

Chiffrement des portables

Journée Mathrice à Rennes

2 octobre 2013

Mohammed Khabzaoui

CNRS UMR8524

Université Lille1



Plan

- *Chiffrement des portables*
- *Outil de chiffrement matériel*
 - *Disque auto-chiffrant*
- *Outils de chiffrement logiciel*
 - *FileVault pour MAC*
 - *dm-crypt pour linux*
 - *BitLocker et Truecrypt pour windows*
- *Conclusion*

Chiffrement des portables

- **Motivations**

- ✓ Nombreux vols de portables
- ✓ Données à forte valeur économique (dépôt d'un brevet)

- **Dispositif**

- ✓ Disque chiffant sur portable du marché mathinfo
- ✓ Chiffrement logiciel (BitLocker / TrueCrypt / dm-crypt / FileVault)

- **Chiffrement des disques obligatoire dans unités CNRS** : Directives et Recommandations : <https://aresu.dsi.cnrs.fr/?rubrique99>

- **Chiffrement des portables** : Mise en œuvre et utilisation <https://aresu.dsi.cnrs.fr/IMG/pdf/manuel.pdf>

Techniques

	Matériel	Win7	Win8	Linux	Mac OS
Portable DELL Portable HP	Oui Oui *	TrueCrypt	BitLocker (> windows7Pro)	dm-crypt	
PC fixe	NON			dm-crypt	
MAC	NON				FileVault

Support amovible : auto-chiffrant & TrueCrypt (compatible avec tous les OS)

Outil de chiffrement matériel

Un disque dur chiffant (Self-Encrypting Drive) est une solution matérielle de chiffrement intégral du disque.

L'authentification est nécessaire au démarrage pour déverrouiller l'accès au disque, qui est inutilisable autrement. Pour l'activer il faut utiliser un software windows "**Dell Data Protection Access**" incompatible avec Windows 8 et Linux

Pour les postes Linux, il faut un windows 7 installé sur une disque USB avec un port eSATA.

Portable DELL : suivre la documentation disponible sur le site de l'Aresu, à l'adresse :

<https://aresu.dsi.cnrs.fr/IMG/pdf/procedure-disque-chiffrant-win7-v1.pdf>

Sur le site DELL :

<http://dell.wave.com/dell-complete-hardware-self-encrypting-drivesed-solution>

Portable HP : ?

Outil de chiffrement matériel

Remarque :

Le verrouillage du disque n'est effectif que pour un cycle d'extinction complet, un simple reboot n'est pas suffisant.

Recouvrement

Déclarer un compte utilisateur ADMIN, ce dernier peut donc y être consacré. Le déverrouillage du disque passe par une étape d'authentification au démarrage.

Mac OS FileVault 2

- Pré-requis : Mac OS X 10.7 (Lion) ou 10.8 (Mountain Lion)
- Transparent à l'utilisateur : l'ouverture d'une session déverrouille l'accès et permet le déchiffrement du disque.

- Références :

https://aresu.dsi.cnrs.fr/IMG/pdf/CNRS-DR4-CRSSI-Chiffrement_FileVault2-v1-0.pdf

http://support.apple.com/kb/HT4790?viewlocale=fr_FR

<https://aresu.dsi.cnrs.fr/IMG/pdf/manuel.pdf>

Ouvrir les préférences système
et cliquer dans « Sécurité et confidentialité »



Cliquer dans « FileVault » :



Cliquez dans le cadenas pour pouvoir activer FileVault :



Cliquez dans « Activer FileVault »



Autoriser les utilisateurs



Saisir le mot de passe de chaque utilisateur autorisé





Tout afficher



La clé de secours est un « filet de sécurité » qui peut servir à déverrouiller le disque si vous avez oublié votre mot de passe.

Effectuez une copie et stockez-la en lieu sûr. Si vous oubliez votre mot de passe et perdez la clé de secours, toutes les données de votre disque seront perdues.

05H5-C27L-KVKP-PYKY-LZWM-JTAV



Annuler

Retour

Continuer



Pour empêcher les modifications, cliquez ici.

Avancé...



Ne jamais stocker la clé de secours dans un tiers



Sécurité et confidentialité



Tout afficher



Cliquez sur le bouton Redémarrer pour redémarrer votre Mac et lancer le processus de chiffrement.

Après avoir redémarré, vous pourrez vous servir de votre Mac pendant le processus de chiffrement. Vous pourrez en vérifier la progression dans les préférences Sécurité et confidentialité.

ATTENTION Vous aurez besoin d'un mot de passe

Une clé de secours sera générée automatiquement

enregistrez votre mot de passe et la clé de secours, vos données seront perdues.

Annuler

Redémarrer

FileVault est désactivé pour le disque « Sans titre ».



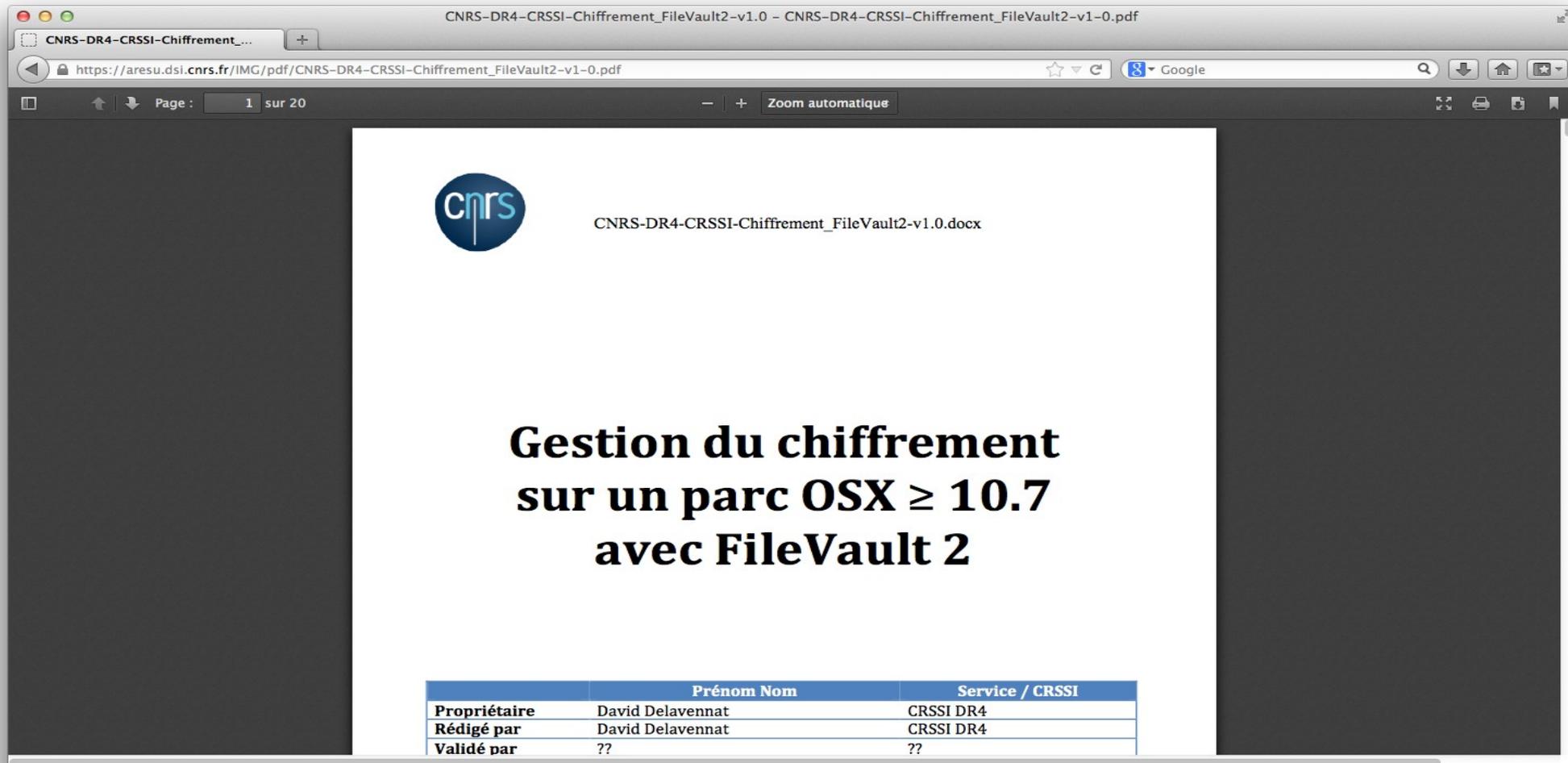
Pour empêcher les modifications, cliquez ici.

Avancé...



Gestion du chiffrement sur un parc de MAC

https://aresu.dsi.cnrs.fr/IMG/pdf/CNRS-DR4-CRSSI-Chiffrement_FileVault2-v1-0.pdf



The screenshot shows a web browser window displaying a PDF document. The browser's address bar shows the URL: https://aresu.dsi.cnrs.fr/IMG/pdf/CNRS-DR4-CRSSI-Chiffrement_FileVault2-v1-0.pdf. The document's title is "CNRS-DR4-CRSSI-Chiffrement_FileVault2-v1.0.docx". The main content of the page is the title "Gestion du chiffrement sur un parc OS X ≥ 10.7 avec FileVault 2". At the bottom of the page, there is a table with three columns: "Prénom Nom", "Service / CRSSI", and "Propriétaire", "Rédigé par", and "Validé par".

 CNRS-DR4-CRSSI-Chiffrement_FileVault2-v1.0.docx

Gestion du chiffrement sur un parc OS X \geq 10.7 avec FileVault 2

	Prénom Nom	Service / CRSSI
Propriétaire	David Delavennat	CRSSI DR4
Rédigé par	David Delavennat	CRSSI DR4
Validé par	??	??

Recouvrement

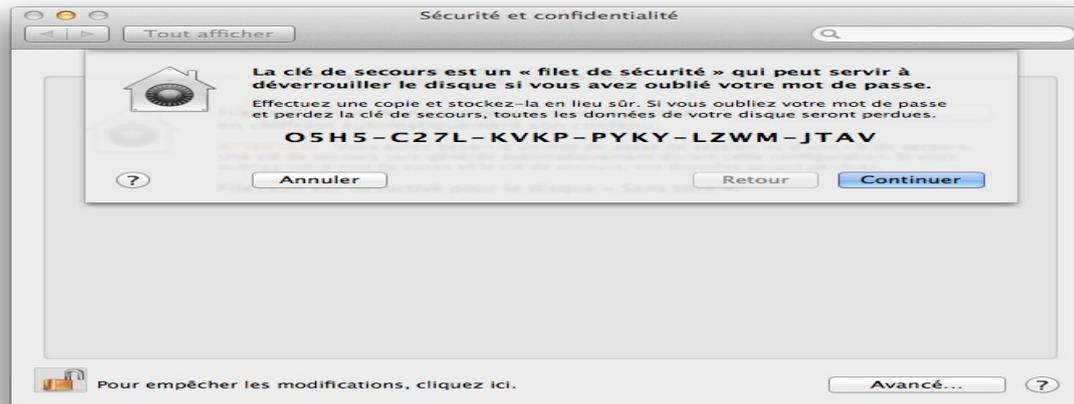
1. Avec un compte admin

Démarrer la machine avec le compte d'admin

Changer le mot de passe de l'utilisateur

2. Avec la clé de recouvrement de la machine générée lors de l'activation de FileVault

au boot, après 3 tentatives de mot de passe infructueuse, cliquer sur le triangle jaune, le prompt de la clé apparaît .



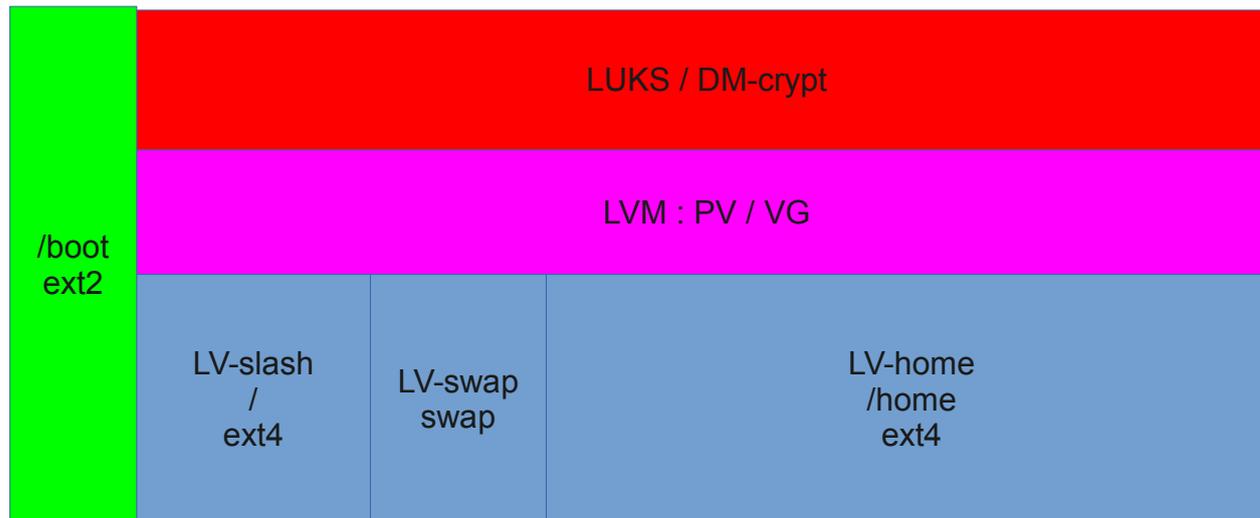
3. Avec un certificat de recouvrement d'établissement commun à tous les disques chiffrés.

