scp使用说明与各类情况的应对

一、解决连接被拒绝问题

在准备通过scp指令将本地文件传输到服务器的时候出现ssh: connect to host *** port 22: Connection timed out 的问题。讲解决过程记录如下：

\1. 首先输入ssh localhost 指令查看ssh是否安装和启动，如果未启动输入service ssh start，如果未安装输入apt-get install openssh-server。

\2. 运行ps -e | grep ssh指令查看sshd是否启动，如果未启动输入service sshd start。

\3. 倘若以上都不可以，检查防火墙是否开启。

二·、解决访问被拒绝问题

使用scp命令准备向目标服务器传输文件，但是遇到Permission denied这个问题，意思就是拒绝访问。解决如下：

1.方法一：修改目录的访问权限（一般）

2.方法二：传输到/tmp目录下，不需要权限（差）

3.方法三：在Client的root和Server的root之间建立安全信任关系（优）

（1）在机器Client上root用户执行ssh-keygen命令，生成建立安全信任关系的证书。

[root@Clientroot]# ssh-keygen -b 1024 -t rsa

Generatingpublic/private rsa key pair.

Enter file inwhich to save the key (/root/.ssh/id_rsa):

Enter passphrase(empty for no passphrase): <-- 直接输入回车则无密码

Enter samepassphrase again: <-- 直接输入回车则无密码

Youridentification has been saved in /root/.ssh/id_rsa.

Your public keyhas been saved in /root/.ssh/id_rsa.pub.

The key fingerprintis:

49:9c:8a:8f:bc:19:5e:8c:c0:10:d3:15:60:a3:32:1croot@Client

[root@Clientroot]#

注意：在程序提示输入passphrase时直接输入回车，表示无证书密码。

上述命令将生成私钥证书id_rsa和公钥证书id_rsa.pub，存放在用户家目录的.ssh子目录中。

（2）将公钥证书id_rsa.pub复制到机器Server的root家目录的.ssh子目录中，同时将文件名更换为authorized_keys。
[root@Client root]# scp -p .ssh/id_rsa.pub root@192.168.3.206:/root/.ssh/authorized_keysroot@192.168.3.206's password: <-- 输入机器Server的root用户密码

id_rsa.pub 100% |**********| 218 00:00

[root@Client root]#

在执行上述命令时，两台机器的root用户之间还未建立安全信任关系，所以还需要输入机器Server的root用户密码。

经过以上2步，就在机器Client的root和机器Server的root之间建立安全信任关系。

三、使用说明

-r 若 source 中含有目录名，则将目录下之档案亦皆依序拷贝至目的地。

-f 若目的地已经有相同档名的档案存在，则在复制前先予以删除再行复制。

-v 和大多数 linux 命令中的 -v 意思一样，用来显示进度 . 可以用来查看连接，认证，或是配置错误 .

-P 选择端口 . 注意 -p 已经被 rcp 使用 .