note pour l'utilisation de veracrypt

22-12-2020

Veracrypt est un logiciel libre de **chiffrement de partition ou de volume** qui a remplacé **TrueCrypt**. Veracrypt permet de créer des volumes chiffrés sur des clés USB, des ordinateurs ou des disques durs. Ces volumes sont transportables mais doivent être ouvertes avec la seule application Veracrypt. # Installation et mise en route (GNU/Linux)

pour la télécharger plusieurs solutions : ## A partir d'un *repository*

```
sudo add-apt-repository ppa:unit193/encryption
sudo apt update
sudo apt install veracrypt
```

A partir du site de VeraCrypt

Pour un téléchargement plus sûr et plus récent, on peut télécharger la dernière version du logiciel mise à dispositions sous la forme d'archive depuis le site de Veracrypt

extraire les fichiers de l'archive :

$ tar -xvf nom_archive_veracypt.tar.bz2

On obtient alors un fichier .deb et une signature .

contrôle de l'intégrité du package

afin d'éviter les attaques du type "MIM" (Man-In-the-Middle), il est important de vérifier l'intégrité du fichier que l'on va installer sur son système pour éviter qu'un acteur malveillant n'y ait introduit une *backdoor* ; pour cela, on va vérifier que le package a bien été signé avec la clé de ses développeurs et pas avec une autre clé. Cette vérification se fait au moyen du gestionnaire de clés GPG qui est installé de base sur la plupart des distributions Linux. On peut en avoir un équivalent pour Windows en chargeant le logiciel GPG4Win

1. Télécharger la clé publique de VeraCrypt

D'après le site de Veracrypt, le fingerprint (hash, empreinte ou "condensat") de la clé des développeurs doit-être :

5069A233D55A0EEB174A5FC3821ACD02680D16DE

2. On va charger la clé publique de Veracrypt qui correspond à cette empreinte

```
$ gpg --import --import-options show-only VeraCrypt_PGP_public_key.asc
# vérifier que le condensat de la clé est bien égal au fingerprint indiqué sur l
```

3. Si ça coïncide, charger dans GPG la clé publique de VeraCrypt

```
$ gpg --import VeraCrypt_PGP_public_key.asc
```

4. Vérifier que la signature chargée avec le produit correspondent bien à la signature publique de Veracrypt.

Cela nécessite au préalable d'avoir charger l'archive et le fichier .sig dans le dossier où on exécute la commande suivante (voir étape précédente)

```
$ gpg --verify veracrypt-1.26.20-Ubuntu-24.04-amd64.deb.sig veracrypt-1.26.20-Ub
```

si on a ce résultat ("Bonne signature"), c'est que la version téléchargée est intègre

gpg: Signature faite le mer. 05 févr. 2025 00:36:17 CET gpg: avec la clef RSA 5069A233D55A0EEB174A5FC3821ACD02680D16DE gpg: Bonne signature de « VeraCrypt Team (2018 - Supersedes Key ID=0x54DDD393) veracrypt@idrix.fr » [inconnu] gpg: Attention : cette clef n'est pas certifiée avec une signature de confiance. gpg: Rien n'indique que la signature appartient à son propriétaire. Empreinte de clef principale : 5069 A233 D55A 0EEB 174A 5FC3 821A CD02 680D 16DE

L'empreinte de la clé principale correspond bien à celle de la clé publique de Veracrypt : le logiciel téléchargé n'a pas été altéré depuis la version contrôlée et signée par le développeur ou la développeuse ; on va pouvoir l'installer en toute sécurité.

installer le logiciel (GNU/Linux)

```
$ sudo -i dpkg version_de_veracrypt.deb
```

note : *dpkg* doit avoir été préalablement installé il est possible d'avoir à charger au préalable des dépendances : *pcscd* et *libccid* Dans ce cas on peut tenter de les installer une par une :

```
$ sudo apt install pcscd
...
$ sudo apt install libccid
```

si procéder de la sorte donne lieu à une erreur, on peut suivre la voie indiquée :

```
$ sudo apt ––fix–broken install
$ sudo apt update
$ sudo –i dpkg version_de_veracrypt.deb
```

on peut aussi forcer l'installation des dépendances qui manquent à partir de la commande suivante :