Voir la références https://aresu.dsi.cnrs.fr/IMG/pdf/CNRS-DR4-CRSSI-Chiffrement_FileVault2-v1-0.pdf

Dm-Crypt / LUKS

Dm-crypt : C'est le chiffrement de devices virtuels en mode bloc

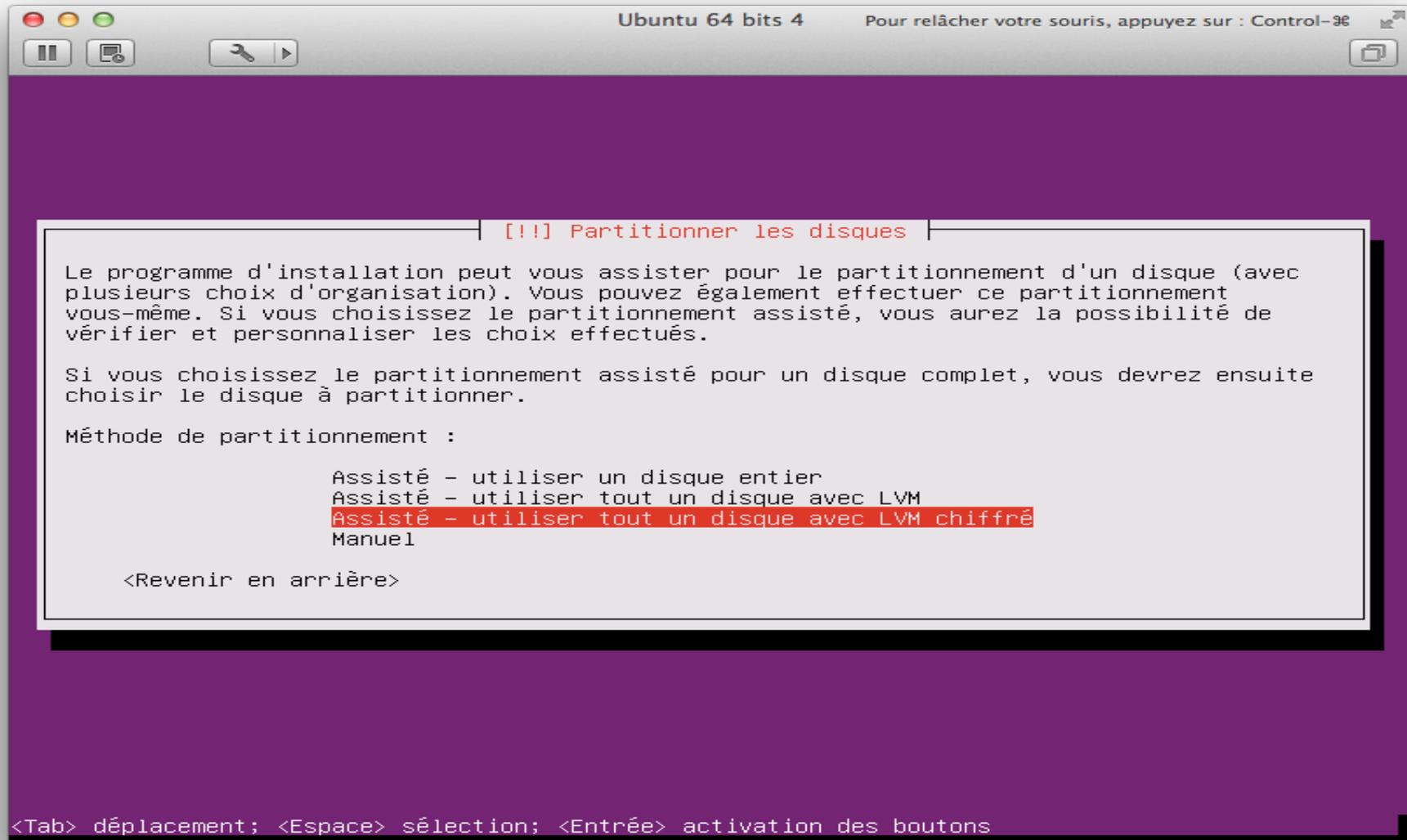
LUKS : Linux Unified Key Setup : standard de gestion du chiffrement



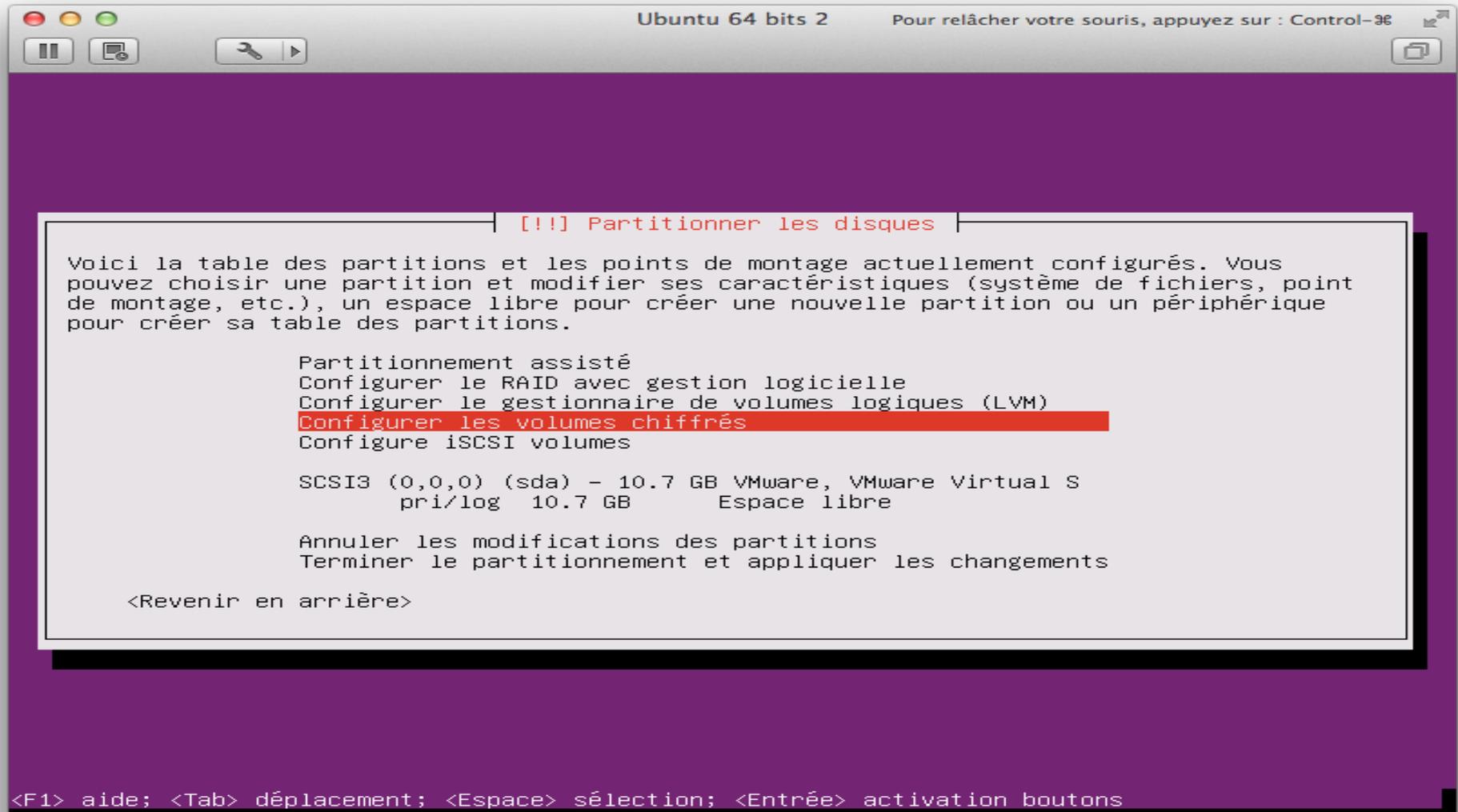
dm-crypt (debian, ubuntu ...)

- **Pendant l'installation de OS**
 - Choisir l'installation sur un disque avec volume LVM chiffré
 - Spécifier une passphrase
 - Sauvegarder une copie de l'entête du volume après le 1er reboot
 - Définir une passphrase additionnelle
- **L'OS est déjà installé**
 - Sauvegarder les données
 - Préparer des partitions chiffrées
 - Restaurer les données

