Chiffrement Luks

Chiffrer une partition

```
#sudo cryptsetup -y -v luksFormat /dev/sdc1
ATTENTION: Le périphérique /dev/sdc1 contient déjà une signature pour un superblock « crypto_LUKS ».

WARNING!
========
Cette action écrasera définitivement les données sur /dev/sdc1.

Are you sure? (Type uppercase yes): YES
Saisissez la phrase secrète pour /dev/sdc1 :
Vérifiez la phrase secrète :
```

Formater la partition

```
#sudo mkfs.ntfs -f /dev/mapper/Samsung
Cluster size has been automatically set to 4096 bytes.
Creating NTFS volume structures.
mkntfs completed successfully. Have a nice day.
```

Lister les blocs et identifier les blocs luks

```
#lsblk --fs

NAME                                  FSTYPE      LABEL UUID                                   FSAVAIL FSUSE% MOUNTPOINT
sda
├─sda1                                vfat            6FE5-9D8C                              163,2M    18% /boot/efi
├─sda2                                ext4            f56409e9-43af-41d4-bf9e-1b3ce3cb11e0    713,9M    20% /boot
└─sda3                                crypto_LUKS     6eb090b6-7304-4843-b357-857c5d92962e
  └─luks-6eb090b6-7304-4843-b357-857c5d92962e LVM2_member      pMkBCr-iN2G-XsPH-4ECF-0zhc-M8uA-wrdQ
    ├─fedora-root                     ext4            d53e789d-3b19-4314-8fd8-6536e094740d       25G    44% /
    ├─fedora-swap                     swap            d4261e47-edb0-4abc-9131-cf8dbc751c7e                  [SWAP]
    └─fedora-home                     ext4            5acd1096-bbde-404f-9122-bec03451397d    146,4G    59% /hom
sdc
└─sdc1                                crypto_LUKS     bd80f01b-bfd0-4bc6-a2bb-bc0a25935ccb
```

Saisir la clef de déchiffrement du disque

```
#sudo cryptsetup luksOpen /dev/sdc1 Samsung
Saisissez la phrase secrète pour /dev/sdc1 :
```

Oublier la clef de chiffrement du disque

```
#sudo cryptsetup luksClose Samsung
```

Dump de l'entête

```
sudo cryptsetup luksDump /dev/sdc1                  SIGINT(2) ↵  10396  15:57:10
LUKS header information
Version:        2
Epoch:          3
Metadata area: 16384 [bytes]
Keyslots area: 16744448 [bytes]
UUID:           f2c5df1a-a6cb-46d9-a5b9-50c233089cc2
Label:          (no label)
Subsystem:      (no subsystem)
Flags:          (no flags)

Data segments:
  0: crypt
        offset: 16777216 [bytes]
        length: (whole device)
        cipher: aes-xts-plain64
        sector: 512 [bytes]

Keyslots:
  0: luks2
        Key:        512 bits
        Priority:   normal
        Cipher:     aes-xts-plain64
        Cipher key: 512 bits
        PBKDF:      argon2i
        Time cost:  6
        Memory:     1048576
        Threads:    4
        Salt:       6c 79 ac 83 62 0b b4 27 8a 51 6f 07 c7 51 ae 48
                    d2 8b 70 88 c0 2a f2 a8 81 2b 9f 5f 05 21 ee 00
        AF stripes: 4000
        AF hash:    sha256
        Area offset:32768 [bytes]
        Area length:258048 [bytes]
        Digest ID:  0
Tokens:
Digests:
  0: pbkdf2
        Hash:       sha256
```

	Iterations: 115380
	Salt: d5 23 f6 2a 06 ea 92 19 45 12 2a 54 d7 a5 2c ee
	 ae 64 f9 2c 85 34 d5 2f a1 3e 71 21 c1 1c e2 07
	Digest: c1 7b 22 74 2e c7 54 6f 73 39 77 2a 1e 5f 67 65
	 54 80 07 43 d3 3d a0 08 d4 f0 b8 6f 76 be 44 70

