ssh 192.168.1.100 # 默认利用当前宿主用户的用户名登录

ssh omd@192.168.1.100 # 利用远程机的用户登录

ssh omd@192.168.1.100 -o stricthostkeychecking=no # 首次登陆免输yes登录

ssh omd@192.168.1.100 "ls /home/omd" # 当前服务器A远程登录服务器B后执行某个命令

ssh omd@192.168.1.100 -t "sh /home/omd/ftl.sh" # 当前服务器A远程登录服务器B后执行某个脚本

1.登录

ssh -p22 omd@192.168.25.137

2.直接执行命令 -->最好全路径

ssh root@192.168.25.137 ls -ltr /backup/data

==>ssh root@192.168.25.137 /bin/ls -ltr /backup/data

3.查看已知主机

at /root/.ssh/known\_hosts

4.ssh远程执行sudo命令

ssh -t omd@192.168.25.137 sudo rsync hosts /etc/

5.scp

1.功能 -->远程文件的安全(加密)拷贝

scp -P22 -r -p /home/omd/h.txt omd@192.168.25.137:/home/omd/

2.scp知识小结

scp是加密远程拷贝，cp为本地拷贝

可以推送过去，也可以拉过来

每次都是全量拷贝(效率不高，适合第一次)，增量拷贝用rsync

6.ssh自带的sftp功能

1.Window和Linux的传输工具

wincp filezip

sftp -->基于ssh的安全加密传输

samba

2.sftp客户端连接

sftp -oPort=22 root@192.168.25.137

put /etc/hosts /tmp

get /etc/hosts /home/omd

3.sftp小结：

1.linux下使用命令： sftp -oPort=22 root@x.x.x.x

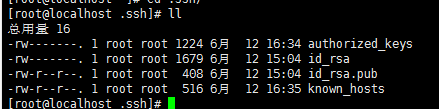
2.put加客户端本地路径上传

3.get下载服务器端内容到本地

4.远程连接默认连接用户的家目录

互信

在一个机器上面用ssh-keygen 在当前用户下生成.ssh目录。就是生成公钥和私钥。这个文件下面还有authorized\_keys文件，和known\_hosts。如下图：



第二步就是将A机器的公钥，添加到B机器authorized\_keys文件中。将B机器的公钥添加到A机器的authorized\_keys文件中。这样A、B机器就互信了。然后A、B机器就可以通过ssh ip命令来免密登录到对方机器上。