

1. **Installation und Startkonfiguration**(Benutzername, IP-Adresse, WOL, Zeitserver)
2. Verwalten der **Updates**
3. **Erweiterungen** inkl. OMV-Extras
4. Konfigurieren des **Benachrichtigungssystems** (das NAS sendet dann bei Fehlern eine E-Mail)
5. **Raids** (Erstellen, Erweitern, Wiederherstellen, Austausch von defekten Festplatten)
6. **S.M.A.R.T.** Überwachung der Festplatten
7. **Spindown** (Ausschalten) der Festplatten bei Nichtbenutzung
8. **AutoShutDown** (Ruhemodus) des ganzen Systems bei Nichtbenutzung
9. **Freigaben**
10. **MySQL** installieren
11. **Backup** des Systemdatenträgers ohne Datenfestplatten
12. **OpenMediaVault First Aid - Erste Hilfe**
13. **Installation des Backports Kernels**
14. **SnapRAID**
15. **Wissenswertes, Tipps und Hinweise**
16. **Hardware-Empfehlung**
17. **Historie dieser Anleitung**

1.1 - Benötigte Software

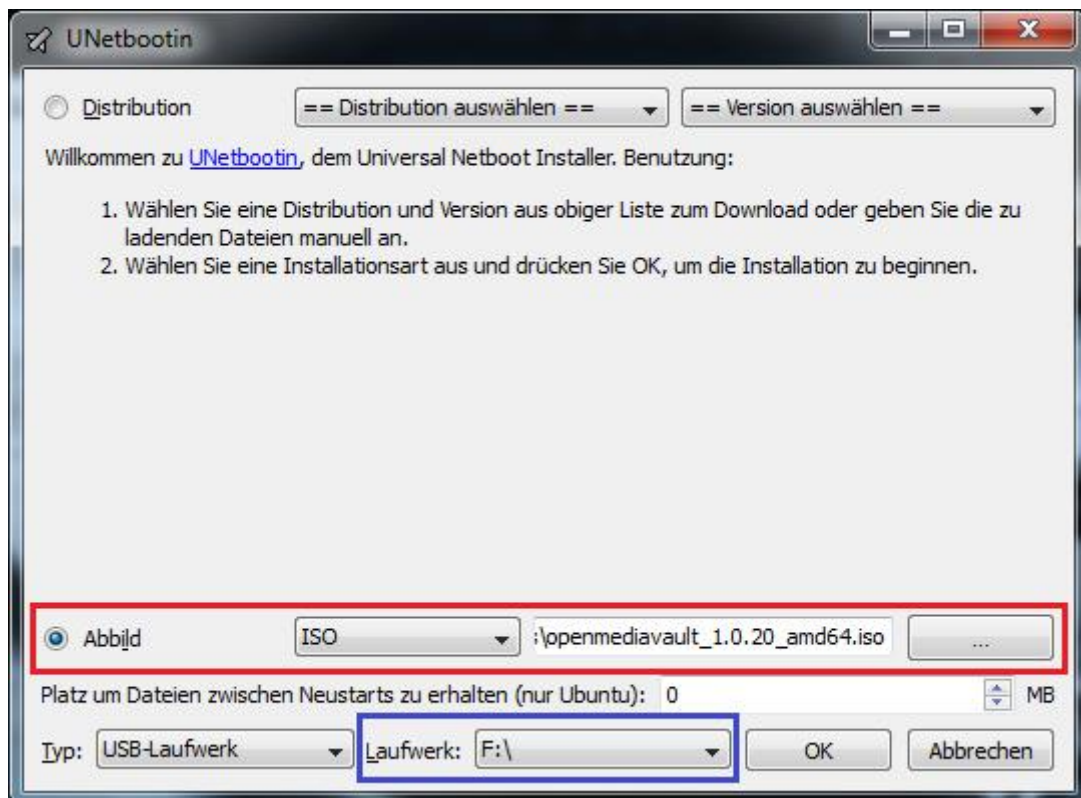
OpenMediaVault in der [neusten Version](#). Ich empfehle die 64bit Version ([Direktdownload der v2.1 vom August 2015](#))

Nun benötigen wir noch ein Tool um das heruntergeladene ISO auf einem USB-Stick zu kopieren und diesen bootfähig zu machen. Hierfür empfehle ich die Freeware [UNetBootin](#) für Windows, Linux oder MacOS

[WOLCmd](#) - Wake-On-Lan für Windows 7/8.1/10 Clients - Damit könnt ihr euer schlafendes OpenMediaVault NAS aufwecken.

1.2 - Erstellung des USB-Boot-Sticks für die Installation

Ihr benötigt einen USB-Stick mit mindestens 4GB Speicher. Formatiert den USB-Stick im **FAT32** Format. Nachdem ihr das ISO von OpenMediaVault sowie UnetBootIn heruntergeladen habt, startet ihr UnetBootIn und wählt Abbild aus. Wählt nun die ISO von OpenMediaVault und unten ein Ziel (USB-Stick) aus. Der Vorgang dauert je nach Stick zwischen 1-5 Minuten.

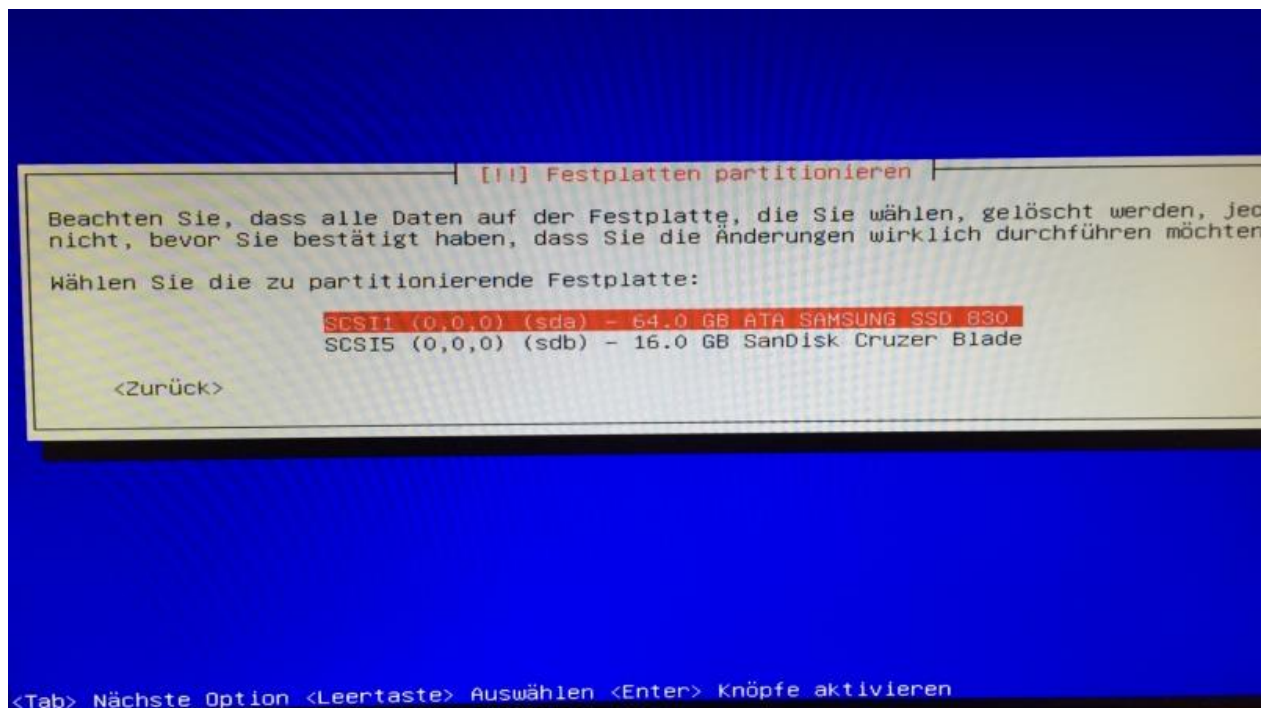


1.3 - Installation von OpenMediaVault von einem USB-Stick

Nachdem ihr den Boot-Stick mit erstellt habt, könnt ihr von diesem Stick booten und OpenMediaVault auf einer Festplatte, einer SSD oder einem zweiten USB-Stick installieren. Aufgrund des Stromverbrauches würde ich von einer gewöhnlichen Festplatte abraten und zu einer SSD tendieren.

Der Installationsassistent ist zwar optisch nicht gerade hübsch, erfüllt aber seinen Zweck und ist einfach und ohne Maus zu bedienen. Nachdem man die gewünscht Sprache gewählt hat, kann man noch eine lokale Domain (nur für Firmenumgebungen interessant) sowie ein Root-Passwort festlegen.

