Chiffrement des postes PC / MAC / LINUX

Mohammed Khabzaoui

UMR 8524 Université Lille1

13 fevrier 2014

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

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

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 chiffrant 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 oeuvre et utilisation : https://aresu.dsi.cnrs.fr/IMG/pdf/manuel.pdf

Chiffrement des portables

- Motivations :
  - Nombreux vols de portables
  - Données à forte valeur économique (dépôt d'un brevet)
- Dispositif :
  - Disque chiffrant 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 oeuvre et utilisation : https://aresu.dsi.cnrs.fr/IMG/pdf/manuel.pdf

Chiffrement des portables

- Motivations :
  - Nombreux vols de portables
  - Données à forte valeur économique (dépôt d'un brevet)
- Dispositif :
  - Disque chiffrant 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 oeuvre et utilisation :

  `https://aresu.dsi.cnrs.fr/IMG/pdf/manuel.pdf`

Chiffrement des portables

- Motivations :
  - Nombreux vols de portables
  - Données à forte valeur économique (dépôt d'un brevet)
- Dispositif :
  - Disque chiffrant 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 oeuvre et utilisation :

  `https://aresu.dsi.cnrs.fr/IMG/pdf/manuel.pdf`

Techniques

•	Matériel	Windows 7	Windows 8	Linux	Mac OS
Portable HP	Oui	TrueCrypt BitLocker SI (Sup windows7Pro)	BitLocker	Dm-crypt	
Portable DELL	Oui				
PC fixe	Non				
MAC	Non				FileVault
Support amovible	Oui	TrueCrypt	TrueCrypt	TrueCrypt	TrueCrypt

Outil de chiffrement matériel

Un disque dur autochiffrant (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.

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.

Outil de chiffrement matériel

- 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-soluti`
- Portable HP : Overview of Self Encrypting Drives : `http://h20195.www2.hp.com/V2/GetPDF.aspx/4AA4-4992ENW.pdf` HP ProtectTools : Manuel de l'utilisateur : `http://h10032.www1.hp.com/ctg/Manual/c01367352.pdf`

Mac OS : FileVault 2

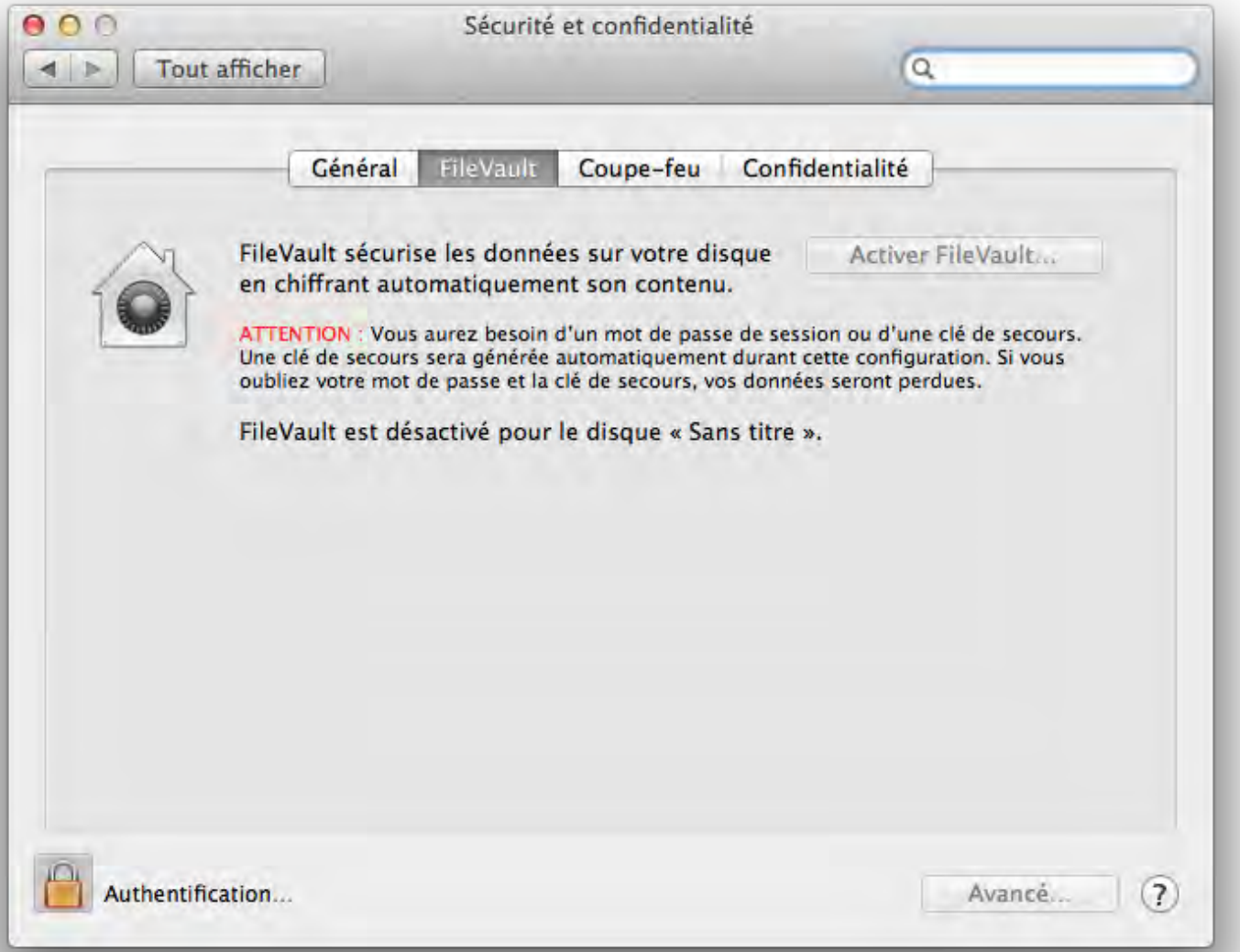
- Pré-requis : Mac OS X 10.7, 10.8 ou 10.9
- Transparent à l'utilisateur : l'ouverture d'une session déverrouille l'accès et permet le déchiffrement du disque.
- Références :
  - `https://aresu.dsi.cnrs.fr/IMG/pdf/CNRS-DR4-CRSSI-Chiffrement_FileVault2-v1-0.pdf`
  - `http://support.apple.com/kb/HT4790?viewlocale=fr_FR`
  - `https://aresu.dsi.cnrs.fr/IMG/pdf/manuel.pdf`

Mac OS : FileVault 2

Ouvrir les préfér ences système et cliquer dans ≪ Sécurité et confidentialité ≫

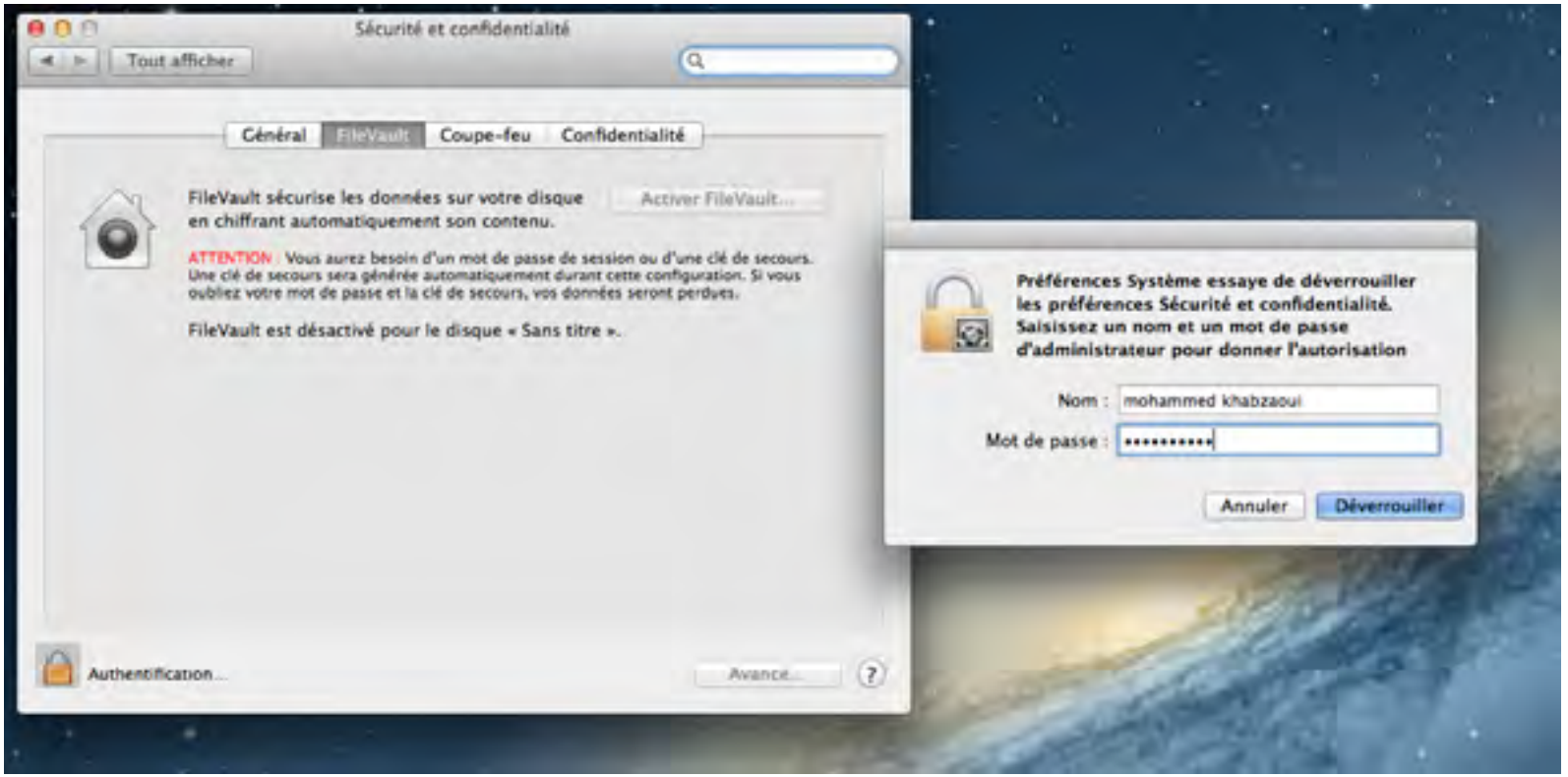
Mac OS : FileVault 2

Cliquer dans ≪ FileVault ≫ :

