

Sauvegarde

- Sauvegarde externalisée vers Cloud
- Sauvegarde externalisée chiffrée vers NAS

Sauvegarde externalisée vers Cloud



Pourquoi sauvegarder ses données vers un service CLOUD comme Dropbox ?

Il faut sauvegarder ses données vers un service Cloud afin de pouvoir récupérer des données qui pourraient être perdues suite à un dysfonctionnement (erreurs, mauvaises manipulations, pertes de données...). Les sauvegarder régulièrement permet d'assurer un meilleur fonctionnement. On peut utiliser des services Cloud pour particuliers ou un service Cloud pour entreprise (celui-ci sera bien plus sécurisé, et on a des sauvegardes des fichiers). Il existe de très nombreux services CLOUD, comme Dropbox par exemple, que nous allons utiliser ici.

Quels outils avez-vous utilisés afin de réaliser cette sauvegarde ?

Afin d'effectuer une sauvegarde, on peut utiliser mysqldump, préinstallé avec MySQL server, combiné avec un fichier Batch, afin de créer un script de sauvegarde. J'ai donc créé un fichier .bat sous Windows, qui une fois exécuté, sauvegarde les bases de données dans une destination souhaitée. Ce script contient la destination des fichiers à sauvegarder, la destination de sauvegarde, l'emplacement de mysqldump. Le script va renommer la sauvegarde selon la date de celle-ci.

Une copie du script Batch est disponible sur GitHub à l'adresse suivante :

<https://github.com/improy/MySQL-DataBase-backup-using-windows-bat-file>

Une fois le script lancé, il est possible d'avoir une erreur :

« [Warning] Using a password on the command line interface can be insecure. »

Ce message signifie en français qu'utiliser un mot de passe dans l'interface de ligne de commande peut être non sécurisé. Une solution peut être de créer un fichier qui contiendra les données de connexion aux bases de données. Au lieu de demander les identifiants, on indiquera la destination du fichier contenant les identifiants.

On aura donc un fichier du type :

```
1 [client]
2 user = root
3 password =
```

Ce fichier doit être dans un autre répertoire que le script.

--defaults-extra-file=/etc/mysql/mysql-backup-script.cnf

On rajoute cette ligne dans le script.

Ainsi, le script va aller chercher ce fichier afin d'avoir les identifiants de la base de données.

Dans le cas d'une sauvegarde non chiffrée :

Pour la planifier, on peut utiliser le planificateur de tâches sous Windows qui va exécuter chaque jour à une heure fixe le fichier Batch, et donc la sauvegarde. La sauvegarde sera compressée pour utiliser un espace disque plus faible.

Une fois que la tâche exécutant le script est planifiée, on planifie ensuite la sauvegarde sous un logiciel de sauvegarde, comme Cobian Backup 11.

Cobian Backup 11 est disponible au téléchargement sur ce site : <https://www.cobiansoft.com/>

On va alors créer une tâche, en choisissant la destination du fichier ou du dossier à sauvegarder, puis la destination de sauvegarde (ici vers Dropbox). On va ensuite choisir la sauvegarde différentielle et les créneaux de sauvegarde puis valider. La sauvegarde est désormais planifiée.

Quels sont les différents types de sauvegardes ?

On distingue 4 types de sauvegardes :

1. **La sauvegarde complète**: elle va sauvegarder toutes les données.
2. **La sauvegarde Incrémentielle**: elle va sauvegarder uniquement les fichiers qui ont été modifiés ou ajoutés.

3. **La sauvegarde différentielle**: sauvegarde de tous les fichiers dont le marqueur est à vrai. Une fois archivé, le fichier garde la position de son marqueur.
4. **La sauvegarde miroir**: il s'agit d'une copie exacte des données sources. Avec un miroir, il n'y a qu'une seule sauvegarde qui contiendra les fichiers, tels qu'ils existaient lors de la dernière sauvegarde.

Sauvegarde externalisée chiffrée vers NAS

Pourquoi sauvegarder ses données vers un NAS ?

