- Copy down kfm_aklog plugin into `/Library/Kerberos Plug-Ins`
- Edit `/etc/authorization` to add optional or required kerberos authentication

How this works

- The changes to the `/etc/authorization` prompt the system to get a kerberos ticket granting ticket when you login to the mac (based on matching userid and password!)
- When kerberos is tapped, it taps the aklog plugin
- Aklog uses the tgt to get itself a token
- See http://www.ibiblio.org/macsupport/kerberos/kerberos10_3.html for details

SSHD and AFS

- SSHD on OS X supports PAM (Pluggable Authentication Modules)
- Download a pam module for AFS pam_afs.so.1 module (works with cells using kaserver or fakeka)
- Pam modules go in /usr/lib/pam
- Edit /etc/pam.d/sshd to include a reference to the pam module

```
# login: auth account password session
auth      required      pam_nologin.so
auth      optional      pam_afs.so.1
auth      sufficient    pam_securityserver.so
auth      sufficient    pam_unix.so
auth      required      pam_deny.so
account   required      pam_permit.so
password  required      pam_deny.so
session   required      pam_permit.so
```

More Info

- <http://help.unc.edu/?id=3748>
- <http://www.ibiblio.org/macsupport/kerberos/>
- <http://www.thok.org/intranet/mac/unixmac.html>
- <http://jeanmatthieu.free.fr/doc/pdf/osx/OpenAFS/OpenAFS.pdf>
- <https://lists.openafs.org/pipermail/openafs-info/2003-February/008230.html>
- <http://www-personal.umich.edu/~arosenbl/kerbio3.html>
- <http://www.mail-archive.com/openafs-devel@openafs.org/msg02009.html>
- <http://www.openafs.org/pages/doc/AdminReference/auarfo58.htm>
- <http://www.csc.ncsu.edu/techsupport/technotes/macafs.php>
- http://hydra.dartmouth.edu/macosex/AFS_install.html
- <http://www.mathematik.uni-karlsruhe.de/~iwrmm/Persons/Schulz/Unix/afs/afs-krb5.html>