Configuration d'un accès SFTP restreint au répertoire chroot

Ce guide décrit comment configurer un environnement chroot avec un accès SFTP uniquement pour les utilisateurs, en utilisant des clés SSH.

Prérequis

- Un serveur exécutant GNU/Linux
- Un accès root au serveur
- OpenSSH installé et en cours d'exécution

Étapes

1. Créer un utilisateur chroot

```
adduser <nom_d'utilisateur>
```

2. Créer un groupe SFTP

```
groupadd sftpusers
```

3. Ajouter l'utilisateur au groupe SFTP

```
usermod -aG sftpusers <nom_d'utilisateur>
```

4. Configurer le répertoire chroot

Créer un répertoire pour les utilisateurs SFTP, en s'assurant que les droits de propriété et les autorisations sont configurés correctement.

```
mkdir -p /sftp/<nom_d'utilisateur>
chown root:root /sftp
chmod 755 /sftp
mkdir /sftp/<nom_d'utilisateur>
chown <nom_d'utilisateur>:<nom_d'utilisateur> /sftp/<nom_d'utilisateur>
chmod 700 /sftp/<nom_d'utilisateur>
```

5. Configurer SSH pour l'accès SFTP

Modifier le fichier `/etc/ssh/sshd_config` pour utiliser SFTP interne et définir les restrictions.

1. Mettre à jour la ligne `Subsystem` :

   ```
   Subsystem sftp internal-sftp
   ```

2. Ajouter un bloc `Match` à la fin :

   ```
   Match Group sftpusers
       ChrootDirectory /sftp/%u
       ForceCommand internal-sftp
       AllowTcpForwarding no
       X11Forwarding no
   ```

6. Configurer les clés SSH de l'utilisateur

Créer et configurer les répertoires SSH pour l'utilisateur :

```
mkdir /home/<nom_d'utilisateur>/.ssh
touch /home/<nom_d'utilisateur>/.ssh/authorized_keys
chmod 700 /home/<nom_d'utilisateur>/.ssh
chmod 600 /home/<nom_d'utilisateur>/.ssh/authorized_keys
chown <nom_d'utilisateur>:<nom_d'utilisateur> /home/<nom_d'utilisateur>/.ssh
chown <nom_d'utilisateur>:<nom_d'utilisateur> /home/<nom_d'utilisateur>/.ssh/authorized_keys
```

Copier la clé publique SSH dans `/home/<nom_d'utilisateur>/.ssh/authorized_keys`.

7. Redémarrer le service SSH

```
systemctl restart sshd
```

Vérification

- Essayez une connexion SFTP pour vérifier que l'accès est restreint.
- Assurez-vous que les utilisateurs ne peuvent pas accéder au shell.

Script qui automatise la configuration :

```
#!/bin/bash

# Ce script configure automatiquement un environnement chroot pour un utilisateur SFTP dans le répertoire /sftp.
# Il crée un utilisateur avec un accès SFTP restreint, met en place la structure de répertoires nécessaire,
# configure les autorisations et ajoute un fichier authorized_keys pour l'authentification par clé.

# Utilisation :
# Enregistrez ce script sous le nom "sftp_chroot.sh" et rendez-le exécutable en exécutant la commande : `chmod +x sftp_chroot.sh`.
# Ensuite, exécutez-le avec les privilèges root en utilisant : `sudo ./sftp_chroot.sh`.
# Le script vous demandera le nom d'utilisateur SFTP, configurera l'environnement chroot nécessaire, définira les autorisations,
# et appliquera les paramètres SSH pour restreindre l'utilisateur à l'accès SFTP uniquement. Enfin, il redémarrera le service SSH pour
# appliquer les modifications.

# Vérifier si le script est exécuté avec les privilèges root
if [[ $EUID -ne 0 ]]; then
    echo "Ce script doit être exécuté en tant que root."
    exit 1
fi

# Demander le nom d'utilisateur SFTP
read -p "Entrez le nom d'utilisateur SFTP : " USERNAME

# Créer l'utilisateur avec le shell /bin/false pour limiter l'accès
useradd -m -d /sftp/$USERNAME -s /bin/false $USERNAME

# Créer l'environnement chroot dans /sftp
```

```
mkdir -p /sftp/$USERNAME
mkdir -p /sftp/$USERNAME/upload
mkdir -p /sftp/$USERNAME/.ssh

# Définir les autorisations pour le répertoire chroot
chown root:root /sftp/$USERNAME
chmod 755 /sftp/$USERNAME
chown $USERNAME:$USERNAME /sftp/$USERNAME/upload

# Créer le fichier authorized_keys
touch /sftp/$USERNAME/.ssh/authorized_keys
chmod 700 /sftp/$USERNAME/.ssh
chmod 600 /sftp/$USERNAME/.ssh/authorized_keys
chown -R $USERNAME:$USERNAME /sftp/$USERNAME/.ssh

echo "L'utilisateur $USERNAME a été configuré avec succès dans un environnement chroot."

# Ajouter la configuration SFTP à sshd_config si nécessaire
if ! grep -q "Match User $USERNAME" /etc/ssh/sshd_config; then
    echo -e "\n# Configuration SFTP pour $USERNAME" >> /etc/ssh/sshd_config
    echo "Match User $USERNAME" >> /etc/ssh/sshd_config
    echo "    ChrootDirectory /sftp/$USERNAME" >> /etc/ssh/sshd_config
    echo "    ForceCommand internal-sftp" >> /etc/ssh/sshd_config
    echo "    AllowTcpForwarding no" >> /etc/ssh/sshd_config
    echo "    PermitTunnel no" >> /etc/ssh/sshd_config
fi

# Redémarrer le service SSH
systemctl restart ssh

echo "Le jail chroot pour $USERNAME a été configuré avec succès. Vous pouvez maintenant
ajouter les clés SSH dans /sftp/$USERNAME/.ssh/authorized_keys"
```

Révision #3
Créé 2025-05-12 22:15:13 CEST par Philippe Favre
Mis à jour 2025-05-12 22:20:09 CEST par Philippe Favre