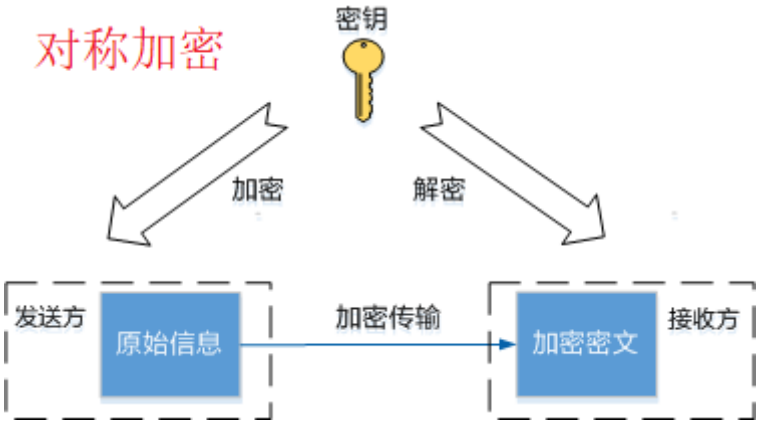
什么是SSH?

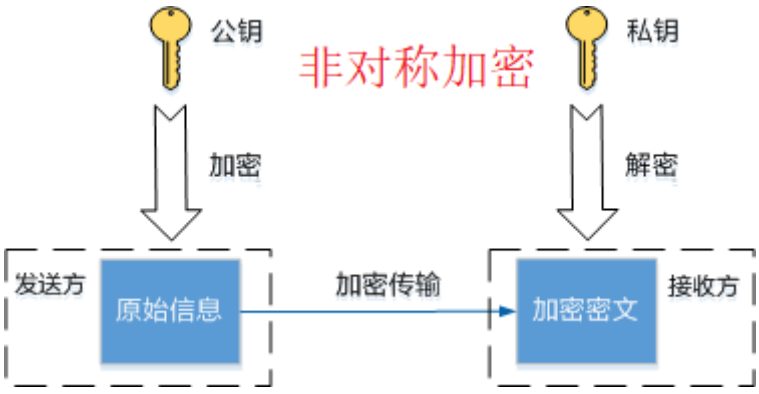
SSH（Secure Shell，安全外壳）是一种网络安全协议，通过加密和认证机制实现安全的访问和文件传输等业务。传统远程登录或文件传输方式，例如Telnet、FTP，使用明文传输数据，存在很多的安全隐患。随着人们对网络安全的重视，这些方式已经慢慢不被接受。SSH协议通过对网络数据进行加密和验证，在不安全的网络环境中提供了安全的登录和其他安全网络服务。作为Telnet和其他不安全远程shell协议的安全替代方案，目前SSH协议已经被全世界广泛使用，大多数设备都支持SSH功能。

SSH使用的默认SSH端口都是22，SSH端口支持修改，更改后当前所有的连接都会断开，SSH服务器开始侦听新的端口。

对称加密和非对称加密

提高安全性的基本方式就是加密，加密算法通过密钥将明文转换为密文进行安全传输。SSH在工作过程中结合使用了对称加密和非对称加密两种类型的算法，通过事先生成的SSH密钥来保证信息传输的安全性。





对称加密算法使用同一个密钥对数据进行加密和解密。SSH连接建立过程中生成的会话密钥就是对称密钥，该对称密钥是由客户端和服务器端基于共享的部分信息和各自的私有数据使用密钥交换算法分别生成的。因为对称加密算法加解密的速度很快，所以适用于传输大量数据的场景。

非对称加密的发送和接收需要使用一对关联的SSH密钥，公钥和私钥。私钥由生成的一方自己保管，公钥可以发送给任何请求通信的其他人。发送方用收到的公钥对自己的通信内容进行加密，只有接收方可以使用私钥进行解密获取通信内容。非对称加密的私钥不需要暴露在网络中，安全性大大增加，但是加解密的速度比对称密钥慢得多。