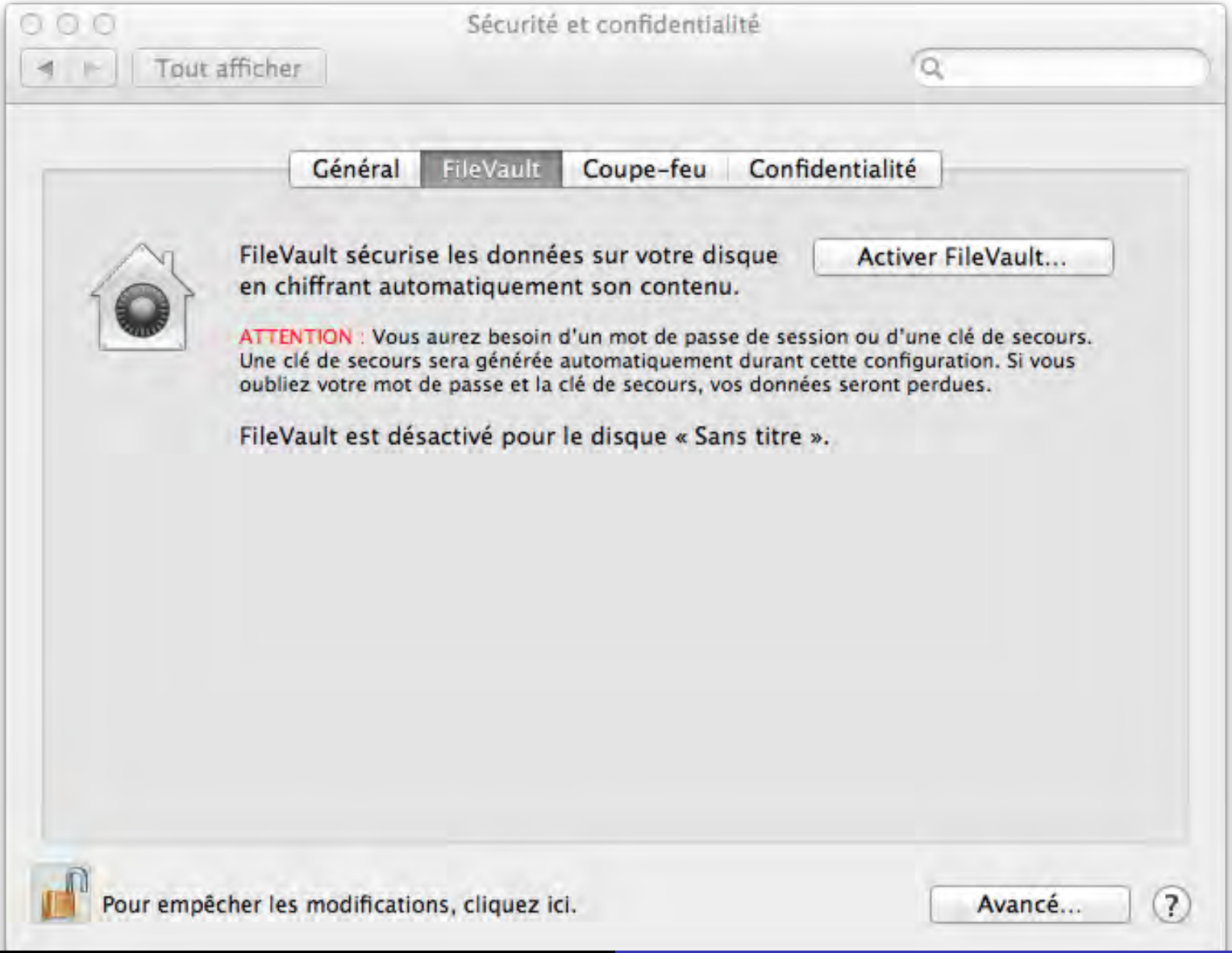


Mac OS : FileVault 2

Cliquez dans le cadenas pour pouvoir activer FileVault :



Cliquez dans « Activer FileVault »

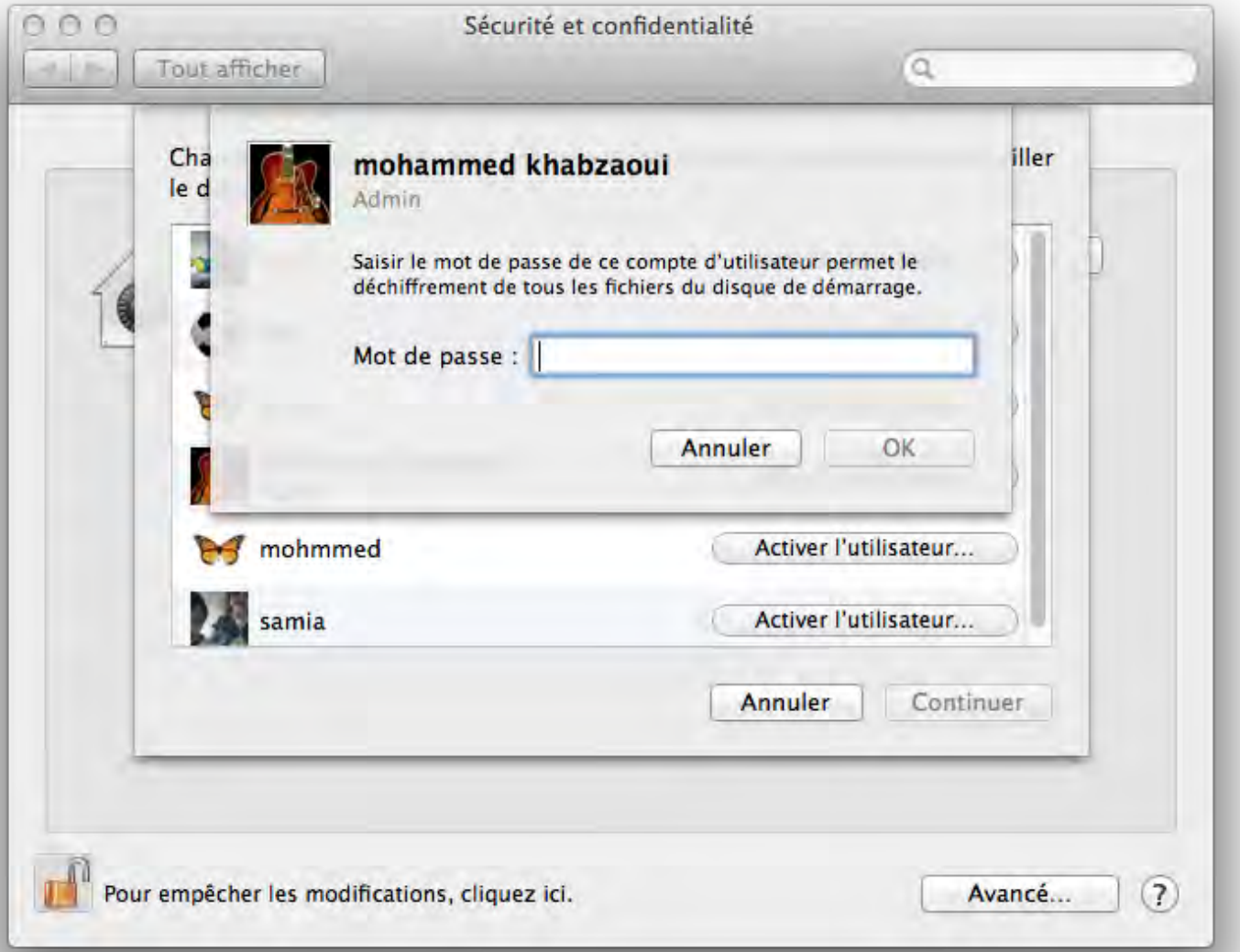


Mac OS : FileVault 2

Autoriser les utilisateurs :

