Explication de la commande `ssh-copy-id`

Riyad Derguini

February 20, 2025

Introduction

La commande `ssh-copy-id` est un outil pratique pour configurer l'authentification par clé SSH sur un serveur distant. Elle permet de copier votre clé publique SSH sur un serveur distant, afin que vous puissiez vous connecter à ce serveur sans avoir à saisir votre mot de passe à chaque fois.

Fonctionnement de `ssh-copy-id`

- **Clé SSH** :
  - SSH utilise une paire de clés cryptographiques : une **clé privée** (gardée secrète sur votre machine locale) et une **clé publique** (copiée sur le serveur distant).
  - La commande `ssh-copy-id` copie votre **clé publique** sur le serveur distant.
- **Authentification sans mot de passe** :
  - Une fois la clé publique copiée sur le serveur, celui-ci l'utilise pour vérifier votre identité lorsque vous vous connectez.
  - Si la clé privée correspondante est présente sur votre machine locale, vous serez authentifié automatiquement sans avoir à saisir votre mot de passe.

Utilisation de base

La syntaxe de la commande est la suivante :

```
ssh-copy-id utilisateur@hôte
```

- `utilisateur` : Le nom d'utilisateur sur le serveur distant.
- `hôte` : L'adresse IP ou le nom d'hôte du serveur distant.

Exemple :

```
ssh-copy-id user@192.168.1.100
```

Ce que fait `ssh-copy-id` en détail

- **Vérifie la présence de clés SSH locales** :
  - La commande cherche les clés publiques dans le répertoire `~/.ssh/` (par défaut, `id_rsa.pub`, `id_ecdsa.pub`, ou `id_ed25519.pub`).
  - Si aucune clé n'est trouvée, elle vous propose d'en générer une avec `ssh-keygen`.
- **Copie la clé publique sur le serveur distant** :
  - La clé publique est ajoutée au fichier `~/.ssh/authorized_keys` sur le serveur distant.
  - Si le fichier `authorized_keys` n'existe pas, il est créé.

- **Configure les permissions** :
  - La commande s'assure que les permissions du fichier `~/.ssh/authorized_keys` et du répertoire `~/.ssh/` sont correctes (généralement `600` pour le fichier et `700` pour le répertoire).
- **Authentification** :
  - Vous devrez saisir votre mot de passe une dernière fois pour que `ssh-copy-id` puisse se connecter au serveur et copier la clé.

Options courantes

- `-i` : Spécifie le fichier de clé publique à utiliser (utile si vous avez plusieurs clés).

```
ssh-copy-id -i ~/.ssh/ma_cle_publique.pub user@192.168.1.100
```

- `-p` : Spécifie un port SSH personnalisé (si le serveur n'utilise pas le port par défaut 22).

```
ssh-copy-id -p 2222 user@192.168.1.100
```

Exemple complet

1. Générez une paire de clés SSH (si ce n'est pas déjà fait) :

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

2. Copiez la clé publique sur le serveur distant :

```
ssh-copy-id user@192.168.1.100
```

3. Connectez-vous au serveur sans mot de passe :

```
ssh user@192.168.1.100
```

Avantages de `ssh-copy-id`

- **Facilité d'utilisation** : Automatise la copie de la clé publique et la configuration des permissions.
- **Sécurité** : L'authentification par clé SSH est plus sécurisée que l'authentification par mot de passe.
- **Confort** : Plus besoin de saisir votre mot de passe à chaque connexion.

Conclusion

La commande `ssh-copy-id` simplifie la configuration de l'authentification par clé SSH en copiant votre clé publique sur un serveur distant. Cela vous permet de vous connecter au serveur sans mot de passe, tout en améliorant la sécurité de vos connexions SSH.