

Configurer son Client SSH

Pourquoi installer et configurer SSH

- sécurisation des transmissions
- si vous utilisez MPICH
- si vous utilisez Condor

Comment Configurer SSH

1. Vérifier que SSH est bien installé sur le réseaux

```
which ssh
```

2. Création de clefs pour SSH

```
ssh-keygen -t rsa
```

3. présentation des clefs

```
clef privéé -> identity
clef publique -> identity.pub
```

4. Publication de sa clef publique

```
cp /.ssh/identity.pub /.ssh/authorized_keys
```

5. Vérification de droit sur le fichier

```
chmod go-rwx /.ssh/authorized_keys
```

6. Création d'un shell secure

```
ssh-agent $SHELL
ssh-add
```

Configurer MPICH avec SSH

1. Configurer MPICH pour qu'il n'utilise plus rsh mais ssh

a. version antérieur à MPICH 1.2.5

```
./configure -rsh=ssh --prefix=/usr/local
```

b. version égale ou supérieur à MPICH 1.2.5

```
tcsch
setenv RSHCOMMAND ssh
./configure --with-comm=shared --prefix=/usr/local
```

2. Vérifier la présence de

```
./ssh/ssh_known_hosts
```

Configurer Condor avec SSH

1. Configurer SSH pour l'utilisateur Condor

2. Editer la liste des machines connues pour qu'elle coïncide avec celles du pool, ces machines sont listées dans

```
/etc/ssh_known_hosts
```

Il existe une commande pour éditer ce fichier

```
make-ssh-known-hosts
```

exemple

```
make-ssh-known-hosts machine.domaine
```

sur les serveurs doivent posséder un fichier de config

```
~root/.ssh/config
```

qui doit contenir les lignes suivantes

```
Host <specific hostname or "*">
BatchMode yes
ConnectionAttempts 1
FallBackToRsh no
```