公众号：黑猫编程
网址：https://noi.hioier.com

SSH连接过程中的两个阶段使用了非对称加密。一个是在密钥交换阶段，服务器和客户端都生成了自己临时的公钥和私钥，用于计算出同一个用于后续加密通信内容的会话密钥。另外一个就是在用户认证阶段，利用只有匹配的私钥可以唯一解密公钥加密的内容这一特点，通过客户端的公钥私钥对验证客户端的身份。

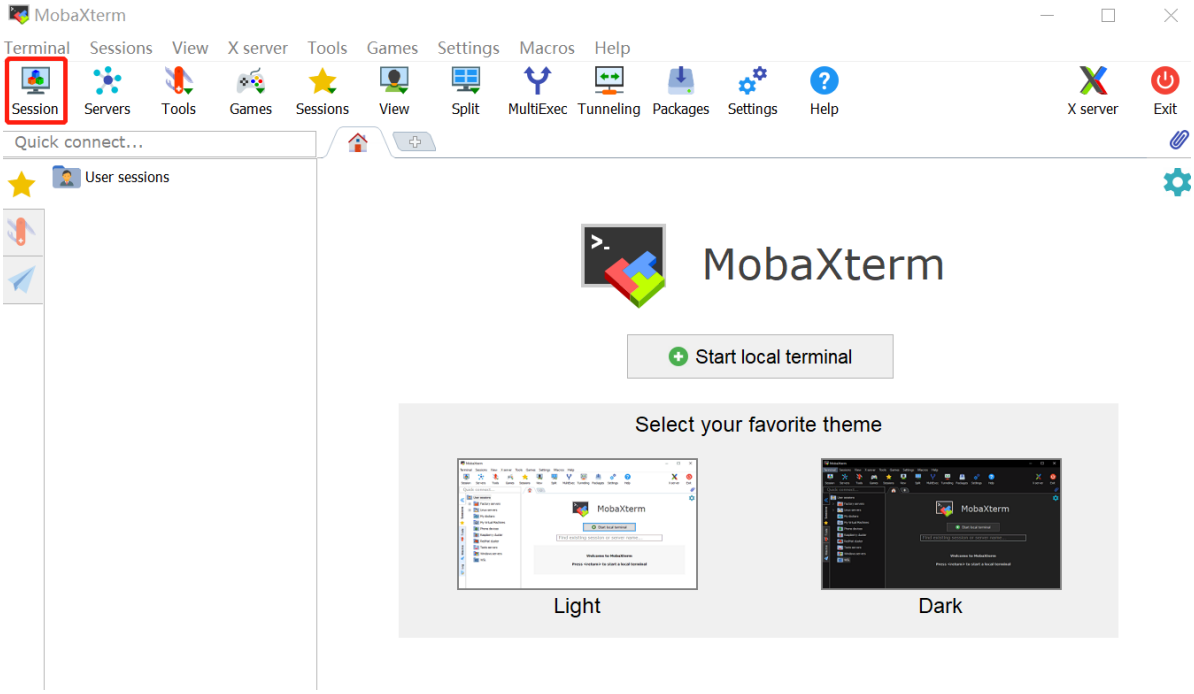
WIndows平台SSH工具

SSH工具非常之多，比如Putty、XShell、SecureCRT等等，本节我们使用Mobaxterm，其他工具使用过程也基本类似。

下载链接

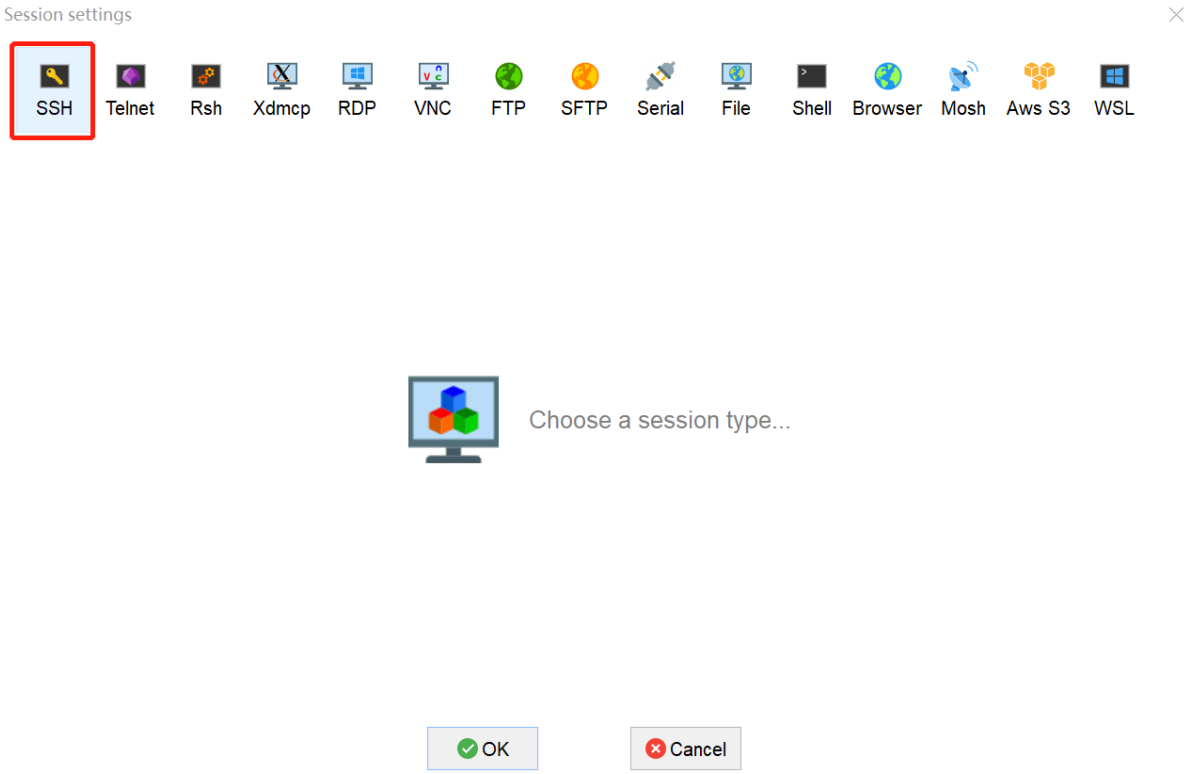
双击打开exe文件

