Plus importants que jamais, les Backups

A une époque qui pousse tant et plus à la dématérialisation des dossiers, du tout informatique et du stockage dans le cloud, il est bon de rappeler quelques précautions élémentaires et bonnes pratiques qui devraient guider vos choix en matière de politique de backups.

Contexte

Avec internet et le développement exponentiel de la technologie informatique, toujours plus performante et toujours moins chère, la profession de comptable (-fiscaliste) a subi ces dernières années des mutations profondes et extrêmement rapides.

Aujourd'hui, la tenue d'une comptabilité passe forcément par l'utilisation d'une application métier, un logiciel de comptabilité, auquel on adjoint parfois un GRC (gestion de relations clients), voire une application de gestion des archives au format numérique, quand ces fonctions ne sont pas prévues sous forme de modules dans le programme de comptabilité.

On observe aussi une tendance généralisée à l'externalisation (cloud computing), en raison principalement de campagnes agressives de marketing en ce sens, et parce que cela décharge le professionnel de tâches de maintenance qui parfois sont perçues par ce dernier comme complexes. Mais est-ce bien le cas ? Et le cloud est-il bien la panacée qu'on nous vante ?

Nécessité & Responsabilité

Afin de mieux répondre à ces questions, il convient de savoir ce que sont précisément les backups, pourquoi ils sont nécessaires, et pourquoi, le cas échéant, on peut être amené à déléguer cette tâche à un prestataire de service (cloud).

L'organisation d'un bureau comptable repose presque entièrement sur les données contenues dans les dossiers. Si ceux-ci sont informatisés, ce qui est la norme aujourd'hui, alors cette organisation repose désormais sur le système informatique, et plus précisément sur ses mémoires de masses : disques durs, SSD, clés USB.

L'opération appelée pompeusement backup consiste simplement en *tout moyen permettant de créer un jeu de données de sauvegarde*, afin de parer à toute éventualité. Crash disque, incendie, dégâts des eaux, vol, piratage ou virus informatique, nous y reviendrons.

Si plus personne aujourd'hui ne doute de l'impérieuse nécessité de réaliser des copies de sauvegarde, il convient en revanche de rappeler aussi qu'en fin de compte, la responsabilité en incombe au comptable lui-même. En effet, lorsque vous déléguez cette tâche à un prestataire de service (p. ex. cloud), ce n'est pas la responsabilité qui est transférée, mais seulement l'obligation contractuelle pour le prestataire d'assurer la sauvegarde des données dans le cadre d'un Accord sur les Niveaux de Service (ANS, en anglais SLA). Ainsi, la responsabilité du prestataire se limite strictement aux termes de l'accord, avec éventuellement l'intervention d'une assurance à concurrence d'un montant à fixer. En d'autres termes, pour le prestataire, vous êtes un client comme un autre, un numéro de contrat. S'il lui arrive un sinistre, ce qui n'est pas impossible, loin s'en faut, il devra s'en remettre à ses propres copies de sauvegarde, voire dédommager ses clients en cas de perte. Ce qui n'aurait pas pour effet de vous dégager de votre propre responsabilité, et, disons-le, de l'embarras que ceci pourrait vous causer.

Ainsi, il y a lieu, si vous choisissez de faire appel à un prestataire de service, de le choisir avec soin, de vous assurer qu'il a mis lui-même en place des politiques de sécurité rencontrant les meilleurs standards, et surtout, de lire très attentivement les clauses du contrat. Tout comme un contrat d'assurance, c'est en cas de problème qu'on risque fortement de regretter de ne pas l'avoir lu. Ce n'est pas parce que c'est *dans le cloud* que ça doit être *nébuleux*.

Ne pas mettre tous les œufs dans le même panier

Au cours des vingt dernières années, le prix des mémoires de masse n'a fait que baisser. Le prix au mégabyte de données s'est littéralement effondré, au point qu'on trouve des disques durs de haute capacité à des prix très abordables aujourd'hui, de l'ordre de quelques dizaines d'Euros. Le développement des mémoires flash de type NAND a également permis le développement des clés USB et des disques SSD à des prix très démocratiques. Légers, résistants aux chocs, et d'encombrement très faible. Les disques durs externes en USB, qu'ils soient de type Winchester ou SSD ont également inondé le marché.

