Chiffrement de disques : Linux et Mac OS X

Matthieu Herrb

LAAS-CNRS

http://homepages.laas.fr/matthieu/talks/chiffrement-linux-mac.pdf

29 janvier 2013

Introduction

- Chiffrement des disques obligatoire dans unités CNRS depuis le 1er janvier...
  `https://aresu.dsi.cnrs.fr/spip.php?rubrique99`
- Techniques retenues :
  - pour Linux : dm-crypt + LUKS sur toutes les partitions
    Applicable simplement sur distributions récentes
  - pour Mac OS X : FileVault 2
  - Supports amovibles : TrueCrypt

Linux

La technologie dm-crypt/LUKS

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

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

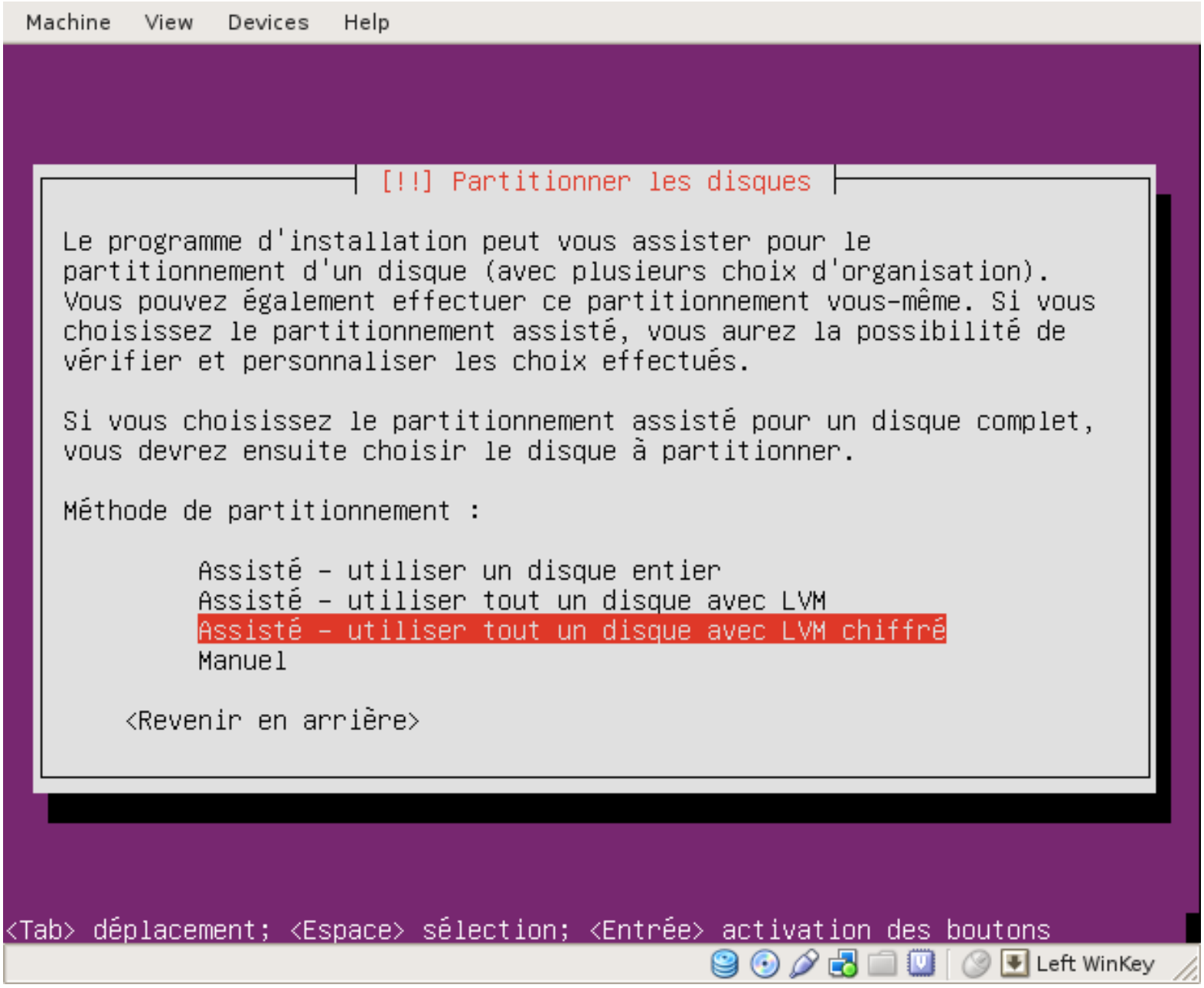
dm-crypt : chiffrement de devices virtuels en mode bloc