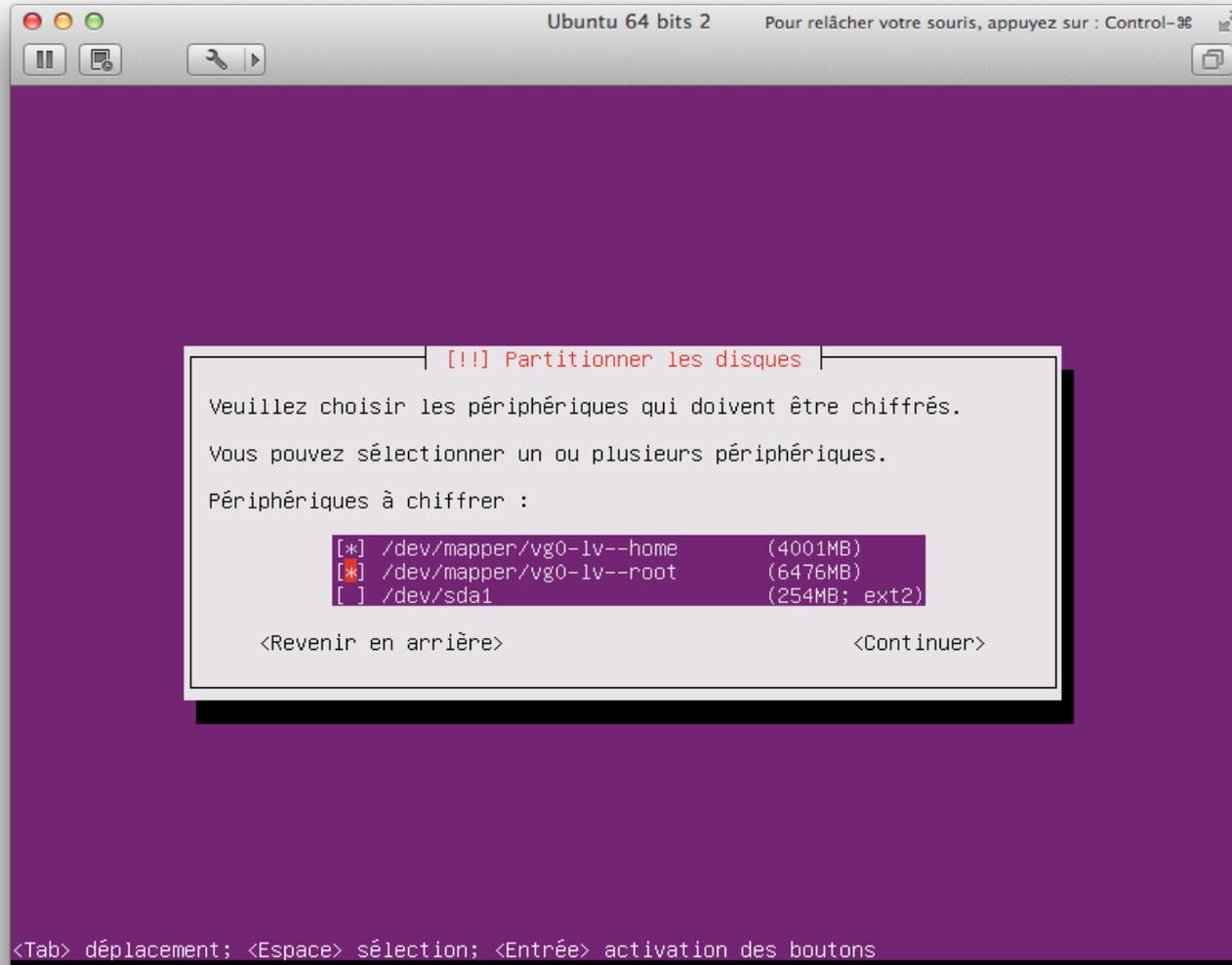
Choisir un disque avec LVM chiffré



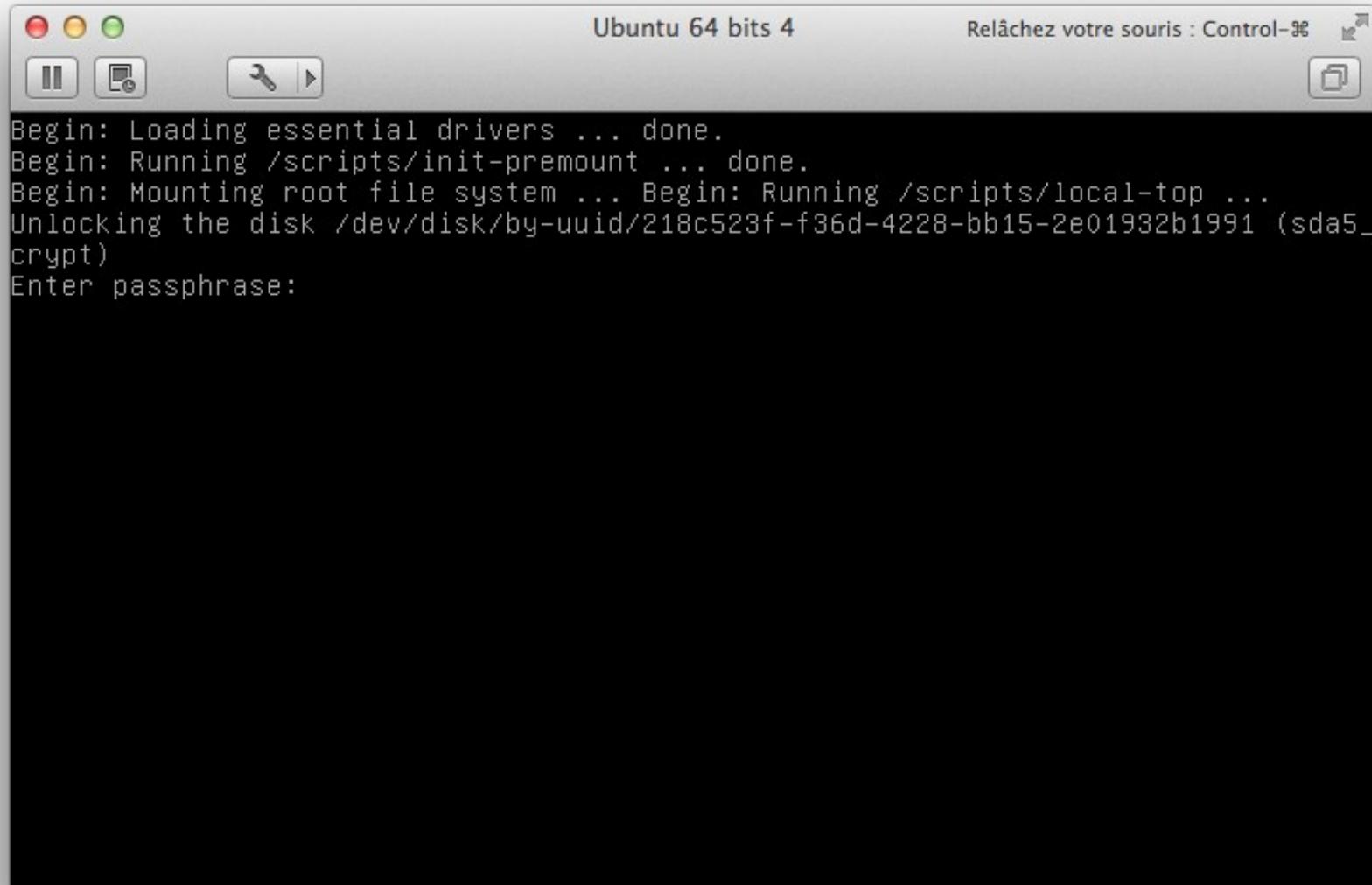
Configurer les volumes



Configurer les volumes chiffrés



Démarrage du système

A terminal window titled "Ubuntu 64 bits 4" with a status bar on the right that says "Relâchez votre souris : Control-⌘". The terminal displays the following text:

```
Begin: Loading essential drivers ... done.  
Begin: Running /scripts/init-premount ... done.  
Begin: Mounting root file system ... Begin: Running /scripts/local-top ...  
Unlocking the disk /dev/disk/by-uuid/218c523f-f36d-4228-bb15-2e01932b1991 (sda5_  
crypt)  
Enter passphrase:
```

Les partitions du disque

```
Ubuntu 64 bits 4                               Relâchez votre souris : Control-⌘
[ Pauses ] [ Copier ] [ Outils ] [ Navigation ] [ Paramètres ] [ Aide ] [ Quitter ]
cfdisk (util-linux 2.20.1)
Unité disque : /dev/sda
Taille : 21474836480 octets, 21.4 Go
Têtes : 255   Secteurs par piste : 63   Cylindres : 2610

Nom          Drap.      Partition  S. Fic.      [Étiq.]      Taille (Mo)
-----
)-----
          Primaire  Espace libre          1,05*
sda1      Amorce     Primaire  ext2          254,81*
          Pri/Log    Espace libre          1,05*
sda5      NC         Logique   crypto_LUKS   21216,89*
          Pri/Log    Espace libre          1,05*

[ Aide ] [ Nouvelle ] [ Afficher ] [ Quitter ] [ Unités ]
[ Écrire ]

Commande incorrecte
Créer une nouvelle partition à partir de l'espace libre_
```

/etc/fstab et /etc/crypttab

```
Ubuntu 64 bits 4 Relâchez votre souris : Control-⌘
khabzaoui@ubuntu:~$ more /etc/fstab
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point> <type> <options> <dump> <pass>
proc /proc proc nodev,noexec,nosuid 0 0
/dev/mapper/ubuntu-root / ext4 errors=remount-ro 0 1
# /boot was on /dev/sda1 during installation
UUID=c8235661-493a-4b22-adf6-ebd778a3a86f /boot ext2 defaults
0 2
/dev/mapper/ubuntu-swap_1 none swap sw 0 0
/dev/fd0 /media/floppy0 auto rw,user,noauto,exec,utf8 0 0
/dev/mapper/cryptswap1 none swap sw 0 0
khabzaoui@ubuntu:~$ more /etc/cr
cron.d/ cron.hourly/ crontab crypttab
cron.daily/ cron.monthly/ cron.weekly/
khabzaoui@ubuntu:~$ more /etc/crypttab
sda5_crypt UUID=218c523f-f36d-4228-bb15-2e01932b1991 none luks
cryptswap1 /dev/dm-2 /dev/urandom swap,cipher=aes-cbc-essiv:sha256
khabzaoui@ubuntu:~$ _
```

Gestion des passphrases

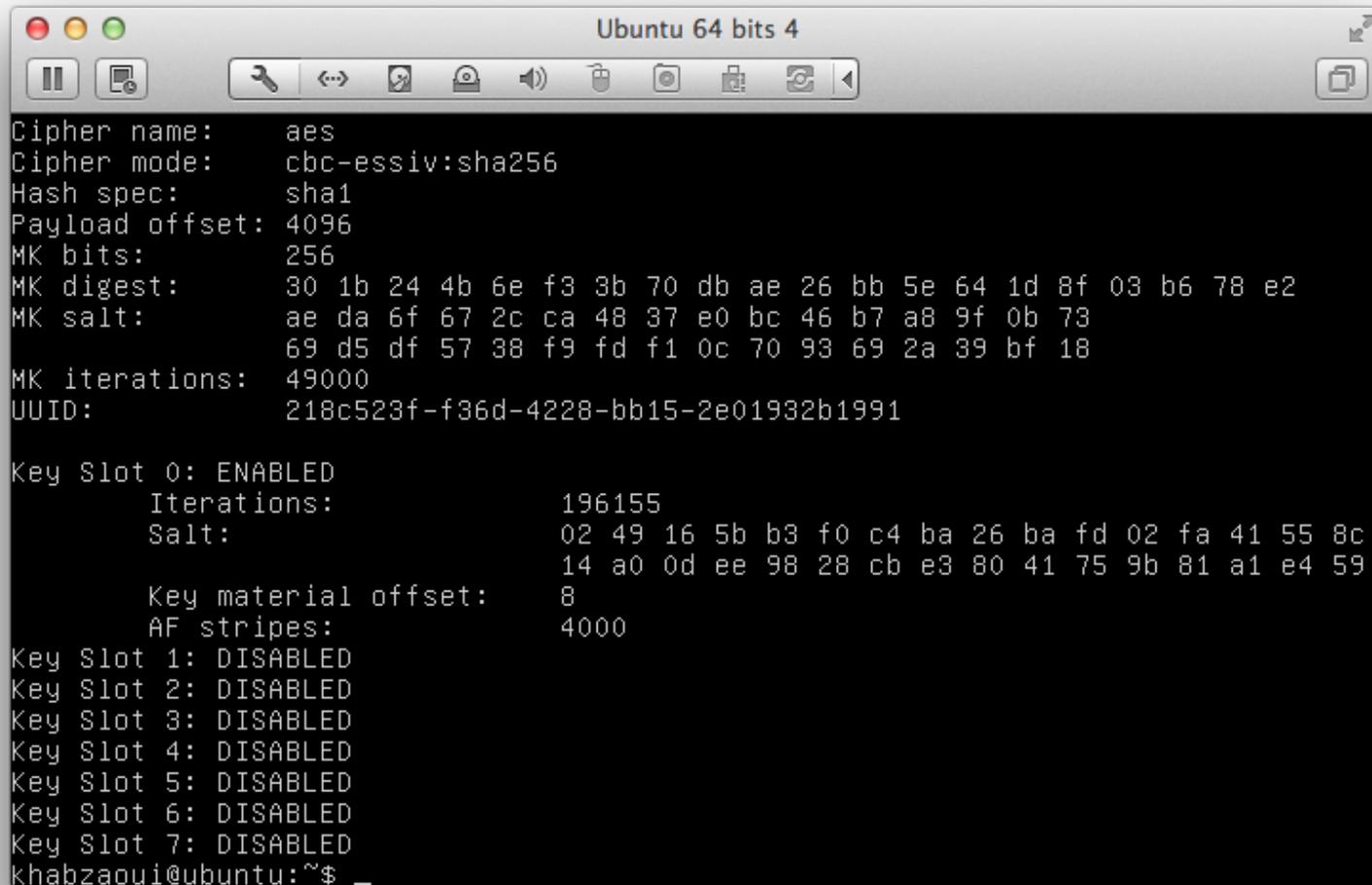
LUKS permet de stocker jusqu'à 8 passphrases

Après le premier reboot ajouter une passphrase pour le service informatique

Si l'entête du conteneur LUKS est endommagé, il ne sera plus possible d'accéder aux données donc il faut sauvegarder la clé de chiffrement en un endroit sûr (coffre-fort)