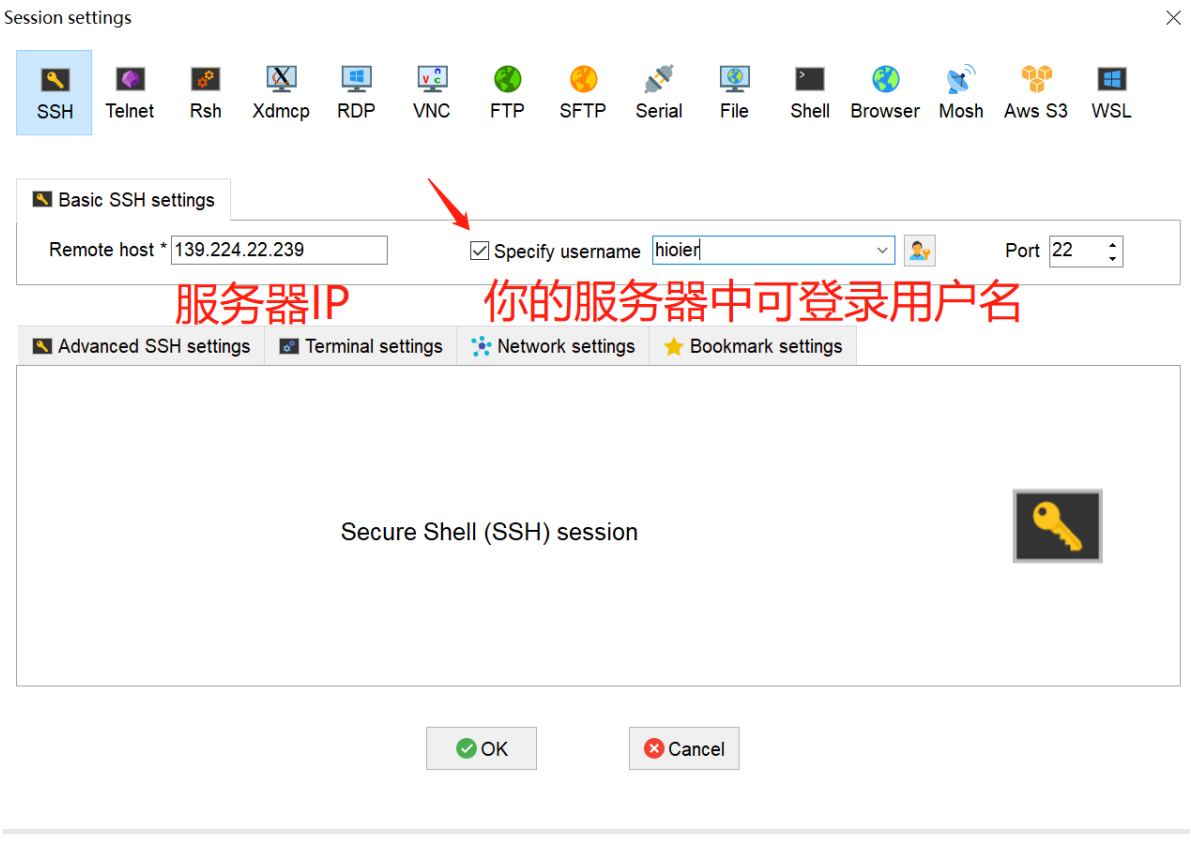
点击Session



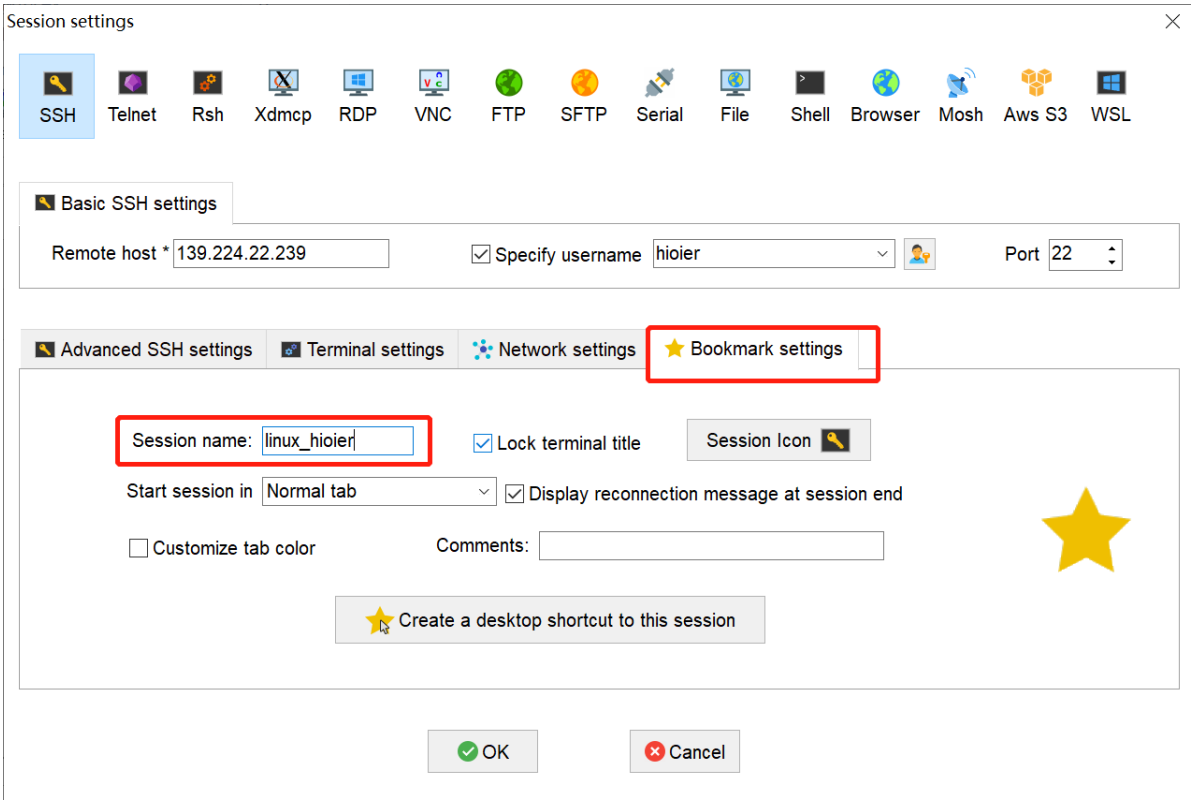
点击SSH

公众号：黑猫编程
网址：https://noi.hioier.com

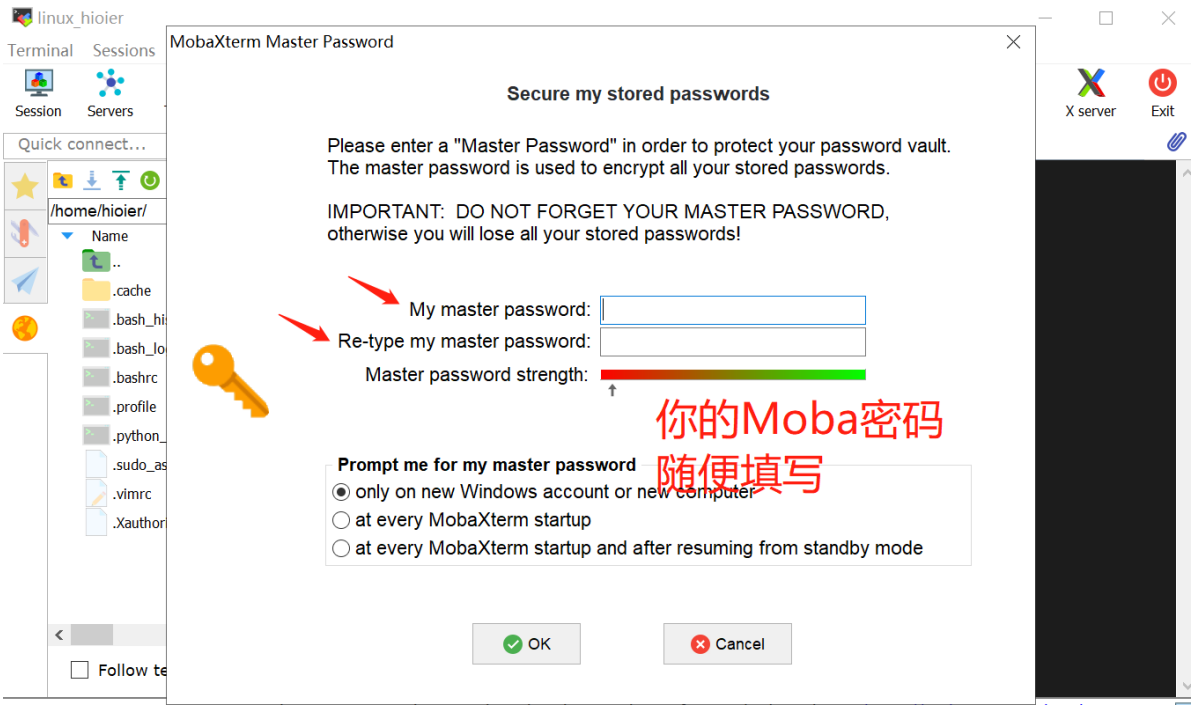




公众号：黑猫编程
网址：https://noi.hioier.com



设置你的Moba密码



Linux配置SSH

首先确保服务器和当前Linux系统安装ssh服务并启动

```
sudo apt install ssh
sudo systemctl status ssh
```

公众号：黑猫编程
网址：https://noi.hioier.com

```
hioier@pc:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: >
     Active: active (running) since Tue 2022-12-06 10:16:36 CST; 38min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 851 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 879 (sshd)
      Tasks: 1 (limit: 2244)
     Memory: 2.2M
     CGroup: /system.slice/ssh.service
             └─879 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

12月 06 10:16:36 pc systemd[1]: Starting OpenBSD Secure Shell server...
12月 06 10:16:36 pc sshd[879]: Server listening on 0.0.0.0 port 22.
12月 06 10:16:36 pc sshd[879]: Server listening on :: port 22.
12月 06 10:16:36 pc systemd[1]: Started OpenBSD Secure Shell server.
lines 1-16/16 (END)
```