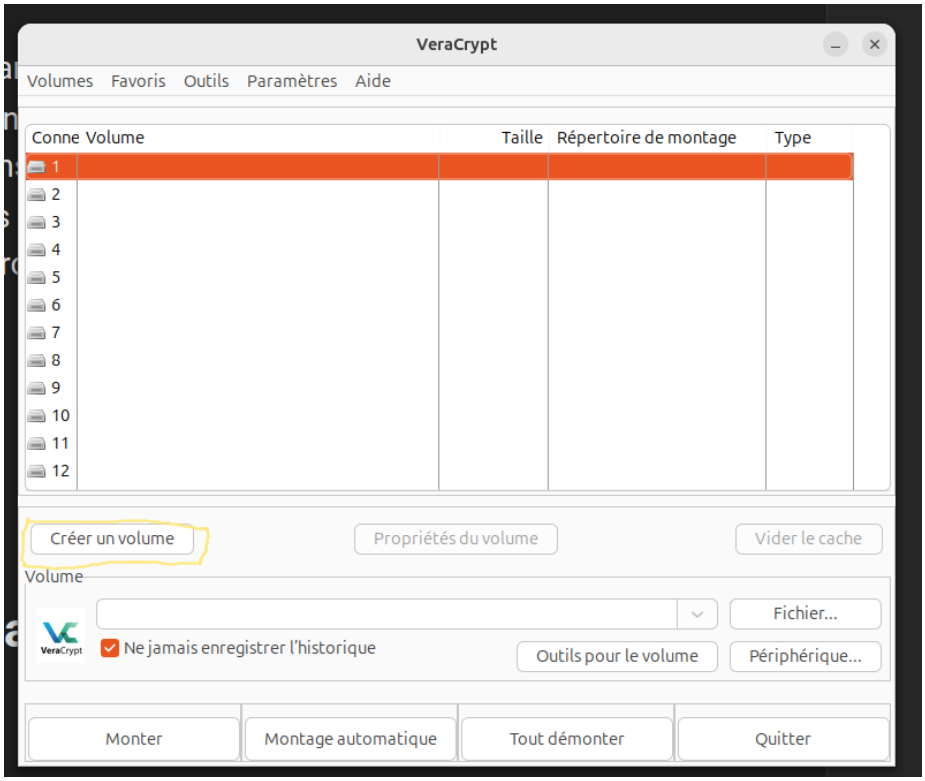
```
$ sudo apt–get install –f
```

Création d'un volume chiffré avec Veracrypt

avec l'interface graphique

ouvrir VeraScript

- Windows : en cliquant sur veracrypt.exe
- GNU/Linux : en allant chercher le logiciel dans la liste des applications, ou bien en tapant
- $ veracrypt dans le terminal ou bien (voir ci-dessous avec les droits de super-utilisateur $ sudo veracrypt)



Dans le popup qui apparaît, cliquer sur "créer un volume"

On peut créer un volume chiffré qui va occuper une clé USB ou bien seulement un espace délimité sur son ordinateur. Considérons le premier cas ; sélectionner “créer un fichier conteneur chiffré”

Il est possible de cacher un volume chiffré indétectable sous un autre volume chiffré. Ainsi, si on est obligé de céder son mot de passe à quelqu'un, cette personne accédera au premier volume de données (anodin) et ne verra pas le deuxième volume de données qui ne s'ouvre qu'avec un autre mot de passe ; un peu comme une valise à double fond.

Sélectionnons cette fonctionnalité

cliquer sur fichier et indiquez un chemin vers un fichier qui n'existe pas encore. Si ce fichier existe, il ne sera pas chiffré mais supprimé et remplacé par l'endroit où se trouvera le volume chiffré. Veracrypt ne chiffre pas des fichiers existants, il constitue des volumes chiffrés dans lesquels on va glisser des fichiers.

Laisser le protocole de chiffrement AES et l'algorithme de hachage SHA-512 qui constituent un bon compromis entre rapidité d'accès et robustesse.

