Chiffrement de surface des disques : Linux

Matthieu Herrb

10 mai 2019

Introduction

- Menace : vol d'un ordinateur ou d'un support contenant des données sensibles.
- Chiffrement des disques obligatoire dans unités CNRS depuis le 1er janvier 2013...
  https://aresu.dsi.cnrs.fr/spip.php?rubrique99
- Techniques retenues :
  - pour Linux : dm-crypt + LUKS sur toutes les partitions
    Applicable simplement sur distributions récentes
  - Supports amovibles et conteneurs : VeraCrypt / Zed !

Choix des outils de chiffrement

Attention aux outils mal utilisés :

- risque de perte de données
- risque de failles de sécurité
- problème de compétences

S'en tenir à des technologies éprouvées et largement déployées.

Pas de chiffrement sans sauvegardes !

Le risque principal est la perte des données.

Le chiffrement aggrave un peu le problème :

- risque de perte de la clé de chiffrement (recouvrement)
- erreurs de lecture $\rightarrow$ perte de la possibilité de déchiffrer

$\Rightarrow$ Commencer par mettre en place une solution de sauvegarde

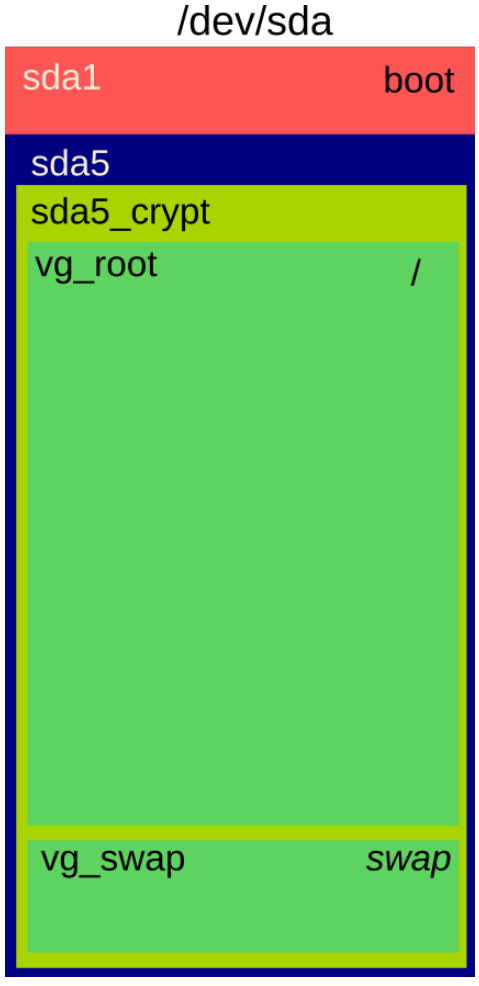
La technologie dm-crypt/LUKS

Device mapper : gestionnaire de périphériques en mode bloc virtuels (disques, partitions)

LVM2 : Logical Volume Manager (v2) : gestionnaire de partitions logiques basé sur device mapper

dm-crypt : chiffrement de périphériques virtuels en mode bloc

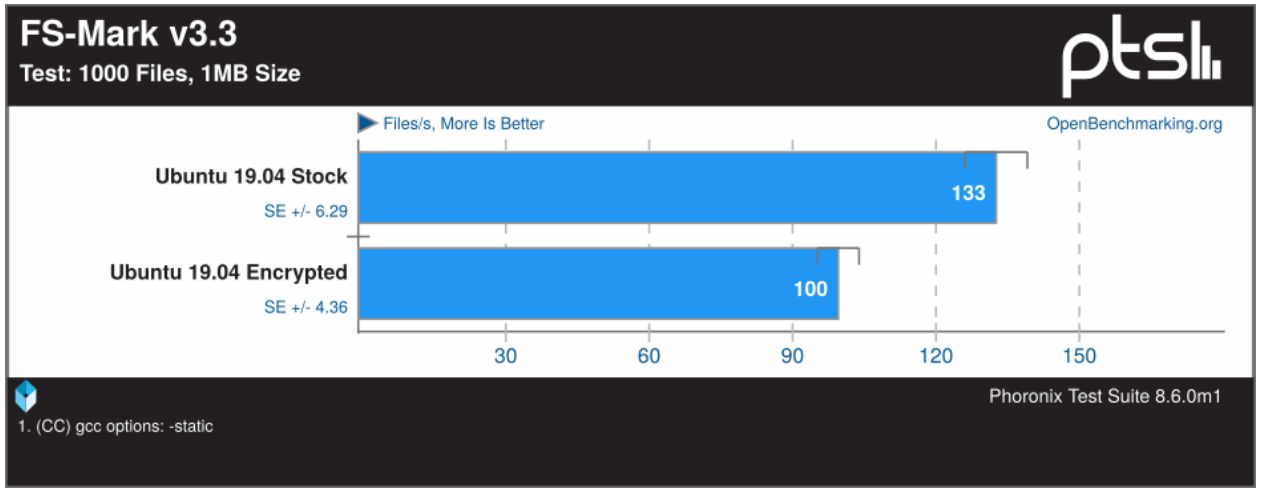
LUKS : Linux Unified Key Setup : standard de gestion du chiffrement