Mac OS : FileVault 2

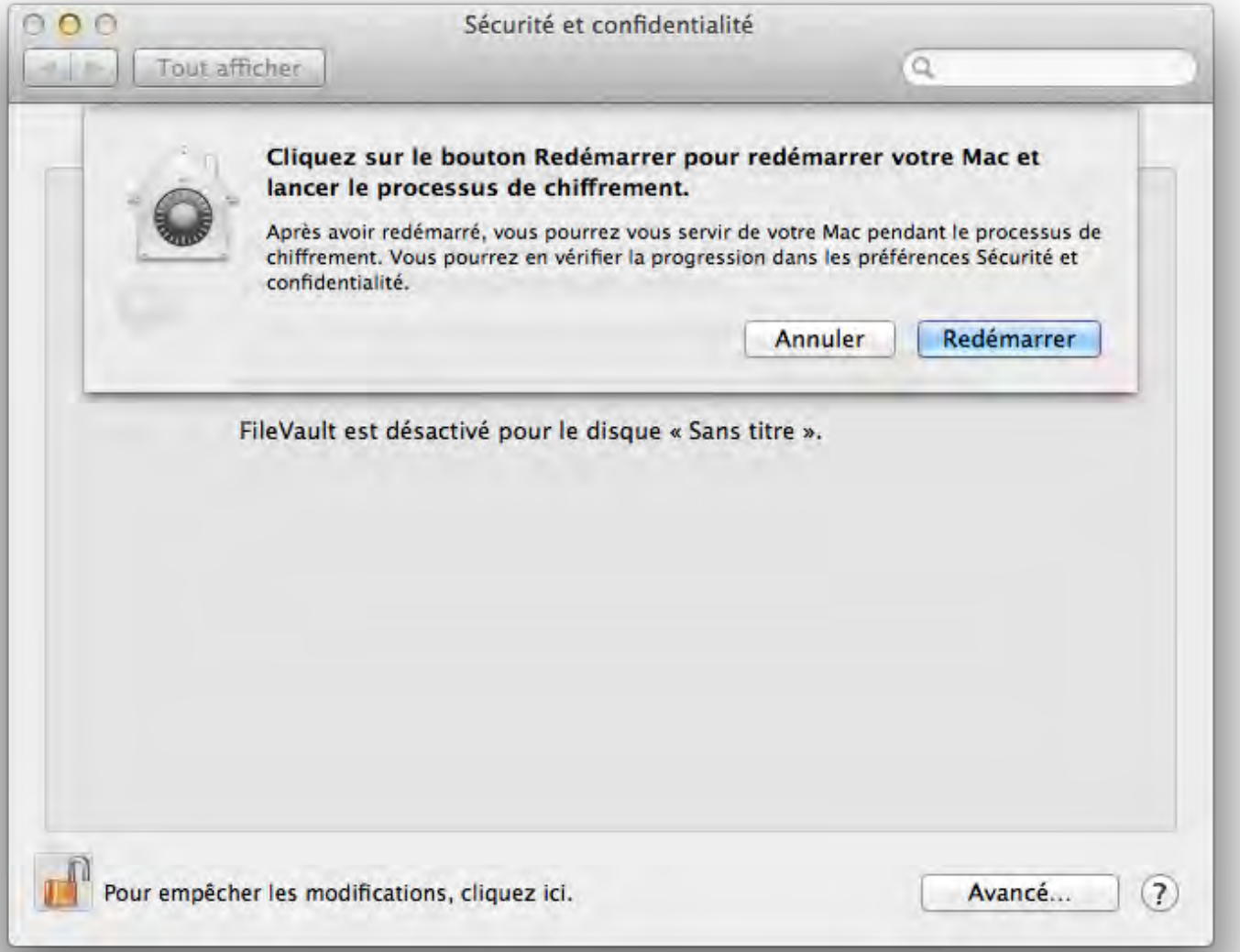
Saisir le mot de passe de chaque utilisateur autorisé



La clé de secours

Ne jamais stocker la clé de secours dans un tiers

Redémarrer


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.
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

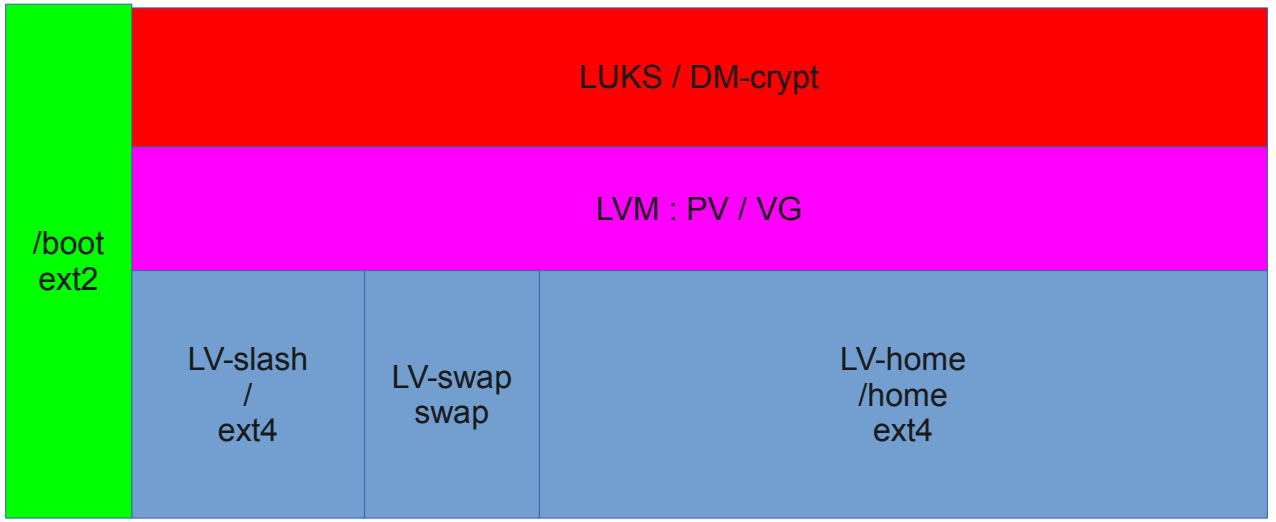
Recouvrement

- Avec un compte admin Démarrer la machine avec le compte d'admin Changer le mot de passe de l'utilisateur
- 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 .
- 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

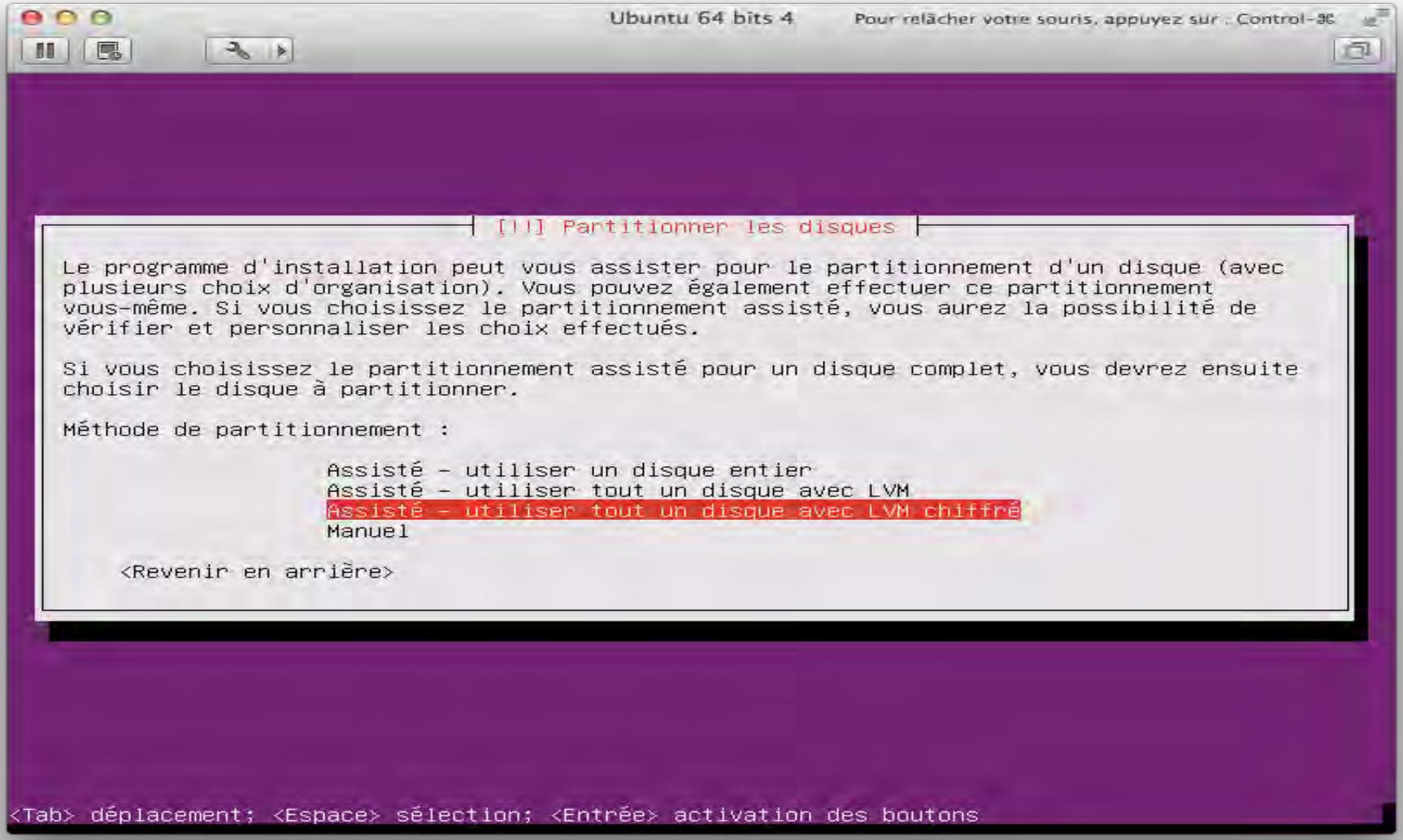
LUKS : Linux Unified Key Setup : standard de gestion du chiffrement



