这里所说的ssh是指OpenSSH SSH客户端，是用于登录远程主机，并且在远程主机上执行命令。它的目的是替换rlogin和rsh，同时在不安全的网络之上，两个互不信任的主机之间，提供加密的、安全的通信连接。X11连接和任意TCP/IP端口均可以通过此安全通道转发。

在RedHat 6.1中，默认安装的OpenSSL是一种比较常见的SSH服务端和客户端软件，默认端口是22。

SSH服务端其实是一个守护进程（daemon），在后台运行并相应来自客户端的连接请求。服务端一般是sshd进程，提供了对远程连接的处理，一般包括公共密钥认证、密钥交换、对称密钥加密和非安全连接等。

SSH客户端程序包括ssh程序，及scp（远程拷贝）、slogin（远程登录）、sftp（安全文件传输）等其他的应用程序。

在有些情况下，需要实现ssh的无密码登录，或者称为免密码登录。比如：**[Hadoop](http://lib.csdn.net/base/20" \o "Hadoop知识库" \t "_blank)**的伪分布式模式部署、完全分布式模式部署。

**配置**

有两台主机：主机A：192.168.1.132，主机B：192.168.1.133，需要配置主机A无密码登录主机A、主机B。

**生成私钥、公钥**

在主机A上：

**[plain]** [view plain](http://blog.csdn.net/liuxinghao/article/details/40082481) [copy](http://blog.csdn.net/liuxinghao/article/details/40082481)

1. $ cd ~/.ssh（如果没有改文件夹，直接创建一个）
2. $ ssh-keygen -t rsa

上面的ssh-keygen命令中，参数-t是生成密钥的方式，有三种方式：协议版本1的rsa1、协议版本2的rsa和dsa。通常选rsa或dsa，既安全，又省事。

这个时候会打印一些执行结果及交互操作，一路回车即可。

**[plain]** [view plain](http://blog.csdn.net/liuxinghao/article/details/40082481) [copy](http://blog.csdn.net/liuxinghao/article/details/40082481)

1. Generating public/private rsa key pair.
2. Enter file in which to save the key (/home/lxh/.ssh/id\_rsa):
3. Enter passphrase (empty for no passphrase):
4. Enter same passphrase again:
5. Your identification has been saved in /home/lxh/.ssh/id\_rsa.
6. Your public key has been saved in /home/lxh/.ssh/id\_rsa.pub.
7. The key fingerprint is:
8. 2e:34:7c:3a:be:e4:3b:93:2f:1d:32:4f:2d:fe:13:a1 lxh@master
9. The key's randomart image is:
10. +--[ RSA 2048]----+
11. |                 |
12. |                 |
13. |                 |
14. |     .    .      |
15. |      + So .     |
16. |     .o=E o      |
17. |      =O.o .     |
18. |     +=o+ .      |
19. |      =B....     |
20. +-----------------+

**生成存放RSA/DSA的公钥**

直接复制生成的id\_rsa.pub文件即可。

**[plain]** [view plain](http://blog.csdn.net/liuxinghao/article/details/40082481) [copy](http://blog.csdn.net/liuxinghao/article/details/40082481)

1. $ cp id\_rsa.pub authorized\_keys
2. $ chmod 600 authorized\_keys

按理说此时就可以无密码登录本机了，即通过命令：

**[plain]** [view plain](http://blog.csdn.net/liuxinghao/article/details/40082481) [copy](http://blog.csdn.net/liuxinghao/article/details/40082481)

1. $ ssh localhost

第一次需要输入一个yes，因为需要在第一次登录该主机时记录有用户登录，之后就不会出现了。

**复制公钥**

然后将公钥文件authorized\_keys拷贝到主机B的相同位置上。

**[plain]** [view plain](http://blog.csdn.net/liuxinghao/article/details/40082481) [copy](http://blog.csdn.net/liuxinghao/article/details/40082481)

1. $ scp authorized\_keys 192.168.1.133:~/.ssh

因为已经在主机A上修改过authorized\_keys的权限，一般主机B上也是600格式，如果不是，就修改主机B上的authorized\_keys文件权限为600。

**[plain]** [view plain](http://blog.csdn.net/liuxinghao/article/details/40082481) [copy](http://blog.csdn.net/liuxinghao/article/details/40082481)

1. $ chmod 600 authorized\_keys

一般情况下，可以通过主机A无密码登录主机A和主机B了。

**FQA**

**登录时出现“Agent admitted failure to sign using the key.”**

在~/.ssh目录中执行

**[plain]** [view plain](http://blog.csdn.net/liuxinghao/article/details/40082481) [copy](http://blog.csdn.net/liuxinghao/article/details/40082481)

1. $ ssh-add

出现下面的信息，就成了：

**[plain]** [view plain](http://blog.csdn.net/liuxinghao/article/details/40082481) [copy](http://blog.csdn.net/liuxinghao/article/details/40082481)

1. Identity added: /home/lxh/.ssh/id\_rsa (/home/lxh/.ssh/id\_rsa)

如果提示下面的信息：

**[plain]** [view plain](http://blog.csdn.net/liuxinghao/article/details/40082481) [copy](http://blog.csdn.net/liuxinghao/article/details/40082481)

1. Could not open a connection to your authenticationh agent

就执行：

**[plain]** [view plain](http://blog.csdn.net/liuxinghao/article/details/40082481) [copy](http://blog.csdn.net/liuxinghao/article/details/40082481)

1. ssh-agent bash

**没有错误信息，但需要输入密码登录**

需要查看一下.ssh目录和authorized*keys文件的权限，需要.ssh目录的权限为700，authorized*keys文件的权限为600。如果主机A连接主机B，就在主机B上执行：

**[plain]** [view plain](http://blog.csdn.net/liuxinghao/article/details/40082481) [copy](http://blog.csdn.net/liuxinghao/article/details/40082481)

1. $chmod 700 ~/.ssh
2. $chmod 600 ~/.ssh/authorized\_keys

**ssh代理未开启**

通过命令查看ssh代理是否开启

**[plain]** [view plain](http://blog.csdn.net/liuxinghao/article/details/40082481) [copy](http://blog.csdn.net/liuxinghao/article/details/40082481)

1. $ ps -ef|grep ssh-agent

如果开启了，直接kill掉，然后启动ssh代理。

**[plain]** [view plain](http://blog.csdn.net/liuxinghao/article/details/40082481) [copy](http://blog.csdn.net/liuxinghao/article/details/40082481)

1. $ ssh-agent

如果还是不行，就重启ssh服务：

**[plain]** [view plain](http://blog.csdn.net/liuxinghao/article/details/40082481) [copy](http://blog.csdn.net/liuxinghao/article/details/40082481)

1. # service sshd restart（需要root权限）