Danach muss der Zieldatenträger für das System gewählt werden (es wird automatisch die ganze Festplatte genutzt):



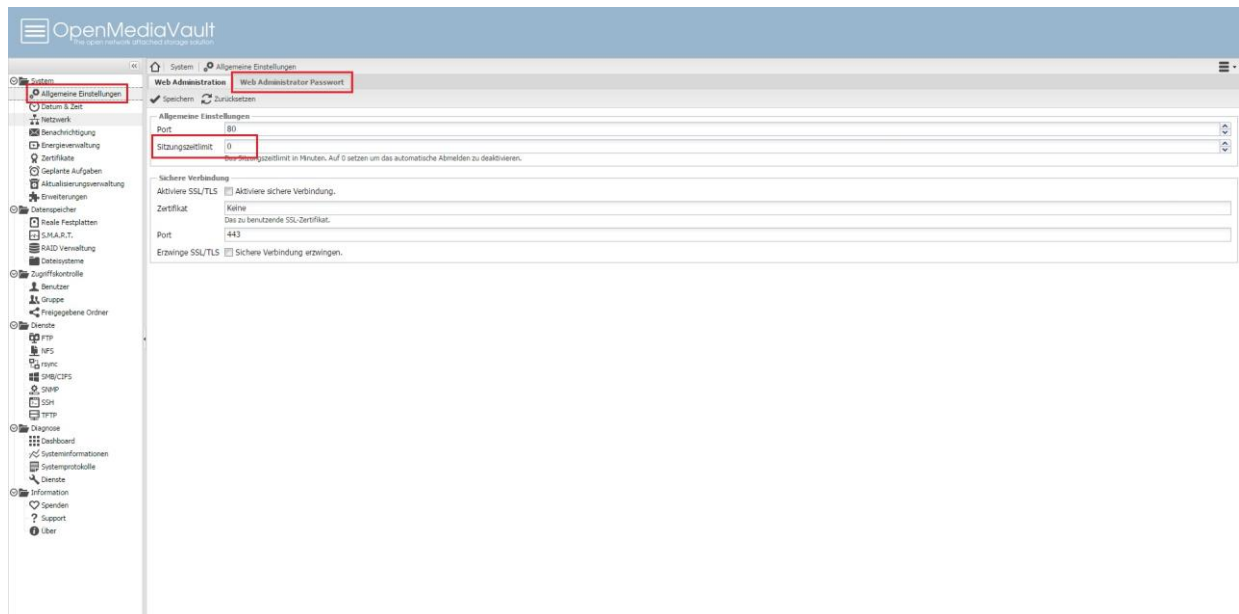
Hinweis: Der Bootloader GRUB2 von Linux versucht sich immer automatisch auf die 1. Festplatte (sda) zu installieren. Ich empfehle daher bei der Installation von OpenMediaVault nur den Installationsstick und den zukünftigen Systemdatenträger einzustecken. Alle anderen Festplatten, die später nur die Daten beherbergen, sollten noch nicht angeschlossen werden!

Da hinter OpenMediaVault ein Debian Linux steckt, darf man während der Installation ein Debian-Repository für automatische Updates auswählen, auch die Verwendung eines Proxys ist möglich. Danach ist die Installation auch schon abgeschlossen.

1.4 - Startkonfiguration

Nachdem OpenMediaVault installiert wurde, könnt ihr euch nun **über einen anderen PC** auf der Weboberfläche von OpenMediaVault anmelden. Dazu könnt ihr jeden aktuellen Browser benutzen, ich empfehle z.B. [Chrome von Google](#).

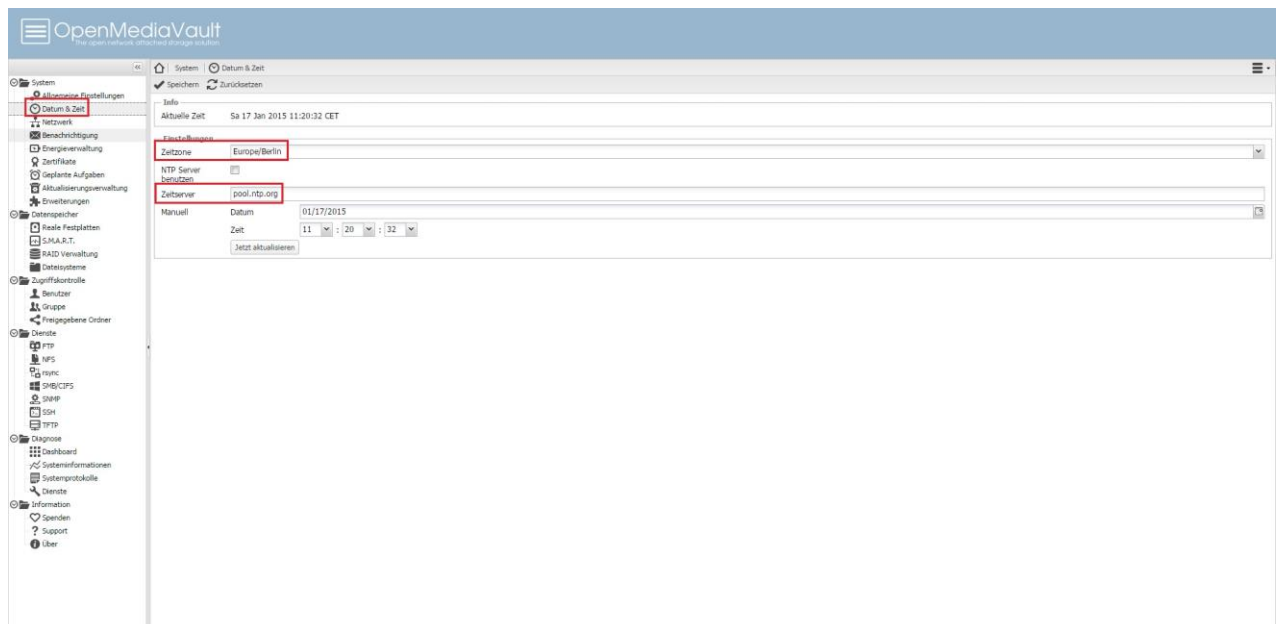
Meldet euch zunächst mit dem Benutzer **admin** und dem Passwort **openmediavault** an. Klickt im linken Menü auf **Allgemeine Einstellungen** und ändert das **Sitzungslimit** auf **0**, damit werdet ihr nicht mehr automatisch abgemeldet. Diese Einstellung ist meine persönliche Präferenz und optional, stellt hier ein was ihr für euch am geeignetsten empfindet.



*Nicht vergessen: Nach jeder Änderung müsst ihr auf die **Speichern** Schaltfläche klicken um die Änderung zu übernehmen!*

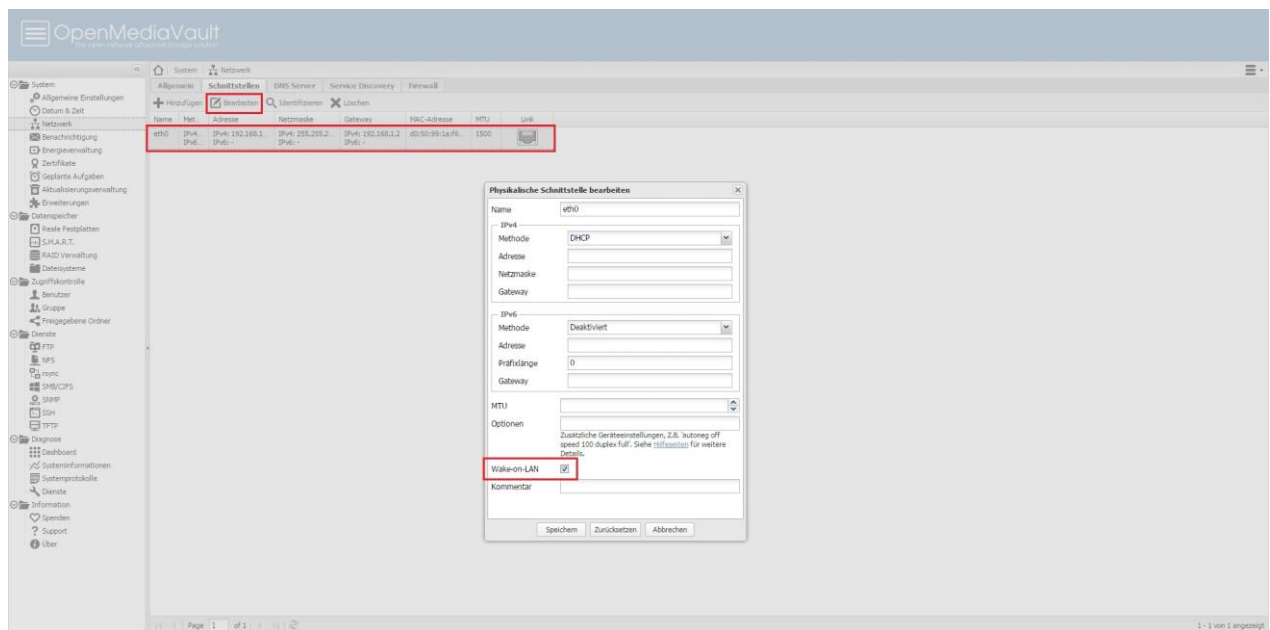
Anschließend klickt ihr oben auf den Reiter **Web Administrator Passwort**. Wählt hier ein neues Passwort aus, die Verwendung des Standardpasswortes sollte möglichst von kurzer Dauer sein.

Klickt nun links auf **Datum & Zeit** und vergewissert euch, dass alle Einstellungen korrekt sind. Eine korrekte Zeit ist bei System- und Fehlermeldungen später unerlässlich.



Im letzten Schritt der Startkonfiguration überprüfen wir die Netzwerkeinstellungen. Klickt dazu links auf **Netzwerk** und dann auf den Reiter **Schnittstellen**. Wählt eure aktive Netzwerkkarte aus und klickt auf **Bearbeiten**. Hier könnt ihr die IP-Adresse des NAS festlegen, DHCP bedeutet, dass euer Router dem NAS automatisch eine IP-Adresse zuweist. Zudem lässt sich hier die Wake-On-Lan Funktionalität von

OpenMediaVault aktivieren.