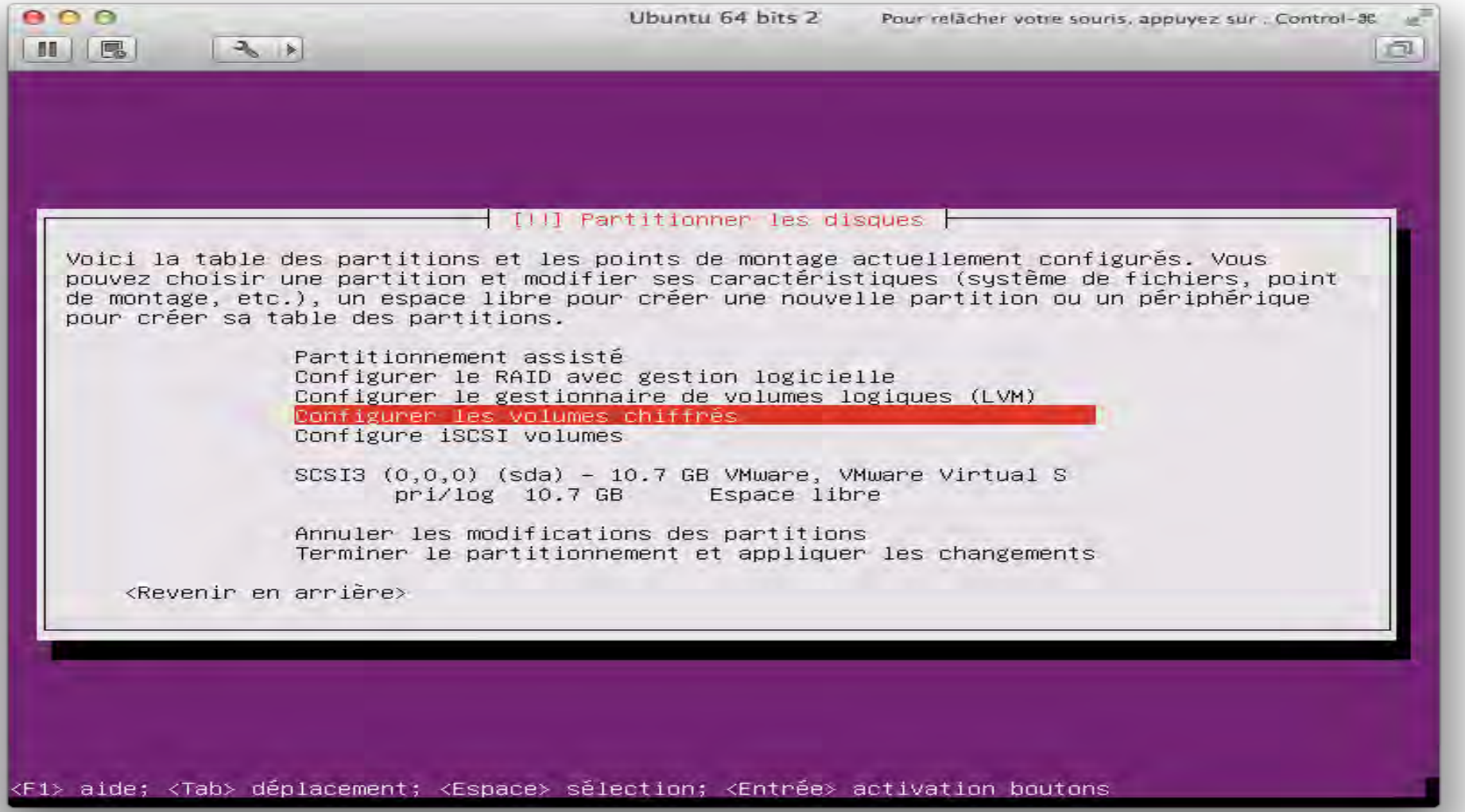
dm-crypt
(debian, ubuntu ...)