Lister les slots initiaux

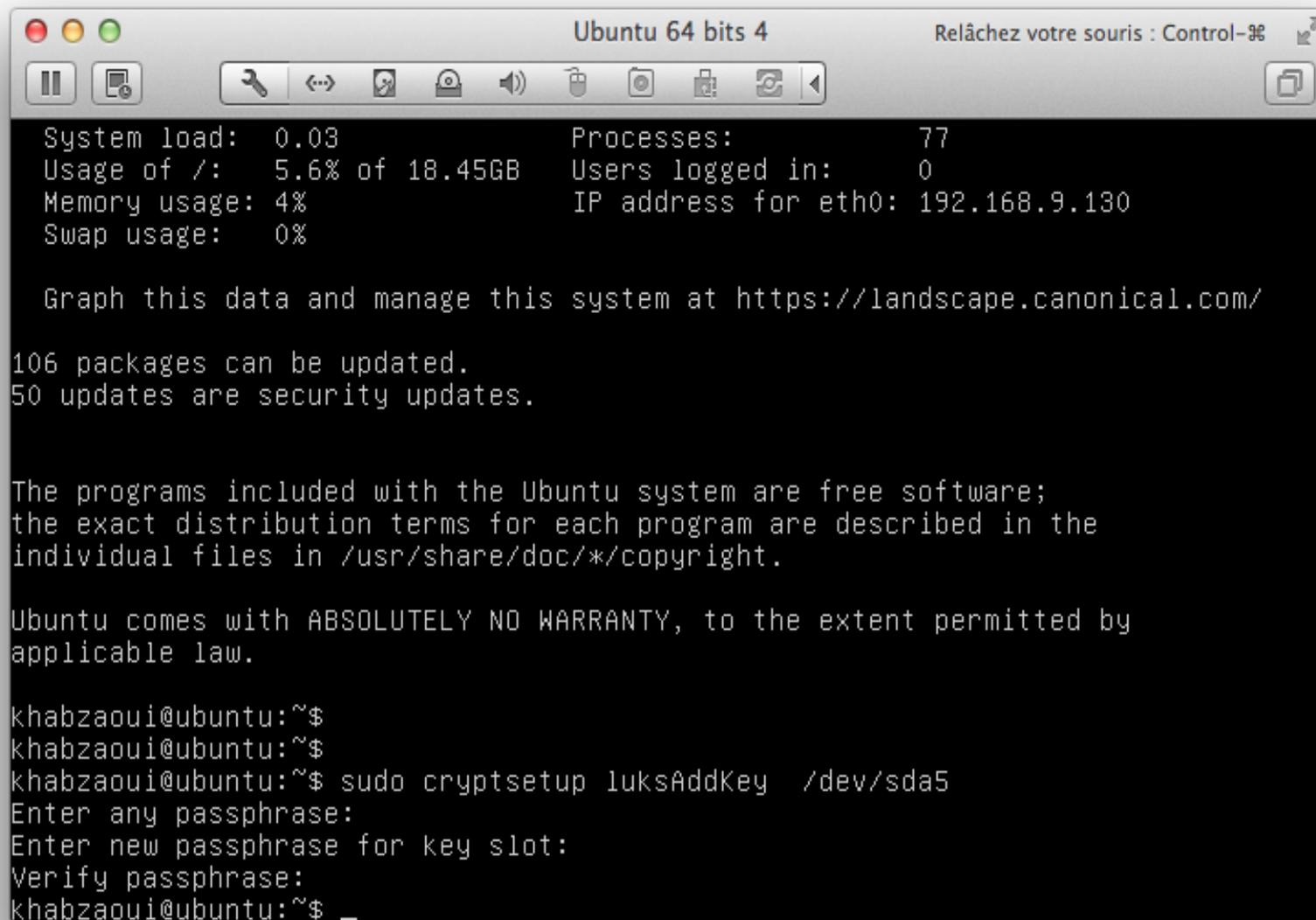
```
sudo cryptsetup luksDump  
/dev/sda5
```



```
Ubuntu 64 bits 4  
Cipher name: aes  
Cipher mode: cbc-essiv:sha256  
Hash spec: sha1  
Payload offset: 4096  
MK bits: 256  
MK digest: 30 1b 24 4b 6e f3 3b 70 db ae 26 bb 5e 64 1d 8f 03 b6 78 e2  
MK salt: ae da 6f 67 2c ca 48 37 e0 bc 46 b7 a8 9f 0b 73  
69 d5 df 57 38 f9 fd f1 0c 70 93 69 2a 39 bf 18  
MK iterations: 49000  
UUID: 218c523f-f36d-4228-bb15-2e01932b1991  
  
Key Slot 0: ENABLED  
Iterations: 196155  
Salt: 02 49 16 5b b3 f0 c4 ba 26 ba fd 02 fa 41 55 8c  
14 a0 0d ee 98 28 cb e3 80 41 75 9b 81 a1 e4 59  
Key material offset: 8  
AF stripes: 4000  
Key Slot 1: DISABLED  
Key Slot 2: DISABLED  
Key Slot 3: DISABLED  
Key Slot 4: DISABLED  
Key Slot 5: DISABLED  
Key Slot 6: DISABLED  
Key Slot 7: DISABLED  
khabzaoui@ubuntu:~$ _
```

Ajout d'une passphrase

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



```
Ubuntu 64 bits 4 Relâchez votre souris : Control-⌘
System load: 0.03 Processes: 77
Usage of /: 5.6% of 18.45GB Users logged in: 0
Memory usage: 4% IP address for eth0: 192.168.9.130
Swap usage: 0%

Graph this data and manage this system at https://landscape.canonical.com/

106 packages can be updated.
50 updates are security updates.

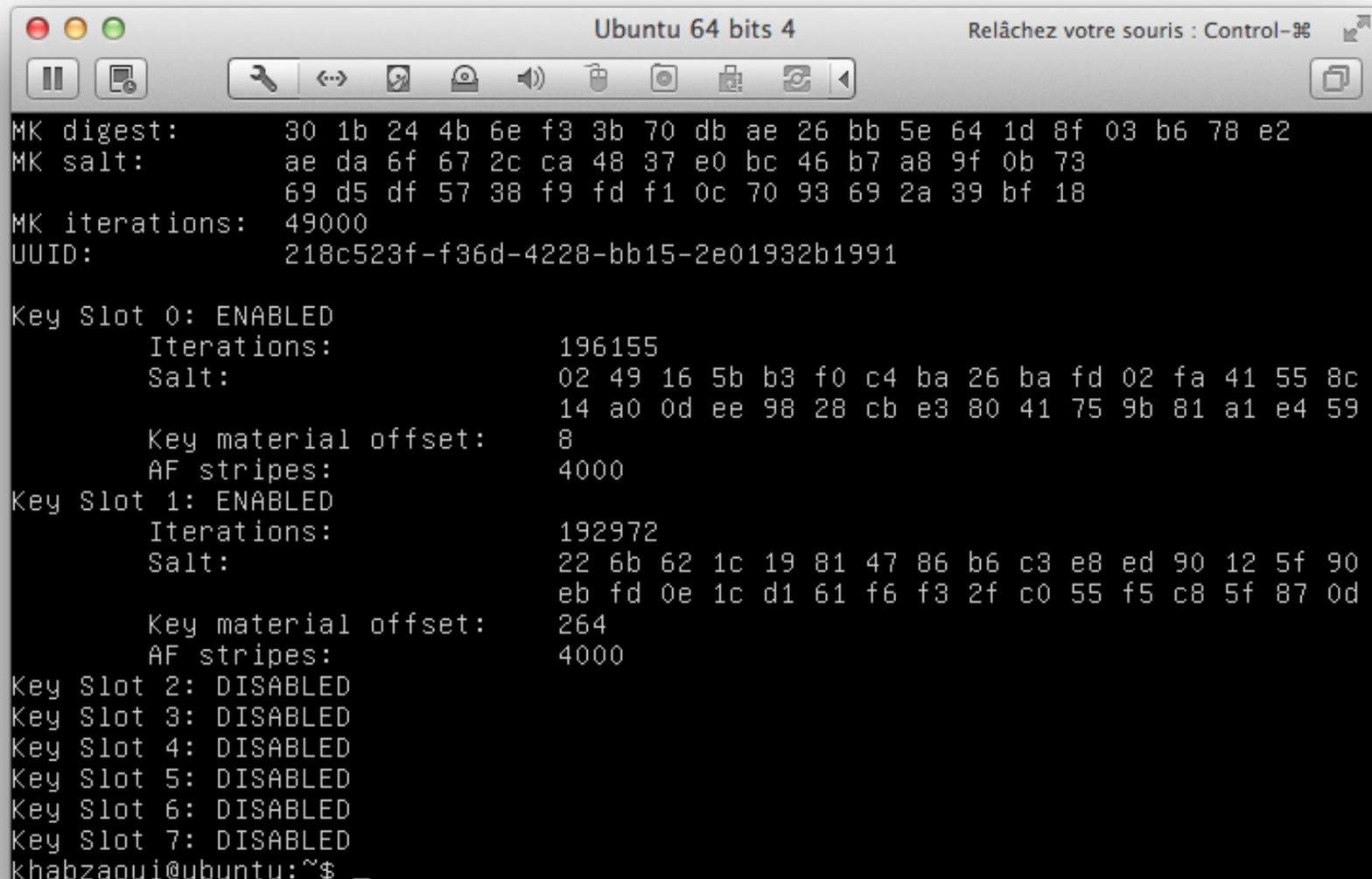
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

khabzaoui@ubuntu:~$
khabzaoui@ubuntu:~$
khabzaoui@ubuntu:~$ sudo cryptsetup luksAddKey /dev/sda5
Enter any passphrase:
Enter new passphrase for key slot:
Verify passphrase:
khabzaoui@ubuntu:~$ _
```

Lister les slots

sudo cryptsetup luksDump /dev/sda5



```
Ubuntu 64 bits 4 Relâchez votre souris : Control-⌘
MK digest: 30 1b 24 4b 6e f3 3b 70 db ae 26 bb 5e 64 1d 8f 03 b6 78 e2
MK salt:   ae da 6f 67 2c ca 48 37 e0 bc 46 b7 a8 9f 0b 73
          69 d5 df 57 38 f9 fd f1 0c 70 93 69 2a 39 bf 18
MK iterations: 49000
UUID:        218c523f-f36d-4228-bb15-2e01932b1991

Key Slot 0: ENABLED
  Iterations: 196155
  Salt:       02 49 16 5b b3 f0 c4 ba 26 ba fd 02 fa 41 55 8c
              14 a0 0d ee 98 28 cb e3 80 41 75 9b 81 a1 e4 59
  Key material offset: 8
  AF stripes: 4000
Key Slot 1: ENABLED
  Iterations: 192972
  Salt:       22 6b 62 1c 19 81 47 86 b6 c3 e8 ed 90 12 5f 90
              eb fd 0e 1c d1 61 f6 f3 2f c0 55 f5 c8 5f 87 0d
  Key material offset: 264
  AF stripes: 4000
Key Slot 2: DISABLED
Key Slot 3: DISABLED
Key Slot 4: DISABLED
Key Slot 5: DISABLED
Key Slot 6: DISABLED
Key Slot 7: DISABLED
khabzaoui@ubuntu:~$ _
```

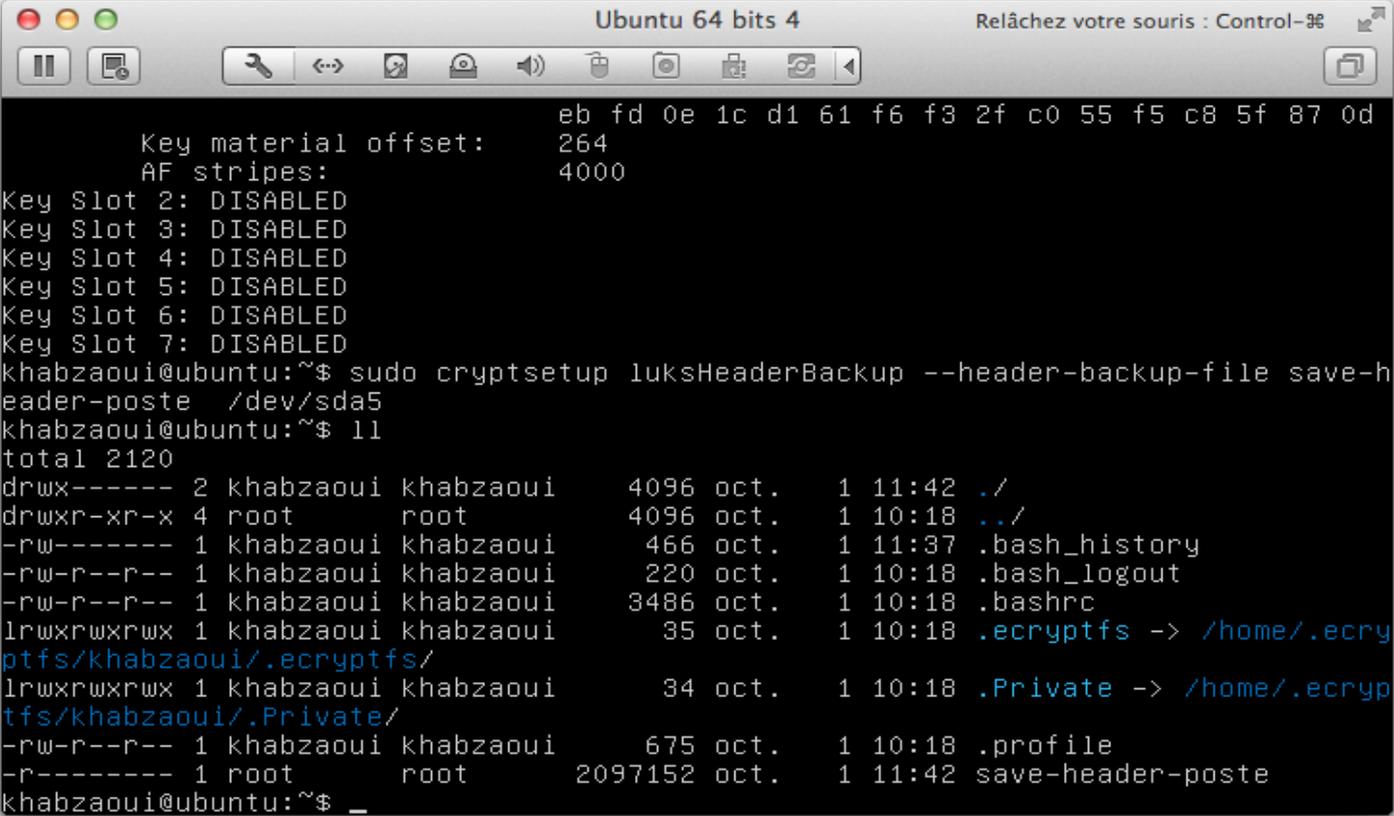
Supprimer une passphrase

Dans cet exemple on supprime la clé présente dans le 2ème slot.

```
sudo cryptsetup luksKillSlot /dev/sda5 2
```