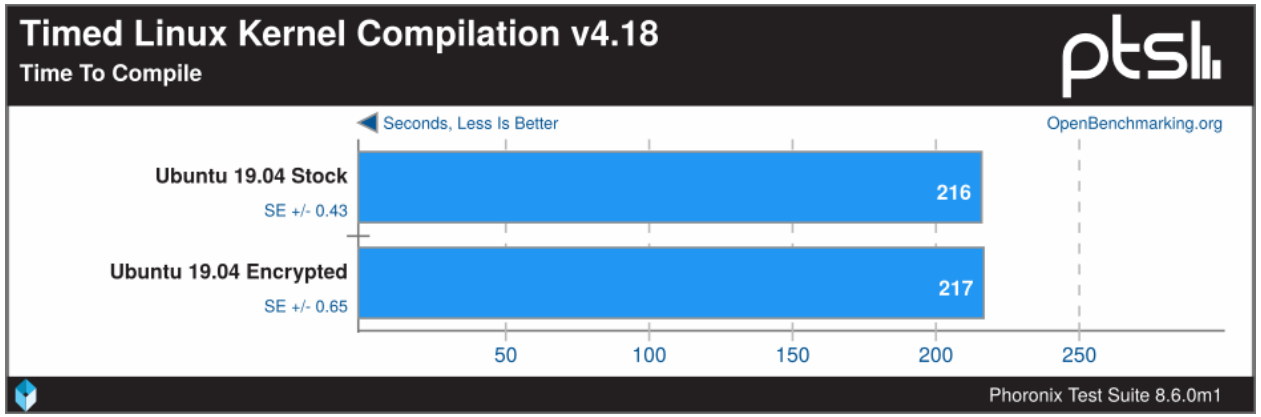


Utilise le mode XTS-AES avec des clés de 256 ou 512 bits.

