Back-up onder Linux (2)

Ton Valkenburgh

In SoftwareBus 2021-1 zijn algemene eisen aan het maken van back-ups besproken. In SoftwareBus 2021-2 heeft Rein de Jong laten zien hoe Duplicati ingezet kan worden voor het maken van back-ups. In SoftwareBus 2021-4 is Déjà-Dup aan de orde geweest. In dit artikel wil ik specifiek ingaan op het maken van back-ups onder Linux met Back-in-Time.

Inleiding

Het kiezen van een programma om back-ups te maken is niet eenvoudig. Er zijn namelijk eenvoudige programma's, maar ook programma's met geavanceerde functies. Ook onder Linux zijn er veel mogelijkheden. In het vorige artikel, in de SoftwareBus 2021-4, heb ik Déjà-Dup besproken. De kracht van dit programma is dat het heel eenvoudig is in het gebruik. Back-in-Time heeft meer configuratiemogelijkheden en is transparanter bij het herstellen van bestanden.
Back-in-Time (link 1.)is qua idee gebaseerd op Flyback (link 2.)en Timevault (link 3.). De ontwikkelaars van Flyback hebben een schuin oog geworpen op Apple's TimeMachine.
Om dit artikel zelfstandig te kunnen lezen worden een aantal zaken herhaald die ook al in het artikel over Déjà-Dup staan.

Back-in-Time

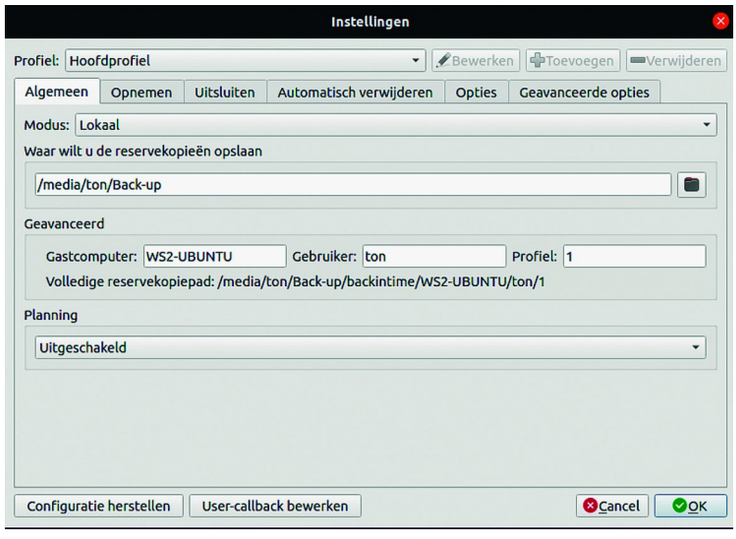
Het programma is er zowel als een uitvoering met commandoregels als met een nette grafische interface. Ik ga uit van de laatste.
Het heeft de volgende kenmerken en functies:

- uitgebreide configuratiemogelijkheden;
- mogelijkheid tot diverse back-up profielen;
- creëert snapshots:
  - *voor ongewijzigde bestanden worden hard-links gebruikt;**
  - hard-links kunnen daarom niet in de back-up worden meegenomen.
- back-up bestaat uit leesbare bestanden;
- optioneel versleutelde back-ups:
  - EncFS wordt gebruikt voor encryptie. Er wordt gewaarschuwd voor zwakheden in deze methode.
- optioneel automatische back-ups;
- lokale opslag, gekoppelde gedeelde bestanden en/of via SSH:
  - bestandssysteem van het opslagmedium moet hard-links ondersteunen;
  - samba (SMB/CIFS) ondersteunt niet standaard symbolische links.
- transparant:
  - leesbare bestanden waardoor de gebruiker direct het te herstellen bestand kan zien;
  - door gebruik van hard-links lijkt iedere snapshot een volledige back-up;
  - geïntegreerde browser.

Back-in-Time kunt u in de meeste Linux-distributies vinden.