Sauvegarde de l'entête LUKS

```
cryptsetup luksHeaderBackup --header-backup-file save-header-poste /dev/sda5
```



```
Ubuntu 64 bits 4 Relâchez votre souris : Control-⌘
Key material offset: eb fd 0e 1c d1 61 f6 f3 2f c0 55 f5 c8 5f 87 0d
AF stripes: 264
4000
Key Slot 2: DISABLED
Key Slot 3: DISABLED
Key Slot 4: DISABLED
Key Slot 5: DISABLED
Key Slot 6: DISABLED
Key Slot 7: DISABLED
khabzaoui@ubuntu:~$ sudo cryptsetup luksHeaderBackup --header-backup-file save-h
header-poste /dev/sda5
khabzaoui@ubuntu:~$ ll
total 2120
drwx----- 2 khabzaoui khabzaoui 4096 oct. 1 11:42 ./
drwxr-xr-x 4 root root 4096 oct. 1 10:18 ../
-rw----- 1 khabzaoui khabzaoui 466 oct. 1 11:37 .bash_history
-rw-r--r-- 1 khabzaoui khabzaoui 220 oct. 1 10:18 .bash_logout
-rw-r--r-- 1 khabzaoui khabzaoui 3486 oct. 1 10:18 .bashrc
lrwxrwxrwx 1 khabzaoui khabzaoui 35 oct. 1 10:18 .ecryptfs -> /home/.ecryp
tfs/khabzaoui/.ecryptfs/
lrwxrwxrwx 1 khabzaoui khabzaoui 34 oct. 1 10:18 .Private -> /home/.ecryp
tfs/khabzaoui/.Private/
-rw-r--r-- 1 khabzaoui khabzaoui 675 oct. 1 10:18 .profile
-r----- 1 root root 2097152 oct. 1 11:42 save-header-poste
khabzaoui@ubuntu:~$ _
```

Restauration de l'entête LUKS

```
cryptsetup luksHeaderRestore --header-backup-file save-header-poste /dev/sda5
```

Recouvrement

Si l'utilisateur a oublié la sienne (**utiliser la passphrase admin**) :

- démarrer la machine avec la passphrase du service informatique
- supprimer le slot correspondant à la clé oubliée (`luksKillSlot`)
- créer une nouvelle passphrase (`luksAddKey`)

Si la passphrase de l'admin a été supprimée ou si l'entête de chiffrement est vérolée (**Restaurer l'entête**)

- connecter le disque à une autre machine
- restaurer l'entête à partir de la sauvegarde avec `luksHeaderRestore`

dm-crypt

Comment crypter un disque

Commandes utiles

Sauvegarder le système complet (un gros tar):

```
tar cSjf /external/sysbackup.tar.bz2 /bin/ /boot/ /etc/ /home/ /lib/ /opt/ /root/ /sbin/ /selinux/ /srv/ /usr/ /var/
```

Installer lvm et cryptsetup :

```
apt-get install lvm2 cryptsetup
```

Activer le module dm-crypt :

```
modprobe dm-crypt
```

On va ensuite créer nos partitions :

- /dev/sda1 non chiffrée pour le boot (/boot).
- /dev/sda2 qui contiendra à la fois la partition système et la partition de swap. Toutes les 2 seront chiffrées

Supprimer de manière sécurisée ce qui se trouve sur sda :

```
shred -n 7 /dev/sda
```

Créer la partition chiffrée sur /dev/sda2 :

```
cryptsetup -c aes-xts-plain -s 256 luksFormat /dev/sda2
```

(Cryptsetup demandera alors un mot de passe)

dm-crypt

Comment crypter un disque

Commandes utiles

Monter sda2 sous le nom lvm_crypt par exemple :

```
cryptsetup luksOpen /dev/sda2 lvm_crypt
```

Initialiser le volume :

```
pvcreate /dev/mapper/lvm_crypt
```

Créer un groupe de volumes qu'on appellera ubuntu :

```
vgcreate ubuntu /dev/mapper/lvm_crypt
```

Créer la swap chiffrée... 8 Gb est suffisant pour 4 Gb de RAM (par exemple) :

```
lvcreate -L8000M -n swap ubuntu
```

Utiliser le reste de la place du disque pour la partition système (root) :

```
lvcreate -l 100%FREE -n root ubuntu
```

Formater les deux partitions :

```
mkswap /dev/mapper/ubuntu-swap
```

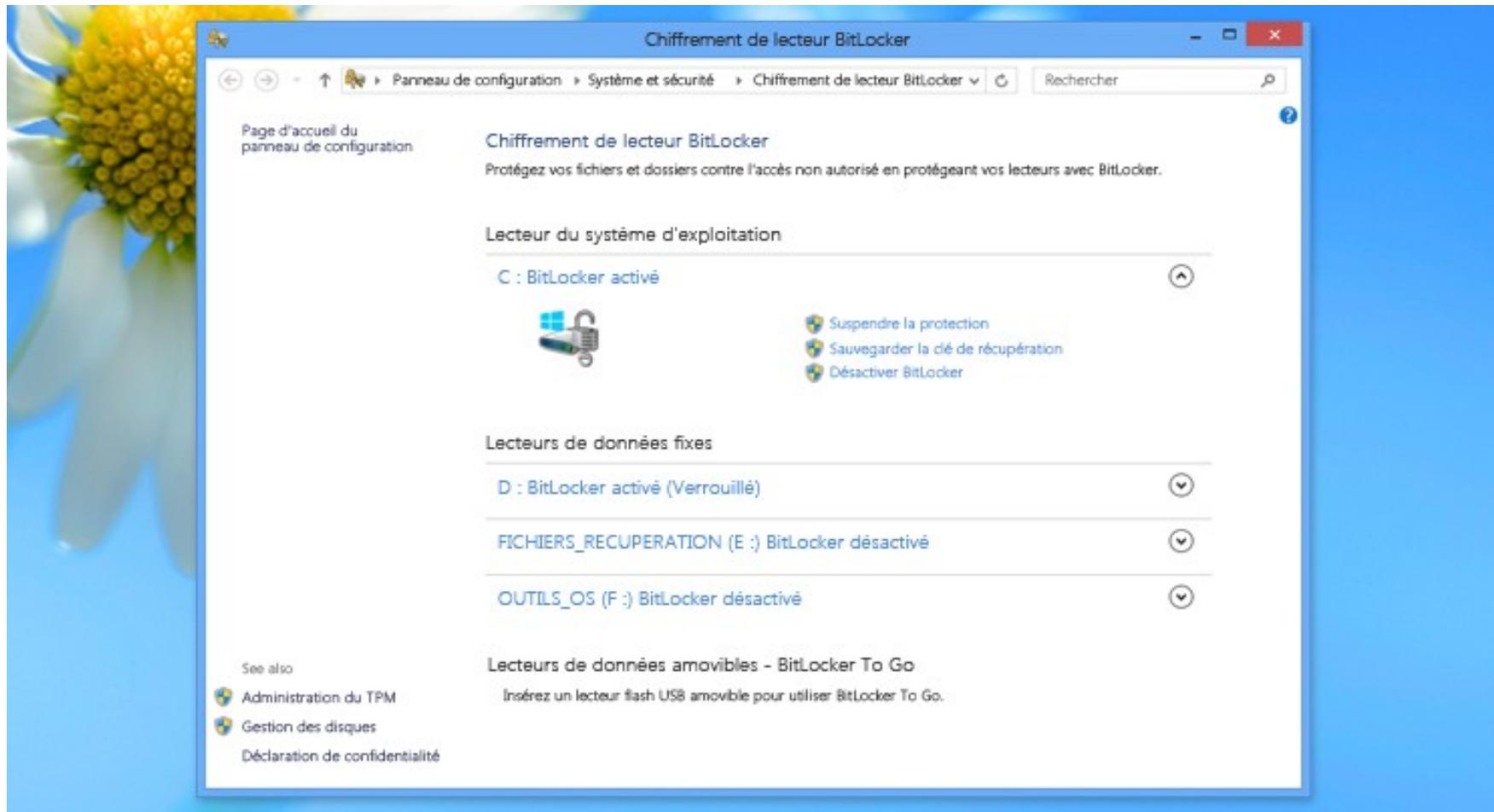
```
mkfs.ext4 /dev/mapper/ubuntu-root
```

Chiffrement des portables Windows

- Disque auto-chiffrant
- BitLocker (solution intégrée dans windows 8)
- TrueCrypt

