Ubuntu Studio (3)

De multimediaversie van Ubuntu

Ton Valkenburgh

In het vorige deel van deze artikelenreeks hebben we Windows voorbereid volgens de ideeën die in het eerste artikel zijn beschreven. Nu gaan we eindelijk aan de slag om Ubuntu Studio te installeren.

1. Inleiding

Linux kent een aantal autorisatieniveaus. Hieronder een korte toelichting om sommige keuzes tijdens de installatie duidelijker te maken. De niveaus zijn:
1. Super-user, het hoogste niveau;
2. Root, het standaard beveiligde niveau;
3. User, de gebruiker, die eventueel ook *root*-autorisatie kan hebben;
4. Gast, een niveau met weinig mogelijkheden.

Tijdens de installatie hebben we met de niveaus *root* en *user* te maken. De andere twee komen in latere artikelen ter sprake.
Het is belangrijk dat gegevens die onder *root*-autorisatie vallen voor een gebruiker niet direct toegankelijk zijn. Hij zal zijn root-autorisatie – als hij die heeft – bewust moeten inschakelen. Dat doet hij door *sudo* voor een commando of programmanaam te zetten. Alvorens het commando uit te voeren of het programma op te starten, wordt om zijn wachtwoord gevraagd.
Als je met een live Linux-dvd opstart, heb je ook *root*-autorisatie. Daarom zijn gegevens onder *root*-autorisatie – net zoals bij Windows – niet echt veilig. Het is daarom verstandig om een systeem geheel te versleutelen of minstens je *home*-map (directory) te versleutelen. Bij de installatieprocedure van Ubuntu krijg je die keuze voorgeschoteld.

2. SSD installeren

De gekozen Samsung SSD 960 EVO is een zogenaamde Self Encrypted Drive. Deze SSD ondersteunt autorisatie volgens het TCG OPAL-protocol. De SSD kan echter direct uit het doosje worden gebruikt. Het activeren van het vergrendelen volgens TCG OPAL doe je nadat het operating systeem is geïnstalleerd.
We willen dat Windows en Ubuntu echt onafhankelijk van elkaar zijn. Dus het verwijderen van de één mag niet tot het niet meer functioneren van de ander leiden. Daarom installeren we Ubuntu op de SSD terwijl de HDD niet aanwezig is. De laptop moet worden opengemaakt om de SSD in het M.2-slot aan te brengen. Nu de laptop toch open is, verwijder je gelijk de HDD. Dit moet, om te voorkomen dat bij het installeren van Ubuntu de bootloader *grub* op de UEFI van de HDD wordt geïnstalleerd. Na het installeren van Ubuntu plaats je de HDD terug.
Om van een NVMe-SSD te kunnen opstarten, moet de schijf een UEFI-schijf zijn. Daarom had ik Windows ook op een UEFI-schijf gezet. In de BIOS heb ik secure boot i.v.m. het gebruik van VeraCrypt al uitgeschakeld. Voor de TCG Opal-implementatie die ik wil gebruiken, is het ook nodig om secure boot uit te schakelen.
Een grote tegenvaller is, dat de open source *TCG Opal sedutil* de NVMe-SSD's in mijn laptop niet goed blijkt te ondersteunen. Of dit specifiek voor mijn laptop is, is mij niet bekend. Meer informatie is te vinden op de website van CompUsers > platform muziek > Encryptie. Daarom kies ik voor softwareversleuteling en uit veiligheidsoverweging gebruik ik geen overprovisioning op de SSD. Uiteraard kun je Ubuntu Studio ook zonder versleuteling installeren.

