REFERÊNCIA RÁPIDA DE SSH

Conexões, chaves, configuração, túneis, SCP, SFTP

Conexão

Conexão Básica

```
ssh user@host                  # conectar ao host
ssh -p 2222 user@host          # porta personalizada
ssh user@host comando           # executar comando remoto
ssh -t user@host "top"         # forçar alocação de TTY
```

Opções de Conexão

`-p porta`	Conectar a uma porta específica
`-i chave`	Usar identidade específica (chave privada)
`-t`	Forçar alocação de pseudo-terminal
`-v / -vv / -vvv`	Depuração detalhada (nível crescente)
`-q`	Modo silencioso (suprime avisos)
`-N`	Sem comando remoto (para túneis)
`-f`	Ir para segundo plano antes do comando
`-J salto`	Host intermediário (ProxyJump)

Gerenciamento de Chaves

Gerar Chaves

```
ssh-keygen -t ed25519 -C "voce@example.com"
ssh-keygen -t rsa -b 4096 -C "voce@example.com"
ssh-keygen -t ed25519 -f ~/.ssh/minhachave
ssh-keygen -p -f ~/.ssh/id_ed25519  # alterar senha
```

Implantar Chave Pública

```
ssh-copy-id user@host
ssh-copy-id -i ~/.ssh/minhachave.pub user@host
# Manual: acrescente .pub ao authorized_keys remoto
cat ~/.ssh/id_ed25519.pub | ssh user@host \
  "mkdir -p ~/.ssh && cat >> ~/.ssh/authorized_keys"
```

Arquivos de Chave

`~/.ssh/id_ed25519`	Chave privada (mantenha em segredo)
`~/.ssh/id_ed25519.pub`	Chave pública (pode compartilhar)
`~/.ssh/authorized_keys`	Remoto: chaves públicas aceitas
`~/.ssh/known_hosts`	Impressões digitais de hosts conhecidos

Arquivo de Configuração

Básico do ~/.ssh/config

```
Host meuservidor
  HostName 192.168.1.100
  User deploy
  Port 2222
  IdentityFile ~/.ssh/chave_deploy

# Então conecte apenas com:
# ssh meuservidor
```

Opções Úteis de Configuração

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

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

Diretivas de Configuração

`Host`	Padrão de alias para a entrada
`HostName`	Nome de host real ou IP
`User`	Nome de usuário para login
`Port`	Porta remota (padrão 22)
`IdentityFile`	Caminho para a chave privada
`ProxyJump`	Passar por outro host
`ServerAliveInterval`	Intervalo de keep-alive (segundos)
`IdentitiesOnly`	Usar apenas as chaves especificadas

Encaminhamento de Porta

Encaminhamento Local (-L)

```
# Acessar porta 5432 remota via porta local 5432
ssh -L 5432:localhost:5432 user@host
# Acessar remote-db:3306 através do host ssh
ssh -L 3306:remote-db:3306 user@host
# Vincular a todas as interfaces
ssh -L 0.0.0.0:8080:localhost:80 user@host
```

Encaminhamento Remoto (-R)

```
# Expor porta local 3000 na porta remota 8080
ssh -R 8080:localhost:3000 user@host
# Permitir conexões remotas de qualquer interface
ssh -R 0.0.0.0:8080:localhost:3000 user@host
```

Encaminhamento Dinâmico (-D)

```
# Proxy SOCKS5 na porta local 1080
ssh -D 1080 user@host
# Proxy SOCKS em segundo plano
ssh -D 1080 -fN user@host
```

SCP e SFTP

SCP (Cópia Segura)

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

SFTP (Transferência Interativa)

```
sftp user@host
# Dentro da sessão sftp:
# put local.txt    – enviar arquivo
# get remote.txt   – receber arquivo
# ls / lcd / cd    – listar / mudar diretório
```

Opções de Transferência

`-r`	Recursivo (copiar diretórios)
`-P porta`	Especificar porta (SCP usa -P, não -p)
`-C`	Habilitar compressão
`-l limite`	Limite de largura de banda em Kbit/s
`-i chave`	Usar arquivo de identidade específico

