SFTP

Man SFTP

Comment limiter les utilisateurs SFTP aux répertoires de base à l'aide de Jail chroot

Dans ce didacticiel, nous verrons comment limiter les utilisateurs SFTP à leurs répertoires personnels ou spécifiques. Cela signifie que l'utilisateur ne peut accéder qu'à son répertoire de départ respectif, pas à l'ensemble du système de fichiers.

Restreindre les répertoires personnels des utilisateurs est essentiel, en particulier dans un environnement de serveur partagé, afin qu'un utilisateur non autorisé ne puisse pas jeter un coup d'œil furtif sur les fichiers et les dossiers des autres utilisateurs.

Le moyen le plus simple de procéder consiste à créer un environnement de prison chrooté pour l'accès SFTP. Cette méthode est la même pour tous les systèmes d'exploitation Unix/Linux. En utilisant un environnement chrooté, nous pouvons limiter les utilisateurs à leur répertoire de base ou à un répertoire spécifique. Limiter les utilisateurs aux répertoires de base

Dans cette section, nous allons créer un nouveau groupe appelé sftpgroup et attribuer les droits de propriété et autorisations appropriés aux comptes d'utilisateur. Il existe deux choix pour limiter les utilisateurs à des répertoires personnels ou spécifiques, nous verrons les deux sens dans cet article.

Limitons l'utilisateur existant, par exemple tecmint , à son répertoire de base nommé /home/tecmint . Pour cela, vous devez créer un nouveau groupe sftpgroup à l'aide de la commande groupadd , comme indiqué:

```
# groupadd sftpgroup
```

Ensuite, attribuez à l'utilisateur "tecmint" le groupe sftpgroup .

```
# usermod -G sftpgroup tecmint
```

Vous pouvez également créer un nouvel utilisateur à l'aide de la commande useradd, par exemple senthil et affecter l'utilisateur au groupe utilisateurs de fichiers .

```
# adduser senthil -g sftpgroup -s /sbin/nologin
# passwd tecmint
```

Ouvrez et ajoutez les lignes suivantes au fichier de configuration /etc/ssh/sshd_config .

Subsystem sftp internal-sftp

Match Group sftpgroup

```
ChrootDirectory /home
```

```
ForceCommand internal-sftp
X11Forwarding no
AllowTcpForwarding no
```

Enregistrez et quittez le fichier, redémarrez le service sshd pour appliquer les nouvelles modifications.

```
# systemctl restart sshd
```

OR

```
# service sshd restart
```

Si vous chrootez plusieurs utilisateurs dans le même répertoire, vous devez modifier les autorisations du répertoire de base de chaque utilisateur afin d'empêcher tous les utilisateurs de parcourir les répertoires de base des autres utilisateurs.

```
# chmod 700 /home/tecmint
```

Il est maintenant temps de vérifier la connexion depuis un système local. Essayez de ssh votre système distant à partir de votre système local.

```
# ssh [email protected]
```

Ici,

```
tecmint – remote system’s username.
192.168.1.150 – Remote system’s IP address.
```

's password: Could not chdir to home directory /home/tecmint: No such file or directory This service allows sftp connections only. Connection to 192.168.1.150 closed.

Ensuite, accédez au système distant en utilisant SFTP.

```
# sftp [email protected]
```

```
[email protected]'s password:
Connected to 192.168.1.150.
sftp>
```

Laissez-nous vérifier le répertoire de travail actuel:

```
sftp&gt pwd
Remote working directory: /
```

```
sftp&gt ls
tecmint
```

Ici, tecmint est le répertoire de base. Accédez au répertoire tecmint et créez les fichiers ou les dossiers de votre choix.

```
sftp&gt cd tecmint
Remote working directory: /
```

```
sftp&gt mkdir test
tecmint
```

Limiter les utilisateurs à un répertoire spécifique

Dans notre exemple précédent, nous limitons les utilisateurs existants au répertoire de base. Nous verrons maintenant comment restreindre un nouvel utilisateur à un répertoire personnalisé.

Créez un nouveau groupe sftpgroup .

```
# groupadd sftpgroup
```

Ensuite, créez un répertoire pour le groupe SFTP et attribuez des autorisations à l'utilisateur root.

```
# mkdir -p /sftpusers/chroot
# chown root:root /sftpusers/chroot/
```

Ensuite, créez de nouveaux répertoires pour chaque utilisateur, auxquels ils auront un accès complet. Par exemple, nous allons créer un utilisateur tecmint et son nouveau répertoire de base avec l'autorisation de groupe appropriée à l'aide de la série de commandes suivante.

```
# adduser tecmint -g sftpgroup -s /sbin/nologin
# passwd tecmint
# mkdir /sftpusers/chroot/tecmint
# chown tecmint:sftpgroup /sftpusers/chroot/tecmint/
# chmod 700 /sftpusers/chroot/tecmint/
```

Modifiez ou ajoutez les lignes suivantes à la fin du fichier:

```
#Subsystem     sftp    /usr/libexec/openssh/sftp-server
Subsystem sftp  internal-sftp
```

Match Group sftpgroup

```
ChrootDirectory /sftpusers/chroot/
ForceCommand internal-sftp
X11Forwarding no
AllowTcpForwarding no
```

Enregistrez et quittez le fichier. Redémarrez le service sshd pour prendre en compte les modifications enregistrées.

```
# systemctl restart sshd
```

OR

```
# service sshd restart
```

Ainsi, vous pouvez vérifier en vous connectant au serveur SSH et SFTP distant en suivant l'étape décrite ci-dessus dans la section Vérification de la connexion SSH et SFTP.

Sachez que cette méthode désactivera l'accès au shell, c'est-à-dire que vous ne pourrez pas accéder à la session shell du système distant à l'aide de SSH. Vous pouvez uniquement accéder aux systèmes distants via SFTP et transférer des fichiers depuis et vers les systèmes locaux et distants. Conclusion

Vous savez maintenant comment restreindre les répertoires personnels des utilisateurs à l'aide d'un environnement Chroot sous Linux. Si vous trouvez cela utile, partagez cet article sur vos réseaux sociaux et indiquez-nous, dans la section commentaire ci-dessous, s'il existe d'autres méthodes pour restreindre les répertoires personnels des utilisateurs.

From:
https://chanterie37.fr/fablab37110/ - **Castel'Lab le Fablab MJC de Château-Renault**

Permanent link:
https://chanterie37.fr/fablab37110/doku.php?id=start:parcours_linux:sftp&rev=1597936889

Last update: **2023/01/27 16:08**