

Восстановление неработоспособной системы (через окружение chroot)

В процессе установки или последующей работы иногда случаются поломки системы, чаще по нашей собственной вине и невнимательности, а также нарушении правил пользования системой. Как следствие система стопорится на этапе загрузки и дальнейшая загрузка не происходит, часто причиной является установка кривых видео-драйверов, обновление системы без загрузочной USB-флешки, неумелое обращение с параметрами загрузки Grub и системного ядра, а также всевозможными фоновыми службами. Начинающие же пользователи продвинутой схемы часто путают в процессе первых установок идентификаторы разделов, в связи с чем загрузка прерывается на самом начальном этапе. Всё это мелочи и опытные пользователи, прошедшие давно первую главу не дадут мне соврать, при умелом обращении и умении читать ошибки, система восстанавливается минут за 5-10. Для решения всех проблем существует режим chroot, если говорить простыми словами, chroot - это монтирование корневого каталога операционной системы Linux в среде live-версии операционной системы, применяется для правки и исправления системных конфигураций.

Привожу ссылку, которая понятным языком описывает что, зачем и почему:

[**https://wiki.archlinux.org/title/Chroot_\(%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9\)**](https://wiki.archlinux.org/title/Chroot_(%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9))

Когда система не имеет шифрования корневого системного каталога вход в chroot является элементарной задачей, но у нас продвинутая схема, а значит есть определённые тонкости в которых начинающий пользователь может запутаться, чтобы избавить юного компьютерного техника от будущих проблем и было создано данное краткое руководство. Как говорится мухомор за щеку и в путь, товарищи.

Краткая последовательность действий:

- ✓ **Загрузка Live-образа** операционной системы Manjaro
- ✓ **Подключение к компьютеру** (открытие) и монтирование зашифрованной флешки **sdb**
- ✓ **Открытие зашифрованного жёсткого диска sda** с помощью ключевого файла и заголовка, которые мы взяли с расшифрованной флешки на предыдущем шаге.
- ✓ **Монтирование (подключение) разделов LVM (store-root и store-home) и boot-флешки (/dev/mapper/cryptboot)** в директорию **/mnt**.
- ✓ **Вход в chroot** окружение.

Шаг 1

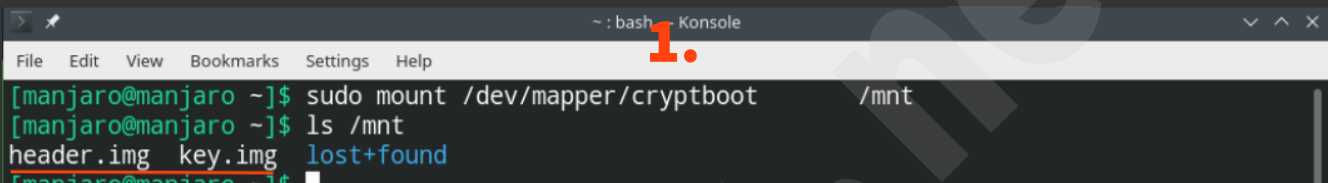
(Загрузка live-образа и открытие зашифрованной флешки)

- ✓ Мы запустили компьютер с live-флешки manjaro
- ✓ Подключили загрузочную шифро-флешку к компьютеру

lsblk проверяем подключённые устройства к компьютеру.

sudo cryptsetup open /dev/sdX1 cryptboot открываем зашифрованный раздел на шифро-флешке и присваиваем ему имя **cryptboot**. Где вместо **X**, буква которой определяется зашифрованная флешка в предыдущем выводе команды **lsblk**.

sudo mount /dev/mapper/cryptboot /mnt монтируем ранее открытый раздел в папку **/mnt**



```
~ : bash - Konsole
File Edit View Bookmarks Settings Help
[manjaro@manjaro ~]$ sudo mount /dev/mapper/cryptboot /mnt
[manjaro@manjaro ~]$ ls /mnt
header.img key.img lost+found
```