C'est dire qu'il y a peu d'excuses aujourd'hui à invoquer pour justifier l'absence de copies de sauvegarde *supplémentaires*. Eh oui, il est souhaitable, même si par ailleurs vous faites appel à un prestataire de service, de réaliser aussi vos propres copies de sauvegarde, afin de répondre à différents besoins.

Types de backup et leur application

Il existe différents types et différents niveaux de backups, ou de conservation de ceux-ci, qui répondent à des besoins différents, on peut citer :

- **La redondance** : sur un bon serveur (qui devrait équiper tout bureau comptable), on privilégiera l'utilisation de disques en miroir, en tout cas pour les disques contenant les répertoires/unités partagées sur le réseau, c'est-à-dire l'endroit où seront stockées les données. Les serveurs, suivant leur prix, sont équipés ou non d'un contrôleur disque spécial appelé RAID permettant la duplication transparente des données d'un disque sur son miroir. Ainsi, en cas de panne matérielle (crash disque), il n'y a qu'à remplacer le disque défaillant (parfois possible sans même éteindre le serveur) pour qu'aussitôt, le contrôleur reconstitue sur le nouveau disque les données présente sur l'autre. Le but étant ici d'assurer la continuité du service.
- **Extra-muros** : il s'agit ici d'une modalité plutôt que d'un type à proprement parler. Il s'agira, après avoir créé un jeu de sauvegarde, de s'assurer qu'il soit conservé en lieu sûr, hors les murs, afin qu'il ne puisse être affecté par les conséquences d'un même sinistre (incendie, cambriolage, inondation...). Ceci peut également être fait en réalisant la copie entre deux implantations directement à travers un réseau VPN (Virtual Private Network). L'installation d'un réseau VPN n'est pas coûteuse, mais elle n'est pas triviale et nécessitera probablement l'intervention d'un informaticien.
- **Backup de la veille** : cela peut avoir l'air dérisoire, mais le plus souvent, lorsque vous perdez un fichier, vous l'aviez encore la veille. Ainsi, à côté de tout autre backup, avoir une copie *incrémentale* de la veille n'est pas inutile. Cela peut prendre la forme d'une simple copie, mais il est évidemment plus simple de créer un petit script pour l'occasion ou d'utiliser un petit logiciel ad-hoc. Par incrémentale, il faut comprendre qu'on y copie les fichiers ne s'y trouvant pas déjà, ou remplaçant des versions plus anciennes par la nouvelle.
- **Historisation** : par historisation, nous entendons une copie indépendante et complète d'un fichier ou d'un ensemble de fichiers correspondant à la date du jour. Cela revient à créer un jeu de sauvegarde distinct de ces données *chaque jour*, et de les conserver. Cela s'appliquera généralement à des ensembles de fichiers de taille raisonnable en se limitant aux fichiers

d'intérêt vital, comme par exemple la comptabilité elle-même. A contrario, il ne paraît ni raisonnable ni même abordable de réaliser une historisation de l'ensemble des données (archives dématérialisées par exemple). Notez au passage que dans l'immense majorité des cas, les backups fournis par les prestataires de service sont de type incrémentaux, et non historisés, ce qui nécessiterait des volumes de stockage bien trop considérables.

- **NAS** : acronyme de Network Access Storage, ou disque accessible en réseau. Il ne s'agit pas d'un type de backup, mais plutôt d'un type de supports de plus en plus répandus et dont le coût est très abordable. En pratique, ce sont de véritables petits serveurs de réseau (LAN), accessible partout depuis le réseau local, et pouvant même être utilisés en VPN permettant de stocker de grandes quantités de données sur des disques en miroir. De petite taille, de faible consommation, ils permettent d'accueillir au moins deux disques durs (achetés séparément), et, après une simple configuration via une interface conviviale, de stocker vos copies de sauvegarde, ou tout ce que vous souhaiteriez y mettre. De tels dispositifs prêts à l'emploi coûtent moins de 500 EUR aujourd'hui.

