Back-ups, belangrijker dan ooit

In een tijd waarin dossiers almaar meer virtueel worden, alles digitaal wordt en wordt opgeslagen in de cloud, is het goed om enkele elementaire voorzorgsmaatregelen en goede praktijken in herinnering te brengen om uw keuzes inzake uw back-upbeleid op te baseren.

Context

Met het internet en de exponentiële ontwikkeling van de computertechnologie, die steeds krachtiger en goedkoper wordt, heeft het beroep van boekouder(-fiscalist) de voorbije jaren grondige en buitengewoon snelle veranderingen ondergaan.

Voor het voeren van een boekhouding kan men vandaag niet meer zonder een gespecialiseerde toepassing, een boekhoudprogramma, soms gekoppeld aan een CRM (customer relationship management – klantenrelatiebeheer) of zelfs een digitale archiefbeheertoepassing, wanneer deze functies niet als modules voorzien zijn in het boekhoudprogramma.

We zien ook een algemene trend naar outsourcing (cloud computing), voornamelijk ten gevolge van agressieve marketingcampagnes in die richting, maar ook omdat dit de professional ontslaat van onderhoudstaken die door hem vaak als complex worden beschouwd. Maar is dat wel zo? Is de cloud wel het wondermiddel dat men ons voorspiegelt?

Noodzaak en verantwoordelijkheid

Om deze vragen beter te kunnen beantwoorden, moeten we weten wat back-ups precies zijn, waarom ze nodig zijn en waarom men eventueel genoodzaakt kan zijn deze taak uit te besteden aan een dienstverlener (cloud).

De organisatie van een boekhoudkantoor berust bijna volledig op de gegevens in de dossiers. Als deze geautomatiseerd zijn, zoals tegenwoordig de norm is, steunt deze organisatie voortaan dus op het computersysteem, en meer bepaald op massageheugens: harde schijven, SSD's, USB-sticks.

De handeling die met een duur woord back-up wordt genoemd, is in feite niet meer dan *een middel om een reservekopie te maken van de gegevens*, om op het ergste voorbereid te zijn. Gecrashte harde schijf, brand, waterschade, diefstal, hacking of computervirus, we komen hier later op terug.

Hoewel vandaag niemand nog twijfelt aan de dwingende noodzaak om reservekopieën te maken, moeten we er toch op wijzen dat per slot van rekening de boekhouder hier zelf verantwoordelijk voor is. Wanneer u deze taak namelijk uitbesteedt aan een dienstverlener (bv. cloud), wordt niet de verantwoordelijkheid overgedragen, maar alleen de contractuele verplichting voor de dienstverlener om de opslag van de gegevens te verzekeren in het kader van een Service Level Agreement (SLA, of dienstenniveau-overeenkomst - DNO). Zo beperkt de verantwoordelijkheid van de dienstverlener zich strikt tot de bepalingen van de overeenkomst, met eventueel de tussenkomst van een verzekering ten belope van een vast te stellen bedrag. Met andere woorden, voor de dienstverlener bent u een klant zoals een ander, een contractnummer. Als hij zelf getroffen wordt door het noodlot, wat niet onmogelijk is, verre van, moet hij terugvallen op zijn eigen reservekopieën, of in geval van verlies zijn klanten vergoeden. Dit zou u echter niet ontheffen van uw eigen verantwoordelijkheid, en, helaas, niet vrijwaren van de problemen die dit voor u zou kunnen veroorzaken.

Als u er dus voor kiest een beroep te doen op een dienstverlener, dient u deze met zorg te kiezen, na te gaan of hij zelf veiligheidsmaatregelen heeft genomen die aan de strengste normen voldoen, en vooral zeer aandachtig de contractbepalingen te lezen. Net zoals bij een verzekeringscontract, is het vaak pas bij problemen dat men het zich berouwt deze overeenkomst niet te hebben gelezen. Het is niet omdat het zich *in de cloud* bevindt dat het *mistig* moet zijn.

Leg niet al uw eieren in dezelfde mand

De voorbije twintig jaar zijn de prijzen van massageheugens alleen maar gedaald. De prijs per megabyte gegevens is letterlijk ingestort, zodat men vandaag harde schijven met hoge capaciteit vindt tegen zeer betaalbare prijzen, in de orde van enkele tientallen euro. Door de ontwikkeling van NAND-flashgeheugens werd het ook mogelijk USB-sticks en SSD-schijven te ontwikkelen tegen zeer democratische prijzen. Deze zijn licht, schokbestendig en zeer compact. Ook externe harde schijven via USB, hetzij van het type Winchester of SSD, hebben de markt overspoeld.