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

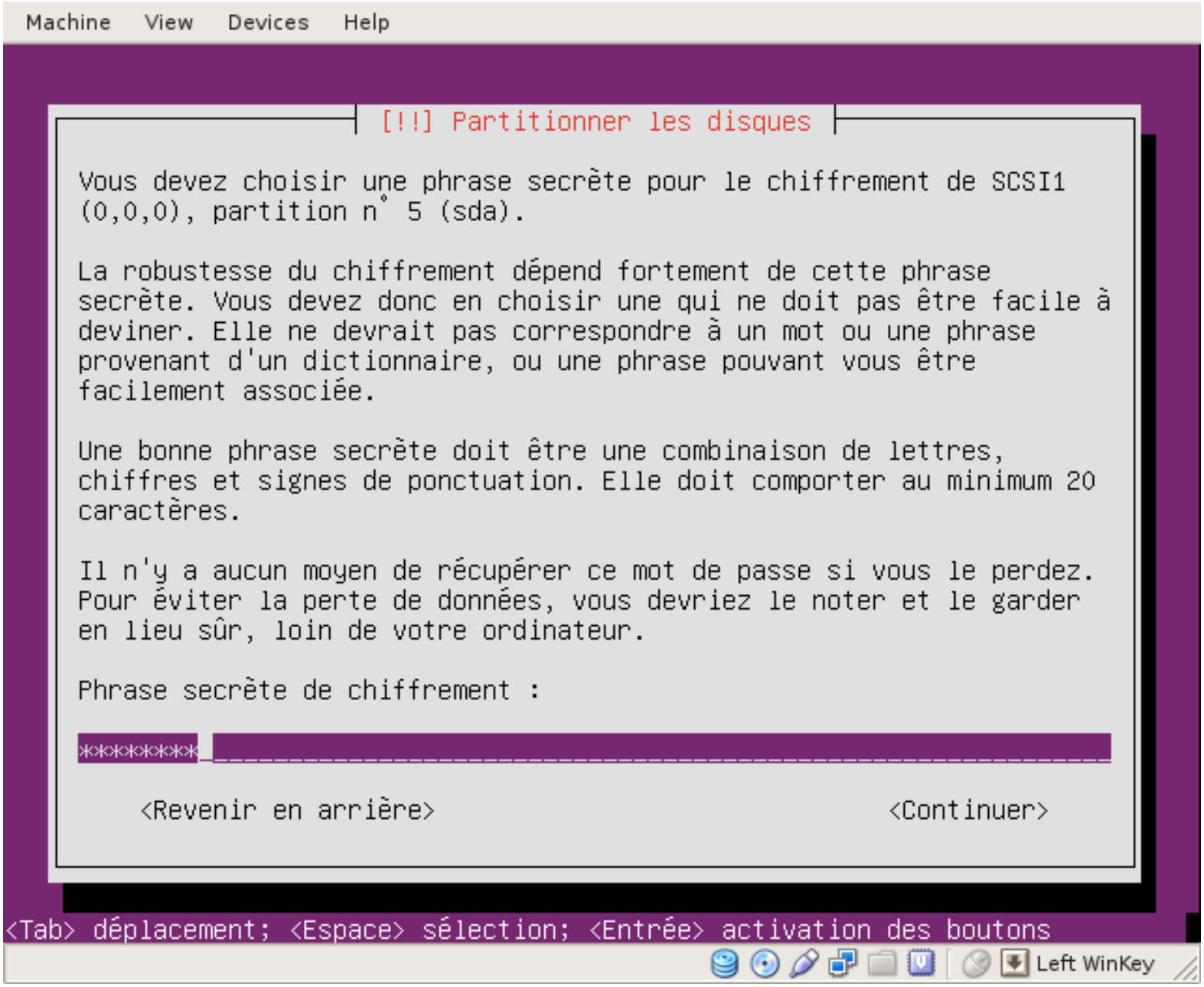
Installation Ubuntu 12.04

- 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.

