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

Table des matières

[Introduction 2](#_Toc81401538)

[dm-crypt 2](#_Toc81401539)

[Mappeur de périphérique 3](#_Toc81401540)

[Frontaux (*frontend*) 3](#_Toc81401541)

[Installation de cryptsetup 4](#_Toc81401542)

[Chiffrement d’un disque 5](#_Toc81401543)

[Chiffrement d’un périphérique avec LUKS 5](#_Toc81401544)

[Ouverture d’un périphérique de stockage chiffré 6](#_Toc81401545)

[Création d'un système de fichiers déchiffré 8](#_Toc81401546)

[Montage du système de fichiers déchiffré 8](#_Toc81401547)

[Démontage du système de fichiers déchiffré 9](#_Toc81401548)

[Fermeture du périphérique de stockage déchiffré 9](#_Toc81401549)

[Modification de la phrase secrète LUKS 10](#_Toc81401550)

[Ajout d'une phrase secrète 10](#_Toc81401551)

[Annexe 01 Chiffrement lors de l’installation de Debian 11](#_Toc81401552)

|  |
| --- |
| **Avertissement** …  Les manipulations présentées ici ont le potentiel de rendre le système inopérant (*inbootable*), de détruire des données si des erreurs sont faites dans l'exécution des commandes. il est fortement conseillé d’effectuer une sauvegarde de l'ensemble des données.  Les opérations d'écriture de données aléatoires sur une partition, de création d'un conteneur chiffré, de formatage provoquent la destruction de toutes les données contenues sur la partition visée. |

# Introduction

Le chiffrement de disque est une technologie qui **protège l’information en la transformant en un code illisible** qui **ne** **peut pas être déchiffré facilement par les personnes qui n’y sont pas autorisées**. Le chiffrement de disque utilise un logiciel de chiffrement de disque ou le matériel de chiffrement de disque pour **chiffrer chaque bit des données** sur un disque dur ou un volume.

**LUKS** ou *Linux Unified Key Setup* est la **norme pour le chiffrement de disque dur Linux**.   
En fournissant un **format** **standard sur disque**, il facilite non seulement la **compatibilité entre les distributions**, mais fournit également une **gestion sécurisée de plusieurs mots de passe utilisateur**.

LUKS stocke toutes les **informations de configuration nécessaires dans l'en-tête de partition**, permettant de **transporter ou de migrer les données** de manière transparente.

Alors que la plupart des logiciels de chiffrement de disque implémentent des formats différents, incompatibles et non documentés, LUKS implémente un **format de disque standard indépendant de la plate-forme** pour une utilisation dans divers outils.   
Cela **facilite non seulement la compatibilité** et **l'interopérabilité** entre les différents programmes, mais **garantit également qu'ils implémentent tous la gestion des mots de passe** de manière **sécurisée** et **documentée**.

LUKS utilise **dm-crypt comme dorsale** (*backend*) de chiffrement de disque.

Un périphérique de stockage peut être chiffré avec LUKS selon **2** **méthodes** **différentes** …

* **Chiffrement par clé**Une **clé de chiffrement** (stockée dans un fichier) est utilisée pour chiffrer le périphérique de stockage.   
  Pour **déchiffrer** le périphérique, la **clé de chiffrement est requise**.   
  Si un périphérique est chiffré de cette manière, on **peut automatiquement déchiffrer le périphérique de stockage au démarrage et le monter**.   
  Cette méthode est bonne pour les serveurs.
* **Chiffrement basé sur la phrase secrète**À l’aide de cette méthode, le périphérique de stockage sera **chiffré avec une phrase secrète**.   
  On sera **obligé de saisir la phrase secrète** à chaque fois que l’on souhaite déchiffrer le périphérique de stockage et l'utiliser.   
  Si on chiffre le périphérique de stockage système de cette manière, la **phrase secrète sera demandée à chaque** **démarrage de l’hôte**.  
  On **ne pourra pas déchiffrer et monter automatiquement le périphérique au démarrage**. Donc, cette méthode est bonne pour les stations de travail.

Le chiffrement basé par la phrase secrète peut également être **utilisé pour les périphériques de stockage externes** (disques durs, SSD externes et clés USB). Comme ces périphériques ne seront pas connectés à un hôte spécifique en permanence et qu’on n'aura **pas besoin de les monter automatiquement**, cette méthode est très appropriée pour ces types de périphériques de stockage.

