Back-up met Duplicati 2.0

Uitgebreide back-up-software voor de desktop-basis

Rein de Jong

Back-uppen is de enige manier om je gegevens veilig te stellen bij een calamiteit; of die nu kwam door een eigen stommiteit,door brand of de hele slimme software van een cryptocrimineel die al je bestanden versleutelt.

Voorwaarde is dat je de back-ups niet thuis, maar buitenshuis of ergens veilig op een server in het internet opslaat. Pas dan kun je zeggen: ik heb een back-up! Duplicati is een mooie gratis oplossing om je gegevens via een back-up veilig te stellen.

In 20161 beschreef ik versie 1.3.4 van Duplicati. Ik ontraadde versie 2.0 omdat deze nog in het bètastadium verkeerde. Nu, vijf jaar later, is Duplicati aanbeland bij versie 2.0.5.1 en nog steeds in bèta. Ik heb een natuurlijke afkeer van bèta-software. Toch moet ik me daar in het geval van Duplicati overheen zetten. Want Duplicati 2.x werkt stabiel en is in de praktijk veilig te gebruiken. Waarom dan wél? Vooral omdat een aantal diensten, waaronder Stack, de verouderde, minder veilige TLS-protocollen (1.0 en 1.1) niet meer ondersteunt.

Duplicati 2.0 is volledig opnieuw ontworpen en draait als een server op je machine. De bediening daarvan gebeurt met een modern ogende, overzichtelijke webinterface. Duplicati is nog steeds gratis en veelzijdig wat back-updoelen betreft.

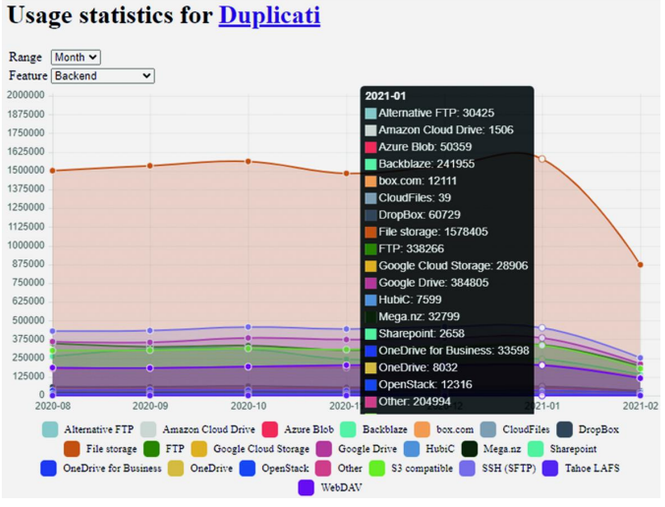
Naast een Windows-versie, die ik hier als uitgangspunt gebruik, zijn er ook versies voor Linux en macOS. Ook biedt het nog steeds veel locaties die versie 1 ook al had, zoals USB-storage (schijf, stick, SSD) en je NAS. Interessanter zijn de Cloud-oplossingen die Duplicati ondersteunt, zoals OneDrive, Google Drive, Dropbox, Jotta, Mega en ownCloud. Dat geldt niet meer voor Amazon Cloud Drive. Daarnaast worden de standaard protocollen: WebDav en (s)FTP ondersteund.

Mocht je ergens op het net opslagruimte hebben, bijvoorbeeld bij je provider of ergens anders gratis of voor weinig geld, dan moet het al gek zijn wil je die niet met Duplicati kunnen gebruiken als back-uplocatie.
Duplicati is veilig! Standaard gebruikt het AES-256[2] voor encryptie en daarnaast kun je GPG[3] gebruiken. Wanneer je daarbij een voldoende lang wachtwoord gebruikt, zijn je gegevens veilig; ook wanneer de back-up in verkeerde handen valt. Ik beschrijf eerst waaraan een back-up moet voldoen en laat dan zien hoe je de installatie en de configuratie bij de eerste start doet. Dit artikel beschrijft de basis: hoe kun je Duplicati snel inzetten om een aanvaardbare back-up te maken. In een ander, uitgebreid artikel, ga ik dieper in op de verdere mogelijkheden van Duplicati.

Vanwege het feit dat de meeste mensen back-uppen naar een NAS of USB-media, leg ik in dit artikel ook uit hoe je de back-up automatisch start wanneer je een USB-storage aansluit op je pc en wat je moet doen om de opslaglocatie op de NAS te beschermen tegen ongewenst overschrijven. Tevens beschrijf ik de back-up naar OneDrive.
In een vervolgartikel beschrijf ik hoe je programmawijde instellingen, zoals de AES-sleutel, templates maken voor de back-up, en e-mail parameters kunt instellen. Daar komt ook aan de orde hoe je beheer op afstand kunt instellen en wat je moet doen om bij een bekende je back-up(s) op te slaan.

Waaraan moet een back-up voldoen?

In het vorige nummer (SWB 2021-1) schreef Ton Valkenburgh in een goed artikel waaraan een back-up moet voldoen. Ik plaats alleen een kanttekening bij zijn aversie tegen de Cloud, met andere woorden: een server op het internet.



De Cloud is, wanneer de data met je eigen wachtwoord versleuteld zijn, de veiligste plek om je back-up op te slaan. Die is namelijk buitenshuis! Hij is, zeker wanneer je back-ups op meerdere plekken opslaat, altijd beschikbaar, en is, afhankelijk van je uploadsnelheid, snel genoeg.
Duplicati maakt in principe maar één keer een volledige back-up naar de server en daarna incrementele back-ups; daarbij worden alleen de gewijzigde bestanden overgebracht naar de Cloud.

