Linux am Dienstag

Verschlüsselter lokaler Raid 10 in der Cloud

Marius Schwarz – Stand 12.10.2021 für Linux-am-Dienstag.de

Verschlüsselter lokaler Raid 10 in der Cloud

Ein Vortrag

von

Marius Schwarz

Verschlüsselter lokaler Raid 10 in der Cloud

Prämisse

Verschlüsselter lokaler Raid 10 in der Cloud

Wir wollen ein lokales Raid 10 mit Spare auf einem Desktop-PC so bauen, daß die Daten bei verschiedenen Hostern in der Cloud liegen können, ohne das diese in die Daten schauen können.

Verschlüsselter lokaler Raid 10 in der Cloud

Grundüberlegungen

Verschlüsselter lokaler Raid 10 in der Cloud

Wieso Raid 10?

Verschlüsselter lokaler Raid 10 in der Cloud

Wieso Raid 10?

- Ein Raid 10 spiegelt Daten
- Ein Raid 10 verteilt die Last auf verschiedene Anbieter
- Ein Raid 10 minimiert den Rebuildprozess, fällt ein Cloudanbieter aus.
- Ein Raid 10 bietet mehr Platz
- Das kleinste bereitgestellte Cloudangebot bestimmt die Blockgröße der Beine.

Verschlüsselter lokaler Raid 10 in der Cloud

Wie werden die Daten zu den Hostern übertragen?

Verschlüsselter lokaler Raid 10 in der Cloud

Wie werden die Daten zu den Hostern übertragen?

Wir übertragen die Daten per SSHFS.

Die Datenübertragung ist dabei vollständig abgesichert,
auch wenn das nicht nötig wäre.

Verschlüsselter lokaler Raid 10 in der Cloud

Wie werden die Daten beim Hoster gesichert?

Verschlüsselter lokaler Raid 10 in der Cloud

Wie werden die Daten beim Hoster gesichert?

Die Daten liegen pro Hoster als eine große Datei vor,
die als LUKS-Container formatiert wurde.

Verschlüsselter lokaler Raid 10 in der Cloud

Wie werden die Daten beim Hoster gesichert?

Hoster freundliche Alternative:

je kleiner die einzelnen Raid 10 Datenfiles sind,
desto besser für den Hoster beim Backup.

Es könnten also pro Hoster mehrere kleine Dateien genutzt werden,
aber das erhöht den Aufwand immens und reduziert die verfügbar Speicherkapazität durch mehrfache Verwaltungsoverheads

Verschlüsselter lokaler Raid 10 in der Cloud

Wie ist die Performance?

Verschlüsselter lokaler Raid 10 in der Cloud

Wie ist die Performance?

Theorie:

Die maximale Transfergeschwindigkeit wird von dem kleinsten Netzwerkübergang bestimmt.

Verschlüsselter lokaler Raid 10 in der Cloud

Wie ist die Performance?

Praxis:

In der Realität bestimmt der Softwareraid und das Filesystem, wie schnell Daten übertragen werden.

Die dabei maximal mögliche Geschwindigkeit hängt von der kleinsten Datenübertragungsrate im Verbund ab.

Verschlüsselter lokaler Raid 10 in der Cloud

Ausfallsicherheit

Verschlüsselter lokaler Raid 10 in der Cloud

Ausfallsicherheit

Die Ausfallsicherheit wird durch einen Spare-Hoster realisiert, dessen Datenfiles zwar dem Raid zugewiesen sind, aber nicht im Verbund genutzt werden.

Fällt ein Hoster aus, übernimmt der Raid den Spare und Synct die nötigen Daten in diesem Segment.

