How do I enable access control on Debathena?

Q: How do I enable access control on Debathena?

Answer

By default, debathena-login and debathena-workstation will configure machines such that any Athena account holder can login locally, while only those users that have local accounts on the system (i.e. those in /etc/passwd) can login remotely. You can reconfigure this as follows:

First, make sure your installation is up-to-date (aptitude update; aptitude dist-upgrade).

Then, edit `/etc/security/access.conf` to configure the access controls. Each line in the file has the following format:

```
permission:user:origins
```

"Permission" is either "+" (access granted) or "-" (access denied). "User" is a list of login names, groups, or "ALL", meaning all users. "Origins" is a list of tty names, host names, domain names, IP addresses or the words "ALL", "NONE", or "LOCAL".

The comments in the default file offer some pretty good documentation. The following example file may also be of help (we do not recommend you copy this file verbatim).

```
# Only root, joeuser, and janeuser can log in
-:ALL EXCEPT root joeuser janeuser:ALL

# Only joeuser and janeuser can log in remotely.
-:ALL EXCEPT joeuser janeuser:ALL EXCEPT LOCAL

# Only users in group myfriends can log in.
-:ALL EXCEPT myfriends:ALL

# Only joeuser and users with local accounts can log in
+:nss-local-users joeuser:ALL
-:ALL:ALL
```

Any group which appears in /etc/security/access.conf must either be a local group, or must be marked as an NFS group in Moira (you can mark a Moira group that you own as an NFS group using blanche -N LIST). Also, be aware that changes to the membership of Athena NFS groups take a few hours to take effect.

In setting your security policy, you may find useful the special groups `nss-local-users` and `nss-nonlocal-users`, which are the users who have (and don't have) local accounts on the system.

Users who are in a very large number of NFS groups may not be reported as being in some of their groups. You can check which groups Hesiod reports for a given user by running:
`hesinfo joeuser grplist`