3. Ubuntu Studio op USB-stick zetten

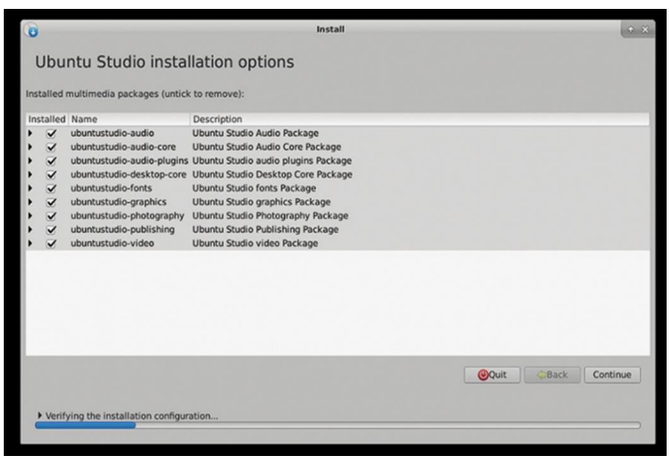
Van de Ubuntu Studio-website haal je Ubuntu Studio 16.04[1] 64-bit op. Dit ISO-bestand kun je op een dvd branden, maar beter is het om van dit ISO-bestand een opstartbare USB-stick te maken. Het installeren van een USB-stick gaat veel trefzekerder en het is trouwens handig om deze stick te bewaren om eventueel reparaties aan te brengen op je geïnstalleerde systeem. Ik gebruik het vrij verkrijgbare programma *Rufus* om deze USB-stick aan te maken. Zorg dat de stick een UEFI-boot-optie bevat.

4. Ubuntu installeren

Ik ga dus werken vanaf de USB-stick; dan gaat de installatie trouwens veel sneller. Hoe je moet opstarten van een USB-

1. Ubuntu Studio 17.04 is beschikbaar, maar is, gezien een paar vervelende bugs, nog niet aan te raden.

stick is bij iedere fabrikant anders. Op mijn ASUS N752VX gaat dat via het BIOS bootmenu. Bij mijn laptop loop ik gelijk tegen het probleem aan dat de nVIDIA Geforce GTX 950 niet goed wordt ondersteund. De opgestarte live USB-stick blijft hangen in het opstartscherm van Ubuntu Studio. Als je dat overkomt is er gelukkig een workaround. Bij het opstarten van de stick kom je in de *grub mode*. Tik dan *e* in en pas grub aan door *quiet splash* in *nomodeset* te veranderen. Daarna kies je *F10*. Nu start de live-stick gewoon op in een lagere schermresolutie. Dat heeft het nadeel dat de knop *Verder* af en toe buiten het beeld valt. Gewoon *Enter* geven werkt gelukkig prima. Bij oudere systemen zal dit probleem waarschijnlijk niet optreden.
Nu de live-stick is opgestart, dubbelklik je op *Install Ubuntu Studio 16.04*. Kies Nederlands en ga *Verder*. Zet vinkjes bij *Haal bijgewerkte pakketten binnen* en bij *Installeer programmatuur van derden*. Ga *Verder*. Bij Installatie-opties kies je de pakketten die je wilt installeren. Je kan ze later altijd weghalen of installeren. Dus laat de vinkjes maar staan.



Ga *Verder*. Als installatie type kiezen we *Wis schijf en installeer Ubuntu Studio*. Je hebt in dit venster ook de extra opties om je systeemdisk te versleutelen of alleen de *Home*-map. De versleuteling is transparant en in het verdere installatieproces merk je er dus niets van. Wil je niet de hele schijf versleutelen, dan raad ik in ieder geval het versleutelen van je *Home*-map aan. Klik op de knop *Verder*.
Volg nu de schermen en vul de gewenste informatie in. Ga *Verder*. De installatie loopt nu.
Zodra de installatie is voltooid, sluit je af. Nu kunnen we de HDD weer aanbrengen.

5. Ubuntu Studio configureren

Start de laptop weer op. Als je last had van het NVIDIA probleem dan tik je in *grub mode* weer *e* in en pas grub aan door *quiet splash* in *nomodeset* te veranderen. Daarna kies je weer *F10*. Bij sommige laptops krijg je dan een zwart scherm; tik dan gewoon je wachtwoord in. Ga via het *menu > Instellingen en systeembeheerder > Extra stuurprogramma's* en selecteer daar de *nVIDIA driver*. Klik daarna op *Wijzigingen doorvoeren*. Je herstart de laptop en je krijgt nu Ubuntu met de juiste resolutie op je scherm.
We gaan eerst kijken of er software updates zijn. Via het *menu > Software* kom je in het *Software Center*. Er wordt waarschijnlijk aangegeven dat er updates zijn. Installeer deze. Dat duurt meestal vrij lang. Wacht tot de melding *Software is up-to-date* verschijnt.
Installeer ook via het *Software Center* de *Firewall Configuration*. Na het installeren kun je deze opstarten via het menu bij *Instellingen en beheer*. Zet de Firewall aan met *Incoming: weigeren* en *Outgoing: toestaan*.
Installeer via het Software Center het antivirusprogramma ClamTk. Configureren kun je doen via het *menu > Systeem > ClamTK*. COMODO biedt een uitgebreidere virusscanner, maar deze is van 2013. Er treden daardoor conflicten op met de nieuwe Ubuntu. Het installeren en configureren van COMODO valt buiten het kader van dit artikel. In een later artikel kom ik terug op het installeren van COMODO voor Linux. We gaan nu de instellingen voor het optimaliseren van Ubuntu voor SSD verzorgen.

