Gocryptfs

Install

```
apt-get install gosciptfs
apt-get install davfs2
apt-get install rsync
```

Mount Stack

First the credentials for TransIP Stack should be added to /etc/davfs2/secrets.

```
$ nano /etc/davfs2/secrets

Add line the following line to this file:

https://ogroot.stackstorage.com/remote.php/webdav/        username
password
```

Now you can mount the TransIP Stack cloud folder:

```
mount -t davfs https://xxxxx.stackstorage.com/remote.php/webdav/ /tmp/STACK
-o rw,users,file_mode=774,dir_mode=774,uid=xxxxx,gid=users
```

Mount Encrypted filesystem

A feature of gocryptfs is the reverse mode function. In reverse mode, point gocryptfs at your unencrypted data, and it will create a mount point with an encrypted view of this data. This is useful for things such as creating encrypted backups. This is easy to do:

```
$ gocryptfs -reverse -init normal_data
Choose a password for protecting your files.
Password:
Repeat:

Your master key is:

    XXXXXXXX-XXXXXXXX-XXXXXXXX-XXXXXXXX-
    XXXXXXXX-XXXXXXXX-XXXXXXXX-XXXXXXXX

If the gocryptfs.conf file becomes corrupted or you ever forget your
password,
there is only one hope for recovery: The master key. Print it to a piece of
paper and store it in a drawer. This message is only printed once.
```

```
The gocryptfs-reverse filesystem has been created successfully.
You can now mount it using: gocryptfs -reverse normal_data MOUNTPOINT
```

This initialisation puts the following file in the root of the directory: *.gocryptfs.reverse.conf*

Now mount the encrypted directory:

```
$ mkdir encrypted_data
$ gocryptfs -reverse normal_data encrypted_data
Password:
Decrypting master key
Filesystem mounted and ready.
```