Mise en place de LUKS

> Afin de protéger au mieux vos données personnelles, il peut être nécessaire de chiffrer vos partitions utilisateur. En effet, si via le système il est impossible d'accéder aux fichiers qui ne vous appartiennent pas, un simple passage sur un livecd permet d'accéder à n'importe quel fichier de votre système. Le chiffrement de partition permet d'éviter ça. Ubuntu intègre en standard les outils nécessaires à une gestion simple de votre sécurité.

source : https://doc.ubuntu-fr.org/cryptsetup

source : https://www.val-r.fr/geek/os/linux/creer-et-utiliser-une-partition-chiffree-avec-luks-sous-linux/

La mise en place d'une partition chiffré se résume en 5 étapes :

- 1/ Installation & Préparation
- 3/ Création de la partition
- 4/ Chiffrement de la partition
- 5/ Utilisation de la partition chiffrée
  - Déverrouillage
  - Montage
  - Démontage
  - Verrouillage

1/ Installation & Préparation

Tout d'abord il est nécessaire d'installer cryptsetup.

```
sudo apt-get install cryptsetup
```

La commande `lsblk` permet de lister les disques et les partitions existantes :

```
NAME            MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINT
sda               8:0    0   20G  0 disk
├─sda1            8:1    0   19G  0 part  /
└─sda5            8:5    0  975M  0 part  [SWAP]
sdb□□□□ 8:16□0□10G□ 0 disk
```

```
└─sdb1          8:17   0   10G  0 part  /mnt/media
sdc             8:32   0 □50G  0 disk□□□□□# Disque a utiliser
```

Dans notre exemple ci-dessus nous avons 3 disques dur avec des partitions sur le serveur :

- Le disque **`sda`** de 20Go
  - Partition **`sda1`** qui monté à la racine du serveur
  - Partition **`sda5`** qui est du SWAP pour le serveur

- Le disque **`sdb`** de 10Go
  - Partition **`sdb1`** qui est monté sur le dossier media.

- Le disque **`sdc`** de 50Go sans partition existante

Nous allons utiliser le disque `sdc` pour créer la partition chiffrés.

3/ Créer une partition

Pour créer la partition, nous allons tout simplement utiliser l'outil Linux `fdisk` :

```
sudo fdisk /dev/sdc

# n   ajouter une nouvelle partition
Commande (m pour l''aide) : n

Type de partition
   p   primaire (0 primaire, 0 étendue, 4 libre)
   e   étendue (conteneur pour partitions logiques)
Sélectionnez (p par défaut) : p
Numéro de partition (1-4, 1 par défaut) :
Premier secteur (2048-105456767, 2048 par défaut) :
Dernier secteur, +/-secteurs ou +/-taille{K,M,G,T,P} (2048-105456767, 105456767 par défaut) :

Une nouvelle partition 1 de type « Linux » et de taille 50,3 GiB a été créée.

# w   écrire la table sur le disque et quitter
Commande (m pour l''aide) : w

La table de partitions a été altérée.
Appel d''ioctl() pour relire la table de partitions.
Synchronisation des disques.
```

Si nous relançons la commande lsblk nous pouvons voir apparaître la nouvelle partition :

```
NAME           MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINT
sda              8:0    0   20G  0 disk
├─sda1           8:1    0   19G  0 part  /
└─sda5           8:5    0  975M  0 part  [SWAP]
sdb□□□□ 8:16□0□10G□ 0 disk
└─sdb1           8:17   0   10G  0 part  /mnt/media
sdc              8:32   0 □50G  0 disk
└─sdc1           8:33   0 □50G  0 part□□□□# Partition créée
```

4/ Chiffrement de la partition

Pour créer une partition LUKS il suffit de lancer la commande suivante :

```
cryptsetup --verbose luksFormat --verify-passphrase /dev/sdc1

WARNING!
========
Cette action écrasera définitivement les données sur /dev/sdc.

Are you sure? (Type 'yes' in capital letters): YES
Saisissez la phrase secrète pour /dev/sdc :
Vérifiez la phrase secrète :
Emplacement de clef 0 créé.
Opération réussie.
```

5/ Utilisation de la partition chiffrée

Déverrouillage

Avant d'utiliser la nouvelle partition, il est nécessaire *d'ouvrir* la partition chiffrée ***(et il faudra le faire à chaque démarrage ou après la fermeture de la partition chiffrée)***.

```
cryptsetup -v luksOpen /dev/sdc1 maPartition
Saisissez la phrase secrète pour /dev/sdc1 :
Emplacement de clé 0 déverrouillé.
Opération réussie.
```

Pour vérifier que la partition a bien été déverrouiller utiliser la commande `lsblk` :

```
NAME           MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINT
sda              8:0    0   20G  0 disk
├─sda1           8:1    0   19G  0 part  /
└─sda5           8:5    0  975M  0 part  [SWAP]
sdb□□□□ 8:16□0□10G□ 0 disk
└─sdb1           8:17   0   10G  0 part  /mnt/media
sdc              8:32   0 □50G  0 disk
└─sdc1           8:33   0 □50G  0 part
  └─maPartition 254:1   0 □50G  0 crypt□□□□# Partition Déverrouillé
```

> Lors de la création d'une partition chiffré il est nécessaire de réaliser un formatage de la partition avant sont utilisation. Dans le cas contraire la partition sera corrompu.

Pour formater la partition déchiffré **(a faire seulement la première fois)** :

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

Montage

Maintenant que la partition est déverrouillé, pour l'utiliser il faut la monter avec un dossier.

> **Attention !**
> A présent, pour accéder au contenu de la partition chiffrée /dev/sdX1, il **ne faut pas** utiliser /dev/sdX1 mais le *mapper* créé lors de l'ouverture de la partition chiffrée :
> **/dev/mapper/monNomDeVolume**
> (le nom du *mapper* a été spécifié lors de l'*ouverture* avec *cryptsetup luksOpen /dev/sdX1* ***monNomDeVolume***).

```
# Création du point de montage
mkdir /mnt/monDossier

# Montage du mapper
```

```
mount -v /dev/mapper/maPartition /mnt/monDossier
```

Maintenant vous pouvez utiliser votre partition comme vous le voulez via le dossier /mnt/monDossier.

Démontage

Avant de verrouiller à nouveau la partition il est nécessaire d'enlever le point de montage.

```
# Démontage du mapper
umount -v /dev/mapper/monVolume


# ou
umount -v /mnt/monVolume
```

Verrouillage

```
cryptsetup -v luksClose maPartition
```

Revision #20
Created 5 June 2023 08:10:29 by gpatruno
Updated 6 June 2023 09:44:19 by gpatruno