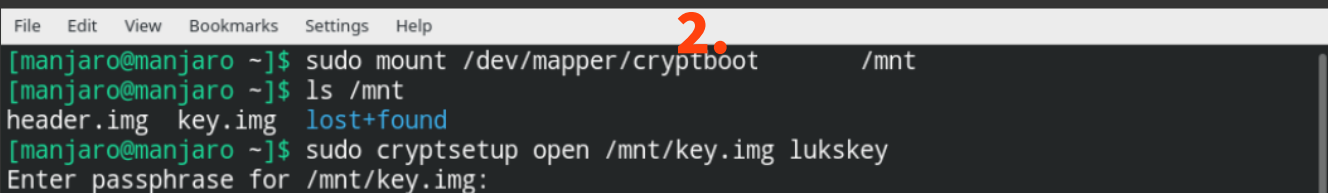
Теперь на смонтированном устройстве у нас стали доступны ключевые файлы и мы можем с помощью их открыть диск **sda**. Обратите внимание, на изображении выше мы на смонтированном разделе видим всего два файла **header** и **key**, однако нет ни ядра, ни раздела загрузчика, хотя должны присутствовать. Всё так, просто я сейчас данный материал компилирую с главы "Резервная копия флешки" и как следствие данных разделов и файлов просто не было на том отрезке времени.

Шаг 2

(разблокируем файл-ключ от /dev/sda и отрываем hdd)

- ✓ Мы расшифровали загрузочный usb-накопитель на котором ядро, загрузчик, заголовок и файл ключ от hdd.
- ✓ Мы смонтировали наш usb-накопитель в **/mnt** для последующего взаимодействия с файлами расположенными на нём.

sudo cryptsetup open /mnt/key.img lukskey открываем файл-ключ от жёсткого диска **/dev/sda** и присваиваем имя **lukskey**



```
File Edit View Bookmarks Settings Help
[manjaro@manjaro ~]$ sudo mount /dev/mapper/cryptboot /mnt
[manjaro@manjaro ~]$ ls /mnt
header.img key.img lost+found
[manjaro@manjaro ~]$ sudo cryptsetup open /mnt/key.img lukskey
Enter passphrase for /mnt/key.img:
```

На изображении ниже можем наблюдать как в выводе команды **lsblk** у нас появился открытый ключ **key.img**, имеющий название **lukskey** и который впоследствии будет использоваться для открытия **sda**.

```
[manjaro@manjaro ~]$ lsblk
```

NAME	MAJ:MIN	RM	SIZE	RO	TYPE	MOUNTPOINT
loop0	7:0	0	20.8M	1	loop	/run/miso/sfs/livefs
loop1	7:1	0	570.1M	1	loop	/run/miso/sfs/mhwdfs
loop2	7:2	0	1.6G	1	loop	/run/miso/sfs/desktopfs
loop3	7:3	0	630.2M	1	loop	/run/miso/sfs/rootfs
loop4	7:4	0	32M	0	loop	
└─lukskey	254:1	0	16M	0	crypt	
sda	8:0	0	50.3G	0	disk	
sdb	8:16	0	8G	0	disk	
└─sdb1	8:17	0	8G	0	part	
sdc	8:32	0	8G	0	disk	
└─sdc1	8:33	0	8G	0	part	
└─cryptboot	254:0	0	8G	0	crypt	/mnt

```
# sudo cryptsetup open --header=/mnt/header.img --key-file=/dev/mapper/lukskey --keyfile-offset=9437 --keyfile-size=8192 /dev/sda cryptroot
```

открываем зашифрованный жёсткий диск `/dev/sda`. Мы видим как после открытия `cryptroot` у нас также открылись внутренние разделы `Lvm store-root` и `store-home`.

```
[manjaro@manjaro ~]$ sudo cryptsetup open --header=/mnt/header.img --key-file=/dev/mapper/lukskey --keyfile-offset=9437 --keyfile-size=8192 /dev/sda cryptroot
```

```
[manjaro@manjaro ~]$ lsblk
```

NAME	MAJ:MIN	RM	SIZE	RO	TYPE	MOUNTPOINT
loop0	7:0	0	20.8M	1	loop	/run/miso/sfs/livefs
loop1	7:1	0	570.1M	1	loop	/run/miso/sfs/mhwdfs
loop2	7:2	0	1.6G	1	loop	/run/miso/sfs/desktopfs
loop3	7:3	0	630.2M	1	loop	/run/miso/sfs/rootfs
loop4	7:4	0	32M	0	loop	
└─lukskey	254:1	0	16M	0	crypt	
sda	8:0	0	50.3G	0	disk	
└─cryptroot	254:2	0	50.3G	0	crypt	
└─└─store-root	254:3	0	15G	0	lvm	
└─└─store-home	254:4	0	35.3G	0	lvm	
sdb	8:16	0	8G	0	disk	
└─sdb1	8:17	0	8G	0	part	
sdc	8:32	0	8G	0	disk	
└─sdc1	8:33	0	8G	0	part	
└─cryptbootbackup	254:0	0	8G	0	crypt	/mnt
sr0	11:0	1	2.9G	0	rom	/run/miso/bootmnt

```
# sudo cryptsetup close lukskey
```