Performances

Ubuntu 19.04



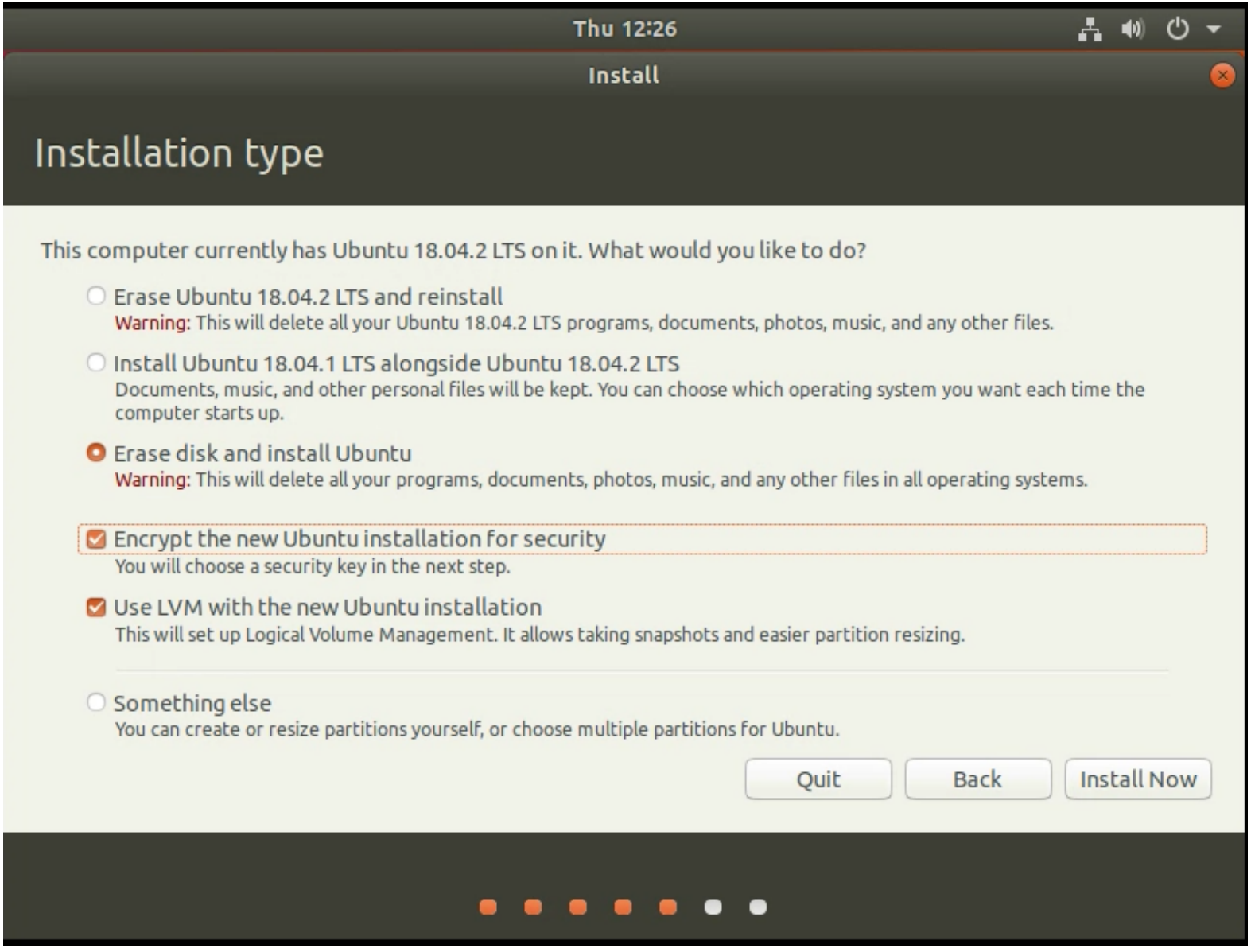


https://www.phoronix.com/scan.php?page=article&item=2019-linux-encrypt

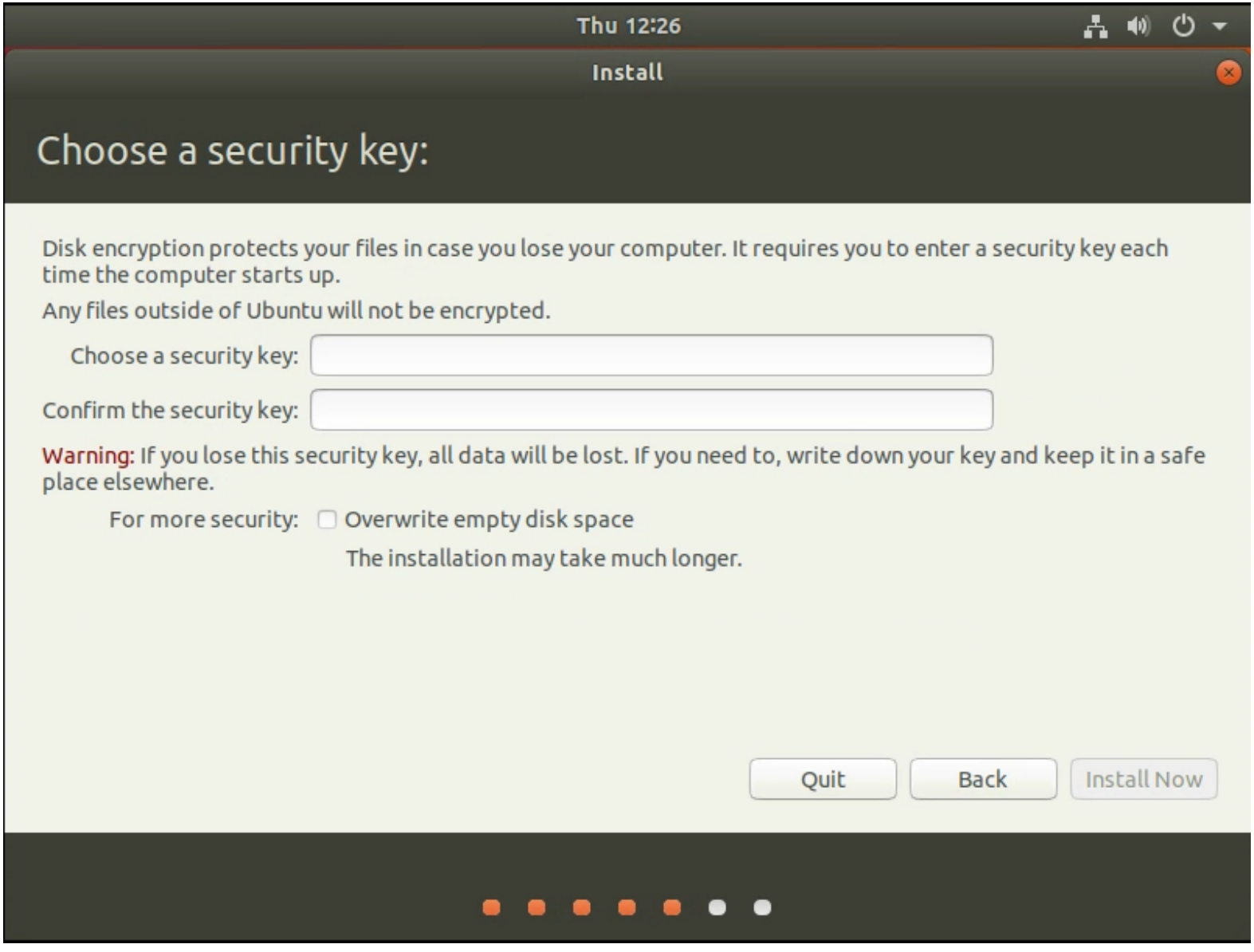
Installation Ubuntu 18.04

- Choisir l'installation sur un disque avec volume LVM chiffré
