

linux 环境下

ssh 无密码登录要使用公钥与私钥。linux下可以用ssh-keygen生成公钥/私钥对，下面我以CentOS为例。

有机器A(192.168.1.155)，B(192.168.1.181)。现想A通过ssh无密码登录到B。

1. 在A机下生成公钥/私钥对。

```
[chenlb@A ~]$ ssh-keygen -t rsa -P ''
```

-P表示密码，-P '' 就表示空密码，也可以不用-P参数，这样就要三车回车，用-P就一次回车。

它在/home/chenlb下生成.ssh目录，.ssh下有id_rsa和id_rsa.pub。

2. 把A机下的id_rsa.pub复制到B机下，

```
[chenlb@A ~]$ scp .ssh/id_rsa.pub chenlb@192.168.1.181:/home/chenlb/id_rsa.pub
```

```
chenlb@192.168.1.181's password:
```

```
id_rsa.pub                                100% 223      0.2KB/s   00:00
```

由于还没有免密码登录的，所以要输入密码。

3. B机把从A机复制的id_rsa.pub添加到.ssh/authorized_keys文件里。

```
[chenlb@B ~]$ cat id_rsa.pub >> .ssh/authorized_keys
```

```
[chenlb@B ~]$ chmod 600 .ssh/authorized_keys
```

authorized_keys的权限要是600。 。(要保证.ssh和authorized_keys都只有用户自己有写权限。否则验证无效。)

4. A机登录B机。

```
[chenlb@A ~]$ ssh 192.168.1.181
The authenticity of host '192.168.1.181 (192.168.1.181)' can't be established.
RSA key fingerprint is 00:a6:a8:87:eb:c7:40:10:39:cc:a0:eb:50:d9:6a:5b.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.181' (RSA) to the list of known hosts.
Last login: Thu Jul  3 09:53:18 2008 from chenlb
[chenlb@B ~]$
```

第一次登录是时要你输入yes。

现在A机可以无密码登录B机了。

小结：登录的机子可有私钥，被登录的机子要有登录机子的公钥。这个公钥/私钥对一般在私钥宿主机产生。上面是用rsa算法的公钥/私钥对，当然也可以用dsa(对应的文件是id_dsa, id_dsa.pub)

想让A, B机无密码互登录，那B机以上面同样的方式配置即可。

参考：SSH-KeyGen 的用法

http://blog.163.com/chen98_2006@126/blog/static/158584272007101862513886/

win7 环境下 下载SecureCRT软件 选项->ssh2->公钥->选择id_rsa.pub文件, 然后SSH登录指定机器则不需要输入密码