Installatie en configuratie

Bij Ubuntu 20.04 ontbreekt het in het Software Center. U heeft de keuze uit twee versies. Bij de root-versie kunt u ook systeemprogramma's back-uppen. Bij de andere versie is dat niet mogelijk. Onder de motorkap gebruikt Back-in-Time rsync.
Na installatie heeft u de beschikking over beide versies. De taal is gelijk aan de taal van uw distributie.
U start Back-in-Time op vanuit Toepassingen tonen.



Afbeelding 1: Back-in-Time hoofdvenster

We kunnen nu kiezen van welke mappen we een back-up willen maken en ook welke mappen we willen uitsluiten. Bij Waar wilt u de reservekopieën opslaan kunnen we kiezen uit: *Lokaal, Lokaal versleuteld, SSH* en *SSH-versleuteld*.

Lokale snapshots kunnen op interne schijven, USB-schijven of extern gekoppelde gedeelde mappen worden opgeslagen. Het doelbestandssysteem moet hard-links ondersteunen. Ook moet het protocol hard-links en symbolische links ondersteunen. Samba ondersteunt standaard geen hard-links . Dit moet worden geactiveerd door in /etc/samba/smb.conf het volgende te definiëren: *follow symlinks* = *yes* en *wide links* = *yes*. *Sshfs* gekoppelde gedeelde mappen ondersteunen geen hard-links.

Omdat ik altijd de beschikking wil hebben over mijn back-up prefereer ik een externe schijf. Ik gebruik twee schijven. Eén daarvan is opgeborgen op een andere locatie. Geregeld worden de schijven omgewisseld. Dit houdt gelijk de sociale contacten in stand. Opslaan in de cloud of op een externe server heeft het nadeel dat als het internet niet beschikbaar is, er ook geen mogelijkheid is om een back-up terug te zetten. Ook speelt hier mee dat de versleuteling een zwak punt kent. Bij het opslaan van uw back-up op een USB-schijf raad ik aan de USB-schijf te versleutelen. In Linux is dat heel makkelijk. Zie hiervoor de appendix.

De eerste keer wordt een volledige back-up gemaakt. De daarop volgende keren zijn het incrementele back-ups. Voor alle zekerheid raad ik aan om na circa drie maanden weer

* Een *hard-link* creëert een apart bestand waarin informatie over het originele bestand en zijn locatie is opgeslagen.
Een *symbolische link* is een bestand dat wijst naar een ander bestand in het virtuele bestandssysteem van Linux.

een volledige back-up te maken. Iedere back-up wordt geverifieerd. Ook wordt af en toe bij de verificatie om het wachtwoord gevraagd. Op die manier wordt getest of u uw wachtwoord nog weet.

Back-up maken

Welke bestanden moeten we in de back-up opnemen? Normaal kiest u alleen voor gebruikersbestanden. Als u ook systeembestanden in de back-up wilt meenemen, gebruikt u Back-in-Time als root.
Back-in-Time heeft een aantal opties die handig kunnen zijn. Ik pik er twee uit:

- Controle-som gebruiken om wijzigingen op te sporen. Hierdoor wordt de inhoud van bestanden vergeleken;
- Maak ook een nieuwe reservekopie als er niets is gewijzigd. Op deze wijze forceert u een volledige back-up.

Voor het instellen van de geavanceerde opties is meer kennis van Linux vereist.

Afbeelding 2: Opties

Het meenemen van systeembestanden in de back-up raad ik af. De back-up duurt dan langer. Als u een systeemcrash heeft en uw systeem wil niet meer opstarten heeft u niets aan een dergelijke back-up. Ook is het niet echt nodig om geregeld een back-up van uw systeembestanden te maken. De meeste wijzigingen zijn updates en die kunt u altijd weer makkelijk installeren. De systeembestanden en de gebruikersbestanden staan bij mij op aparte schijven. Als u slechts één schijf in uw systeem heeft kunt u aparte partities gebruiken. Ik maak alleen een back-up van mappen waarin gebruiksgegevens staan. Dat zijn zowel mappen op mijn pc als op mijn NAS.

Gebruikt u virtuele machines? De bestanden van virtuele machines kunnen groot zijn: zeker de bijbehorende virtuele disk. Na ieder gebruik van een virtuele machine is dit bestand gewijzigd en het wordt dus bij iedere incrementele back-up volledig meegenomen. Dit vertraagt de back-up aanzienlijk. Sluit deze bestanden dus uit. Het is beter van de virtuele machine bestanden een back-up met behulp van een speciaal scenario te maken en dat minder vaak te doen dan uw reguliere back-up.