- 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

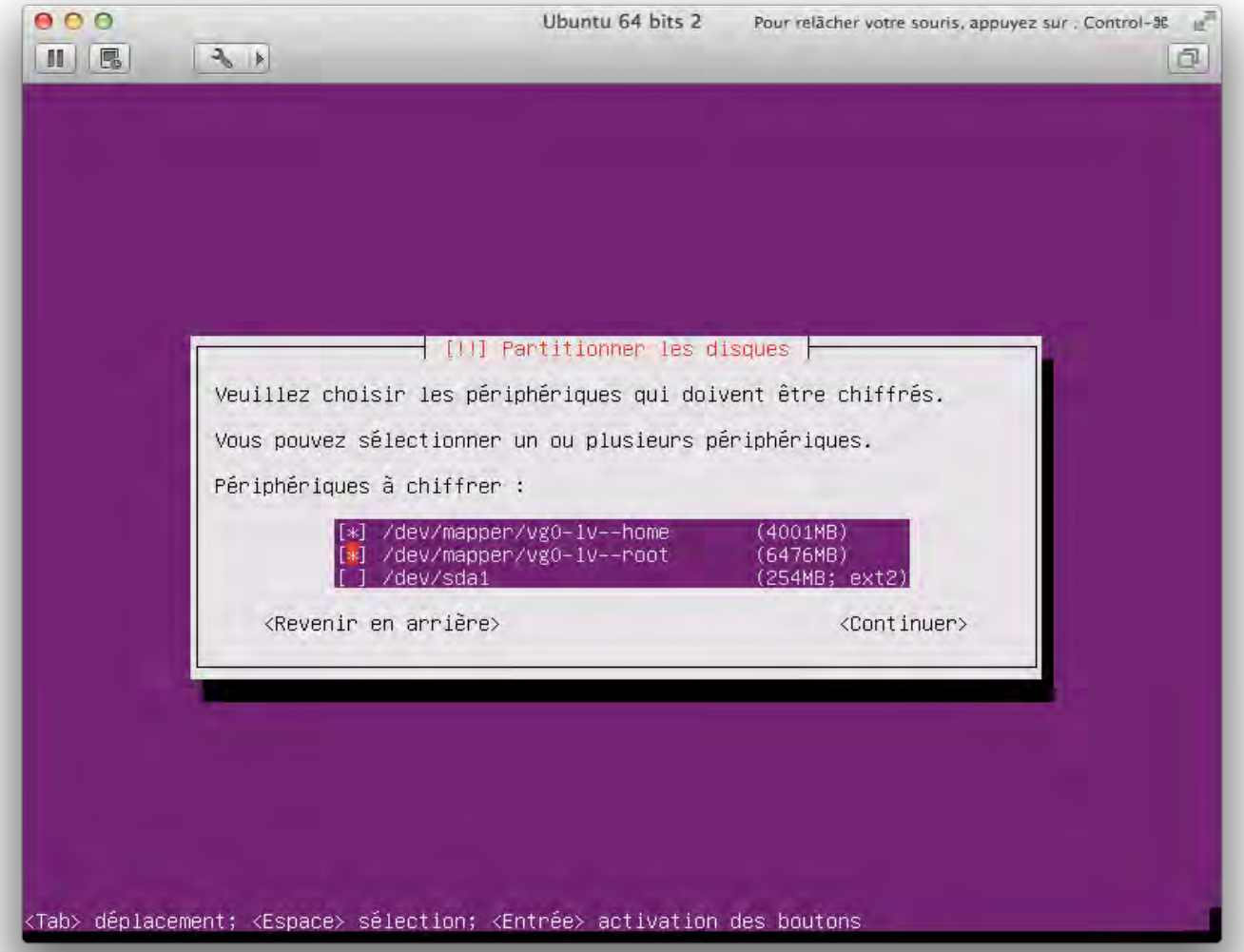
Choisir un disque avec LVM chiffré



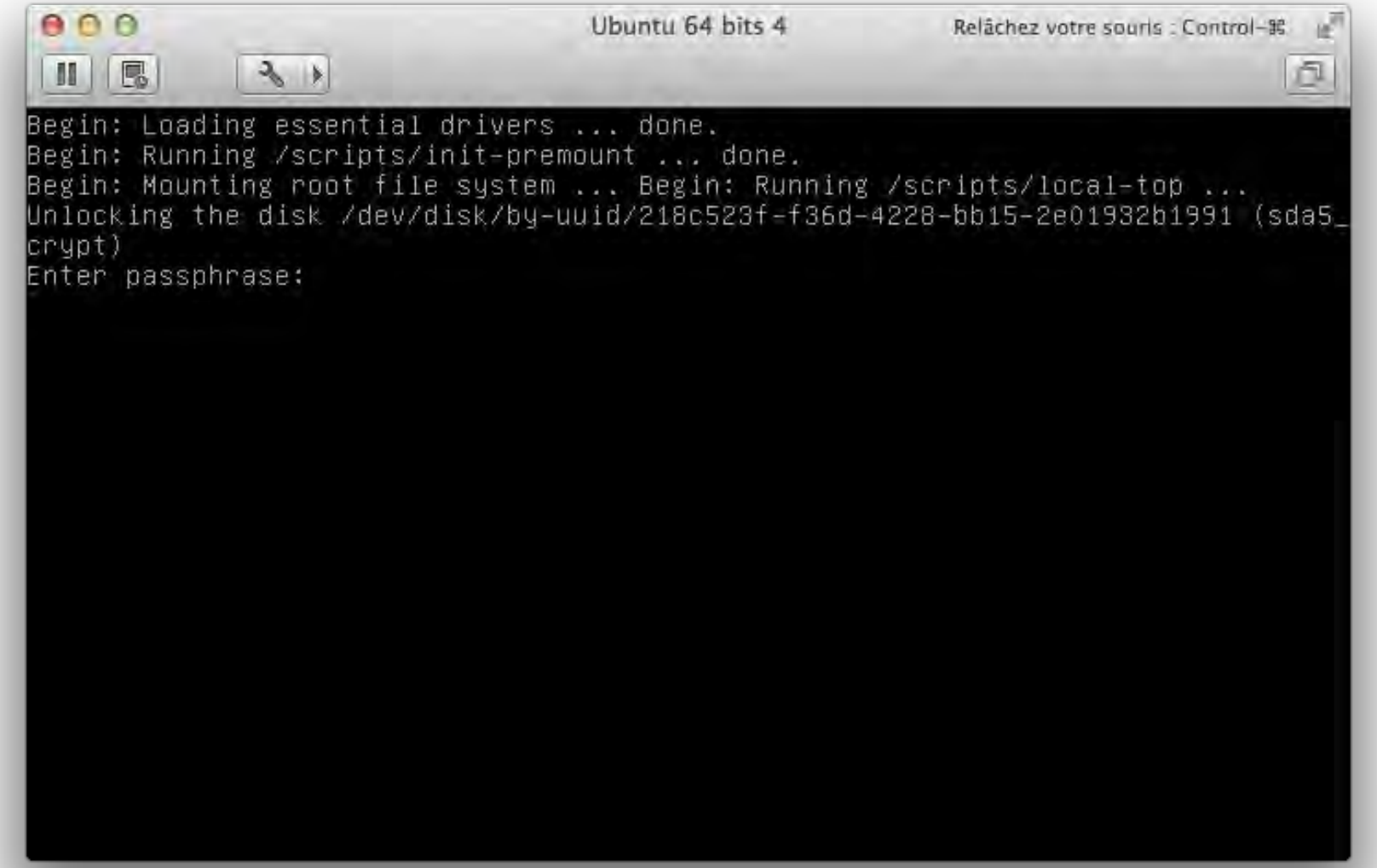
Configurer les volumes



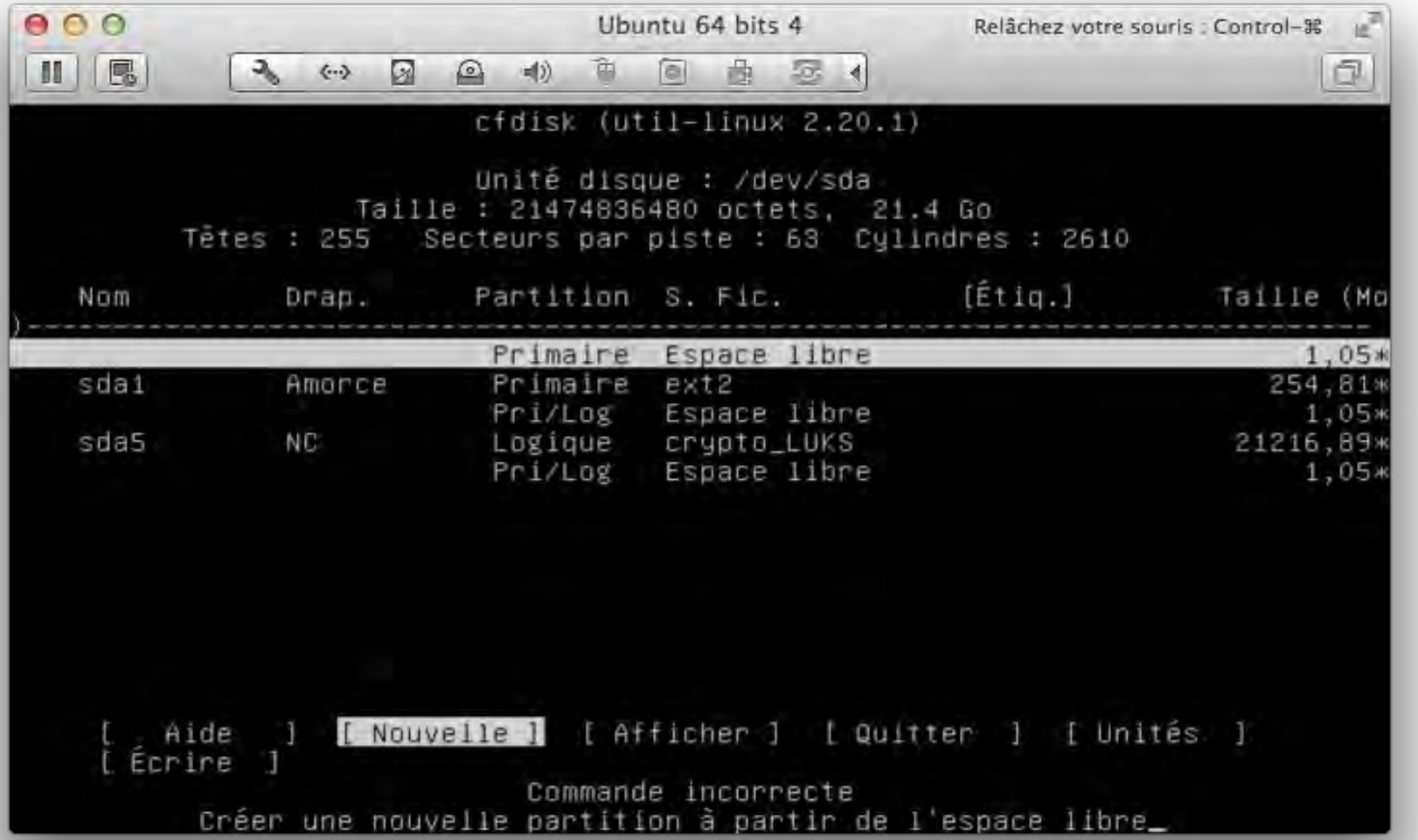
Configurer les volumes chiffrés



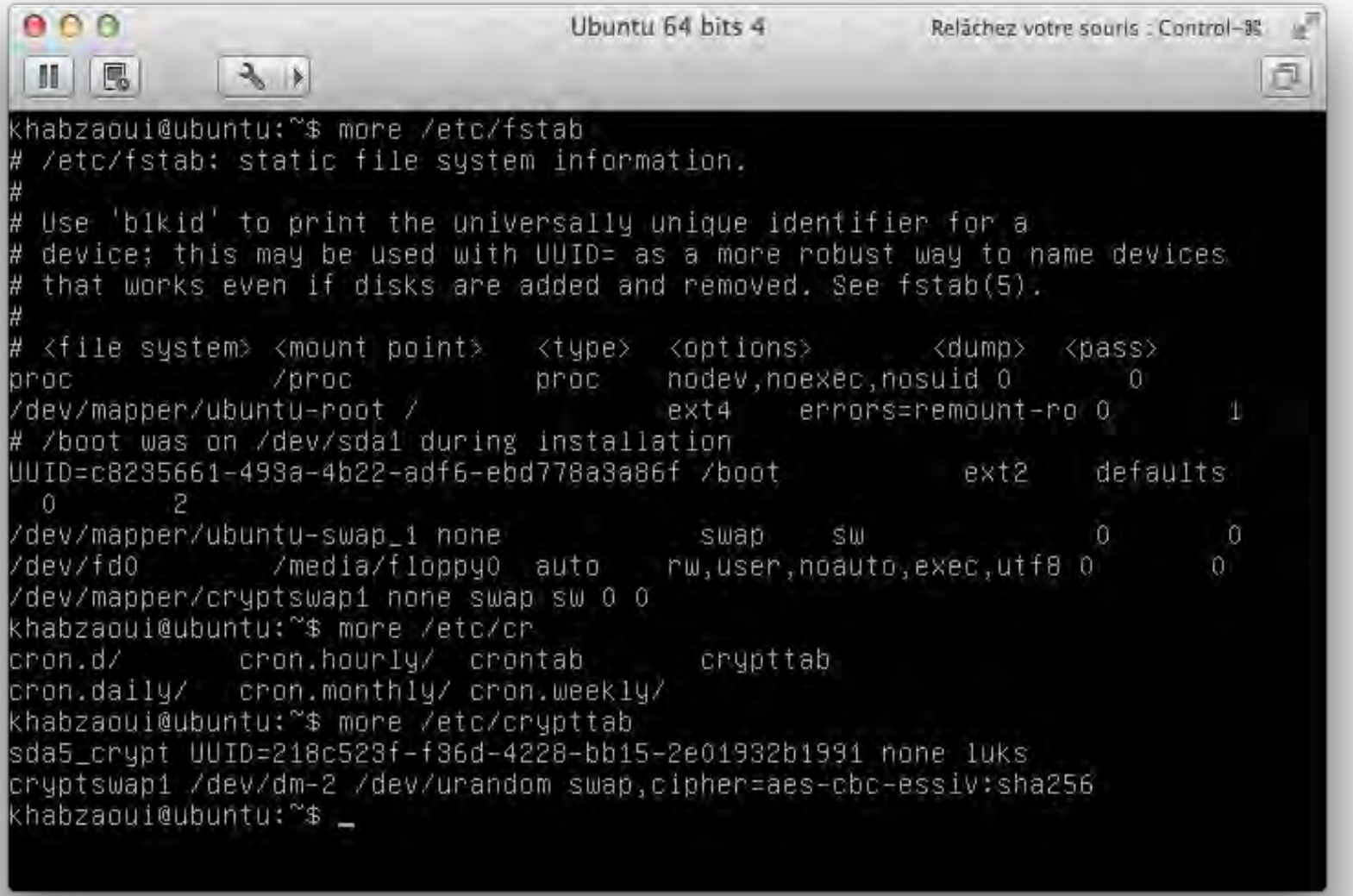
Démarrage du système



Les partitions du disque



/etc/fstab et /etc/crypttab



Gestion des passphrases

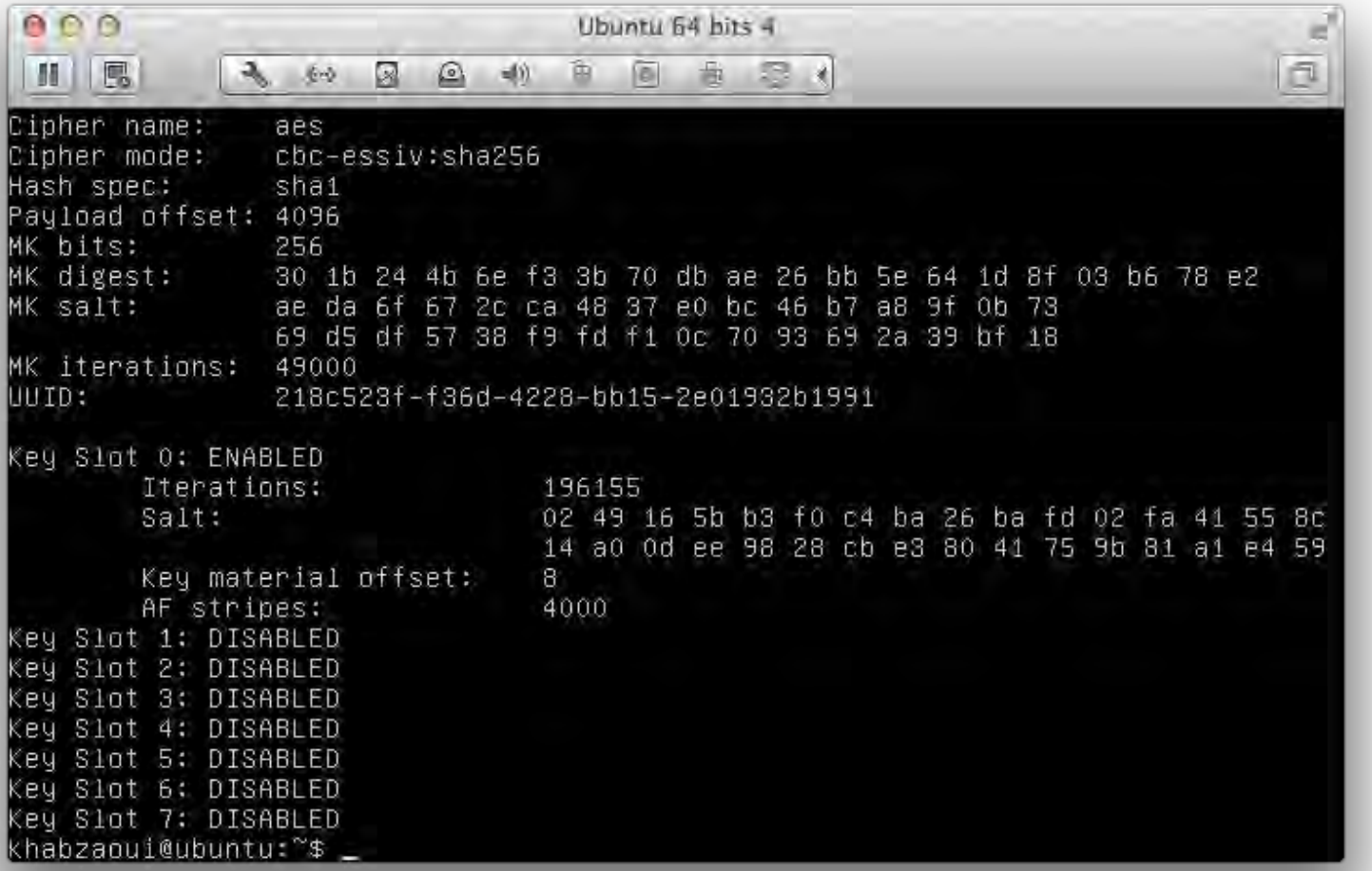
LUKS permet de stocker jusqu’à 8 passphrases