- Spécifier une phrase secrète
- Après le 1er reboot, créer une copie de sauvegarde de l'entête du volume
- Éventuellement définir une phrase secrète additionnelle.

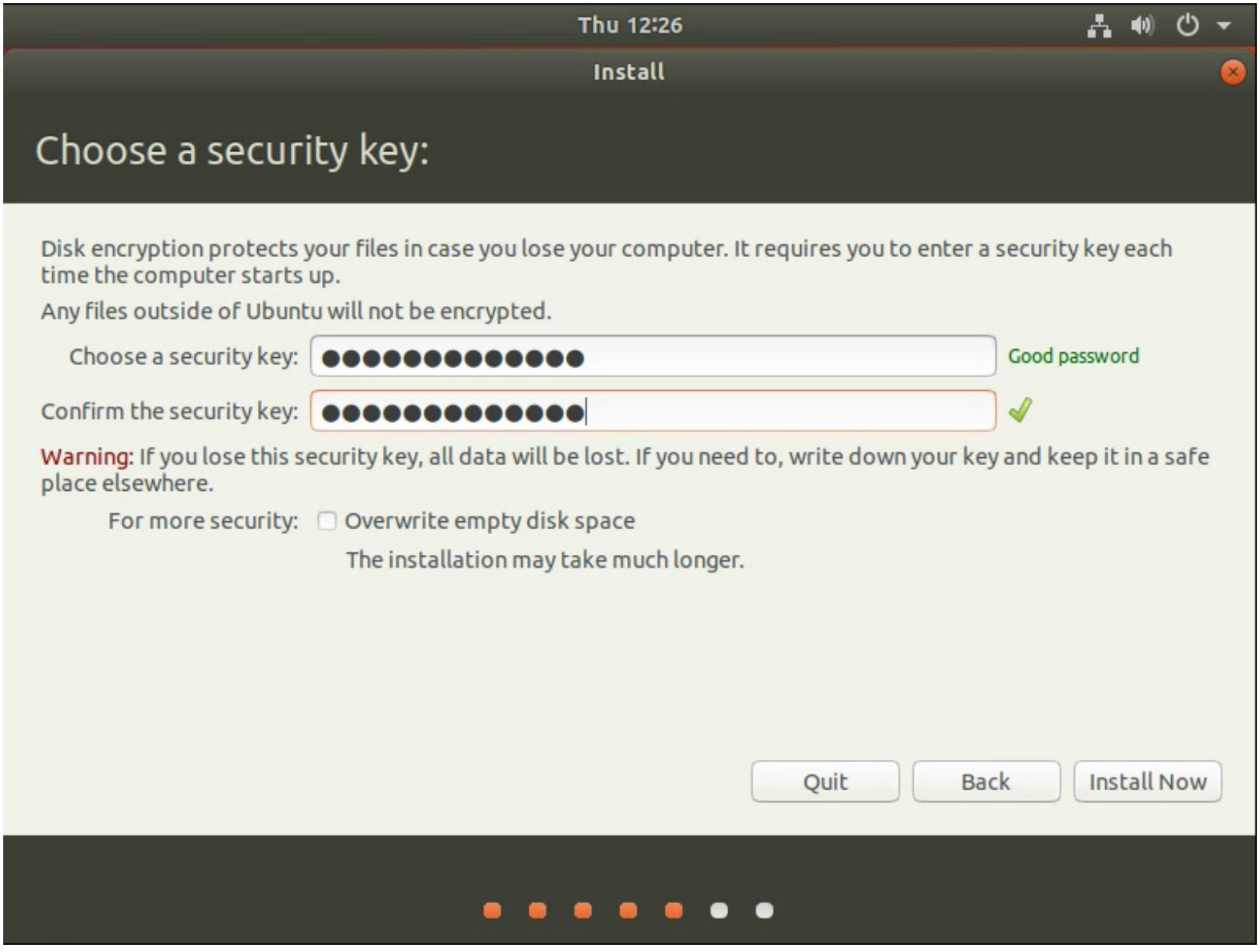
Choisir un disque avec volume LVM chiffré :



