Setting Up Passwordless SSH (SSH Keys) on the Clusters

Background

Passwordless SSH is required on the Shared Computing Resources if you need to run MPI jobs using *srun*, or need to use other specialized software which uses SSH for communication between nodes. The *srun* command spawns copies of your executable on all of the nodes allocated to you by SLURM. It will communicate with these nodes via SSH so it is necessary that SSH is configured with SSH host keys (passwordless SSH) for your account. This document describes how to enable passwordless SSH on these systems.

Create Host Key

The first step in establishing passwordless SSH is to create your public host keys. Login to the cluster and run the *ssh-keygen* command. Accept all of the default values and do not enter a passphrase.

```
[beaker@login1 ~]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/beaker/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/beaker/.ssh/id_rsa.
Your public key has been saved in /home/beaker/.ssh/id_rsa.pub.
The key fingerprint is:
06:2c:2c:c5:e9:74:f0:ed:25:59:d1:fc:c3:90:4f:75 beaker@login1.nots.rice.edu
The key's randomart image is:
+--[ RSA 2048]----+
|    .oo  o+ . .. E|
|    o+o.o .= .   . |
|   .oo.+ + .*     |
|   ... o o  =     |
|        S    .    |
|        .         |
+-----------------+
```

Add Host Key to authorized_keys File

After you have created your public host key above, append the contents of *~/.ssh/id_rsa.pub* to *~/.ssh/authorized_keys*. This will enable *mpirun* to login from one compute node to another using SSH without a password.

```
[beaker@login1 ~]$ cat .ssh/id_rsa.pub >> .ssh/authorized_keys
```

> ⊘ Your secret key (id_rsa) is all that is needed to log into your account now. Ensure that nobody else may read it or copy it from your account

> ⊘ **Create authorized_keys file**
> You should create your authorized_keys file if it does not exist.

Disable SSH Host Key Checking

To avoid ssh prompts when automatically logging into compute nodes allocated by the scheduler, configure ssh to not use strict host key checking. Create the file *~/.ssh/config* as shown below.

```
Host *
    StrictHostKeyChecking no
    UserKnownHostsFile /dev/null
    LogLevel QUIET
```

This will also suppress creation of entries in *~/.ssh/known_hosts* and reduce log messages.