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)

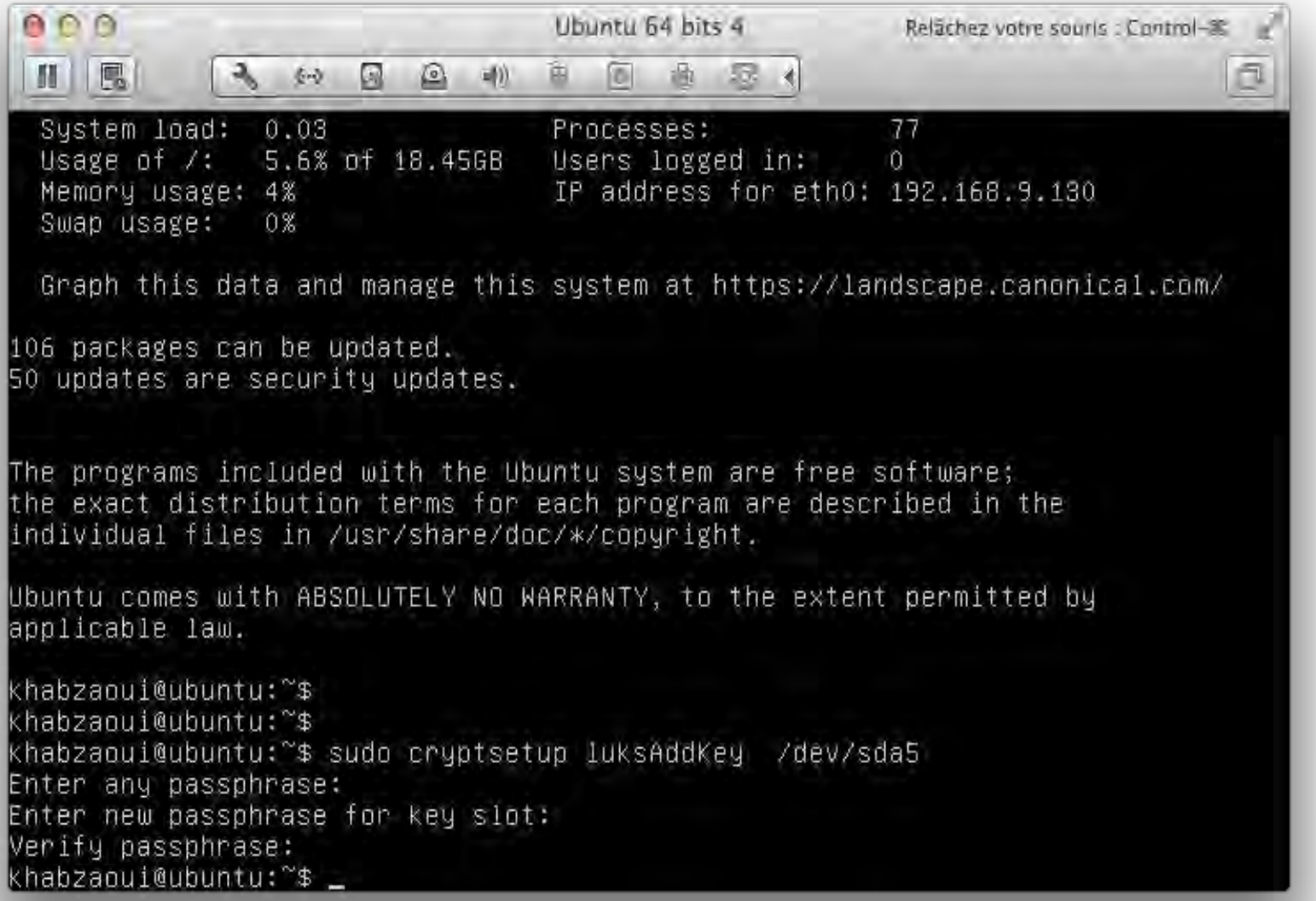
Lister les slots initiaux

sudo cryptsetup luksDump /dev/sda5



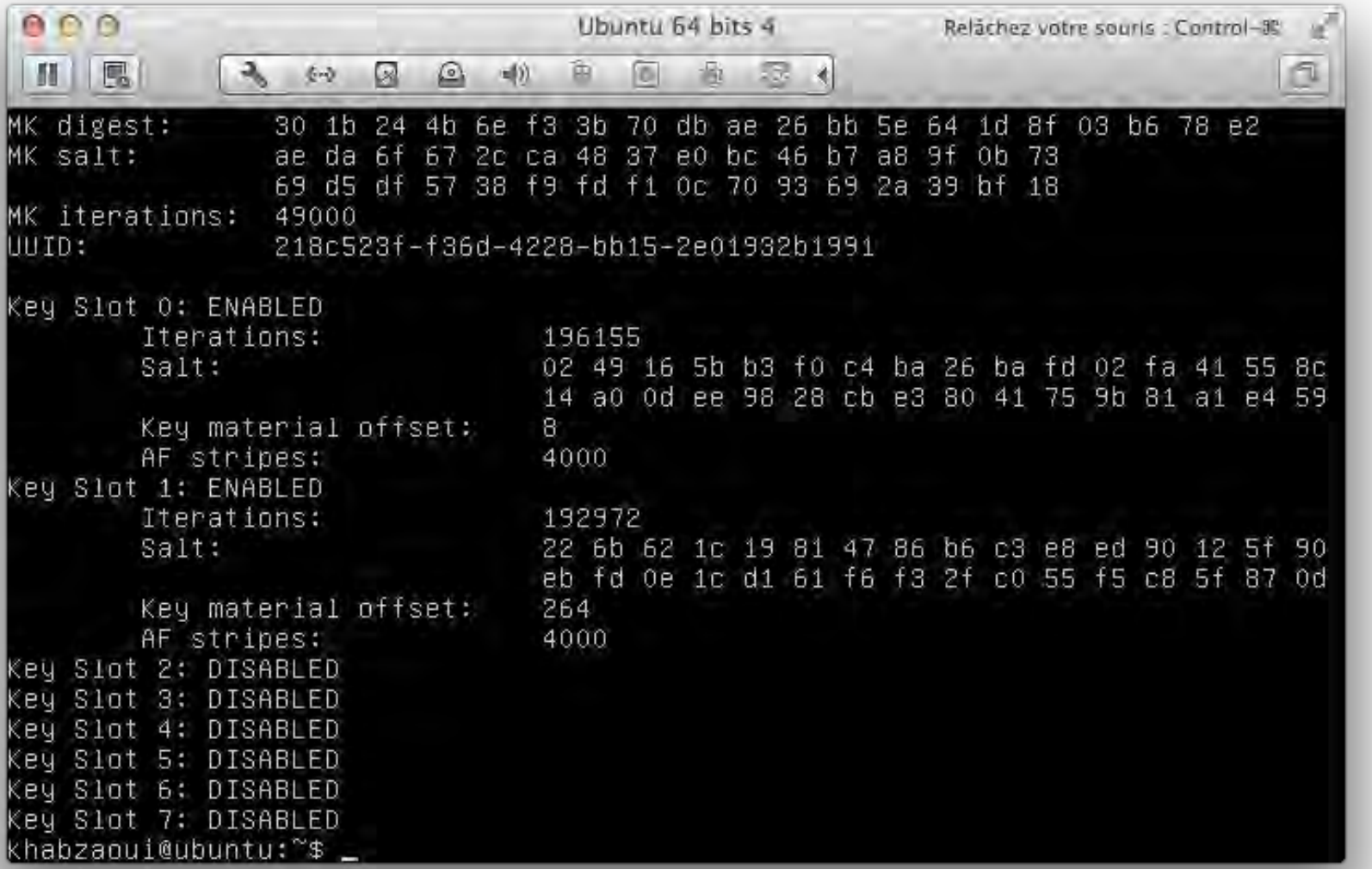
Ajout d'une passphrase

sudo cryptsetup luksAddKey /dev/sda5



Lister les slots

sudo cryptsetup luksDump /dev/sda5



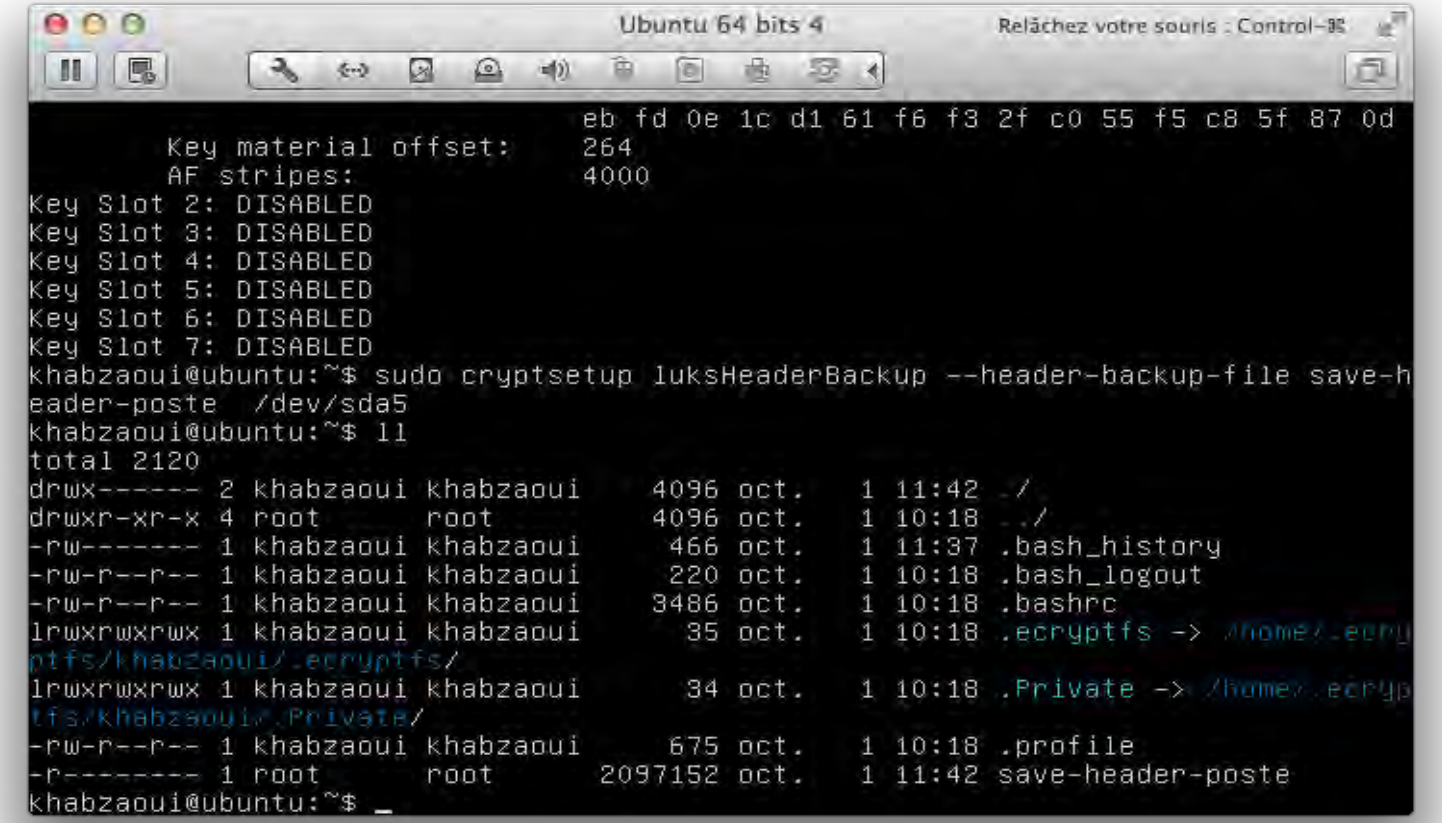
Supprimer une passphrase