Un NAS est un serveur de stockage en réseau. Il est important de sauvegarder vers un serveur externe comme un NAS afin de sécuriser les données. Il faut sauvegarder ses données vers un NAS afin de pouvoir récupérer des données qui pourraient être perdues suite à un dysfonctionnement (erreurs, mauvaises manipulations, pertes de données...). Les sauvegarder régulièrement permet d'assurer un meilleur fonctionnement.

Pourquoi chiffrer ses données avant transfert vers un NAS ?

Il faut chiffrer ses données avant transfert vers un NAS afin de sécuriser l'échange et donc les données. Une fois sur les NAS, les données sont chiffrées et quasiment impossible à récupérer.

Quels outils utiliser afin de réaliser cette sauvegarde ?

Il existe une multitude d'outil. Dans notre cas nous allons utiliser un script de sauvegarde, que l'on planifiera. La sauvegarde sera effectué dans un fichier dit « conteneur » crée par VeraCrypt, permettant de chiffrer les données.

Quels sont les différents types de sauvegarde ?

On distingue 4 types de sauvegardes :

1. **La sauvegarde complète**: elle va sauvegarder toutes les données.
2. **La sauvegarde Incrémentielle**: elle va sauvegarder uniquement les fichiers qui ont été modifiés ou ajoutés.
3. **La sauvegarde différentielle**: sauvegarde de tous les fichiers dont le marqueur est à vrai. Une fois archivé, le fichier garde la position de son marqueur.
4. **La sauvegarde miroir**: il s'agit d'une copie exacte des données sources. Avec un miroir, il n'y a qu'une seule sauvegarde qui contiendra les fichiers, tels qu'ils existaient lors de la dernière sauvegarde.

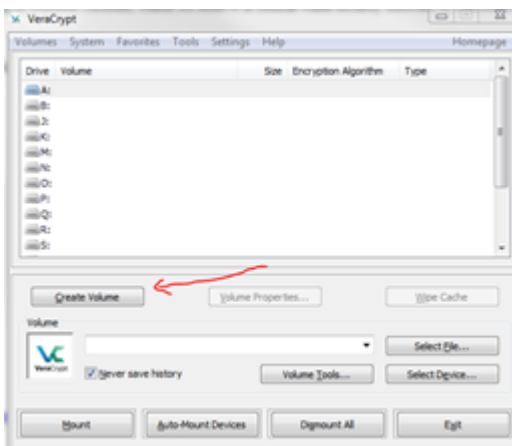
Réalisation du TP

Nous allons utiliser un script de sauvegarde disponible dans le dossier où se compte-rendu se trouve. Nous avons modifié la ligne 44 en y ajoutant le nom de la base de données à sauvegarder. Dans notre cas, « ppe ». Nous avons également changer la destination de la sauvegarde vers le lecteur A : « A:\ ». Nous verrons cela plus tard.

Commençons tout d'abord par installer VeraCrypt. Il est disponible sur leur site internet <https://www.veracrypt.fr/en/Downloads.html>. Nous avons pris ici la version Installer de Windows.

Une fois installé, on lance l'application.

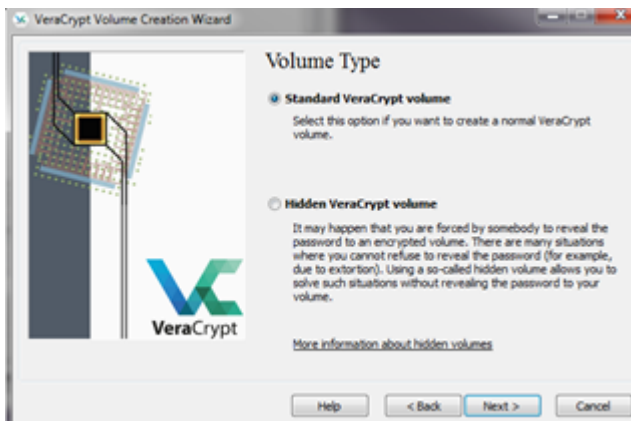
On clique sur Create Volume.



