

1. Сгенерировать ключ-файл с помощью команды dd

dd if=/dev/urandom of=/home/vagrant/my.key bs=1 count=1024

```
[vagrant@localhost ~]$ dd if=/dev/urandom of=/home/vagrant/my.key bs=1 count=1024
1024+0 records in
1024+0 records out
1024 bytes (1.0 kB) copied, 0.00254757 s, 402 kB/s
```

2. Создать на основе созданного ключа криптоконтейнер

sudo cryptsetup -v -s 512 luksFormat /dev/sdb1 /home/vagrant/my.key

```
[vagrant@localhost ~]$ sudo cryptsetup -v -s 512 luksFormat /dev/sdb1 /home/vagrant/my.key

WARNING!
=====
This will overwrite data on /dev/sdb1 irrevocably.

Are you sure? (Type uppercase yes): YES
Command successful.
```

3. Открыть контейнер с помощью ключа

sudo cryptsetup luksOpen -d /home/vagrant/my.key /dev/sdb1 secrets

sudo mkfs.xfs /dev/mapper/secrets

sudo mkdir /secrets

sudo mount /dev/mapper/secrets /secrets

```
[vagrant@localhost ~]$ sudo cryptsetup luksOpen -d /home/vagrant/my.key /dev/sdb1 secrets
[vagrant@localhost ~]$ sudo mkfs.xfs /dev/mapper/secrets
meta-data=/dev/mapper/secrets      isize=512    agcount=4, agsize=655168 blks
=                               sectsz=512   attr=2, projid32bit=1
=                               crc=1        finobt=0, sparse=0
data     =                       bsize=4096   blocks=2620672, imaxpct=25
=                               sunit=0       swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=1
log      =internal log          bsize=4096   blocks=2560, version=2
=                               sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                  extsz=4096   blocks=0, rtextents=0
```

```
[vagrant@localhost ~]$ sudo mkdir /secrets
[vagrant@localhost ~]$ sudo mount /dev/mapper/secrets /secrets
```

4. Заполнить контейнер произвольными данными

```
[vagrant@localhost ~]$ cd /secrets/
[vagrant@localhost secrets]$ sudo touch xfiles.txt
[vagrant@localhost secrets]$ sudo chown vagrant:vagrant xfiles.txt
[vagrant@localhost secrets]$ echo "\"The Truth Is Out There\" - Agent FBI Fox William Mulder" > xfiles.txt
[vagrant@localhost secrets]$ cat xfiles.txt
"The Truth Is Out There" - Agent FBI Fox William Mulder
[vagrant@localhost secrets]$
```

5. Закрыть контейнер

`sudo umount /secrets`

`sudo cryptsetup luksClose secrets`

```
[vagrant@localhost ~]$ cd ~  
[vagrant@localhost ~]$ sudo umount /secrets/  
[vagrant@localhost ~]$ sudo cryptsetup luksClose secrets
```

6. Открыть контейнер (неожиданно :))

`sudo cryptsetup luksOpen -d /home/vagrant/my.key /dev/sdb1 secrets`

`sudo mount /dev/mapper/secrets /secrets`

```
[vagrant@localhost ~]$ sudo cryptsetup luksOpen -d /home/vagrant/my.key /dev/sdb1 secrets  
[vagrant@localhost ~]$ sudo mount /dev/mapper/secrets /secrets
```

7. Проверить, что все на месте

```
[vagrant@localhost ~]$ cat /secrets/xfiles.txt  
"The Truth Is Out There" - Agent FBI Fox William Mulder
```

8. Создать дополнительный ключ (либо ключевой файл)

8.1. для начала посмотрим занятость слотов

`sudo cryptsetup luksDump /dev/sdb1 | grep Slot`

```
[vagrant@localhost ~]$ sudo cryptsetup luksDump /dev/sdb1 | grep Slot  
Key Slot 0: ENABLED  
Key Slot 1: DISABLED  
Key Slot 2: DISABLED  
Key Slot 3: DISABLED  
Key Slot 4: DISABLED  
Key Slot 5: DISABLED  
Key Slot 6: DISABLED  
Key Slot 7: DISABLED
```

8.2. Создаем доп.ключ файл

`dd if=/dev/urandom of=/home/vagrant/x-files.key bs=1 count=1024`

```
[vagrant@localhost ~]$ dd if=/dev/urandom of=/home/vagrant/x-files.key bs=1 count=1024  
1024+0 records in  
1024+0 records out  
1024 bytes (1.0 kB) copied, 0.00178441 s, 574 kB/s  
[vagrant@localhost ~]$ ls  
my.key  x-files.key
```

