Tham Khảo Nhanh SSH

Kết nối, khóa, cấu hình, tunnel, SCP, SFTP

Kết nối

Kết nối cơ bản

```
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
```

Cờ kết nối

-p port	Kết nối tới cổng cụ thể
-i key	Dùng identity cụ thể (private key)
-t	Bắt buộc phân bổ pseudo-terminal
-v / -vv / -vvv	Debug chi tiết (mức độ tăng dần)
-q	Chế độ yên lặng (ẩn cảnh báo)
-N	Không chạy lệnh từ xa (dùng cho tunnel)
-f	Chạy nền trước khi thực thi lệnh
-J jump	Jump host (ProxyJump)

Quản lý khóa

Tạo khóa

```
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
```

Triển khai Public Key

```
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"
```

Các file khóa

~/.ssh/id_ed25519	Private key (giữ bí mật)
~/.ssh/id_ed25519.pub	Public key (chia sẻ thoải mái)
~/.ssh/authorized_keys	Remote: các public key được chấp nhận
~/.ssh/known_hosts	Fingerprints host đã biết

File cấu hình

Cơ bản về ~/.ssh/config

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

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

Tùy chọn Config hữu ích

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

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

Chỉ thị Config

Host	Mẫu alias cho mục này
HostName	Hostname thực tế hoặc IP
User	Tên đăng nhập
Port	Cổng từ xa (mặc định 22)
IdentityFile	Đường dẫn tới private key
ProxyJump	Nhảy qua host khác
ServerAliveInterval	Khoảng keep-alive (giây)
IdentitiesOnly	Chỉ dùng các khóa đã chỉ định

Chuyển tiếp cổng

Chuyển tiếp cục bộ (-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
```

Chuyển tiếp từ xa (-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
```

Chuyển tiếp động (-D)

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

SCP & SFTP

SCP (Secure Copy)

```
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 (Chuyển file tương tác)

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

Cờ chuyển file

-r	Đệ quy (sao chép thư mục)
-P port	Chỉ định cổng (SCP dùng -P, không phải -p)
-C	Bật nén
-l limit	Giới hạn băng thông tính bằng Kbit/s
-i key	Dùng file identity cụ thể

Agent Forwarding

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
```

Chuyển tiếp Agent

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

Lưu ý về Agent

> 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.

Tunnels

Tunnel bền vững

```
# 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
```

Jump Hosts / Bastion

```
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
```

Quản lý Tunnel

-f	Chạy nền sau xác thực
-N	Không có lệnh từ xa
-T	Tắt pseudo-terminal
~.	Kết thúc phiên SSH bị treo (escape)
~C	Mở command line để chuyển tiếp
~#	Liệt kê các kết nối đã chuyển tiếp

Khắc phục sự cố

Debug kết nối

```
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
```

Các vấn đề thường gặp

Permission denied	Sai khóa, user, hoặc quyền ~/.ssh (700/600)
Host key changed	Chạy ssh-keygen -R host rồi kết nối lại
Connection timed out	Kiểm tra firewall, cổng, và khả năng tiếp cận host
Too many auth failures	Dùng -i để chỉ định khóa hoặc IdentitiesOnly
Broken pipe	Thêm ServerAliveInterval vào config

Quyền file

```
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
```

Thực hành bảo mật tốt nhất

Tăng cường Server

PasswordAuthentication no	Tắt đăng nhập bằng mật khẩu
PermitRootLogin no	Tắt SSH root
AllowUsers deploy	Danh sách trắng người dùng được phép
Port 2222	Cổng không mặc định (tránh scanner)
MaxAuthTries 3	Giới hạn số lần xác thực

Tham Khảo Nhanh SSH

Thực hành về khóa

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

Multiplexing

Chia sẻ kết nối

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

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

Lợi ích của Multiplexing

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).

Escape Sequences

Lệnh Escape SSH

~.	Kết thúc kết nối (kết thúc phiên bị treo)
~^Z	Tạm dừng phiên SSH
~C	Mở command line (thêm chuyển tiếp)
~#	Liệt kê các kết nối đã chuyển tiếp
~&	Chạy nền SSH (đợi kết nối)
~?	Hiển thị trợ giúp escape
~~	Gửi ký tự tilde thực