远程:SecureCRT使用RSA密钥登陆 H PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/293/2021_2022__E8_BF_9C_E7_A8_8B_Sec_c103_293957.htm 一直在SecureCRT 上使用密码和键盘交互方式登陆ssh ，一直没试成功，今天无意在一篇文章里受了点启发，顺便就在前些天装的虚拟机上试成了。客户端用的SecureCRT5.5.1，服务端为openSUSE10.3上默认安装的OpenSSH_4.6p1. 首先配置SecureCRT上的RSA密钥，打开SecureCRT→Quick Connect→Authentiation→PublicKey →Properties→Create Identity File,Key选择RSA；Passphrase可以不同于密码，任意的字符串即可；Key length in为加密长度，可为512到2048位，要是在linux上可配置4096；下一步为生成过程，需要不停在进度条附近晃动鼠标，选择在x:\%USERPROFILE%\Application Data\VanDyke下生成两个文件，并且格式为Openssh Key format，要是选默认的Standard Public Key and VanDyke Private Key可能还需要格式转换或有兼容问题，公钥Identity.pub和私钥Identity。 然后在opensuse上要使用密钥方式登陆的的用户目录下建立.ssh目录，这里我偷懒直接运行ssh-keygen工具创建本机密钥会自动创建.ssh目录并设置合适目录权限。 lxuser@suse10:/etc/ssh> ssh-keygen Generating public/private rsa key pair. Enter file in which to save the key (/home/lxuser/.ssh/id_rsa): Created directory /home/lxuser/.ssh. Enter passphrase (empty for no passphrase): Enter same passphrase again: Your identification has been saved in /home/lxuser/.ssh/id_rsa. Your public key has been saved in /home/lxuser/.ssh/id_rsa.pub. The key fingerprint is:

d8:07:b9:d6:f9:4d:0c:e3:c7:8c:82:f4:a3:20:71:f4 lxuser@suse10 利用sftp或其他方式将公钥Identity.pub上传到刚建立好的.ssh目录里，修改文件名为authorized_keys2,这是因为使用的是authorized_keys这个文件，而用的ssh版本为2(openSUSE默认也仅使用Protocol 2). lxuser@suse10:~/.ssh> mv Identity.pub authorized_keys2 为安全起见，修改该文件的访问权限，保证除属主外没人能修改 lxuser@suse10:~/.ssh> chmod 600 authorized_keys2 lxuser@suse10:~/.ssh> ll 总计 16 -rw------- 1 lxuser users 234 11-02 20:20 authorized_keys2 -rw------- 1 lxuser users 1743 11-02 19:23 id_rsa -rw-r--r-- 1 lxuser users 395 11-02 19:23 id_rsa.pub 再回到SecureCRT，在Quick Connect →Authentiation处仅勾选PublicKey，并设置属性Properties，指定Use identity or certificate file为私钥Identity，确定后连接，正常的话会提示输入前面设置的Passphrase，若成功则直接登陆了。 Last login: Fri Nov 2 20:38:21 2007 from printer.mshome.net Have a lot of fun... 至此任务算基本成功了。既然已经成功使用了ssh的RSA功能，那么索性让openssh只支持RSA验证，否则既支持普通密码又支持RSA就没什么意思了，根本没把安全提高。 修改ssh_config配置文件 lxuser@suse10:/etc/ssh> vi ssh_config 取消密码登陆验证 PasswordAuthentication no 然后重启sshd服务再次尝试用键盘和密码交互登陆，就提示不成功了，而使用PublicKey是方便了许多，免去了反复输入密码的麻烦，安全较高(不过要是客户端宿主机本身不安全，那后果也就.....)。 suse10:/etc/ssh # vi ssh_config suse10:/etc/ssh # rcsshd restart Shutting down SSH daemon done Starting SSH daemon done 100Test 下载频道开通，各类考试题目直接下载。详细请访问