|  |  |
| --- | --- |
| LUKS: Disk Encryption - Guardian Project | Chiffrement d’un disque dur LUKS |

# Introduction

**dm-crypt**

dm-crypt est un **sous-système de chiffrement de disque transparent** dans les versions 2.6 et ultérieures du noyau Linux. Il **fait partie de l'infrastructure du mappeur de périphériques** (dm) et utilise les routines cryptographiques de l'API Crypto du noyau.

**Mappeur de périphérique**

Le mappeur de périphériques (*device mapper*) est un cadritiel (*framework*) fourni par le noyau Linux afin de **mapper des périphériques de blocs physiques sur des périphériques de blocs virtuels de niveau supérieur**.   
Il constitue la **base du gestionnaire de volumes logiques** (LVM), des **RAID logiciels** et du **chiffrement de disque** **dm‑crypt** , et offre des fonctionnalités supplémentaires telles que les **instantanés du système de fichiers**.

Le mappeur de périphérique fonctionne en **transmettant les données d'un périphérique de bloc virtuel**, fourni par le mappeur de périphérique lui-même, **à un autre périphérique de bloc**.  
 Les **données peuvent également être modifiées** **en transition**, ce qui est effectué, par exemple, dans le cas d'un mappeur de périphérique fournissant un chiffrement de disque ou une simulation de comportement matériel non fiable.

**Frontaux (*frontend*)**

La cible du mappeur de périphérique **dm-crypt réside entièrement dans l'espace du noyau** et ne concerne que le chiffrement du périphérique de bloc - elle n'interprète aucune donnée elle-même. Il s'appuie sur les frontaux de l'espace utilisateur pour créer et activer des volumes chiffrés et gérer l'authentification.

Au moins **deux interfaces sont actuellement disponibles** … **cryptsetup** et **cryptmount**.

**cryptsetup**cryptsetup est un utilitaire utilisé pour **configurer facilement le chiffrement du disque** basé sur le module du noyau dm‑crypt.

**cryptmount**L'interface cryptmount est une **alternative à l'outil cryptsetup** qui permet à **tout utilisateur de monter et de démonter** un système de fichiers dm-crypt en cas de besoin, **sans avoir besoin de privilèges de super-utilisateur** une fois que le périphérique a été configuré par un super-utilisateur.

# Installation de cryptsetup

cryptsetup est disponible dans le référentiel de paquets officiel de Debian.   
Ainsi, on peut l'installer facilement sur l’hôte.

On met à jour le cache du référentiel de paquets APT …  
**>> sudo apt update**

On met à jour le système …  
**>> sudo apt upgrade -y**

On installe l’utilitaire cryptsetup …  
**>> sudo apt install cryptsetup --install-suggests**

L'utilitaire cryptsetup est utilisé comme suit …  
**>> sudo** **cryptsetup <option(s)> <Action> <Action-specific-options> <Device> <dm-name**>

# Chiffrement d’un disque

Pour trouver le nom ou l'ID du périphérique de stockage …  
**>> sudo lsblk**

**Chiffrement d’un périphérique avec LUKS**

Pour chiffrer le périphérique de stockage /dev/sdb (ou avec l’UUID bf979925-5ae9-46e9-a49e-c9540b8c373d) avec une phrase secrète …  
**>> sudo cryptsetup --verbose --verify-passphrase luksFormat /dev/sdb**ou **>> sudo cryptsetup -v -y luksFormat /dev/sdb**

Le périphérique de stockage est maintenant chiffré avec LUKS et la phrase secrète LUKS est définie.  
Une phrase peuvent contenir jusqu'à 512 caractères.

