Référence rapide SSH

Connexions, clés, config, tunnels, SCP, SFTP

Connexion

Connexion de base

```
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
```

Options de connexion

-p port	Se connecter à un port spécifique
-i key	Utiliser une clé privée spécifique
-t	Forcer l'allocation d'un pseudo-terminal
-v / -vv / -vvv	Débogage verbeux (détail croissant)
-q	Mode silencieux (supprimer les avertissements)
-N	Aucune commande distante (pour les tunnels)
-f	Passer en arrière-plan avant la commande
-J jump	Hôte de rebond (ProxyJump)

Gestion des clés

Générer des clés

```
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
```

Déployer la clé publique

```
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"
```

Fichiers de clés

~/.ssh/id_ed25519	Clé privée (garder secrète)
~/.ssh/id_ed25519.pub	Clé publique (partager librement)
~/.ssh/authorized_keys	Distant : clés publiques acceptées
~/.ssh/known_hosts	Empreintes des hôtes connus

Fichier de configuration

Bases de ~/.ssh/config

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

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

Options de configuration utiles

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

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

Directives de configuration

Host	Modèle d'alias pour l'entrée
HostName	Nom d'hôte ou IP réel
User	Nom d'utilisateur de connexion
Port	Port distant (défaut 22)
IdentityFile	Chemin vers la clé privée
ProxyJump	Rebondir via un autre hôte
ServerAliveInterval	Intervalle keep-alive (secondes)
IdentitiesOnly	Utiliser uniquement les clés spécifiées

Redirection de port

Redirection locale (-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
```

Redirection distante (-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
```

Redirection dynamique (-D)

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

SCP & SFTP

SCP (Copie sécurisée)

```
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 (Transfert interactif)

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

Options de transfert

-r	Récursif (copier des répertoires)
-P port	Spécifier le port (SCP utilise -P, pas -p)
-C	Activer la compression
-l limit	Limiter la bande passante en Kbit/s
-i key	Utiliser un fichier d'identité spécifique

Transmission d'agent

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
```

Transmettre l'agent

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

Notes sur l'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 persistant

```
# 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
```

Hôtes de rebond / 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
```

Gestion des tunnels

-f	Arrière-plan après authentification
-N	Aucune commande distante
-T	Désactiver le pseudo-terminal
~.	Tuer une session SSH bloquée (séquence d'échappement)
~C	Ouvrir la ligne de commande pour la redirection
~#	Lister les connexions redirigées

Dépannage

Déboguer la connexion

```
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
```

Problèmes courants

Permission denied	Mauvaise clé, utilisateur, ou permissions ~/.ssh (700/600)
Host key changed	ssh-keygen -R host, puis se reconnecter
Connection timed out	Vérifier le pare-feu, le port, l'accessibilité de l'hôte
Too many auth failures	Utiliser -i pour spécifier la clé ou IdentitiesOnly
Broken pipe	Ajouter ServerAliveInterval à la configuration

Permissions des fichiers

```
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
```

Référence rapide SSH

Bonnes pratiques de sécurité

Durcissement du serveur

`PasswordAuthentication no`	Désactiver la connexion par mot de passe
`PermitRootLogin no`	Désactiver l'accès SSH en tant que root
`AllowUsers deploy`	Liste blanche des utilisateurs autorisés
`Port 2222`	Port non standard (éviter les scanners)
`MaxAuthTries 3`	Limiter les tentatives d'authentification

Bonnes pratiques pour les clés

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.

Multiplexage

Partage de connexion

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

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

Avantages du multiplexage

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).

Séquences d'échappement

Commandes d'échappement SSH

`~.`	Terminer la connexion (tuer une session bloquée)
`~^Z`	Suspendre la session SSH
`~C`	Ouvrir la ligne de commande (ajouter une redirection)
`~#`	Lister les connexions redirigées
`~&`	Mettre SSH en arrière-plan (en attente de connexions)
`~?`	Afficher l'aide des séquences d'échappement
`~~`	Envoyer un tilde littéral