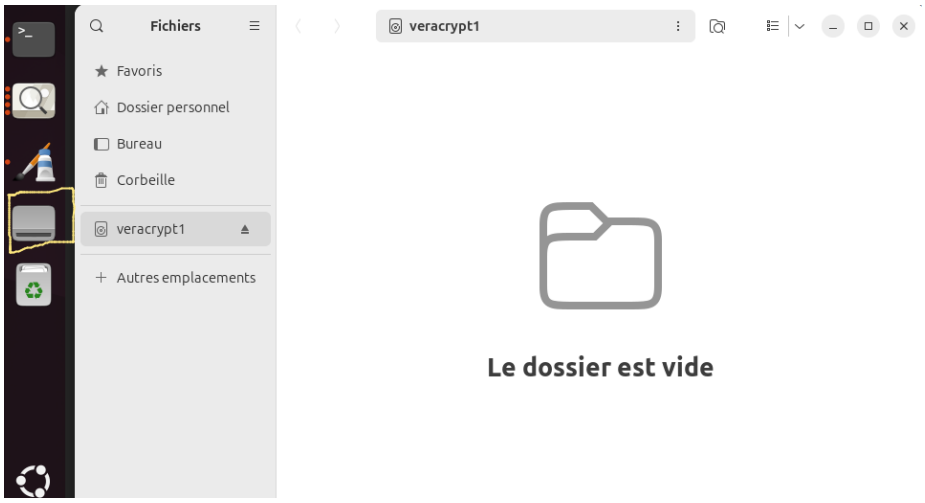
Indiquer un volume pour cette partition chiffrée (en fonction de vos besoins, prévoir une volumétrie des données) On va d'abord donner un espace au volume extérieur, puis à l'intérieur de celui-ci un espace au volume intérieur (volume caché)

choisir un mot de passe pour le volume extérieur

Il faut ensuite choisir la manière dont le volume va être formaté. Pour que le système d'exploitation puisse séparer ce volume des autres espaces de stockage de fichiers présents sur l'ordinateur, il est important de lui indiquer comment ce volume est organisé, comment il doit lire et analyser les fichiers qui y seront rangés ; c'est ce qu'on appelle le formatage de volume. FAT est un format de volume qui est à l'origine la production de Microsoft mais est reconnu par l'ensemble des OS ; ext2,3 et 4 correspondent à des volumes pour les systèmes Linux. Dans le cas où notre partition pourrait se retrouver tant sur une machine Windows que sur une machine Linux, on va choisir FAT (par défaut)

Dans l'étape suivante, on va générer la clé ; pour qu'elle soit unique, il faut y mettre de l'entropie ; faire des gestes de souris aléatoires dans le cadre de cette fenêtre pendant quelques temps, puis cliquer sur "formater"

