

# PC Linux chiffré (dm-crypt)

J.Beigbeder, 25 juin 2013

## Installation double-boot

Avec Ubuntu, prendre le CD alternate (text only)

[linux1.ogv] : usuel

Au moment de partitionner le disque, passer en manuel ([linux2.ogv], 1mn 26s):

- créer une partition /boot: /dev/sda5 ([linux2.ogv], 1mn42s à 1mn50s)
- avec l'espace libre, créer une partition pour encryption (1mn50s à 2mn03s)
- la configurer en encrypted (2mn9s à 2mn20s)
- l'installateur demande la clé (2mn26s)
- configurer LVM (2mn39s à 2mn54s)
- = créer un volume group (2mn55s à 3mn3s)
- = puis 3 logical volumes (3m4s à 3mn40s)
- et mettre dans chacun des 3 volumes: /, swap, /home (3mn44s à 4mn22s)

[linux3.ogv] : usuel

[linux4.ogv] : installation grub

Si dual-boot **AVEC** Windows chiffré, attention!  
Installer grub sur /dev/sda5!! ([linux4.ogv], 0m59s à 1mn7s)  
Donc bien en prévenir l'utilisateur (mises à jour).

Le boot/grub Linux demande le mot de passe: [linux5.ogv].

Principes du dual-boot ([linux5.ogv], 0mn16s):

- soit on tape le mot de passe TrueCrypt, et le Windows chiffré démarre
- soit on tape Escape, il y a alors recherche de partitions bootables, donc on arrive sur le grub sur /dev/sda5.
- et on voit alors le menu grub (qui ne propose pas Windows) (non reconnaissable par grub-install car chiffré.

## Vérifications (boot sur support externe)

LVM et dm-crypt ont faits:

```
# cryptsetup luksOpen /dev/sda6
# ls -l /dev/mapper/
total 0
drwxr-xr-x  2 root root    140 Jun 25  2013 ./
drwxr-xr-x 19 root root   4520 Jun 25 09:43 ../
crw-----  1 root root 10, 236 Jun 25 09:31 control
lrwxrwxrwx  1 root root     7 Jun 25 09:31 linux-home -> ../dm-3
lrwxrwxrwx  1 root root     7 Jun 25 09:31 linux-slash -> ../dm-1
lrwxrwxrwx  1 root root     7 Jun 25 09:31 linux-swap -> ../dm-2
lrwxrwxrwx  1 root root     7 Jun 25 09:31 sda6_crypt -> ../dm-0
```

dm-crypt permet de mettre jusqu'à 8 clés:

```
# cryptsetup luksAddKey /dev/sda6
# cryptsetup luksKillSlot /dev/sda6 1
```

truecrypt (Linux) permet d'accéder à la partition Windows chiffrée:

```
# truecrypt /dev/sda3 /mnt
# df
# truecrypt -d /dev/sda3
```

## Clonage ou ré-installation

Si clonage, il faut d'abord créer les partitions pour /boot et la partition LVM chiffrée:

```
# fdisk /dev/sda
... 200 Mo pour /boot (disons /dev/sda5)
... le reste pour LVM (disons /dev/sda6)
# cryptsetup -verbose -verify-passphrase -c aes-cbc-plain luksFormat /dev/sda6
# cryptsetup luksOpen /dev/sda6 sda6
# pvcreate /dev/mapper/sda6
# vgcreate ubuntu /dev/mapper/sda6
# lvcreate -L 15G -n slash ubuntu
# lvcreate -L 8G -n swap ubuntu
# vgdisplay -C (affiche l'espace libre)
# lvcreate -L LE_RESTE -n home ubuntu
# mkswap /dev/mapper/ubuntu-swap
```

Si ré-installation, il faut déchiffrer et sauver quelques informations:

```
# cryptsetup luksOpen /dev/sda6 sda6
# mount /dev/mapper/ubuntu-slash /mnt
# chroot /mnt
# tar cf /TARS /etc
# dpkg -l > /ALL-PKGS
# exit
# mkdir /a/USER
# cp /mnt/TARS /mnt/ALL-PKGS /a/USER
# umount /mnt
```

Clonage ou ré-installation, cela est:

```
# mkfs.ext3 -j /dev/sda5
# mkfs.ext4 -j /dev/mapper/ubuntu-slash
# mount /dev/mapper/ubuntu-slash /mnt
# cd /mnt
# restore rf /a/IMG/laptop-12.04/laptop-root.dump
# mount /dev/sda5 /mnt/boot
# cd /mnt/boot
# restore rf /a/IMG/laptop-12.04/laptop-boot.dump
# mount --bind /dev /mnt/dev
# mount --bind /sys /mnt/sys
# mount --bind /proc /mnt/proc
# chroot /mnt
# vi /etc/crypttab
sda6_crypt UUID=175e2dbd-bd18-4551-bf07-afb1b5c20934 none luks
où 175e2dbd-bd18-4551-bf07-afb1b5c20934 correspond à crypto_LUKS dans la sortie de blkid.
# vi /etc/initramfs-tools/conf.d/cryptroot
target=sda6_crypt,source=UUID=175e2dbd-bd18-4551-bf07-afb1b5c20934,key=none,rootdev,lvm=ubuntu-slash
target=sda6_crypt,source=UUID=175e2dbd-bd18-4551-bf07-afb1b5c20934,key=none,lvm=ubuntu-swap
où 175e2dbd-bd18-4551-bf07-afb1b5c20934 correspond à crypto_LUKS dans la sortie de blkid.
# update-initramfs -k all -c
# update-grub
# grub-install /dev/sda si Windows est non chiffré
# grub-install --force /dev/sda5 si Windows est chiffré
# vi /etc/fstab
Vérifier les types de partition (ext3, ext4), mettre le bon UUID pour /boot.
# vi /etc/passwd /etc/shadow /etc/group /etc/lightdm/lightdm.conf
passwd : mettre le bon utilisateur
shadow : recopier le mot de passe chiffré
group : mettre le bon utilisateur
lightdm.conf (si auto-login) : mettre le bon utilisateur et sa session préférée
# exit
# reboot
```