Encrypt Partitions with LUKS/dm-crypt

Prerequisites

Install cryptsetup with the following command:

```
sudo apt update
sudo apt upgrade
sudo apt install cryptsetup
```

Find the Block Device Name of Your Partition. Enter the following command:

```
lsblk

NAME   MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
sda      8:0    0 232,9G  0 disk
├─sda1   8:1    0   100M  0 part
├─sda2   8:2    0  69,9G  0 part
├─sda3   8:3    0 153,7G  0 part /
└─sda4   8:4    0   9,2G  0 part [SWAP]
sdb      8:16   0 698,7G  0 disk
└─sdb1   8:17   0 698,7G  0 part /media/user/PORTABLE-BACKUP
sr0     11:0    1  1024M  0 rom
```

Set Up LUKS Header

Once you’re certain you have the right device name, add a LUKS header to the partition.

```
sudo cryptsetup luksFormat /dev/sdb1
```

Type “YES” and then choose a strong password for your encrypted partition. Type the same password when asked to verify the passphrase.

Create a Filesystem on the Partition

You have to map this physical device to a virtual device. What gets written to the virtual device will be encrypted before being stored on the physical device.

```
sudo cryptsetup luksOpen /dev/sdb1 encrypted-partition
```

The partition needs a filesystem to be usable. Create an ext4 filesystem with this command:

```
sudo mkfs.ext4 /dev/mapper/encrypted-partition
```

Mount Encrypted Partition

Create the directory where you will mount the filesystem from the partition.

```
mkdir /media/PORTABLE-BACKUP
```

Mount the filesystem and change to that mounted directory:

```
sudo mount /dev/mapper/encrypted-partition /media/PORTABLE-BACKUP
cd /media/PORTABLE-BACKUP
```

Change ownership and rights

At the moment, only the root user can write here. Give your user permission to write in this filesystem by making it the owner of the upper level directory. Copy and paste the whole command, including the "." at the end.

```
sudo chown $USER:$USER .
```

Restrict other users from reading or writing to this directory.

```
chmod o= .
```

Access from file manager

At this point, most file managers should show you the new encrypted device in the interface. This shows how it looks in the Thunar file manager, the default used in the XFCE desktop environment.

If the volume is not mounted, when you click on it you will be asked for the volume password and your sudo password. The volume will be mounted automatically, and you will be able to browse it. The mountpoint will be different from "~/encrypted-storage." It could be something like "/media/user/f42f3025-755d-4a71-95e0-37eaeb761730/,"

That is unimportant; permissions you set earlier still apply. What is important is to remember to right-click it and unmount when you finish working with the volume. Unmounting and closing the virtual device guarantees that no one can read the data from the encrypted partition, not even your operating system.

Manual (un)mounting

If, for some reason, your file manager doesn't support this feature, you can mount from the terminal.

```
sudo cryptsetup luksOpen /dev/vda3 encrypted-partition
sudo mount /dev/mapper/encrypted-partition ~/encrypted-storage
```

You can now access the volume by going to “/home/username/encrypted-storage” in the file manager. When you’re done, unmount the filesystem and close the virtual device:

```
cd && sudo umount /dev/mapper/encrypted-partition
sudo cryptsetup luksClose /dev/mapper/encrypted-partition
```

From:
https://wiki.oscardegroot.nl/ - **HomeWiki**

Permanent link:
https://wiki.oscardegroot.nl/doku.php?id=linux:debian:disk-enryption&rev=1607690361

Last update: **2022/01/15 11:38**