Serveur OpenSSH

Précédent Suivant

Introduction

Cette section du guide du serveur Ubuntu présente un ensemble d'outils puissants appelé *OpenSSH* pour le contrôle à distance et le transfert de données entre des ordinateurs en réseau. Vous apprendrez également quelques paramètres de configuration possibles avec l'application serveur OpenSSH et comment les changer sur votre système Ubuntu.

OpenSSH est une version libre de la famille d'outils du protocole Secure Shell (SSH) pour le contrôle à distance ou le transfert des fichiers entre les ordinateurs. Les outils traditionnels utilisés pour accomplir ces fonctions tels que *telnet* ou *rcp* ne sont pas sécurisés et transmettent le mot de passe utilisateur en clair lors de leurs utilisations. OpenSSH fournit un démon de serveur et des outils pour les clients afin de sécuriser le contrôle à distance chiffré et les opérations de transfert de fichiers, remplaçant ainsi les anciens outils.

Le serveur OpenSSH, *sshd*, attend en permanence des connexions depuis des clients. Quand une requête de connexion a lieu, *sshd* établit la connexion correcte en fonction du type de client. Par exemple, si un client se connecte avec le client *ssh*, le serveur OpenSSH va établir une connexion sécurisée après une authentification. Si un client se connecte avec *scp*, le serveur OpenSSH va commencer un transfert de fichier sécurisé entre le serveur et le client après une authentification. OpenSSH peut utiliser de nombreuses méthodes d'authentification, par exemple un mot de passe, une clé publique, ou un ticket *Kerberos*.

Installation

L'installation des applications client et serveur d'OpenSSH est simple. Pour installer les applications clientes d'OpenSSH sur votre système Ubuntu, tapez cette commande dans un terminal :

```
sudo apt install openssh-client
```

Pour installer le serveur OpenSSH et les fichiers nécessaires, utilisez cette commande dans un terminal :

```
sudo apt install openssh-server
```

Le paquet *openssh-server* peut aussi être sélectionné pour s'installer pendant la procédure d'installation de l'édition serveur.

Configuration

Vous pouvez configurer le comportement par défaut du serveur OpenSSH, *sshd*, en modifiant le fichier `/etc/ssh/sshd_config`. Pour des informations sur les options de configuration utilisées dans ce fichier, veuillez lire le manuel approprié en tapant la commande suivante dans un terminal :

```
man sshd_config
```

Il existe de nombreuses directives dans le fichier de configuration *sshd* contrôlant des choses telles que les paramètres de communication et les modes d'authentification. Ce qui suit sont des exemples de directives de configuration modifiables en éditant le fichier `/etc/ssh/sshd_config`.

> Avant de modifier le fichier de configuration, vous devriez faire une copie du fichier original et le protéger en écriture de façon à conserver les paramètres d'origine en référence et à pouvoir les réutiliser en cas de besoin.
>
> Copiez le fichier `/etc/ssh/sshd_config` et protégez le en écriture en tapant la commande suivante dans un terminal :
>
> ```
> sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.original
> sudo chmod a-w /etc/ssh/sshd_config.original
> ```

Voici des exemples de directives de configuration que vous pouvez changer :

1. Pour que OpenSSH écoute sur le port TCP 2222 au lieu du port par défaut 22, changez la directive Port comme ceci :

   Port 2222

2. Pour que *sshd* accepte les informations de connexion basées sur une clef publique, il suffit d'ajouter ou de modifier la ligne :

   PubkeyAuthentication yes

   Si la ligne est déjà présente, alors assurez-vous qu'elle n'est pas commentée.

3. Pour que le serveur OpenSSH affiche le contenu du fichier `/etc/issue.net` comme une invite avant l'affichage de l'écran de connexion, il suffit d'ajouter ou de modifier la ligne :

   Banner /etc/issue.net

   dans le fichier `/etc/ssh/sshd_config`

dans le fichier `/etc/ssh/sshd_config`.

Après avoir modifié le fichier `/etc/ssh/sshd_config`, enregistrez-le et redémarrez le service *sshd* afin de prendre en compte les changements. Pour cela, saisissez la commande suivante dans un terminal :

```
sudo systemctl restart sshd.service
```

> Beaucoup d'autres directives de configuration *sshd* sont disponibles pour changer le comportement de l'application serveur en fonction de vos besoins. Soyez averti, cependant, si votre seul moyen d'accès à un serveur est *ssh* et que vous faites une erreur dans la configuration *sshd* dans le fichier `/etc/ssh/sshd_config`, vous pouvez vous retrouver bloqué sur le serveur lors de son redémarrage. En outre, si une directive de configuration incorrecte est fournie, le serveur *sshd* peut refuser de démarrer, soyez donc très prudent lorsque vous modifiez ce fichier sur un serveur distant.

Clés SSH

Les *clés* SSH permettent l'authentification entre deux hôtes sans avoir besoin de mot de passe. L'authentification par clé SSH utilise deux clés, une clé *privée* et une clé *publique*.

Pour générer les clés, dans un terminal tapez :

```
ssh-keygen -t rsa
```

Cela générera les clés à l'aide de l'*Algorithme RSA*. Pendant le processus, vous serez invité à entrer un mot de passe. Appuyez simplement sur *Entrée* lorsque vous y êtes invité pour créer la clé.

Par défaut, la clé *publique* est sauvegardée dans le fichier `~/.ssh/id_rsa.pub`, alors que la clé *privée* est dans `~/.ssh/id_rsa`. Copiez maintenant le fichier `id_rsa.pub` sur l'hôte distant et ajoutez le à `~/.ssh/authorized_keys` en entrant :

```
ssh-copy-id identifiant@hôte
```

Pour finir, vérifiez les permissions du fichier `authorized_keys`. Seul l'utilisateur authetifié doit avoir les droits en lecture et écriture. Si les permissions sont incorrectes, changez-les en tapant :

```
chmod 600 .ssh/authorized_keys
```

Vous devriez maintenant pouvoir établir une connexion SSH vers l'hôte sans avoir à saisir de mot de passe.

Références

1. Pour plus d'information, consultez la page du Wiki Ubuntu consacrée à SSH.
2. Site Web de OpenSSH
3. Page Wiki sur OpenSSH avancé

Précédent Suivant