Ter illustratie: met mijn 100 Mbps uploadsnelheid duurde een back-up van 840 GB dertig uur. Dat was naar een (s)FTP-server die bij een bekende staat, met ook een 100/100 verbinding. De volgende dag werd 1,5 GB in vijf minuten geback-upt. Voordat je een back-up maakt moet je weten aan welke eisen een back-up moet voldoen om je veilig te weten bij calamiteiten. Ik heb daarvoor vier criteria geformuleerd:

1. Veilig
- Opgeslagen op een veilige plek
- Niet in te zien door onbevoegden
- Altijd beschikbaar voor herstel
- Niet te benaderen vanaf een standaard gebruikers-account

2. Volledig
- Alle unieke gegevens op een systeem
- Meerdere versies van de gegevens
- Opslag op meerdere locaties is sterk aan te bevelen: Cloud/LAN of Cloud/Cloud of Cloud/NAS; vul zelf maar

in.

3. **Eenvoudig**
   - Simpel in gebruik
   - Mappen en bestanden eenvoudig te selecteren
   - Herstellen (Restore) van je data moet gemakkelijk zijn
   - Restoren is mogelijk naar een andere locatie/machine dan die van de oorspronkelijke data.

4. **Fire and Forget (Opstarten en vergeten)**
   - Eenmalig starten en daarna doet het zijn werk
   - Wordt uitgevoerd door een taakplanner (scheduler)
   - Het enige wat je niet moet vergeten is: periodiek een proefrestore te doen. Je zult niet de eerste zijn die bedrogen uitkomt doordat er minder is geback-upt dan verwacht of er verkeerde data zijn veiliggesteld.

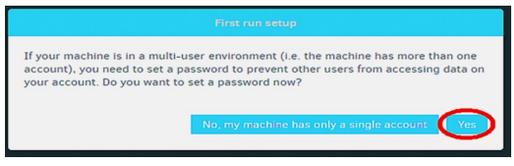
Duplicati voldoet aan alle gestelde eisen. Of de opslag van de back-up veilig en volledig is, is iets waar je zelf voor moet zorgen. Voorbeelden van onveilige opslag zijn:
Back-uppen naar een NAS of USB-apparaat bij je thuis.
Als je Duplicati alleen maar laat back-uppen naar een thuis opgeslagen drager ben je niet veilig voor brand of diefstal. Je kunt dat oplossen door meerdere gegevensdragers te hebben die je laat rouleren en buitenshuis opslaat. Helaas voldoe je daarmee niet aan regel vier die aangeeft dat je, na de eerste start, de back-up kunt vergeten. Het rouleren moet je zelf actief initiëren. Ook ben je niet veilig voor ransomware die sluimert, en eerst al je back-ups versleutelt voordat die zich bekend maakt.

Back-up naar een locatie met je gewone gebruikersaccount.
Als je de back-up uitvoert naar een USB-apparaat, of een andere locatie die je kunt beschrijven vanaf je normale gebruikersaccount, dan vraag je om problemen! Word je besmet met ransomware, dan gaat deze eerst op zoek naar je back-uplocatie en versleutelt daar de back-up.
Dit is op te lossen door een apart back-upaccount aan te maken dat je data kan benaderen en op de back-uplocatie kan schrijven. Zorg ervoor dat je 'normale' account de bestanden op de back-uplocatie alleen maar kan lezen! Dan kan sluimerende ransomware je back-up bestanden niet versleutelen wanneer die onder je eigen account actief is.

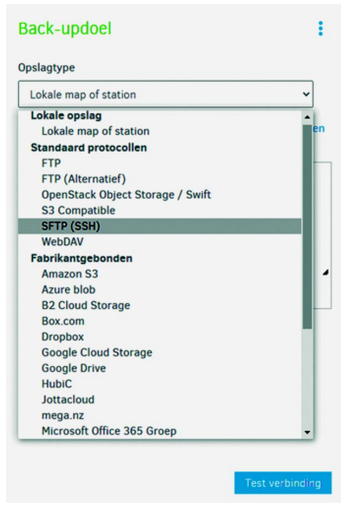
Kopiëren van je gegevens.
Veel pc-gebruikers denken dat een kopie een back-up is. Een kopie voldoet echter niet aan regel twee. Daarin wordt gesteld dat je meerdere versies van een bestand moet hebben, om te voorkomen dat je er vandaag achter komt dat een bestand maanden geleden is verminkt. Heb je dan alleen een wekelijks kopiesysteem op drie USB-apparaten volgens het grootvader, vader, zoonsysteem, dan ben je de pineut!
Een back-up maken met Duplicati is een fluitje van een cent. Met een aantal muisklikken stel je de back-up in en je hoeft je niet meer druk te maken wanneer er een calamiteit plaatsvindt.

Installatie en eerste start

De installatie start door op de site van de makers[4] het installatieprogramma (.msi) op te halen en dat uit te voeren. Wanneer je de aanwijzingen op het scherm volgt, is het 'een eitje'. Duplicati wordt automatisch bij de systeemstart uitgevoerd. Ben je van plan om alleen back-ups te maken naar via USB aangesloten apparaten, schakel dat dan uit. Daarover later meer. Start nu Duplicati via de link op het bureaublad of direct vanuit een browser met de link **http://localhost:8200**. Duplicati vraagt nu of je de pc met meerdere mensen gebruikt. Mijn advies is om altijd 'Ja' te kiezen en in het zich dan openende Instellingenscherm een wachtwoord voor de interface te kiezen. Doe je dat niet, dan kan slimme malware de interface ook openen en je wachtwoorden achterhalen.