Om maar te zeggen dat er vandaag nog weinig excuses zijn om géén *extra* reservekopieën te maken. En ja, zelfs als u daarbuiten een beroep doet op een dienstverlener, is het wenselijk dat u uw eigen reservekopieën maakt om aan verschillende noden tegemoet te komen.

Soorten back-up en hun toepassing

Er zijn verschillende types en verschillende niveaus van back-ups, of van bewaring hiervan. Deze beantwoorden aan verschillende noden, zoals:

- **Redundantie**: op een goede server (die in elk boekhoudkantoor aanwezig zou moeten zijn) geeft men de voorkeur aan het gebruik van gespiegelde schijven, in ieder geval voor de schijven die de directory's/eenheden bevatten die op het netwerk gedeeld worden, dit wil zeggen de plaats waar de gegevens worden opgeslagen. Afhankelijk van hun prijs, zijn de servers al dan niet uitgerust met een speciale schijfcontroller of RAID, waarmee de gegevens op een schijf transparant worden gedupliceerd op haar spiegelschijf. In geval van een hardwarefout (gecrashte schijf) moet dus enkel de falende schijf worden vervangen (wat soms zelfs mogelijk is zonder de server uit te schakelen), waarna de controller op de nieuwe schijf onmiddellijk de gegevens herstelt die aanwezig zijn op de andere. Het doel hiervan is de continuïteit van de dienstverlening te garanderen.
- **Extra-muros**: dit is eerder een modaliteit dan echt een type. Nadat een back-upset is gecreëerd, komt het erop aan ervoor te zorgen dat deze op een veilige plaats wordt bewaard, buiten de muren, zodat hij niet kan worden getroffen door de gevolgen van een ramp (brand, inbraak, overstroming...). Dit kan ook gebeuren door de kopie tussen twee geheugenplaatsen rechtstreeks via een VPN-netwerk (Virtual Private Network) te maken. De installatie van een VPN-netwerk is niet duur, maar het is niet eenvoudig en vereist waarschijnlijk de hulp van een informaticus.
- **Back-up van de vorige dag**: dit kan belachelijk lijken, maar meestal is het zo dat wanneer u een bestand verliest, u het de vorige dag nog had. Naast een andere back-up, is een *incrementele* kopie van de vorige dag dus niet onzinnig. Dit kan de vorm aannemen van een gewone kopie, maar het is natuurlijk makkelijker hiervoor een klein script te creëren of een klein specifiek programma te gebruiken. Met incrementeel wordt bedoeld dat de bestanden erin worden gekopieerd die er nog in stonden, of dat oudere versies worden vervangen door de nieuwe.
- **Historisatie**: met historisatie bedoelen we een onafhankelijke en volledige kopie van een bestand of een aantal bestanden met de datum van vandaag. Dit betekent dat er *elke dag* een aparte back-upset van deze gegevens wordt gecreëerd en opgeslagen. Dit zal over het

algemeen worden toegepast op groepen bestanden van redelijke omvang, en worden beperkt tot bestanden van vitaal belang, zoals de boekhouding zelf. Het lijkt immers niet verstandig en zelfs niet haalbaar om een historisatie te doen van alle gegevens (gedematerialiseerd archief bijvoorbeeld). We merken terloops op dat in de overgrote meerderheid van de gevallen de door de dienstverleners geleverde back-ups incrementeel zijn en niet gehistoriseerd, wat veel te grote opslagvolumes zou vereisen.

- **NAS**: acroniem van Network Access Storage, of via netwerk toegankelijke opslag. Dit is geen type back-up, maar eerder een type van dragers die steeds vaker worden toegepast en die zeer betaalbaar zijn. In de praktijk zijn het heuse kleine netwerkservers (LAN) die overal toegankelijk zijn vanuit het lokale netwerk en die zelfs als VPN kunnen worden gebruikt om grote hoeveelheden data op gespiegelde schijven op te slaan. Ze zijn klein, verbruiken weinig en zijn geschikt voor minimaal twee (apart gekochte) harde schijven. Na een eenvoudige configuratie via een gebruiksvriendelijke interface, kunt u er uw reservekopieën opslaan of alles wat u er maar op wilt zetten. Een dergelijk gebruiksklaar systeem kost vandaag minder dan 500 euro.

