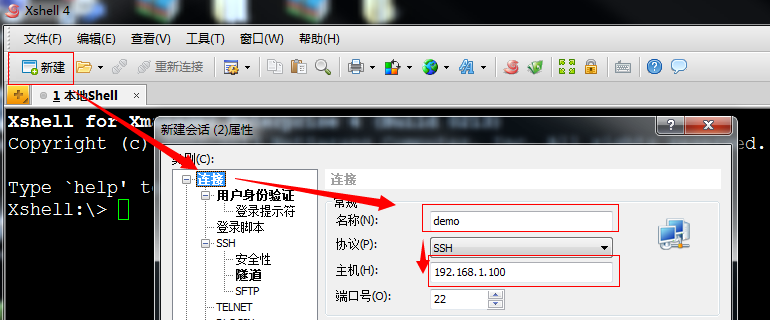
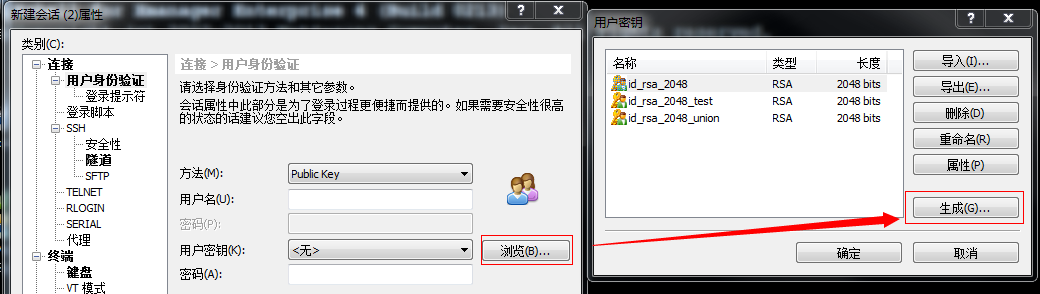
1.创建密钥文件

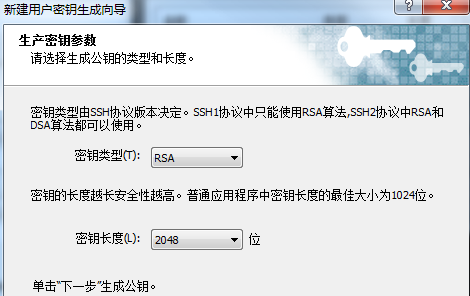
打开xshell，新建会话，填写名称如demo，填写主机如192.168.1.100，如下：



点左侧的用户身份验证，方法选择public key，用户密钥点浏览，打开用户密钥窗口，如下：



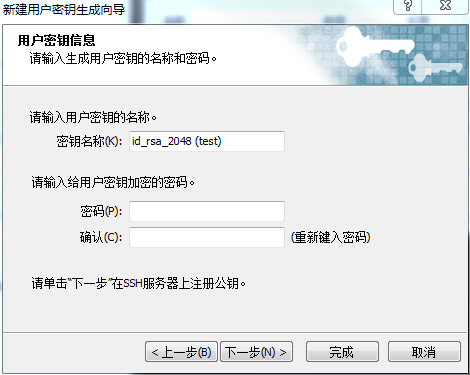
点生成，打开新建用户密钥生成向导，选择密钥类型RSA，密钥长度2048位，如下：



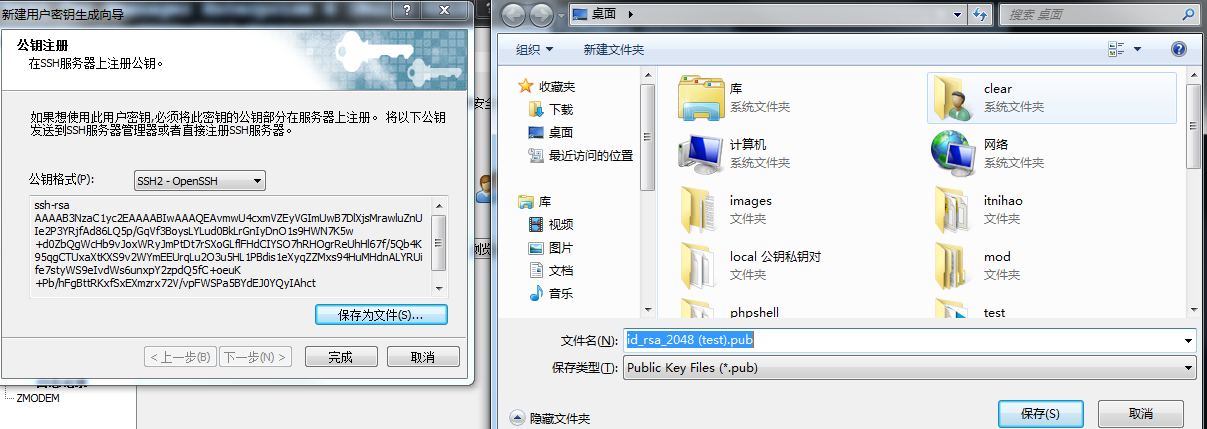
点下一步，开始生成公钥和私钥对，提示公钥对已成功生成，如下：



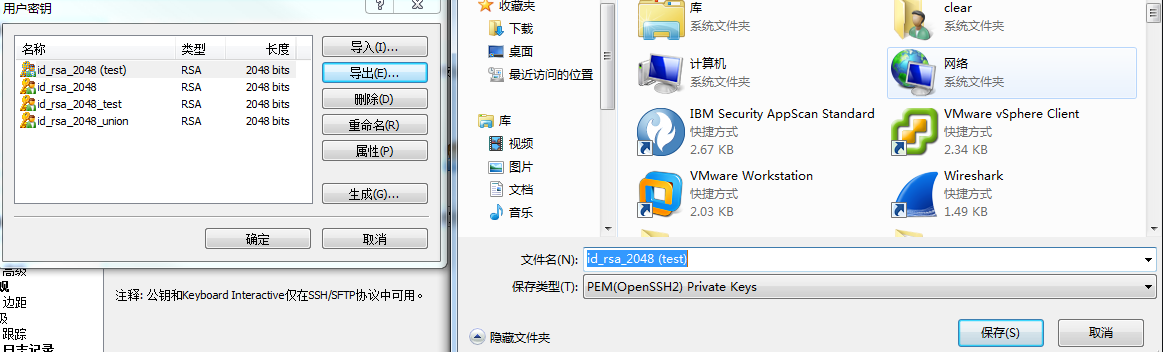
点击下一步输入用户密钥的名称和密码，密码可以留空，如下：



点下一步，提示在SSH服务器上注册公钥。点保存为文件，把刚产生的公钥文件保存下来。



点完成后，自动会在用户密钥的窗口，添加一个密钥（私钥），名称和公钥的一样。点导出：



点确定，结束密钥创建过程。

2.修改服务器认证方式。

使用密码登录上服务器，修改ssh的配置文件/etc/ssh/sshd\_config，主要修改前三项：

[root@localhost ~]# vim /etc/ssh/sshd\_config

|  |
| --- |
| PubkeyAuthentication yes  AuthorizedKeysFile /root/id\_rsa\_2048.pub  PasswordAuthentication no  UseDNS no |

点ESC，输入:wq保存退出。查看selinux状态，如果为enforcing使用setenforce 0修改

[root@localhost ~]# getenforce

[root@localhost ~]# setenforce 0 && service sshd restart

注：在linux下登录的话可以使用 ssh 192.168.1.1 -i /root/id\_rsa\_2048\*