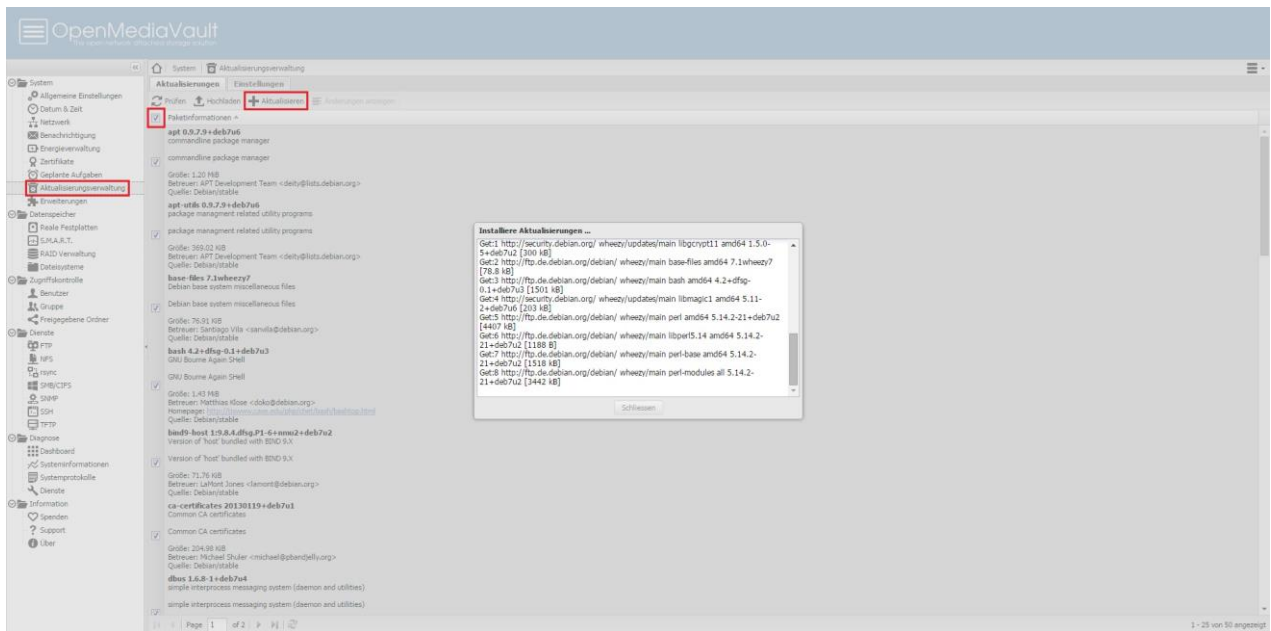


Da ein NAS meist eine feste IP-Adresse hat, könnt ihr entweder in OpenMediaVault die IP-Adresse auf **Statisch** stellen und eine freie IP-Adresse in eurem Netzwerk eingeben oder - und das ist die bessere Methode - die IP-Adresse über euren Router konfigurieren. Verwendet ihr z.B. eine Fritzbox, findet ihr den Eintrag unter **Heimnetz** und dort **Bearbeiten** der IP-Adresse des NAS.



2. - Verwalten von Updates

Zuerst empfiehlt es sich über die **Aktualisierungsverwaltung** die neuesten Pakete aus dem Debian Repository nachzuladen. Dazu reicht ein Klick auf den **Aktualisieren** Button der sich oben in der Aktualisierungsverwaltung befindet.



3. - OpenMediaVault Erweiterungen

In OpenMediaVault habt ihr die Möglichkeit weitere Programme nachzuinstallieren. Folgendes ist möglich:

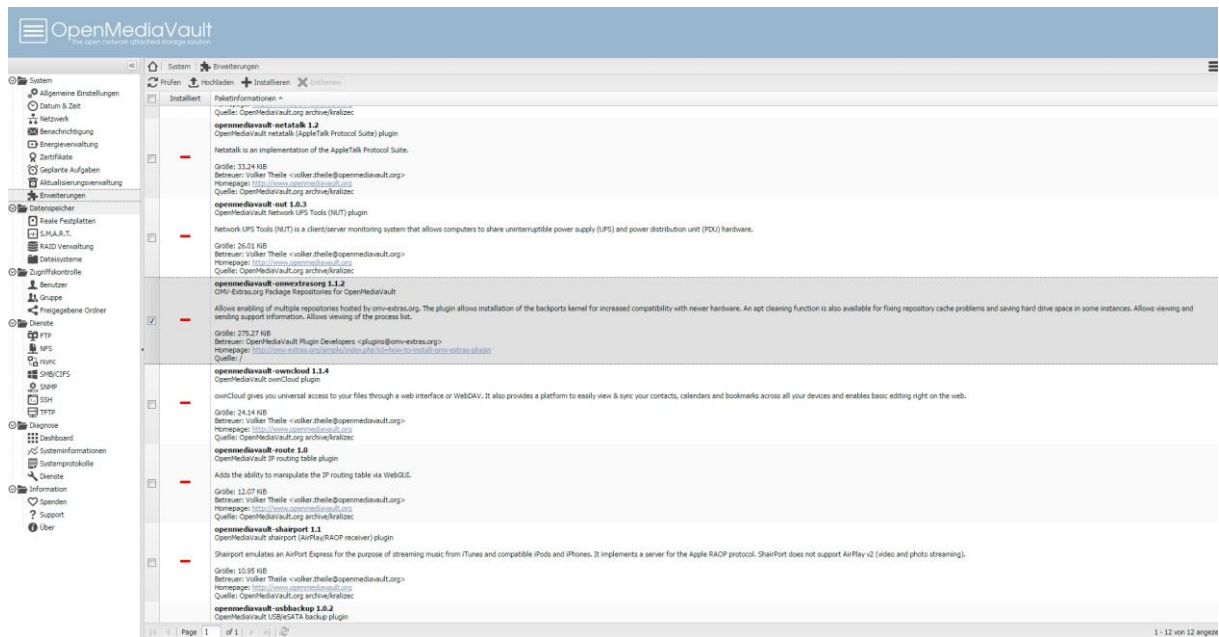
Erweiterung	Bemerkung
ClamAV	Virenschanner
Forked-DAAPd	iTunes kompatibler DAAP Media Server
iSCSI Enterprise Target	iSCSI über TCP
LDAP	Benutzerauthentifizierung via LDAP
LVM	Level Volume Management für Firmen

NetaTalk	AppleTalk
Network UPS Tools	Support für Unterbrechungsfreie Stromversorgungen
OwnCloud Server	Unterstützt Web Interface und WebDAV
Route	Einfache Verwaltung von IP-Routing-Tabellen
Shairport / AirPlay Server	Emuliert einen AirPort Express um Music via iTunes auf Applegeräte zu streamen
USB Backup	Automatische Synchronisation / Backup mit einem externen USB Datenträger

3.1 - Installation von OMV-Extras

Um noch mehr Erweiterungen freizuschalten, sollte das Plugin von OMV-Extras.org nachinstalliert werden. Dies lohnt sich meiner Meinung nach schon alleine für das Autoshtutdown Plugin auf welches ich gleich eingehen möchte. Doch zuvor muss wie gesagt erst das OMV-Extras Plugin installiert werden.

1. Ladet euch das OMV-Extras Plugin herunter: [Download](#).
2. In der OpenMediaVault Weboberfläche navigiert ihr zu den Erweiterungen, klickt auf die Button "Hochladen" und wählt das heruntergeladene OMV-Extras Plugin aus.
3. In den Erweiterungen sollte nun ein neuer Eintrag mit dem Namen "openmediavault-omvextrasorg" existieren. Hakt diesen Eintrag an und klickt oben auf die Schaltfläche "Installieren".



Die Installation dauert ca. 1 Minute. Danach sollten deutlich mehr Einträge unter dem Punkt Erweiterungen zu finden sein:

Erweiterung	Bemerkung
Anacron	Fehlgeschlagene Cron-Jobs werden automatisch nachgeholt
AUFS	AUFS Dateisystem
AutoShutDown	Versetzt das NAS bei Nichtgebrauch in den Standby
Backup	Erstellt ein Backup der Systemfestplatte
Calibre	E-Book Management
CUPS	Netzwerk Management für Drucker
Downloader	HTTP/HTTPS/FTP/BitTorrent Downloader
Extplorer / Links	Hinzufügen von Links zum OMV Webinterface
miniDLNA	DLNA / UPnP Server
Mumble Server	Kostenlose Sprachkonferenzsoftware
MySQL	MySQL Datenbank
Nginx	Webserver
RemoteShare	Verbinden mit entfernten SMB/CIFS oder NFS Freigaben
Roundcube	IMAP client

rsnapshot	Ermöglicht inkrementale, rotierende Backups
SnapRaid	Backup/Raid-Ersatz speziell für größere Dateien auf einem Raid
Transmission	BitTorrent client
WOL	Senden von magic pakets (aufwecken von anderen Computern)
Wordpress	Websoftware zur Erstellung eines eigenen Blogs

Wie man sieht ist die Auswahl nun deutlich größer. Über den neuen Menüpunkt "OMV-Extras.org" könnt ihr sogar noch mehr Paketquellen auswählen.

Hinweis: Auch wenn OpenMediaVault sehr unempfindlich gegen einen Virusbefall ist, empfehle ich euch den kostenlosen VirenScanner ClamAV zu installieren. Auch wenn die meisten Viren keinen Schaden an euren NAS anrichten können, könnte es sein das ein Client - z.B. mit Windows Betriebssystem - eine infizierte Datei von eurem NAS herunterlädt und sich infiziert. Daher ist der Einsatz eines Virenschanners auch auf einem Linux Betriebssystem wie OpenMediaVault zu empfehlen.