5.1 Optimalisatie voor SSD

Omdat de levensduur van een SSD door schrijfacties wordt beperkt, is het van belang zoveel mogelijk de schrijfacties te beperken.

Iedere keer als een bestand wordt gelezen wordt de *access time* van het bestand bijgehouden. Deze onnodige schrijfacties willen we voorkomen.
Allereerst installeer je de editor *leafpad* via het *Software Center*. Je opent daarna via *menu > Terminal* het equivalent van de Windows DOS-prompt.
Tik in de terminal: *sudo leafpad /etc/fstab*. Hierna wordt om het wachtwoord gevraagd. Tik dit in - het veld blijft blank - en geef *Enter*.

Verander de regel:
```
UUID=xxxxx  /  ext4 errors=remount-ro  0  1
```
in:
```
UUID=xxxxx  /  ext4 noatime,errors=remount-ro  0  1
```

en sla het resultaat op.
Denk er om geen spaties rondom de komma!

Omdat we geen overprovisioning hebben aangebracht is het van belang dat het Trim-commando zeer regelmatig wordt gegeven. Trim staat in Ubuntu standaard aan op wekelijks. We gaan het omzetten naar dagelijks.
Geef hiervoor het commando:
```
sudo mv -v /etc/cron.weekly/fstrim /etc/cron.daily
```

Het virtuele geheugen (swap-bestand) veroorzaakt ook veel schrijfacties. Daarom beperken we het schrijven naar het swap-bestand.
Geef het volgende commando:
```
sudo leafpad /etc/sysctl.conf
```

Voeg onderaan in het bestand de volgende regels toe en sla op:
```
# Verminder de swapneiging ten zeerste
vm.swappiness=1
```

Bij SATA-SSD's moet je checken of de scheduler op *deadline* staat. NVMe-SSD's gebruiken de traditionele scheduler niet, maar de blk-mq-module. Een check is daarom bij NVMe-SSD's niet nodig.

Firefox schrijft ook regelmatig naar het geheugen. Op Internet is er discussie of de volgende Firefox-optimalisatie nodig is; ik heb hem wel uitgevoerd:

Klik met de rechter muisknop op de *Menuknop* (met de drie liggende streepjes) en zet een vinkje bij *Menu Balk*.
Je kunt de schrijfacties van Firefox als volgt beperken:

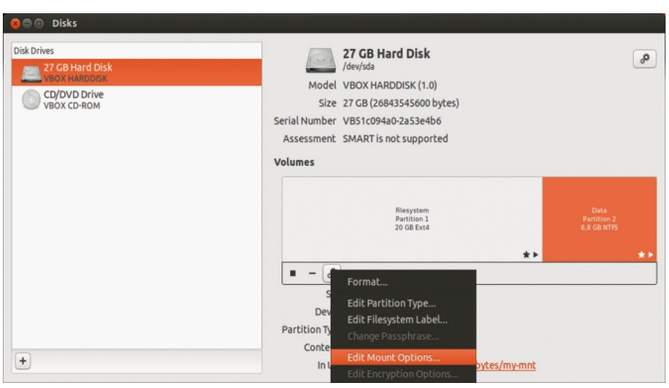
- Zet de cache op 0:
  Kies *Bewerken>Voorkeuren> Geavanceerd> Tabblad Netwerk*
  Gebufferde webinhoud: vink aan: *Automatisch bufferbeheer negeren* en zet de buffer op 0.
- Tik *about:config* in de adresbalk van Firefox en druk op Enter. Klik vervolgens op de knop om het risico te aanvaarden.
  In de zoekbalk tik je de zoekterm *sessionstore*.
  Dubbelklik op de term *browser.sessionstore.interval*. De standaardwaarde is *15000*, wat staat voor 15 seconden.
  Voeg drie nullen toe aan de bestaande waarde, zodat die *15000000* wordt. Druk op de OK-knop.
  Schakel daarna de volgende drie sessionstore-functies uit, eenvoudigweg door ze te dubbelklikken (waardoor "true" verandert in "false"):