ouvrir le volume externe

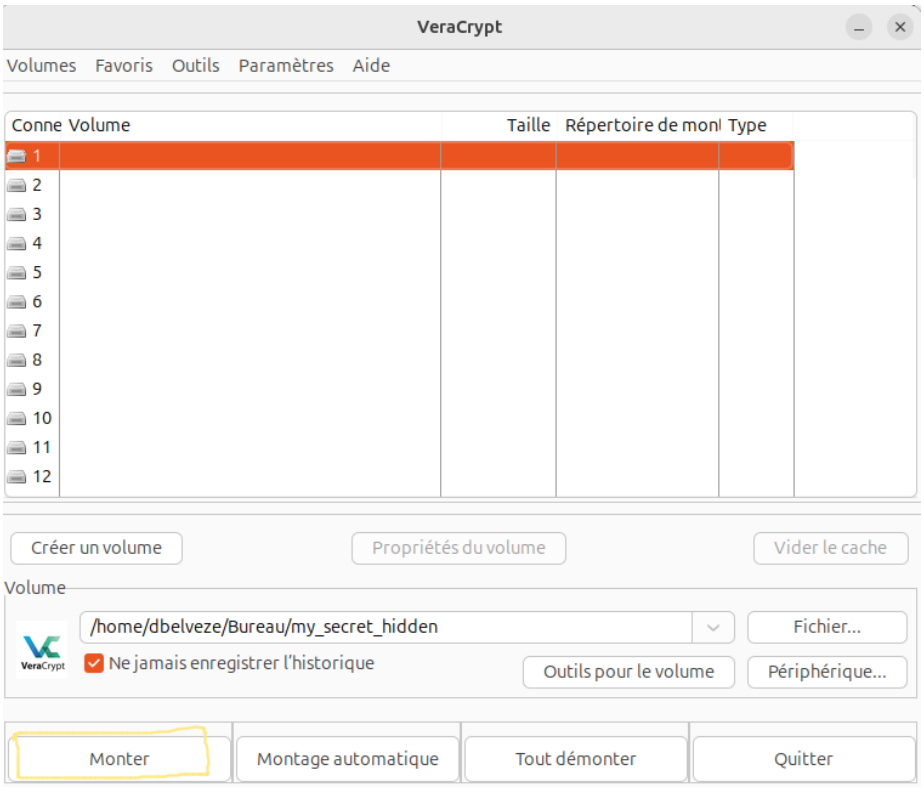


le volume chiffré vient d'être monté copier des fichiers de données qui ne présentent pas d'intérêt sensible dans ce volume (media/veracrypt1) fermer la fenêtre où le contenu du volume apparaît avec les nouveaux fichiers que vous y avez mis. cliquer sur "suivant"

Paramétrer le volume caché comme cela a été fait pour le volume extérieur (mêmes options de protocole, algorithme, volume de fichier mais bien sûr un mot de passe différent du premier)

quitter l'interface de création du volume

Pour accéder au volume créé, revenir sur la fenêtre d'accueil de Veracrypt qui doit toujours être ouverte



en cliquant sur le bouton “fichier”, parcourez les fichiers jusqu’à celui qui contient le volume chiffré extérieur (au passage, “my_secret_hidden” n’est pas un bon nom de fichier, de préférence utiliser des noms qui n’incitent pas à la curiosité) cliquer sur “Monter”

entrer le mot de passe du volume chiffré extérieur (non sensible) ; le volume est monté. On accède aux fichiers non sensibles.

Pour accéder au volume caché, le principe est assez différent de celui de la valise à double fond, à savoir qu’on ne passe pas par la partition non sensible du conteneur pour aller vers la partition sensible. Démonter le volume Monter de nouveau le volume, mais cette fois entrer le mot de passe relatif au volume caché : vous accédez directement au volume caché.

Ainsi, si quelqu’un (par exemple un douanier, il est de plus en plus courant que les chercheurs et chercheuses soient obligés d’ouvrir leurs appareils aux passages de frontières) voit que vous disposez de veracrypt sur votre appareil et vous demande la localisation de votre volume chiffé ainsi que votre mot de passe. Il accèdera au données non sensibles, mais ne pourra pas affirmer qu’il existe un autre volume de données sensibles ouvrable avec un autre mot de passe.

avec le terminal

On peut bien entendu réaliser les opérations décrites ci-dessus directement depuis le terminal :

$ veracrypt −t −c

si on ne souhaite pas cacher le dossier Veracrypt dans une partition, choisir "1: normal" insérer le lien vers le volume caché (par exemple ~/Bureau/hidden_secret)

indiquer ensuite la taille (292K minimum), pour 100 MB, taper 100[M]

choisir ensuite l'[[algorithme]] de chiffrement et l'algorithme de hachage (AES + SHA 512)

Choisir ensuite la fonction de formatage (FAT par exemple). Si le fichier choisi est déjà écrit, il sera effacé.

pim et chemin vers le fichier servant de clé : ne rien mettre (taper entrée)

entropie : taper une succession aléatoire de 320 touches et faire entrée.

voir l'ensemble des commandes disponibles pour le terminal dans la documentation de Veracrypt ## erreurs possibles :

Après certaines installations, un message d'erreur de ce type apparaît quelque fois :

Mauvais descripteur de fichier - VeraCrypt::CoreService::StartElevated:567

Pour créer un disque chiffré ou bien le monter, Veracrypt demande le mot de passe administrateur (après le mot de passe de la partition chiffrée) ; ça ne se passe pas forcément bien selon la manière dont le paramétrage d'accès aux droits d'utilisateur par un logiciel a été réalisé. Si on ne se sent pas capable de reparamétrer cet accès, pour éviter ces erreurs, il suffit de ne pas ouvrir Veracrypt à partir du lanceur mais à partir du terminal en mode *sudo*, ainsi on va d'abord fournir le mot de passe d'administrateur dont Veracrypt a besoin pour créer ou monter un volume puis seulement ensuite le mot de passe de ce volume, puisque la séquence inverse produit une erreur.

Pour ouvrir Veracrypt avec les droits d'administrateur, entrer dans le terminal

```
$ sudo veracrypt
```