

Connexion entre deux machines via SSH

Objectif

L'objectif de cette documentation est d'apprendre à établir une connexion sécurisée entre deux machines (un serveur et un client) à l'aide du protocole **SSH (Secure Shell)**.

SSH est un protocole réseau crypté qui permet aux administrateurs système de se connecter à distance à un ordinateur pour le contrôler et l'administrer de manière sécurisée.

Étapes globales

1. Installer et activer le service SSH
2. Établir une première connexion SSH entre deux machines
3. Générer des **clés SSH** (clé publique et clé privée)
4. Transférer la clé publique sur le serveur
5. Modifier la configuration SSH pour renforcer la sécurité
6. Redémarrer et vérifier le service SSH
7. Tester une connexion avec et sans clé SSH

1. Installation du serveur SSH

Sur la machine **serveur**, exécute les commandes suivantes pour mettre à jour les paquets et installer OpenSSH :

```
sudo apt update && sudo apt upgrade -y  
  
sudo apt install openssh-server -y
```

2. Connexion entre les deux machines

Côté serveur

Vérifie l'adresse IP de la machine :

```
ip a
```

Note l'adresse IP (ex : 192.168.1.100).

Côté client

Depuis la machine cliente, tente une connexion SSH :

```
ssh nom_utilisateur@adresse_ip_du_serveur
```

Exemple :

```
ssh otniel@192.168.1.100
```

3. Génération des clés SSH

Sur la **machine cliente** :

```
ssh-keygen -t rsa -b 4096
```

Appuie sur **Entrée** pour valider les options par défaut.

Puis vérifie les fichiers générés :

```
cd ~/.ssh/
```

```
ls
```

Tu verras deux fichiers :

- id_rsa : **clé privée** (confidentielle)
- id_rsa.pub : **clé publique**

4. Envoi de la clé publique vers le serveur

A. Automatique avec `ssh-copy-id` (recommandé)

```
ssh-copy-id nom_utilisateur@adresse_ip_du_serveur
```

B. Manuelle

Sur le client :

```
cat ~/.ssh/id_rsa.pub
```

Copie le contenu, puis colle-le sur le serveur dans ce fichier :

```
~/.ssh/authorized_keys
```

✂ 5. Modification de la configuration SSH (optionnel)

Sur la **machine serveur**, édite le fichier de configuration :

```
sudo nano /etc/ssh/sshd_config
```

Tu peux par exemple :

- Désactiver l'authentification par mot de passe : `PasswordAuthentication no`
- Restreindre l'accès à un utilisateur spécifique : `AllowUsers nom_utilisateur`

6. Redémarrer le service SSH et vérifier son statut

Redémarre SSH pour appliquer les modifications :

```
sudo systemctl restart sshd
```

Vérifie que le service est bien actif :

```
sudo systemctl status sshd
```

7. Connexion avec ou sans clé privée

Connexion avec clé privée

Depuis la **machine cliente** :

```
ssh -i ~/.ssh/id_rsa nom_utilisateur@adresse_ip
```

Connexion sans clé (avec mot de passe)

```
ssh nom_utilisateur@adresse_ip
```

 **attention : si l'authentification par mot de passe a été désactivée sur le serveur, cette méthode ne fonctionnera pas.**

Conclusion

Avec SSH, tu sécurises tes accès distants et ouvres la voie à des pratiques avancées d'administration système. La maîtrise des clés SSH est une compétence essentielle pour tout futur administrateur réseau.