# **[scp免密码传送文件](http://www.cnblogs.com/peizhe123/p/5699052.html)**

在Linux环境下，两台主机之间传输文件一般使用scp命令，通常用scp命令通过ssh获取对方linux主机文件的时候都需要输入密码确认。

不过通过建立信任关系，可以实现不输入密码。

这里假设A的IP：192.168.10.1

B的IP：192.168.10.2

需要从A免密码输入复制文件至B。

**1**. 在主机A上执行如下命令来生成配对密钥：   
**ssh-keygen -t rsa**  
按照提示操作，注意，不要输入passphrase。提示信息如下   
Generating public/private rsa key pair.   
Enter file in which to save the key (/root/.ssh/id\_rsa):    
Enter passphrase (empty for no passphrase):    
Enter same passphrase again:    
Your identification has been saved in /root/.ssh/id\_rsa.   
Your public key has been saved in /root/.ssh/id\_rsa.pub.   
The key fingerprint is:   
ff:8e:85:68:85:94:7c:2c:46:b1:e5:2d:41:5c:e8:9b  root@localhost.domain   
  
**2**. 将 .ssh 目录中的 id\_rsa.pub 文件复制到 主机B 的 ~/.ssh/ 目录中，并改名为  authorized\_keys。   
scp .ssh/id\_rsa.pub 192.168.10.2:/root/.ssh/authorized\_keys   
  
以后从A主机scp到B主机就不需要密码了。

**3**.使用此方法需要注意：复制的两台计算机需要用相同的账户名，这里都是用的root。为了安全起见，需要在两台机器中创建相同的账号，然后在A上用su命令切换至账号下，执行第1步，第二步中复制文件时可能.ssh目录并不存在，需要手动创建。

在第2步中如果机器中已经存在authorized\_keys文件，则需注意，这个文件可以包含多个SSH验证信息，这时可用 cat >>命令将验证文件内容附加上去。

比如复制到scp .ssh/id\_rsa.pub 192.168.10.2:/root/.ssh/a.pub

然后执行cat ~/.ssh/a.pub >> ~/.ssh/authorized\_keys