Full Disk Encryption sous Arch Linux (systemd)

Introduction

Cette documentation permet d'installer Arch Linux avec du chiffrement intégrale du disque dur en mode EFI.

Une autre méthode est aussi décrite sur le wiki, mais elle est beaucoup moins bien sur bien des points.

AVANTAGE	**INCONVENIENT**
Chiffrement quasi intégrale	initramfs non chiffré!
Utilisation de l'EFI	En cas d'erreur a la première saisie, il faudra taper le mot de passe autant de fois qu'il y a de partitions
Une seule passphrase à taper au boot	
Rapide a démarrer	
possibilité d'utilisé une animation au démarrage (plymouth)	
L'“hibernation” du système est fonctionnelle et chiffrée	

Cette solution repose sur le fait que systemd peut garder en cache la passphrase que vous tapez pour l'utiliser sur les partitions suivante.

Voici l'agencement des partitions utilisé dans cette documentation. La seule réel contrainte sont les deux partitions **/boot** et **/boot/efi** :

```
+----------------------+-----------------------+-----------------------+----
------------------+
|ESP partition:        |Partition Boot:        |Partition Root:
|Partition SWAP         |
|                      |                       |                       |
|
|/boot/efi             |/boot                  |/
|[SWAP]                 |
|                      |                       |                       |
|
|                      |                       |/dev/mapper/cryptoroot
|/dev/store/cryptoswap  |
|                      |                       |UUID=<UUID-VOL-ROOT>
|UUID=<UUID-VOL-SWAP>   |
|                     +                       +-----------------------+----
------------------+
|/dev/sda1             |/dev/sda2              |/dev/sda3
|/dev/sda4              |
|UUID=<UUID-PART-ESP>  |UUID=<UUID-PART-BOOT>  |UUID=<UUID-PART-ROOT>
```

```
|UUID=<UUID-PART-SWAP>  |
|non-chiffré           |chiffré                |chiffré
|chiffré                |
+----------------------+-----------------------+-----------------------+----
------------------+
```

Installation

Boot en mode EFI

Il vous faut boot en mode EFI sur l'ISO de Archlinux, pour vérifier, le dossier **/sys/firmware/efi/efivars/** doit exister

Changer le Layout du clavier

Vu qu'en France nous avons un clavier AZERTY, il faut le changer pour se simplifier la vie :

```
# loadkeys fr
```

Se connecter à Internet

Là je vous renvoie vers la documentation officiel, ce sujet est bien trop exhaustif

Partitionnement des disques

Pour cela, je vous renvoie vers de la documentation de fdisk

Il faut ensuite mettre le système de fichier FAT32 sur la partition **/boot/efi**

```
# mkfs.fat -F32 /dev/sda1
```

et le système de fichier ext4 sur la partition **/boot**

```
# mkfs.ext4 /dev/sda2
```

Ensuite on chiffre nos partitions avec la même passphrase :

```
# cryptsetup luksFormat /dev/sda3
```

```
# cryptsetup luksFormat /dev/sda4
```

Maintenant on va les déchiffrés :

```
# cryptsetup open /dev/sda3 cryptroot
```

```
# cryptsetup open /dev/sda4 cryptswap
```

puis de les formater :

```
# mkfs.ext4 /dev/mapper/cryptroot
```

```
# mkswap /dev/mapper/cryptswap
```

puis on les montes :

```
# mount /dev/mapper/cryptroot /mnt/
```

```
# mkdir /mnt/boot
```

```
# mount /dev/sda2 /mnt/boot/
```

```
# mkdir /mnt/boot/efi
```

```
# mount /dev/sda1 /mnt/boot/efi
```

Installation de Arch Linux

On va commencer par choisir notre miroir pour les dépots Arch en modifiant le fichier **/etc/pacman.d/mirrorlist** en sélectionnant le pays de son choix

On va ensuite mettre a jour les clés des packet

```
# pacman -Sy archlinux-keyring
```

et enfin on installe Arch en lancant :

```
# pacstrap /mnt base base-devel
```

puis on se chroot pour faire la configuration:

```
# arch-chroot /mnt
```

Configuration de Arch

On commence par configurer le time zone :

```
# ln -sf /usr/share/zoneinfo/Europe/Paris /etc/localtime
```

```
# hwclock --systohc
```

Puis on génère le langage français :

```
# echo "fr_FR.UTF-8 UTF-8" > /etc/locale.gen && locale-gen && echo
"LANG=fr_FR.UTF-8" > /etc/locale.conf && echo "KEYMAP=fr" >
/etc/vconsole.conf
```

Puis on installe les paquets utiles :

```
# pacman -Syu efibootmgr grub mkinitcpio linux
```

Ensuite on configure le nom d'hôte dans le fichier **/etc/hostname** :

```
arch-0000
```

ainsi que le fichier **/etc/hosts** :

```
127.0.0.1   localhost.localdomain    localhost
::1     localhost.localdomain    localhost
127.0.1.1   arch-0000.localdomain    arch-0000
```

Configuration du boot

On modifie le fichier **/etc/default/grub**, il faut modifié cet ligne comme tel:

```
GRUB_CMDLINE_LINUX_DEFAULT="quiet splash luks.name=<UUID-ROOT>=cryptroot
luks.name=<UUID-SWAP>=cryptswap luks.option=<UUID-SWAP>=swap
root=UUID=<UUID-VOL-CRYPTROOT> resume=UUID=<UUID-VOL-CRYPTSWAP>"
```

ainsi que la ligne suivante:

et pour finir décommente la ligne :

```
GRUB_ENABLE_CRYPTODISK=y
```

Ensuite on génère la config grub :

```
# grub-mkconfig -o /boot/grub/grub.cfg
```

```
# grub-install --target=x86_64-efi --efi-directory=/boot/efi --bootloader-
id=LINUX --recheck
```

Maintenant on va générer l'image **initramfs** pour le déchiffrement, pour cela il faut aller modifier le fichier **/etc/mkinitcpio.conf** en modifiant le champ **HOOKS** de cet manière : [1)]

```
HOOKS=(base systemd autodetect modconf keyboard sd-vconsole block sd-encrypt
filesystems fsck)
```

puis on génère l'image :

```
# mkinitcpio -p linux
```

Et pour finir le fichier **/etc/fstab** :

```
UUID=<UUID-ESP>          /boot/efi          vfat        defaults          0 1
UUID=<UUID-BOOT>         /boot              ext4        defaults          0 1
UUID=<UUID-VOL-ROOT>          /                   ext4        defaults
0 1
UUID=<UUID-VOL-SWAP>          none                swap        defaults
0 0
```

1)

Si vous utilisez plymouth, il faut ajouter **sd-plymouth** après **systemd**