Athena Configurations for Stock Redhat 9.0 Install

By: Tim Boyden – Systems Administrator, MIT Department of Facilities

The following instructions are what I did to configure a stock Redhat 9.0 Linux box to allow Athena users to login with their Kerberos principle and password and have their Athena lockers mounted as their home drive without having a user profile configured locally on the desktop machine. Why did I do this when I could use Linux Athena? I did this for a couple of reasons: 1) I wanted a cleaner user interface similar to a Windows or Macintosh desktop that normal administrative users would be comfortable in using, 2) I wanted more freedom in configuration of installed software and updated versions, 3) I wanted to take advantage of more of the GUI administrative tools that come with the stock Redhat install, 4) I am using this as a learning resource to learn more about the inner workings of Linux that can hopefully be reused on some of my other projects such as Athena configurations for Mac OS X.

Information contained in these instructions have been compiled from a number of sources including, but not limited to; OpenAFS.org, Redhat.com, Linux.org, MIT SIPB Linux Athena members and others. To all, thank you very much for your help! As you work through these instructions please keep in mind this is not supported in any way by the MIT Helpdesk, Athena OLH, me, etc.. your own your own here. However if you have any questions feel free to email me at trboyden@mit.edu and I'll do my best to help you out or point you in the right direction. Along those lines, these instructions are written to a certain level of expectation of technical competence, you should know how to follow instructions, lookup information on the web on your own, download files from the web, install an operating system, burn ISO images to cd-rom, etc.. If you have no idea what I just said, well these instructions are not for you!

With all that being said, here we go and good luck!

Operating system installation

To start, first we need a desktop computer with a stock Redhat 9.0 install. To do this we'll need to download the cd-rom images and burn them to cd-roms. There are 3 iso images so you will need 3 blank cd-roms.

- ✗ Go to http://rpmfind.net/linux/redhat/9/en/iso/i386 and download the 3 shrike-i386-disc*X*.iso images.
- ✗ Burn each image to a cd-rom using your preferred cd-burning application.
- ✗ Put the first disc in the machine you want to install Redhat on and reboot, the installer will start automatically (or you might have to hit a key to boot from the cd-rom)
- ✗ The first time you use the cd-roms you should allow the install program test the media for defects, otherwise you can skip it.
- ✗ In general you'll want to just follow the on-screen instructions and choose the defaults, some of the answers will be machine specific so plug-in your machine's information. Make sure you select the Personal Desktop installation type to keep things simple and reduce the amount of hard disk space you'll need. You may want to add some additionally packages just for ease of use, you can always install more later using the Add/Remove packages tool. Here are some of the additional packages I installed:
  - Text-based Internet > pine – this is for the Pico text editor, great for editing config files
  - System Tools – Selected to add additional System Tools (see below)
  - System Tools > rdesktop – this is for connecting to a Windows Terminal Server
- ✗ The install process can take awhile so you might want to start this at lunch time ;-)
- ✗ After you've rebooted you'll go through the first boot setup wizard. One of the things it will

have you do is setup a regular (non-root) local user account. You will probably never use this account, but make sure you give it a username that is different then all of your users' Kerberos principles. When you login, the desktop machine will check against the local user profiles before it consults the Kerberos KDC for your user accounts. Having a local username the same as a Kerberos principle will cause the desktop machine to load the local profile with the local permission settings that are different than the MIT Athena permission settings, thus making it so you can't access your AFS home drive. Also during the wizard, it asks you to register your system with Redhat and create a Redhat Network account. I highly recommend you do this so you take advantage of the automatic system updates.

- Once you've completed the first-boot wizard you'll be presented with the Redhat login screen (which you can modify the look and feel of later on). Log on as root so we can set the Athena configurations up. You do remember the root password you setup way back in the beginning of the install right!? ;-p

Configuring your Redhat 9.0 box for the Athena environment

Now that we have a pristine Redhat 9.0 installation, we can go ahead and configure the desktop to enable AFS mounting, Hesiod lookups, and Kerberos authentication. We'll use a combination of the Nautilus file browser and Gedit to do our configuration file edits. Where possible we'll take advantage of the built-in GUI system administration tools to do some pre-configuration before we dive into the depths of the Linux operating system.

Before we get started we need to do one important thing. Athena defaults to using the tcsh shell environment out of /bin/athena. Most *nix systems run this straight out of /bin. We'll need to make the athena directory in /bin and add a symlink to /bin/tcsh or else we'll get kicked out when we try to login. The easiest way to do this is:

- Click on the Redhat icon (similar to the Windows Start menu) and hover on System Tools then click Terminal and type the following at the prompt: *cd /bin*
- Next type: *mkdir athena*
- Next type: *cp -l /bin/tcsh /bin/athena*

Now let's start configuring Kerberos and Hesiod. Support for Kerberos and Hesiod is built into Redhat 9.0 and to top that off there is a great and easy GUI configuration tool to set them up.

