LCLS Controls Shared Accounts

How-to Add Users to a Shared Account

References

Getting Started with SSH

How-To Obtain Access to a Shared Account

There are methods to provide users access to a shared password-lesss account. The first method requires adding the ssh2 key to the ssh2 authorization file of the shared account. Alternatively, SCCS has a mechanism in place that allows the login to a password-less account, to be automatically tied to the membership of AFS groups. This allows any member of the "owner" AFS group, to control who has login access to the shared account without any need to mess with SSH keys.

Method 1: Using SSH2 Keys to gain access to a shared account

The command ssh-keygen should only be run once. If your ~/.ssh/id_rsa.pub file is not empty then do not run this command.

STEP 1.
First you will need to generate a rsa publich key. To do this you will need to log into your afs account and issue the following command. Responds to all questions with a return.

ssh-keygen -t rsa

Generating public/private rsa key pair.
Enter file in which to save the key (/u/cd/<username>/.ssh/identity.pub): <return>
Enter passphrase (empty for no passphrase): <return>
Enter same passphrase again: <return>
Your identification has been saved in /u/cd/<username>/.ssh/identity.pub.
Your public key has been saved in /u/cd/<username>/.ssh/identity.pub.

STEP 2.
Send a request to the owner of the shared account, asking that they add your ssh key to that account.
In the exapmle below, to find out the owner of the the NIS group or netgroup is cdvx type the following from the Unix shell.

ypgroup examine -group cdvx
Group 'cdvx':
GID: 2127
Comment:
Last modified at Dec 10 16:21:19 2007 by user
Owners: <usernames>
Members: user1 user2 user3 ...

To add the SSH2 Keys to the account authorization file the owner of the account will type the following from the Unix shell.

cat <username>/.ssh/identity.pub >> <shared_account>/.ssh/authorized_keys2

_Note: This leaves the shared account as the owner of authorized_keys but with changed contents. Also, the authorized_keys file will work only if it is owned by shared account. To determine the owner of an AFS "password-less" account group use the unix command _

$ ypmatch <shared_account> passwd

To determine the shared account groups, type the following. Note that the first group in the list is the primary group, and all others are considered secondary groups.

groups <shared_account>

To add a new user to an NIS group see the example below:

ypgroup adduser -group cdvx -user <username>

To add the new user to the primary AFS Group:
pts adduser -user <username> -group <shared_account>:<shared_account>

If the new user needs to run cron jobs under shared account and wants to receive email regarding problems with any of these jobs, then add the email address of the new user to

<shared_account>/.forward

Add new user to the NIS Group
To find out the members in the <shared_account> NIS group use the following unix command

$ ypmatch <shared_account> group

Done. The user can now log into the shared account using ssh

Method 2: Using ACLs to gain access to a shared account
Send email to the owner of the account ACL, and request that you be added to users ACL listed in the .k5login.README file, located in the home directory of the shared account. See the example below.

/u/cd/cdvx> more .k5login.README

Do not edit the .k5login file for this account. The .k5login file for this
account is being maintained by an automated process and your changes will
be deleted after a few minutes.

If you want to add a user for access to this account you need to add that
unix id to the appropriate AFS PTS Group. The groups/ids being used to
construct the .k5login account for this account are

PTS(cdvx:owner-cdvx) PTS(cdvx:cdvx) ID(cdvx)

See: http://www.slac.stanford.edu/comp/unix/ssh_shared.html

for more details or contact unix-admin@slac.stanford.edu

To find out the ACLs of an account, changeto the home directory of that account and type the following:

fs listacl

To find out the members of the "owner" ACL follow the example below, where the "owner" group is cdvx:owner-cdvx

/u/cd/cdvx>pts members cdvx:owner-cdvx
Members of cdvx:owner-cdvx (id: -5085) are:
user1
user2

user3

Finally, find out if you are already a member of the "user" ACL, by following the example below where cdvx:cdvx is the "user" ACL.

/u/cd/cdvx>pts members cdvx:ocdvx
Members of cdvx:cdvx (id: -5086) are:
user1
user2
user3

If you're not a member of the "user" ACL, then send the "owner" ACL an email requesting that you be added to the "user" ACL of that account.