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



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 :

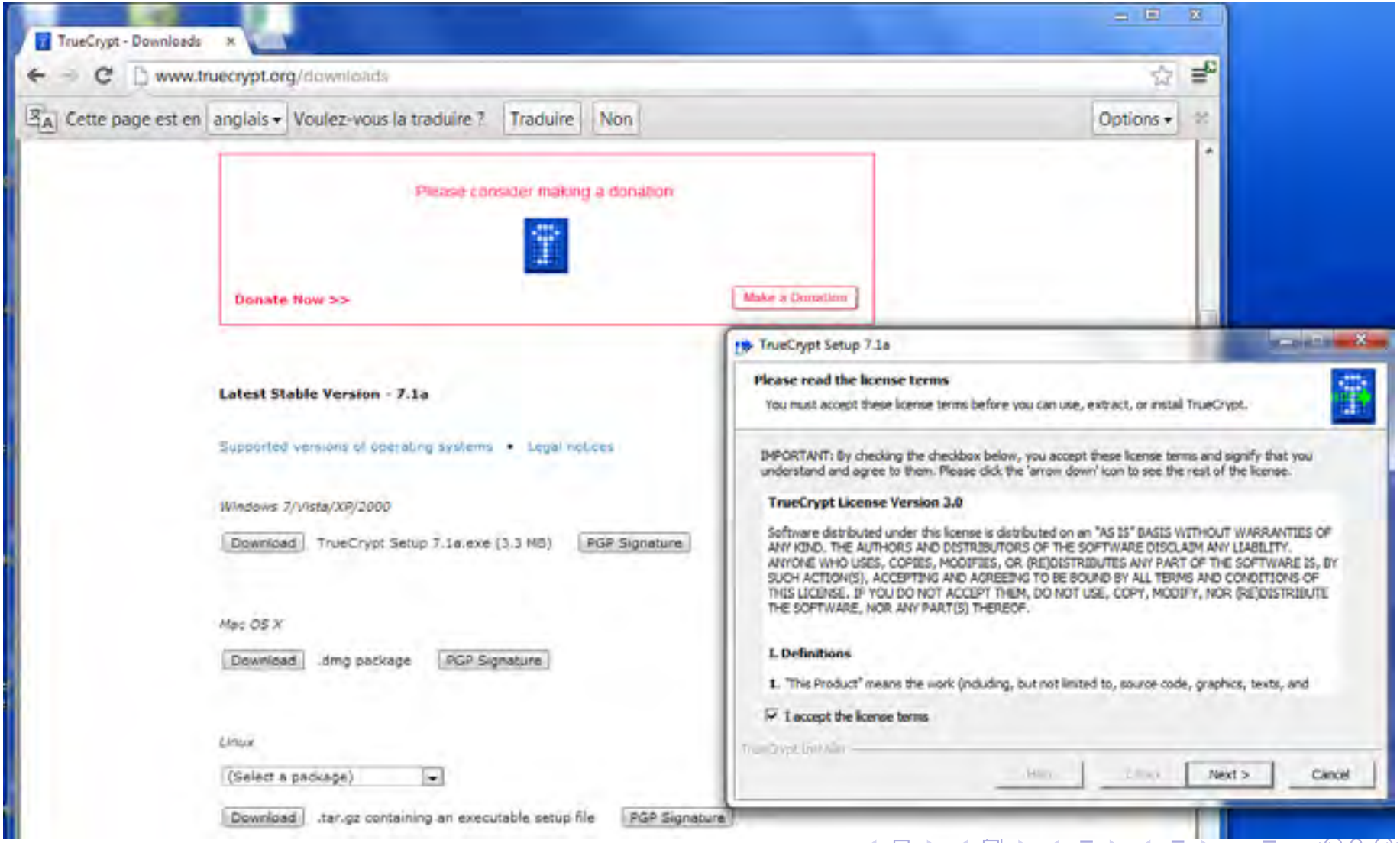
mkswap /dev/mapper/ubuntu-swap

mkfs.ext4 /dev/mapper/ubuntu-root

Chiffrement des portables Windows

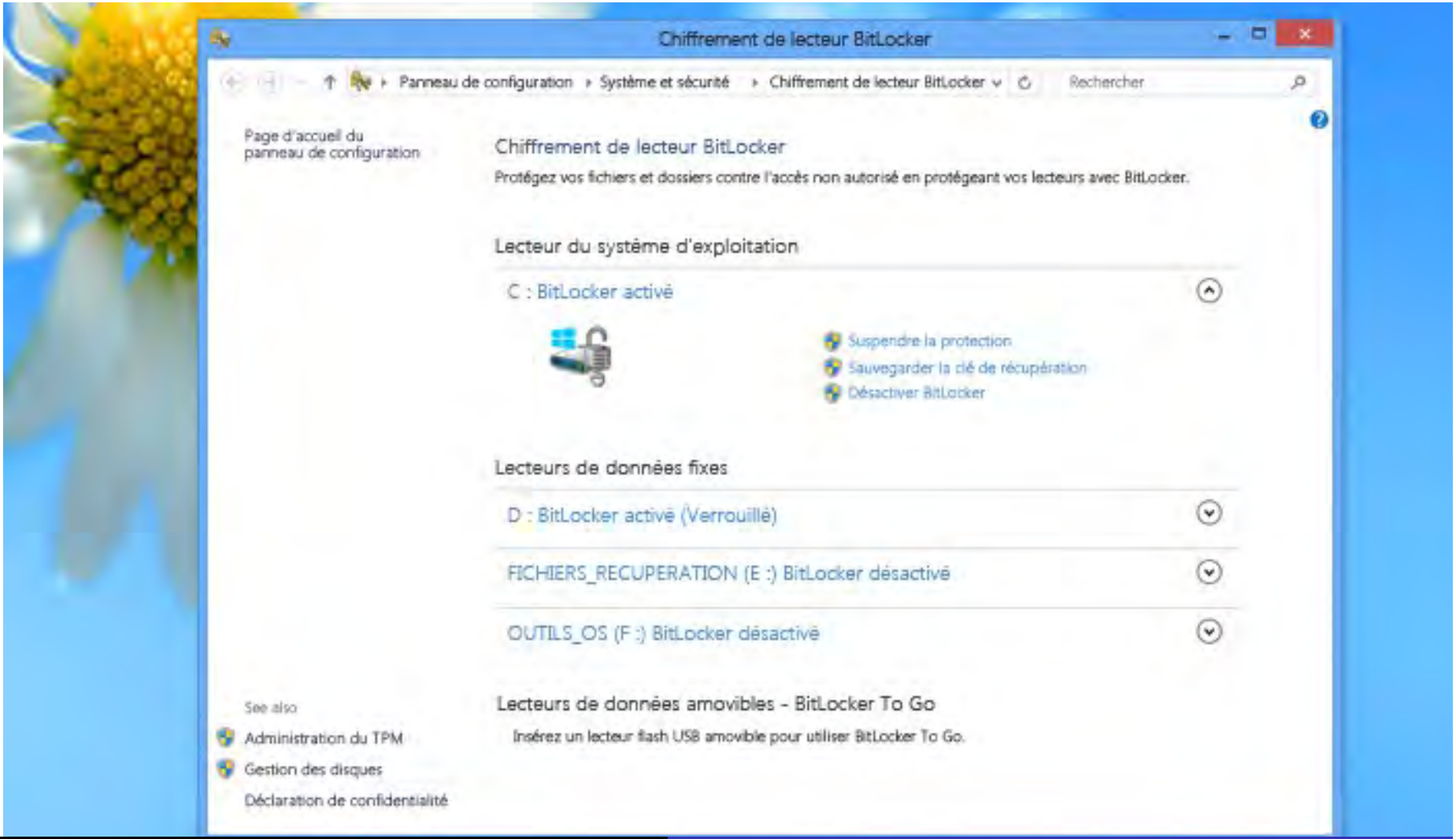
- Disque auto-chiffrant
- TrueCrypt
- BitLocker (solution intégrée dans windows 8)

