About & Using AFS

General Overview of OpenAFS

The CNF fileservers run OpenAFS (just AFS for short).

AFS (Andrew File System or A File System) is a distributed file system. The top directory of the AFS hierarchy is the same all over the world, and is ***/afs.***

Every institution in the world with AFS fileservers has its own unique "cell" subdirectory under /afs. CNF's cell is named ***"cnf.cornell.edu"*** and is located at ***/afs/cnf.cornell.edu***

Within a cell, files are located on fileservers and are grouped within entities named volumes. Volumes are partitions of physical disks (of the data servers), in which quotas are applied. Backups of data can also be performend on a per-volume basis. And, data on readonly volumes can be replicated across multiple fileservers.

Authentication

To have full access to AFS, you need to get a token. You will get tokens automatically when logging into a CNF windows or linux machine with your Cornell netid or guestid.

Your token has a limited lifetime, which is 8 hours at CNF. To check your token's expiration date, do the following:

Windows

Use the AFS "Authentication" application to obtain new AFS tokens or view your current tokens. Check your system tray for two lock icons, possibly with a red 'x' over them.

Of the potentially two lock icons, the correct one for AFS authentencation is the one that says "AFS Client" when you mouse over the icon. The other one will mention AFS and its version number and is not the correct one – this will start the related and separate Keberos for Windows application if you click it.

If you don't see the correct lock icon in your system tray, you can start the AFS Authentication application from the Windows start menu ... Start - O - OpenAFS - Authentication .

In the AFS Authentication application window, to obtain new tokens, click "Obtain new tokens"... your username will be formatted as one of two ways depending on if you have a Cornell NetID or Cornell GuestID:

- netids are: your_netid@CIT.CORNELL.EDU
- guestids are your_guestid@CORNELL.EDU

both are case sensitive... the part after the '@' symbol must be all caps. While your netid or guestid itself must be lowercase.

Linux

Look for the Key icon at the top right of your screen and mouse over the icon. A popup will tell you when your credentials will expire (if renewable the credentials will be renewed). You can also right click on the key icon and choose "List Tickets"... look for the tickets labeled "afs/cnf.cornell.edu@CNF.CORNELL.EDU" . If the key icon has a yellow exclamation or a red x, then you should manually obtain new credentials. Simply left click on the key icon – you will be prompted for your password.

Or from the commandline, type "tokens" to see your tokens.

To obtain new tokens, either use the GUI application (key icon) mentioned above or from the commandline type in kinit <username> followed by entering your password followed by typing in: aklog. See below for proper formatting of your username.

Newer versions of the gui krb5-auth-dialog application (the key icon mentioned above) have the ability to obtain and renew AFS tokens – you can install and configure this application on your local Linux system.

Macintosh

The built-in System Preferences panel for managing AFS tokens does not work properly in the CNF environment. Do not use it.

We suggest using the GUI AFSLog application . This application will first open the Kerberos Ticket Viewer. After logging into Kerberos, exit the Kerberos Ticket Viewer. In approximately 5 seconds, the AFSLog application will either bounce for your attention or pop up a new window. The new window will show you your AFS tokens.

Alternatively, you may use the commandline. Open a terminal.On the commandline, type in kinit <username> followed by aklog .See below for proper formatting of your username. The "tokens" command will list your AFS tokens.

General

You can both destroy your existing tokens and obtain new tokens using the above Windows and Linux applications.

When obtaining new tokens, if using a Cornell netid, your username must be formatted as:
netid@CIT.CORNELL.EDU (@CIT.CORNELL.EDU must be all caps).

If using a Cornell GuestID (gid-xxxx), your username must be formatted as:
guestid@CORNELL.EDU (@CORNELL.EDU must be all caps).

Access Control Lists

An Access Control List (ACL) is the AFS mechanism which let you access directories and files. This access mechanism works as follows:

*base permissions apply to directories (not files)
*new sub-directories inherit from parent directory permissions
*files have no individual protection. They inherit the protection from the directory they sit in.

