Chiffrement d'une partition (LUKS)

Même s'il est totalement recommandé de le faire sur une nouvelle partition afin d'éviter tout problème de perte de données, cryptsetup peut être utilisé sur une partition fraîchement crée ou une déjà existante.

Ce tuto est fait en étant déjà root, si vous ne l'êtes pas rajouter le mot clé "sudo" devant vos commandes en cas de manque de droit

> La partition que nous allons chiffrer n'est pas essentiel au démarrage, cela veut dire qu'elle n'est pas montée automatiquement et aucun mot de passe ne sera demandé lors du démarrage, pour la montée automatiquement voir du côté de /etc/fstab

Installer le paquet cryptsetup si vous ne l'avez pas avec la commande :

```
apt install cryptsetup -y
```

Les disques linux se nomment très souvent comme /dev/sda avec comme partitions (/dev/sda1, /dev/sda2 etc...)

Ces noms peuvent varier selon le type de disque vous avec, pour du nvme ça sera par exemple /dev/nvme0n1p1 etc..

Considérons que nous souhaitons chiffrer la partitions /dev/sde1, utiliser la commande :

```
```

> cryptsetup luksFormat --cipher aes-xts-plain64 --key-size 256 --hash sha256 --verify-passphrase /dev/sde1

Un Warning vous avertie que les données sur cette partitions seront écrasées, soyez sur de ne plus avoir besoin de ces dernières, ou avoir fait une sauvegarde au préalable.

> Faites attention à ne pas chiffrer les partitions de votre premier disque (/dev/sda) qui contient les fichiers de votre système, soyez certain de la partition que vous souhaitez verrouiller.

```
ATTENTION: Le périphérique /dev/sde1 contient déjà une signature pour un superblock « crypto_LUKS
».

WARNING!
========
Cette action écrasera définitivement les données sur /dev/sde1.

Are you sure? (Type 'yes' in capital letters):
```

Tapez "YES" en majuscule. Ensuite saisissez votre phrase secrète.

```
Cette action écrasera définitivement les données sur /dev/sde1.

Are you sure? (Type 'yes' in capital letters): YES
Saisissez la phrase secrète pour /dev/sde1 :
Vérifiez la phrase secrète :
root@beta:~#
```

Nous allons maintenant déchiffrer notre partition qu'on vient de chiffrer et donner un nom à notre mappage pour la partition LUKS ouverte. Faites la commande :

> cryptsetup luksOpen /dev/sde1 private_partition

Entrez la phrase secrète pour valider l'opération.

```
root@beta:~# cryptsetup luksOpen /dev/sde1 private_partition
Saisissez la phrase secrète pour /dev/sde1 :
root@beta:~#
```

Nous allons mettre notre partition chiffrée au format ext4 avec la commande :

> mkfs.ext4 /dev/mapper/private_partition

Il ne nous reste plus qu’à monter notre partition chiffrée sur le répertoire /mnt/private_partition par exemple.

Faites ces commandes là :

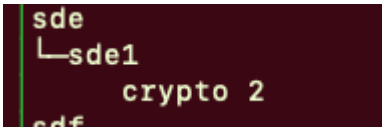
> mkdir /mnt/private_partition
> mount /dev/mapper/private_partition /mnt/private_partition

Pour vérrouiller à nouveau la partition, il faut démonter le système de fichier avant, ensuite refermer notre partition.

Faites ces commandes là :

> umount /mnt/private_partition
> cryptsetup luksClose private_partition

Avec l'option '-f' de lsblk vous pourrez voir les partitions chiffrées de votre machine, qui apparaissent avec le mot clé crypto_LUKS ou crypto 2



Revision #8
Created 5 February 2025 16:43:36 by Bibi
Updated 15 February 2025 16:15:39 by Bibi