基于密钥的认证

系统环境

```
OS:centos7
连接工具：xshell
IP:192.168.0.120
```

生成ssh认证的私钥和公钥

```
ssh-keygen
```

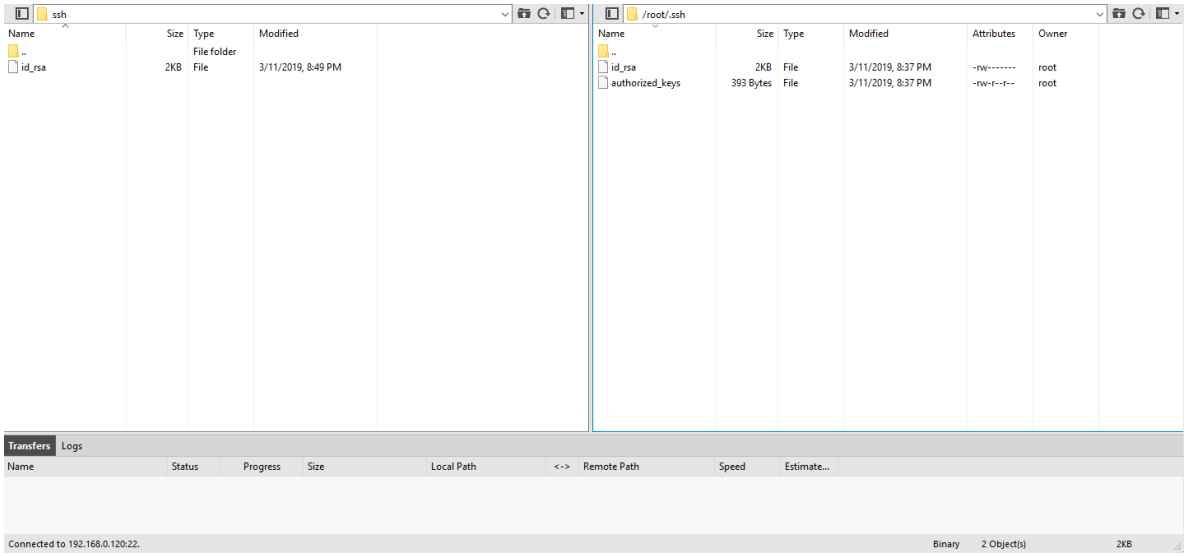
```
[root@Server /]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:yMv5o0LKmNOhDeEiU7+DzfHllsBqC58uYlOqp/R4cFI root@Server
The key's randomart image is:
+---[RSA 2048]----+
|                 |
|                 |
|                 |
|. .E . .         |
|.o..  o.S        |
|=+..=. o+        |
|o@+X.++o o .     |
|* #.Bo+o. +      |
|oB.+ **o.o       |
+----[SHA256]-----+
[root@Server /]#
```

将公钥制作成key

```
mv id_rsa.pub authorized_keys
```

```
[root@Server .ssh]# pwd
/root/.ssh
[root@Server .ssh]# ls
id_rsa  id_rsa.pub
[root@Server .ssh]# mv id_rsa.pub authorized_keys
[root@Server .ssh]# ls
authorized_keys  id_rsa
[root@Server .ssh]#
```