Verschlüsselter lokaler Raid 10 in der Cloud

Ausfallsicherheit

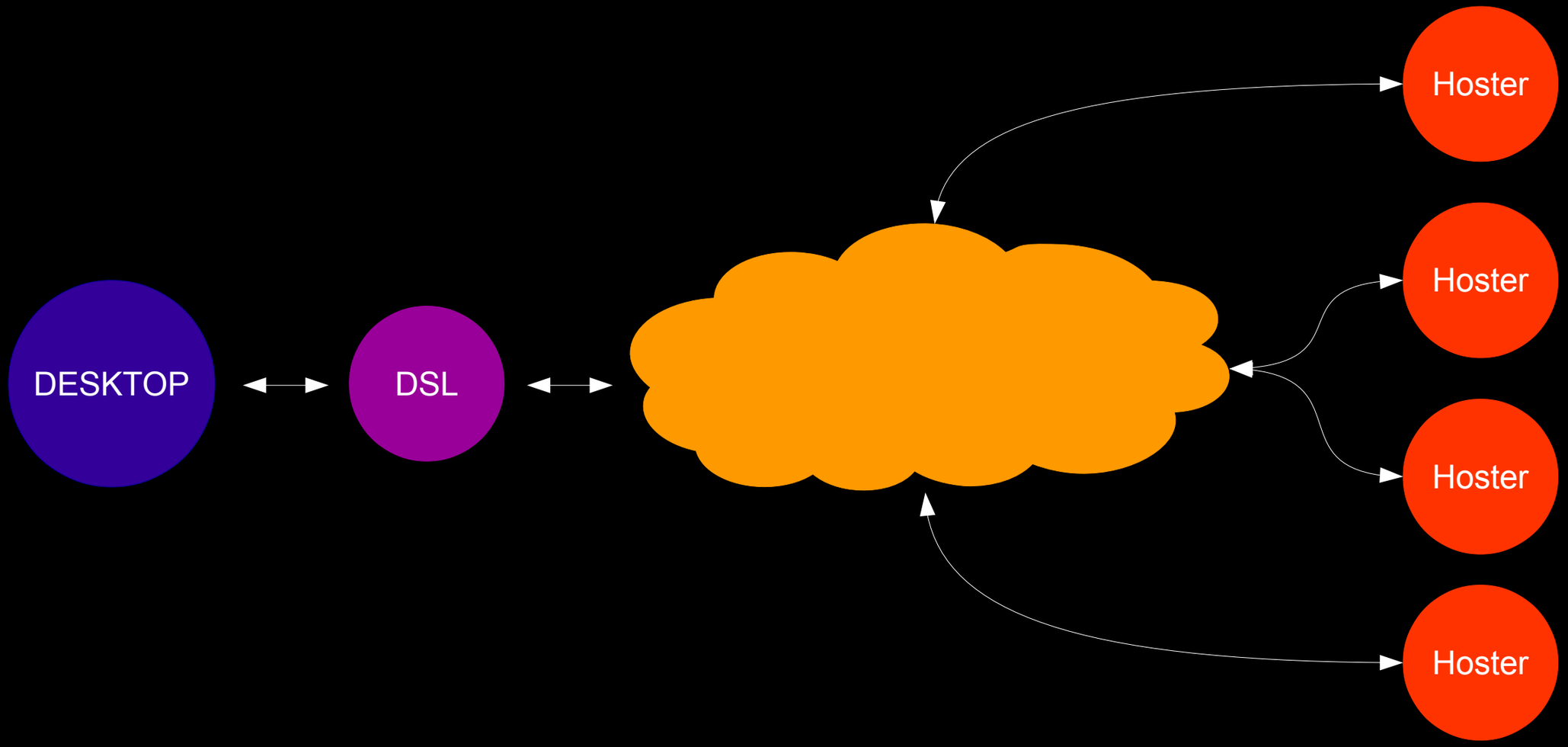
Wie bei allen Software Raids

können die wildesten Dinge passieren ;)

