Installing Cheyenne SSH keys

Install your SSH keys on a remote system as shown below and you will not need to authenticate each time you transfer files to that system from your GLADE file spaces. This simplifies the process of making both manual and unattended file transfers.

Not all systems accept such SSH key-based transfers.

Adding SSH keys to remote systems

First, log in to Cheyenne and generate a key pair by executing **ssh-keygen** on your command line.

```
ssh-keygen
```

The output will look like this:

```
Generating public/private rsa key pair.
Enter file in which to save the key (/glade/u/home/username/.ssh/id_rsa):
```

Hit **Enter** at that point. If the **id_rsa** file already exists, overwrite it.

```
/glade/u/home/username/.ssh/id_rsa already exists.
Overwrite (y/n)? y
```

When you're asked to enter a passphrase, just hit **Enter** both times.

```
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /glade/u/home/username/.ssh/id_rsa.
Your public key has been saved in /glade/u/home/username/.ssh/id_rsa.pub.
The key fingerprint is:
43:a2:d2:a5:c3:bb:dd:12:43:ad:8a:98:b2:a2:9b:5d username@cheyenne6
The key's randomart image is:
+--[ RSA 2048]----+>
|           ..    |
|          + ..   |
|         + o ++  |
|         .o ++ ..|
|        R .=o + +|
|          ...o * |
|           .. + .|
|        ...    . |
|        E+o      |
+-----------------+
```

Next, rename the public key file and transfer it to **~/.ssh** on the remote machine, which we'll call "Supersystem" for this example.

```
cp id_rsa.pub newname
scp .ssh/newname username@supersystem.univ.edu:.ssh
The authenticity of host 'supersystem (138.117.215.218)' can't be established.
RSA key fingerprint is 43:a2:d2:a5:c3:bb:dd:12:43:ad:8a:98:b2:a2:9b:5d
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'supersystem,138.117.215.218' (RSA) to the list of known hosts.
username@supersystem.univ.edu's password:
newname 100% |*******************| 607   00:00
```

Log in to the remote system, authenticating as required, then append the new file to the **authorized_keys** file on that machine.

```
cd ~/.ssh
cat newname >> authorized_keys
```

Finally, change the permissions of authorized_keys and the .ssh directory.

```
chmod 600 authorized_keys
cd ..
chmod 700 .ssh
```

You will no longer need to enter a password on the remote machine when you transfer files to it using Cheyenne.