Entièrement automatique, on vous dit !

Oui, sauf pour la dernière étape, qui consiste à vérifier régulièrement que vos backups ont été effectués correctement et que les données s'y trouvent bien ! C'est très joli d'avoir un programme qui fait les backups pour vous et qui tous les matins vous envoie un rapport de cinquante pages pour en détailler les opérations. Le problème, c'est qu'après une semaine, vous ne le lirez probablement même plus. Et vous ne verrez rien, le jour où le rapport contiendra des messages d'erreur signalant que le backup n'a pas pu être effectué correctement.

A l'inverse, on pourrait choisir de ne recevoir les rapports que lorsqu'un problème a été rencontré, mais là encore, ce n'est pas aussi simple. Pour le logiciel, le fait qu'il n'ait pas pu ouvrir un fichier, par exemple parce qu'il était verrouillé par un autre poste constitue une erreur de nature à générer tout un rapport. Ce que nous voulons dire ici, c'est qu'il ne suffit pas d'avoir une politique de backup, encore faut-il régulièrement s'assurer qu'elle reste d'actualité, et que les copies de sauvegarde se passent bien. Changement de serveur, ajout d'utilisateurs, de répertoires partagés, changements de mots de passe système sont autant d'événements qui ont souvent des conséquences de ce point de vue.

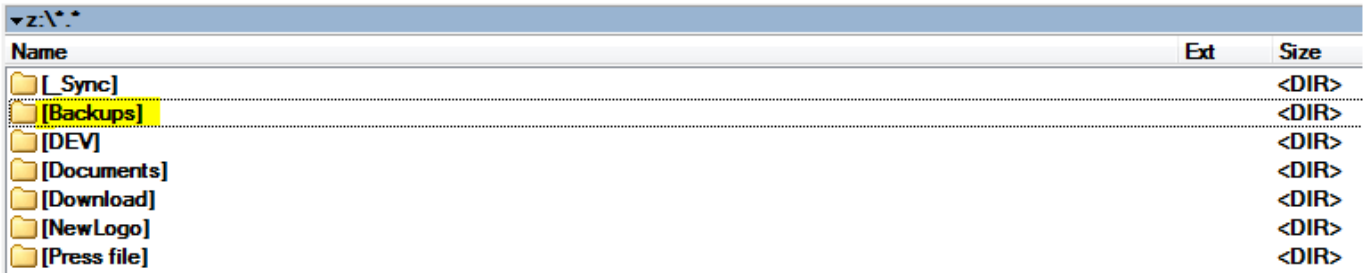
Des logiciels gratuits et performants existent

Il n'est pas toujours nécessaire de se ruiner en frais de logiciels pour réaliser des copies de sauvegarde professionnelles. Un certain nombre de programmes existent, permettant de réaliser la chaîne complète des opérations, tout en restant gratuits, légers, et simples d'utilisation. Parmi eux, nous citerons nos préférés (sous windows) qui sont SyncBack et Cobian. Ils permettent de réaliser de manière planifiée un ensemble de tâches de copies ou de synchronisation de répertoires, avec ou sans compression, et pour Cobian, avec ou sans encryption des fichiers de destination au cas où vous souhaiteriez les stocker sur un serveur ou la confidentialité n'est pas garantie (Google Drive, etc.). Ils permettent l'un comme l'autre d'être appelés directement à partir de la ligne de commande, ce qui permet de les inclure dans des scripts à vocation plus large (maintenances diverses). Ces programmes gèrent tous les aspects d'un backup : exécution d'autres tâches avant/après, planification, copie/synchronisation et notification par email.