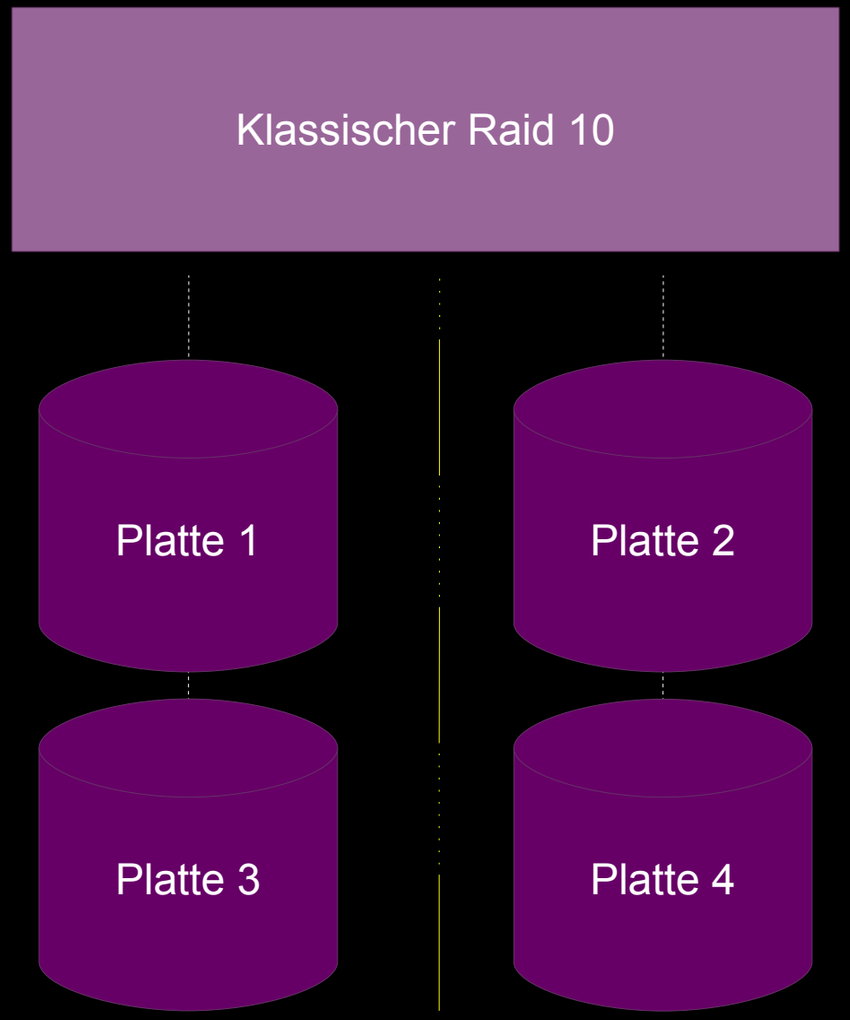
Verschlüsselter lokaler Raid 10 in der Cloud

Das Raidmodell

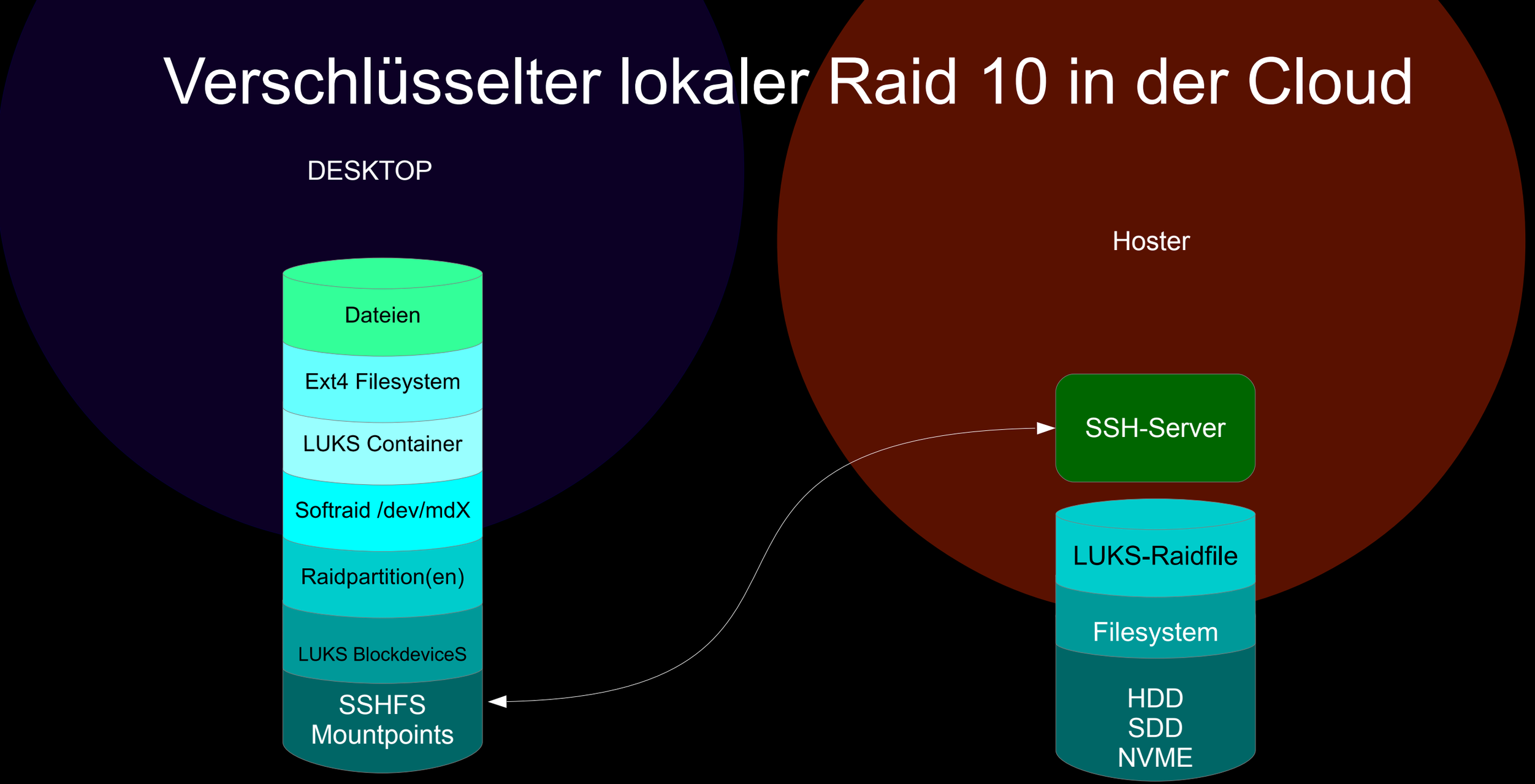
Verschlüsselter lokaler Raid 10 in der Cloud