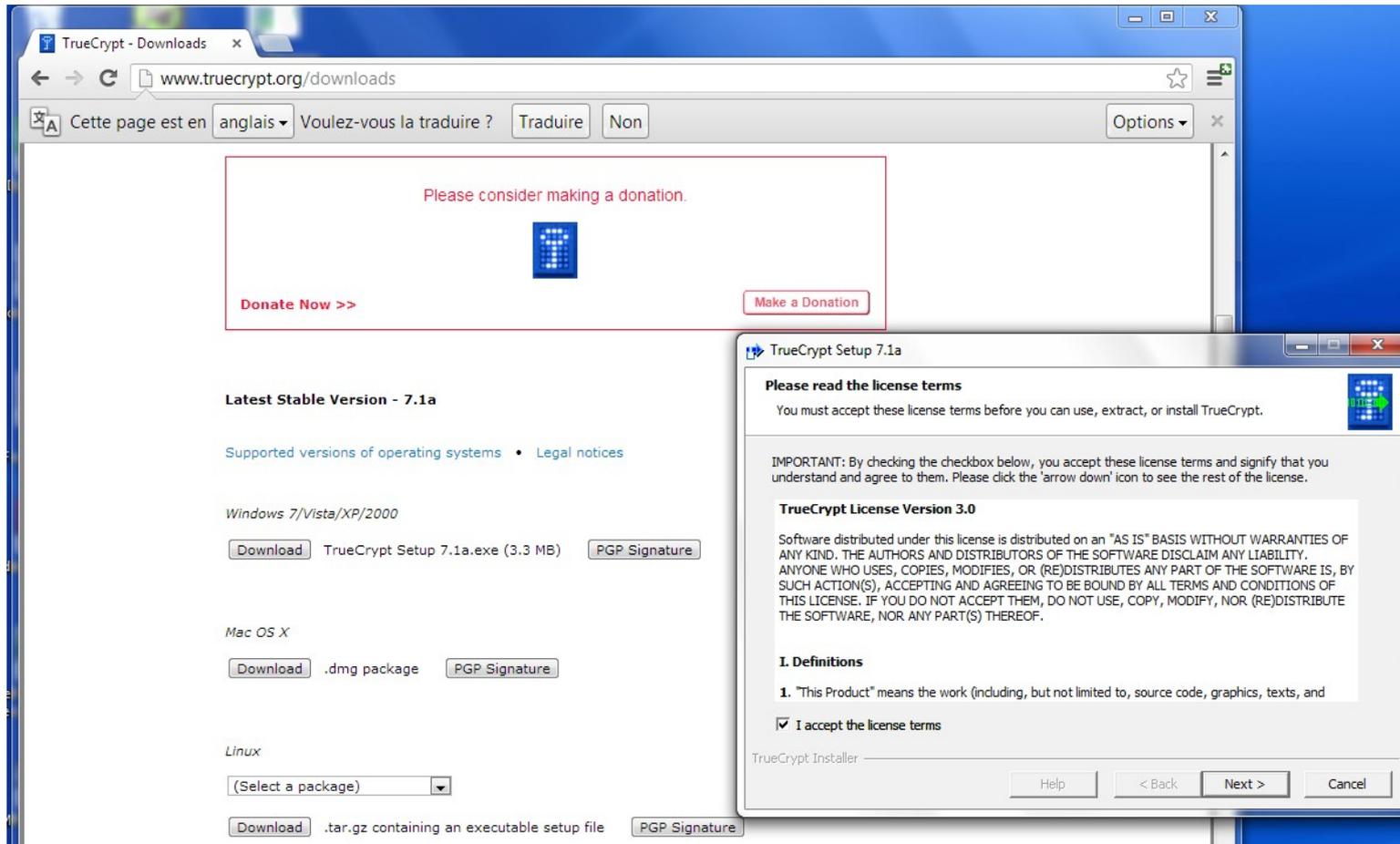
BitLocker

- <http://windows.microsoft.com/fr-FR/windows-8/bitlocker>

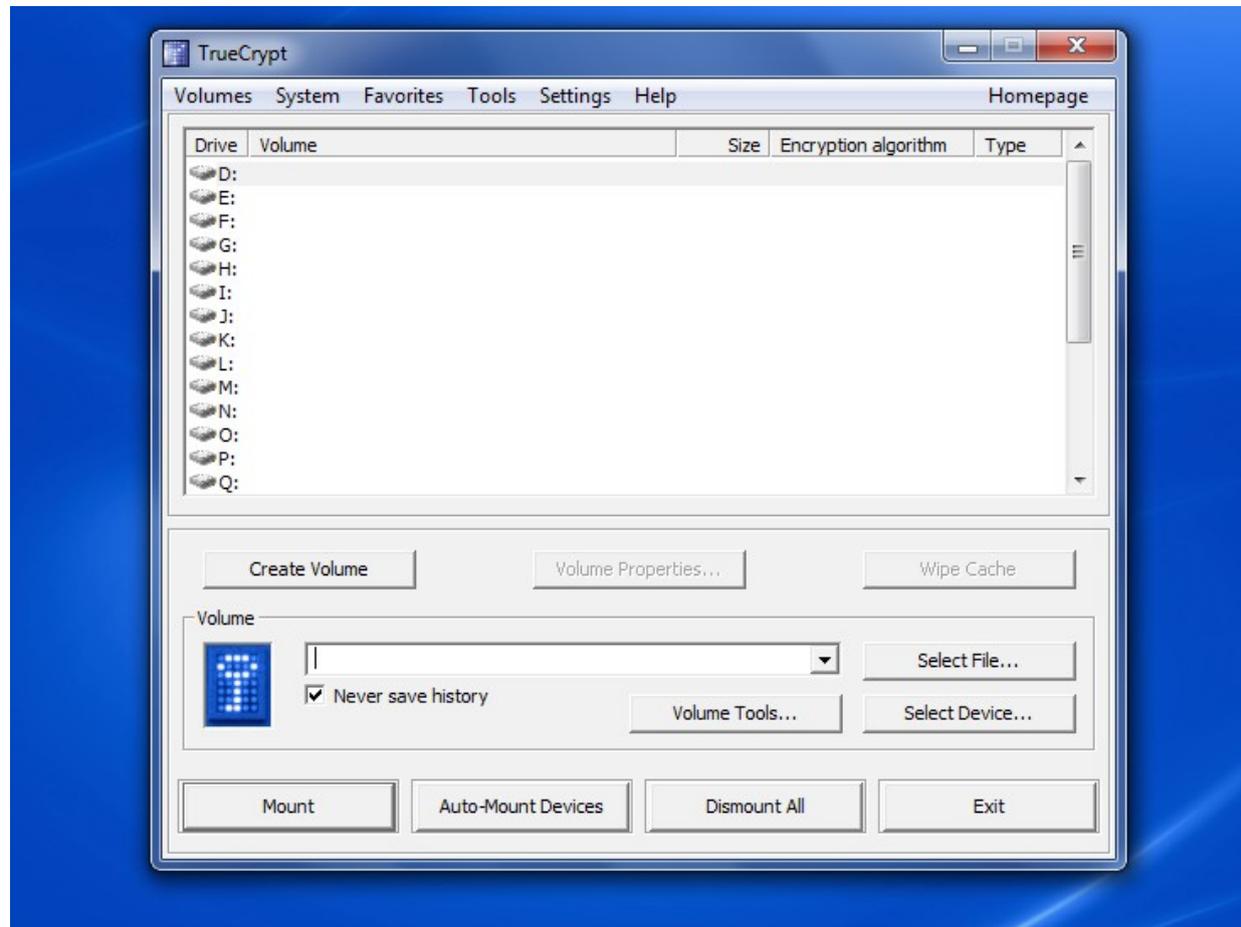


TrueCrypt

pour Windows (disponible aussi pour mac et linux)



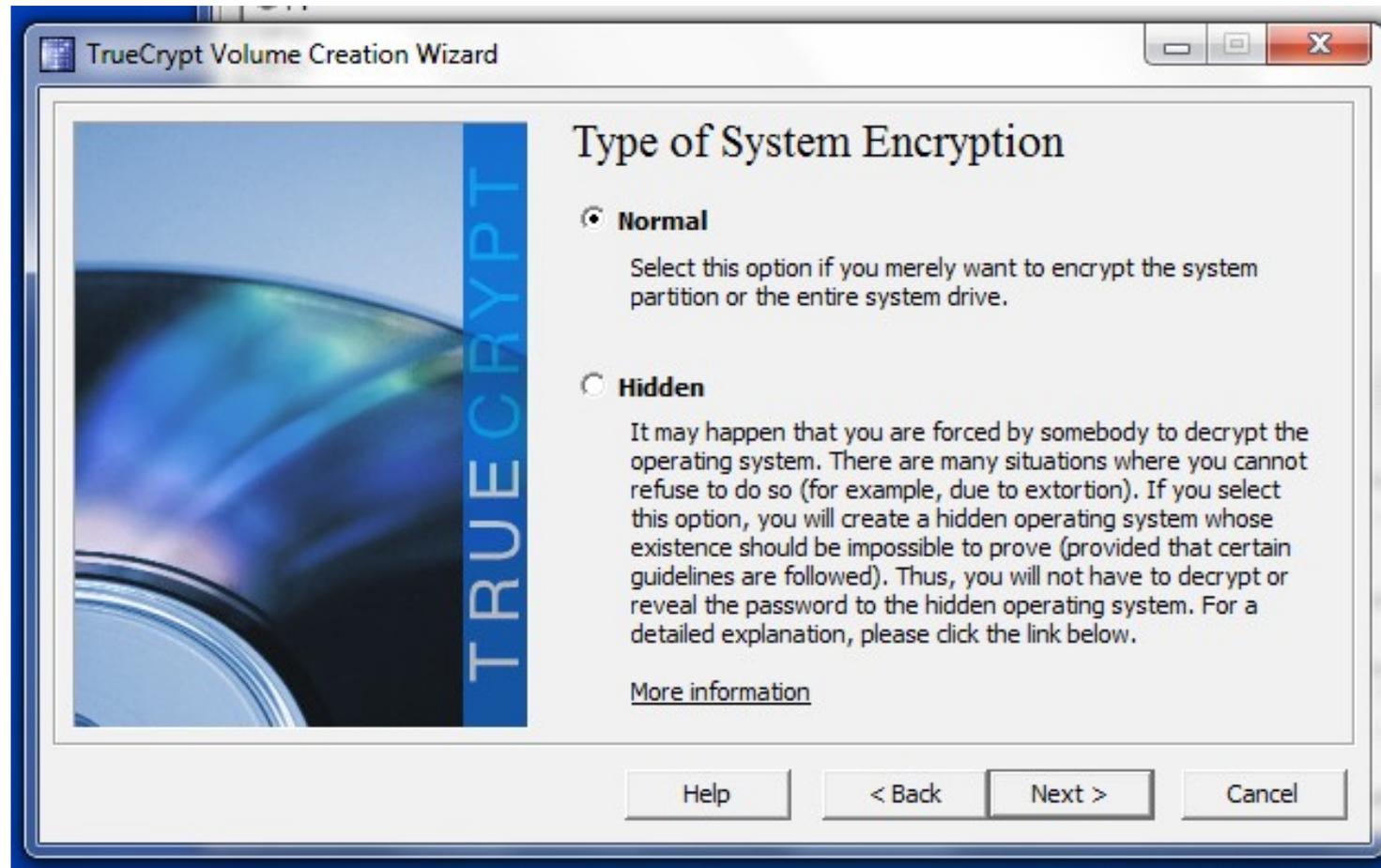
Créer un nouveau volume



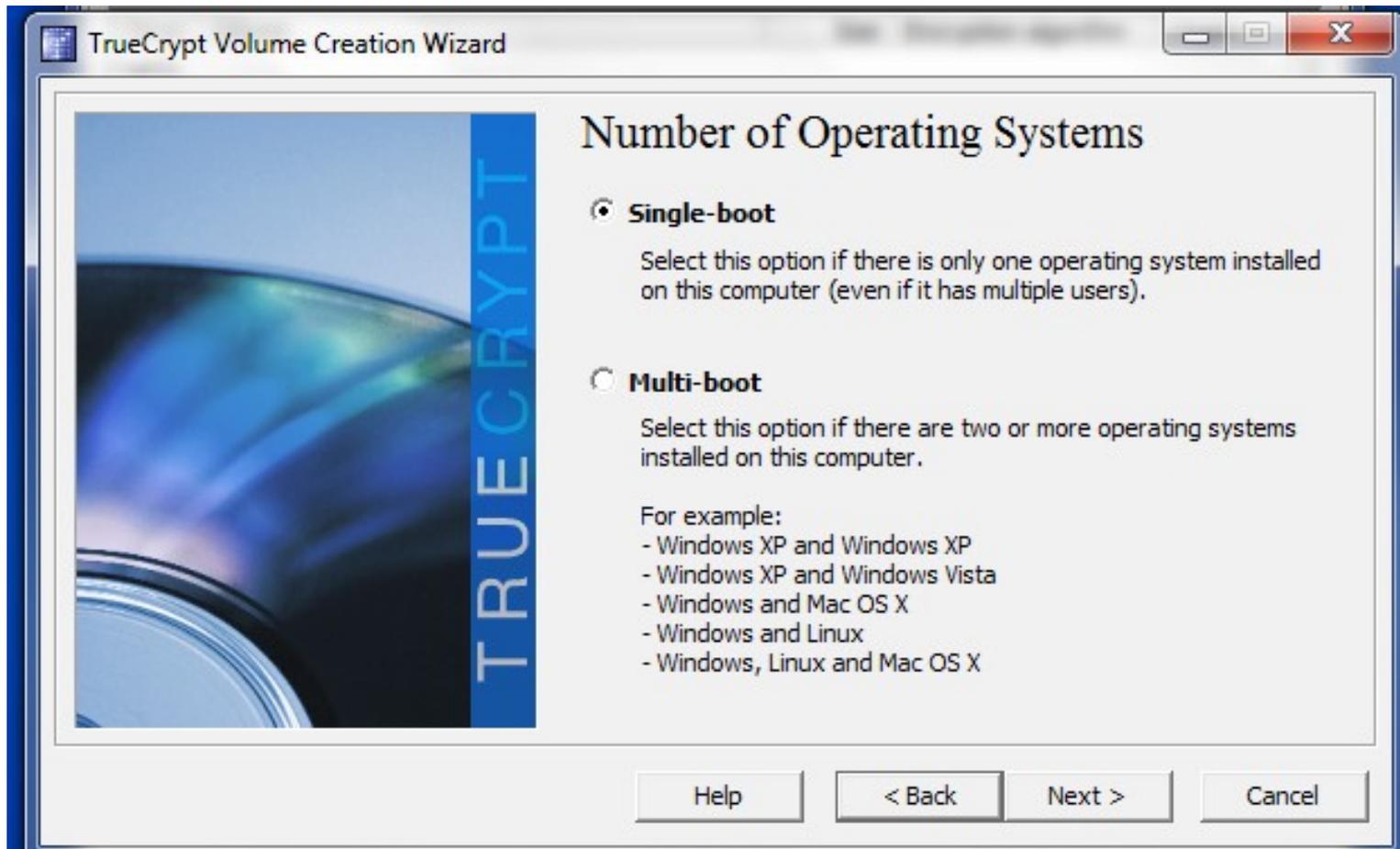
Créer un simple conteneur chiffré, chiffrer une partition qui ne contienne pas d'OS (clé USB) ou une partition /disque système