Volledig automatisch!

Jazeker, met uitzondering van de laatste fase, die erin bestaat regelmatig te controleren of uw back-ups correct zijn uitgevoerd en of de gegevens wel degelijk aanwezig zijn! Het is gemakkelijk, een programma dat de back-ups in uw plaats doet en u elke ochtend een gedetailleerd rapport van vijftig pagina's stuurt. Het probleem is dat u het wellicht na een week al niet meer leest. De dag dat het rapport foutmeldingen bevat die aangeven dat de back-up niet correct kon worden uitgevoerd, zult u het niet zien.

U zou er omgekeerd voor kunnen kiezen alleen rapporten te ontvangen als er een probleem werd vastgesteld, maar dat is nog niet zo simpel. Voor de software is het feit dat een bestand niet kon worden geopend, bijvoorbeeld omdat het vergrendeld was door een andere post, een fout waarvoor een rapport wordt gegenereerd. Wat wij hier willen zeggen, is dat het niet volstaat een back-upbeleid te hebben, maar dat men regelmatig moet controleren of het nog actueel is en of de reservekopieën goed verlopen. Een verandering van server, toevoeging van gebruikers, van gedeelde directory's, verandering van systeemwachtwoord zijn stuk voor stuk factoren die vaak gevolgen hebben op dit vlak.

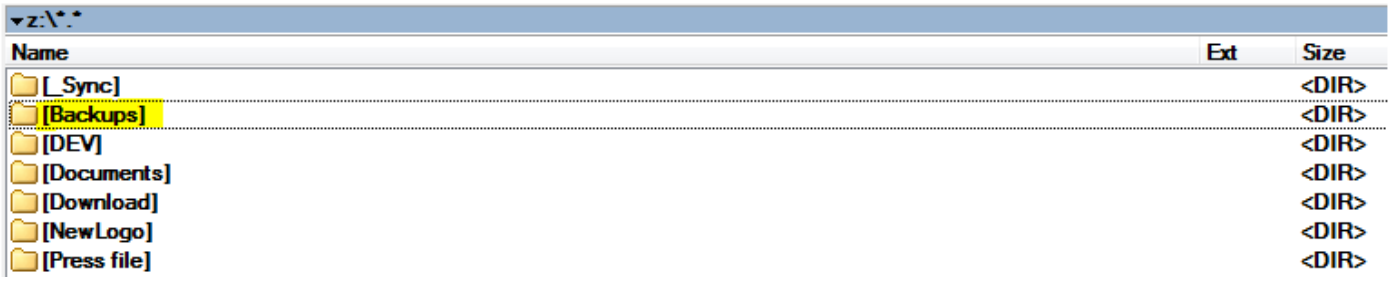
Er bestaan goede gratis programma's

Het is niet altijd nodig zich blauw te betalen aan software om professionele back-ups te maken. Er bestaan een aantal programma's die de hele reeks van handelingen voor hun rekening nemen, en die toch gratis, licht en gebruiksvriendelijk zijn. Onze favorieten (voor windows) zijn SyncBack en Cobian. Zij maken het mogelijk een aantal kopieer- of synchronisatietaken planmatig uit te voeren, met of zonder compressie, en wat Cobian betreft met of zonder versleuteling van de doelbestanden indien u deze op een server wenst op te slaan of als de vertrouwelijkheid niet gewaarborgd is (Google Drive, ...). Beide kunnen rechtstreeks vanuit de opdrachtregel worden aangeroepen, waardoor ze kunnen worden opgenomen in scripts met een ruimer opzet (allerhande onderhoudsdoeleinden). Deze programma's beheren alle aspecten van een back-up: uitvoering van andere taken ervoor/erna, planning, kopiëren/synchroniseren en kennisgeving via e-mail.