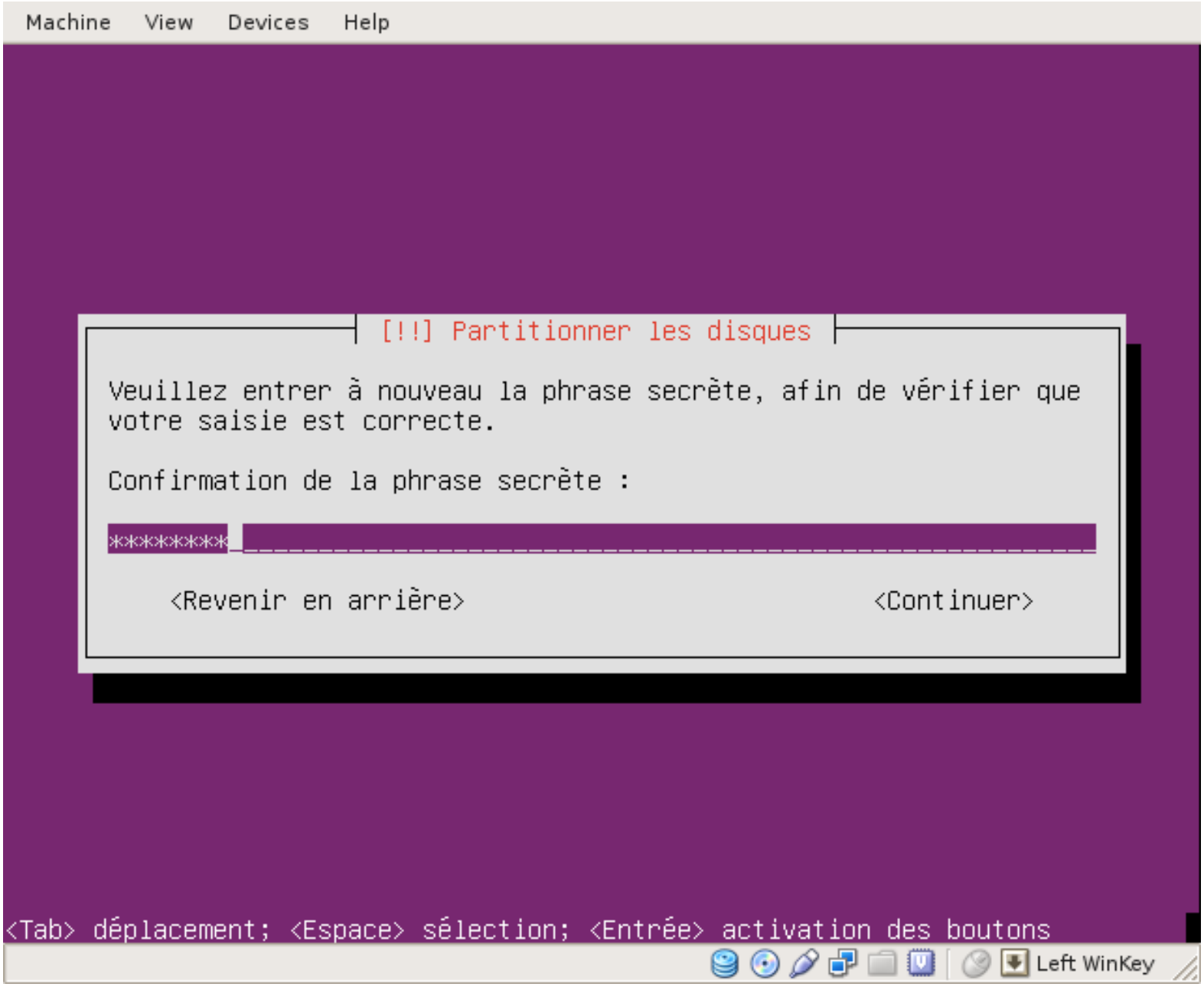
Choisir un disque avec volume LVM chiffré :