Dat wil je niet! Kies je een wachtwoord, plaats dan ook een vinkje bij: **'Voorkomen automatisch inloggen door systeemvak-pictogram'.** De Duplicati server maakt zich namelijk in het systeemvak kenbaar. Word je, net als ik, in het Engels begroet, kies dan **MENU** en blader naar beneden en zet de interface handmatig op Nederlands. Ik vind de vertaling af en toe gebrekkig, maar wel helder in de uitleg. Op de website van Duplicati vind je meer hulp: een collectie artikelen, een handboek en een forum.



Gebruik

Duplicati werkt met een logische volgorde (wizard) om je eerste back-up in te stellen. Bij de eerste start is een *'Nieuwe back-up toevoegen'* al geselecteerd. Zo niet, start dan desgewenst eerst de interface, die je benadert via de link **http://localhost:8200** of zoek Duplicati in het systeemvak. Klik dan op **Menu > Back-up toevoegen.** Kies een logische naam en omschrijf wat de back-up doet. Laat de versleuteling maar op AES-256 staan en maak een voldoende lange wachtwoordzin. Hoe langer de wachtwoordzin, des te meer moeite zal een hacker ondervinden om de sleutel te kraken.

Je kunt het AES-wachtwoord ook laten genereren door Duplicati zelf, maar die wachtwoorden vind ik te kort. Mijn advies is meer dan twintig tekens, waarbij lengte belangrijker is dan tekenset; liever **s2** dan **shift+2** tikken voor het **@**. Heb je moeite om een lang wachtwoord te verzinnen, herhaal dan bijvoorbeeld je wachtwoord een aantal keren. Noteer het wachtwoord, of nog beter, sla het op in een wachtwoordmanager zoals **LastPass** of **1Password**. Ben je het wachtwoord vergeten, dan is de back-up nooit meer herstellen. Wanneer je de back ups op een vertrouwde plek opslaat, zou je kunnen overwegen om geen AES-wachtwoord in te stellen.

Een klik op **[Volgende]** en het Back-updoel wordt gevraagd. Klik op het **afrolpijltje** om uit de lange lijst jouw bestemming te kiezen. Duplicati ondersteunt een veelheid van standaardprotocollen zoals (s)FTP en WebDav; daarnaast ook nog veel bekende online-opslagdiensten. Wij gaan een bestemming in de Cloud kiezen. Ik ga voor **OneDrive**.

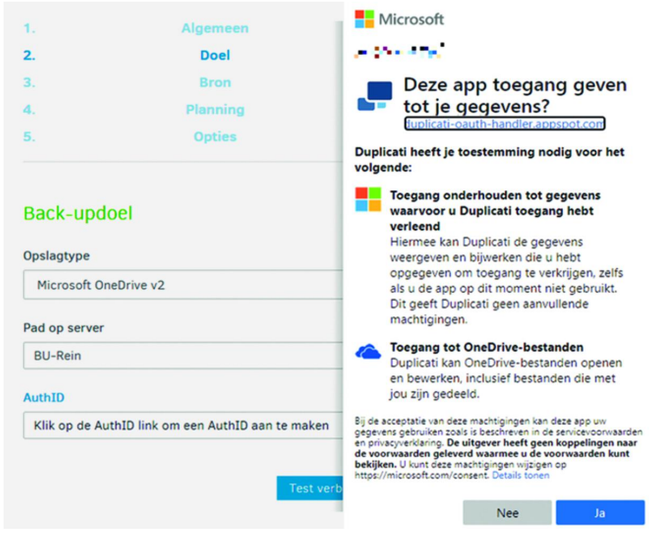
Als je voor € 99,- per jaar een Office 365 family-account aanschaft, heb je de beschikking over maximaal zes accounts met elk 1 TB aan opslag. Voor de back-up gebruik je dan één (of meer) OneDriveaccount(s), enkel en alleen voor de back-up. De andere deel je dan uit onder de familie. Geen enkele aanbieder geeft je zoveel ruimte: 6 TB voor zo weinig geld en dan is het Officepakket er ook nog eens bij inbegrepen.

Will je de back-up op een USB-opslag, dan kies je hier voor Lokale map of station. Je bladert naar de opslaglocatie; dat kan ook een netwerklocatie op je NAS zijn.

NB! Wanneer de back-uplocatie een Stick of USB-schijf is, zorg er dan voor dat deze met NTFS geformatteerd is. Dat is voorwaarde om toegangsrechten in te kunnen stellen.

Nu de keuze voor opslagtype en het **'Pad op de server'**. Bestaat de map niet, dan wordt die aangemaakt. Wil je meerdere back-ups op een locatie opslaan, dan kies je voor elke

back-uptaak een andere map. Klik je op **AuthID**, dan wordt een venster geopend dat je helpt met het vastleggen van de inlog voor OneDrive. Je klikt op de blauwe knop en er wordt naar het Microsoft-account gevraagd. Maak de stappen af en er wordt een ID gegeven waarmee je je back-uplocatie kunt benaderen. Voor Google Drive zijn de stappen soortgelijk.
Test de verbinding! De 'geavanceerde opties' komen in het



vervolgartikel aan de orde.
Het volgende scherm laat je de brongegevens kiezen aan de hand van een boomstructuur. Kies de bestanden en mappen die je wilt veiligstellen. Merk op dat je ook verborgen mappen kunt tonen door het corresponderende vinkje aan te zetten. Je kunt filters definiëren om alleen bepaalde bestandstypen te kiezen.