Pour chiffrer un disque, on doit **installer cryptsetup sur l’hôte** et **chiffrer un système de fichiers** avec le chiffrement de la phrase secrète LUKS.

## 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**.

dm-crypt a été conçu pour **prendre en charge des modes de fonctionnement avancés**, tels que XTS , LRW et ESSIV afin d'éviter les **attaques par filigrane**.

dm-crypt est **implémenté en tant que cible de mappeur de périphérique** et peut être empilé sur d'autres transformations de mappeur de périphérique.   
Il peut ainsi chiffrer des disques entiers, y compris …

* les **supports amovibles** ;
* des **partitions** ;
* des **volumes RAID logiciels** ;
* des **volumes logiques**   
  ainsi que
* des **fichiers**.

Il **apparaît comme un périphérique de** bloc, qui peut être utilisé pour sauvegarder des systèmes de fichiers, une partition d’échange (*swap*) ou comme un volume physique LVM.

Certaines distributions Linux prennent en charge l'utilisation de dm-crypt sur le système de fichiers racine.   
Ces **distributions utilisent initrd pour inviter l'utilisateur à saisir une phrase secrète** sur la console ou à insérer une carte à puce avant le processus de démarrage normal.

## Mappeur de périphérique

Le mappeur de périphériques (*device mapper*) est un cadriciel (*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**.

L'interface cryptsetup (en ligne de commande) **n'écrit aucun en-tête sur le volume chiffré** et ne fournit donc que l'essentiel …

* les **paramètres de chiffrement doivent être fournis chaque fois que le disque est monté** (bien qu'ils soient généralement utilisés avec des scripts automatisés)  
  et
* **uniquement une clé peut être utilisée par volume** ; la clé de chiffrement symétrique est directement dérivée de la phrase secrète fournie .

Parce qu'il manque un sel, l'utilisation de **cryptsetup est moins sécurisée** dans ce mode que ce n'est le cas avec   
Linux Unified Key Setup (LUKS).   
Cependant, la **simplicité de cryptsetup le rend utile** lorsqu'il est **combiné avec un logiciel tiers**, par exemple, avec l'authentification par carte à puce.

cryptsetup fournit également des **commandes pour gérer le format LUKS sur disque**.   
Ce format fournit des **fonctionnalités supplémentaires telles que la gestion des clés et l'extension des clés** (à l'aide de PBKDF2), et se souvient de la configuration du volume chiffré lors des redémarrages.

**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 superutilisateur** une fois que le périphérique a été configuré par un superutilisateur.

### Caractéristiques

Le fait qu'un **logiciel de chiffrement de disque** (chiffrement de volume) **comme dm-crypt** ne traite que le chiffrement transparent de périphériques de blocs abstraits lui donne **beaucoup de flexibilité**.   
Cela signifie qu'il peut être utilisé pour chiffrer tous les systèmes de fichiers sauvegardés sur disque pris en charge par le système d'exploitation, ainsi que l'espace d'échange (*swap*) ; les barrières d'écriture implémentées par les systèmes de fichiers sont préservées.  
Les volumes chiffrés peuvent être **stockés sur des partitions de disque**, des **volumes logiques**, des **disques entiers** ainsi que des **images de disque sauvegardées sur fichier**.   
dm-crypt peut également être configuré pour chiffrer les volumes RAID et les volumes physiques LVM .

**dm-crypt** peut également être configuré pour **fournir une authentification de pré-démarrage à l’aide d’un initrd**, chiffrant ainsi toutes les données sur un hôte - à l'exception du chargeur de démarrage, du noyau et de l'image initrd elle-même.

# 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> <dmname**>

# Chiffrement d’un disque

Afin de chiffrer un périphérique de stockage, on doit connaître le nom ou l'ID de ce périphérique de stockage.