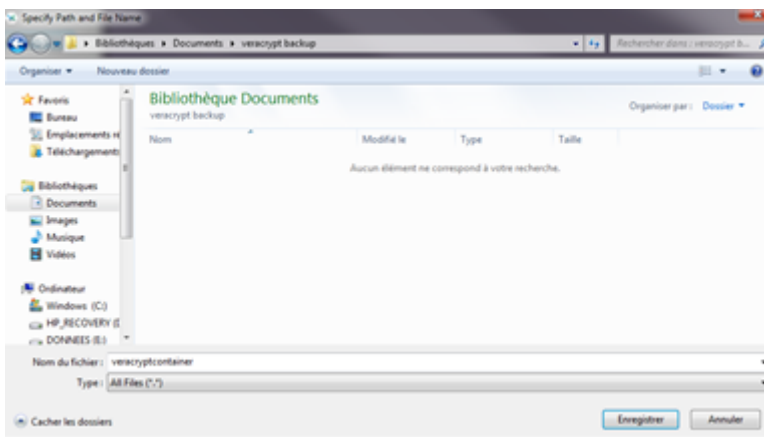
On fait suivant.



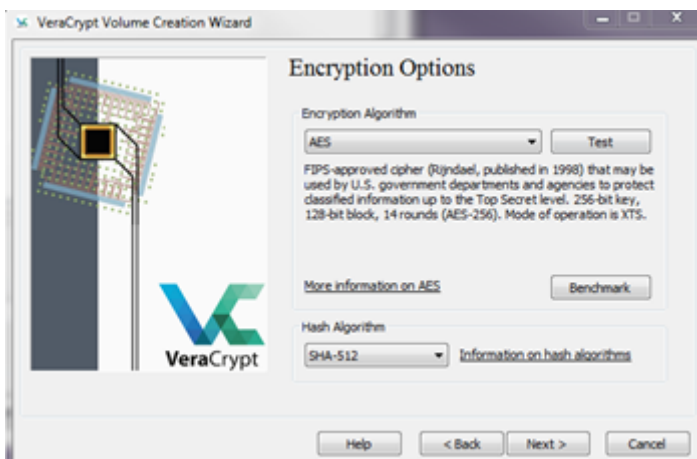
Encore suivant.



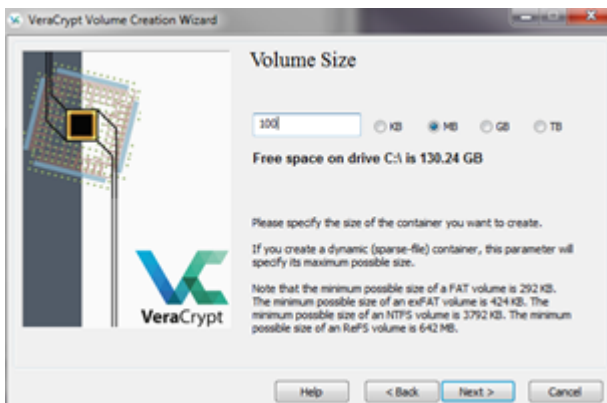
On va ensuite définir la destination du fichier conteneur. Dans notre cas, dans Documents puis veracrypt backup. Enregistrer puis suivant.



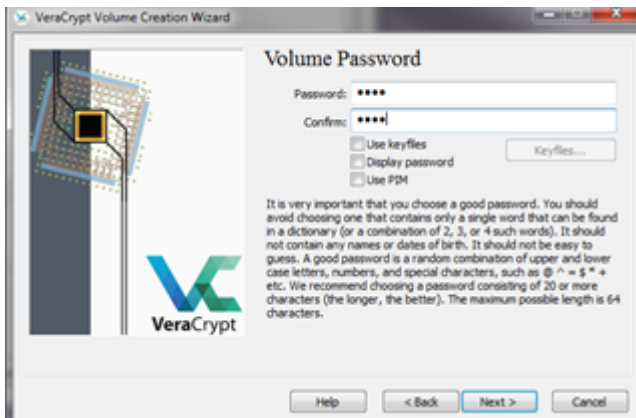
On définit ensuite l'algorithme de chiffrement puis suivant.



