PLEXDRIVE + RCLONE ‘crypt’ v0.2

Antes de lo siguiente, suponemos que ya tenemos configurado un remote rclone en el que subimos contenido encriptado/cifrado. No se recomienda encriptar/cifrar desde la raíz del propio Drive, se recomienda a partir de un subdirectorio (vamos a suponer que se llama ‘crypted’ dicho directorio).

ADVERTENCIA: PLEXDRIVE ES UNA HERRAMIENTA DE SOLO LECTURA. POR TANTO, ES OBVIO EXTRAER QUE EL OBJETIVO ES MONTAR EL DRIVE EN NUESTRO SISTEMA LINUX EN MODO ‘SOLO LECTURA’. DEL MISMO MODO, RECOMIENDO HACER UNA LECTURA DE LA GUÍA AL COMPLETO ANTES DE REALIZAR NADA, INCLUYENDO LAS NOTAS Y ACLARACIONES QUE SE ENCUENTRAN AL FINAL DEL DOCUMENTO.

1. Montar el drive con plexdrive en el sistema (no me paro a explicarlo, no es el objetivo, aunque dejaré un enlace sobre el uso de plexdrive al final del documento). Pongamos como ejemplo que lo montamos en ‘/plexdrive’. En este punto (y antes de continuar) ya deberíamos poder listar el directorio de montaje, y deberíamos ver que bajo nuestro directorio ‘crypted’ está el contenido cifrado.
2. Ejecutamos rclone config, y creamos un remote nuevo, seleccionando ‘Local Disk’ (a este remote lo llamaré ‘Temp’, cada uno que lo llame como considere). Este remote representará nuestro sistema de archivos Linux a grosso modo:
   ```
   10 / Local Disk
      \ "local"
   ```
3. Volvemos a crear un nuevo remote; en esta ocasión va a ser un remote tipo ‘crypt’:
   ```
   5 / Encrypt/Decrypt a remote
     \ "crypt"
   ```
4. Tomamos como base el remote local creado en el paso 2, y le indicamos la ruta de montaje de plexdrive y el directorio en el que tenemos el contenido encriptado (en este caso vamos a suponer que dicho directorio se llama ‘crypted’, tal como comenté al principio de la guía, y continuando con el ejemplo):
   ```
   Storage> 5
   Remote to encrypt/decrypt.
   Normally should contain a ':' and a path, eg "myremote:path/to/dir",
   "myremote:bucket" or maybe "myremote:" (not recommended).
   remote> Temp:/plexdrive/crypted
   ```
5. A continuación, seguimos indicando la misma configuración (IMPRESCINDIBLE QUE SEA EXACTAMENTE LA MISMA) que elegimos cuando creamos nuestro remote ‘crypt’ (Supongo que se han elegido cifrar también los nombres de los ficheros, y que indicamos una contraseña propia, yo siempre lo hago así y es lo que recomiendo, pero

si teníais opciones diferentes, cada uno que ponga las propias):

```
How to encrypt the filenames.
Choose a number from below, or type in your own value
 1 / Don't encrypt the file names.  Adds a ".bin" extension only.
   \ "off"
 2 / Encrypt the filenames see the docs for the details.
   \ "standard"
 3 / Very simple filename obfuscation.
   \ "obfuscate"
filename_encryption> 2
Password or pass phrase for encryption.
y) Yes type in my own password
g) Generate random password
y/g> y
Enter the password:
password:
```

6. El password Salt, yo siempre lo dejo en blanco, pero si creasteis uno debéis indicarlo:

```
Password or pass phrase for salt. Optional but recommended.
Should be different to the previous password.
y) Yes type in my own password
g) Generate random password
n) No leave this optional password blank
```

7. Termináis, salís de la configuración de rclone; y ya simplemente montáis este remote 'crypt' como acostumbramos con rclone: 'rclone mount …'.
8. Si todo ha salido bien, podréis ver el contenido descifrado en vuestro punto de montaje. Enjoy it!!!

NOTAS Y ACLARACIONES:

- OJO, esto no es para subir contenido al drive. Es para usar nuestro drive con contenido encriptado/cifrado (privacidad), y a su vez beneficiarse de usar plexdrive a modo de caché y evitar los bantemps por peticiones.
- Para subir el contenido al drive (aunque se da por entendido, lo explico para evitar confusiones), ES NECESARIO tener un remote 'crypt' independiente y enlazado a nuestro drive. Realmente son 2, el remote base en el que conectamos nuestra cuenta de drive (llamémosle a modo ejemplo GDrive, y en este creamos un directorio para almacenar el contenido encriptado, por ej, 'crypted'), y el remote encriptado que usa como base este anterior (lo llamaríamos por ej GDrive_enc, el cual crearíamos con base 'GDrive:/crypted', si seguimos los ejemplos anteriores). Así subiríamos el contenido a través de rclone browser, ó rclone al drive (encriptado al vuelo) haciendo uso directamente de este último remote crypt; y con la solución expuesta en esta miniguía, montaríamos el Drive en nuestro sistema para tener caché y descifrar al vuelo.
- Plexdrive no monta directorios a no ser que se indique explícitamente, es decir, por defecto monta el Drive desde la raíz. En caso de querer montar solamente una parte del drive (es decir, un subárbol), tenemos que indicar mediante el flag '–root-node-id' que 'nodo' del árbol queremos elegir como raíz (hay que extraer el id del directorio que queramos para ello, que es lo que hay que indicar en el flag).
- Con el uso de plexdrive, no necesitamos añadir flags de control en rclone, como tpslimit, ya que plexdrive es quien se comunica con Drive. Rclone actualmente queda como un simple programa que desencripta al vuelo lo que recoge plexdrive, pero para

rclone, es transparente la existencia de plexdrive; es decir, rclone piensa que el contenido está localmente (recordad que hicimos un remote 'local').

- Para entender mejor el punto anterior, este sería el flujo de información (dependencias): Drive -> plexdrive -> system -> rclone -> system
- Del punto anterior se extrae que SIEMPRE es necesario que plexdrive esté previamente montado, antes de que rclone ejecute su montaje. Si plexdrive falla, rclone fallará (es una 'cadena'). Aunque es obvio, que quede claro para los despistados. Es decir, si pretendemos hacer un automontaje en el inicio del sistema, será necesario que primero se monte plexdrive, y después es cuando podrá montarse rclone.
- Las capturas se hicieron hace tiempo, con una versión d rclone antigua, y hay opciones adicionales en la creación del remote. No obstante la base y lo relevante sigue siendo lo mismo.
- Para el uso de plexdrive, escribí una miniguía en github. Dejo el enlace por si a alguien le sirve de ayuda y aclaración, ya que además, esta miniguía sería su complemento: https://github.com/SpikeSP87/plexdrive_use

De esta forma conseguimos privacidad (mediante el cifrado), y evitar bantemps por peticiones al Drive (mediante plexdrive).

La alternativa es usar directamente rclone, y tengo pendiente volver a realizar tests del modo caché combinado con 'crypt', el cual en mis últimas pruebas (con rclone 1.39), fallaba (no mostraba correctamente los nombres de los ficheros/directorios básicamente). Pero en el momento que rclone y su cache funcionen correctamente, podremos prescindir de plexdrive.

Sugerencias y mejoras:

Telegram: @Sergi_0