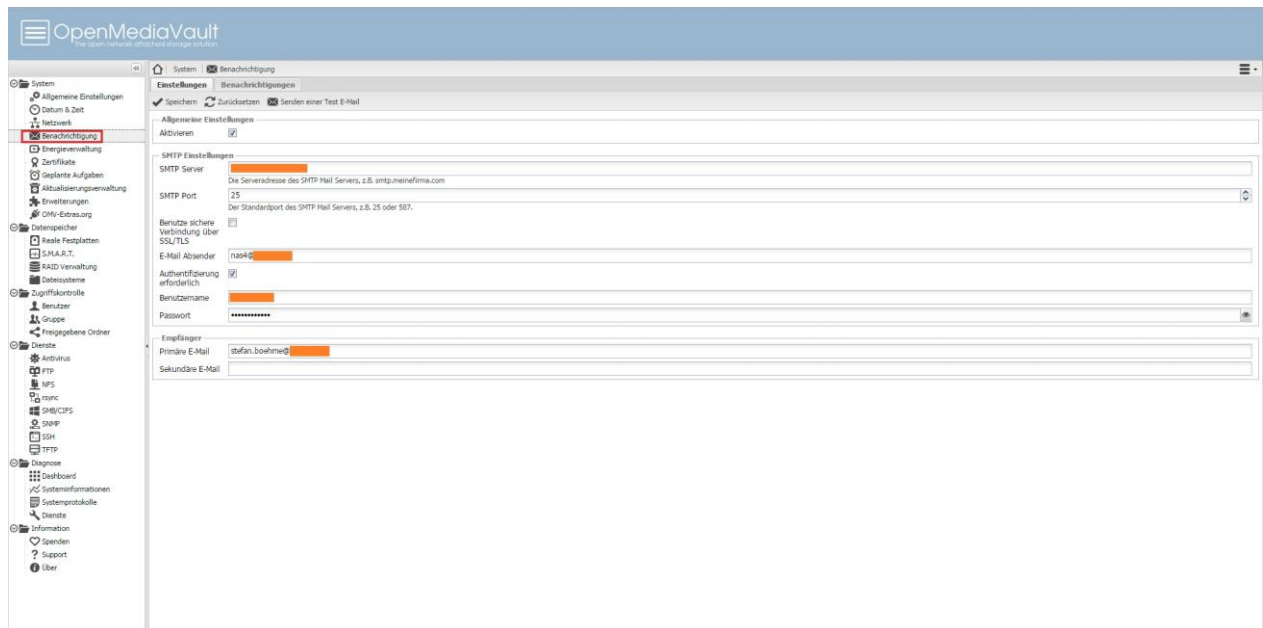
Nachdem ihr die Erweiterung ClamAV installiert habt, müsst ihr den Virenscanner noch im Menü unter dem Punkt **Antivirus** aktivieren! Wenn ihr möchtet, könnt ihr hier auch festlegen ob bestimmte Verzeichnisse regelmäßig geprüft werden sollen.

4 - Benachrichtigungsfunktion konfigurieren

OpenMediaVault kann euch bei einem Fehler automatisch durch den Versand einer E-Mail benachrichtigen. Da man sich ja nicht täglich auf sein NAS einloggt, ist dies sehr zu empfehlen um möglichst schnell auf einen Ausfall reagieren zu können. Alles was ihr dafür benötigt ist ein E-Mail Account bei einem Provider eurer Wahl.

Klickt im Menü links auf Benachrichtigung und gebt euren SMTP-Server und (meist benötigt) euren Benutzernamen und das Passwort für diesen Account ein. Am Besten erstellt ihr euch einen neuen E-Mail Account mit einer eindeutigen Absenderadresse, z.B. nasxxx@euredomain.de oder so ähnlich.

Gebt unten bei Empfänger dann noch eure E-Mail Adresse ein, an die die Nachrichten geschickt werden sollen. Unter dem Reiter Benachrichtigungen könnt ihr festlegen ob ihr auch bei anderen Ereignissen informiert werden möchtet.