Un exemple concret (avec SyncBack)

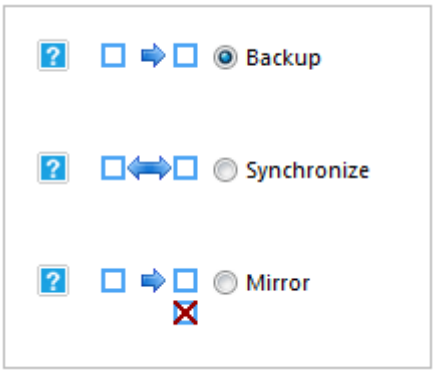
Après avoir téléchargé le logiciel et installé celui-ci, nous nous proposons de réaliser une copie de sécurité de notre répertoire G:\Documents vers notre NAS, dont le partage s'appelle COMMON et porte la lettre Z:\

D'abord, sur notre NAS, nous créons un répertoire Backups qui contiendra notre copie de sauvegarde :



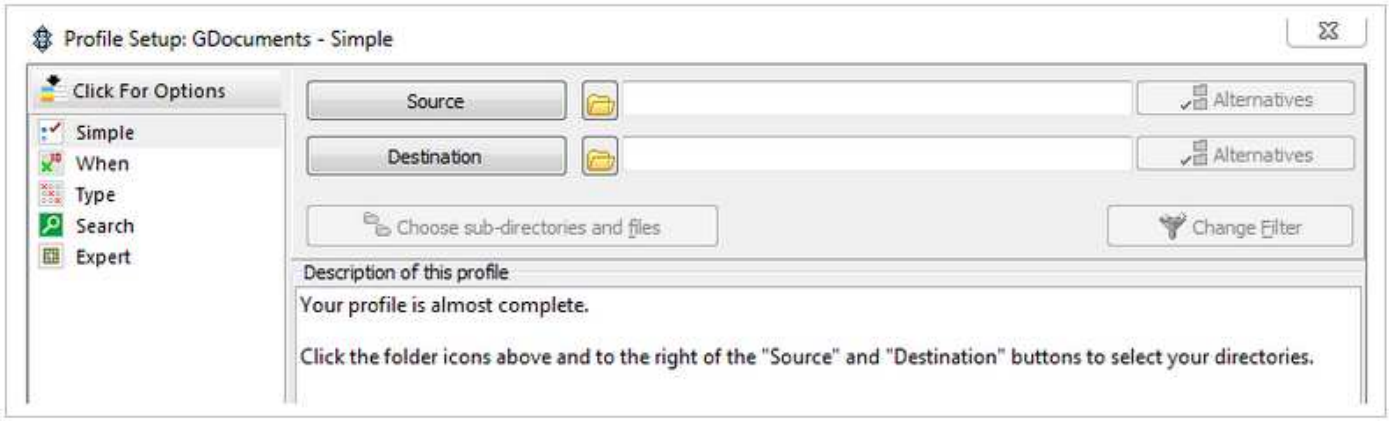
Ensuite, nous lançons SyncBack et nous allons dans Profiles > New pour créer une nouvelle tâche, et nous lui donnons un nom (GDocuments). Notez qu'il est possible, via le menu Preferences > Language, d'avoir le programme en français. Personnellement, nous utilisons rarement cette facilité parce que les traductions sont parfois fantaisistes ou déroutantes.

Nous choisissons ensuite le type de tâche qui nous intéresse (backup)

