

Esche's IT-Blog*Remember Concepts To Convert Know-How Into IT*

Diskstation DSM – Verschlüsselte gemeinsame Ordner mittels eCryptfs unter Linux entschlüsseln

Publiziert am 16.12.2013 von admin

Seit der Firmware-Version DSM 2.3 gibt es die Möglichkeit „Gemeinsame Ordner“ mittels [eCryptfs](#) zu verschlüsseln. Für einen verschlüsselten Ordner wird auf der Diskstation immer ein Ordner „@NAME_DES_ORDNERS@“ erstellt, in dem die verschlüsselten Daten liegen. Zusätzlich gibt es einen Ordner „NAME_DES_ORDNERS“, über dem auf die entschlüsselten Daten zugegriffen werden kann. Es ist nicht nur möglich einen verschlüsselten Ordner über die Synology Diskstation zu entschlüsseln, sondern auch unter einem Linux-Betriebssystem wie Knoppix oder Ubuntu. Dieses Vorgehen kann dann sinnvoll sein, wenn die Diskstation defekt ist oder die Festplatten aus einem anderen Grund direkt an einem Computer angeschlossen werden.

Voraussetzung

Zur Entschlüsselung wird vorausgesetzt, dass der Zugriff auf das gemountete Laufwerk besteht, auf den sich der zu entschlüsselnde Ordner befindet.

Notwendige Pakete

Es muss das Paket „**ecryptfs-utils**“ installiert sein!

Je nach Linux-Betriebssystem, gibt es unterschiedliche Vorgehensweisen wie Pakete installiert werden können:

Ubuntu: sudo apt-get install ecryptfs-utils

Knoppix: Startmenü -> Einstellungen -> Synaptic Paketverwaltung -> Paket „**ecryptfs-utils**“ zum Installieren vormerken -> Anwenden

This website uses cookies to improve your experience. We'll assume you're ok with this, but you can opt-out if you wish.

sselter Ordner entschlüsselt werden:

1. Ordner zum Einhängen erstellen

```
1 | cd /media
2 | sudo mkdir ecryptdata
```

2. Verschlüsselter Ordner entschlüsselt einhängen

```
1 | sudo mount -t ecryptfs /media/VOLUME/@ecryptdata@ /media/ecryptdata
```

Wenn dieser Befehl ausgeführt wird, müssen nachfolgende Fragen wie folgt beantwortet werden:

- **Passphrase:** Hier muss das Passwort zum Entschlüsseln eingegeben werden
- **Select cypher:** Auswahl: 1 (aes)
- **Select key bytes:** Auswahl: 2 (32)
- **Enable plaintext passthrough:** Antwort n
- **Enable filename encryption:** Antwort: y
- **Filename Encryption Key:** mit Enter-Taste bestätigen

- **Would you like to proceed with the mount?** Antwort: yes
- **Would you like to append sig to..:** Antwort: no

Die notwendigen Einstellungen können auch direkt als Parameter mit angegeben werden:

```
1 sudo mount -t ecryptfs /media/VOLUME/@ecryptdata@ /media/ecryptdata \  
2 -o \  
3 key=passphrase:passphrase_passwd=PASSWORD,ecryptfs_cipher=aes,no_sig_cache,\  
ecryptfs_key_bytes=32,ecryptfs_passthrough=n,ecryptfs_enable_filename_crypto
```

Ausführen und „Filename Encryption Key“ mit der Enter-Taste bestätigen

Bei erfolgreicher Ausführung sollte als Bestätigung „***Mounted eCryptfs***“ ausgegeben werden.

Jetzt kann auf die entschlüsselten Daten über den Pfad „***/media/ecryptdata***“ zugegriffen werden.

Ordner aushängen

Mittels diesem Befehl kann der gemountete Ordner wieder ausgehängt werden

```
1 sudo umount /media/ecryptdata
```



Dieser Beitrag wurde unter [NAS](#) veröffentlicht. Setze ein Lesezeichen auf den [Permalink](#).