Déverrouillage Automatique Autres Partition

> Pour réaliser ce tuto il est nécessaire d'avoir au préalable créé une partition chiffrée avec LUKS.

source : https://www.howtoforge.com/automatically-unlock-luks-encrypted-drives-with-a-keyfile

L'automatisation du déverrouillage d'une partition chiffrée au démarrage peut-être mis en place en suivant les étapes suivantes :

- 1/ Création d'un fichier de clé random
- 2/ Ajouter le fichier de clé à la partition LUKS
- 3/ Créer le mapper
- 4/ Monter la partition

1/ Création d'un fichier de clé random

la commande suivante créera un fichier au contenu aléatoire d'une taille de 4096 bits (mieux qu'un mot de passe de 20/30 caractères....). Vous pouvez utiliser n'importe quel fichier comme fichier clé, mais je pense qu'un fichier de 4kb avec un contenu aléatoire convient bien.

```
sudo dd if=/dev/urandom of=/root/keyfile bs=1024 count=4
```

Comme vous pouvez le voir avec l'arrtibut `of` , le fichier sera généré dans le dossier `/root` avec le nom `keyfile`.

Avant d'utiliser la nouvelle clé, rendre le fichier clé accessible en lecture seule à root

```
sudo chmod 0400 /root/keyfile
```

> Cela rendra le fichier clé lisible uniquement par root. Si quelqu'un accède à ce fichier clé, vous avez de toute façon un problème plus important sur votre serveur.

> Une autre solution consiste à attribuer à root:root le droit d'accès au fichier clé souhaité et à le placer dans le dossier /root.

2/ Ajouter le fichier à LUKS

Les dispositifs LUKS/dm_crypt peuvent contenir jusqu'à 10 fichiers clés/mots de passe différents. Ainsi, en plus du mot de passe déjà configuré, nous allons ajouter ce fichier clé comme méthode d'autorisation supplémentaire.

```
sudo cryptsetup luksAddKey /dev/sdX /root/keyfile
```

Il vous sera d'abord demandé d'entrer un mot de passe (existant) pour déverrouiller le lecteur.

3/ Création du Mapper

Les périphériques LUKS doivent créer un mappeur qui peut ensuite être référencé dans la fstab. Ouvrez /etc/crypttab :

```
sudo nano /etc/crypttab
```

et ajouter la ligne suivante dans le fichier :

```
# MapperNAme□partition□keyfile□□method
sdc_crypt      /dev/sdc1  /root/keyfile  luks

# OU
# MapperName□device UUID□□□□□□□□□□□□keyfile□□  method
sdX_crypt      /dev/disk/by-uuid/247ad289-dbe5-4419-9965-e3cd30f0b080  /root/keyfile  luks

# OU encore
sdc1_crypt □   UUID=d4eca898-8155-4c4d-b1ed-48f696a6ad99 □□□  /root/keyfile    luks
```

sdX_crypt est le nom du mappeur qui est créé. Vous pouvez utiliser n'importe quel nom, par exemple "music" ou "movies" ou "sfdsfawe" ....

Sauvegardez et fermez le fichier.

Ce que nous avons fait ici, c'est dire que le fichier /root/keyfile sera utilisé au lieu du mot de passe pour déverrouiller le lecteur.

4/ Monter la partition

Maintenant, nous avons un périphérique déverrouillé (enfin, pas encore, mais lorsque le système sera démarré) et nous avons juste besoin de le monter. Ouvrez le fichier /etc/fstab :

```
sudo nano /etc/fstab
```

puis ajouter une nouvelle ligne comme ci-dessous :

```
# MapperName□□  folder location□□
/dev/mapper/sdX_crypt  /media/sdX     ext3    defaults        0       2
```

Assurez-vous que le nom du mappeur que vous avez ajouté à l'étape 3 est correct. Assurez-vous également que le point de montage/dossier existe. Après l'avoir ajouté, enregistrez à nouveau le fichier et fermez-le.

Revision #5
Created 2023-06-05 16:49:45 UTC by gpatruno
Updated 2025-06-30 11:47:09 UTC by gpatruno