SSH公钥登录

公钥介绍

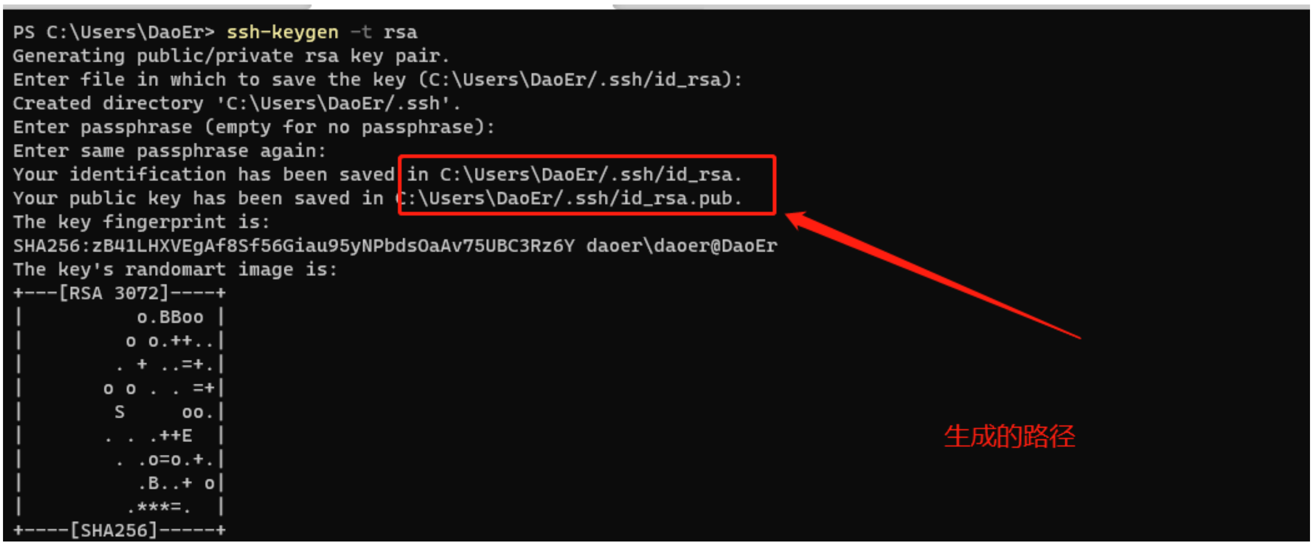
使用密码登录，每次都必须输入密码，非常麻烦。好在SSH还提供了公钥登录，可以省去输入密码的步骤。 所谓"公钥登录"，原理很简单，就是用户将自己的公钥储存在远程主机上。登录的时候，远程主机会向用户发送一段随机字符串，用户用自己的私钥加密后，再发回来。远程主机用事先储存的公钥进行解密，如果成功，就证明用户是可信的，直接允许登录shell，不再要求密码。

公钥维持

1、在需要登录服务器的机器上生成公钥和私钥，我使用的windows就用windos生成

```
ssh-keygen -t rsa
```

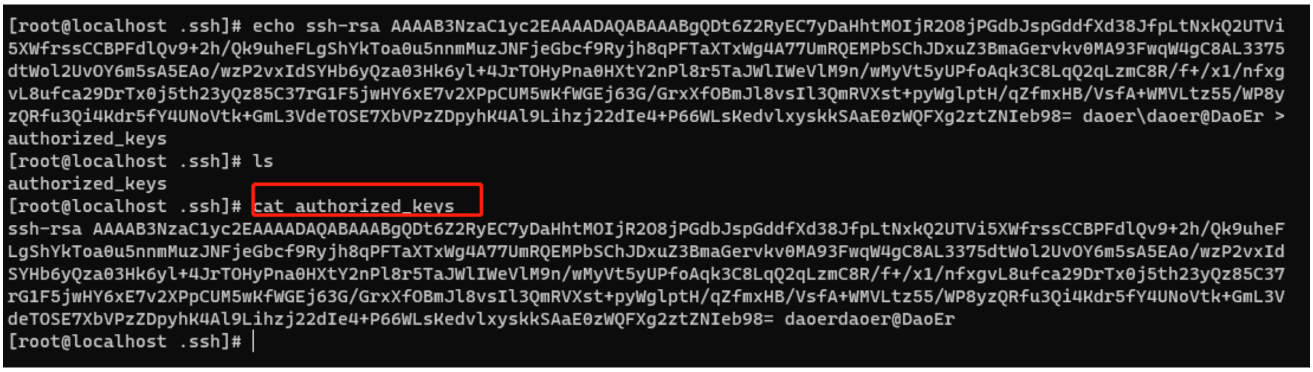
中间按3此回车



```
PS C:\Users\DaoEr> ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\DaoEr/.ssh/id_rsa):
Created directory 'C:\Users\DaoEr/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\DaoEr/.ssh/id_rsa.
Your public key has been saved in C:\Users\DaoEr/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:zB41LHXVEgAf8Sf56Giau95yNPbdsOaAv75UBC3Rz6Y daoer\daoer@DaoEr
The key's randomart image is:
+---[RSA 3072]----+
|          o.BBoo |
|         o o.++..|
|        . + ..=+.|
|       o o . . =+|
|        S     oo.|
|       . . .++E  |
|        . .o=o.+.|
|          .B..+ o|
|         .***=.  |
+----[SHA256]-----+
```