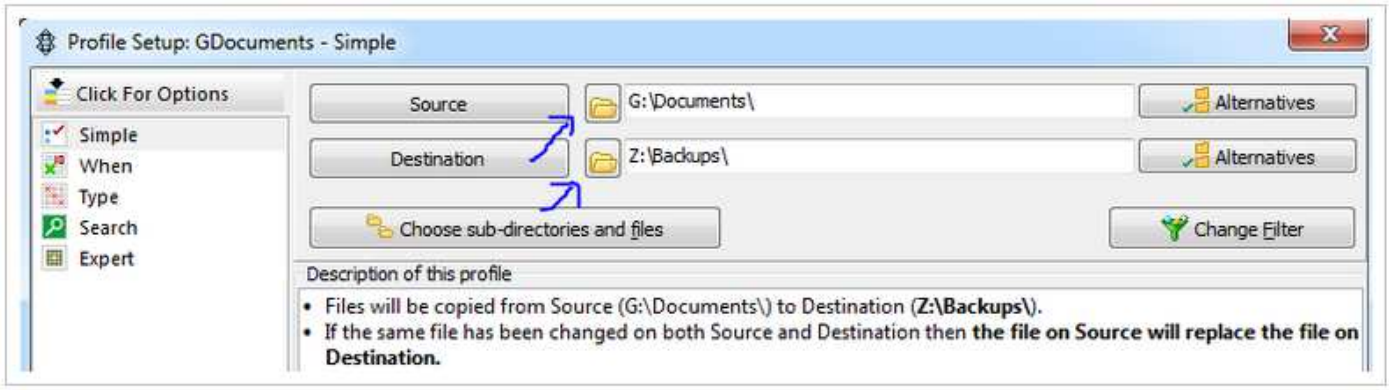


Ensuite, le programme nous demandera s'il s'agit de copie à travers des disques ou à travers le réseau (FTP = File Transfer Protocol, à éviter si les fichiers ne sont pas encryptés).

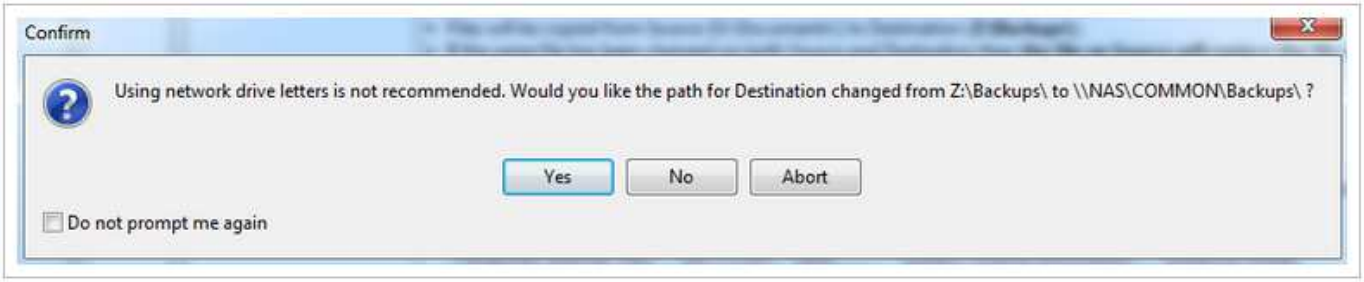
Par après, le programme ouvrira le profil en question afin qu'on puisse préciser les modalités.



Ensuite, nous spécifions la source et la destination :