browser.sessionstore.restore_on_demand
en:
browser.sessionstore.resume_from_crash
en:
services.sync.prefs.sync.browser.sessionstore.restore_on_demand

Sluit Firefox en start hem opnieuw. Nu heb je de sessie-herstelfunctie geheel verwijderd.

6. NTFS-disk automatisch koppelen

Als geen versleutelde NTFS-schijf hebt, maar wel een NTFS-schijf, dan vind je hier hoe je de NTFS-disk automatisch kan laten aankoppelen.
Installeer via het *Software Center* het programma *NTFS Disk-beheer*. Na het installeren start je dit programma en kies je voor automatisch aankoppelen. Het bestand *fstab* wordt nu aangepast en bij het opstarten van de laptop zullen alle NTFS-schijven worden aangekoppeld.
Heb je voor versleuteling van je Windows-systeem met VeraCrypt gekozen, dan kun je in *10.1. VeraCrypt installeren en configureren* de benodigde informatie vinden om de toegang tot een versleutelde NTFS-schijf in Ubuntu in te stellen.



7. Dual boot

Nu is het tijd om dual boot te gebruiken. In *grub* staan nu alleen *Ubuntu-items* en *Systeem*. De laatste is om naar je BIOS te gaan. Windows 10 moet nu worden toegevoegd.
In de terminal geven we het commando: *sudo update-grub*. Hierna herstarten we de laptop. In het *grub-menu* vind je nu ook Windows.

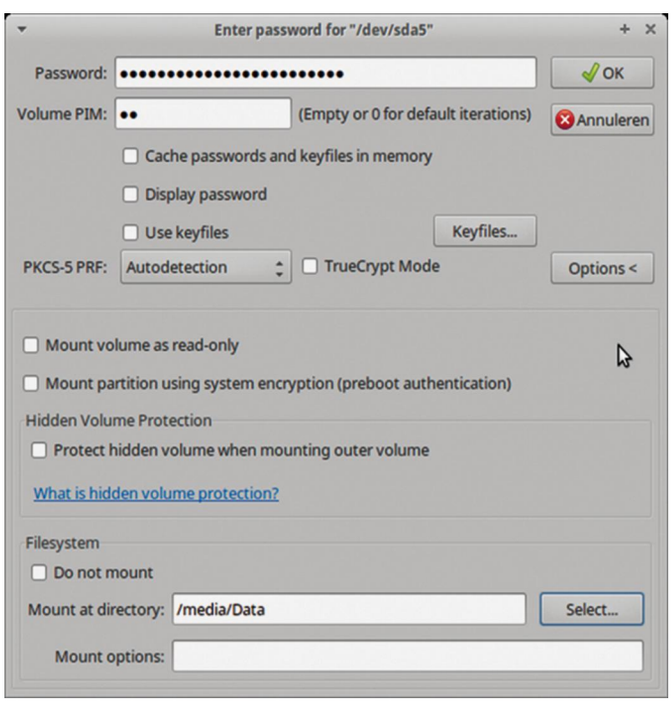
8. Netwerktijd synchronisatie

Er staat je een onaangename verrassing te wachten bij het gebruik van dual boot met een Linux- en Windows-systeem. Linux slaat namelijk in de BIOS *Greenwich Mean Time* op. Windows echter de *actuele tijd*. Je merkt dus een verschil van één à twee uur, een en ander afhankelijk van zomer- of wintertijd. Linux synchroniseert zijn tijd bij het opstarten met de netwerktijd. Windows doet dit echter niet standaard. Dit moeten we dus in Windows aanpassen.
We starten Windows 10 op. Ga naar het *Configuratiescherm* en klik op *Systeembeheer*. Dubbelklik op *Taakplanner* en kies dan *Task scheduler-bibliotheek* > *Microsoft* > *Windows* > *Time Synchronization*. Dubbelklik op *Force Synchronization Time*. Klik op *Triggers* en kies *Nieuw*. Bij *Start deze Taak* kies je voor *Bij opstarten*. Klik op *OK*. Selecteer tab *Aangepaste Trigger* en *Verwijder deze*. Klik op *OK*. Sluit de *Taakplanner* af.
Nu wordt ook bij Windows 10 de tijd bij het opstarten gesynchroniseerd.