- Again, click on the Redhat icon and hover on System Settings, then click on Authentication. The Authentication Configuration tool lets you configure where the system gets its user information from and where the system should authenticate to. Options for user information are NIS, LDAP or Hesiod. Options for authentication are LDAP, Kerberos or SMB authentication (Windows domain controllers).
- On the User Information tab, first check on Cache User Information, this will make user information lookups quicker, then check on Enable Hesiod Support and click the Configure Hesiod button. In the Hesiod LHS text box type: *.ns* ,in the Hesiod RHS text box type: *.athena.mit.edu* then click OK.
- Click on the Authentication tab. Check on Enable Kerberos Support, then click the Configure Kerberos button. In the Realm text box type: *ATHENA.MIT.EDU* in the KDCs text box type: *kerberos.mit.edu* and in the Admin Servers text box type: *kerberos.mit.edu:749* and click OK. Click OK to exit the Authentication tool.

Your desktop is now configured to do Hesiod lookups to determine user and printer information including AFS locker location and to use Kerberos to determine if a user logging on has a valid Kerberos account. This does not actually set the desktop machine up to get Kerberos tickets and AFS tokens on login, we'll do that later on when we setup PAM (pluggable authentication modules). If a user logging on has a local account such as root, these configurations are ignored.

Next we'll need to download and install OpenAFS so we can mount our AFS lockers.

- ✗ Open the web browser and go to http://openafs.org . In the Downloads section in the navigation bar click on the Latest Release link. Scroll down to the Redhat 9.0 section, you'll want to download the following files:
  - openafs-1.2.9-rh9.0.1.i386.rpm
  - openafs-client-1.2.9-rh9.0.1.i386.rpm
  - openafs-compat-1.2.9-rh9.0.1.i386.rpm
  - openafs-debuginfo-1.2.9-rh9.0.1.i386.rpm
  - openafs-kernel-1.2.9-rh9.0.1.i386.rpm
  - openafs-kernel-source-1.2.9-rh9.0.1.i386.rpm
  - openafs-kpasswd-1.2.9-rh9.0.1.i386.rpm
  - openafs-krb5-1.2.9-rh9.0.1.i386.rpm

  You'll want to create a folder to put them in to make installation easier.
- ✗ Open a terminal window (System Tools) at the prompt CD to the folder you downloaded or moved the files into. Now at the prompt type the following command: *rpm -Uvh *.rpm* this will install the OpenAFS packages using the Redhat package manager utility. If you didn't see any error messages your all set. If you did, refer to the documentation and forums on OpenAFS.org to troubleshoot. Assuming your all set, close the terminal window and we'll configure OpenAFS.
- ✗ OpenAFS is configured through text files located in /usr/vice/etc . We'll also need to modify a few files in /etc to control the correct mounting locations and AFS/Kerberos authentication routines. Double-click on the “root's home” icon on the desktop. This will open the Nautilus file manager and it will default to showing the currently logged on user's home folder. In the URL text box type: */usr/vice/etc* and press enter. The files we're looking for are ThisCell and CellServDB . ThisCell is where we configure the AFS cell that we want to mount. CellServDB is a list of all of the globally available AFS cells. CellServDB gets updated often and the latest version can be obtained from http://grand.central.org .
- ✗ To set MIT's cell, right-click on ThisCell hover over Open with and click gedit. This will open the ThisCell file in the Gnome text editor and allow us to modify the file. The file will have one line of text like: *openafs.org* select this text and replace it with *athena.mit.edu* then save the file and exit gedit. Optionally you can edit the CellServDB file and delete all the non-MIT entries, this can make AFS searches quicker.
- ✗ Now let's configure AFS mounting. Normally Athena machines use Attach to mount AFS lockers, most Linux distributions don't ship with this but they do ship with AutoFS which recent releases now have support for Hesiod lookups. To properly mount our default AFS share we'll want to edit the /etc/auto.master file. In the file browser window, click in the URL text box and type: */etc* then open the auto.master file in gedit like we did for ThisCell. This file will be empty except for some brief configuration hints that are commented out with #s. Move to a line below the instructions that doesn't have a # sign and type the following: */mit hesiod* the space between /mit and hesiod is a tab space. Save the file and close gedit. Now when the system boots up and a user logs in their Athena locker will now be able to be mounted in the correct /mit/username mount point as referenced in the user's hesiod lookup entry (hesinfo username filsys).
- ✗ Now for the most tedious part, integrating AFS and Kerberos together through the various pluggable authentication modules (PAM). PAM is how *nix operating systems allow for configuring and extending the authentication routines that programs that require

authentication use. Generally this is done in one of two ways: either one pamd.conf file that every program that requires authentication has an entry in or a pam.d directory that contains a separate configuration file for each program that requires authentication. If both exist the pam.d directory takes preference. Redhat uses the pam.d directory so that is what I'll detail here. Of all the modifications we've done so far, the following changes are the only ones that can really mess up your installation badly. So I highly recommend you backup these files prior to modifying them. You should also have an emergency boot disk (you did make this way back during the O/S install right!?) handy just in case of a mistake, it may be the only way you can get back into your system. Essentially the files we are mainly concerned with are: login, gdm, xdm, and xscreensaver. You may want to modify some of the other ones such as sshd if you want to enable AFS/Kerberos support for those programs. login, gdm, and xdm control the initial user login process and in the case of xscreensaver, return from a sleep or screen lock mode. Typically the files look like this:

```
#%PAM-1.0
auth       required     pam_env.so
auth       required     pam_stack.so service=system-auth
auth       required     pam_nologin.so
account    required     pam_stack.so service=system-auth
password   required     pam_stack.so service=system-auth
session    required     pam_stack.so service=system-auth
session    optional     pam_console.so
```