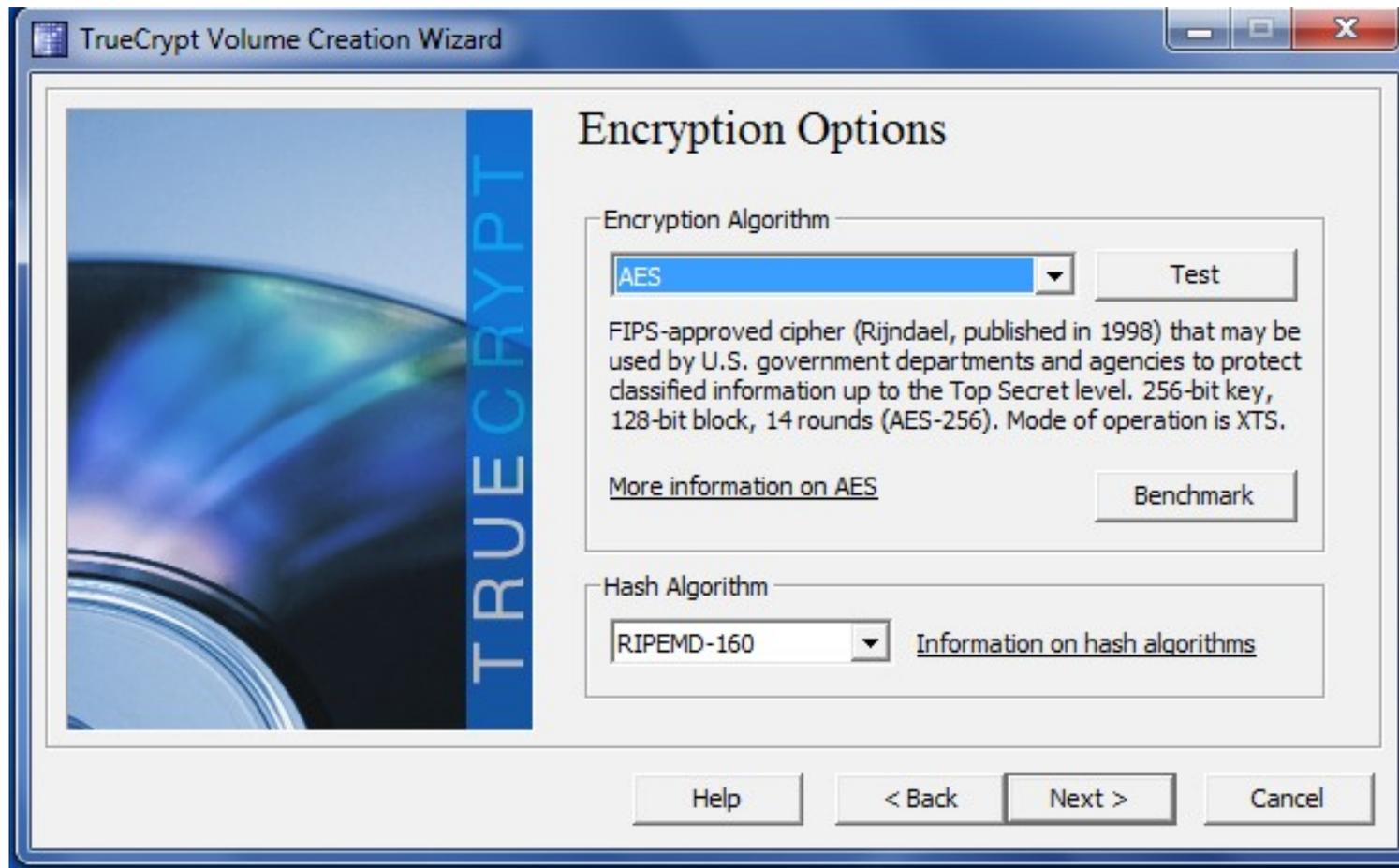
Choisir une partition normale



Un seul OS ou plusieurs (multi boot)



Sélectionner l'algorithme de chiffrement et l'algorithme de hash



Choisir un mot de passe avec des lettres majuscules, minuscules, et des symboles



The image shows a screenshot of the TrueCrypt Volume Creation Wizard window. The title bar reads "TrueCrypt Volume Creation Wizard". The main content area is titled "Password" and contains two input fields: "Password:" and "Confirm:". Below these fields is a checkbox labeled "Use keyfiles" and a button labeled "Keyfiles...". A detailed instruction paragraph is provided below the checkbox, explaining the requirements for a good password. At the bottom of the window, there are four buttons: "Help", "< Back", "Next >", and "Cancel".

TrueCrypt

Password

Password:

Confirm:

Use keyfiles

It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = \$ * + etc. We recommend choosing a password consisting of more than 20 characters (the longer, the better). The maximum possible length is 64 characters.

Bouger votre souris de manière aléatoire





Keys Generated

The keys, salt, and other data have been successfully generated. If you want to generate new keys, click Back and then Next. Otherwise, click Next to continue.

Header Key: B3908048F4BDD9927D9F92F05DE8EC70...
Master Key: D4BF8C9460FE9FC52402524012C82633...

Display generated keys (their portions)

Help

< Back

Next >

Cancel

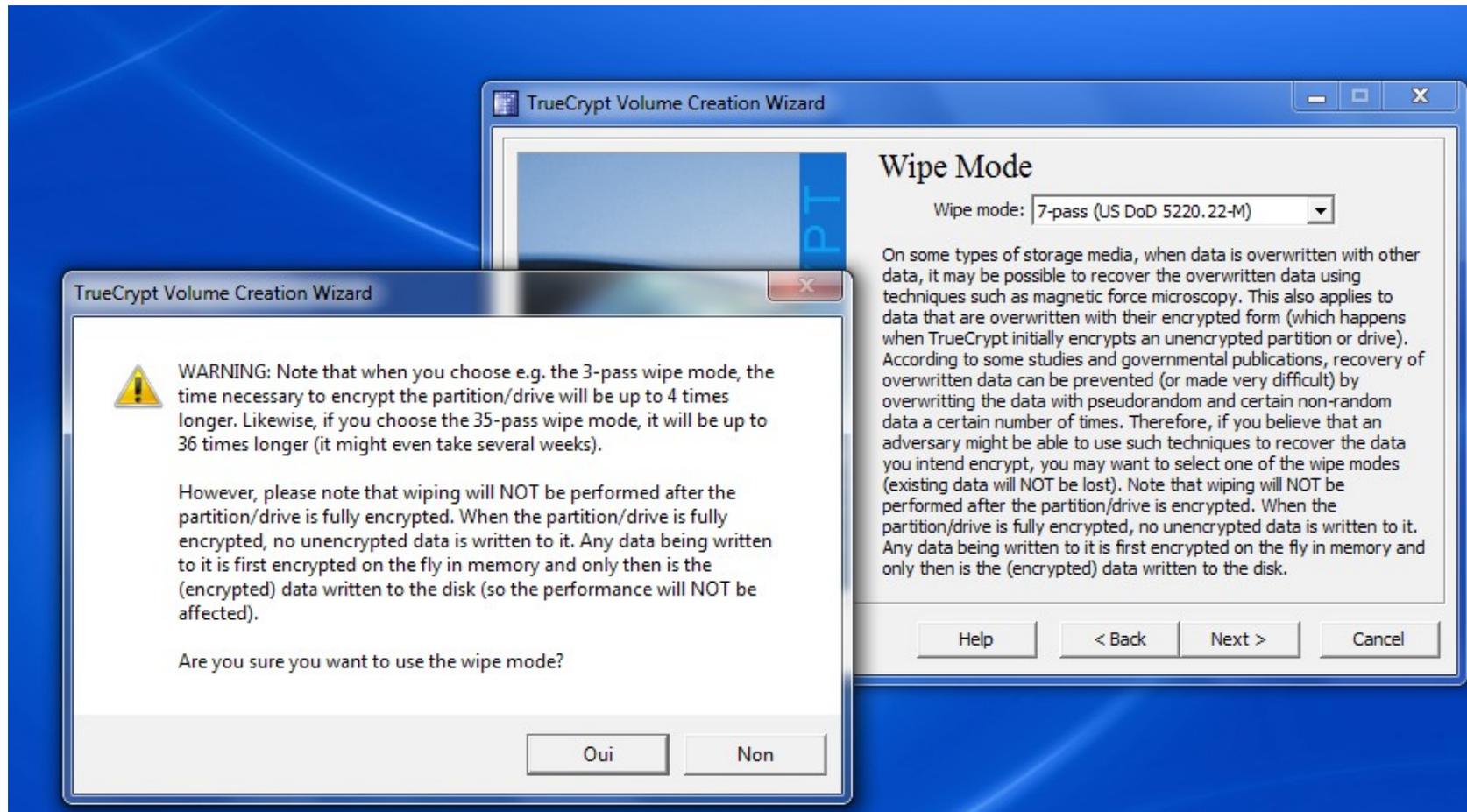
Dismount All

Exit

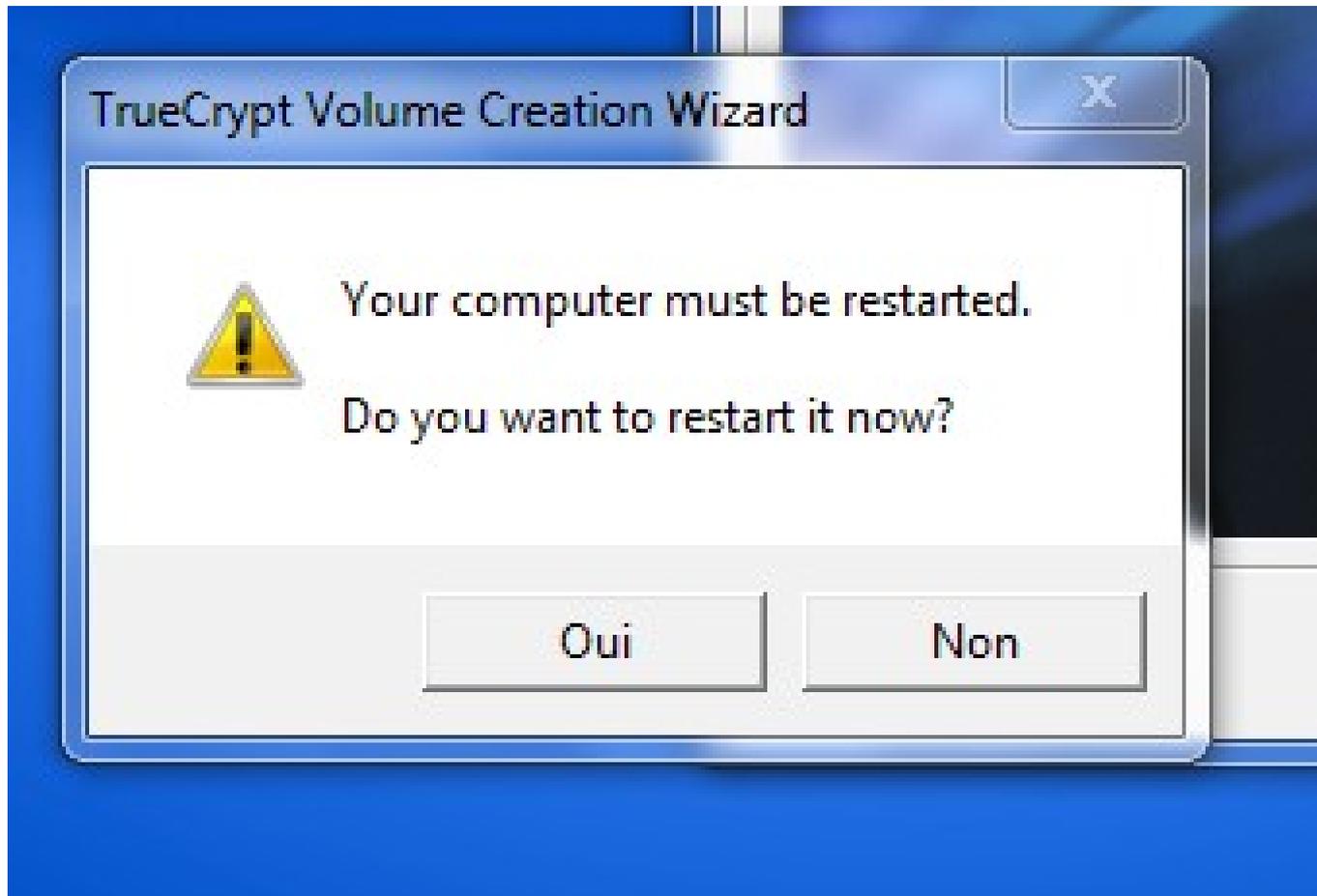
Création d'un disque de récupération, il vous faudra obligatoirement un CD vierge ou une clé USB pour l'étape suivante



Comment effacer/réécrire les données existantes en évitant que les anciennes soient irrécupérables.



