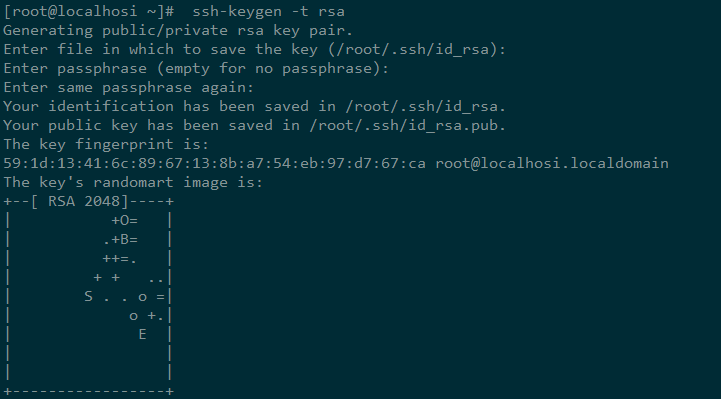
A为本地主机(即用于控制其他主机的机器) ;

B为远程主机(即被控制的机器Server), ip为192.168.254.10 ;

A和B的[系统](http://www.2cto.com/os/)都是[Linux](http://www.2cto.com/os/linux/)

在A上的命令:

# ssh-keygen -t rsa (连续三次回车,即在本地生成了公钥和私钥,不设置密码)



把A主机生成的id\_rsa.pub拷贝到B主机/root/.ssh/下

# scp ~/.ssh/id\_rsa.pub root@192.168.254.10:.ssh/id\_rsa.pub (需要输入密码)

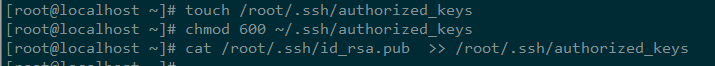


在B上的命令:

# touch /root/.ssh/authorized\_keys (如果已经存在这个文件, 跳过这条)

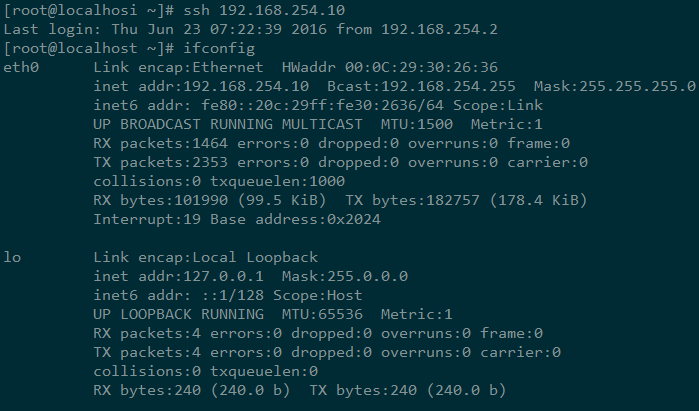
# chmod 600 ~/.ssh/authorized\_keys  (# 注意： 必须将~/.ssh/authorized\_keys的权限改为600, 该文件用于保存ssh客户端生成的公钥，可以修改服务器的ssh服务端配置文件/etc/ssh/sshd\_config来指定其他文件名）

# cat /root/.ssh/id\_rsa.pub  >> /root/.ssh/authorized\_keys (将id\_rsa.pub的内容追加到 authorized\_keys 中, 注意不要用 > ，否则会清空原有的内容，使其他人无法使用原有的密钥登录)



回到A机器:

# ssh root@192.168.254.10 (不需要密码, 登录成功)



至此，已经设置好免密码登录了。