Uitsluitingen wijst zichzelf, hoewel het wijs is om systeem- en tijdelijke bestanden uit te sluiten. Ook kun je overwegen om heel grote bestanden niet mee te nemen en die apart met een lagere frequentie te back-uppen. Nu verschijnt de dialoog die je een planning laat instellen. Dat heeft alleen zin wanneer de opslaglocatie altijd beschikbaar is. Wanneer je werkt met een roulerend systeem van sticks: vink het uit. Hoe vaak de back-up moet worden uitgevoerd, stel je in bij **'Voer uit iedere'**. Verder wijst het zichzelf. Denk goed na over het interval, belangrijke bestanden misschien om de zoveel uur? En grote bestanden, ISO's, films misschien maar eens per maand?
Vervolgens kom je in het laatste scherm waar nog twee belangrijke opties gekozen kunnen worden:

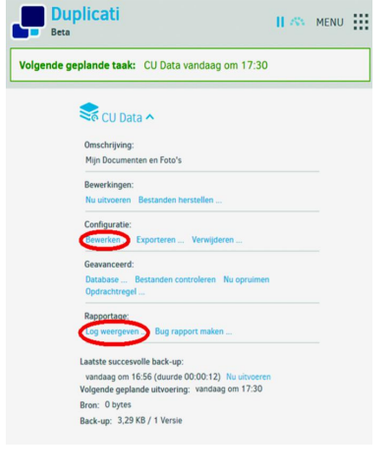
Remotevolumegrootte
Verwar dit niet met de maximumruimte voor back-up op de doellocatie. *Remote volumegrootte* geeft de grootte van de tijdelijke bestanden weer die Duplicati gebruikt om de omvang van de ZIP-containers te bepalen. Duplicati maakt tijdens het back-upproces zo'n container aan met de hier gegeven omvang en vult die met de te back-uppen bestanden. Is het bestand vol, of is de back-up klaar, dan wordt dat bestand desgewenst eerst versleuteld en dan naar de opslaglocatie verplaatst. Anders gezegd: het zijn de blokjes back-up die verzonden worden. De standaardwaarde van 50 MB is prima voor het verzenden van back-ups naar een server op het internet. Dat geeft een betrouwbare back-up; ook wanneer je een trage of slechte internetverbinding hebt. Tevens biedt het voordelen bij herstel. Bij het herstellen van een enkel bestand hoeft er maar een kleine container te worden opgehaald.
Weet je niet wat hierbij wijsheid is? Laat dan gewoon de standaardwaarde van 50 MB staan.

Back-up-retentie
Duplicati kun je instrueren om oudere back-ups automatisch te verwijderen. Je laat dan bestandsversies verwijderen die meer dan x maanden oud zijn. Kies daarvoor een ruime periode. Voor je het weet is net dat ene bestand gewist dat een half jaar geleden nog goed was. Mijn advies is om hier de **Slimme back-up retentie** te kiezen. Dan regelt Duplicati voor je dat je altijd ten minste een jaar terug kunt. Is de opslagruimte groot genoeg? Dan behoud je alle back-ups.

De knop **[Opslaan]** maakt de taak actief en deze zie je terug op de opstartpagina. Zo maak je verschillende back-uptaken aan die automatisch worden uitgevoerd. De web-interface-startpagina laat zien wanneer de eerstvolgende back-up wordt uitgevoerd.

Back-up bewerken

Klik je in het hoofdscherm op een back-uptaak, dan zie je verschillende opties waarvan Bewerken, Uitvoeren en Log weergeven in dit kader de belangrijkste zijn. Over andere opties lees je in het vervolgartikel.



Uitvoeren
Hiervoor hoef je de taak niet uit te klappen. De optie: 'Nu uitvoeren' wordt immers op het overzichtsscherm getoond.

Bewerken
De keuze om te kijken hoe de taak is aangemaakt en om wijzigingen door te voeren. Vergeet niet om bij het wijzigen van een taak door te klikken tot het laatste scherm. Pas dan kun je **[Opslaan]** kiezen. Vergeet je dat, dan moet je opnieuw beginnen!
Log weergeven
Om inzicht te krijgen in de werking van de back-up of wanneer de back-up niet doet wat je wenst en/of er waarschuwingen of fouten worden gemeld, dan krijg je hier de gewenste informatie. Waarschuwingen en fouten worden na het uitvoeren van een taak ook door een gekleurde pop-up getoond.

Herstel

Een back-up maken is één ding; terugzetten wanneer nodig is twee! Het back-uppen zelf is een taak die je volledig kunt automatiseren. Herstellen van bestanden moet je altijd handmatig doen. Ook het regelmatig testen van het herstel is niet iets wat je kunt automatiseren. Je kunt het wel agenderen voor een moment dat bijna altijd wel uitkomt. Zo had ik in mijn werkzame leven altijd de vrijdagmiddag, naast eigen ontwikkeling, voor dit soort routineklussen gereserveerd, die ik dan als eerste deed met de leukere taken in het vooruitzicht. Plan je het zo, dan is er eigenlijk altijd wel gelegenheid. Sla je de back-up op verschillende gegevensdragers op, dan moet je ook zo verstandig zijn die van tijd tot tijd te testen. Zekerheid voor alles!

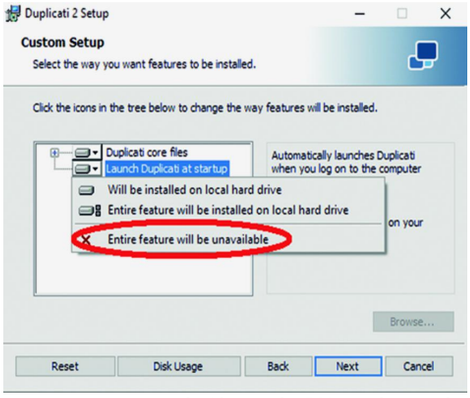
Duplicati controleert zelf de teruggeplaatste bestanden aan de hand van een **hash** (controlegetal). Krijg je geen foutmeldingen op de restore, dan mag je ervan uitgaan dat de bestanden goed zijn.