 закрываем `lukskey`

```
# sudo umount /mnt
```

 размонтируем подключенные устройства из папки `/mnt`

```
[manjaro@manjaro ~]$ sudo cryptsetup close lukskey
```

```
[manjaro@manjaro ~]$ sudo umount /mnt
```

```
[manjaro@manjaro ~]$
```

Шаг 3

(монтируем 'подключаем' LVM, флешку как boot и входим в окружение chroot)

- ✓ Мы открыли диск `sda` и подготовили всё для завершающего действия.
- ✓ Мы размонтировали всё из директории `/mnt`

sudo mount /dev/store/root /mnt монтируем корневой каталог в папку **/mnt**

sudo mount /dev/store/home /mnt/home монтируем домашний каталог в папку **/mnt/home**

sudo mount /dev/mapper/cryptboot /mnt/boot монтируем нашу шифро-флешку **cryptboot** в загрузочную папку **/mnt/boot**

```
6.
[manjaro@manjaro ~]$ lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
loop0        7:0    0  20.8M 1 loop /run/miso/sfs/livefs
loop1        7:1    0 570.1M 1 loop /run/miso/sfs/mhwdfs
loop2        7:2    0   1.6G 1 loop /run/miso/sfs/desktopfs
loop3        7:3    0 630.2M 1 loop /run/miso/sfs/rootfs
sda          8:0    0  50.3G 0 disk
├─cryptroot 254:2    0  50.3G 0 crypt
├─store-root 254:3    0   15G 0 lvm
└─store-home 254:4    0  35.3G 0 lvm
sdb          8:16    0    8G 0 disk
├─sdb1       8:17    0    8G 0 part
├─sdc        8:32    0    8G 0 disk
├─sdc1       8:33    0    8G 0 part
└─cryptbootbackup 254:0    0    8G 0 crypt
sr0         11:0    1   2.9G 0 rom  /run/miso/bootmnt
[manjaro@manjaro ~]$ sudo mount /dev/store/root /mnt
[manjaro@manjaro ~]$ sudo mount /dev/store/home /mnt/home/
[manjaro@manjaro ~]$ sudo mount /dev/mapper/cryptbootbackup /mnt/boot/
[manjaro@manjaro ~]$
```

Обратите внимание, при успешном монтировании в директории **/mnt** появились наши системные файлы и раздел **/boot**

```
7.
[manjaro@manjaro ~]$ ls /mnt
bin boot dev etc home hostlvm lib lib64 lost+found mnt opt proc root run sbin snap srv sys tmp usr var
[manjaro@manjaro ~]$ ls /mnt/boot/
header.img key.img lost+found
[manjaro@manjaro ~]$
```

Не забываем проверить правильность монтирования разделов!!!

```
8.
[manjaro@manjaro ~]$ lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
loop0        7:0    0  20.8M 1 loop /run/miso/sfs/livefs
loop1        7:1    0 570.1M 1 loop /run/miso/sfs/mhwdfs
loop2        7:2    0   1.6G 1 loop /run/miso/sfs/desktopfs
loop3        7:3    0 630.2M 1 loop /run/miso/sfs/rootfs
sda          8:0    0  50.3G 0 disk
├─cryptroot 254:2    0  50.3G 0 crypt
├─store-root 254:3    0   15G 0 lvm → /mnt
└─store-home 254:4    0  35.3G 0 lvm → /mnt/home
sdb          8:16    0    8G 0 disk
├─sdb1       8:17    0    8G 0 part
├─sdc        8:32    0    8G 0 disk
├─sdc1       8:33    0    8G 0 part
└─cryptbootbackup 254:0    0    8G 0 crypt → /mnt/boot
sr0         11:0    1   2.9G 0 rom  /run/miso/bootmnt
[manjaro@manjaro ~]$
```

manjaro-chroot /mnt входим в окружение **chroot** для завершения настроек

Вот и всё, после этого решаем задачи для восстановления системы и перезагружаемся в уже работающую систему.