1 Komplett verschlüsseltes Linux-Mint 21

1.1 Festplattenstruktur

Das Ziel ist ein vollständig verschlüsseltes Linux-Mint, bei dem das Dateisystem Ext4 benutzt werden soll. Es soll verteilt auf 2 Festplatten installiert werden. Die Installationsoption Vollverschlüsselung im Linux-Mint Setup ist für dieses Ziel nicht benutzbar. Diese Option benutzt nur eine Festplatte. Es soll eine Struktur wie im folgenden Bild erstellt werden.

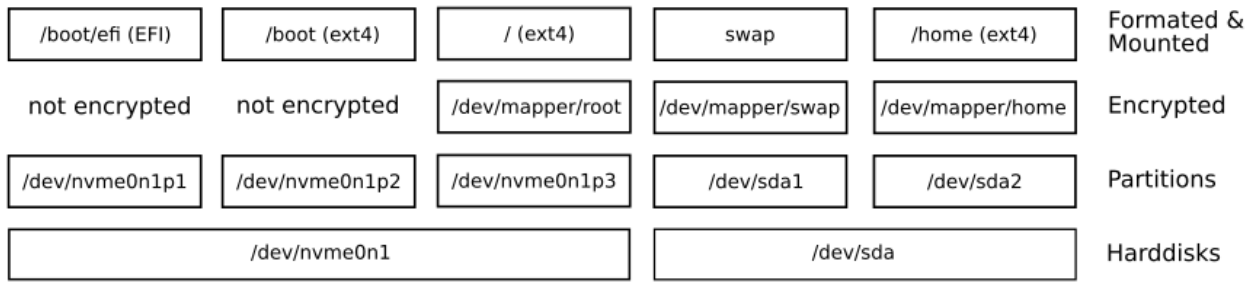


Abbildung 1: Festplattenstruktur

Die unverschlüsselte FAT32 formatierte EFI System Partition und die unverschlüsselte Boot-Partion sind notwendig, damit das Linux Mint auf PC's mit UEFI startfähig ist. Der LVM wird nicht benutzt, da das Zusammenfassen der Festplatten den Grad der Datensicherheit auf den Festplatten verringert. Fällt bei zusammengefassten Festplatten eine davon aus, verliert man komplett alle Daten. Für die einmalige Eingabe des Verschlüsselungskennwortes wird auf anderem Weg als mit dem LVM gesorgt.

1.2 Vorbereitungen

Die notwendigen Tools cryptsetup und gparted sind im Linux-Mint 21 Livesystem bereits vorinstalliert. mit dem folgenden Befehl wird ein benötigtes Kernel-Modul geladen:

```
sudo modprobe dm-crypt
```

Mit dem folgenden Befehl kann überprüft werden, ob das Modul geladen wurde. Der Unterstrich anstatt des Bindestrichs oben ist kein Fehler:

```
sudo lsmod | grep dm_crypt
```

Die Festplatten können mit dem folgenden Befehl mit Zufallszahlen überschrieben werden. Je nach Größe der Festplatten kann dieser Vorgang aber mehrere Stunden bis Tage dauern. Bei SSD's sollte man von diesem Schritt absehen.

```
sudo shred -vn 1 /dev/sda
```

1.3 Festplatten Partitionierung

Die Vollverschlüsselung des Linux-Mint Setups setzt bei mir eine 513MiB große EFI System Partition und eine 1,67GiB große Boot-Partition. Da ich keine Platzprobleme habe, wähle ich großzügig 1GiB und 2GiB als Partitionsgrößen. Wenn Suspend-to-disk als Ruhezustand benutzt werden soll, sollte die SWAP-Partition 1,3mal so groß sein wie der RAM (ca. 64GiB*1,3≈83,2GiB).

Die folgenden Partitionen müssen angelegt werden:

Tabelle 1: Partitionen

Partition	"LUKS"-Name	Dateisystem	Einhängepunkt	Größe
/dev/nvme0n1p1	-	FAT32	/boot/efi	1GiB
/dev/nvme0n1p2	-	EXT4	/boot	2GiB
/dev/nvme0n1p3	/dev/mapper/root	EXT4 (verschlüsselt)	/	restlicher Platz
/dev/sda1	/dev/mapper/swap	SWAP (verschlüsselt)	-	83,2GiB
/dev/sda2	/dev/mapper/home	EXT4 (verschlüsselt)	/home	restlicher Platz

Für die Partitionierung der Festplatten wird das Tool geparted gestartet:

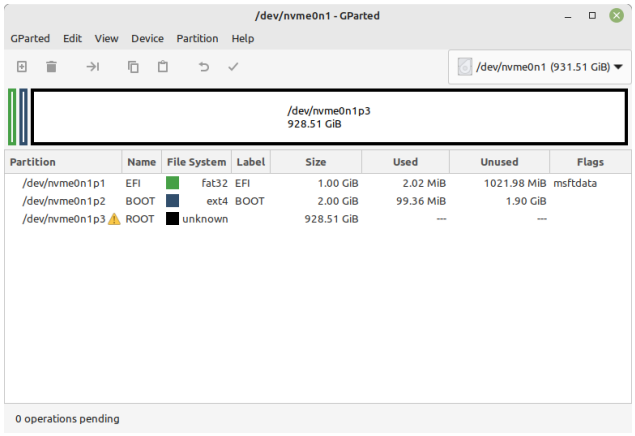
```
sudo geparted
```

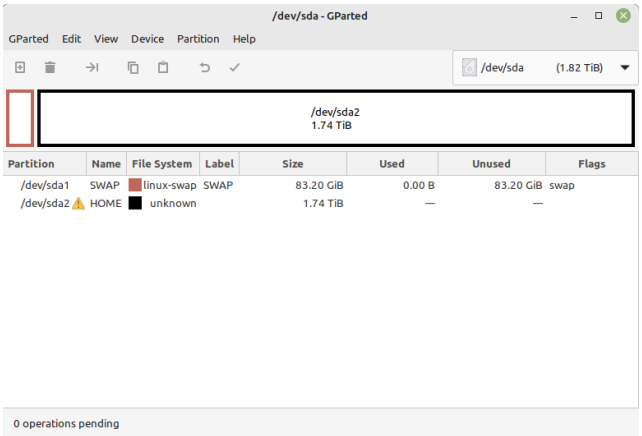
Zuerst muss pro Festplatte eine Partitionstabelle erzeugt werden. Nachdem rechts oben die jeweilige Festplatte ausgewählt wurde, erzeugt man die Partitionstabelle. Bei den heutigen Festplattengrößen wähle ich "gpt". Dieser Schritt wird für beide Festplatten wiederholt.

```
Device -> Create Partition Table -> Den Punkt "gpt" wählen.
```

Rechts oben die Festplatte /dev/nvme0n1 auswählen. Mit "Partition -> New" werden die Partitionen erstellt. Bevor zur zweiten Festplatte gewechselt werden kann, müssen die Änderungen mit dem Häckchen "Apply All Operations" in der Iconzeile übernommen werden.

Danach wählt man rechts oben die Festplatte /dev/sda aus, und wiederholt die Schritte im vorherigen Absatz. Auf beiden Festplatten wird für die zu verschlüsselnden Partitionen als Formatierung "unformatiert" ausgewählt.





Danach wird das Programm "geparted" geschlossen.

1.4 Partitionen verschlüsseln und formatieren

Die Partitionen werden mit den folgenden Befehlen verschlüsselt. Dabei muß jeweils ein Kennwort eingegeben werden. Das Kennwort sollte mindestens 8 Zeichen lang sein, es gilt aber "je länger desto besser". Damit später beim Systemstart nur einmal das Kennwort zum Entschlüsseln eingegeben werden muß, sollten die Kennwörter für alle Partitionen identisch sein.

```
sudo cryptsetup -c aes-xts-plain64 -y -s 512 luksFormat /dev/nvme0n1p3
sudo cryptsetup -c aes-xts-plain64 -y -s 512 luksFormat /dev/sda1
sudo cryptsetup -c aes-xts-plain64 -y -s 512 luksFormat /dev/sda2
```

Damit das Linux-Mint Setup die verschlüsselten Partitionen ansprechen kann, müssen diese geöffnet und mit einem Namen versehen werden.

```
sudo cryptsetup luksOpen /dev/nvme0n1p3 root
sudo cryptsetup luksOpen /dev/sda1 swap
sudo cryptsetup luksOpen /dev/sda2 home
```

Um später im Linux-Mint Setup eventuelle Probleme zu vermeiden, sollten jetzt alle Partitionen manuell formatiert werden.

```
sudo mkfs.vfat -F32 /dev/nvme0n1p1       (EFI-Systempartition)
sudo mkfs.ext4 /dev/nvme0n1p2            (/boot)
sudo mkfs.ext4 /dev/mapper/root          (/)
sudo mkfs.ext4 /dev/mapper/home          (/home)
sudo mkswap /dev/mapper/swap             (Swappartion)
```

1.5 Installation des eigentlichen Systems

Nun startet man die grafische Linux-Mint Installation durch einen Doppelklick auf das Desktop-CD-Symbol. Wie gewohnt folgt man den Anweisungen des Installationsassistenten.

Erreicht man das Fenster "Installationsart", werden die Punkte "Festplatte löschen und Linux Mint installieren" und "Etwas Anderes" angezeigt. Wir wählen jetzt den Punkt "Etwas Anderes."