Hoe dan?

In het taakoverzicht klap je een back-up uit door te klikken op het afrolpijltje achter de taak. Dan kun je op **'Bestanden herstellen …'** klikken. Eerst selecteer je wat je wenst terug te zetten. Dat kan door in de boomstructuur de map of bestanden te selecteren, maar ook door specifiek een bestand te zoeken via het zoekvak. Het volgende scherm laat je kiezen waar je de herstelde bestanden wilt schrijven en toont de herstelopties. Ik kies, ook bij daadwerkelijk herstel, altijd een alternatieve locatie. De afbeelding toont welke opties ik eigenlijk altijd kies. Kies je daar een map die niet bestaat, dan zal Duplicati die aanmaken. Een klik op **[Herstellen]** laat het zijn werk doen. Zonodig, eigenlijk alleen bij herinstallatie, wordt de sleutel van de back-up gevraagd. Naast het herstellen vanuit een taak, kun je ook via het Menu herstellen. Daar zijn twee aanvullende mogelijkheden voor herstel, t.w. **'Rechtstreeks herstellen vanuit back-upbestanden'** en **'Herstel vanuit configuratie'.** Zo kun je back-ups herstellen waarvoor je geen taak hebt; bijvoorbeeld nadat je een systeem opnieuw hebt moeten opbouwen. Ook kun je zo back-ups herstellen die op een andere computer zijn gemaakt.

USB automatisch starten

De webinterface maakt het makkelijk om Duplicati in te stellen. Het back-upprogramma is echter tot veel meer in staat en is tot in detail te configureren. Duplicati is ook volledig te besturen vanaf de commandoregel met de opdracht *Duplicati.CommandLine.exe* die in de installatiemap staat. Start je het zonder parameters, dan krijg je een uitgebreide **help**. Als je alleen maar op een USB-stick of verwisselbare schijf je back-up uitvoert, is het onzinnig om Duplicati met je pc mee te laten starten. Start Duplicati toch automatisch, dan kun je dat uitschakelen met **Win+X > 'Apps en Onderdelen'**, zoek daar Duplicati, klik erop en kies **[Wijzigen],** kies **[Change]** en schakel dan deze functie uit bij *'Launch Duplicati at startup'*. Als je de BU-stick aansluit kun je de taakplanner automatisch een Duplicati-BU-script laten starten. Dat is een samenspel tussen een te maken cmd-file (script) met de opdrachten en een regel in de taakplanner die het aansluiten van de stick herkent.

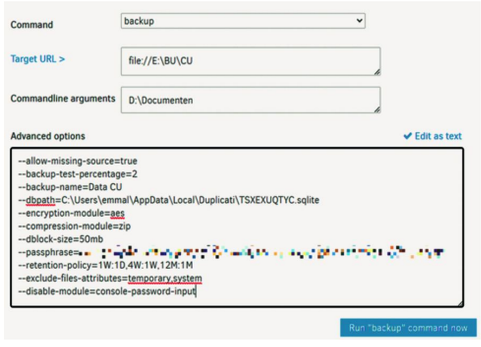


Commandfile maken

Maak eerst de taak die back-upt naar de stick. Deze wordt de basis voor script dat wordt uitgevoerd in de taakplanner. Als de taak klaar is gebruik je die om de instellingen over te brengen naar het script. Open eerst een editor; dat kan Kladblok zijn. Je begint met invoeren van het pad naar de commandlinetool:

```
"C:\Program Files\Duplicati 2\
    Duplicati.CommandLine.exe"
```

Let op de dubbele aanhalingstekens; overal waar spaties in een pad staan moet het volledige pad met dubbele aanhalingstekens worden omsloten. Daarna komt het commando: `backup`, dan het doel: `'Target URL'`, vervolgens de `'Commandline arguments'` en tot slot de `'Advanced options'` (alles scheiden door een spatie). Al deze informatie halen we uit de webinterface (klik op het **afrolpijltje** achter de taak). Klik je daar op **'Opdrachtregel'** dan worden de invulgegevens getoond. Om de Advanced options te zien en te kunnen kopiëren klik je achter de tekst op: **'Edit as tekst'**. Nu heb je alle gegevens om de opdracht samen te stellen. Vergeet niet om alles achter elkaar op één regel te plaatsen (verwijder daarvoor al de regeleinden). Het is immers één enkele opdracht. Doe je dat goed, dan ziet het er uit zoals hieronder.




```
"C:\Program Files\Duplicati 2\
    Duplicati.CommandLine.exe"
backup file://E:\BU\CU "D:\Mijn Documenten"
--backup-name=Data CU
--dbpath=C:\Users\gebruiker\AppData\Local\Duplicati\
  THXEXUQTYC.sqlite
--encryption-module=aes
--compression-module=zip
--dblock-size=50mb
--passphrase=xxxxxxxxxxxxxxxxxxxxxxxxx
--retention-policy=1W:1D,4W:1W,12M:1M
--exclude-files-attributes=system,temporary
--disable-module=console-password-input
```

Sla nu de het script op als *bu-Data_CU.cmd*; of kies zelf een naam. De extensie **.cmd** is verplicht, alles vóór de punt mag je zelf verzinnen. Het is wijs om dat dezelfde naam te geven als de back-up: hier is dat Data_CU.
Het is nu zaak om deze opdracht te testen op goed functioneren. Open daarvoor een Commandprompt en voer daarin de commandfile uit (Kopiëren/Plakken) totdat het functioneert zoals je wenst. Je ziet dat het wachtwoord leesbaar is. Op dezelfde computer is dat niet bezwaarlijk. Daar is immers toch al toegang tot de te back-uppen bestanden.
Sowieso gebruiken we voor back-uptaken een apart wachtwoord dat nergens anders voor wordt gebruikt. Toch? Laat je de laatste parameter weg, dan vraagt Duplicati eerst naar het console-wachtwoord voordat de taak wordt uitgevoerd. Wanneer je het cmd-bestand op het bureaublad plaatst, kun je de back-uptaak starten door er dubbel op te klikken. Dan heb je de webinterface niet meer nodig.

