Table of Contents

Setting up an encrypted hard drive with LUKS and BTRFS

Simple mode, adding to this site to serve as reference for friends.

This guide assumes `sda` as the drive letter, and `sda1` as your partition

Format the disk

```
sudo cfdisk /dev/sda
```

- choose GPT if you have a MBR vs GPT option
- pick create, choose max size (or whatever you want)
- then write to disk

That should create /dev/sda1 as a partition.

Setup encryption

```
sudo cryptsetup luksFormat --type luks2 --cipher aes-xts-plain64 --key-size
512 --hash sha512 --iter-time 5000 --sector-size 4096 /dev/sda1
```

pick your password

the luks is like a shell/container/box around your actual filesystem.
big abstraction layer like HTTPS.

then unlock so we can create a partition in it.

```
sudo cryptsetup luksOpen /dev/sda1 foobar-hdd
```

Note ^ above is not name of disk, just what the decrypted drive name is

Make a filesystem

Then, make a filesystem. I like btrfs, but ext4 and XFS are also good options

```
sudo mkfs.btrfs -L yolohdd -f /dev/mapper/foobar-hdd
```

then you can mount it

sudo mount /dev/mapper/foobar-hdd /mnt/your-mountpoint

Then make a subvolume if you want

sudo btrfs subvolume create /mnt/your-mountpoint/@your-subvolume

Automount on boot

Get UUIDs

With this, do an lsblk -f and take note of the UUIDs. You will need it (or you can use labels, but UUID is better since you can have duplicate labels)

to automount at boot, here is my UUIDs as an example

```
NAME                  FSTYPE      FSVER    LABEL          UUID
FSAVAIL FSUSE% MOUNTPOINTS
sda
`-sda1                crypto_LUKS 2                       208fae7b-ed03-48cd-
a4f6-f37f9dd28732
  `-hdd               btrfs                HDD            fbd95406-4a52-4fe2-
b1a7-17743a037149    991.4G    45% /hdd
```

Update crypttab to decrypt

in /etc/crypttab, add this disk. this does decryption

```
hdd             UUID=208fae7b-ed03-48cd-a4f6-f37f9dd28732    none
```

First is the name when decrypted. The UUID is the UUID of the encrypted shell, that is the one in sda1

This will decrypt it, then we can mount the filesystem in the encrypted container

Add to fstab to mount

now add it to /etc/fstab to handle auto mounting

```
# /dev/sda1 LABEL=hdd
UUID=fbd95406-4a52-4fe2-b1a7-17743a037149       /hdd            btrfs
rw,relatime,nofail,space_cache=v2,compress=zstd
```

The UUID in here is the one of the filesystem, not the LUKS, so notice how it's under the hdd name in my lsblk.

You can also just use /dev/mapper/hdd or your decrypted name, but UUID is more predictable.

nofail will make it so if it fails to mount, your computer can still turn on (highly recommend)