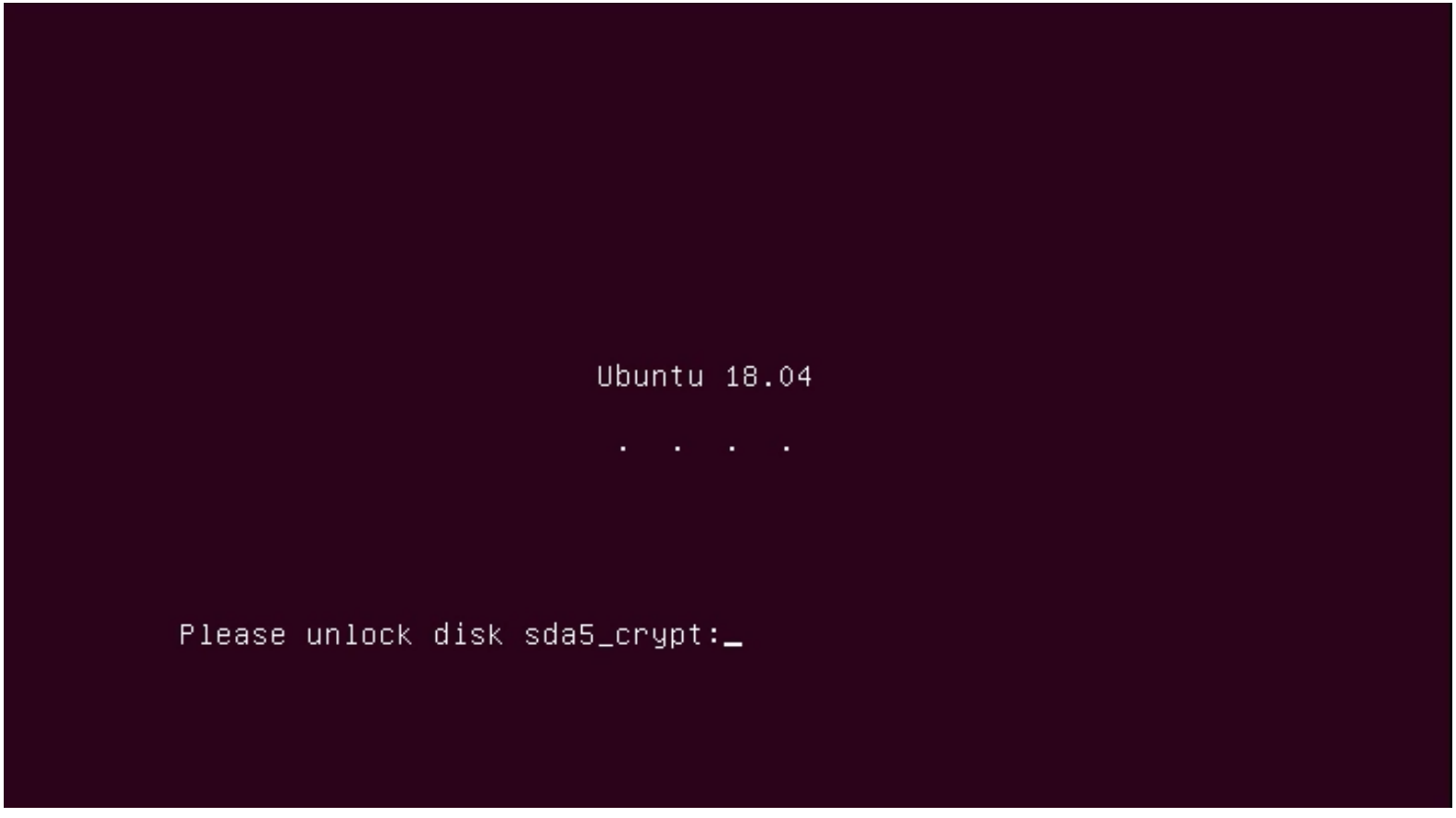
Spécifier une phrase secrète :