Taakplanner instellen

Het net gemaakte commando voor het instellen van de back-up is een prima basis voor het geautomatiseerd starten van de back-up vanuit de taakplanner. De taakplanner biedt ook de mogelijkheid om de back-up met een apart back-up-account uit te voeren (zie onder 7). Je kunt zo verschillende taken maken zodat het onnodig is om Duplicati bij systeem-

start te laden. Dat belast jouw systeembronnen minder. Tevens kun je back-uptaken maken die starten bij systeemstart, of systeemvergrendeling; maar ook wanneer je een USB-apparaat (Stick/Schijf) aansluit. Dat laatste wordt hier beschreven. Om dit te kunnen verwezenlijken moeten we eerst het apparaatpad van de stick of schijf achterhalen. De taakplanner kunnen we laten reageren op de gebeurtenis dat de betreffende stick wordt aangesloten. Ik schrijf hier over stick, maar je kunt daar ook andere USB-opslagmedia voor lezen zoals: USB-schijf of USB-SSD.

Achterhalen van het apparaatpad
Hiervoor moeten we in de logboeken duiken. Start Logboeken **(WIN+X > Logboeken)**, blader nu naar het Logboek, *'Logboeken Toepassingen en Services > Microsoft > Windows > DriverFrameworks-UserMode > Operational'*. Klik met rechts op **Operational** en dan op **'Logboek inschakelen'**. Nu worden de gebeurtenissen in dat logboek vastgelegd. Sluit vervolgens de stick aan, klik dan met rechts in het midden van het lege venster en klik op vernieuwen of druk op F5. Klik nu op de eerste gebeurtenis, kijk in het detailvenster en kopieer daar de tekenreeks die achter InstanceID staat. In mijn geval ziet dat er zo uit:

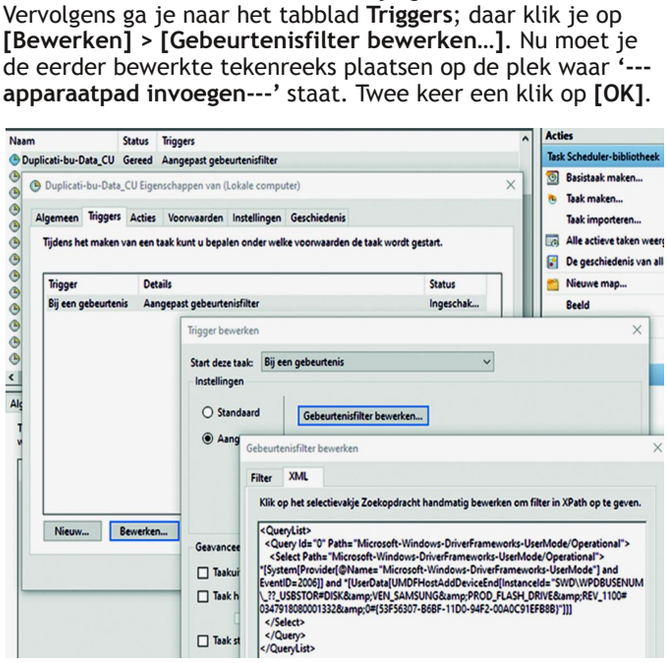
```
SWD\WPDBUSENUM\_??_USBSTOR#DISK&VEN_SAMSUNG&PROD_FLASH_DRIVE&REV_1100#03479180800001332&0#{53F56307-B6BF-11D0-94F2-00A0C91EFB8B}
```

Om deze reeks in de taakplanner te kunnen gebruiken moeten vreemde tekens, zoals de &, nog worden omgezet naar XML-code. Daarvoor gebruik je deze site[5] die dat voor je doet. Dan krijg je dit:

```
SWD\WPDBUSENUM\_??_USBSTOR#DISK&amp;VEN_SAMSUNG&amp;PROD_FLASH_DRIVE&amp;REV_1100#03479180800001332&amp;0#{53F56307-B6BF-11D0-94F2-00A0C91EFB8B}
```

Nu de voorbereidingen zijn gedaan kunnen we de **Taakplanner** starten om de taak te maken. Start de taakplanner door op de **Windows-toets** te drukken en dan *taak* in te tikken of zoek het op in het Startmenu. Om het makkelijker te maken staat er op mijn site een voorbeeld ter download[6] dat je in de taakplanner kunt importeren.

In de taakplanner klik je onder **Acties** op **'Taak importeren'**. Je kiest daar het .XML-bestand dat je gedownload hebt. Vervolgens ga je naar het tabblad **Triggers**; daar klik je op **[Bewerken] > [Gebeurtenisfilter bewerken…]**. Nu moet je de eerder bewerkte tekenreeks plaatsen op de plek waar **'---apparaatpad invoegen---'** staat. Twee keer een klik op **[OK]**.