Een concreet voorbeeld (met SyncBack)

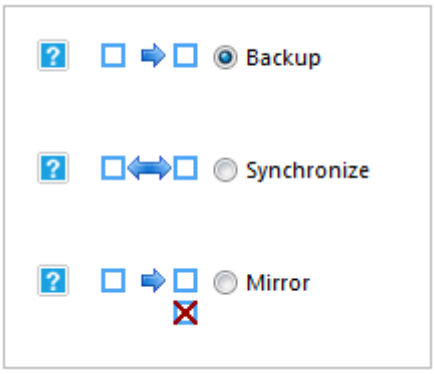
Nadat we het programma hebben gedownload en geïnstalleerd, willen wij een reservekopie maken van onze directory G:\Documenten naar onze NAS, die de naam COMMON heeft en de letter Z:\ draagt

Eerst maken we op onze NAS een directory Back-ups aan, waar onze reservekopie zal worden opgeslagen:



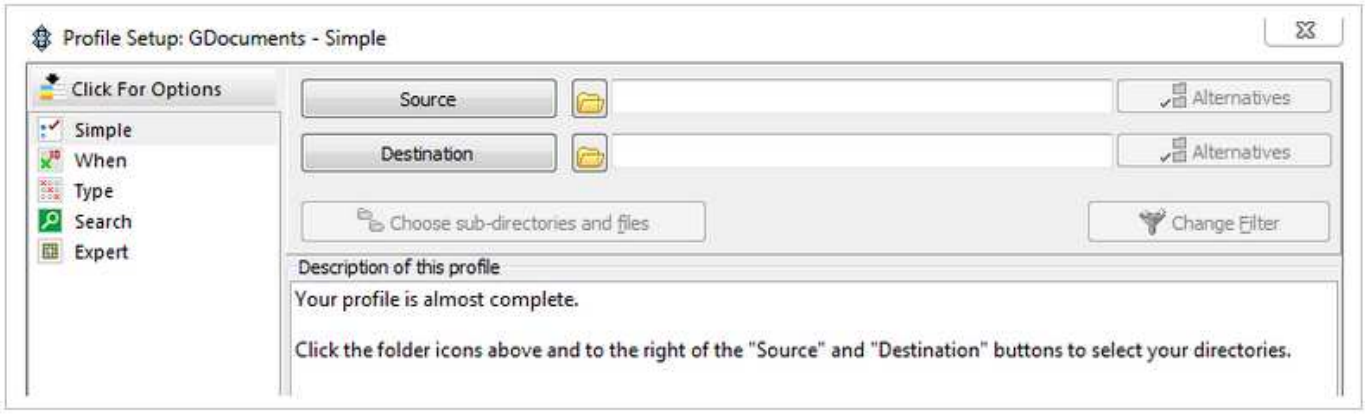
Vervolgens starten we SyncBack en gaan we naar Profiles > New om een nieuwe taak aan te maken, die we een naam geven (GDocuments). Merk op dat het via het menu Preferences > Language mogelijk is het programma weer te geven in het Nederlands. Persoonlijk gebruiken wij deze mogelijkheid zelden omdat de vertalingen soms onbetrouwbaar of verwarrend zijn.

Vervolgens kiezen we het gewenste soort taak (back-up)

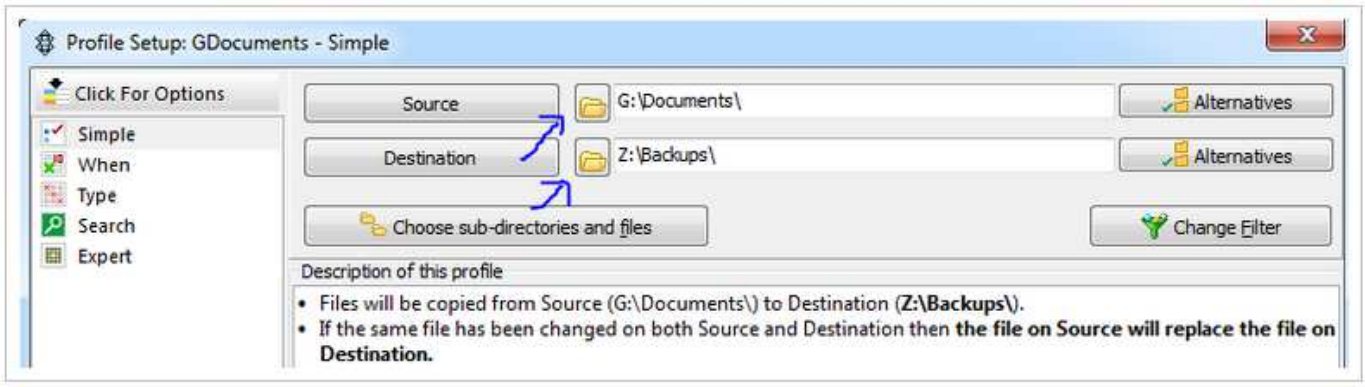


Het programma vraagt ons dan of het om een kopie via de schijven of via het netwerk gaat (FTP = File Transfer Protocol, te mijden als de bestanden niet versleuteld zijn).