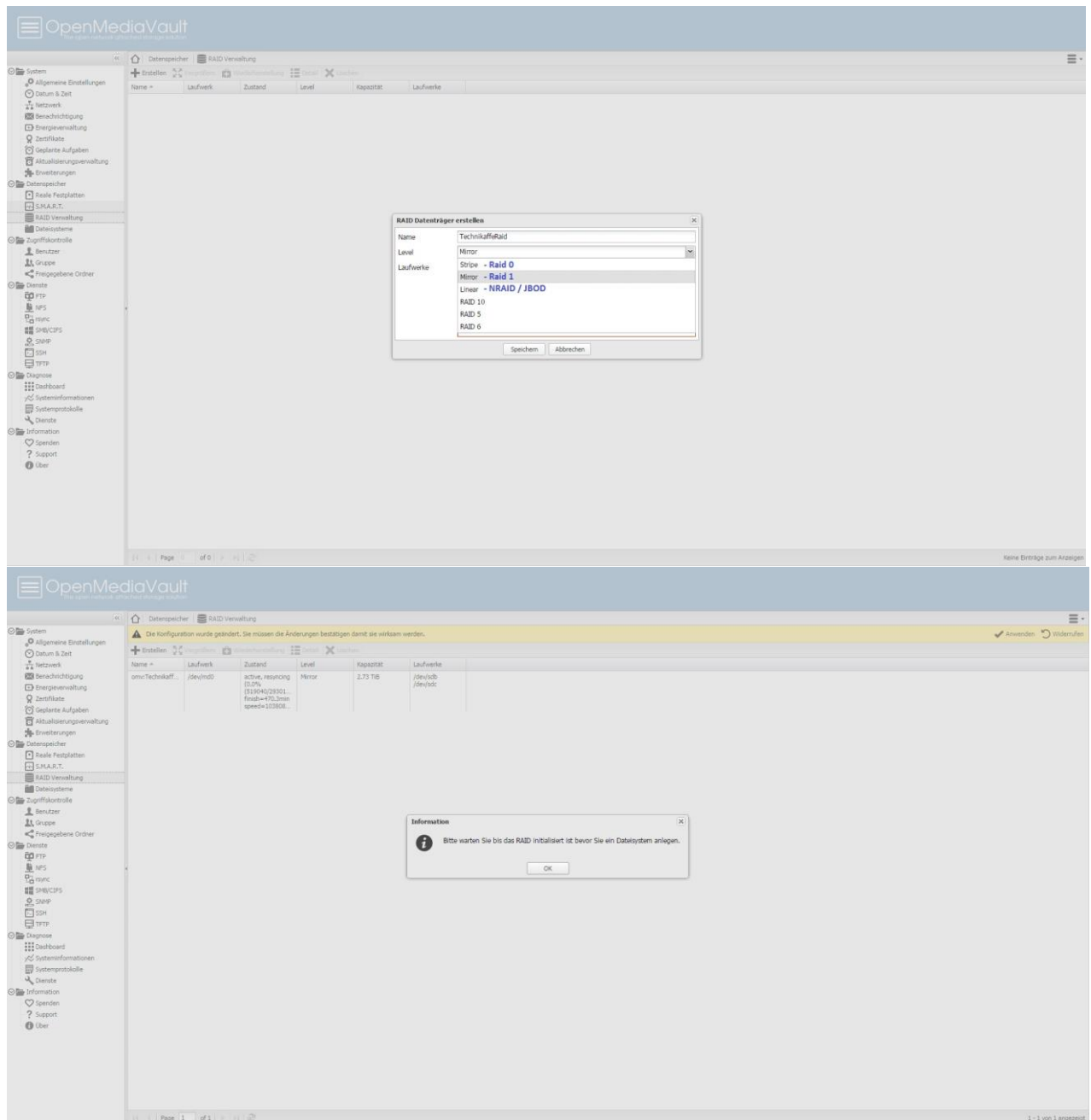


5 - Raids unter OpenMediaVault

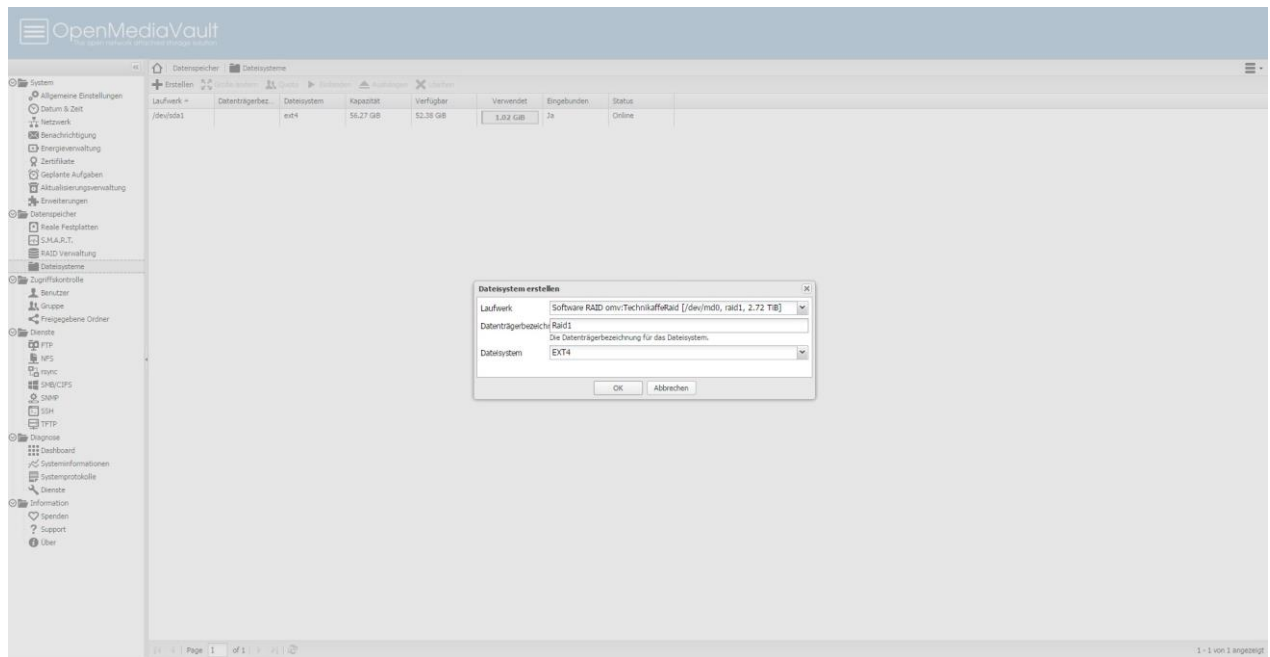
Ein Raid ist ein Verbund aus mehreren Festplatten. Ein Raid wird in einem NAS meist eingesetzt um eine erhöhte Ausfallsicherheit der Festplatten zu gewährleisten. Es gibt mehrere Raid-Arten, für welche ihr euch entscheidet liegt bei euch, üblich sind Raid-1 für kleinere NAS-Systeme oder Raid-5 und Raid-6 für NAS-Systeme mit mehr als 3 Festplatten. Ab 5 Festplatten empfehle ich einen Raid-6. Mehr Infos über die [Raid-Level findet ihr bei Wikipedia](#).

5.1 - Einrichtung eines Raids

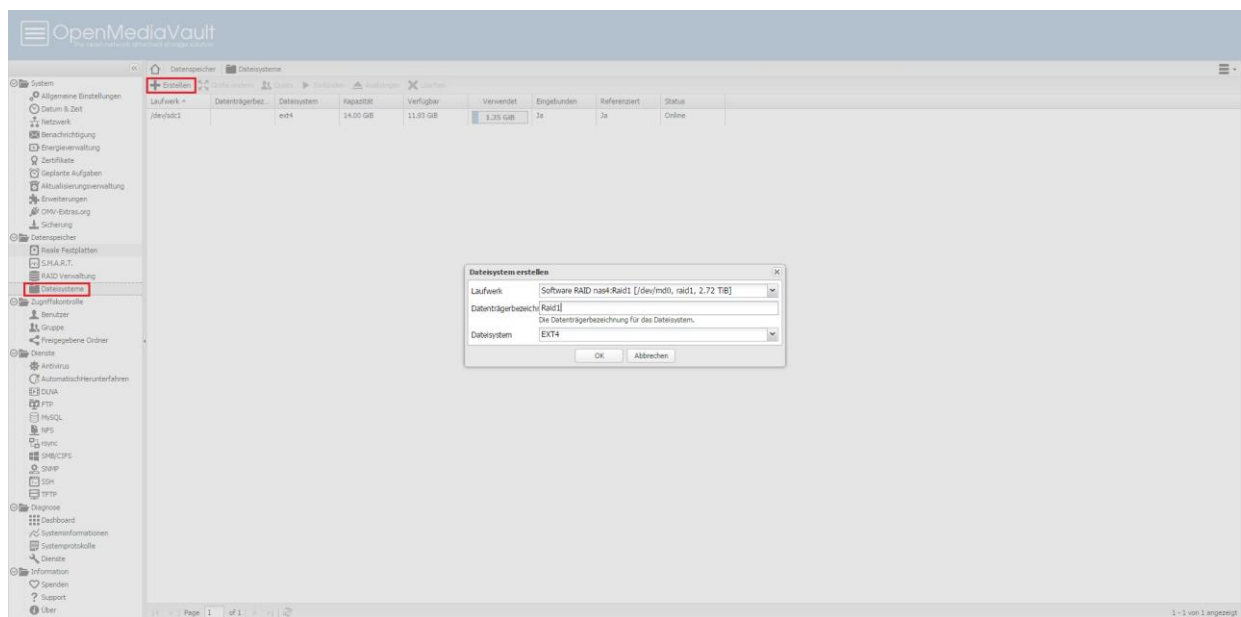
Über die RAID Verwaltung lässt sich aus den Datenfestplatten mit Leichtigkeit ein Raid-Verbund erstellen. Dazu wählt man zuerst den gewünschten Raid-Typ (Raid 0,1,5,6 oder JBOD) aus.



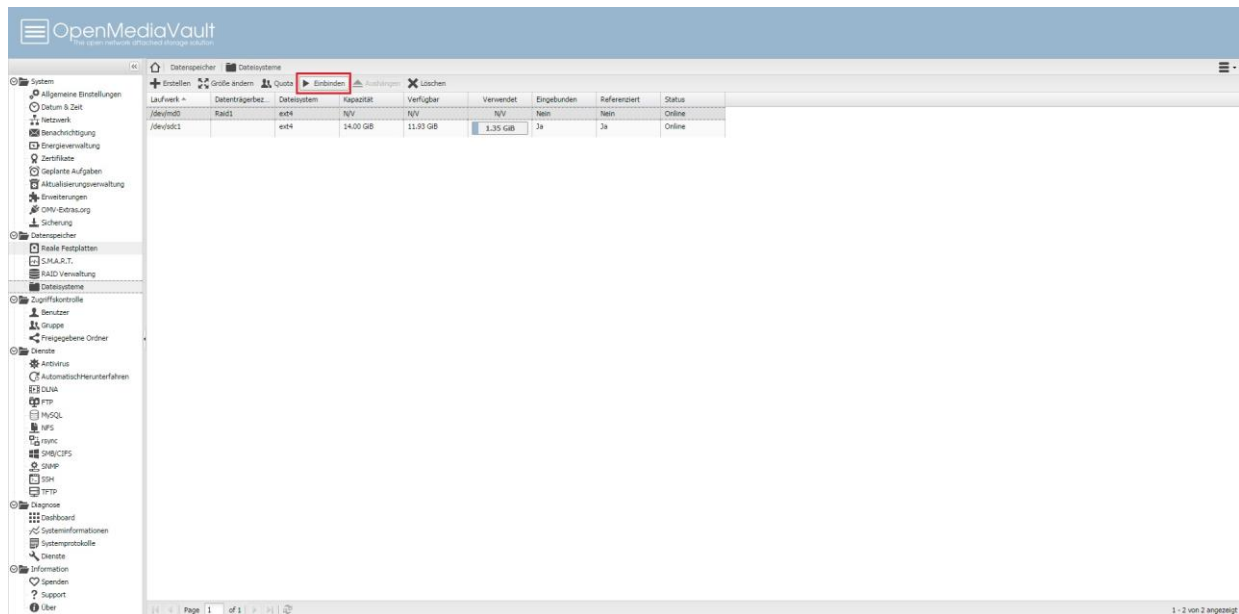
Ist der Raid erstellt, muss dieser zunächst initialisiert werden, was ca. 3 Stunden pro Festplatte (also 6 Stunden bei 2 Festplatten und 12 Stunden bei 4 Festplatten) dauert.



Im Anschluss kann dann ein Dateisystem (ich empfehle Ext4) angelegt werden. Klickt dazu auf den Menüpunkt **Dateisysteme** und dort auf die Schaltfläche **Erstellen**.

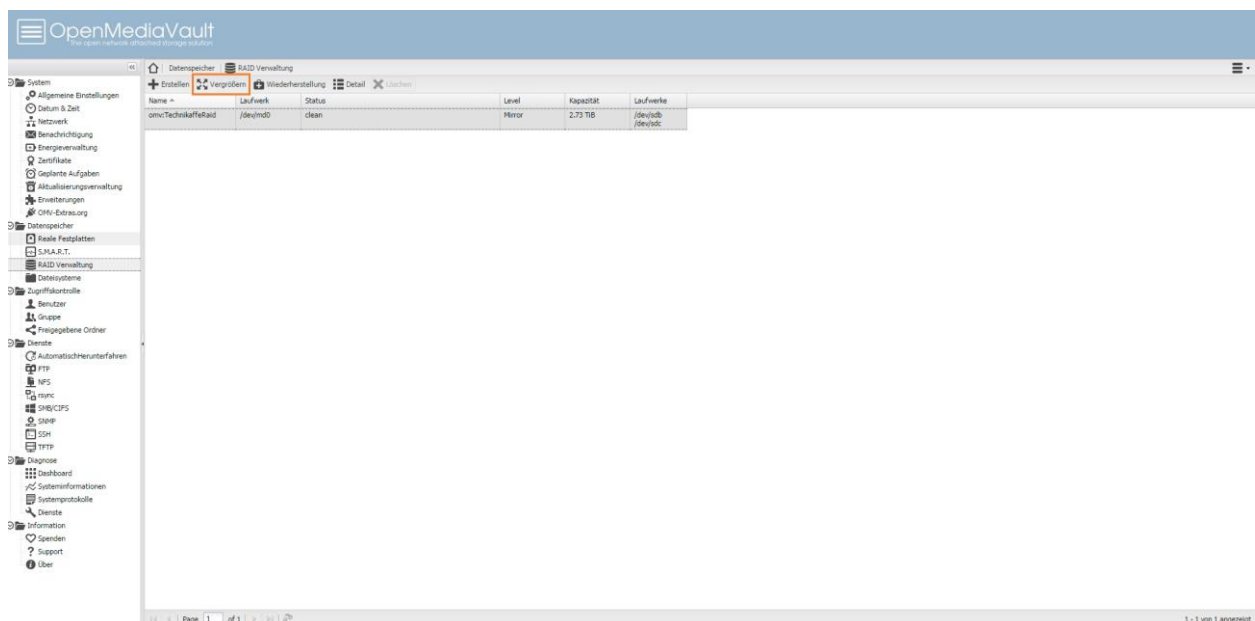


Nach dem Anlegen des Dateisystems muss der Raid noch eingebunden werden - ansonsten ist dieser nicht nutzbar.