远程连接服务器

```
ssh user@hostname
ssh hioier@139.224.22.239
```

```
hioier@pc:~$ ssh hioier@139.224.22.239
The authenticity of host '139.224.22.239 (139.224.22.239)' can't be established
.
ECDSA key fingerprint is SHA256:5zi2+Sef7a+MoeRG4O7WibpYCI9AA/1wnzERbPlzeCo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '139.224.22.239' (ECDSA) to the list of known hosts.
hioier@139.224.22.239's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-125-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
New release '22.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Welcome to Alibaba Cloud Elastic Compute Service !

Last login: Tue Dec  6 10:50:00 2022 from 58.39.4.19
```

第一次登录时会提示：

```
The authenticity of host '123.57.47.211 (123.57.47.211)' can't be
established.
ECDSA key fingerprint is SHA256:iy237yysfCeO13/l+kpDGfEG9xxHxmOdnxnAbJTPpG8.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

输入yes，然后回车即可。
这样会将该服务器的信息记录在~/.ssh/known_hosts文件中。

之后再次登录只需要输入服务器密码。

公众号：黑猫编程
网址：https://noi.hioier.com

给登录账号起别名

每次连接远程服务器，都需要填写`user@hostname`，不容易记忆，可以给这个信息起一个别名。

创建文件`~/.ssh/config`。

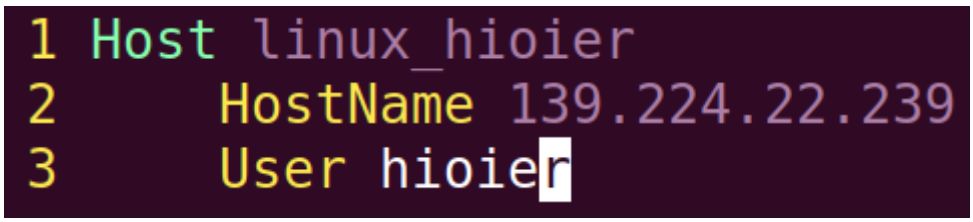
然后在文件中输入：

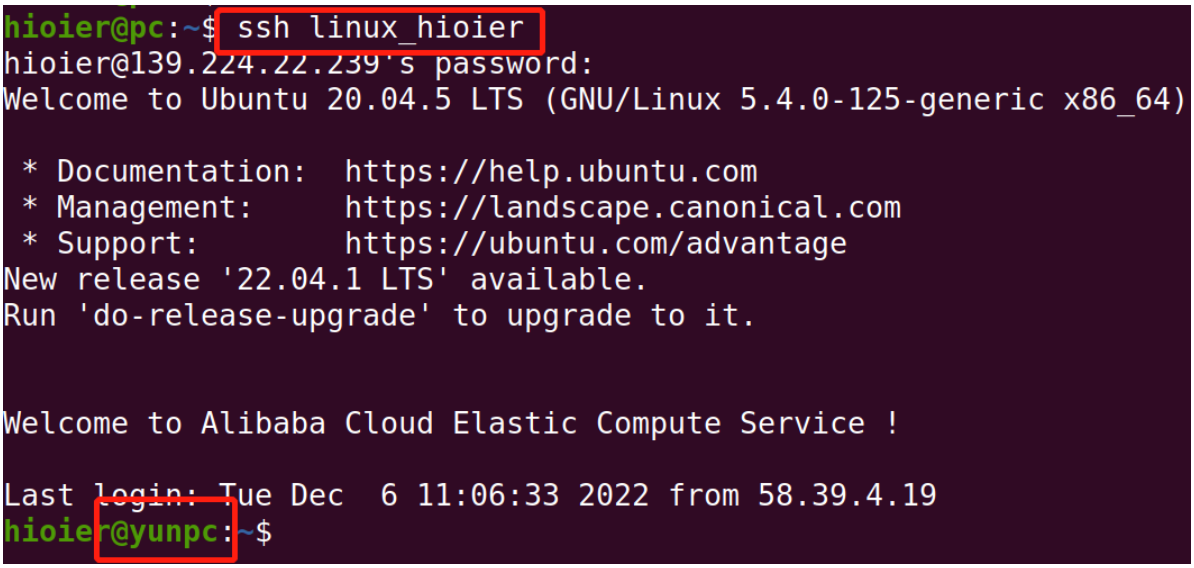
```
Host myserver1
    HostName IP地址或域名
    User 用户名