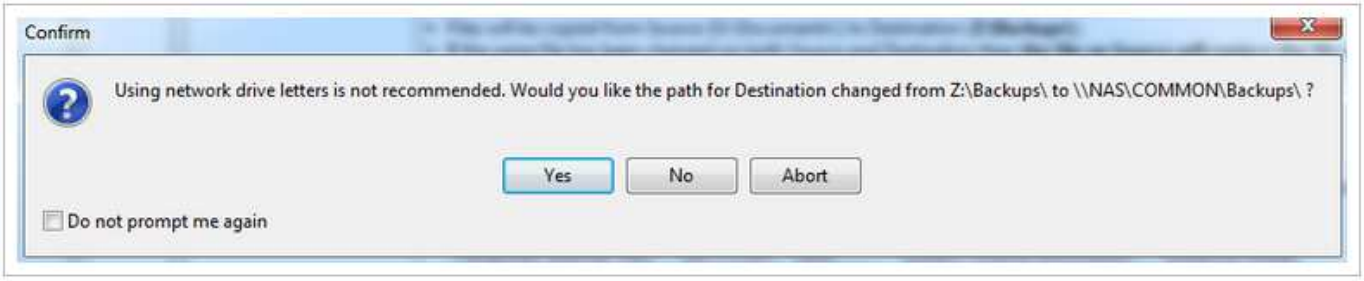
Daarna opent het programma het betreffende profiel zodat we de modaliteiten kunnen specificeren.



Vervolgens geven wij de bron en het doel op:

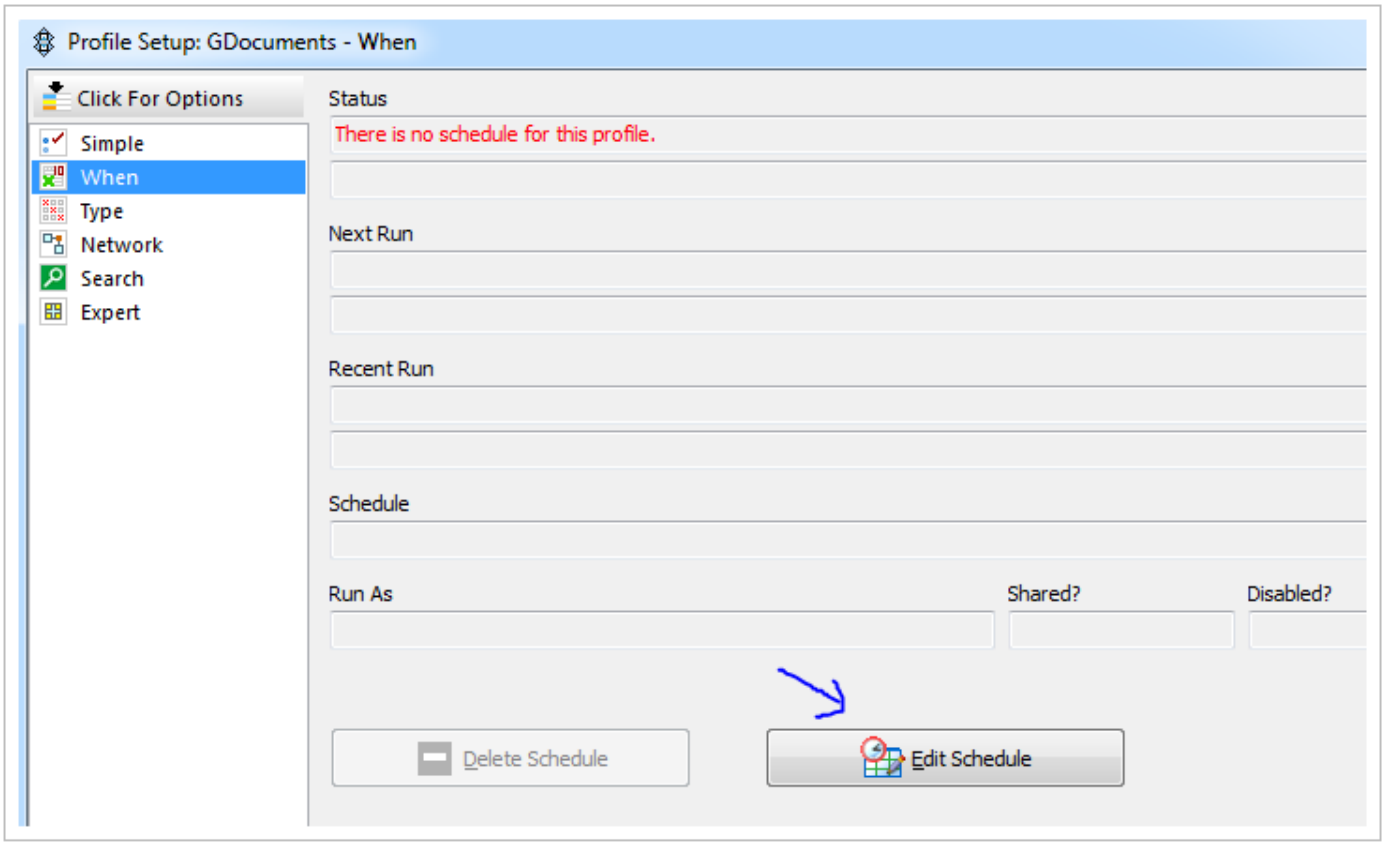


Het programma detecteert dan dat ons doel in feite een netwerkschijf is, en stelt dus voor het windowspad om te zetten in een compleet netwerkpad (UNC).