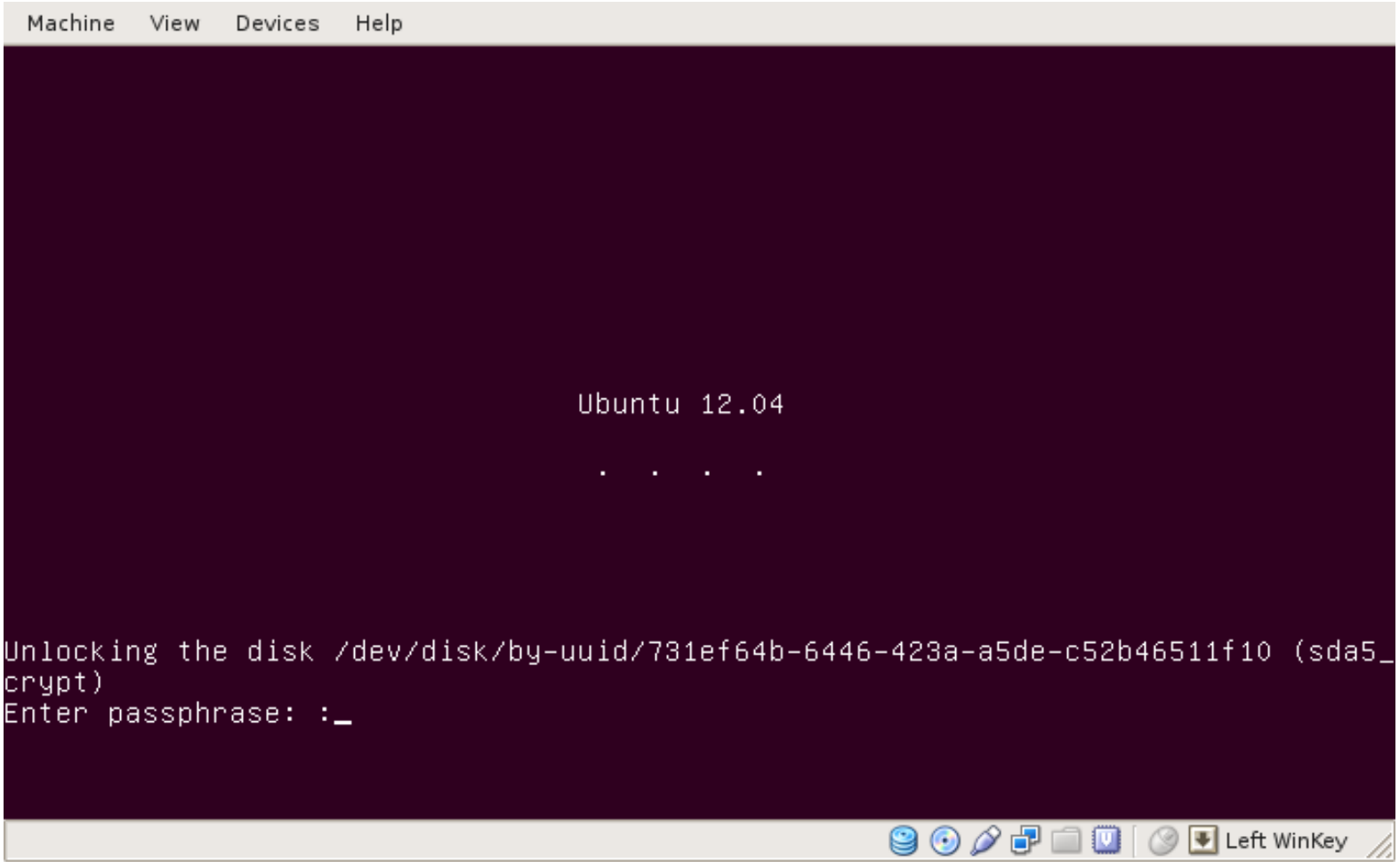
Spécifier une phrase secrète :