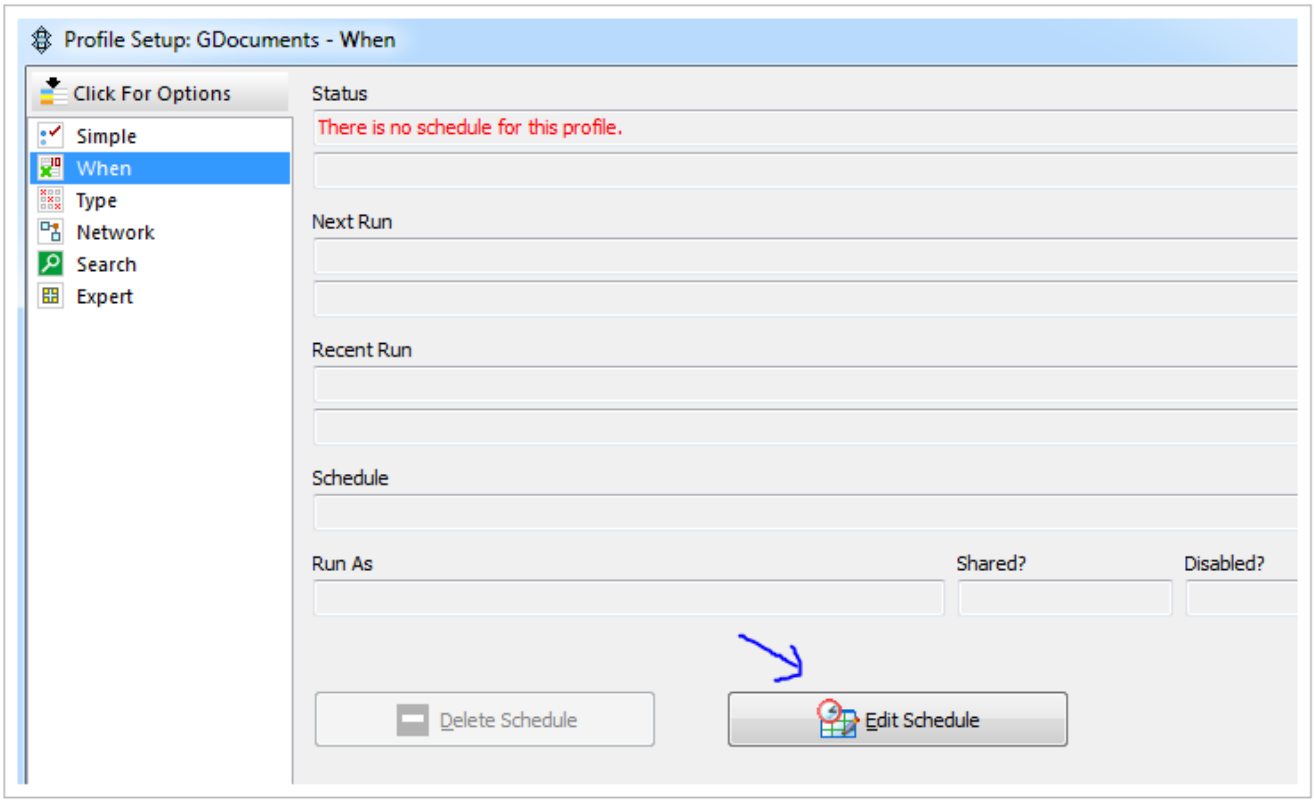


Et le programme détecte que notre destination est en fait un disque réseau, donc il nous propose de convertir le chemin windows en chemin réseau complet (UNC).