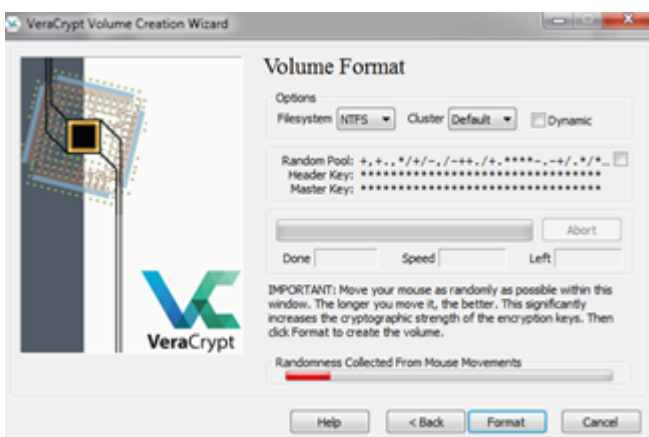
On définit ensuite la taille du conteneur. Dans notre cas, 100MB suffisent.



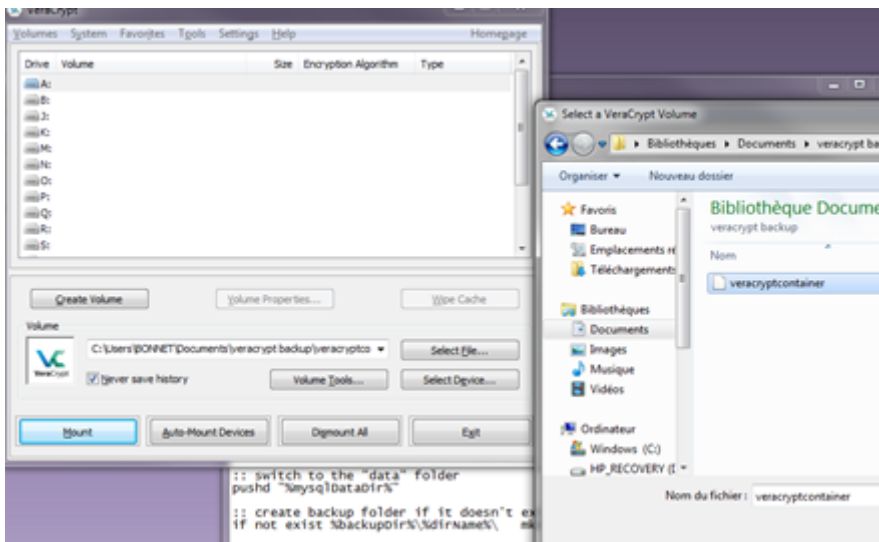
On définit ensuite le mot de passe du volume. Plus il est long, mieux c'est.



On bouge la souris afin de générer la clé du volume jusqu'à que la barre soit verte puis suivant. On peut quitter.



On clique sur Select file puis on choisit le fichier que l'on a créé via VeraCrypt.



On clique sur Ouvrir puis Mount en bas à gauche. On rentre le mot de passe puis OK.

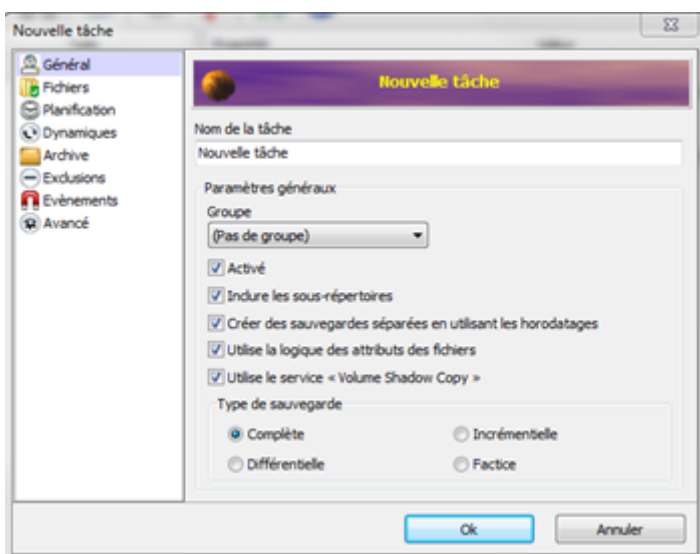
Désormais, dans l'explorateur de fichiers, nous avons un nouveau disque nommé « Disque Local (A:) ». Notre fichier chiffré est prêt.