Verschlüsselter lokaler Raid 10 in der Cloud

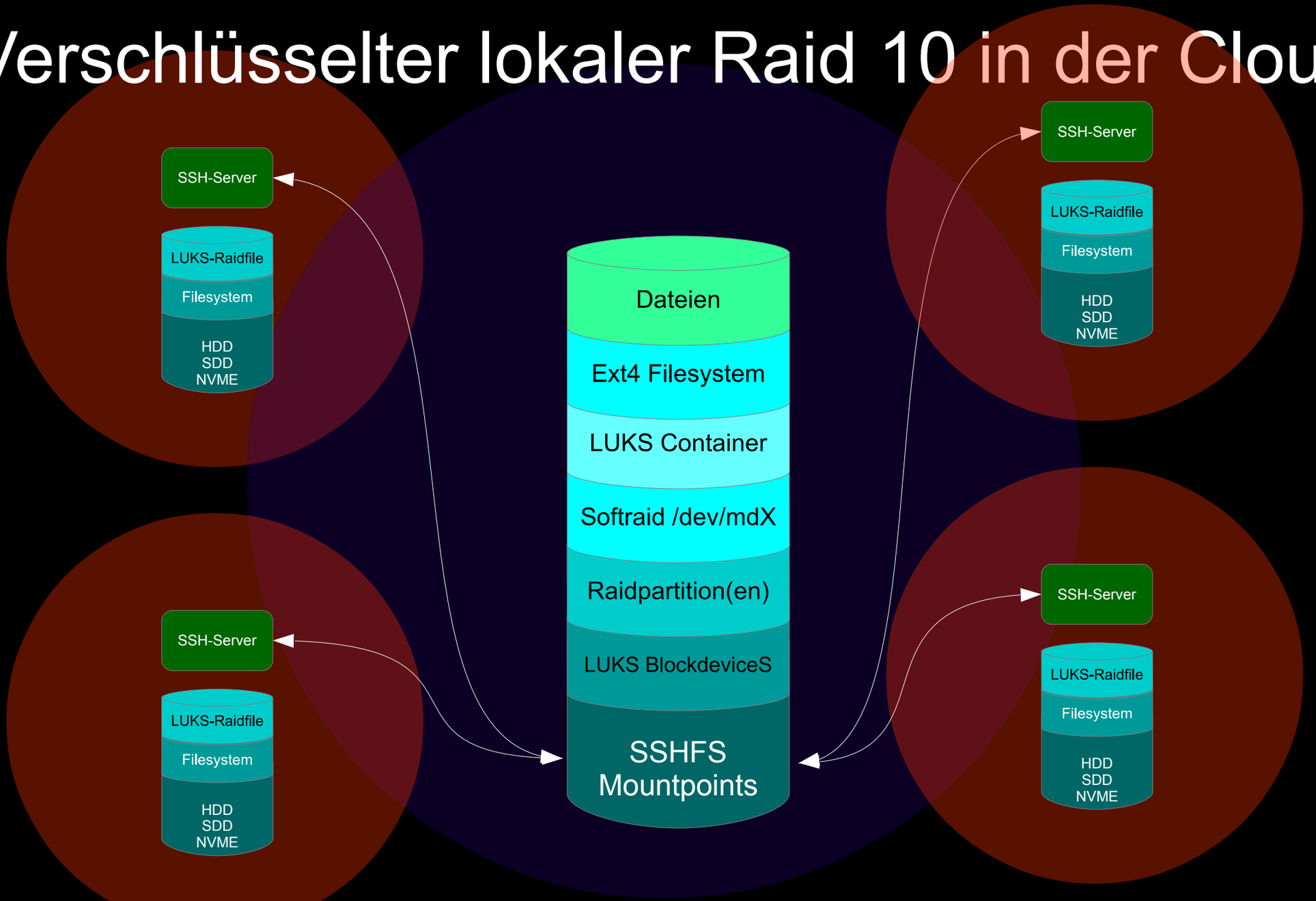


Verschlüsselter lokaler Raid 10 in der Cloud



Marius Schwarz – Stand 12.10.2021 für Linux-am-Dienstag.de

Verschlüsselter lokaler Raid 10 in der Cloud



Marius Schwarz – Stand 12.10.2021 für Linux-am-Dienstag.de

Verschlüsselter lokaler Raid 10 in der Cloud

Webstorage mounten

Verschlüsselter lokaler Raid 10 in der Cloud

Webstorage mounten

Am Beispiel Server „1“

```
sshfs user@server1:/ ~/raid/server1
-o idmap=user -o uid=$(id -u) -o gid=$(id -g) -o allow_root
-o direct_io -o sshfs_sync -o ServerAliveInterval=3
```

Verschlüsselter lokaler Raid 10 in der Cloud

Webstorage mounten

Begriffe

user Benutzername zum Anmelden an Webaccount
server1 Domainname des Webaccounts
~/raid/server1 Verzeichnis wo der Webaccount lokal erreichbar ist
„-o ServerAliveInterval=3“
SSHFS Option zum schnellen Erkennen von Serverfails.

Verschlüsselter lokaler Raid 10 in der Cloud

Webstorage mounten

Die restlichen Optionen dienen dazu...

...daß die Benutzerrechte stimmen.
… daß die Netzwerkaktivitäten optimal ablaufen.
... daß ROOT diese Laufwerke benutzen kann.

Verschlüsselter lokaler Raid 10 in der Cloud

Webstorage mounten

Insgesamt müssen alle 4 (oder wenn ein Spare gewünscht wird, 5)

Webaccounts auf ähnliche Art angebunden werden.

Es empfiehlt sich Verzeichnisse wie
raid/server1 raid/server2 raid/server3 raid/server4
etc. etc. zu verwenden

Verschlüsselter lokaler Raid 10 in der Cloud

Die LUKS-Container vorbereiten

Verschlüsselter lokaler Raid 10 in der Cloud

Die LUKS-Container vorbereiten