Leider ist das folgende Fenster unübersichtlich, da es sich nicht in seiner Größe verändern läßt. Wir konzentrieren uns auf die "Laufwerke" in der Tabelle 1 (Abschnitt 1.3), und konfigurieren ausschließlich diese entsprechend der Tabelle.

```
/dev/nvme0n1p1; /dev/nvme0n1p2;                      (unverschlüsselt)
/dev/mapper/root; /dev/mapper/home; /dev/mapper/swap (verschlüsselt)
```

Auf der Registerkarte "Wer sind Sie?" Sollte man die Option "Meinen persönlichen Ordner verschlüsseln" nicht auswählen, immerhin sind ja bereits die Partitionen verschlüsselt.

Am Ende der Installation darf NICHT neu gestartet werden. Es sind noch manuelle Nacharbeiten notwendig. Wir kehren mit "Fortfahren mit Testen" zum Livesystem zurück.

1.6 Manuelle Nacharbeiten

Wenn man jetzt neu starten würde, könnte man das System nicht hochfahren. Es verfügt nämlich noch nicht über die nötige Software, um das verschlüsselte Laufwerk ansprechen zu können, und den Benutzer nach dem Passwort zum Entschlüsseln zu fragen. Daher wechselt man mittels "chroot" in das gerade auf die Festplatte kopierte System und installiert die benötigten Pakete "cryptsetup" und "keyutils".

1.6.1 Chroot starten und Paket installieren

Um die fehlenden Pakete installieren zu können, müssen wir mittels des Befehls "chroot" in das bereits installierte System wechseln. Dafür müssen die Partitionen des installierten Systems aber zunächst gemountet werden. Danach erfolgt der Wechsel in das installierte System, und die Installation der Pakete.

```
sudo mount /dev/mapper/root /mnt
sudo mount /dev/mapper/home /mnt/home
sudo mount /dev/nvme0n1p2 /mnt/boot
sudo mount /dev/nvme0n1p1 /mnt/boot/efi
sudo mount -o bind /dev /mnt/dev
sudo mount -t proc proc /mnt/proc
sudo mount -t sysfs sys /mnt/sys
sudo cp /etc/resolv.conf /mnt/etc/resolv.conf
sudo chroot /mnt /bin/bash
apt install cryptsetup keyutils
```

Normalerweise sollten die Pakete "cryptsetup" und "keyutils" schon vorher installiert sein. ***Die chroot-Umgebung noch nicht verlassen!***

1.6.2 Entschlüsseln der Partitionen

Damit die Crypto-Laufwerke direkt beim Booten automatisch zur Entschlüsselung angefordert werden, muss noch die Datei "/etc/crypttab" um entsprechende UUID-Einträge der verschlüsselten Partitionen ergänzt werden. Die folgenden Befehle ermitteln die UUID's und schreiben die benötigten Zeilen in die Datei "/etc/crypttab". Die Label "root", "swap" und "home" am Anfang der folgenden Befehle stammen aus den Gerätebezeichungen /dev/mapper/root, /dev/mapper/swap und /dev/mapper/home, die so auch in der /etc/fstab stehen. Durch die identischen Namen ist die Zuordnung der Definitionen in beiden Dateien zueinander gegeben. Linux-Mint liefert ein Kennwort-Chaching-Script "decrypt_keyctl" mit dem "cryptsetup" Paket aus. Das Skript "decrypt_keyctl" stellt mehreren verschlüsselten LUKS-Zielen das selbe Kennwort zur Verfügung, so daß man es nicht mehrfach eingeben muß.

```
echo "root UUID=$(cryptsetup luksUUID /dev/nvme0n1p3)
crypt_disks luks,discard,keyscript=decrypt_keyctl" >> /etc/crypttab

echo "swap UUID=$(cryptsetup luksUUID /dev/sda1)
crypt_disks luks,discard,keyscript=decrypt_keyctl" >> /etc/crypttab

echo "home UUID=$(cryptsetup luksUUID /dev/sda2)
crypt_disks luks,discard,keyscript=decrypt_keyctl" >> /etc/crypttab
```

Die Änderungen an der Datei "/etc/crypttab" müssen jetzt noch übernommen werden. Danach kann die Chroot-Umgebung verlassen und das System neu gestartet werden.

```
update-initramfs -u -k all
exit
sudo reboot
```

Damit ist das komplettverschlüsselte Linux-Mint installiert und startfähig.

Diese Anleitung basiert im Kern auf der folgenden Internetseite:

`https://blog.andreas-haerter.com/2011/06/18/ubuntu-festplattenvollverschluesselung-lvm-luks`

Das Verfahren hier in diesem Dokument wurde vereinfacht, und den heute aktuellen Rechnern angepaßt. Die Informationen wurden nach besten Wissen und Gewissen zusammengestellt und ausprobiert. Es kann nicht garantiert werden, daß die beschriebene Installation immer wie erwartet von statten geht. Deshalb wird für direkte oder indirekte Schäden die durch Nutzung der Informationen in diesem Dokument entstehen, keine Garantie oder Haftung übernommen.

THE+SWISS+GRID (2022)

`WWW:      https://swissgrid.opensim.ch`
`LoginURI: http://swissgrid.opensim.ch:8002`

Jules Dreki