Encaminhamento de Agente

Agente SSH

```
eval "$(ssh-agent -s)"          # iniciar agente
ssh-add ~/.ssh/id_ed25519       # adicionar chave ao agente
ssh-add -l                      # listar chaves carregadas
ssh-add -D                      # remover todas as chaves
```

Encaminhando o Agente

```
ssh -A user@host                # encaminhar agente
# Ou em ~/.ssh/config:
# Host meuservidor
#   ForwardAgent yes
```

Notas sobre o Agente

O encaminhamento de agente permite ao host remoto usar suas chaves locais sem copiá-las. Use apenas com hosts confiáveis. Prefira ProxyJump ao encaminhamento de agente quando possível.

Túneis

Túnel Persistente

```
# Túnel em segundo plano que permanece aberto
ssh -fNT -L 5432:localhost:5432 user@host
# Túnel com reconexão automática (com autossh)
autossh -M 0 -fNT -L 5432:localhost:5432 user@host
```

Hosts Intermediários / Bastion

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

Gerenciamento de Túnel

`-f`	Segundo plano após autenticação
`-N`	Sem comando remoto
`-T`	Desabilitar pseudo-terminal
`~.`	Matar sessão SSH travada (escape)
`~C`	Abrir linha de comando para encaminhamento
`~#`	Listar conexões encaminhadas

Solução de Problemas

Depurando a Conexão

```
ssh -vvv user@host              # verbosidade máxima
ssh -G user@host                # exibir config (simulação)
ssh-keyscan host                # buscar chaves do host
ssh-keygen -R host              # remover de known_hosts
```

Problemas Comuns

`Permissão negada`	Chave, usuário ou permissões de ~/.ssh incorretos (700/600)
`Chave do host alterada`	ssh-keygen -R host, então reconectar
`Tempo de conexão esgotado`	Verificar firewall, porta e acessibilidade do host
`Muitas falhas de autenticação`	Use -i para especificar a chave ou IdentitiesOnly
`Pipe quebrado`	Adicionar ServerAliveInterval à configuração

Permissões de Arquivo

```
chmod 700 ~/.ssh
chmod 600 ~/.ssh/id_ed25519     # chave privada
chmod 644 ~/.ssh/id_ed25519.pub # chave pública
chmod 600 ~/.ssh/authorized_keys
chmod 644 ~/.ssh/known_hosts
```

Melhores Práticas de Segurança

Endurecimento do Servidor

`PasswordAuthentication no`	Desabilitar login por senha
`PermitRootLogin no`	Desabilitar acesso SSH como root
`AllowUsers deploy`	Lista de usuários permitidos
`Port 2222`	Porta não padrão (evitar scanners)
`MaxAuthTries 3`	Limitar tentativas de autenticação

Práticas com Chaves

Prefira chaves Ed25519 (menores, mais rápidas, mais seguras).
Sempre defina uma senha nas chaves privadas.
Use ssh-agent para evitar redigitar senhas.
Rotacione chaves periodicamente; revogue chaves não utilizadas.
Use IdentitiesOnly para controlar qual chave é oferecida.

Multiplexação

Compartilhamento de Conexão

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

# Criar diretório de socket
mkdir -p ~/.ssh/sockets
```

Benefícios da Multiplexação

Reutiliza uma única conexão TCP para múltiplas sessões SSH ao mesmo host. Elimina handshakes repetidos — conexões mais rápidas e menor sobrecarga.
ControlPersist mantém o master ativo (segundos).

Sequências de Escape

Comandos de Escape SSH

`~.`	Encerrar conexão (matar sessão travada)
`~^Z`	Suspender sessão SSH
`~C`	Abrir linha de comando (adicionar encaminhamento)
`~#`	Listar conexões encaminhadas
`~&`	Colocar SSH em segundo plano (aguardando conexões)
`~?`	Exibir ajuda de escape
`~~`	Enviar til literal