5.2 - Raid nachträglich vergrößern

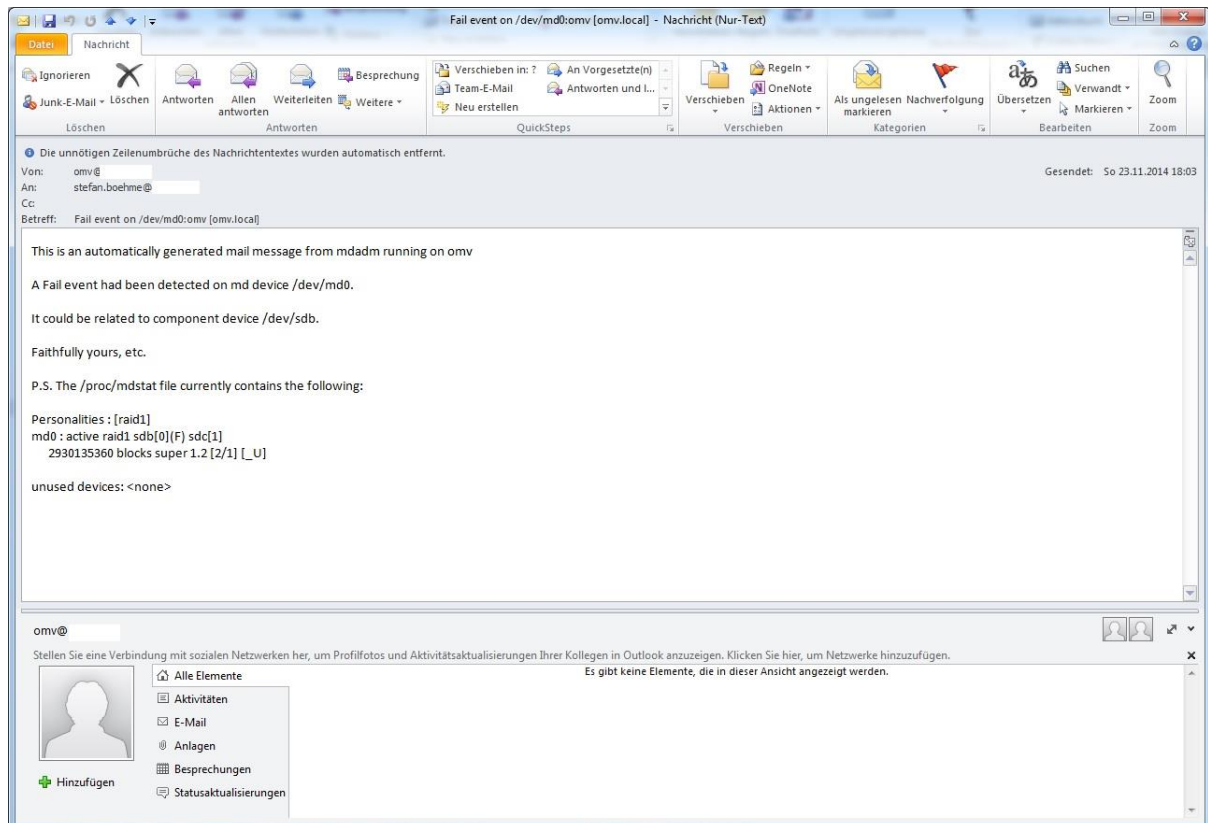
Sollte der Speicherplatz mit der Zeit nicht mehr ausreichen, ist es möglich den Raid-Verbund nachträglich - und ohne Datenverlust - um eine oder mehrere Festplatten zu erweitern. Dies ist allerdings nur bei einem 5 oder 6 möglich.



Nachdem eine neue Festplatte hinzugefügt wurde muss unter dem Punkt "Dateisysteme" die Partition des Raids auf die nun neue Größe erweitert werden. Dies geschieht alles ohne Datenverlust.

5.3 - Defekte Festplatte austauschen

Fällt in eurem NAS eine Festplatte aus, solltet ihr über die Benachrichtigungsfunktion von OpenMediaVault über diesen Ausfall informiert werden. Wie ihr die Benachrichtigungsfunktion konfiguriert, steht weiter unten in dieser Anleitung. Die Nachricht sollte dann so aussehen:



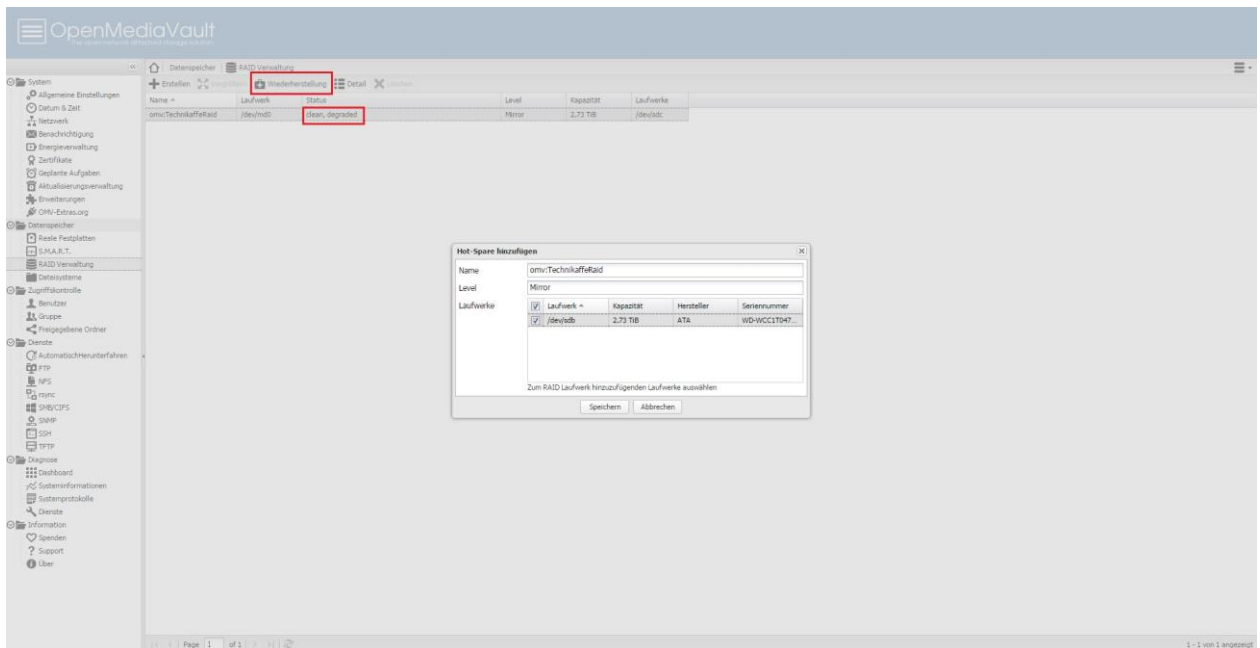
Ist die Festplatte zum ersten Mal auffällig geworden und funktioniert diese noch, könnt ihr der Festplatte eine zweite Chance geben. Überprüft auch die S.M.A.R.T. Werte der Festplatte. Ganz gleich ob ihr die alte Festplatte wieder einbaut oder euch für eine neue Festplatte entscheidet, die RAID-Verwaltung von OpenMediaVault erwartet nun eine Aktion.

Fahrt zuerst OpenMediaVault herunter, schließt dann die neue Ersatzfestplatte an und startet euer NAS. Benutzt die in OpenMediaVault angezeigte Seriennummer der Festplatte um zu verifizieren, dass ihr auch die richtige Festplatte erwischt!

In der RAID-Verwaltung steht bei eurem RAID-Verbund nun "clean, degraded" was aussagt, dass der Ausfallschutz im Raid nicht mehr gewährleistet ist, da mindestens eine Festplatte aus dem Verbund entfernt wurde.

Klickt im linken Menü nun auf den Punkt "Reale Festplatten" und löscht die ausgefallene Festplatte (schnell). Dies ist notwendig, damit wir diese Festplatte im Anschluss wieder in den Raid-Verbund aufnehmen können. Anschließend benutzt ihr in der RAID-Verwaltung die Funktion **Wiederherstellung** um die neue Festplatte

dem Raid hinzuzufügen.



