

Recover Encrypted Volume from only one disk in RAID 1 from a failed Synology NAS

I dismounted hard drive from Synology NAS device. I recall that file system on disk is not corrupted and HDD is not broken. Just Synology crashed. You need to connect HDD to computer, you can insert and connect it directly into desktop computer via SATA cables or use e-Sata connector or USB docking station (my case).
On a RAID1, you only need 1 disk.

1. Create a Easy2Boot USB stick <http://www.easy2boot.com/make-an-easy2boot-usb-drive/>
We will start Ubuntu from USB stick, so no OS installation is needed and no changes will be made. Download Ubuntu desktop ISO file and USB installer from url: <http://www.ubuntu.com/download/desktop>
Put the iso in _ISO/LINUX
2. Boot Ubuntu from USB stick.
Connect NAS HDD and USB stick to computer, then turn it on. Select boot from USB stick (press Esc or F12 or F11 or DEL, depends on computer, for boot menu and select your USB device. Choose the linux iso.

In OS first menu, select first option 'Run Ubuntu from this USB'.

3. Check HDD drive.
When desktop boots, press Windows key (it's funny, I know, but it works) and type Disk. You should see Disk Utility icon. Double click it. You should see an Extended Partition and RAID component (Or just your SAN disk).
4. Install RAID drivers.
Now we need to install Linux RAID driver. Press Win key, search for Terminal and run it. Type this and press enter: It will require Postfix installation, install it and select 'No configuration' in installation menu. (mdadm and other packages might already on your Ununtu distribution depending on version)

Code: Select all

```
sudo apt-get install mdadm
```

Now we will search and assemble RAID arrays.

Code: Select all

```
sudo mdadm --assemble --scan
```

Open Disk Utility again and you should see RAID array components.

5. Install LVM2 driver.

```
sudo apt-get install lvm2  
sudo vgscan --mknodes
```

Code: Select all

Now run Disk Utility, you should be able to see the volumes. (/dev/vg1/volume_x)
Select the Encrypted volume, then hit "Play" icon.

Now you will see the mount point like : (/media/ubuntu/1.41.12-2647/volume_x/)

6. Create a mount point for the filesystem

```
sudo mkdir /mnt/extract
```

7. Mount the encrypted folder

```
sudo mount -t ecryptfs /media/ubuntu/1.41.12-2647/volume_x/@MyFolder@ /mnt/extract
```

NOTE: The @MyFolder@ really is with 2 "@", that's the one you need to target. You can see it browsing in file explorer on 1st mount.

Enter the passphrase you used to to encrypt the drive when prompted

9. Choose the **AES** cipher

10. Choose **32** bytes as the key size

11. Choose **n** for *Enable plaintext passthrough*

12. Choose **y** for *Enable filename encryption*

13. Press return to accept the default for the *Filename Encryption Key (FNEK) Signature*

14. The first time you do this you may get the following warning

WARNING: Based on the contents of [/root/.ecryptfs/sig-cache.txt], it looks like you have never mounted with this key before. This could mean that you have typed your passphrase wrong.

15. Choose **yes** to proceed with the mount and **NO** to append the sig to the cache file

You may choose yes, but the day your computer get stolen, someone WILL get access to your data.

16. Done. Go to /mnt/extract and retrieve your data.

REFERENCES:

<https://www.techrepublic.com/article/how-to-install-and-use-ecryptfs-on-ubuntu/>
<https://robertcastle.com/2012/10/howto-recover-synology-encrypted-folders-in-linux/>
<https://forum.synology.com/enu/viewtopic.php?t=51393>