Ein Passwortfile nimmt einem viel Tipparbeit ab,
sollte aber nur verwendet werden,
wenn eine aktive Festplattenverschlüsselung vorliegt.

Verschlüsselter lokaler Raid 10 in der Cloud

Die LUKS-Container vorbereiten

Ein Passwortfile nimmt einem viel Tipparbeit ab,
sollte aber nur verwendet werden,
wenn eine aktive Festplattenverschlüsselung vorliegt.

Alle Passwörter können natürlich auch getippt werden.

Verschlüsselter lokaler Raid 10 in der Cloud

Die LUKS-Container vorbereiten

1. Passwortfile erzeugen

```
echo "EinechtellenlangesPasswort" > ~/.config/container.pass
```

Verschlüsselter lokaler Raid 10 in der Cloud

Die LUKS-Container vorbereiten

Ein Containerfile erzeugen

```
fallocate -l 100M raid.luks
```

Verschlüsselter lokaler Raid 10 in der Cloud

Die LUKS-Container vorbereiten

mit LUKS formatieren

```
cat ~/.config/container.pass  | cryptsetup luksFormat raid.luks
```

Verschlüsselter lokaler Raid 10 in der Cloud

Die LUKS-Container vorbereiten

mit cryptsetup den LUKS-Container öffnen

```
cat ~/.config/container.pass | sudo cryptsetup open
PATH_TO_FILE/raid.luks raid
```

Verschlüsselter lokaler Raid 10 in der Cloud

Die LUKS-Container vorbereiten

Das LUKS Blockdevice einrichten

```
sudo parted -a optimal /dev/mapper/raid mklabel msdos

sudo parted -a optimal /dev/mapper/raid mkpart primary ext4 0% 100%

sudo parted -a optimal /dev/mapper/raid set 1 raid on
```

Verschlüsselter lokaler Raid 10 in der Cloud

Die LUKS-Container vorbereiten

Hinweis: parted hat heimlich eine Partition verfügbar gemacht

als /dev/mapper/raid1

Diese muß vor dem LUKS Close entfernt werden.