Pour trouver le nom ou l'ID du périphérique de stockage …  
**>> sudo lsblk   
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT  
sda 8:0 0 40G 0 disk  
 sda1 8:1 0 39G 0 part /  
 sda2 8:2 0 1K 0 part  
 sda5 8:5 0 975M 0 part [SWAP]  
sdb 8:16 0 40G 0 disk  
 sdb1 8:17 0 37,3G 0 part  
sdc 8:32 0 40G 0 disk  
sdd 8:48 0 40G 0 disk  
sr0 11:0 1 377M 0 rom**

## 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  
>> sudo cryptsetup -v -y luksFormat /dev/sdb  
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.**

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  
Saisissez la phrase secrète pour /dev/sdb : …  
Emplacement de clé 0 déverrouillé.  
Opération réussie.**

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**  
**Saisissez la phrase secrète pour /dev/sdb : …  
Emplacement de clé 0 déverrouillé.  
Opération réussie.**

On peut constater qu’un nouveau périphérique de stockage de données a été créé et il est du type crypt …  
**>> sudo lsblk  
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT…  
…  
sdb 8:16 0 40G 0 disk  
 data 254:0 0 40G 0 crypt  
…**

On peut utiliser la commande ls -l pour afficher les détails du mappage …  
**>> ls -l /dev/mapper/data  
lrwxrwxrwx 1 root root 7 29 aoû 14:08 /dev/mapper/data -> ../dm-0**

On peut utiliser la commande qui suit pour afficher l'état du mappage …  
**>> sudo** **cryptsetup -v status data  
/dev/mapper/data is active.  
 type: LUKS2  
 cipher: aes-xts-plain64  
 keysize: 512 bits  
 key location: keyring  
 device: /dev/sdb  
 sector size: 512  
 offset: 32768 sectors  
 size: 83853312 sectors  
 mode: read/write  
Opération réussie.**

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  
LUKS header information**

**Version: 2**

**Epoch: 7**

**Metadata area: 16384 [bytes]**

**Keyslots area: 16744448 [bytes]**

**UUID: df24a7e4-8f0d-4f52-8455-3cb466fabba0**

**Label: (no label)**

**Subsystem: (no subsystem)**

**Flags: (no flags)**

**Data segments:**

**0: crypt**

**offset: 16777216 [bytes]**

**length: (whole device)**

**cipher: aes-xts-plain64**

**sector: 512 [bytes]**

**Keyslots:**

**0: luks2**

**Key: 512 bits**

**Priority: normal**

**Cipher: aes-xts-plain64**

**Cipher key: 512 bits**

**PBKDF: argon2i**

**Time cost: 4**

**Memory: 395625**

**Threads: 1**

**Salt: ca 60 86 35 82 92 fb 48 fd 25 02 88 9a 01 33 a5**

**0f 42 32 8a 8b 92 08 7e e9 79 7f 84 4c 12 8e 75**

**…**

**Tokens:**

**Digests:**

**0: pbkdf2**

**Hash: sha256**

**Iterations: 85780**

**Salt: f1 9e 0f 58 5b 21 31 0e 2e 1a 07 2e 48 ac eb aa**

**26 b2 a7 e0 34 89 e7 87 2c c6 94 8c 6a c9 96 a5**

**Digest: 41 94 eb 3a f8 24 d6 80 fd 1e a8 34 90 9c 08 a4**

**75 73 3d 5e e1 4d 77 79 18 8c c1 38 67 d9 3e 94**

## 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**

Cette commande allouera des données de bloc avec des zéros.   
Cela garantit que le monde extérieur verra cela comme des données aléatoires, c'est-à-dire qu'il protègera contre la divulgation des modèles d'utilisation.

**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**

Pour créer un système de fichiers ext4 déchiffrées du périphérique de stockage identifié comme data …  
**>> sudo mkfs.ext4 -L data /dev/mapper/data  
mke2fs 1.46.2 (28-Feb-2021)  
Creating filesystem with 10481664 4k blocks and 2621440 inodes  
Filesystem UUID: 301e2354-3f38-4df6-846e-8984573b9f11  
Superblock backups stored on blocks:  
 32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,  
 4096000, 7962624  
  
Allocating group tables: done  
Writing inode tables: done  
Creating journal (65536 blocks): done  
Writing superblocks and filesystem accounting information: done**

Alternativement. On peut également utiliser la commande …  
**>> sudo badblocks -wt random /dev/sdb1**

## 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 -v /mnt/data  
mkdir: création du répertoire '/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  
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT…  
sdb 8:16 0 40G 0 disk  
 data 254:0 0 40G 0 crypt /mnt/data  
…**

## 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  
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT…  
…  
sdb 8:16 0 40G 0 disk  
 data 254:0 0 40G 0 crypt  
…**

## Fermeture du périphérique de stockage déchiffré

Il est également possible de fermer le périphérique de stockage data déchiffré.  
La prochaine fois que l’on voudra utiliser le périphérique de stockage, il faudra le déchiffrer à nouveau si on le ferme.