Pour Windows (disponible aussi pour mac et linux)



Windows 8 : BitLocker

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

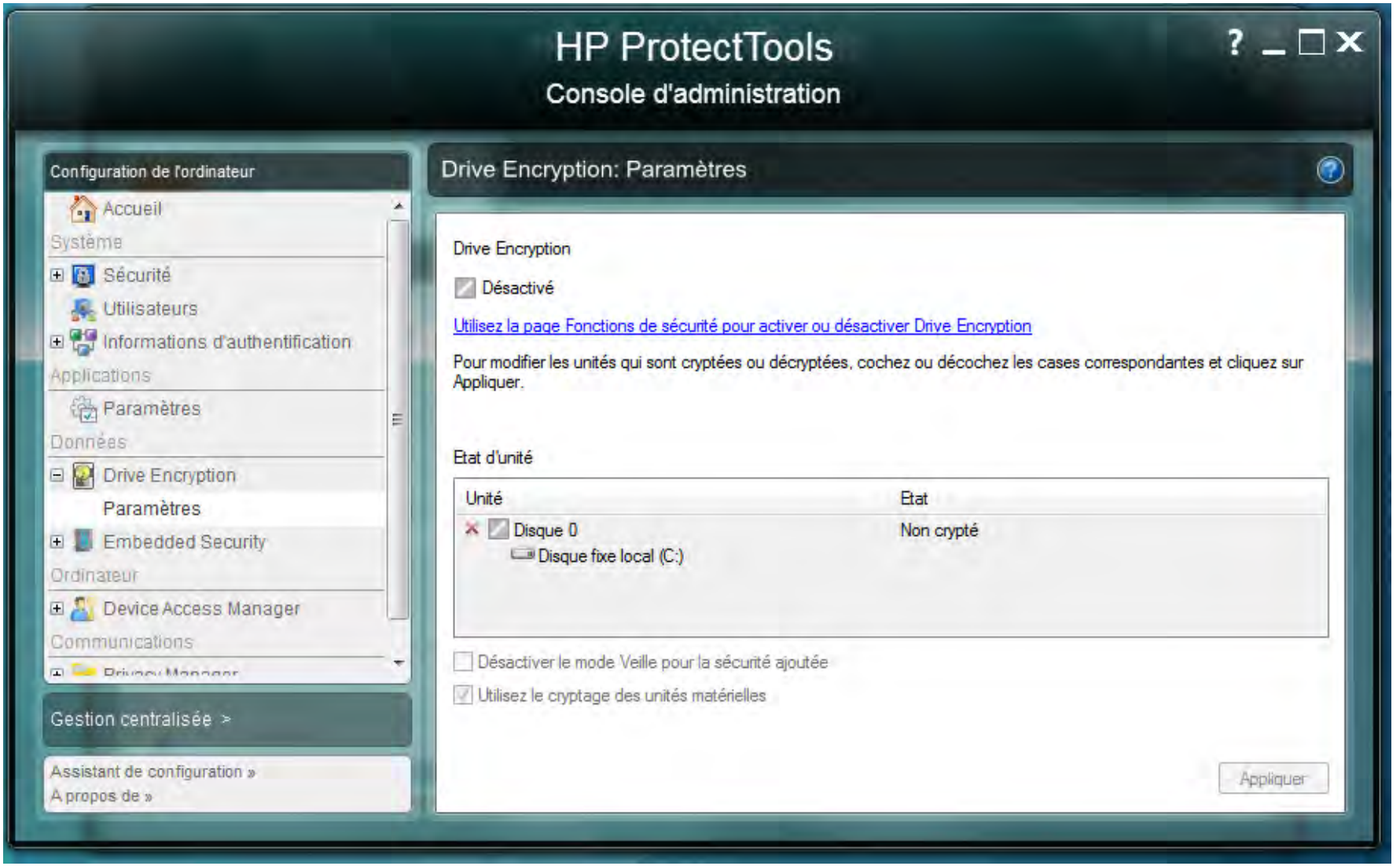


HP ProtectTools Security Manager

http://h10032.www1.hp.com/ctg/Manual/c01957815.pdf
Cliquez sur Démarrer ¿Tous les programmes¿Console d'administration de HP ProtectTools ou Cliquez sur le lien **Administration** dans le coin inférieur gauche de la console Security Manager.

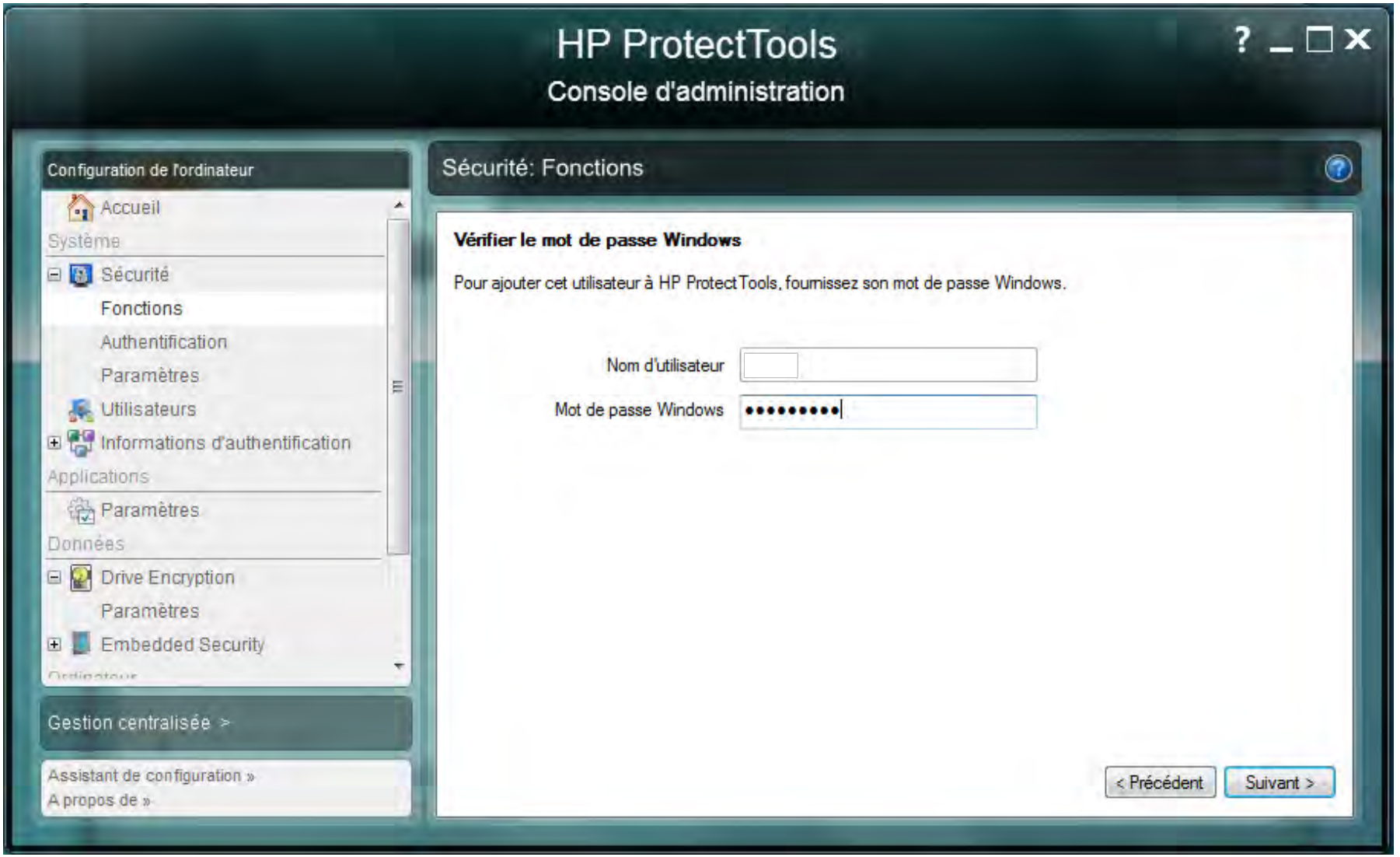
HP ProtectTools Security Manager

HP ProtectTools Security Manager



HP ProtectTools Security Manager

HP ProtectTools Security Manager



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 portable OK mais à quel Prix !

- Choix limité : Disque Chiffrant sur portables du marché
- Est-ce que les Disques Chiffrants sont utiles aujourd'hui ? (Chiffrement integré dans l'OS : Windows (Bitlocker), Mac (Filevault2), Linux (Dm-crypt))
- 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
  - Cloud privé
  - Clé USB chiffrée (matériel ou logiciel)