将私钥下载到本地



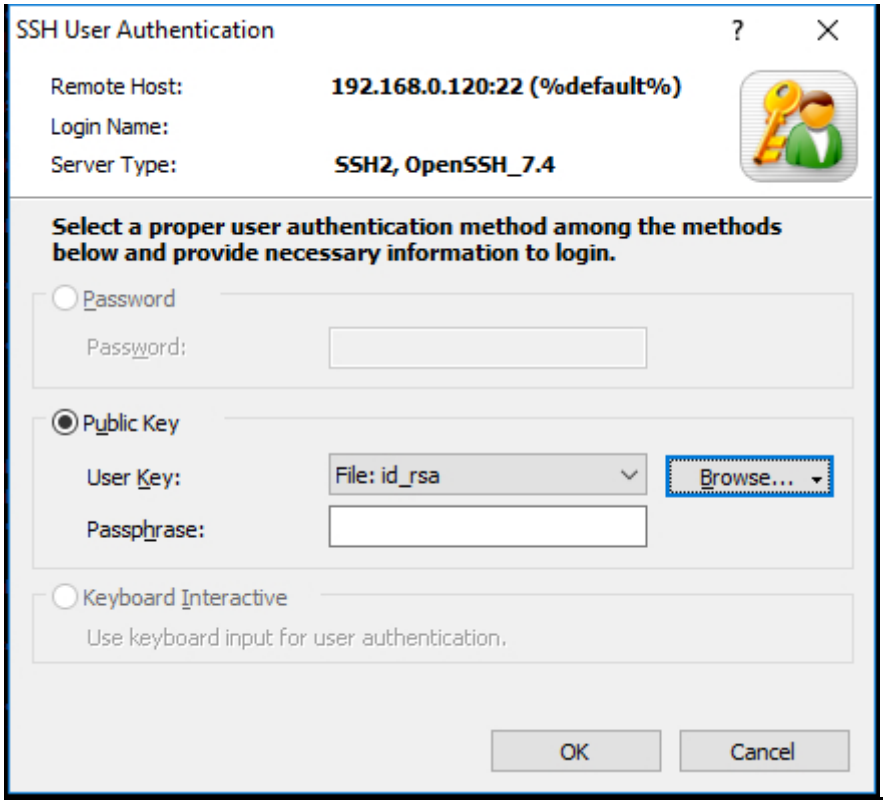
编辑配置文件允许公钥认证，关闭口令认证

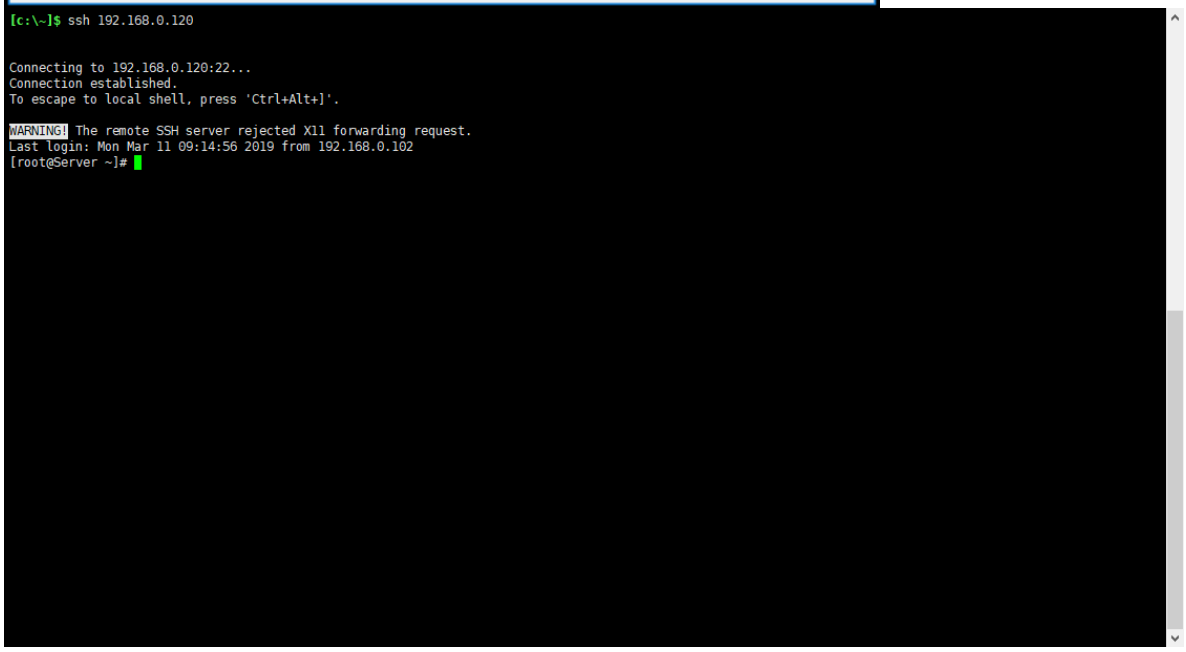
```
# Logging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
                        去掉注释
PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile      .ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no
                        关闭密码认证
PasswordAuthentication no

# Change to no to disable s/key passwords
-- INSERT --                                                    65,26         28%
```

重启ssh服务

```
service sshd restart
```

利用密钥进行连接


SSH User Authentication
Remote Host:
192.168.0.120:22 (%default%)
Login Name:
Server Type:
SSH2, OpenSSH_7.4
Select a proper user authentication method among the methods below and provide necessary information to login.
Password
Password:
Public Key
User Key:
File: id_rsa
Browse...
Passphrase:
Keyboard Interactive
Use keyboard input for user authentication.
OK
Cancel


[c:\~]$ ssh 192.168.0.120
Connecting to 192.168.0.120:22...
Connection established.
To escape to local shell, press 'Ctrl+Alt+]'.
WARNING! The remote SSH server rejected X11 forwarding request.
Last login: Mon Mar 11 09:14:56 2019 from 192.168.0.102
[root@Server ~]#