

# Using Kerberos, LDAP, and AFS with ASURITE

\$Date: 2004/06/22 17:46:42 \$      \$Revision: 1.10 \$

## 1 Introduction

This document describes how to configure a machine running Red Hat Linux to use Kerberos and LDAP to authenticate to the ASURITE domain and gain access to shared file space using AFS. This configuration is ideal for the scenario that any user with an ASURITE account should be given access to a machine. No manual configuration is required to grant access to specific individual users.

If you would like to grant access to the machine on a per-user basis, follow the instructions in the document “Using Kerberos to Authenticate to ASURITE” instead.

## 2 Prerequisites

Before you begin you must have the following packages installed. These packages are all available as part of the Red Hat distribution.

```
krb5-libs
krb5-workstation
krbafs
pam_krb5
openldap
openldap-clients
nss_ldap
```

In addition, you must install the following packages to use AFS. These packages are not included with Red Hat but are available at <http://www.openafs.org>. Separate packages are built for each version of Red Hat; install the appropriate packages for your system.

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

To simplify configuration you can use GUI tools provided by Red Hat. These tools are provided by

```
authconfig
authconfig-gtk
```

## 3 Configuring Kerberos

The first step is to configure Kerberos to authenticate to the ASURITE domain. Edit the file `/etc/krb5.conf` to include the following:

```
[libdefaults]
    default_realm = ASU.EDU
    default_tkt_enctypes = des3-hmac-sh1 des-cbc-crc
    default_tgs_enctypes = des3-hmac-sh1 des-cbc-crc

[realms]
ASU.EDU = {
    kdc = krb1.asu.edu:88
```

```

kdc = krb2.asu.edu:88
kdc = krb3.asu.edu:88
admin_server = krb1.asu.edu:749
default_domain = asu.edu
}

[domain_realm]
.asu.edu = ASU.EDU
asu.edu = ASU.EDU

```

You will also need to edit the files `/etc/krb.conf` and `/etc/krb.realms` for compatibility with Kerberos v4. The file `krb.conf` should contain the following:

```

ASU.EDU
ASU.EDU authen1.asu.edu
ASU.EDU authen2.asu.edu
ASU.EDU author2.inre.asu.edu admin server

```

and `krb.realms` should contain:

```

.asu.edu asu.edu
.inre.asu.edu asu.edu

```

The next step is to configure the operating system to use Kerberos to authenticate users.

## 4 Configuring PAM

Red Hat uses PAM (Pluggable Authentication Modules) for authentication. Since most Linux applications that perform authentication use PAM, changing the system-wide PAM configuration can change the way the system uses authentication without making changes to each application.

### 4.1 Automatic Configuration Tools

If you have the `authconfig` and `authconfig-gtk` packages installed, you can run `redhat-config-authentication` to configure PAM to use Kerberos. Choose the tab labeled “Authentication” and select the checkbox “Enable Kerberos Support”. You do not have to click “Configure Kerberos” because the appropriate settings have already been added to `krb5.conf`. Choose “OK” to apply the changes.

If you have the `authconfig` package installed but not `authconfig-gtk`, you can run a console-based program to make the same changes. Run `authconfig` as root. From the first page of settings, choose “Next”. On the second page choose “Use Kerberos 5”. The Kerberos settings in the right-hand column should show the settings added to `krb5.conf`. Choose “OK” to apply the changes.

#### 4.1.1 Important Addition

The version of PAM included with all recent versions of Red Hat (including Red Hat 9 and Red Hat Enterprise 3) has a bug that makes it impossible for local users (including root) to log in if the machine loses network connectivity. As a workaround, it is necessary to edit the PAM configuration file by hand, even if you use the automatic configuration tools described above.

Edit the file `/etc/pam.d/system-auth` and add the following line to the account section:

```
account    sufficient    /lib/security/$ISA/pam_localuser.so
```

In the account options line (beginning with `account [default=bad ... ]`) add the following directive:

```
authinfo_unavail=ignore
```

## 4.2 Manual Configuration

If you don't have `authconfig`, you can manually edit the PAM configuration file. The file `/etc/pam.d/system-auth` should contain the following:

```
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/$ISA/pam_unix.so
account   sufficient    /lib/security/$ISA/pam_localuser.so
account   [default=bad success=ok user_unknown=ignore service_err=ignore
        system_err=ignore authinfo_unavail=ignore] /lib/security/$ISA/pam_krb5afs.so

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

Note that the account options line (`account [default=bad ... ] ... pam_krb5.so`) should be entered as one long line, not wrapped as shown here.

## 5 Configuring LDAP

ASU uses LDAP (Lightweight Directory Access Protocol) to identify users. The easiest way to configure LDAP is to use one of `authconfig-gtk` or `authconfig`, if available. Run the tool and select "Enable LDAP Support". For LDAP settings, use the following values:

```
LDAP Search Base DN  dc=asu,dc=edu
LDAP Server          ldap1.asu.edu
```

Do not select the TLS option.

If `authconfig` is not available, you need to edit the relevant configuration files by hand. First, edit `/etc/ldap.conf` to contain the following:

```
host ldap1.asu.edu
base dc=asu,dc=edu
ssl no
pam_password md5
```

Next, edit the file `/etc/nsswitch.conf` and add `ldap` to the `passwd`, `shadow`, `group`, `protocols`, `services`, `netgroup`, and `automount` lines. When you are done, the file should contain the following lines:

```
passwd:      files ldap
shadow:      files ldap
group:       files ldap
protocols:   files ldap
services:    files ldap
netgroup:    files ldap
automount:   files ldap
```

## 6 Configuring AFS

After you have installed the appropriate packages (see Section 2), 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.

### 6.1 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.

### 6.2 Configuring PAM

To integrate AFS into the login procedure, we need to configure PAM to use the `pam_krb5afs.so` library to handle Kerberos authentication and AFS access. The default Kerberos configuration written by the graphical configuration tools 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 PAM configuration is shown in Section 4.2.

### 6.3 Starting AFS

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 username`, where `username` 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.

### 6.4 Home Directories

By default, each user's home directory will be set to their AFS space (this is handled by LDAP). If you would like a user to have a local home directory instead, add a local account. Then the user can log in using his or her ASURITE password and use a home directory on the local machine. This is done with the `useradd` command. You do not have to set a password for the user (this will be handled by Kerberos) but you should take care to set the numeric UID to

match the user's ASURITE UID. This is required to gain access to the NetApp's NFS shares. To add a user with a certain UID, run the command `useradd -u uid username`.

Note that any kernel version prior to 2.4 cannot handle the large UIDs used by ASU. To determine the version of the kernel on a machine, you can run `uname -r`. If it is not 2.4.x, you must upgrade the kernel to finish the installation.

## 7 Finishing Up

After Kerberos, PAM, LDAP, and AFS have been configured, the system should be ready to authenticate to ASURITE. Some notes about this configuration:

- The configuration changes take effect immediately. There is no need to reboot the machine.
- Under this configuration, a user can authenticate successfully using either a local password (if a local account exists) or a Kerberos password.
- No special changes are needed to allow for graphical logins using `xdm` or `gdm`.