Ajouter une clef

On ajoute une clef supplémentaire en slot 2 sur la base d'un mot de passe

```
sudo cryptsetup luksAddKey --key-slot 1 /dev/sdc1
Entrez une phrase secrète existante :
Entrez une nouvelle phrase secrète pour l'emplacement de clé :
Vérifiez la phrase secrète :
```

Ou sur la base d'un fichier qui fait office de clef (cette méthode est préférable afin de rendre la chose plus robuste et automatisé pour le montage) :

```
dd if=/dev/urandom of=/home/dugravot6/Securite/Samsung_disk_secret_key bs=512 count=8
sudo cryptsetup -v luksAddKey /dev/sdc1 /home/dugravot6/Securite/Samsung_disk_secret_key
```

Le dump présentera le slot2 occupé :

```
LUKS header information
Version:       	2
Epoch:         	4
Metadata area: 	16384 [bytes]
Keyslots area: 	16744448 [bytes]
UUID:          	f2c5df1a-a6cb-46d9-a5b9-50c233089cc2
Label:         	(no label)
Subsystem:     	(no subsystem)
Flags:       	(no flags)

Data segments:
  0: crypt
	offset: 16777216 [bytes]
	length: (whole device)
	cipher: aes-xts-plain64
	sector: 512 [bytes]

Keyslots:
  0: luks2
	Key:        512 bits
	Priority:   normal
	Cipher:     aes-xts-plain64
	Cipher key: 512 bits
	PBKDF:      argon2i
	Time cost:  6
	Memory:     1048576
```

```
	Threads:    4
	Salt:       6c 79 ac 83 62 0b b4 27 8a 51 6f 07 c7 51 ae 48
	            d2 8b 70 88 c0 2a f2 a8 81 2b 9f 5f 05 21 ee 00
	AF stripes: 4000
	AF hash:    sha256
	Area offset:32768 [bytes]
	Area length:258048 [bytes]
	Digest ID:  0
  1: luks2
	Key:        512 bits
	Priority:   normal
	Cipher:     aes-xts-plain64
	Cipher key: 512 bits
	PBKDF:      argon2i
	Time cost:  4
	Memory:     1020932
	Threads:    4
	Salt:       6d 0f 29 10 c8 5b 9a e3 58 30 f4 3e 8e 8f 2d 60
	            0b f8 17 5f 18 fa dd 42 9c fe 38 d7 07 7d 2c d4
	AF stripes: 4000
	AF hash:    sha256
	Area offset:290816 [bytes]
	Area length:258048 [bytes]
	Digest ID:  0
Tokens:
Digests:
  0: pbkdf2
	Hash:       sha256
	Iterations: 115380
	Salt:       d5 23 f6 2a 06 ea 92 19 45 12 2a 54 d7 a5 2c ee
	            ae 64 f9 2c 85 34 d5 2f a1 3e 71 21 c1 1c e2 07
	Digest:     c1 7b 22 74 2e c7 54 6f 73 39 77 2a 1e 5f 67 65
	            54 80 07 43 d3 3d a0 08 d4 f0 b8 6f 76 be 44 70
```

Supprimer une clef

On précise le slot a supprimer :

```
sudo cryptsetup luksKillSlot /dev/sdc1 1
Entrez toute phrase secrète restante :
```

Monter automatiquement la partition

Le fichier `/etc/crypttab` permet de définir les entrées et les options de montage :

```
Samsung UUID=5ab227f5-f69e-4a2f-b85a-32b7637d42be /home/dugravot6/Securite/Samsung_disk_secret_key luk
```

Le format est le suivant :

```
<target name> <source device> <key file> <options>
```

Ici, l'UUID correspondant sera monté grace à la clef (/home/dugravot6/Securite/Samsung_disk_secret_key) que l'on a associée précédemment en slot 2.

Revision #6
Created 10 February 2023 17:04:45 by Stephane DUGRAVOT
Updated 10 February 2023 17:43:15 by Stephane DUGRAVOT