

Ubuntu - Encrypter son Répertoire Home



Il est possible d'encrypter votre répertoire personnel (homedir) après l'installation d'Ubuntu, mais cela peut être un processus délicat. Voici les deux principales options pour le faire après coup :

Option 1 : Utilisation de `ecryptfs` pour chiffrer le répertoire personnel

`ecryptfs` est un système de fichiers qui permet de chiffrer facilement un répertoire personnel. Ubuntu propose un outil intégré pour cela, mais gardez à l'esprit que cela nécessite de déplacer temporairement vos fichiers et peut entraîner des complications si vous ne suivez pas correctement les étapes.

Étapes :

1. **Installer les paquets nécessaires** : Si `ecryptfs` n'est pas encore installé, vous pouvez l'installer en exécutant :

```
sudo apt update  
sudo apt install ecryptfs-utils
```

2. **Créer une sauvegarde de vos données** : Avant de procéder, il est fortement recommandé de sauvegarder votre répertoire personnel pour éviter toute perte de données.
3. **Monter et chiffrer votre répertoire personnel** : Vous pouvez maintenant configurer l'encryptage de votre répertoire personnel avec la commande suivante :

```
sudo ecryptfs-migrate-home -u <votre_nom_utilisateur>
```

Remplacez `<votre_nom_utilisateur>` par votre nom d'utilisateur. Cette commande va déplacer vos fichiers vers un répertoire chiffré tout en maintenant votre homedir accessible.

4. **Vérification** : Après avoir effectué cette opération, vous pouvez vérifier si le répertoire est bien chiffré en consultant le contenu du répertoire. Les fichiers devraient maintenant être stockés dans un format chiffré.
5. **Redémarrage et vérification** : Redémarrez votre machine et vérifiez si l'encryptage fonctionne en vous reconnectant. Le répertoire devrait être monté de manière transparente lors de la connexion.

Option 2 : Utilisation de `LUKS` pour chiffrer une partition

Si vous préférez un chiffrement de niveau disque, vous pouvez utiliser LUKS pour chiffrer une partition entière qui contiendra votre homedir. Cela nécessite de créer une nouvelle partition ou de réutiliser une partition existante.

Étapes :

1. **Sauvegarde** : Avant tout, faites une sauvegarde de vos données actuelles, car cette opération risque de tout effacer sur la partition cible.

2. **Créer une nouvelle partition (si nécessaire)** : Utilisez `gparted` ou `fdisk` pour créer une nouvelle partition ou redimensionner une partition existante pour allouer de l'espace pour le répertoire personnel.
3. **Chiffrer la partition avec LUKS** : Utilisez `cryptsetup` pour chiffrer la partition :

```
sudo cryptsetup luksFormat /dev/sdX
```

Remplacez `/dev/sdX` par l'identifiant de votre partition. Vous devrez entrer une passphrase pour le chiffrement.

4. **Ouvrir la partition chiffrée** : Après avoir chiffré la partition, vous devez l'ouvrir avec :

```
sudo cryptsetup luksOpen /dev/sdX my_encrypted_home
```

5. **Créer un système de fichiers sur la partition** : Créez un système de fichiers sur la partition chiffrée :

```
sudo mkfs.ext4 /dev/mapper/my_encrypted_home
```

6. **Monter la partition et transférer vos fichiers** : Montez la partition chiffrée et copiez vos fichiers personnels dedans :

```
sudo mount /dev/mapper/my_encrypted_home /mnt  
rsync -av /home/<votre_nom_utilisateur> /mnt/
```

7. **Mettre à jour `/etc/fstab` et `/etc/crypttab`** : Ajoutez la partition chiffrée à `/etc/crypttab` pour qu'elle soit ouverte automatiquement au démarrage :

```
my_encrypted_home /dev/sdX none luks
```

Ensuite, modifiez `/etc/fstab` pour ajouter la partition dans le système de fichiers :

```
/dev/mapper/my_encrypted_home /home ext4 defaults 0 2
```

8. **Redémarrage et vérification** : Redémarrez votre machine pour vérifier que tout fonctionne correctement. Vous devrez entrer la passphrase pour ouvrir la partition chiffrée au démarrage.

Conclusion

- Si vous souhaitez une méthode plus simple, `ecryptfs` est une bonne option, mais elle n'est plus aussi largement recommandée pour les nouvelles installations.
- Si vous souhaitez un chiffrement de niveau disque, `LUKS` offre une solution plus robuste mais nécessite plus d'étapes et peut impliquer des risques si les données ne sont pas correctement sauvegardées avant.

Dans les deux cas, il est important de bien comprendre les implications de la gestion des clés et des mots de passe, car perdre la clé de chiffrement peut rendre vos données irrécupérables.

🔄 Révision #2

★ Créé 2 janvier 2025 10:19:17 par Marc Leroi

✍ Mis à jour 2 janvier 2025 10:23:48 par Marc Leroi