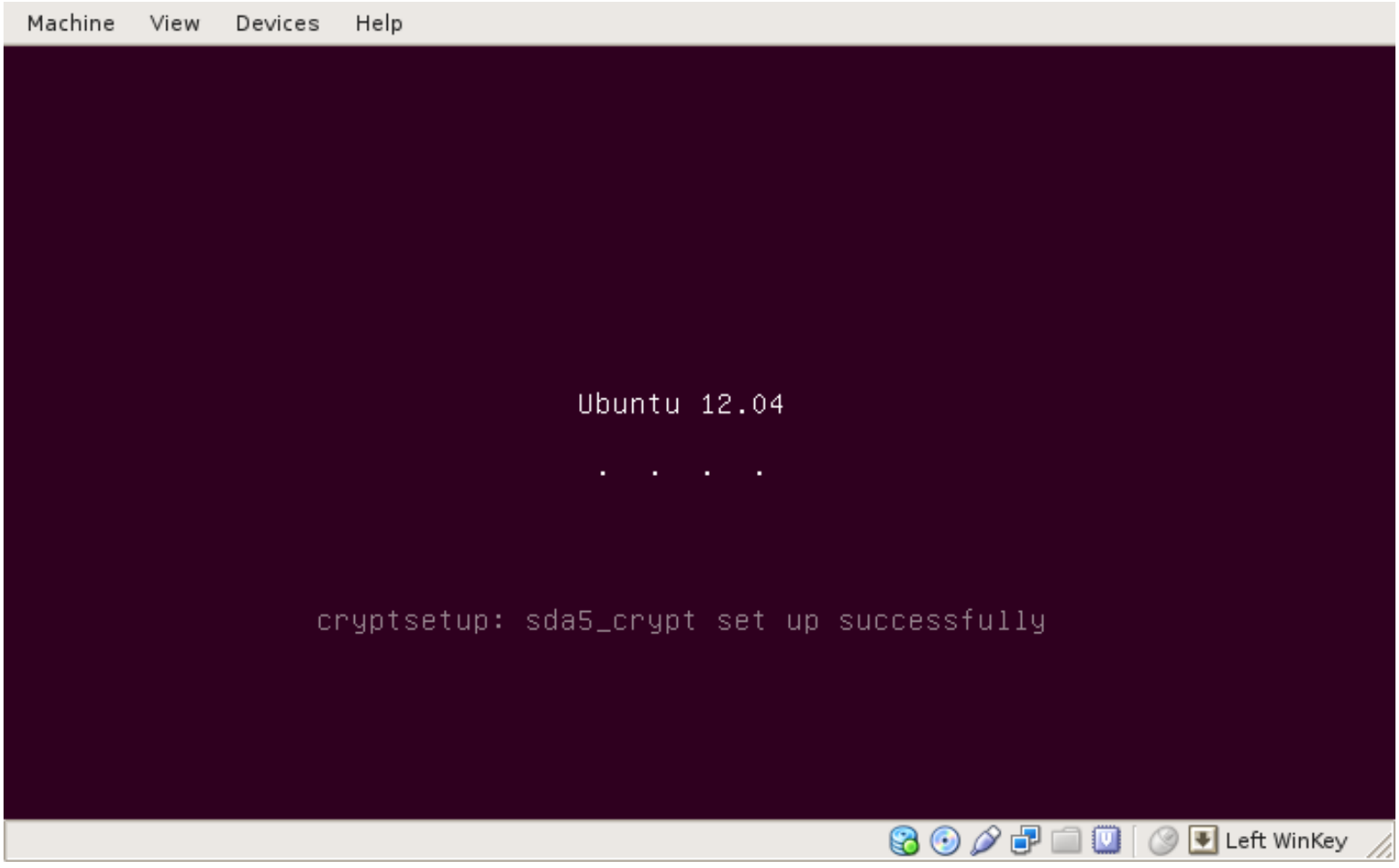
Confirmer la phrase secrète :