Verschlüsselter lokaler Raid 10 in der Cloud

Die LUKS-Container vorbereiten

mit cryptsetup den LUKS-Container wieder schliessen

```
sudo dmsetup remove /dev/mapper/raid1
```

```
sudo cryptsetup close /dev/mapper/raid
```

Verschlüsselter lokaler Raid 10 in der Cloud

Die LUKS-Container vorbereiten

Nun den Container 4x zu den Webaccounts kopieren

```
cp raid.luks raid/server1/
cp raid.luks raid/server2/
cp raid.luks raid/server3/
cp raid.luks raid/server4/
...
cp raid.luks raid/serverX/
```

Verschlüsselter lokaler Raid 10 in der Cloud

Die LUKS-Container vorbereiten

Profi Tip:

```
gzip -1 raid.luks

cp raid.luks.gz raid/serverX/

ssh user@serverX “gzip -d raid.luks.gz“
```

Verschlüsselter lokaler Raid 10 in der Cloud

Den Raid zusammenbauen

Verschlüsselter lokaler Raid 10 in der Cloud

Den Raid zusammenbauen

LUKS - Container öffnen

```
cat ~/.config/container.pass | sudo cryptsetup open ~/raid/server1/raid.luks server1
cat ~/.config/container.pass | sudo cryptsetup open ~/raid/server2/raid.luks server2
cat ~/.config/container.pass | sudo cryptsetup open ~/raid/server3/raid.luks server3
cat ~/.config/container.pass | sudo cryptsetup open ~/raid/server4/raid.luks server4
```

Partitionen verfügbar machen

```
kpartx -a /dev/mapper/server1
kpartx -a /dev/mapper/server2
kpartx -a /dev/mapper/server3
kpartx -a /dev/mapper/server4
```

Verschlüsselter lokaler Raid 10 in der Cloud

Den Raid zusammenbauen

Also bauen wir das Software Raid

```
sudo mdadm --create /dev/md0 --level=10 --raid-devices=4  \
/dev/mapper/server1p1 /dev/mapper/server2p1 \
/dev/mapper/server3p1 /dev/mapper/server4p1 ;
```

Verschlüsselter lokaler Raid 10 in der Cloud

Den Raid zusammenbauen

Wir müssen jetzt abwarten, bis das Raid initialisiert ist.

```
sudo mdadm --detail /dev/md0
```

Wenn der Status auf „clean“ geht, ist das Raid bereit.

Verschlüsselter lokaler Raid 10 in der Cloud

Den Raid zusammenbauen

Jetzt noch schnell das Filesystem aufbringen

```
sudo mkfs.ext4 /dev/md0
```

und als Laufwerk einbinden und für alle nutzbar machen

```
sudo mount /dev/md0 raid/platte
sudo chmod 777 raid/platte
```

Verschlüsselter lokaler Raid 10 in der Cloud

Den Raid zusammenbauen

Das eigentliche Dateisystem,

mit dem wir am Ende arbeiten wollen,

ist jetzt bereit.

Verschlüsselter lokaler Raid 10 in der Cloud

Den Raid zusammenbauen

jetzt speichern wir die Information über das Raid noch...

```
sudo mkdir /etc/mdadm/
sudo mdadm --detail --scan > /etc/mdadm/mdadm.conf
```

