

SSH 环境搭建

安装

- [安装 SSH 客户端](#)
- [安装 SSH 服务端](#)
- [ssh-keygen 生成密钥对](#)
 - [生成密钥对](#)
 - [指定密钥对名称](#)
- [安装 SSH 服务端](#)
- [ssh-copy-id 复制公钥到远程主机](#)
- [ssh-agent 管理密钥对](#) [ssh-add 添加密钥对](#)
 - [使用 ssh-agent](#)
 - [ssh-add 添加密钥对](#)
- [配置 SSH 配置文件](#)

SSH

SSH 是一种安全的网络传输协议，用于在计算机之间进行安全通信。它通过加密和认证来确保数据的安全性和完整性。

密钥对

SSH 使用公钥加密技术，需要生成一对密钥：公钥（public key）和私钥（private key）。公钥用于加密数据，而私钥用于解密数据。只有拥有私钥的人才能解密用公钥加密的数据。

SSH

SSH 是一种安全的网络传输协议，用于在计算机之间进行安全通信。它通过加密和认证来确保数据的安全性和完整性。

SSH 是一种安全的网络传输协议，用于在计算机之间进行安全通信。它通过加密和认证来确保数据的安全性和完整性。

████████

SSH ██████████

████████ ssh-keygen ██████████

██

████████████████ SSH ██████

████████████████ SSH ███

██

██

██████

ssh-keygen ██████████

██████

██ OpenSSH ██████████ ssh-keygen ██████████

██████ ssh-keygen ███

```
$ ssh-keygen
```

████████ -t ██████████

```
$ ssh-keygen -t dsa
```

████████ -t ███ DSA ███ RSA
██ RSA ███

████████████████ ssh-keygen ██████████

```
$ ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/username/.ssh/id_dsa): press ENTER
Enter passphrase (empty for no passphrase): *****
```

```
Enter same passphrase again: *****

Your identification has been saved in /home/username/.ssh/id_dsa.
Your public key has been saved in /home/username/.ssh/id_dsa.pub.
The key fingerprint is:
14:ba:06:98:a8:98:ad:27:b5:ce:55:85:ec:64:37:19 username@shell.isp.com
```

```
Enter same passphrase again: *****

Your identification has been saved in /home/username/.ssh/id_dsa.
Your public key has been saved in /home/username/.ssh/id_dsa.pub.
The key fingerprint is:
14:ba:06:98:a8:98:ad:27:b5:ce:55:85:ec:64:37:19 username@shell.isp.com
```

```
Enter same passphrase again: *****

Your identification has been saved in /home/username/.ssh/id_dsa.
Your public key has been saved in /home/username/.ssh/id_dsa.pub.
The key fingerprint is:
14:ba:06:98:a8:98:ad:27:b5:ce:55:85:ec:64:37:19 username@shell.isp.com
```

```
Enter same passphrase again: *****

Your identification has been saved in /home/username/.ssh/id_dsa.
Your public key has been saved in /home/username/.ssh/id_dsa.pub.
The key fingerprint is:
14:ba:06:98:a8:98:ad:27:b5:ce:55:85:ec:64:37:19 username@shell.isp.com
```

```
Enter same passphrase again: *****

Your identification has been saved in /home/username/.ssh/id_dsa.
Your public key has been saved in /home/username/.ssh/id_dsa.pub.
The key fingerprint is:
14:ba:06:98:a8:98:ad:27:b5:ce:55:85:ec:64:37:19 username@shell.isp.com
```

Diagram illustrating the generation of SSH keys using the `ssh-keygen` command. The command is entered in a terminal, and the resulting files, `~/.ssh/id_dsa` and `~/.ssh/id_dsa.pub`, are shown.

[illegible]

passphrase

passphrase

Linux

password

" " "

[illegible]

```
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAvpB4lUbAaEbh9u6HLig7amsfywD4fqSZq2ikACIUbn3GyRPfeF93l/
weQh702ofXbDydZAKMcDvBJqRhUotQUwqV6HJxqoqPDlPGUyo8RDIkLUIPRyq
ypZxmK9aCXokFiHoGCXfQ9imUP/w/jfb9ByDtG97tUJF6nFMP5WzhM= username@shell.isp.com
```

Diagram illustrating the structure of a shell command line. The command line is shown as a sequence of tokens: a box containing 'username@shell.isp.com', followed by a box containing 'username', and then a box containing 'shell.isp.com'. Below the main command line, the components are further broken down: 'username' is shown in a box, and 'shell.isp.com' is shown in a box, with the '@' symbol separating them.