The field order is: module type, success control, module location, module arguments. See the man entry for pam.d for more information. We'll want to modify the files so they each have a new entry under each module type. Therefore the modified file should look like this:

```
#%PAM-1.0
auth       required     pam_env.so
auth       required     pam_stack.so service=system-auth
auth       required     pam_nologin.so
auth       optional     pam_krb5afs.so use_first_pass minimum_uid=0
account    required     pam_stack.so service=system-auth
account    optional     pam_krb5afs.so use_first_pass minimum_uid=0
password   required     pam_stack.so service=system-auth
password   optional     pam_krb5afs.so use_first_pass minimum_uid=0
session    required     pam_stack.so service=system-auth
session    optional     pam_console.so
session    optional     pam_krb5afs.so use_first_pass minimum_uid=0 krb4_convert
tokens
```

The xscreensaver file should look like this:

```
#%PAM-1.0
 # Red Hat says this is right for them, as of 7.3:
auth       required     pam_stack.so service=system-auth
```

auth optional pam_krb5afs.so use_first_pass minimum_uid=0 krb4_convert tokens

This is what we were using before:

auth required pam_pwdb.so shadow nullok

Note: each line should be continuous. So as you can see, we added a new entry for each module type of auth, account, password, and session. The success control for all of these new entries should be *optional* that way local account logins won't be affected when the user doesn't exist in the Kerberos user database. The AFS/Kerberos PAM module we're using is pam_krb5afs.so. This module is part of the OpenAFS distribution and was installed when we installed OpenAFS. See the man entry for pam_krb5afs for definitions of the arguments. Each field should be separated by a tab and each argument by a space. You will need to repeat these modifications for each of the login, gdm, xdm and xscreensaver files and for any additional files you want to add AFS/Kerberos authentication support for.

- Once you've made all of those changes we are ready for the trial by fire. Go ahead and reboot the desktop machine and attempt to login using your Kerberos principle and password. If your able to login, congratulations! If not, you'll get an error message and will be bounced back out to the login screen in defeat. Log back on as root and double-check your modifications.

Additional Notes

Now that you have a Redhat Linux desktop machine that can login Athena users, you may be asking “Cool, now what do I do with this?”. Well, that's up to you. Redhat 9.0 comes with many applications pre-installed such as OpenOffice (a Microsoft Office compatible office suite), Mozilla web browser (Netscape is based on this), The Gimp (a Photoshop like graphics application), and many more. There's even an SAP client for Linux... You can also download and install many other applications mostly for free, some at low cost. Maybe you want to consider replacing that bottomless hole in your budget that is a Windows or Macintosh network with a Linux network? Again that's up to you.

Before you go crazy installing Linux desktops, here are some things to consider:

- **AFS on notebooks = BAD.** Because AFS is a network based file system as soon as you disconnect your notebook from the net it will not be happy and some apps will cease to work and you will lose access to your files and preferences. Work is being done to improve upon disconnected AFS usage.
- **Only works on campus.** This maybe an isolated issue with my ISP, however after doing this setup at home I was unable to login with my Kerberos principle because it couldn't verify I had a valid Kerberos account. What's weird is it did know my correct mount point so I know Hesiod support is working.
- **Linux is not for dummies.** Even with the really great graphical utilities and improvements with the core desktop applications, Linux still requires a certain level of computer skill or retraining to do everyday functions that your users (and even some Sys Admins) are comfortable at doing. Some file conversion will still be needed to be able to exchange files back and forth with Windows and Macintosh users, though compatibility is getting a lot better.
- **No campus I/S support.** Again this setup is not supported in any way whatsoever by campus I/S, Athena OLH, SIPB, me etc... The good news is that Redhat provides excellent support though at a fee per desktop, and you can get excellent free support by browsing the various newsgroups at Linux.org and others.

If your interested in learning more about Linux, campus I/S currently offers two classes on Linux – Linux Fundamentals and Linux System and Network Administration. Visit the I/S training

website at http://web.mit.edu/is/training to get more information and register for the classes. Redhat also offers certification courses if your interested in getting Linux certified. Visit their site at http://www.redhat.com for more information.

If you have any comments or questions regarding the information contained in this document, contact Tim Boyden trboyden@mit.edu . Support related requests will be ignored and will be destined for my spamscreen folder.

Good luck and have fun!

Sites with more information:

http://www.redhat.com

http://www.openafs.org

http://www.linux.org

http://web.mit.edu/kerberos

http://www.mit.edu/afs/athena.mit.edu/astaff/project/hesioddev/doc/

ftp://ftp.sap.com/pub/sapgui/java/630/README.TXT

http://www.openoffice.org

http://www.gimp.org

http://www.rpmfind.net

http://www.gnome.org