Selecteer nu het tabblad **Acties**, en kies daar het batchbestand zoals in 6.1 beschreven.
In het ZIP-bestand zit een voorbeeld van het door mij gebruikte cmd-bestand. Dat opent een cmd-venster en toont in eerste instantie alleen de tekst: *'opgestart …'* met een tijdstempel.
Dat is alleen bedoeld om te testen of de taak werkt wanneer je een stick aansluit; pas later haal je dat deel weg en voer je het aangepaste back-upcommando uit. Kijk ook nog even de andere *tabbladen* na of er nog dingen bij staan die je aan zou willen passen. Ben je tevreden klik dan op **[OK]** om de wijzigingen op te slaan.

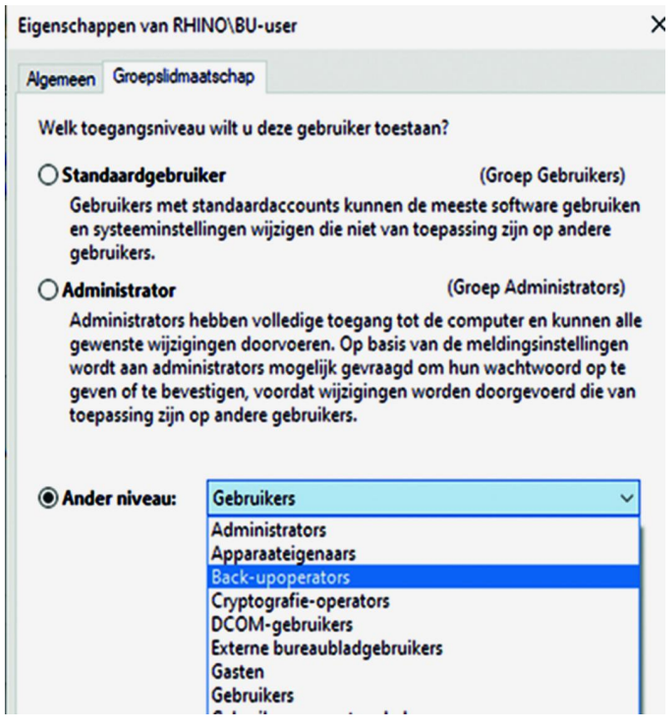
Testen van de taak doe je eerst door de taak in de taakplanner te selecteren en dan op **Uitvoeren** te klikken. Start de batch, dan kun je vervolgens de stick aansluiten en moet het cmd-venster verschijnen.

Om hackers geen kans te geven is het wijs om de stick direct na de back-up te ontkoppelen. Dat kan simpel door een commando in de batchfile op te nemen dat dit voor je doet. Je kunt daarvoor het programma **RemoveDrive**[7] downloaden. Nadat je de stick een naam hebt gegeven, geef je het commando: `RemoveDrive BU-stick -L`. In plaats van *BU-stick* vul je de naam van je eigen apparaat in of de schijfletter die het heeft. Zo is de stick of schijf zo kort mogelijk aangesloten.

Apart back-upaccount

Back-up je met het account waarmee je dagelijks werkt, dan is het voor malware heel eenvoudig de back-up te versleutelen en jou vervolgens te chanteren. Gebruik een apart back-upaccount om dat te voorkomen.

Dat back-upaccount geef je schrijfrechten op de back-uplocatie en je normale account ontneem je schrijfrechten en sta je alleen-lezen toe. Ook ontneem je de groep administrators de schrijfrechten op de back-uplocatie. Alleen het back-upaccount heeft daar de schrijfrechten en is eigenaar van de locatie.



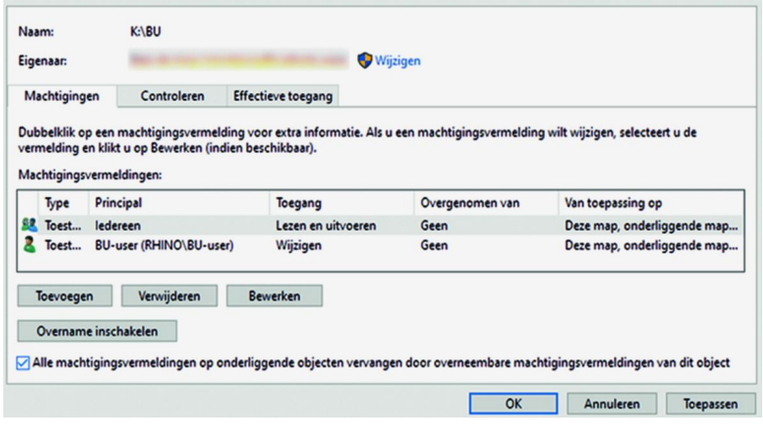
Gebruik back-upaccount
Afhankelijk van de back-uplocatie zijn de instellingen of de manier waarop je met die locatie binnen je normale werkomgeving omgaat verschillend.

Cloud
Synchroniseer je de ruimte in de Cloud met je pc, dan kan malware daar ook bij. Gebruik daarom zo mogelijk een ander account of synchroniseer de data niet met je pc. Een andere mogelijkheid is, de map waarin de back-up wordt opgeslagen uit te sluiten van synchronisatie. Dat maakt de toegang voor malware niet onmogelijk, maar wel een stuk lastiger.
Bij *Stack* kun je meerdere gebruikers aanmaken. Maak voor de back-up een apart account aan en gebruik dat om de back-up met (s)FTP veilig te stellen. Heb je een Office 365-familieaccount, dan gebruik je een of meer van de zes mogelijke gebruikers voor de back-up. Bij alle andere aanbieders moet je apart ruimte kopen.