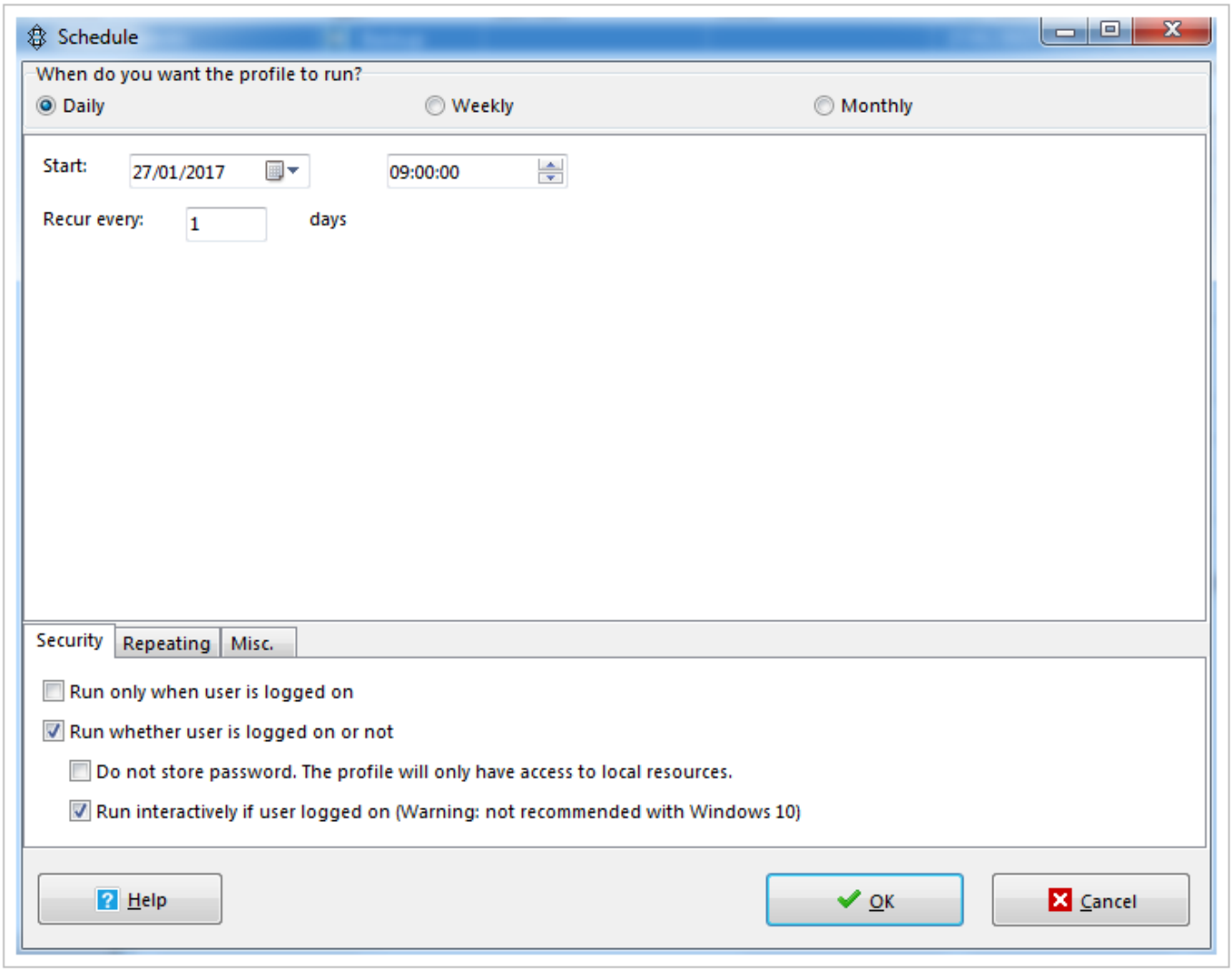


Ensuite, le programme nous proposera une simulation pour vérifier que tous les fichiers sont accessibles (optionnel).

Après quoi, en double-cliquant sur le profile, on peut choisir de l'éditer, et en cliquant (colonne gauche) sur When, on peut créer un schedule, soit une planification pour cette tâche :