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` en 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`

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 TrueCrypt et chiffrer avec TrueCrypt

Attention au séquestre des mots de passe de chiffrement

Mac OS X

Introduction

- Technique retenue : FileVault 2
- Pré-requis : Mac OS X 10.7 (Lion) ou 10.8 (Mountain Lion)
- Références :
  - `https://aresu.dsi.cnrs.fr/IMG/pdf/CNRS-DR4-CRSSI-Chiffrement_FileVault2-v1-0.pdf`
  - `http://support.apple.com/kb/HT4790`

Modes de recouvrement

- à l'aide d'un certificat de recouvrement d'établissement, commun à tous les disques chiffrés.
- à l'aide d'une clé de recouvrement générée lors de l'activation de FileVault.

Génération d'un certificat de recouvrement

Sur une machine d'admin :

1. Créer le mot de passe principal via le panneau « utilisateurs et groupes », bouton « services »
2. Copier `/Library/Keychains/FileVaultMaster.keychain` vers un endroit sûr.
3. Ouvrir le trousseau FileVaultMaster et supprimer la « password key »
4. Quitter l'application trousseau de clés.
5. Le fichier `/Library/Keychains/FileVaultMaster.keychain` est prêt à être utilisé pour chiffrer des disques.

Installation

- FileVault s'active *après* l'installation du système.
  - Soit via l'outil préférences système
  - Soit en ligne de commande : `fdesetup`
- Définit une liste d'utilisateurs autorisés.

Sans certificat de recouvrement

- Plus adapté pour une machine isolée ou un petit parc de machines.
- Créer un utilisateur d'admin dont on conserve le mot de passe en lieu sûr.
- Lancer le chiffrement, en autorisant l'utilisateur créé ci-dessus à ouvrir le disque :

```
sudo fdesetup enable -user <login>
```

- à la fin du chiffrement copier dans un lieu sûr la clé de recouvrement (chaîne de la forme AAAA-BBBB-CCCC-DDDD-EEEE-FFFF)

Avec un certificat de recouvrement

- copier le trousseau FileVaultMaster dans `/Library/Keychains/` sur la machine à chiffrer
- démarrer le chiffrement :

```
sudo fdesetup enable -keychain -norecoverykey
    -forcerestart
```

- vérifier l'avancement du chiffrement

```
sudo fdesetup status
```

Ajout d'utilisateurs

Seuls les utilisateurs déclarés apparaissent dans l'écran de boot et peuvent donc démarrer la machine.

```
fdesetup add -usertoadd <login>
```

Liste des utilisateurs

```
sudo fdesetup list
```

Recouvrement

Le plus simple

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

Avec la clé de recouvrement de la machine

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

Avec un certificat maître

- Booter de la partition de réparation (Cmd-R)
- Monter un disque externe ou une clé USB contenant la copie de sauvegarde du trousseau
- débloquer le volume chiffré avec le trousseau de secours

Supports Amovibles

En fonction de l'usage :

- lecture seulement par des Macs :
  via Utilitaire Disque, formatter avec chiffrement
- partage avec autres systèmes :
  Installer TrueCrypt et chiffrer avec TrueCrypt

Attention au séquestre des mots de passe de chiffrement

Autres systèmes

- Android : chiffrement mémoire flash et carte SD à partir de la version 3.0 - pas de recouvrement
- IOS (iTrucs) : `http://www.ilounge.com/index.php/articles/comments/ios-encryption-and-data-protection/`
- OpenBSD : softraid(4) + clé sur support externe `http://www.undeadly.org/cgi?action=article&sid=20110530221728`
- FreeBSD : `http://www.freebsd.org/doc/fr_FR.ISO8859-1/books/handbook/disks-encrypting.html`