Host myserver2
    HostName IP地址或域名
    User 用户名
```

之后再使用服务器时，可以直接使用别名myserver1、myserver2。

例如：





密钥登录

进一步地，如果不想 每次输入密码，免密登录，可以创建密钥：

```
ssh-keygen
```

公众号：黑猫编程
网址：https://noi.hioier.com

```
hioier@pc:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/hioier/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/hioier/.ssh/id_rsa
Your public key has been saved in /home/hioier/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:DvY48LTpd7h9fs2nXo+yfAX/ptJ9T+mkiBCuh57A1As hioier@pc
The key's randomart image is:
+---[RSA 3072]----+
|                 |
|                 |
|                 |
|    .        .   |
|   E..+.S      o |
|  o .=oB.       +|
|   o .Boo.    . B+|
|    .ooo+.o.= B+X|
|    .+o..+.++O==*|
+----[SHA256]-----+
```

然后一直回车即可。

执行结束后，~/.ssh/目录下会多两个文件：

id_rsa：私钥
id_rsa.pub：公钥

在服务器添加公钥

```
1 ssh-copy-id myserver
2 ssh-copy-id linux_hioier
```

公钥内容会写入到服务器`~/.ssh/authorized_keys`

```
hioier@pc:~$ ssh-copy-id linux_hioier
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
 out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are promp
ted now it is to install the new keys
hioier@139.224.22.239's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'linux_hioier'"
and check to make sure that only the key(s) you wanted were added.
```

客户端

```
hioier@yunpc:~$ cat ~/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDZH+puNvkf7gtEE1rjvn+yBZ9Ivl8S6Hl/Dd6QdVU
sv2gsiUB4Ue6PXzyBMcplg7HIV1sqF4fvMnueA6URD59RsLe13JNjmYScF21Q4dhfCFtDCiXguqvNOf
9RyX40fc8KBAxKpO2Q/MMsRfkCSBZHjMAMfayh1S0xmg9e73YxJoYHtA6gdJP39r2lH4WrO0hTB0JEj
O2ebnOwj8AMbAUqD/kl9n3qE9fFKGUYOJNx8tuUOA3jSXdarncf3rvX5CZVlQGQx1PYEIdurs1JLPf+
F6ESX+P3Qi/xuD3BIja8cKMzwURRUS6oO9Q+hBQKVnhY79otatfEZrGhY/p/oVXu1oVK9TM2xty8Ue6
rhrEmM8fOpQrFWOr+dh+wXxZRxOy8oN2hxhTj314+mdRU9+vI0g1MoVpgBcsAeWLsM87w2sYS/qjbxj
gFZStXsTplbTPFG30oaolpBhENUMhh4I80vD3p72qBINX4UE0XDMbt35K6KLMkHW65IN+7yUt/EDc=
hioier@pc
```

服务器

公众号：黑猫编程
网址：https://noi.hioier.com

文件传输

将source路径下的文件复制到destination中

```
scp source destination
```

一次复制多个文件

```
scp source1 source2 destination
```

复制文件夹到服务器

```
scp -r AA/ linux_hioier:
```

```
hioier@pc:~$ mkdir AA
hioier@pc:~$ touch AA/1.txt AA/2.txt
hioier@pc:~$ ls AA/
1.txt  2.txt
hioier@pc:~$ scp -r AA/ linux_hioier:
1.txt                                         100%    0     0.0KB/s   00:00
2.txt                                         100%    0     0.0KB/s   00:00
```

从服务器复制文件到本地

```
scp -r linux_hioier:AA/ .
```

公众号：黑猫编程
网址：https://noi.hioier.com