Dans le script, nous allons modifier la destination de sauvegarde pour « A:\Backup », Backup étant notre dossier de sauvegarde.

Nous allons ensuite planifier la sauvegarde de la sauvegarde de la base via le script à l'aide de Cobian Backup 11.

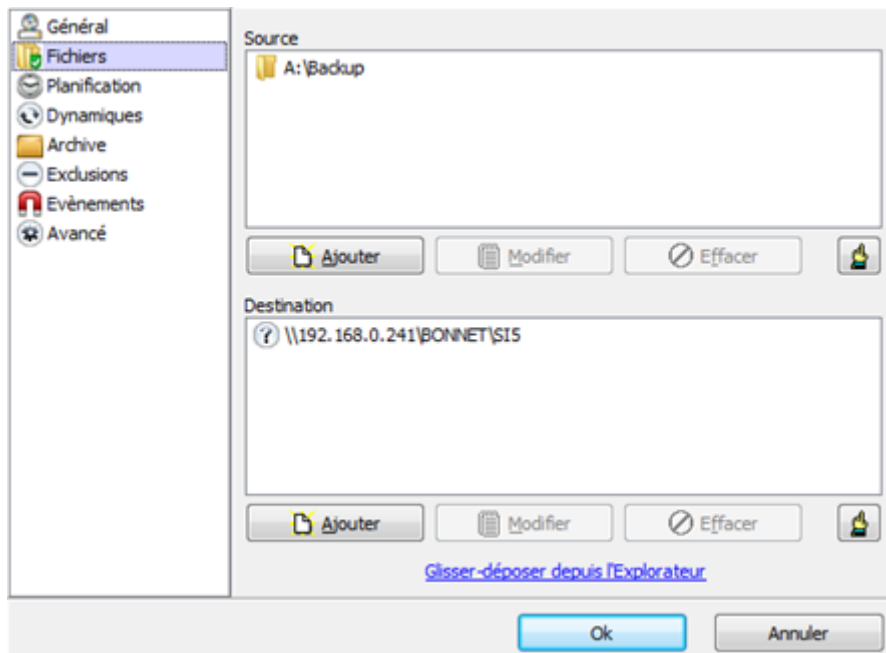
On va dans « Tâche » puis « Nouvelle tâche ».

On nomme notre tâche et on choisit le type de sauvegarde.

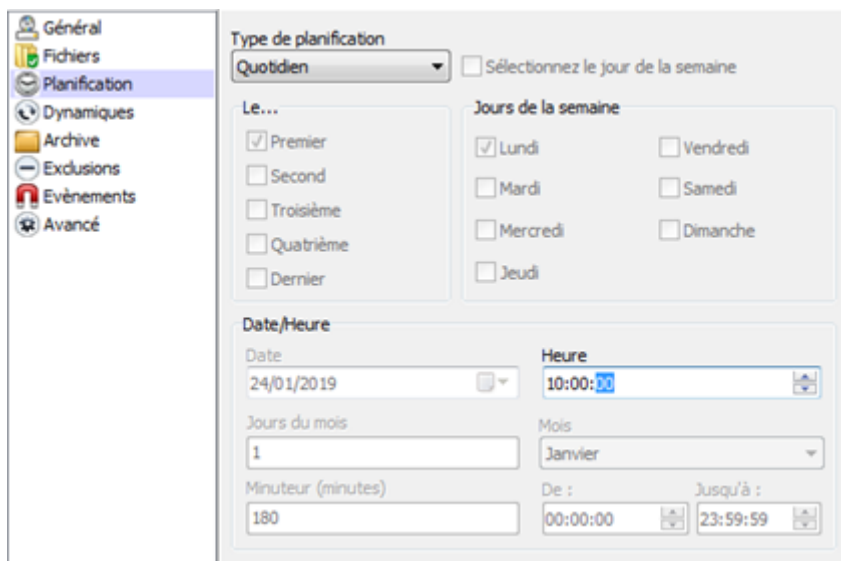


Dans « Fichiers », on clique « Ajouter » afin d'ajouter la source donc le fichier à sauvegarder. Ici « A:\Backup ». Ensuite on clique sur « Ajouter » en bas afin d'ajouter la destination de la

sauvegarde. Ici « \\192.168.0.241\bonnet\SIS », la destination étant le serveur NAS.