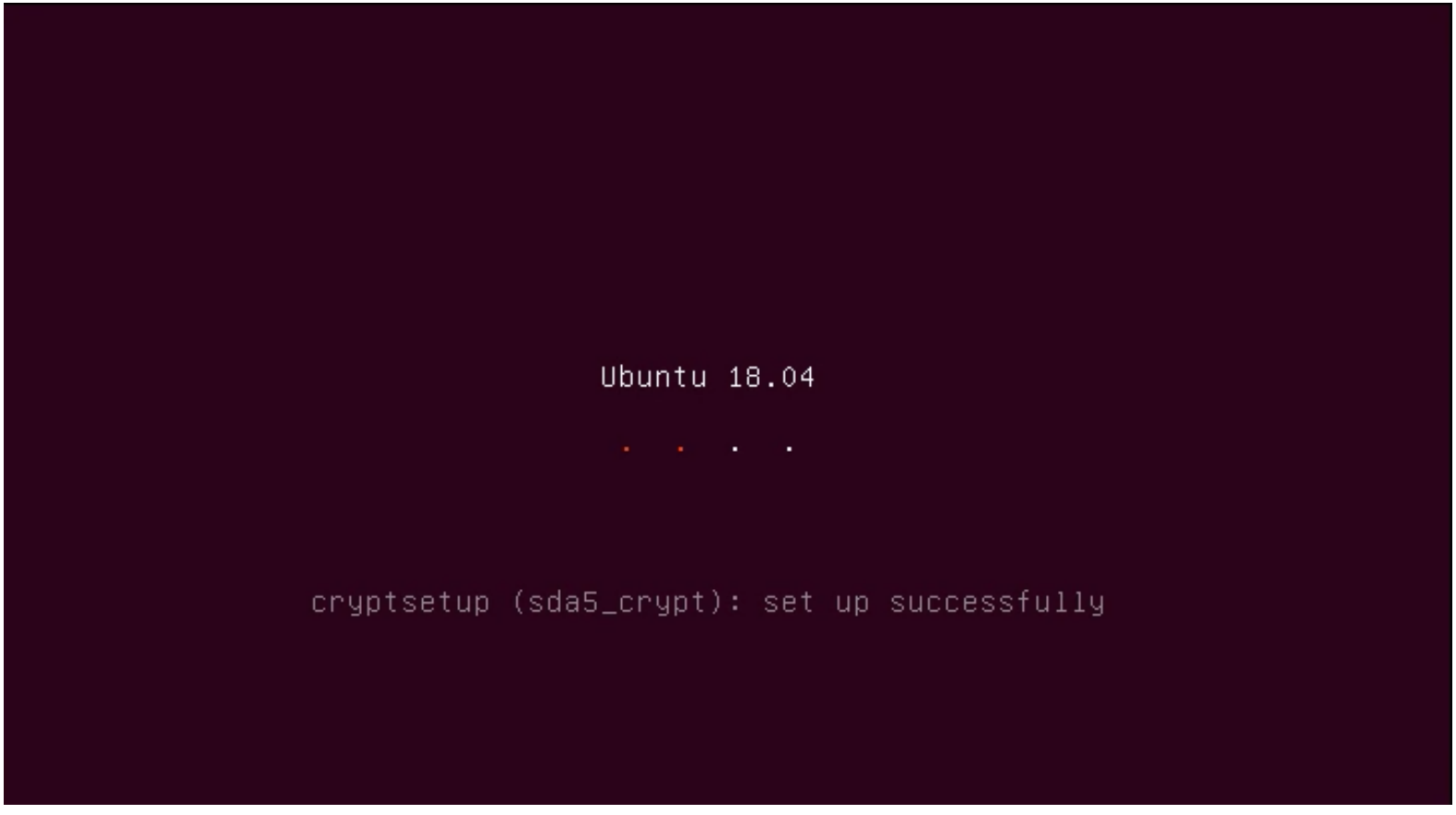
Confirmer la phrase secrète :