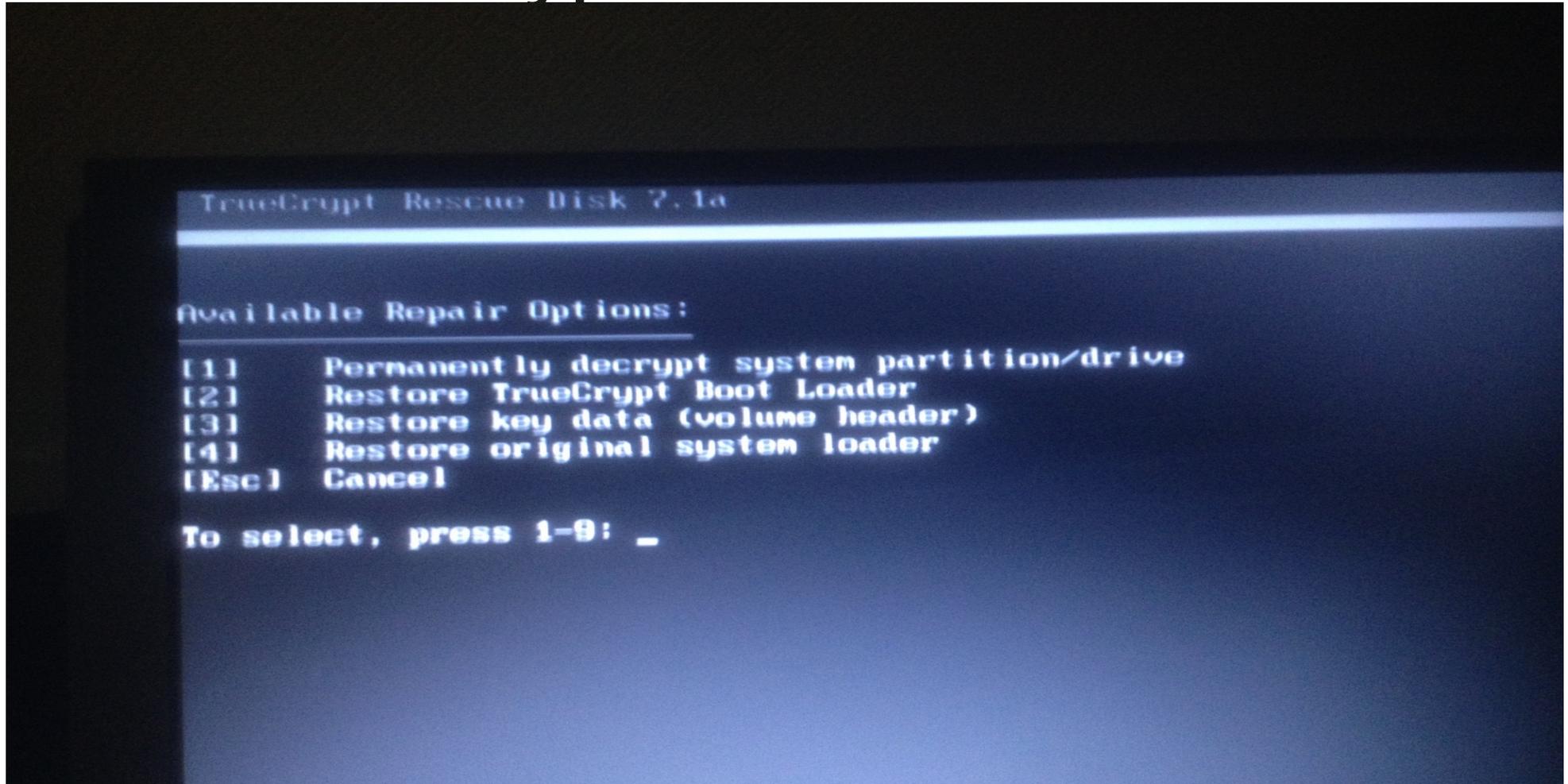
Reboot



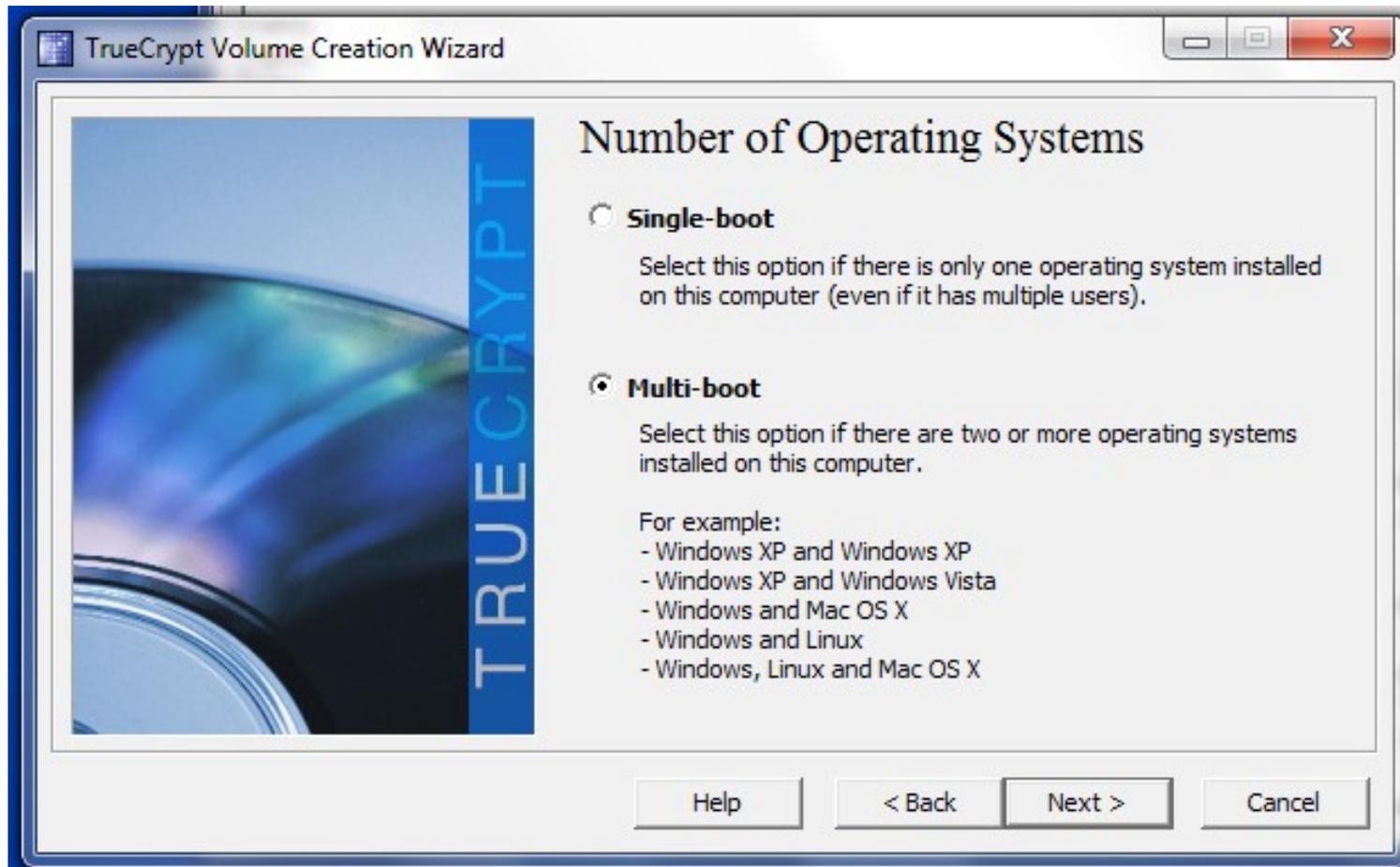
2 heures pour 17GO sur un disque SSD

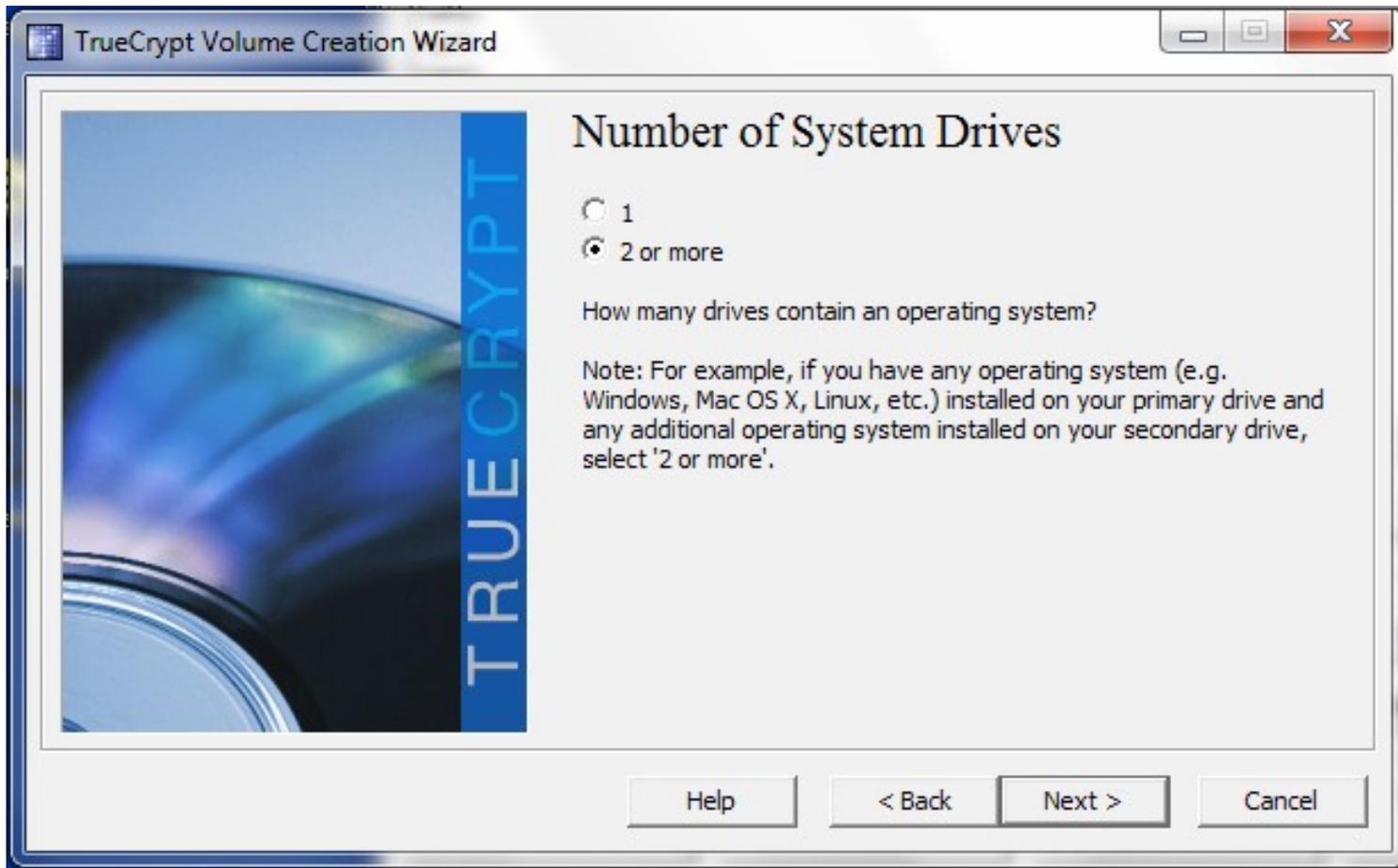


Recouvrement : TrueCrypt Rescue Disk.iso



DUAL BOOT





TrueCrypt Volume Creation Wizard

Number of System Drives

- 1
- 2 or more

How many drives contain an operating system?

Note: For example, if you have any operating system (e.g. Windows, Mac OS X, Linux, etc.) installed on your primary drive and any additional operating system installed on your secondary drive, select '2 or more'.

TRUECRYPT

Séquestre de clé de chiffrement

- Dans un coffre fort physique
- Un media de stockage contenant une copie de tous les passphrases et les entêtes ainsi que tous les disques de récupération.
- En format papier si possible (clés de chiffrements)



Conclusion

Chiffrer les portables OK mais à quel Prix !

- *Choix limité : Disque Chiffrant sur portables du marché actuel : SSD 256 =175 euros*
- Est-ce que les *Disques Chiffrants* sont utiles aujourd'hui ?
- Charge de l'ASR (activation, installation, sauvegarde, recouvrement ...)
- Un compte de service admin / passphrase admin sur tous les ordinateurs
- Mise en place d'un serveur pour la sauvegarde des portables
- PB : Sauvegarde externe non chiffrée (dropbox et autres)
 - Faire des sauvegarde chiffrées
 - Clé USB chiffrée (matériel ou logiciel)