

Accessing ASU Shared File Space

\$Date: 2004/06/21 19:05:28 \$ \$Revision: 1.3 \$

1 Introduction

This document describes how to install and configure software to enable Red Hat Linux to access ASU files shared over AFS. It assumes a working Kerberos configuration; for information on configuring Kerberos, see “Using Kerberos to Authenticate to ASURITE.”

If you would like to give access to any user with a ASURITE account, see instead “Using Kerberos, LDAP, and AFS with ASURITE.” This is a single document describing how to configure authentication using AFS home directories.

2 Prerequisites

After you have a working Kerberos configuration, the first step is to acquire the necessary packages. Red Hat does not include AFS client software but the packages are available as RPMs at <http://www.openafs.org>. Different packages are available for different versions of Red Hat, including 7.3, 8, 9, Enterprise 3, and Fedora. The required packages are:

```
openafs
openafs-client
openafs-compat
openafs-kernel
openafs-krb5
```

3 Configuring AFS

After you have installed the appropriate packages, edit the file `/usr/vice/etc/ThisCell` to contain the following line:

```
asu.edu
```

This should be the only line in the file.

Next add the following information to `/usr/vice/etc/CellServDB`. You can add these lines to the top of the file.

```
>asu.edu                               #Arizona State University Tempe
129.219.10.69                         #authen2.asu.edu
129.219.10.70                         #authen1.asu.edu
129.219.10.72                         #authen3.asu.edu
```

The next step is to configure Kerberos' interaction with AFS.

4 Configuring Kerberos

To configure Kerberos, add this information to `/etc/krb5.conf`:

```
[appdefaults]
pam = {
    debug = false
    ticket_lifetime = 36000
    renew_lifetime = 36000
    forwardable = true
```

```

    krb4_convert = true
    afs_cells = asu.edu
}

```

Now we have to configure the Linux authentication system to get AFS tokens when a user logs in.

5 Configuring PAM

Authentication in Linux is handled by PAM (Pluggable Authentication Modules). We would like to configure PAM to use the `pam_krb5afs.so` library to handle Kerberos authentication and AFS access. The default Kerberos configuration uses `pam_krb5.so`. To change this, edit the file `/etc/pam.d/system-auth` and change all occurrences of `pam_krb5.so` to `pam_krb5afs.so`. A complete sample configuration file looks like this:

```

auth      required      /lib/security/$ISA/pam_env.so
auth      sufficient    /lib/security/$ISA/pam_unix.so likeauth nullok
auth      sufficient    /lib/security/$ISA/pam_krb5afs.so use_first_pass
auth      required      /lib/security/$ISA/pam_denial.so

account   required      /lib/security/$ISA/pam_unix.so
account   [default=bad success=ok user_unknown=ignore service_err=ignore system_err=ignore] /lib/security/$ISA/pam_unix.so

password  required      /lib/security/$ISA/pam_cracklib.so retry=3 type=
password  sufficient    /lib/security/$ISA/pam_unix.so nullok use_authtok md5 shadow
password  sufficient    /lib/security/$ISA/pam_krb5afs.so use_authtok
password  required      /lib/security/$ISA/pam_denial.so

session   required      /lib/security/$ISA/pam_limits.so
session   required      /lib/security/$ISA/pam_unix.so
session   optional     /lib/security/$ISA/pam_krb5afs.so

```

6 Finishing Up

OpenAFS includes a service to start all the necessary software and load the requisite kernel modules. This service should be configured to run when the system starts, for example by running `chkconfig afs on`.

To start AFS for the first time, start the `afs` service by running `service afs start`. To test the configuration, run `klog -principal user`, where `user` is an ASURITE username. You will be prompted for your ASURITE password. This will give you an AFS ticket. ASU shared files should be available in `/afs/asu.edu` with user directories in the `/afs/asu.edu/users` hierarchy.