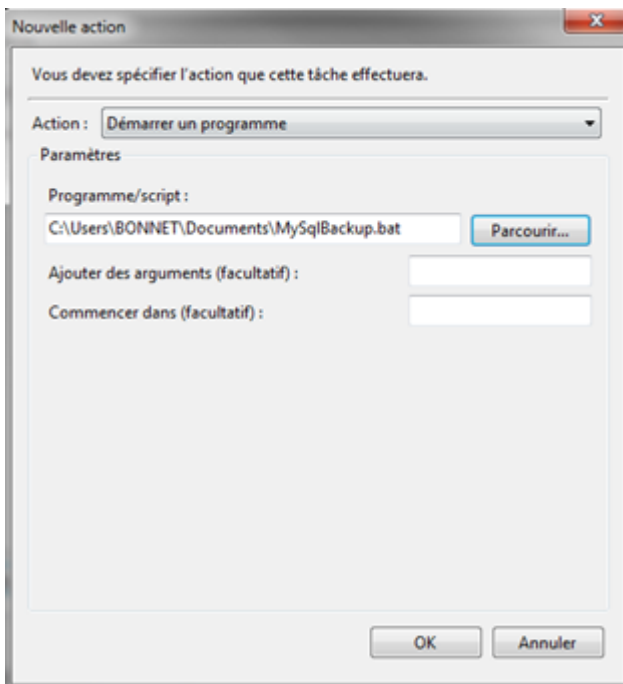


Dans « Planification », on peut choisir à quel moment se fait la sauvegarde. Dans notre cas, tous les jours à 10h00.

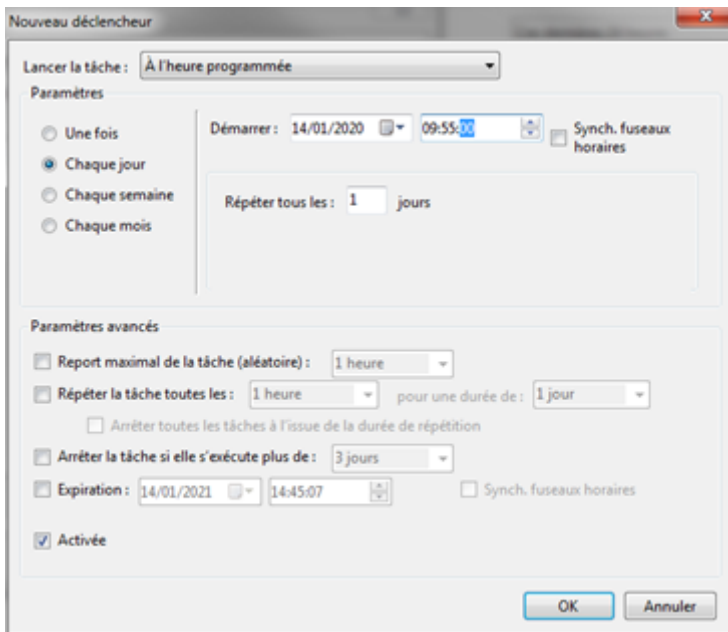


On peut cliquer sur OK.

Maintenant, à l'aide du planificateur de tâches de Windows, nous allons planifier la tâche pour 09h55. On clique sur créer une tâche en haut à droite. On nomme la tâche. Dans « Actions », on clique sur Nouveau... puis Démarrer un programme. On choisit la destination du script.



Dans « Déclencheurs » on clique sur « Nouveau... » On planifie chaque jour à 9h55.



On fait OK. C'est fini !

Pour tester, on attend 9h55. On regarde si le fichier a été modifié.

Voici le résultat : la sauvegarde a bien eu lieu, et le contenu a changé.

