REFERENCIA RÁPIDA DE SSH

Conexiones, claves, configuración, túneles, SCP, SFTP

Conexión

Conexión Básica

```
ssh user@host                   # conectar al host
ssh -p 2222 user@host           # puerto personalizado
ssh user@host command            # ejecutar comando remoto
ssh -t user@host "top"          # forzar asignación de TTY
```

Opciones de Conexión

`-p port`	Conectar a un puerto específico
`-i key`	Usar identidad específica (clave privada)
`-t`	Forzar asignación de pseudo-terminal
`-v / -vv / -vvv`	Depuración detallada (nivel creciente)
`-q`	Modo silencioso (suprimir advertencias)
`-N`	Sin comando remoto (para túneles)
`-f`	Ir al fondo antes del comando
`-J jump`	Host de salto (ProxyJump)

Gestión de Claves

Generar Claves

```
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  # cambiar frase de contraseña
```

Desplegar Clave Pública

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

Archivos de Claves

`~/.ssh/id_ed25519`	Clave privada (mantener en secreto)
`~/.ssh/id_ed25519.pub`	Clave pública (compartir libremente)
`~/.ssh/authorized_keys`	Remoto: claves públicas aceptadas
`~/.ssh/known_hosts`	Huellas digitales de hosts conocidos

Archivo de Configuración

Configuración Básica ~/.ssh/config

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

# Luego conectar solo con:
# ssh myserver
```

Opciones de Configuración Útiles

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

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

Directivas de Configuración

`Host`	Patrón de alias para la entrada
`HostName`	Nombre de host o IP real
`User`	Nombre de usuario de inicio de sesión
`Port`	Puerto remoto (por defecto 22)
`IdentityFile`	Ruta a la clave privada
`ProxyJump`	Saltar a través de otro host
`ServerAliveInterval`	Intervalo de keep-alive (segundos)
`IdentitiesOnly`	Usar solo las claves especificadas

Reenvío de Puertos

Reenvío Local (-L)

```
# Acceder al puerto remoto 5432 via puerto local 5432
ssh -L 5432:localhost:5432 user@host
# Acceder a remote-db:3306 a través del host ssh
ssh -L 3306:remote-db:3306 user@host
# Enlazar a todas las interfaces
ssh -L 0.0.0.0:8080:localhost:80 user@host
```

Reenvío Remoto (-R)

```
# Exponer el puerto local 3000 en el puerto remoto 8080
ssh -R 8080:localhost:3000 user@host
# Permitir conexiones remotas desde cualquier interfaz
ssh -R 0.0.0.0:8080:localhost:3000 user@host
```

Reenvío Dinámico (-D)

```
# Proxy SOCKS5 en puerto local 1080
ssh -D 1080 user@host
# Proxy SOCKS en segundo plano
ssh -D 1080 -fN user@host
```

SCP y SFTP

SCP (Copia Segura)

```
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 (Transferencia Interactiva)

```
sftp user@host
# Dentro de la sesión sftp:
# put local.txt    — subir archivo
# get remote.txt   — descargar archivo
# ls / lcd / cd    — listar / cambiar directorio
```

Opciones de Transferencia

`-r`	Recursivo (copiar directorios)
`-P port`	Especificar puerto (SCP usa -P, no -p)
`-C`	Activar compresión
`-l limit`	Límite de ancho de banda en Kbit/s
`-i key`	Usar archivo de identidad específico

Reenvío de Agente

Agente SSH

```
eval "$(ssh-agent -s)"          # iniciar agente
ssh-add ~/.ssh/id_ed25519       # agregar clave al agente
ssh-add -l                      # listar claves cargadas
ssh-add -D                      # eliminar todas las claves
```

Reenviar el Agente

```
ssh -A user@host                # reenviar agente
# O en ~/.ssh/config:
# Host myserver
#   ForwardAgent yes
```

Notas sobre el Agente

El reenvío de agente permite que el host remoto use tus claves locales sin copiarlas. Usar solo con hosts de confianza. Prefiere ProxyJump sobre el reenvío de agente cuando sea posible.

Túneles

Túnel Persistente

```
# Túnel en segundo plano que permanece abierto
ssh -fNT -L 5432:localhost:5432 user@host
# Túnel con reconexión automática (con autossh)
autossh -M 0 -fNT -L 5432:localhost:5432 user@host
```

Hosts de Salto / Bastión

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

Gestión de Túneles

`-f`	Segundo plano tras autenticación
`-N`	Sin comando remoto
`-T`	Deshabilitar pseudo-terminal
`~.`	Matar sesión SSH bloqueada (escape)
`~C`	Abrir línea de comandos para reenvío
`~#`	Listar conexiones reenviadas

Resolución de Problemas

Depurar la Conexión

```
ssh -vvv user@host              # máxima verbosidad
ssh -G user@host                # volcar configuración (simulacro)
ssh-keyscan host                # obtener claves del host
ssh-keygen -R host              # eliminar de known_hosts
```

Problemas Comunes

`Permission denied`	Clave, usuario o permisos de ~/.ssh incorrectos (700/600)
`Host key changed`	ssh-keygen -R host, luego reconectar
`Connection timed out`	Verificar firewall, puerto y accesibilidad del host
`Too many auth failures`	Usar -i para especificar clave o IdentitiesOnly
`Broken pipe`	Agregar ServerAliveInterval a la configuración

Permisos de Archivos

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

Buenas Prácticas de Seguridad

Endurecimiento del Servidor

`PasswordAuthentication no`	Deshabilitar inicio de sesión con contraseña
`PermitRootLogin no`	Deshabilitar acceso SSH como root
`AllowUsers deploy`	Lista blanca de usuarios permitidos
`Port 2222`	Puerto no estándar (evitar escáneres)
`MaxAuthTries 3`	Limitar intentos de autenticación

Prácticas con Claves

Prefiere claves Ed25519 (más pequeñas, rápidas y seguras).
Siempre establece una frase de contraseña en las claves privadas.
Usa ssh-agent para evitar escribir la frase repetidamente.
Rota las claves periódicamente; revoca las claves no usadas.
Usa IdentitiesOnly para controlar qué clave se ofrece.

Multiplexación

Compartir Conexiones

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

# Crear directorio de sockets
mkdir -p ~/.ssh/sockets
```

Beneficios de la Multiplexación

Reutiliza una sola conexión TCP para múltiples sesiones SSH al mismo host. Elimina los handshakes repetidos — conexiones más rápidas y menor sobrecarga. ControlPersist mantiene el maestro activo (en segundos).

Secuencias de Escape

Comandos de Escape SSH

`~.`	Terminar conexión (matar sesión bloqueada)
`~^Z`	Suspender sesión SSH
`~C`	Abrir línea de comandos (agregar reenvío)
`~#`	Listar conexiones reenviadas
`~&`	Poner SSH en segundo plano (esperando conexiones)
`~?`	Mostrar ayuda de escape
`~~`	Enviar tilde literal