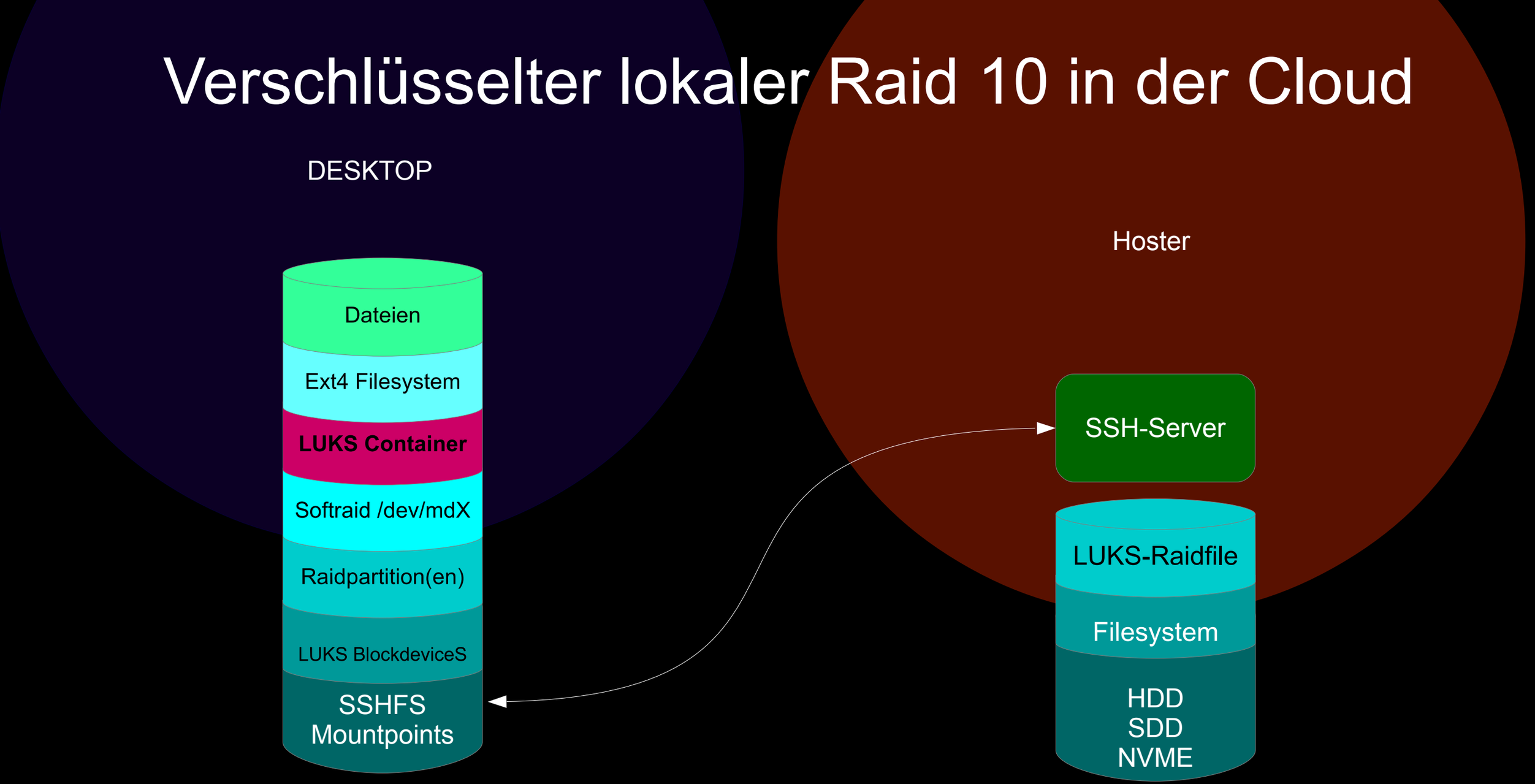
und sind durch.

Verschlüsselter lokaler Raid 10 in der Cloud

Den Raid zusammenbauen

Nun hatten wir in diesem Diagramm noch ein LUKS mehr drin...

Verschlüsselter lokaler Raid 10 in der Cloud



Marius Schwarz – Stand 12.10.2021 für Linux-am-Dienstag.de

Verschlüsselter lokaler Raid 10 in der Cloud

Den Raid zusammenbauen

Diese Lage LUKS Verschlüsselung ist OPTIONAL
da ja die Speicherdateien auf den Servern schon verschlüsselt sind.

Mit den hier vorgestellten Methoden,
sollte es kein Problem für Euch sein,
diese Lage einzufügen.

Verschlüsselter lokaler Raid 10 in der Cloud

Das Raid UNmounten

Verschlüsselter lokaler Raid 10 in der Cloud

Das Raid UNmounten

```
sudo umount ~/raid/platte/
sudo mdadm --stop /dev/md0

for i in {1..X}; do \
sudo dmsetup remove /dev/mapper/server${i}p1;\
sudo cryptsetup close /dev/mapper/server${i};\
fusermount -u ~/raid/server${i}; done
```

wobei X die Anzahl der Server ist, die man benutzt.

Verschlüsselter lokaler Raid 10 in der Cloud

Das Raid mounten

Verschlüsselter lokaler Raid 10 in der Cloud

Das Raid mounten

SSHF Mounts für Server durchführen, dann...

```
for i in {1..X}; do \
cat ~/.config/container.pass | sudo cryptsetup open
/home/benutzername/raid/server$i/raid.luks server$i;
sudo kpartx -a /dev/mapper/server$i; done
```

```
sudo mdadm --assemble /dev/md0
sudo mount /dev/md0 /home/benutzername/raid/platte
```

wobei X die Anzahl der Server ist, die man benutzt.