NAS
Back-up je naar een NAS, dan maak je op de NAS een aparte share (opslaglocatie) en een apart account waarmee je die kunt beschrijven. Afhankelijk van de NAS benader je die via een share of een (s)FTP-verbinding. Verifieer of je met je werkaccount de share wel kunt benaderen, maar niet kunt wijzigen of verwijderen. Staat je NAS, net zoals die van mij, bij een bekende en back-up je daar via (s)FTP, dan is dat nog veiliger. Je hebt dan je eigen privécloud.

USB-stick of -schijf
Voorwaarde is dat je het NTFS-bestandssysteem gebruikt. Daar kun je de rechten zo instellen dat alleen de BU-user daar kan schrijven. De BU-user maak je het makkelijkst aan met WIN+R en de opdracht *Netplwiz* uit te voeren. Maak dan een nieuwe lokale gebruiker die je lid maakt van de groep *gebruikers* (Home) of *Back-upoperators* (Pro).

Stel de rechten voor de back-up-map in. Klik daartoe met **rechts** op de map > **Eigenschappen > Tab: Beveiliging > [Geavanceerd].** In het volgende venster, Kies je **[Overname uitschakelen] > "-> Converteer de overgenomen …"**. Klik nu op **[Toevoegen] > "Principal selecteren"** > Tik daarin de gekozen gebruikersnaam (hier: **BU-user**) > Geef toestemming voor alles, behalve **Volledig beheer** > Klik op [OK].

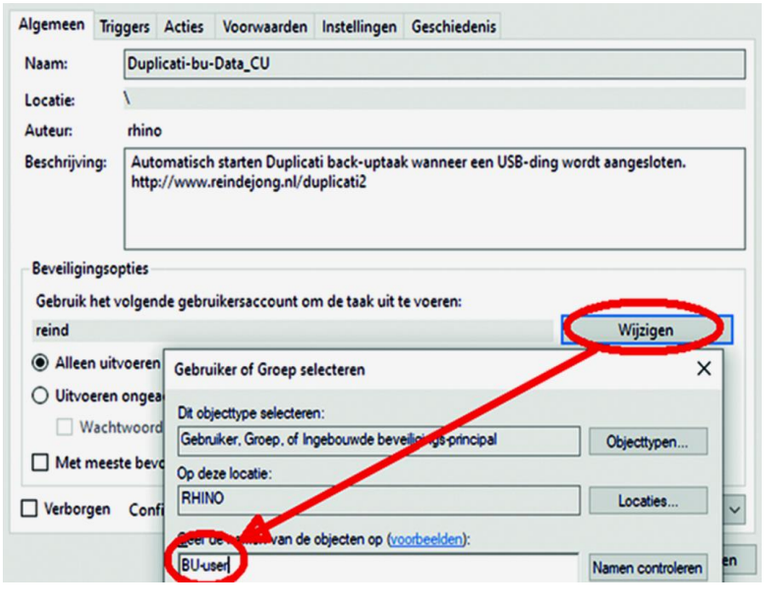


Nu staat er nog dat iedereen *Volledig beheer* heeft. Dat moet worden gewijzigd in *alleen-lezen en uitvoeren*. Plaats vervolgens een vinkje bij **"Alle machtigingsvermeldingen op onderliggende …."** en druk op **[OK].**

Start je de taak met de taakplanner, dan kun je de back-up-taak daarop aanpassen door in het tabblad: **Algemeen**, onder **Beveiligingsopties** het gebruikersaccount waarmee de taak wordt gestart te wijzigen in *BU-user* en het wachtwoord daarvan in te voeren. Voortaan wordt de taak dan gestart met het account dat de back-upmap van de stick of de USB-schijf kan beschrijven.

Tot slot

Duplicati is een erg veelzijdig back-upprogramma dat je gratis en voor niks ter beschikking wordt gesteld.



In een volgend artikel ga ik dieper in op de uitgebreide mogelijkheden van Duplicati.
Voor elke configuratiewijziging in de web-interface geldt dat je niet moet vergeten op de knop **[OK]** of **[Opslaan]** te klikken om deze vast te leggen. Vergeet je dat? Dan kun je weer opnieuw beginnen! Dus als je een back-uptaak bewerkt, dan doorklikken op **[Volgende]** totdat je op de knop **[Opslaan]** kunt klikken!

Zoals altijd, vind je dit artikel op mijn site[8] en ter download als pdf-bestand. Heb je vragen en/of opmerkingen, dan kun je die daar stellen.

Waarschuwing OneDrive
Als je een back-up naar OneDrive uitvoert, kan het zijn dat je, hoewel de back-up goed wordt uitgevoerd, steeds een waarschuwing krijgt dat er iets mis schijnt te zijn: **'—auth password is not supported'**.

Vreemd genoeg is dat nog steeds niet opgelost. De oplossing is lastig te vinden, maar je kunt het oplossen in de webinterface:
1. Bewerk de back-uptaak, de tweede stap: **Doel**
2. Daar zie je het drie-puntjes-menu. Klik daar op > **Kopieer doel naar Klembord**
3. Verwijder daar het deel: &auth-password=xxxxx > Klik op **[Kopie] > [OK]**
4. Druk weer op de drie puntjes > **Importeer Doel URL** > Plak hier het klembord **(Ctrl-V)**.

Links

1. Duplicati 1.3.4	http://bit.ly/r-d134
2. AES	http://bit.ly/r-AES
3. GPG	http://bit.ly/r-gpg
4. Duplicati	http://bit.ly/r-dupl
5. XML Escape	http://bit.ly/r-xmlesc
6. ZIP	http://bit.ly/r-dzip
7. RemoveDrive	http://bit.ly/r-dtw
8. Dit artikel	http://bit.ly/r-d2b
9. Statistieken	http://bit.ly/r-dstats
10. Tutorials Youtube	http://bit.ly/r-dtut