Démarrage du système 1/2



Démarrage du système 2/2



Séquestre de l'entête (clé de chiffrement)

luksHeaderBackup

```
cryptsetup luksHeaderBackup /dev/sda5 \
       --header-backup-file /tmp/HeaderBackup.img
```

Puis copier le fichier `HeaderBackup` vers un endroit sûr.

Ajout de phrases secrètes supplémentaires

luksAddKey

```
cryptsetup luksAddKey /dev/sda5
```

LUKS permet de stocker jusqu'à 8 phrases secrètes.

Recouvrement

Avec la phrase secrète de l'admin

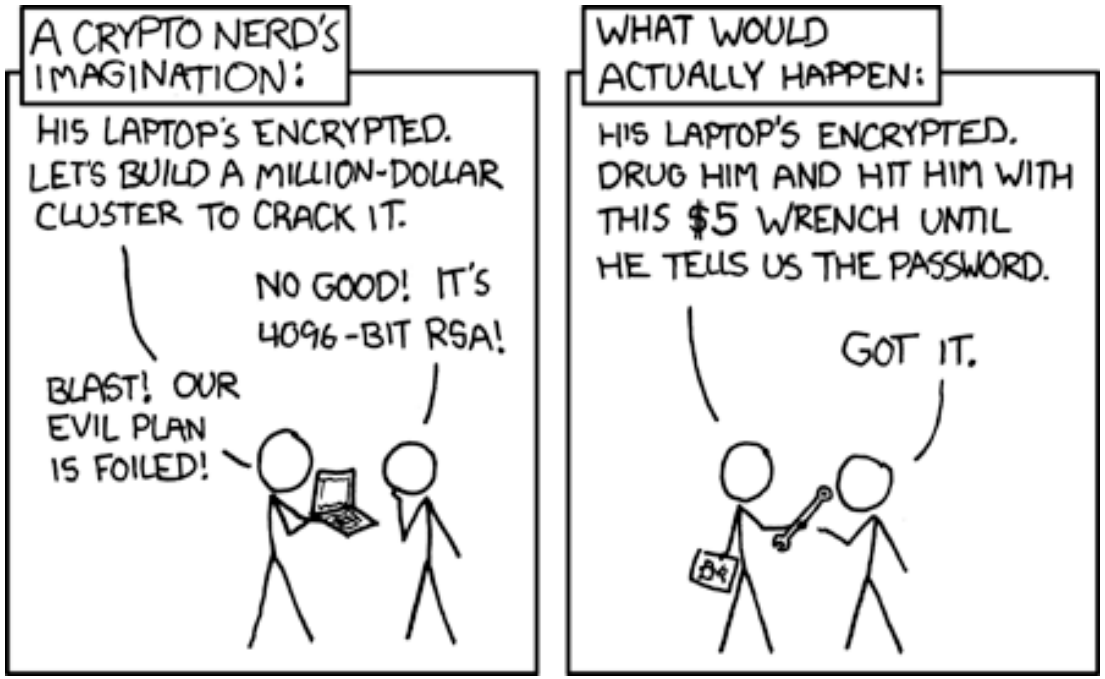
- créer une phrase secrète pour le service informatique.
- si l'utilisateur à oublié la sienne :
  1. démarrer la machine avec la phrase secrète du service informatique
  2. supprimer le slot correspondant à la clé oubliée (luksKillSlot)
  3. créer une nouvelle phrase secrète (luksAddKey)