**Ouverture d’un périphérique de stockage chiffré**

Une fois que le périphérique de stockage est chiffré, on peut le déchiffrer et le lier (*map*) en tant que data sur l’hôte …  
**>> sudo cryptsetup --verbose open /dev/sdb data  
>> sudo cryptsetup -v open /dev/sdb data**

Il existe une autre commande pourchiffrer et le lier en tant que data sur l’hôte …  
**>> sudo cryptsetup --verbose luksOpen /dev/sdb data  
>> sudo cryptsetup -v luksOpen /dev/sdb data**

On peut constater qu’un nouveau périphérique de stockage de données a été créé et il est du type crypt …  
**>> sudo lsblk**

On peut utiliser la commande ls -l pour afficher les détails du mappage …  
**>> ls -l /dev/mapper/data**

On peut utiliser la commande qui suit pour afficher l'état du mappage …  
**>> sudo** **cryptsetup --verbose status data**ou **>> sudo** **cryptsetup -v status data**

On peut utiliser la commande cryptsetup luksDump afin de vérifier que le périphérique a été formaté avec succès pour le chiffrement …  
**>> sudo** **cryptsetup luksDump /dev/sdb**

**Création d'un système de fichiers déchiffré**

Une fois que l’on a déchiffré un périphérique de stockage et l'avoir lié (*map*) en tant que périphérique de stockage de données, on peut utiliser les données du périphérique de stockage lié comme d'habitude.

On écrit des zéros sur la partition chiffrée LUKS …  
**>> sudo** **dd if=/dev/zero of=/dev/mapper/data**

**Remarque** …  
La commande dd peut prendre plusieurs heures.   
Il est recommandé d'utiliser la commande pv pour surveiller la progression …  
**>> sudo pv -tpreb /dev/zero | sudo dd of=/dev/mapper/data bs=128M**

**Remarque** …  
Il est possible que l’on doive installer l’utilitaire pv.

Pour créer un système de fichiers ext4 déchiffrées du périphérique de stockage identifié comme data …  
**>> sudo mkfs.ext4 -L data /dev/mapper/data**

**Montage du système de fichiers déchiffré**

Une fois que l’on a créé un système de fichiers sur le périphérique de stockage, on peut le monter sur l’hôte comme d'habitude.

Tout d'abord, on crée un point de montage /mnt/data …  
**>> sudo mkdir --verbose /mnt/data**ou **>> sudo mkdir -v /mnt/data**

Ensuite, on monte data sur le répertoire /mnt/data …  
**>> sudo mount /dev/mapper/data /mnt/data**

Comme on peut le constater, le périphérique de stockage data déchiffré est monté dans le répertoire /mnt/data …  
**>> sudo lsblk**

**Démontage du système de fichiers déchiffré**

Une fois que l’on a terminé de travailler avec le périphérique de stockage data déchiffré, on peut le démonter …  
**>> sudo umount /dev/mapper/data**

Comme on peut le voir, le périphérique de stockage data déchiffré n’est plus monté sur le répertoire /data …  
**>> sudo lsblk**

**Fermeture du périphérique de stockage déchiffré**

Pour fermer le périphérique de stockage data déchiffré …  
**>> sudo cryptsetup --verbose close data**ou  
**>> sudo cryptsetup --verbose luksClose data**

Comme on peut le constater, les données déchiffrées du périphérique de stockage ne sont plus disponibles.  
**>> sudo lsblk**

**Modification de la phrase secrète LUKS**

Pour modifier la phrase secrète LUKS du périphérique de stockage chiffré …  
**>> sudo cryptsetup --verbose luksChangeKey /dev/sdb**ou **>> sudo cryptsetup -v luksChangeKey /dev/sdb**

**Remarque** …  
L’opération peut prendre un certain temps.

**Ajout d'une phrase secrète**

On peut ajouter une nouvelle phrase secrète à celle déjà existante …  
**>> sudo cryptsetup luksAddKey /dev/sdb**

On peut alors accéder au volume chiffré …  
**>> sudo cryptsetup --verbose open /dev/sdb data**ou **>> sudo cryptsetup -v open /dev/sdb data**

On peut saisir le nouveau mot de passe.