Ik maak mijn back-ups niet automatisch, maar start ze op met de hand. Het gevaar van automatische back-ups is, dat u niet zeker weet of de back-up gelukt is. Het kan zijn dat door een update de back-up niet meer wordt opgestart. Op het moment dat u uw back-up nodig heeft blijkt dat er misschien al een lange tijd geen back-up is gemaakt. Zo'n verrassing wilt u toch voorkomen?

Voor de back-up van de systeembestanden gebruik ik Clonezilla (link 4.). Clonezilla maakt het mogelijk om een schijf of partitie versleuteld op te slaan. Als u slechts een enkele schijf in uw systeem heeft is het verstandig om de gebruikersgegevens op een aparte partitie te zetten. Wat u dan met Clonezilla moet back-uppen is kleiner, dus de back-up duurt korter. Met Clonezilla is het ook mogelijk een gecrasht systeem weer te herstellen. Een alternatief is Rescuezilla (zie SoftwareBus 2021-3). Rescuezilla (link 5.) is door zijn grafische interface gebruiksvriendelijker en is compatibel met Clonezilla. Helaas ondersteunt Rescuezilla geen versleuteling. Ik vind dat een back-up moet worden versleuteld. Er staan tenslotte altijd gevoelige gegevens in. Het gebruik van Clonezilla valt buiten het kader van dit artikel.

Herstellen vanuit een back-up

U kunt een back-up volledig terugzetten. Dat is niet altijd handig. Vaak weet u wat u wilt herstellen. Back-in-Time staat u toe de te herstellen map of bestanden te selecteren. U kunt in de gemaakte snapshot de mappen en bestanden zien.

U klikt met de rechter muisknop op de betreffende map of het gewenste bestand en kiest uit de volgende mogelijkheden: *Herstellen, Herstellen naar..., Reservekopieën, Toevoegen om op te nemen, Toevoegen om uit te sluiten en Verborgen bestanden tonen.*

Afbeelding 3: Herstelvenster

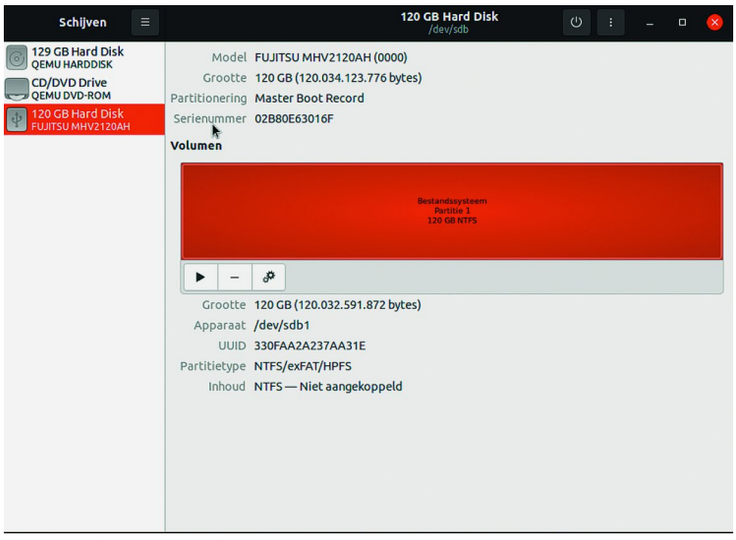
Epiloog

Back-in-Time is eenvoudig in het gebruik, maar biedt ook een aantal extra opties. Als u een back-up van bestanden op een NAS of bestanden naar een NAS wilt back-uppen, moet u er wel wat dieper induiken om problemen te voorkomen. Déjà-Dup is dan handiger. De transparantie van de back-up met de oorspronkelijke bestandsnamen is voor menigeen een belangrijk criterium. Uw back-up neemt wel meer plaats in omdat de bestanden niet worden gecomprimeerd.

