INIST-CNRS

Chiffrement sous linux avec dm-crypt

Fabien PASCALE

Situation sur la machine
Avant chiffrement

Inist
Institut de l'Information Scientifique et Technique
Pôle système d'information

- Dual Boot : Windows 7 – Linux Debian
- Bootloader : Grub
- Utiliser LVM + chiffrer une partition existante :
  Partition linux système + données

Inist
Institut de l'Information Scientifique et Technique
Pôle système d'information

- Pré requis sur le système de départ :
  apt-get install lvm2 cryptsetup

- Boot LiveCD, sauvegarde des données
  # mount /dev/sda6 /mnt/sys
  # rsync -az /mnt/sys /mnt/backup

- Effacer les données du volume
  # shred /dev/sda6

Inist
Institut de l'Information Scientifique et Technique
Pôle système d'information

Chiffrement de la partition sda6

```
# cryptsetup --verbose --cipher "aes-cbc-essiv:sha256" --key-size 256 --verify-passphrase luksFormat /dev/sda6

# cryptsetup luksOpen /dev/sda6 sda6_crypt
```

Inist
Institut de l'Information Scientifique et Technique
Pôle système d'information

- Création des partitions LVM

```
# pvcreate /dev/mapper/sda6_crypt
# vgcreate sys /dev/mapper/sda6_crypt
# lvcreate -L2000 -nswap sys
# lvcreate -L10000 -nroot sys
# vgchange -a y sys
```

- Formatage des partitions
- Recopie des données

Inist
Institut de l'Information Scientifique et Technique
Pôle système d'information

Prise en compte du chiffrement

```
# mount -t proc none /mnt/crypt_sys/proc
# mount -t sysfs none /mnt/crypt_sys/sys
# mount --bind /dev /mnt/crypt_sys/dev
# chroot /mnt/crypt_sys

# vi /etc/crypttab
Ajouter : sda6_crypt /dev/sda6 none luks
```

Inist
Institut de l'Information Scientifique et Technique
Pôle système d'information

Éditer le fichier /etc/fstab

/dev/mapper/sys-root / ext3 erros=remount-ro 0 1
/dev/sda5 /boot ext3 defaults 0 2
/dev/mapper/sys-swap swap sw 0 0

Editer /etc/initramfs-tools/conf.d/resume et modifier la ligne "RESUME=..." par RESUME=/dev/mapper/sys-swap

Modifier le fichier /etc/mtab

Inist
Institut de l'Information Scientifique et Technique
Pôle système d'information

$ cat /proc/mounts> /etc/mtab

Effacer toutes les lignes jusqu'à /dev/mapper/sys-root pour obtenir quelque chose comme:

/dev/mapper/sys-root / ext3 rw,errors=remount-ro 0 0
tmpfs /lib/init/rw tmpfs rw,nosuid,mode=0755 0 0
proc /proc proc rw,noexec,nosuid,nodev 0 0
sysfs /sys sysfs rw,noexec,nosuid,nodev 0 0
udev /dev tmpfs rw,mode=0755 0 0
tmpfs /dev/shm tmpfs rw,nosuid,nodev 0 0
devpts /dev/pts devpts rw,noexec,nosuid,gid=5,mode=620 0 0

grub-mkconfig

Ajout de GRUB2 au MBR:
update-grub2 /dev/sda
update-initramfs -k all -u
Sortir du chroot et démonter toutes les partitions du disque local
Redémarrer.
Une phrase doit vous être demandée au démarrage de la machine juste après le choix du système à démarrer dans grub.

Inist
Institut de l'Information Scientifique et Technique
Pôle système d'information

Utilisation au quotidien

- Pas de perte de performance constatée
- Sauvegarde dans un conteneur chiffré avec bacula