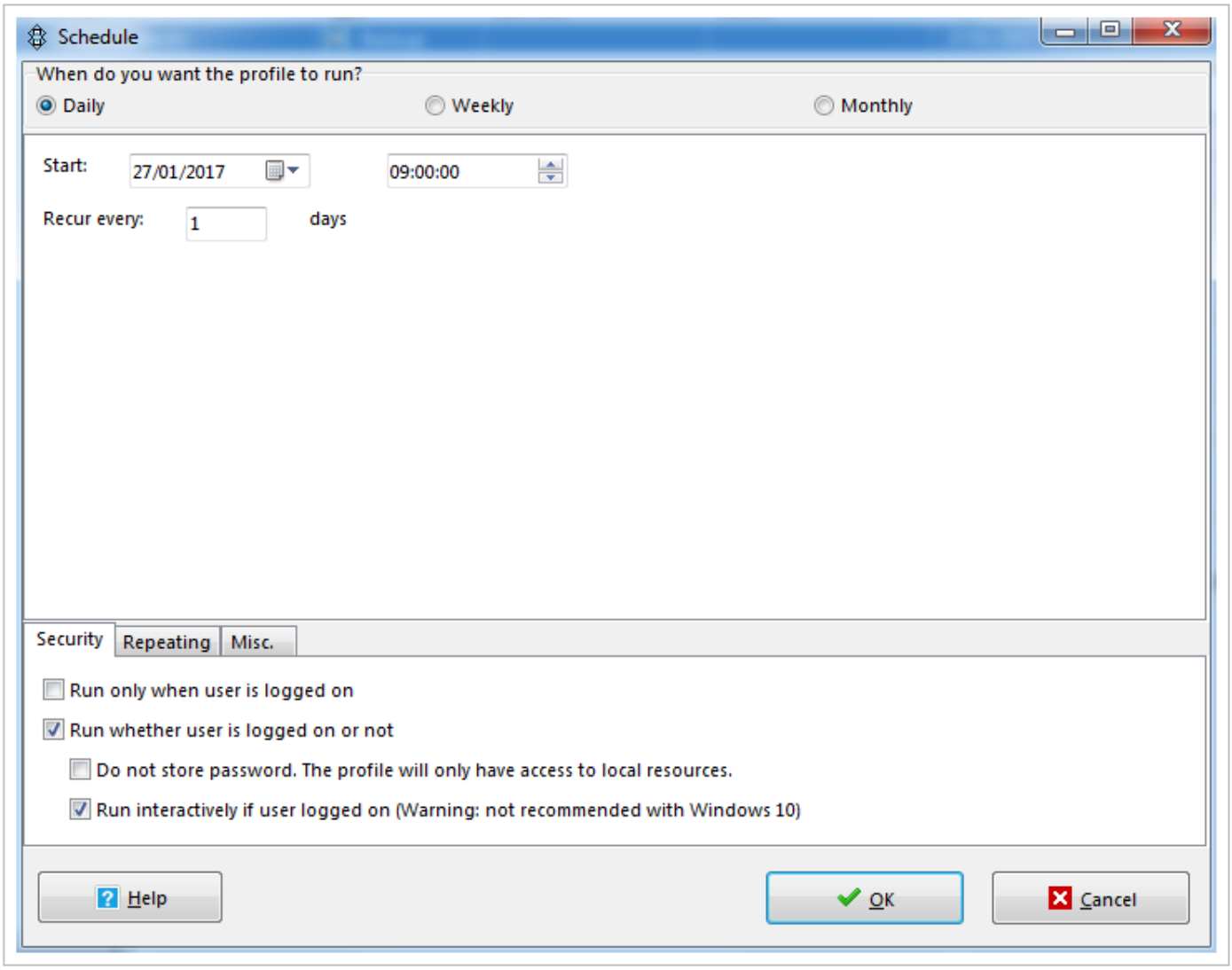


Daarna stelt het programma een simulatie voor om na te gaan of alle bestanden toegankelijk zijn (optioneel).

Door daarna te dubbelklikken op het profiel, kunnen we dit bewerken. Door (in de linker kolom) op "When" te klikken, kunnen we een schedule aanmaken, d.w.z. een planning voor deze taak:

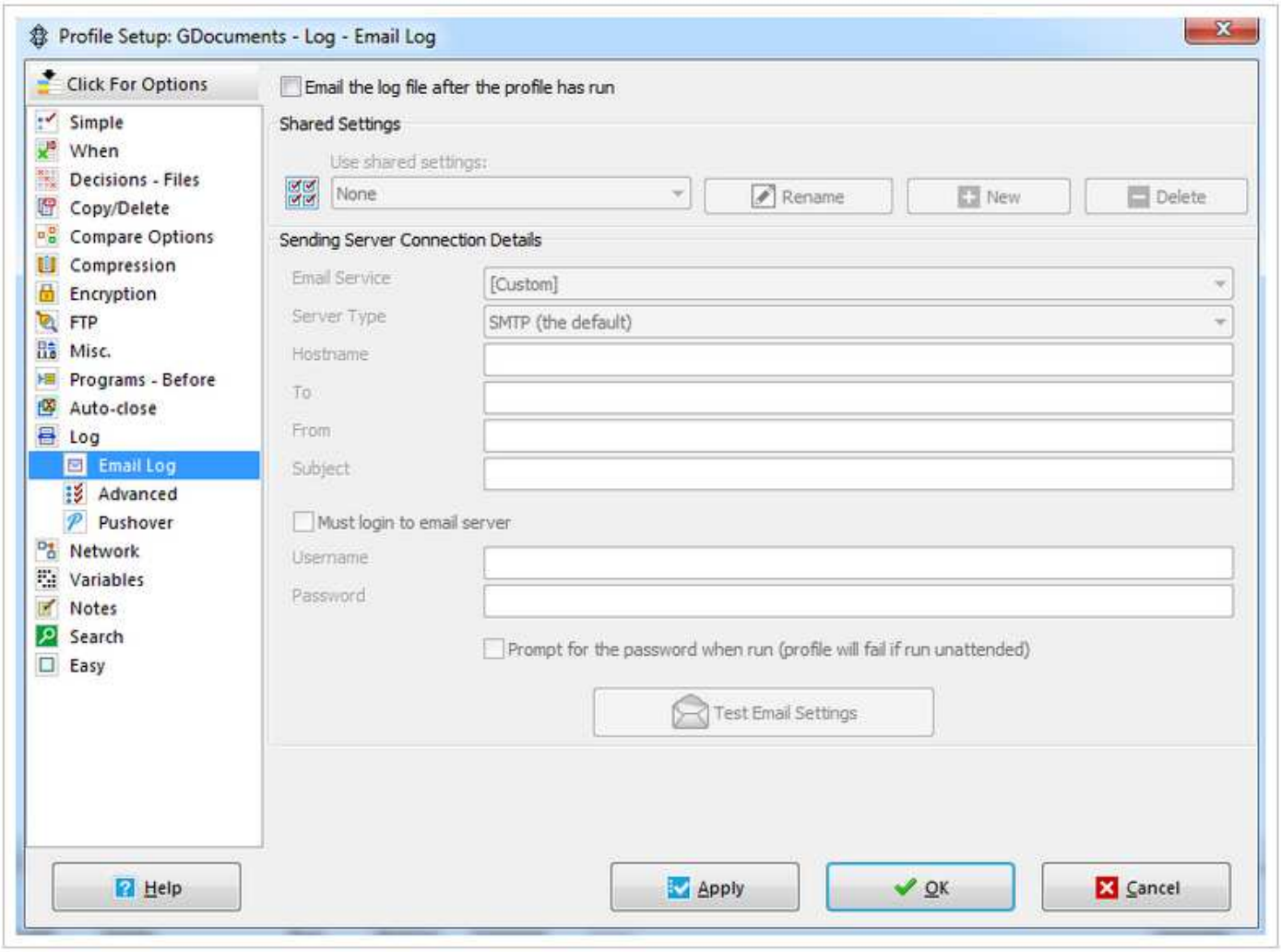

Profile Setup: GDocuments - When
Click For Options
Simple
When
Type
Network
Search
Expert
Status
There is no schedule for this profile.
Next Run
Recent Run
Schedule
Run As
Shared?
Disabled?
Delete Schedule
Edit Schedule

U moet dan het wachtwoord ingeven waarmee u toegang hebt tot de computer en vervolgens de planningsgegevens invoeren:



daarna OK en klaar!

Als u bijvoorbeeld de logs, dus de historische overzichten (die aangeven of alles al dan niet goed is verlopen) wenst te ontvangen via e-mail, moet u in de linker kolom op Expert > Log > Email Log klikken,



waarin u dan de te gebruiken account dient op te geven. Als u uw eigen e-mailserver hebt, kunt u het adres daarvan opgeven of een account van uw provider (Skynet, enz.) gebruiken door de instellingen in te voeren, net zoals bij het configureren van een e-mail client, behalve dat hier alleen de uitgaande server (SMTP) wordt opgegeven.

In expertmodus kan de software een enorm aantal verschillende taken uitvoeren, zoals historisatie, encryptie en compressie. Dit is handig om directory's te synchroniseren (let echter op voor het wissen van brondirectory's!), om eenvoudige kopieën te maken of om in één keer een aantal taken uit te voeren (groep van profielen die bij aanmaak kunnen worden gekozen).

Dit zijn maar enkele tools die al gauw onmisbaar kunnen worden.

Tot besluit

U hebt ongetwijfeld begrepen dat het opzet van dit artikel vooral was u erop te wijzen dat men nooit *te veel* back-ups heeft, net zoals men nooit *te* gezond kan zijn. In het licht van wat het kost, moet men wel erg onbekommerd of erg zelfverzekerd zijn om na te laten ook zelf back-ups te maken.

Gezien de opflakkering van ransomware, virussen die alle bestanden van een computer of een netwerk versleutelen en daarna een online betaling eisen om de decryptiesleutel te ontvangen, kunnen we u alleen maar aansporen om verschillende back-ups toe te passen en regelmatig de integriteit van uw bestanden te controleren (op een andere computer bijvoorbeeld). Daarnaast adviseren wij natuurlijk op elke computer van het kantoor een antiviruspakket dat up-to-date is. Denk eraan dat in 95% van de gevallen virussen *door de gebruikers* zelf worden geïnstalleerd nadat ze ermee hebben ingestemd om ze te installeren (hoewel het virus zich als iets heel anders voordoet). Het is dus verstandig altijd twee keer na te denken voor u een programma installeert. En misschien is het nuttig het te controleren met de antiviruswebsite VirusTotal, die het scant met een vijftigtal verschillende antivirusscanners en u zal zeggen of het programma betrouwbaar is. Dit is niet onfeilbaar, maar veel beter dan niets.

Philippe Huysmans
IT-verantwoordelijke BIBF