9.Conclusie

We hebben nu een dual boot-systeem gerealiseerd waarbij de gegevens door beide systemen kunnen worden gedeeld. De volgende stap is om Ubuntu Studio klaar te maken voor muziektoepassingen.
Hierover meer in het volgende artikel.

10. Appendix



10.1 VeraCrypt installeren en configureren
Als je Windows met VeraCrypt hebt versleuteld, wil je de versleutelde data-partitie op de HDD automatisch aankoppelen. Eerst bepalen we waar de gegevens van deze partitie straks zijn te vinden. We maken daarom een map *Data* aan in de map waar bij Linux normaal de aangekoppelde partities en schijven terecht komen. Geef in de terminal de volgende commando's:

```
sudo mkdir /media/Data
sudo chown <naam> /media/Data
```
(waarin <naam> je gebruikersnaam is)

Nu halen we de Linux-versie op van de VeraCrypt-website. Navigeer met bestandssysteem naar de map waarin VeraCrypt is opgeslagen. Dubbelklik op het VeraCrypt-bestand om het uit te pakken. Open de map waar de bestanden zijn opgeslagen. Dat is standaard de map Downloads van de gebruiker. Klik met de rechtermuisknop boven deze map en kies *Open hier een terminalvenster*.
Tik in het terminalvenster:
```
sudo ./veracrypt-1.19-setup-gui-x64.
```
Volg de aanwijzingen en VeraCrypt wordt geïnstalleerd. Je kan VeraCrypt nu vinden bij *menu* > *hulpmiddelen*.
Start VeraCrypt. Klik op *Select device*... en kies in het volgende scherm de gewenste partitie. In ons geval */dev/sda5*. Kies nu *Mount* en vul het wachtwoord in. Vink *Use PIM* aan en vul dit in. Kies daarna Options. Bij *Mount at Directory* vul je */media/Data* in. Klik nu op *OK*.

Na het aankoppelen kies je *Add All Mounted Volumes to Favorites*…
Start VeraCrypt en *mount* de Data-partitie met als locatie */media/Data*; voeg deze partitie toe aan *favorites*.

We gaan nu zorgen dat deze Datapartitie automatisch wordt aangekoppeld bij het opstarten van Ubuntu. We zorgen er wel voor dat het wachtwoord van deze partitie niet voor iedereen zichtbaar is.
Creëer met leafpad een verborgen bestand `/home/<naam>/.veracryptcredentials` en zet hierin op de eerste regel (<naam> is de gebruikersnaam):
```
--pim=<pim> --password=<pw>[2]
```

Geef het commando:
```
chmod 600 /home/<naam>/.veracryptcredentials
```

Maak root de eigenaar met het commando:
```
sudo chown root /home/<naam>/.veracryptcredentials
```
Maak in */home/<naam>* een map scripts met het commando
```
mkdir /home/<naam>/scripts
```

Maak in deze map met leafpad het bestand `mount_data.sh` aan met de volgende inhoud:
```
#!/bin/bash
# Mount VeraCrypt Data Disk
#
cd /usr/bin
sudo ./verascript
```

Maak het executable met het commando:
```
chmod +x /home/<naam>/scripts/mount_data.sh
```
Geef het commando:
```
sudo leafpad /usr/bin/verascript
```

Zet in dit bestand het volgende:
```
#!/bin/bash
# Veracscript - mounting VeraCrypt drives
#
# Mount favorites veracrypt drives
# started until it is shut down again.
file="/home/ton/.veracryptcredentials"
/usr/bin/veracrypt $(cat "$file") -automount=
favorites
```

Geef het commando:
```
sudo chmod 640 /usr/bin/verascript
```
Geef het commando:
```
sudo chmod +x /usr/bin/verascript
```