ACLs are composed of pairs [protection group or user, access rights]. For example, grp_users (the group of all users) might have read permissions on a particular directory.

Access Rights

There are seven access rights. Four deal with directories:

*a (administer) : right to administer of the ACLs of this directory
*l (lookup) : right to list the content of the directory
*d (delete) : right to delete files or sub-directories
*i (insert) : right to create new files or directories

The three others, while set on the directory, apply to the files within the directory:

*r (read) : right to read a file
*w (write) : right to write in a file
*k (lock) : right to lock a file

Some aliases of the above ACLs:

*read = rl
*write = rlidwk
*all = rlidwka
*none = no right at all

Unix group and other mode bits on files are ignored.

Protection Groups

There are several pre-existing AFS protection groups:

*system:administrators
: whose members are the AFS administrators of the current cell

*system:anyuser
: every user, being or not authenticated within this cell or another cell

*grp_all
: everyone who has an account on our fileserver

*grp_staff
: all CNF staff

*grp_users
: all CNF users

*grp_it
: Your friendly CNF IT staff

*cnfhosts
: Every computer on the CNF office and lab networks (but not on RedRover)

Working with AFS Protection Groups

Windows

Open up a command prompt (Start - Run - cmd). View your group membership with the following command:

pts membership

Linux

From a terminal (XTerm from the Applications - CNF Applications menu on CNF Thin, or simply a terminal on your own Linux box), type in (**all lower case**):

```
   pts membership netid@cit.cornell.edu
```

or for a GuestID:

```
   pts membership gid-guestid@cornell.edu
```

Substituting your netid or guestid for "netid" and "gid-guestid" above.

Working with Directory ACLs

Windows

Right click on a folder in AFS. Choose AFS, and then choose Access Control Lists. You may edit ACLs on folders for which you have "all" (rlidwka) permissions (for example, those in your AFS home directory)

Linux

Use the linux commandline...

From a terminal, use fs la directory and fs sa directory acl. For example:

```
$ fs la /afs/cnf.cornell.edu
Access list for /afs/cnf.cornell.edu is
Normal rights:
  cnfhosts rl
  grp_all rl
  grp_it rlidwka
  system:administrators rlidwka
  system:anyuser rl
```

If I was in the system:administrators group, I could change the ACLs on /afs/cnf.cornell.edu to, for example, give system:anyuser write access:

```
$ fs sa /afs/cnf.cornell.edu system:anyuser write
```

Home Directories

Every CNF user has a personal home directory in its own volume under AFS. User home directories are located at /afs/cnf.cornell.edu/home/users/username . Initial quota is TBD. Staff home directories are located at /afs/cnf.cornell.edu/home/staff/ .

On Windows, your W drive is your AFS home directory. And your X drive is the top level of the CNF AFS cell.

In your home directory are a few pre-defined folders with permissions set appropriately:

*public - others can read but not write to this directory. You can place files to be shared with others, here.

*private - as implied by the name, no one but you can get to or even see the files here

*incoming - others can place files for you here (but not read or modify existing files in this directory)

*windows_profile - where your Windows XP roaming profile is stored (Desktop, My Documents, etc)

*win_folders - where your Windows 7 Desktop, My Documents, Downloads, Pictures, etc folders are stored

*Yesterday - a daily snapshop of the files and folders in your AFS home directory.

The rest of the folders and files, by default, can be seen, but not read, by others. So, feel free to create other directories in your home directory. You can, of course, also change the Access Control Lists on any of these predefined folders however you choose.

CNF Shares

CNF Public Share

Located at /afs/cnf.cornell.edu/shares/public/cnf
Anyone on a computer on one of the CNF networks any any user of our files server can read, write, create, modify, and delete files here.

CNF Outside Users Share

Located at /afs/cnf.cornell.edu/shares/public/outside_users
Only staff can write to this share.
Files in this share can be read by anyone anywhere in the world.