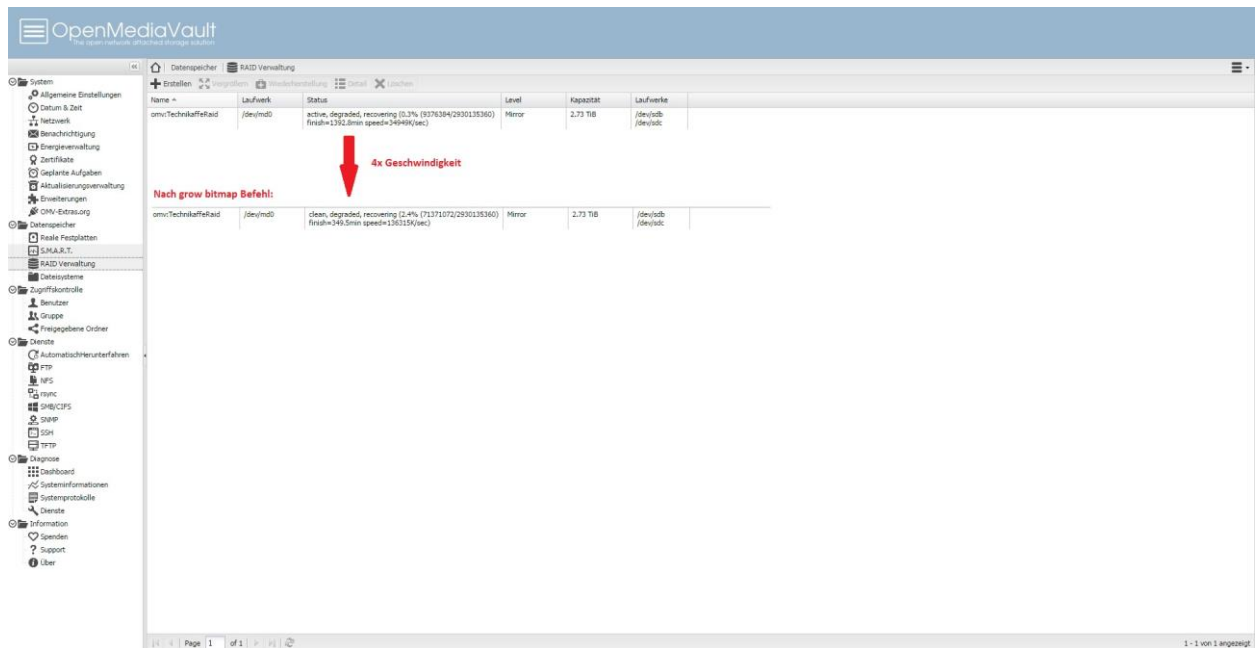
Der Rebuild des Raids (also die Wiederaufnahme der ausgefallenen Festplatte) kann je nach Raid-Level bis zu 48 Stunden dauern. Die hohe Rebuilddauer ist eigentlich der einzige wirkliche Nachteil bei einem Software Raid (ein guter Hardware Raidcontroller ist 5x so schnell). Die etwas höhere CPU-Auslastung beim Datenzugriff ist in einem privaten NAS uninteressant und zu vernachlässigen.

Doch es gibt Abhilfe: Mittels eines kleinen Befehls über die Konsole lässt sich die Rebuild-Geschwindigkeit vervierfachen:

```
sudo mdadm --grow --bitmap=internal /dev/md0
```

nach dem Rebuild nimmt man dem Befehl dann wieder zurück:

```
sudo mdadm --grow --bitmap=none /dev/md0
```



Führt diesen Befehl unbedingt VOR der Wiederherstellung aus. Durch diesen Befehl lässt sich die Rebuild-Dauer deutlichst beschleunigen, meist hat der Befehl eine Verdrei- bis Vervierfachung der Geschwindigkeit zur Folge. Den Befehl muss man nur zurücknehmen, wenn man eine Verschlechterung der Raid-Performance nach dem Rebuild feststellen sollte. Bei mir war dies nicht der Fall, also habe ich die Bitmap weiterhin aktiviert gelassen.

Während des Rebuilds kann der Raid weiterhin benutzt werden und das NAS kann auch zwischendurch neugestartet oder heruntergefahren werden, der Rebuild wird nach dem Neustart an der Stelle fortgesetzt. Im wirklichen Ernstfall würde ich allerdings dazu raten das NAS während eines Rebuild nicht zu benutzen um die Wahrscheinlichkeit eines weiteren Ausfalls zu verringern.

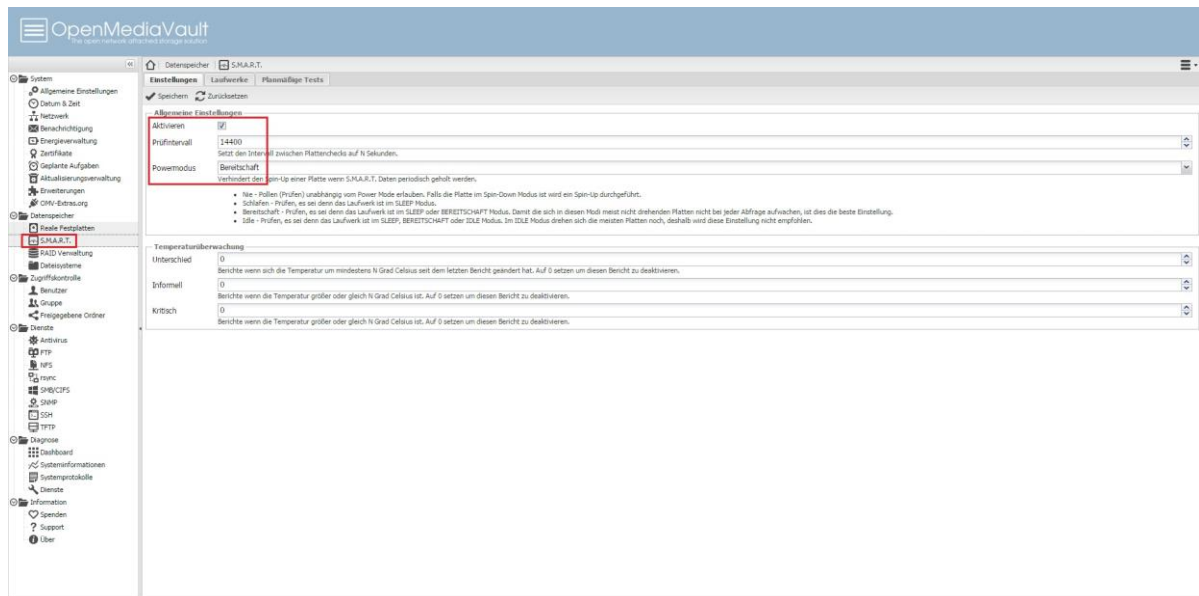
Solltet ihr ein AutoShutDown Script (Erklärung weiter unten in dieser Anleitung) benutzen, empfiehlt es sich dieses während des Rebuilds zu deaktivieren, damit das NAS den Rebuild zügig und in einem Stück durchführt.

6 - S.M.A.R.T. für Ausfallvorhersagen nutzen

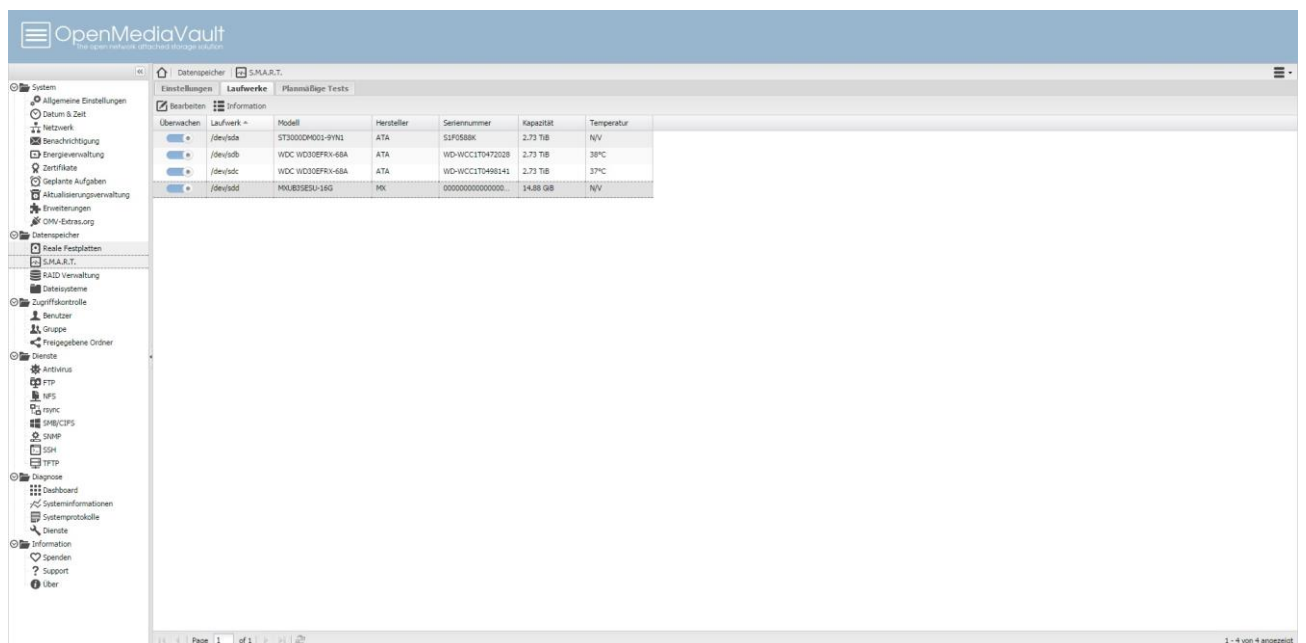
S.M.A.R.T steht für Self-Monitoring, Analysis and Reporting-Technology und beschreibt einen in Festplatten eingebauten Standard. Die Festplatte kann unter einem Betriebssystem ausgelesen und die S.M.A.R.T-Werte analysiert werden.

