Cheatsheet for lam-mpi

Oliver Koch

March 5, 2008

Setup

login to pool: From outside you first need to log into www.numa.uni-linz.ac.at. If you are going to run 32bit MPI-code log into any host in the pool (pool2-01 .. pool2-12) and use the following .bhost file:

```
pool2-01 cpu=1
pool2-02 cpu=2
pool2-03 cpu=2
pool2-04 cpu=2
pool2-05 cpu=2
pool2-06 cpu=2
pool2-07 cpu=2
pool2-08 cpu=2
```

(The hosts pool2-09 to pool2-12 are not listed because of their slow Pentium3 CPU)
If you are going to run 64bit MPI-code log into one of the 64bit hosts instead (pool2-03 .. pool2-08) and adapt your .bhost file:

```
pool2-03 cpu=2
pool2-04 cpu=2
pool2-05 cpu=2
pool2-06 cpu=2
pool2-07 cpu=2
pool2-08 cpu=2
```

Enabling passwordless logins via ssh-agent

First you need to generate a key-pair by issuing the command ssh-keygen. Enter a passphrase when asked. Use at least 10 characters, including numbers, captial and non captial letters. If you cannot think of a good password use pwgen which generates mnemonic passwords for you.

```
$ pwgen 10 1
Ga8Woowut2
```

$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/poseidon2/koch/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in id_rsa.
Your public key has been saved in id_rsa.pub.
The key fingerprint is:
a0:45:2f:f8:40:83:0a:f5:cd:ac:17:e2:ce:16:61:2e user@www

Then you have to give authorization to log in with the keypair by putting the public key into .ssh/authorized_keys:
$ cat .ssh/id_rsa.pub >> .ssh/authorized_keys
Now you shifted authentication from system password to the passphrase you provided when generating the keypair. These steps have do be done only once.
Make the computer remember this passphrase by using keychain and we have arrived at a reasonably secure passwordless login.
$ eval ‘keychain –eval id_rsa‘
After entering the passphrase you used when generating the keypair, you should be able to login to all the hosts in the pool without being asked for a password or passphrase. With the standard options for keychain the computer will remember the passphrase as long as your keychain process and its siblings (ssh-agent) run. I recommend you to start the keychain command everytime after you login before you start lamboot for the first time in that session.
Now check if all hosts are available:
$ recon
If you get the ‘Woo hoo!’ message everything is all right and you can continue with the next section. If less than 8 hosts are up you have to remove the host(s) not listed in this output from your .bhost file. Also drop a line to oliver.koch@numa.uni-linz.ac.at stating which host is not up, please.

starting lam service

$ lamboot
This should not take longer than 5 seconds. If you see an error message consult the man pages. Contact me (KG 506, Tel. 9166) if you can’t solve the problem on your own.
$ man lamboot

starting your lam-mpi programs

$ mpirun -np < # > <mpi_executable>
< # > gives the number of processes to start
After you are done don’t forget to use lamhalt to stop the lam session. If you leave lam sessions hanging around they will be killed without warning.
$ lamhalt