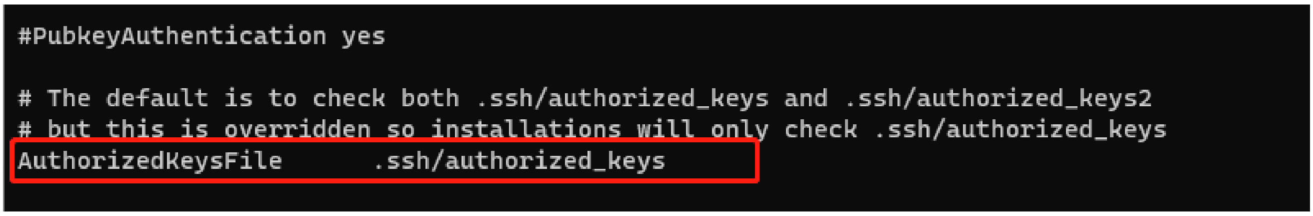
生成的路径

2、将生成的`id_rsa.pub`文件复制到服务器的`/root/.ssh/authorized_keys`文件中



```
[root@localhost .ssh]# echo ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDt6Z2RyEC7yDaHhtMOIjR2O8jPGdbJspGddfXd38JfpLtNxkQ2UTVi
5XWfrssCCBPFdlQv9+2h/Qk9uheFLgShYkToa0u5nnmMuzJNFjeGbcf9Ryjh8qPFTaXTxWg4A77UmRQEMPbSChJDxuZ3BmaGervkv0MA93FwqW4gC8AL3375
dtWol2UvOY6m5sA5EAo/wzP2vxIdSYHb6yQza03Hk6yl+4JrTOHyPna0HXtY2nPl8r5TaJWlIWeVlM9n/wMyVt5yUPfoAqk3C8LqQ2qLzmC8R/f+/x1/nfxg
vL8ufca29DrTx0j5th23yQz85C37rG1F5jwHY6xE7v2XPpCUM5wKfWGEj63G/GrxXfOBmJl8vsIl3QmRVXst+pyWglptH/qZfmxHB/VsfA+WMVLtz55/WP8y
zQRfu3Qi4Kdr5fY4UNoVtk+GmL3VdeTOSE7XbVPzZDpyhK4Al9Lihzj22dIe4+P66WLsKedvlxyskkSAaE0zWQFXg2ztZNIeb98= daoer\daoer@DaoEr >
authorized_keys
[root@localhost .ssh]# ls
authorized_keys
[root@localhost .ssh]# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDt6Z2RyEC7yDaHhtMOIjR2O8jPGdbJspGddfXd38JfpLtNxkQ2UTVi5XWfrssCCBPFdlQv9+2h/Qk9uheF
LgShYkToa0u5nnmMuzJNFjeGbcf9Ryjh8qPFTaXTxWg4A77UmRQEMPbSChJDxuZ3BmaGervkv0MA93FwqW4gC8AL3375dtWol2UvOY6m5sA5EAo/wzP2vxId
SYHb6yQza03Hk6yl+4JrTOHyPna0HXtY2nPl8r5TaJWlIWeVlM9n/wMyVt5yUPfoAqk3C8LqQ2qLzmC8R/f+/x1/nfxgvL8ufca29DrTx0j5th23yQz85C37
rG1F5jwHY6xE7v2XPpCUM5wKfWGEj63G/GrxXfOBmJl8vsIl3QmRVXst+pyWglptH/qZfmxHB/VsfA+WMVLtz55/WP8yzQRfu3Qi4Kdr5fY4UNoVtk+GmL3V
deTOSE7XbVPzZDpyhK4Al9Lihzj22dIe4+P66WLsKedvlxyskkSAaE0zWQFXg2ztZNIeb98= daoerdaoer@DaoEr
[root@localhost .ssh]# |
```

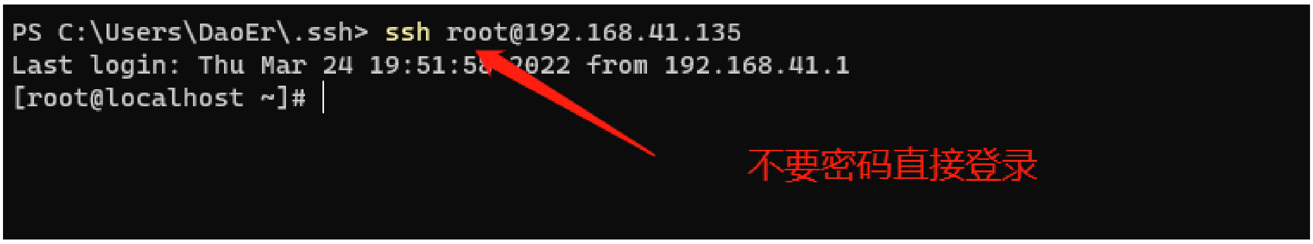
3、查看服务器中/etc/ssh/sshd_confg文件是否开启了公私钥登录`cat /etc/ssh/sshd_config`



```
#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
```

4、尝试登录



```
PS C:\Users\DaoEr\.ssh> ssh root@192.168.41.135
Last login: Thu Mar 24 19:51:58 2022 from 192.168.41.1
[root@localhost ~]# 
```

不要密码直接登录