8.3. добавляем доп.ключ убеждаемся что ключ добавился

`sudo cryptsetup luksAddKey /dev/sdb1 /home/vagrant/x-files.key`

`--key-file=/home/vagrant/my.key`

`sudo cryptsetup luksDump /dev/sdb1 | grep Slot`

```
[vagrant@localhost ~]$ sudo cryptsetup luksAddKey /dev/sdb1 /home/vagrant/x-files.key --key-file=/home/vagrant/my.key
[vagrant@localhost ~]$
[vagrant@localhost ~]$
[vagrant@localhost ~]$
[vagrant@localhost ~]$
[vagrant@localhost ~]$ sudo cryptsetup luksDump /dev/sdb1 | grep Slot    t/x-files.key --key
Key Slot 0: ENABLED
Key Slot 1: ENABLED
Key Slot 2: DISABLED
Key Slot 3: DISABLED
Key Slot 4: DISABLED
Key Slot 5: DISABLED
Key Slot 6: DISABLED
Key Slot 7: DISABLED
```

з.ы. на скриншоте shell немного глюкнуло поэтому появился артефакт `t/x-files.key --key`

9. Удалить старый ключ

Здесь можно пойти 2мя способами

1 способ: просто удалить ключ из каталога командой `rm my.key`

```
[vagrant@localhost ~]$ ls
my.key  x-files.key
```

```
[vagrant@localhost ~]$ rm my.key
```

```
[vagrant@localhost ~]$ ls
x-files.key
```

И тогда нам придется выполнять пункт 10 поскольку если мы выполним команду

`sudo cryptsetup luksDump /dev/sdb1 | grep Slot`

```
[vagrant@localhost ~]$ sudo cryptsetup luksDump /dev/sdb1 | grep Slot
Key Slot 0: ENABLED
Key Slot 1: ENABLED
Key Slot 2: DISABLED
Key Slot 3: DISABLED
Key Slot 4: DISABLED
Key Slot 5: DISABLED
Key Slot 6: DISABLED
Key Slot 7: DISABLED
```

увидим что слот до сих пор занят.

2 способ в начале удаляем ключ из слота

`sudo cryptsetup luksRemoveKey -d /home/vagrant/my.key /dev/sdb1`

а затем безопасно удаляем сам ключ способом 1.

```
[vagrant@localhost ~]$ sudo cryptsetup luksRemoveKey -d /home/vagrant/my.key /dev/sdb1
[vagrant@localhost ~]$ ls
my.key  x-files.key
[vagrant@localhost ~]$ sudo cryptsetup luksDump /dev/sdb1 | grep Slot
Key Slot 0: DISABLED
Key Slot 1: ENABLED
Key Slot 2: DISABLED
Key Slot 3: DISABLED
Key Slot 4: DISABLED
Key Slot 5: DISABLED
Key Slot 6: DISABLED
Key Slot 7: DISABLED
```

10. очистить слот от старого ключа

Но в пункте 9 мы пошли по первому сценарию и теперь при попытке очистить слот командой

```
sudo cryptsetup luksRemoveKey -d /home/vagrant/my.key /dev/sdb1
```

мы получаем вот такую неприятную запись

```
[vagrant@localhost ~]$ sudo cryptsetup luksRemoveKey -d /home/vagrant/my.key /dev/sdb1
Failed to open key file.
```

но мы не унываем и выполняем команду

```
sudo cryptsetup luksKillSlot /dev/sdb1 0
```

```
--key-file=/home/vagrant/x-files.key
```

```
[vagrant@localhost ~]$ sudo cryptsetup luksKillSlot /dev/sdb1 0 --key-file=/home/vagrant/x-files.key
[vagrant@localhost ~]$ sudo cryptsetup luksDump /dev/sdb1 | grep Slot
Key Slot 0: DISABLED
Key Slot 1: ENABLED
Key Slot 2: DISABLED
Key Slot 3: DISABLED
Key Slot 4: DISABLED
Key Slot 5: DISABLED
Key Slot 6: DISABLED
Key Slot 7: DISABLED
```

11. проделать пункты 6-7 с новым ключом

```
sudo cryptsetup luksOpen -d /home/vagrant/x-files.key /dev/sdb1 secrets
```

```
sudo mount /dev/mapper/secrets /secrets
```

```
cat /secrets/xfiles.txt
```

```
[vagrant@localhost ~]$ sudo cryptsetup luksOpen -d /home/vagrant/x-files.key /dev/sdb1 secrets
[vagrant@localhost ~]$ sudo mount /dev/mapper/secrets /secrets
[vagrant@localhost ~]$ cat /secrets/xfiles.txt
"The Truth Is Out There" - Agent FBI Fox William Mulder
[vagrant@localhost ~]$
```

12. отмонтировать контейнер

```
sudo umount /secrets
```

```
sudo cryptsetup luksClose secrets
```

```
[vagrant@localhost ~]$ cd ~  
[vagrant@localhost ~]$ sudo umount /secrets/  
[vagrant@localhost ~]$ sudo cryptsetup luksClose secrets
```