Restauration de l'entête

- si la clé secrète de l'admin a été supprimée
- ou si l'entête de chiffrement est vérolée...
  1. connecter le disque à une autre machine
  2. restaurer l'entête à partir de la sauvegarde avec `luksHeaderRestore`

Précautions / Limitations

- Configurer le verrouillage de la session si mise en veille.
- Pas possible d'authentifier l'utilisateur avant déchiffrement.
- `/boot` reste en clair (possibilité de *evil maid attack*).
- Limite à 8 passphrases dans l'entête.



Installation sur plusieurs disques

Création d'une partition chiffrée à l'aide d'une clé dérivée de la clé du disque principal :

```
/lib/cryptsetup/scripts/decrypt_derived sda5_crypt > /tmp/key.txt
cryptsetup luksFormat /dev/sdb1 /tmp/key.txt
rm /tmp/key.txt
```

Chaînage des clés via `/etc/crypttab` :

```
data /dev/sdb1 sda5_crypt \
   luks,keyscript=/lib/cryptsetup/scripts/decrypt_derived
```

Installation automatique Ubuntu

Via Preseed :

```
d-i partman-auto/method string crypto
d-i partman-crypto/passphrase string ChangeMe
d-i partman-crypto/passphrase-again string ChangeMe
d-i partman-auto/choose_recipe select boot-crypto
d-i partman-auto-lvm/new_vg_name string crypt
d-i partman-auto/expert_recipe string boot-crypto :: \
       1024 1024 1024 ext4 $primary{ } $bootable{ } \
       method{ format } format{ } \
       use_filesystem{ } filesystem{ ext4 } \
       mountpoint{ /boot } \
       .\
       3072 7500 1000000000 ext4 $lvmok{ } lv_name{ root } \
       in_vg { crypt } method{ format } format{ } \
       use_filesystem{ } filesystem{ ext4 } mountpoint{ / } \
       .\
       100% 1024 200% linux-swap $lvmok{ } lv_name{ swap } \
       in_vg { crypt } method{ swap } format{ } \
       .\
d-i partman-partitioning/confirm_write_new_label boolean true
```

Conversion sur place

`https://github.com/johndoe31415/luksipc`

Pas testé !

Supports Amovibles

En fonction de l'usage :

- lecture seulement par du Linux :
  - via Utilitaire Disque, formatter avec chiffrement
  - en ligne de commande

```
cryptsetup luksFormat /dev/sdb
cryptsetup luksOpen /dev/sdb maClefUSB
mkfs -t ext4 /dev/mapper/maClefUSB
mount /dev/mapper/maClefUSB /media/maClefUSB
...
cryptsetup luksClose maClefUSB
eject /dev/sdb
```

- partage avec autres systèmes :
  Installer VeraCrypt et chiffrer avec VeraCrypt

Attention au séquestre des mots de passe de chiffrement

Autres systèmes

- Android : chiffrement mémoire flash et carte SD à partir de la version 4.0 - pas de recouvrement
- OpenBSD : softraid(4) http://www.undeadly.org/cgi?action=article&sid=20110530221728
- FreeBSD : http://www.freebsd.org/doc/fr_FR.ISO8859-1/books/handbook/disks-encrypting.html

Références

- Chiffrement des ordinateurs et protection des smartphones professionnels, *Note du DGDR du CNRS aux DU*, Novembre 2018.
- FAQ Chiffrement, *Intranet CNRS*, Décembre 2018.
- Les règles élémentaires de sécurité - Le poste de travail, *Intranet CNRS*, mai 2012.
- dm-crypt/Device encryption, *Arch Linux Wiki*, Avril 2019.
- Linux Encrypted Filesystem with dm-crypt, *CentOS wiki*.
- Partition Chiffrée avec Cryptsetup, *Ubuntu-fr* Janvier 2018.
- Chiffrement de fichiers et de partitions avec VeraCrypt, *Ubuntu-fr*, Octobre 2018.