LUKS

Basisinfo: https://de.opensuse.org/SDB:Sicherheit_Verschl%C3%BCsselung_mit_LUKS

https://wiki.ubuntuusers.de/LUKS/

Vor LEAP: Image *.img reparieren

Die *.key Datei ist auch verschlüsselt, daher geht es nicht direkt siehe dazu https://forums.opensuse.org/showthread.php/501003-How-to-check-encrypted-home-directory-by-fsck

```
openssl aes-256-cbc -d -in /home/image.key | cryptsetup luksOpen
/home/image.img my_home
```

Danach fsck auf /dev/mapper/my_home

Mit luksclose wird das Image geschlossen

```
cryptsetup luksClose my_home
```

Ab Leap werden normale LUKS Partitionen benutzt.

LUKS Partitionen (ab OpenSUSE Leap)

Die Partition wird über ein Loop Setup ins Dateisystem gemountet:

```
dev/sda1              932G  352G  578G  38% /srv/vm
/dev/mapper/cr-auto-1  120G   89G   32G  74% /home
tmpfs                  3.2G     0  3.2G   0% /run/user/497
```

Die Zuordnung der gemappten Partition zur Partition auf der Platte steht in in /etc/crypttab

```
less /etc/crypttab

cr_swap UUID=8e3cdf66-aea2-4a93-a5f3-bb8bd8d1d77f
cr_home UUID=a8332074-8ff7-474b-9b07-ae15cfc71ca0
cr_root UUID=eb9ebba2-262a-4ab8-aa31-2b024d825679 none x-initrd.attach
```

Die Befehle für cryptsetup funktionieren nur an der Originalpartition, auch über /dev/disk/by-uuid/

```
less /etc/crypttab

cr_swap  UUID=8e3cdf66-aea2-4a93-a5f3-bb8bd8d1d77f
cr_home  UUID=a8332074-8ff7-474b-9b07-ae15cfc71ca0
cr_root  UUID=eb9ebba2-262a-4ab8-aa31-2b024d825679  none  x-initrd.attach
```

```
odysseus3:~ # cryptsetup luksDump /dev/nvme0n1p3
```

```
LUKS header information for /dev/nvme0n1p3

Version:        1
Cipher name:    aes
Cipher mode:    xts-plain64
Hash spec:      sha256
Payload offset: 4096
MK bits:        256
MK digest:      1f 06 0e 96 37 13 1c 25 d8 03 cd 64 df 2a 67 94 26 a5 6b 69
MK salt:        e2 b4 a9 e0 c3 89 84 e6 cc 6f cb d0 fc da 3a 92
                ce 52 95 ce c4 ca fa 65 7b bf 06 a8 ea 8a 03 3e
MK iterations:  173146
UUID:           7b1703a0-0ff9-4836-b67a-9e9e951b5182

Key Slot 0: ENABLED
        Iterations:             2770346
        Salt:                   f1 de c8 30 e1 80 5e eb 66 93 0d 03 b6 9a ee
90
                                75 5b a5 29 1c 50 17 79 18 b9 4d 5f c2 82 61
38
        Key material offset:    8
        AF stripes:             4000
Key Slot 1: ENABLED
        Iterations:             3912596
        Salt:                   89 fc dd 4c 1c f9 6f ff b2 4e 2e 40 03 a7 a4
5f
                                de 7a 7a 08 3e 72 16 58 b2 5f 24 c8 b6 87 86
c0
        Key material offset:    264
        AF stripes:             4000
Key Slot 2: DISABLED
Key Slot 3: DISABLED
Key Slot 4: DISABLED
Key Slot 5: DISABLED
Key Slot 6: DISABLED
Key Slot 7: DISABLED
```

Passphrase hinzufügen:

```
cryptsetup luksAddKey /dev/nvme0n1p3 --key-slot 0
```

Passphrase in Slot gezielt ändern:

```
cryptsetup luksChangeKey /dev/nvme0n1p3 --key-slot 3
```

Passphrase entfernen

```
cryptsetup luksKillSlot /dev/nvme0n1p3 --key-slot 3
```

Passphrase testen

```
cryptsetup luksOpen --test-passphrase
```