Het verdient aanbeveling om af en toe te testen of het lukt om een bestand terug te halen.
Back-in-Time ondersteunt meer back-upscenario's. Dat biedtt de mogelijkheid selecties te maken voor bijvoorbeeld een dagelijkse, een wekelijkse en maandelijkse back-up.

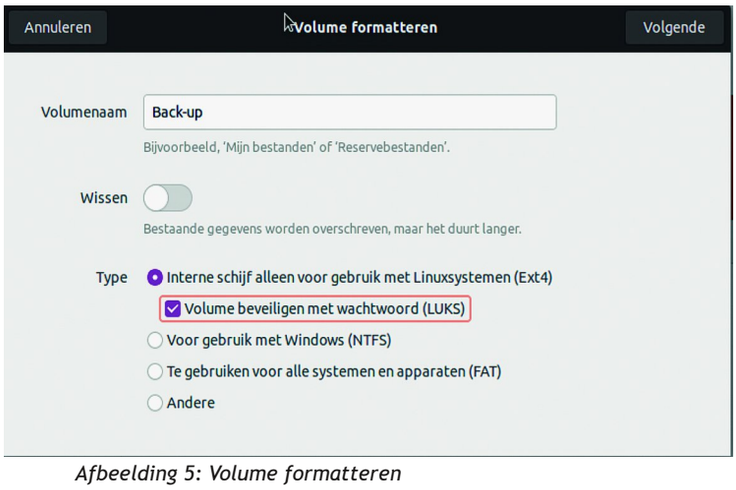
Appendix

Om een schijf te versleutelen gebruikt u het standaard in Ubuntu aanwezige *Gnome schijven*. U sluit de USB-schijf die u wilt versleutelen aan en start *Schijven* op. Selecteer de gewenste schijf.



Afbeelding 4: Gnome Schijven

Klik op de twee tandwieltjes en kies *Partitie formatteren*. Vul een Volumenaam in.
Kies *Interne schijf alleen voor gebruik met Linuxsystemen (Ext4)* en zet een vinkje bij *Volume beveiligen met wachtwoord (LUKS)*. Kies *Volgende*. Vul nu tweemaal het gewenste wachtwoord in. Kies *Volgende* en daarna *Formatteren*.

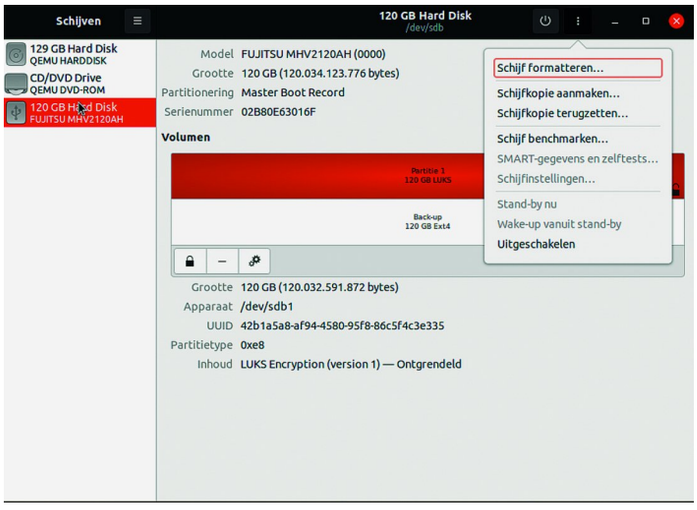


Afbeelding 5: Volume formatteren

Links

1. https://backintime.readthedocs.io/en/latest/
2. https://en.wikipedia.org/wiki/FlyBack
3. https://wiki.ubuntu.com/TimeVault
4. https://clonezilla.org/
5. https://rescuezilla.com/

Als het formatteren is afgelopen kunt u de schijf afkoppelen door te klikken op de drie puntjes en Uitschakelen te kiezen.



Afbeelding 6: Schijf afkoppelen

Verbreek de USB-verbinding en sluit de schijf weer aan. U krijgt nu het volgende venster te zien.

Afbeelding 7: Wachtwoord invoeren

Voer het wachtwoord in en zet een vinkje bij *Wachtwoord onthouden*. Klik op *Ontgrendelen*. U hoeft nu niet meer het wachtwoord in te tikken als u de schijf aansluit op uw systeem.