[illegible]

```
$ ls -l ~/.ssh/id_*.pub
```

```
$ chmod 600 ~/.ssh/id_rsa
$ chmod 600 ~/.ssh/id_rsa.pub
```

[illegible]

ssh-keygen

1 -b

-b

1024 2048

2 -c

-C username@host

4096 RSA

```
$ ssh-keygen -t rsa -b 4096 -C "your_email@domain.com"
```

3 -f

-f

```
$ ssh-keygen -t dsa -f mykey
```

mykey mykey.pub

4 -F

-F known_hosts

```
$ ssh-keygen -F example.com
```

5 -N

-N passphrase

```
$ ssh-keygen -t dsa -N secretword
```

6 -p

-p passphrase -N ssh

7 -R

-R known_hosts

```
$ ssh-keygen -R example.com
```

8 -t

-t

dsa rsa

OpenSSH

~/.ssh/authorized_keys

~/.ssh/authorized_keys

```
$ cat ~/.ssh/id_rsa.pub | ssh user@host "mkdir -p ~/.ssh && cat >> ~/.ssh/authorized_keys"
```

user@host

authorized_keys

644

SSH

```
$ chmod 644 ~/.ssh/authorized_keys
```

OpenSSH

```
$ ssh -l username shell.isp.com
Enter passphrase for key '/home/you/.ssh/id_dsa': *****
Last login: Mon Mar 24 02:17:27 2014 from ex.ample.com
shell.isp.com>
```

SSH

passphrase

ssh-copy-id

OpenSSH

ssh-copy-id

~/.ssh/authorized_keys

~/.ssh/authorized_keys

ssh-copy-id

```
$ ssh-copy-id -i key_file user@host
```

```
##### -i ##### user ##### host
#####
##### .pub ##### ssh-copy-id ##### ~/.ssh #####
```

```
$ ssh-copy-id -i id_rsa user@host
```

```
##### ~/.ssh/id_rsa.pub 
ssh-copy-id #####
##### ssh-copy-id ##### authorized_keys ##### authorized_keys
#####
##### authorized_keys ##### ssh-copy-id ##### authorized_keys
#####
```

ssh-agent ssh-add

```
#####
```

```
##### scp
#####
ssh-agent ##### Bash    session
##### SSH
#####
#####
```

```
$ ssh-agent bash
```

```
##### Bash ##### Shell ##### zsh   fish
##### ssh-agent #####
```

```
$ eval `ssh-agent`
```

```
##### ssh-agent #####
```

```
$ ssh-agent
SSH_AUTH_SOCK=/tmp/ssh-barrett/ssh-22841-agent; export SSH_AUTH_SOCK;
SSH_AGENT_PID=22842; export SSH_AGENT_PID;
echo Agent pid 22842;
```

```
eval [REDACTED]
```

```
ssh-agent [REDACTED]
```

```
[REDACTED]
```

```
Shell [REDACTED]
```

```
ssh-add [REDACTED]
```

```
~/.ssh/id_rsa [REDACTED]
```

```
~/.ssh/id_dsa [REDACTED]
```

```
~/.ssh/id_ecdsa [REDACTED]
```

```
~/.ssh/id_ed25519 [REDACTED]
```

```
$ ssh-add
Enter passphrase for /home/you/.ssh/id_dsa: *****
Identity added: /home/you/.ssh/id_dsa (/home/you/.ssh/id_dsa)
```

```
[REDACTED]
```

```
[REDACTED]
```

```
[REDACTED]
```

```
ssh-add [REDACTED]
```

```
$ ssh-add my-other-key-file
```

```
[REDACTED]
```

```
my-other-key-file [REDACTED]
```

```
[REDACTED]
```

```
ssh [REDACTED]
```

```
$ ssh remoteHost
```

```
[REDACTED]
```

```
remoteHost [REDACTED]
```

```
ssh [REDACTED]
```

```
ssh
```

```
[REDACTED]
```

```
[REDACTED]
```

```
ssh [REDACTED]
```

```
-i [REDACTED]
```

```
$ ssh -i OpenSSHPrivateKey remoteHost
```

```
[REDACTED]
```

```
ssh-agent [REDACTED]
```

```
Shell [REDACTED]
```

```
Ctrl + d [REDACTED]
```

```
$ ssh-agent -k
```

ssh-add [REDACTED]

```
ssh-add [REDACTED]
```

```
ssh-agent [REDACTED]
```

1 -d

-d

```
$ ssh-add -d name-of-key-file
```

2 -D

-D

```
$ ssh-add -D
```

3 -l

-l

```
$ ssh-add -l
```

OpenSSH sshd /etc/ssh/sshd_config PasswordAuthentication no

```
PasswordAuthentication no
```

sshd

- #2
- cocobook-sync 2026-10-28 10:51:02 UTC
- cocobook-sync 2026-10-28 11:29:02 UTC