Verschlüsselter lokaler Raid 10 in der Cloud

Das Raid mounten

Eigentlich eine einfache Prozedur.

Verschlüsselter lokaler Raid 10 in der Cloud

Dem Raid einen Spare hinzufügen

Verschlüsselter lokaler Raid 10 in der Cloud

Dem Raid ein Spare hinzufügen

Bei laufendem Raid einfach ...

sudo mdadm /dev/md0 --add /dev/mapper/serverXp1

Wobei selbstverständlich vorher der Webaccount angebunden, das Raidfile erzeugt und vorbereitet werden muß.

Verschlüsselter lokaler Raid 10 in der Cloud

Nachbetrachung

Verschlüsselter lokaler Raid 10 in der Cloud

Der an sich in Einzelschritten nicht komplizierte,
aber in Masse doch recht aufwendige Prozess einen Raid 10
mit Cloudhostern zu bauen,

Zeichnet sich durch die Redundanz aus, denn...

Verschlüsselter lokaler Raid 10 in der Cloud

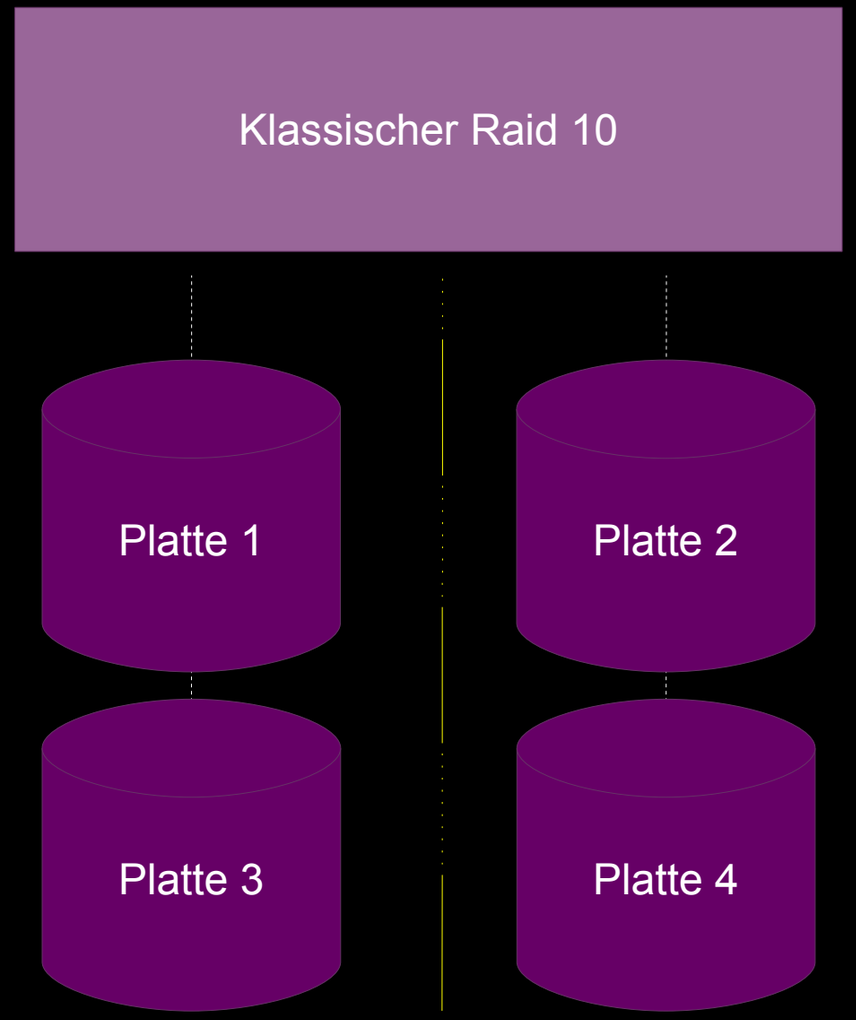
…die Cloudhoster backupen täglich die Daten.
…es reichen 2 der Hoster aus um die Daten wieder verfügbar zu machen.

Verschlüsselter lokaler Raid 10 in der Cloud

ABER

Verschlüsselter lokaler Raid 10 in der Cloud

Fallen die zwei Hoster mit den Platten 1+2 gleichzeitig aus, ist das Raid unwiederbringlich zerstört.



Verschlüsselter lokaler Raid 10 in der Cloud

Aber natürlich kann man das Spielchen mit beliebig vielen Hostern und Kopien spielen ;)

Verschlüsselter lokaler Raid 10 in der Cloud

Danke fürs Zuhören.