

SSH 快速参考

连接、密钥、配置、隧道、SCP 与 SFTP

连接

基本连接

```
ssh user@host # connect to host
ssh -p 2222 user@host # custom port
ssh user@host command # run remote command
ssh -t user@host "top" # force TTY allocation
```

连接标志

```
-p port 连接到指定端口
-i key 使用指定身份 (私钥)
-t 强制分配伪终端
-v / -vv / -vvv 详细调试 (逐级增加)
-q 静默模式 (抑制警告)
-N 不执行远程命令 (用于隧道)
-f 命令前转入后台
-J jump 跳板主机 (ProxyJump)
```

密钥管理

生成密钥

```
ssh-keygen -t ed25519 -C "you@example.com"
ssh-keygen -t rsa -b 4096 -C "you@example.com"
ssh-keygen -t ed25519 -f ~/.ssh/mykey
ssh-keygen -p -f ~/.ssh/id_ed25519 # change passphrase
```

部署公钥

```
ssh-copy-id user@host
ssh-copy-id -i ~/.ssh/mykey.pub user@host
# Manual: append .pub to remote authorized_keys
cat ~/.ssh/id_ed25519.pub | ssh user@host \
"mkdir -p ~/.ssh && cat >> ~/.ssh/authorized_keys"
```

密钥文件

```
~/.ssh/id_ed25519 私钥 (保密)
~/.ssh/id_ed25519.pub 公钥 (可自由分享)
~/.ssh/authorized_keys 远程: 已授权的公钥
~/.ssh/known_hosts 已知主机指纹
```

配置文件

~/.ssh/config 基础

```
Host myserver
  HostName 192.168.1.100
  User deploy
  Port 2222
  IdentityFile ~/.ssh/deploy_key

# Then connect with just:
# ssh myserver
```

实用配置选项

```
Host *
  ServerAliveInterval 60
  ServerAliveCountMax 3
  AddKeysToAgent yes
  IdentitiesOnly yes

Host bastion
  HostName bastion.example.com
  User admin
```

配置指令

```
Host 条目的别名模式
HostName 实际主机名或IP
User 登录用户名
Port 远程端口 (默认 22)
IdentityFile 私钥路径
ProxyJump 经由另一主机跳转
ServerAliveInterval 保活间隔 (秒)
IdentitiesOnly 仅使用指定的密钥
```

端口转发

本地转发 (-L)

```
# Access remote port 5432 via local port 5432
ssh -L 5432:localhost:5432 user@host
# Access remote-db:3306 through ssh host
ssh -L 3306:remote-db:3306 user@host
# Bind to all interfaces
ssh -L 0.0.0.0:8080:localhost:80 user@host
```

远程转发 (-R)

```
# Expose local port 3000 on remote port 8080
ssh -R 8080:localhost:3000 user@host
# Allow remote connections from any interface
ssh -R 0.0.0.0:8080:localhost:3000 user@host
```

动态转发 (-D)

```
# SOCKS5 proxy on local port 1080
ssh -D 1080 user@host
# Background SOCKS proxy
ssh -D 1080 -fN user@host
```

SCP 与 SFTP

SCP (安全复制)

```
scp file.txt user@host:/remote/path/
scp user@host:/remote/file.txt ./local/
scp -r dir/ user@host:/remote/path/
scp -P 2222 file.txt user@host:/path/
```

SFTP (交互式传输)

```
sftp user@host
# Inside sftp session:
# put local.txt - upload file
# get remote.txt - download file
# ls / lcd / cd - list / change directory
```

传输标志

```
-r 递归 (复制目录)
-P port 指定端口 (SCP 用 -P, 非 -p)
-C 启用压缩
-l limit 带宽限制 (Kbit/s)
-i key 使用指定身份文件
```

Agent 转发

SSH Agent

```
eval "$(ssh-agent -s)" # start agent
ssh-add ~/.ssh/id_ed25519 # add key to agent
ssh-add -l # list loaded keys
ssh-add -D # remove all keys
```

转发 Agent

```
ssh -A user@host # forward agent
# Or in ~/.ssh/config:
# Host myserver
# ForwardAgent yes
```

Agent 说明

Agent forwarding lets the remote host use your local keys without copying them. Use only with trusted hosts. Prefer ProxyJump over agent forwarding when possible.

隧道

持久隧道

```
# Background tunnel that stays open
ssh -fNT -L 5432:localhost:5432 user@host
# Auto-reconnecting tunnel (with autossh)
autossh -M 0 -fNT -L 5432:localhost:5432 user@host
```

跳板机 / 堡垒机

```
ssh -J bastion user@internal-host
ssh -J user1@hop1,user2@hop2 user@target
# Config equivalent:
# Host internal
# HostName 10.0.0.5
# ProxyJump bastion
```

隧道管理

```
-f 认证后转入后台
-N 不执行远程命令
-T 禁用伪终端
~. 断开卡住的 SSH 会话 (转义序列)
~C 打开命令行用于添加转发
~# 列出已转发的连接
```

故障排查

调试连接

```
ssh -vvv user@host # max verbosity
ssh -G user@host # dump config (dry run)
ssh-keyscan host # fetch host keys
ssh-keygen -R host # remove from known_hosts
```

常见问题

Permission denied 密钥、用户或 ~/.ssh 权限错误 (700/600)
Host key changed 执行 ssh-keygen -R host, 然后重新连接
Connection timed out 检查防火墙、端口和主机可达性
Too many auth failures 用 -i 指定密钥或设置 IdentitiesOnly
Broken pipe 在配置中添加 ServerAliveInterval

文件权限

```
chmod 700 ~/.ssh
chmod 600 ~/.ssh/id_ed25519 # private key
chmod 644 ~/.ssh/id_ed25519.pub # public key
chmod 600 ~/.ssh/authorized_keys
chmod 644 ~/.ssh/known_hosts
```

SSH 快速参考

安全最佳实践

服务器加固

| | |
|----------------------------------|-------------------|
| PasswordAuthentication no | 禁用密码登录 |
| PermitRootLogin no | 禁止 root 通过 SSH 登录 |
| AllowUsers deploy | 白名单允许的用户 |
| Port 2222 | 非默认端口 (规避扫描) |
| MaxAuthTries 3 | 限制认证尝试次数 |

密钥实践

Prefer Ed25519 keys (smaller, faster, more secure).
Always set a passphrase on private keys.
Use ssh-agent to avoid retying passphrases.
Rotate keys periodically; revoke unused keys.
Use IdentitiesOnly to control which key is offered.

连接复用

连接共享

```
# In ~/.ssh/config
Host *
  ControlMaster auto
  ControlPath ~/.ssh/sockets/%r@%h-%p
  ControlPersist 600

# Create socket directory
mkdir -p ~/.ssh/sockets
```

连接复用优势

Reuses a single TCP connection for multiple SSH sessions to the same host. Eliminates repeated handshakes — faster connects and lower overhead.
ControlPersist keeps the master alive (seconds).

转义序列

SSH 转义命令

| | |
|---------------|-------------------|
| ~. | 终止连接 (断开卡住的会话) |
| ~^Z | 挂起 SSH 会话 |
| ~C | 打开命令行 (添加转发) |
| ~# | 列出已转发的连接 |
| ~& | 将 SSH 转入后台 (等待连接) |
| ~? | 显示转义帮助 |
| ~~ | 发送字面量波浪号 |