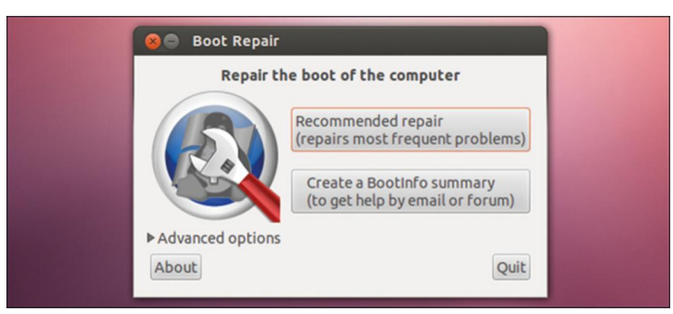
2. De punt aan het begin van de bestandsnaam geeft aan dat het een verborgen bestand is.
<pim> en <pw> zijn de gebruikte pim en password voor de betreffende partitie.

Bij het gebruik van VeraCrypt moet je zowel het gebruikerswachtwoord als het wachtwoord van de aan te koppelen partitie opgeven. Bij het opstarten kunnen we dit echter voor het aankoppelen niet intoetsen. Daarom gaan we zorgen dat voor VeraCrypt dit wachtwoord niet nodig is.

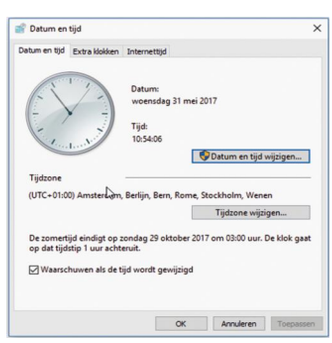
Ga naar de map */etc/sudoers.d* en open hier de terminal;
Geef het commando: `sudo visudo -f veracrypt`
Zet op de eerste regel:
```
<naam> ALL = (root) NOPASSWD: /usr/bin/
   verascript,/usr/bin/veracrypt
```
Sla het met *Ctrl+O* op met de bestandsnaam *veracrypt*.
Geef daarna het commando:
```
sudo chmod 640 veracrypt
```
Voeg bij *instellingen en systeembeheerder* bij *Sessie en Opstart* de volgende regel toe:
```
/home/<naam>/scripts/mount_data.sh
```

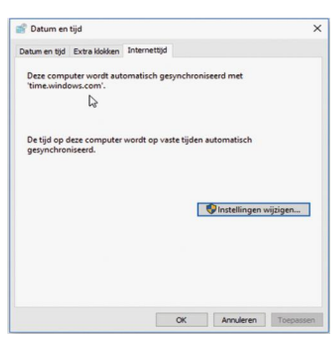
Bij het opstarten van de laptop zal nu automatisch de versleutelde Data-partitie worden aangekoppeld. Bij deze opzet is het van belang dat de systeempartitie, maar in ieder geval de *Home*-map is versleuteld. Anders zou door middel van bijvoorbeeld een live dvd het wachtwoord van de versleutelde Data-partitie kunnen worden achterhaald.
Ubuntu is nu klaar voor gebruik.

10.2 Dual boot met versleutelde Windows
In *GRUB* staan nu alleen *Ubuntu-items* en *Systeem*. De gegeven methode zoals aangegeven in Dual boot werkt niet als Windows is versleuteld. Met *boot-repair* is dit te regelen, maar dit wil nog wel eens misgaan en dan moet je Windows en Ubuntu weer opnieuw installeren.



Het is daarom verstandig om tussen Windows en Ubuntu te wisselen via de BIOS. BIOS ondersteunt meestal het kiezen van het op te starten systeem. Bij mijn laptop activeer je dit door *ESC* in te toetsen tijdens het BIOS opstartscherm. Bij HP is dit *F12* en bij MSI *F11*. Afhankelijk van de BIOS moet je eventueel je BIOS administratiewachtwoord in tikken en daarna kies je het op te starten systeem.
Nu moet je nog zorgen dat de netwerktijdsynchronisatie in Windows goed staat. Ga hiervoor naar Netwerktijdsynchronisatie.





Links

- **https://ubuntustudio.org/**
- **https://rufus.akeo.ie/**
- **https://veracrypt.codeplex.com/**