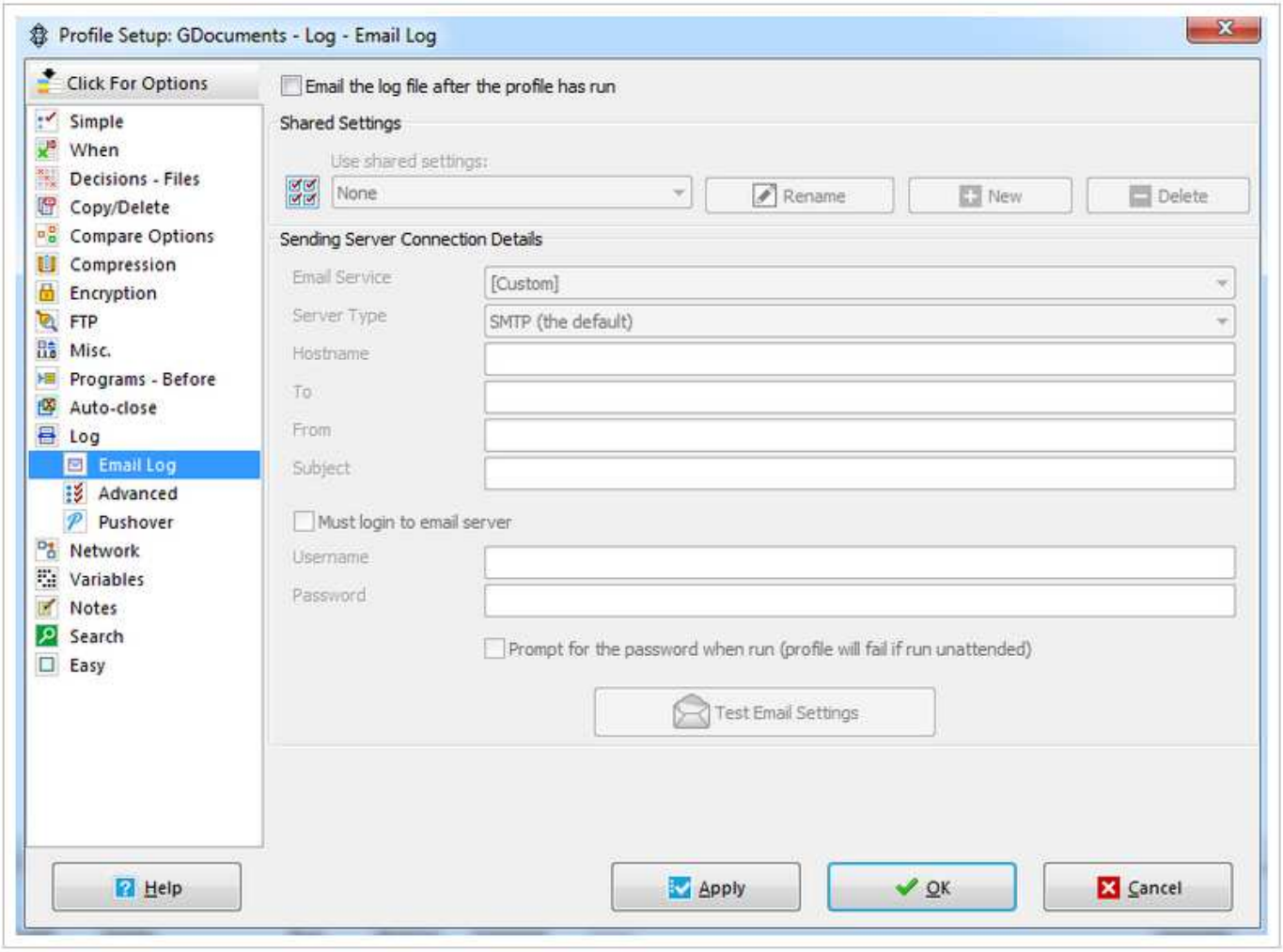


Il vous faudra donner le mot de passe avec lequel vous vous connectez sur l'ordinateur, puis préciser les données de planification :



Puis, OK, et c'est tout !

Si vous voulez par exemple vous faire envoyer les logs, donc les historiques (indiquant que tout s'est bien passé ou non) par courriel, il vous faudra cliquer en colonne gauche sur Expert > Log > Email Log



dans lequel vous devrez préciser le compte à utiliser. Si vous avez votre propre serveur de courrier, vous pourrez donner son adresse, ou alors utiliser un compte de votre fournisseur (Skynet, etc.) en précisant les paramètres, de la même manière que lorsqu'on configure un client e-mail sauf qu'ici, on ne spécifie que le serveur sortant (SMTP).

Le logiciel, en mode expert, permet de réaliser un nombre impressionnant de tâches différentes, y compris l'historisation, l'encryption et la compression. On peut s'en servir pour synchroniser des répertoires (attention toutefois à l'effacement dans les répertoires sources !), pour faire de simples copies, ou pour réaliser en une seule fois un ensemble de tâches (groupe de profils que l'on peut choisir à la création).

Cela fait partie de ces utilitaires qui peuvent vite se rendre indispensable.

Mot de la fin

Vous l'aurez compris, sans doute, le sens de cet article était avant tout de vous dire qu'on n'a jamais *trop* de backups, tout comme on n'a jamais une *trop* bonne santé. Au prix où cela coûte, il faudrait être vraiment insouciant ou décidément très confiant pour se permettre de ne pas en réaliser aussi par vous-même.

Vu la recrudescence des ransomwares, ces virus qui encryptent tous les fichiers d'un ordinateur ou d'un réseau puis qui après, exigent un paiement en ligne pour que la clé de décryption soit envoyée, nous ne pouvons que vous encourager à avoir divers backups et de vérifier régulièrement l'intégrité de vos fichiers (sur un autre ordinateur par exemple). En complément d'avoir bien sûr un antivirus à jour sur chaque machine du bureau. Rappelons que dans 95% des cas, les virus sont installés *par les utilisateurs* eux-mêmes après qu'ils aient accepté de les installer (et même si le virus prétend être tout autre chose). Il convient donc de réfléchir toujours à deux fois avant d'installer quelque programme que ce soit. Et pourquoi ne pas le soumettre au site VirusTotal qui le passera au crible d'une cinquantaine d'antivirus différents et vous dira si ce programme est fiable. Ce n'est pas infaillible, mais c'est beaucoup mieux que rien.

Philippe Huysmans
Responsable Informatique IPCF