Pour fermer le périphérique de stockage data déchiffré …  
**>> sudo cryptsetup -v close data  
Opération réussie.**ou  
**>> sudo cryptsetup -v luksClose data  
Opération réussie.**

Comme on peut le constater, les données déchiffrées du périphérique de stockage ne sont plus disponibles.  
**>> sudo lsblk  
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT…  
…  
sdb 8:16 0 40G 0 disk  
 data 254:0 0 40G 0 disk  
…**

## Modification de la phrase secrète LUKS

Il est également possible de modifier la phrase secrète LUKS des périphériques de stockage chiffrés LUKS.

Pour modifier la phrase secrète LUKS du périphérique de stockage chiffré …  
**>> sudo cryptsetup -v luksChangeKey /dev/sdb  
Entrez la phrase secrète à changer : …  
Emplacement de clé 1 déverrouillé.  
Entrez la nouvelle phrase secrète : …  
Vérifiez la phrase secrète : …  
Emplacement de clef 0 créé.  
Opération réussie.**

**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  
Entrez une phrase secrète existante : …  
Entrez une nouvelle phrase secrète pour l'emplacement de clé : …  
Vérifiez la phrase secrète : …**

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

On peut saisir le nouveau mot de passe.

# Annexe 01 Chiffrement lors de l’installation de Debian

Il est possible de **chiffrer un disque lors de l’installation** d’un nouveau système Debian.

Lors d’une installation standard, l’installateur propose les étapes suivantes …

* Choix de la langue ;
* Configuration du clavier ;
* Détection et montage du support d’installation ;
* Chargement des composants depuis le support d’installation ;
* Détection et configuration du matériel réseau ;
* Création des utilisateurs et des mots de passe ;
* Configuration de l’horloge ;
* **Détection des disques et partitionnement** ;
* Installation de base ;
* Configuration de l’outil de gestion des paquets ;
* Choix et installation des logiciels ;
* Installation du programme de démarrage GRUB ;
* Fin de l’installation et redémarrage du système.

C’est lors de l’étape de la détection des disques et partitionnement que la configuration du chiffrement s’effectue.

| **Étapes** | |
| --- | --- |
| **Partitionner les disques**  On choisit l’option … **Assisté – utiliser tout un disque avec LVM Chiffré** |  |
| **Partitionner les disques**  On sélectionne le disque à chiffrer … |  |
| **Partitionner les disques**  On sélectionne de ne créer qu’une seule partition, partition qui occupe tout l’espace disponible … |  |
| **Partitionner les disques**  On confirme la modification de la table des partitions … |  |
| **Partitionner les disques**  Lors de cette étape, l’installateur écrit des données aléatoires sur la partition. Ceci est une mesure de sécurité importante.  Cette étape de l’installation peut être longue … |  |
| **Partitionner les disques**  On choisit, lors de cette étape une phrase secrète pour l’accès au disque. Ce mot de passe peut être différent (cela est préférable) de celui de l’utilisateur par défaut ou de root. Ce mot de passe sera demandé lors du démarrage de la station … |  |
| **Partitionner les disques**  On peut, à cette étape, choisir la portion du disque qui sera chiffré. Il peut s’agir du disque entier ou seulement une portion de l’espace disponible … |  |
| **Partitionner les disques**  L’installateur propose le bilan de la table de partition et des points de montage. On confirme le tout avec … **Terminer le partitionnement et appliquer les changements** … |  |
| **Partitionner les disques**  On doit confirmer à cette étape les choix effectués lors des étapes précédentes … |  |
| **Démarrage du système**  À chaque démarrage, le système demandera de saisir le mot de passe pour accéder à la partition chiffrée et démarrer le système. Sans ce mot de passe, il sera impossible d’accéder aux données présentes dur le disque  (donc l’incapacité de charger le système d’exploitation) … |  |