安全攻略SSH服务连接时常见问题解答 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/245/2021_2022__E5_AE_89_E5_85_A8_E6_94_BB_E7_c103_245705.htm 什么是SSH呢? SSH的英文全称是Secure SHell。通过使用SSH，你可以把所有传输的数据进行加密，这样"中间人"这种攻击方式就不可能实现了，而且也能够防止DNS和IP欺骗。还有一个额外的好处就是传输的数据是经过压缩的，所以可以加快传输的速度。SSH有很多功能，它既可以代替telnet，又可以为ftp、pop、甚至ppp提供一个安全的"通道"。SSH客户端与服务器端通讯时，用户名及口令均进行了加密，有效防止了对口令的窃听。最初SSH是由芬兰的一家公司开发的。但是因为受版权和加密算法的限制，现在很多人都转而使用OpenSSH。OpenSSH是SSH的替代软件，而且是免费的，可以预计将来会有越来越多的人使用它而不是SSH。SSH是由客户端和服务端的软件组成的。SSH安装容易、使用简单，而且比较常见，一般的Unix系统、Linux系统、FreeBSD系统都附带有支持SSH的应用程序包。 SSH的安全验证是如何工作的? 从客户端来看，SSH提供两种级别的安全验证。 第一种级别(基于口令的安全验证)只要你知道自己帐号和口令，就可以登录到远程主机。所有传输的数据都会被加密，但是不能保证你正在连接的服务器就是你想连接的服务器。可能会有别的服务器在冒充真正的服务器，也就是受到"中间人"这种方式的攻击。 第二种级别(基于密匙的安全验证)需要依靠密匙，也就是你必须为自己创建一对密匙，并把公用密匙放在需要访问的服务器上。如果你要连接到SSH服务器上，客户端软件就会

向服务器发出请求，请求用你的密匙进行安全验证。服务器收到请求之后，先在你在该服务器的家目录下寻找你的公用密匙，然后把它和你发送过来的公用密匙进行比较。如果两个密匙一致，服务器就用公用密匙加密"质询"(challenge)并把它发送给客户端软件。客户端软件收到"质询"之后就可以用你的私人密匙解密再把它发送给服务器。 用这种方式，你必须知道自己密匙的口令。但是，与第一种级别相比，第二种级别不需要在网络上传送口令。 第二种级别不仅加密所有传送的数据，而且"中间人"这种攻击方式也是不可能的(因为他没有你的私人密匙)。但是整个登录的过程可能需要10秒。 命令的格式 首先、确保server端的ssh服务是开的（service shhd start） 然后在client端输入： ssh usrname@serverip （远程登录） scp filename usrname@serverip：/URL (远程传输) 常出现的问题： 问题一 ssh登录的时候链接端口失败 提示（1）： # ssh 172.16.81.221 ssh: connect to host 172.16.81.221 port 22: No route to host 这由于server端没有开机或是网络不通（这个原因很多，最简单的是网线没有插。还有就是可能会是网卡down了等） 提示（2）： # ssh work@172.16.81.221 ssh: connect to host 172.16.81.221 port 22: Connection refused 这是由于对方server的ssh服务没有开。这个server端开启服务即可。 问题二、 ssh到server上的时候密码是对的但是报如下信息： # ssh 172.16.81.221 root@172.16.81.221s password: Permission denied, please try again. 这个是由于如果不输入用户名的时候默认的是root用户，但是安全期间ssh服务默认没有开root用户的ssh权限 解决方法： 要修改root的ssh权限，即修改 /etc/ssh/sshd_config文件中 PermitRootLogin no 改为

PermitRootLogin yes 问题三 登录是出现如下提示： ssh root@172.16.81.221 @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@ @ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @ @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@ IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY! Someone could be eaves0dropping on you right now (man-in-the-middle attack)! It is also possible that the RSA host key has just been changed. The fingerprint for the RSA key sent by the remote host is 76:fb:b3:70:14:48:19:d6:29:f9:ba:42:46:be:fb:77. Please contact your system administrator. Add correct host key in /home/fante/.ssh/known_hosts to get rid of this message. Offending key in /home/fante/.ssh/known_hosts:68 RSA host key for 172.16.81.221 has changed and you have requested strict checking. Host key verification failed. server端密码或是其他发生改变的时候。解决方法一般就需要删除~/.ssh/known_hosts的对应行，然后再登录即可。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com