Verschlüsselung von Daten

Um Daten auf dem HPC-System verschlüsselt zu speichern, empfiehlt sich die Nutzung der Software gocryptfs

Die Software ermöglicht eine transparente Verschlüsselung von Daten und lässt sich mit jedem Programm verwenden. Die Daten liegen dabei in einem verschlüsselten Container und lassen sich nur mit dem dazugehörigen Passwort lesen und ändern.

Diese Passwörter sollten selbstverständlich nicht im HPC-System gespeichert werden, da sonst ein Angreifer diese direkt mit klauen kann. Dies ist vergleichbar mit der EC-Karten-Pin, welche niemals mit im Portemonnaie sein sollte.

Verwendung im Cluster

Die Software ist auf dem HPC-System als Modul verfügbar und muss vor der Verwendung geladen werden.

```
module load gocryptfs/1.7.1
```

⚠ Container dürfen nicht gleichzeitig an mehreren Stellen gemountet sein. Dies kann zur Zerstörung der Daten führen.

Anlegen eines Containers

Um einen Container zu erzeugen, benötigt man ein leeres Verzeichnis welche man als Container einrichtet.

```
mkdir /gpfs/project/$USER/container_1
gocryptfs -init /gpfs/project/$USER/container_1
```

Bei diesem Vorgang wird man nach einem Passwort gefragt, welches genutzt wird um die Daten zu verschlüsseln. Dieses Passwort muss sicher abgelegt werden. Zudem wird ein Master-Key ausgegeben, der am besten in einen Tresor gelegt wird. Mit diese Key können die Daten gerettet werden, falls die Konfigurationsdatei verloren geht.

Öffnen eines Containers

Um den Container zu öffnen, benötigt man ein leeres Verzeichnis, wo die Daten eingebunden werden sollen und das Passwort des Containers.

```
mkdir -p /tmp/$USER/container_1_unencrypted
gocryptfs /gpfs/project/$USER/container_1 /tmp/$USER/container_1_unencrypted
```

Mit diesem Befehl wird der verschlüsselte Inhalt von container_1 als unverschlüsselte Daten in container_1_unencrypted angezeigt.

Der Entschlüsselte Pfade sollte dabei auf einer lokalen Festplatte liegen und nicht auf einem gemounteten Filesystem.

Verwendung der Daten

Nach dem öffnen des Containers können die Daten mit einem beliebigen Programm in container_1_unencrypted verwendet werden.

Beispiele

```
ls /tmp/$USER/container_1_unencrypted
echo "test" > /tmp/$USER/container_1_unencrypted/test_datei
cat /tmp/$USER/container_1_unencrypted/test_datei
```

Löschen von Daten im Container

Um Daten im Container zu löschen, muss er zunächst geöffnet sein. Danach können Dateien wie üblich gelöscht werden.

```
rm /tmp/$USER/container_1_unencrypted/Datei
```

Löschen eines Containers

Um einen Container zu löschen, muss lediglich der verschlüsselt Ordner gelöscht werden.

```
rm -rf /gpfs/project/$USER/container_1
```

Schließen des Containers

Wenn man mit den Arbeiten fertig ist, muss der Container geschlossen werden.

```
fusermount -u /tmp/$USER/container_1_unencrypted
```

Verwendung auf dem eigenen Gerät

Für Windows gibt es einen kompatiblen Client unter dem Namen cppcryptfs . Für macOS lässt sich die Software über Brew installieren.

Um die Container auf dem eigenen Gerät zu verwenden, muss das Filesystem per Samba gemountet sein. Dies ist im Wiki Artikel Dateisysteme einhängen erklärt.