Laut einer Google Studie aus dem Jahr 2007, bei der Ergebnisse von mehr als 100.000 Festplatten ausgewertet wurden, lassen sich rund 2/3, also 66% aller Festplattenausfälle durch S.M.A.R.T. vorhersagen. Daher macht es Sinn die S.M.A.R.T. Überwachung von OpenMediaVault zu aktivieren.

Klickt auf **S.M.A.R.T.** und setzt einen Haken bei aktivieren. Möchtet ihr die Festplatten alle 4 Stunden prüfen, wählt bei **Prüfintervall** 14400 (60 [Sekunden] * 60 [Minuten] * 4 [Stunden]) aus. Der Powermodus sollte auf **Bereitschaft** stehen, damit eure Festplatten nicht bei jeder Prüfung geweckt werden.



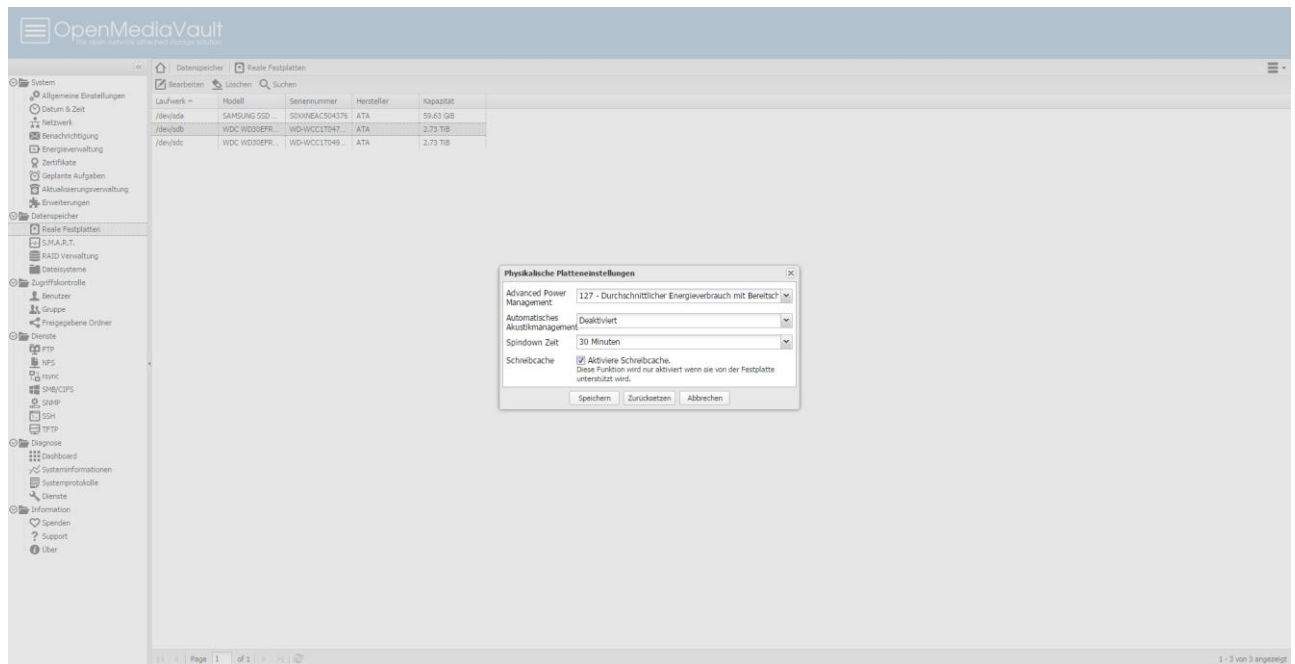
Anschließend müsst ihr unter dem Reiter **Laufwerke** manuell die S.M.A.R.T. Überprüfung für jede Festplatte aktivieren!



7 - Spindown und Energieverwaltung der Festplatten

Ein NAS läuft meistens für mehrere Stunden, daher ist es sinnvoll die Festplatten in einen energiesparenden Zustand zu versetzen, sofern diese nicht benötigt werden -

denn die Festplatten sind die größten Energieverbraucher in einem NAS. Klickt dazu auf den Punkt **Reale Festplatten**, wählt eine Festplatte aus und klickt auf **Bearbeiten**.

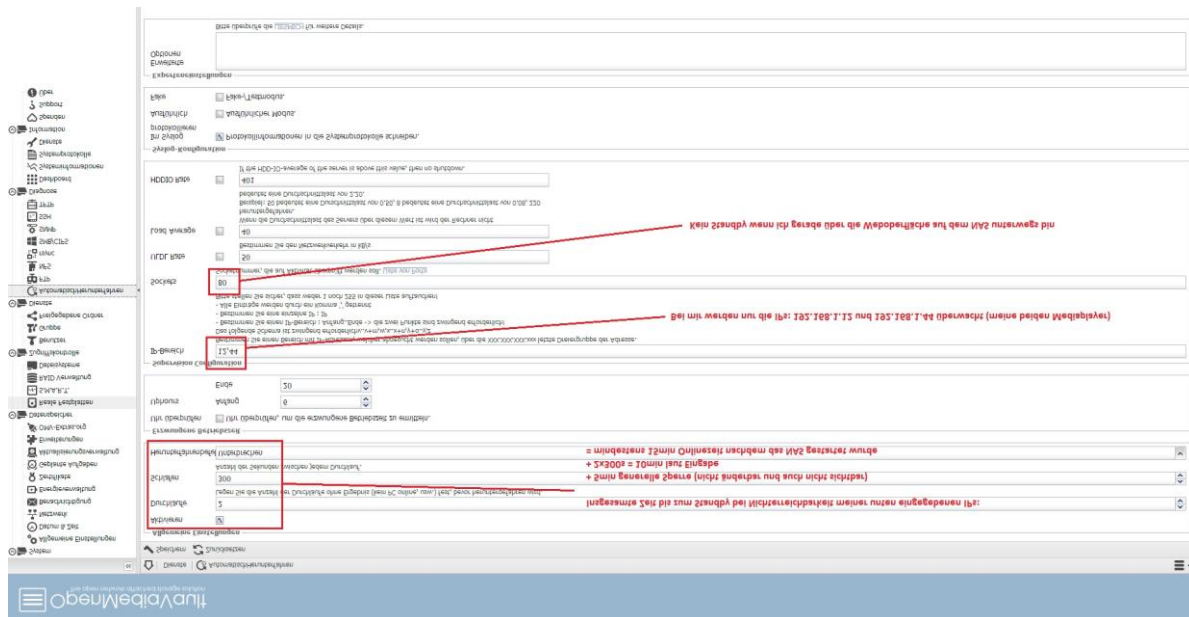


In meinem NAS benutze ich eine Spindownzeit von 30 Minuten, es kann aber auch Sinn machen die Zeit auf 60 Minuten zu erhöhen. Findet in der eingestellten Zeit kein Zugriff auf die Festplatten statt, werden diese in einen energiesparenden Zustand versetzt.

8 - Konfiguration von AutoShutDown

AutoShutDown funktioniert wie LightsOut für Windows: Es prüft ob bestimmte Geräte in einem Netzwerk aktiv sind. Ist dies der Fall wird nichts unternommen. Sind alle gewünschten Netzwerkgeräte offline (z.B. alle Mediaplayer) wird das NAS in den Ruhezustand / Standby versetzt um Energie zu sparen. Moderne Mediaplayer wie XBMC/Kodi oder auch Windows Computer können das NAS dann bei Verwendung per WOL (Wake-On-Lan) über das Netzwerk automatisch in den aktiven Modus zurückholen.

Autoshutdown kann mittels der über OMV-Extras (siehe Punkt Erweiterungen) eingebundenen Plugins installiert werden.



Da das NAS dann nur aktiv ist wenn es benötigt wird, lässt sich viel Energie sparen. Allerdings ist manchmal etwas Feintuning notwendig, z.B. sind bestimmte Geräte wie Smartphones oder Tablets meist dauerhaft online, so dass diese von der Prüfung ausgenommen werden sollten, da diese unter Umständen den Standby des NAS verhindern können.

Ich habe hier mal die wichtigsten Einstellungen herausgesucht und erklärt, gerade bei der Eingabe der zu überwachenden IP-Adressen kann man leicht einen Fehler machen:

Option	Bemerkung
Aktivieren	Dieser Haken muss gesetzt werden um das AutoShutDown Script zu nutzen
Durchläufe	Wie häufig nach euren Kriterien geprüft werden soll, bis das NAS in den Standby geschickt wird
Schlafen	Zeit in Sekunden zwischen den Durchläufen.
Herunterfahrenbefehl	"Unterbrechen = Standby" (empfohlen), "Ruhezustand", "Herunterfahren"
Uhr überprüfen	Aktivieren, wenn die Prüfung für eine bestimmte Zeit deaktiviert werden soll. Das NAS wird in dieser Zeit dann nicht in den Standby geschickt. Anfangs und Endzeit könnt ihr auswählen.
IP-Bereich	Wählt hier eine oder mehrere IPs aus oder auch einen Bereich.

	IPs werden wie folgt eingegeben: "12,50,100" - Prüfung der IPs 192.168.x.12, usw. NICHT die ganze IP-Adresse eingeben sondern nur die letzten Stellen!
Sockets	Überprüft die Ports auf dem NAS. Port 80 überwacht z.B. ob ihr gerade über die Weboberfläche angemeldet seid.

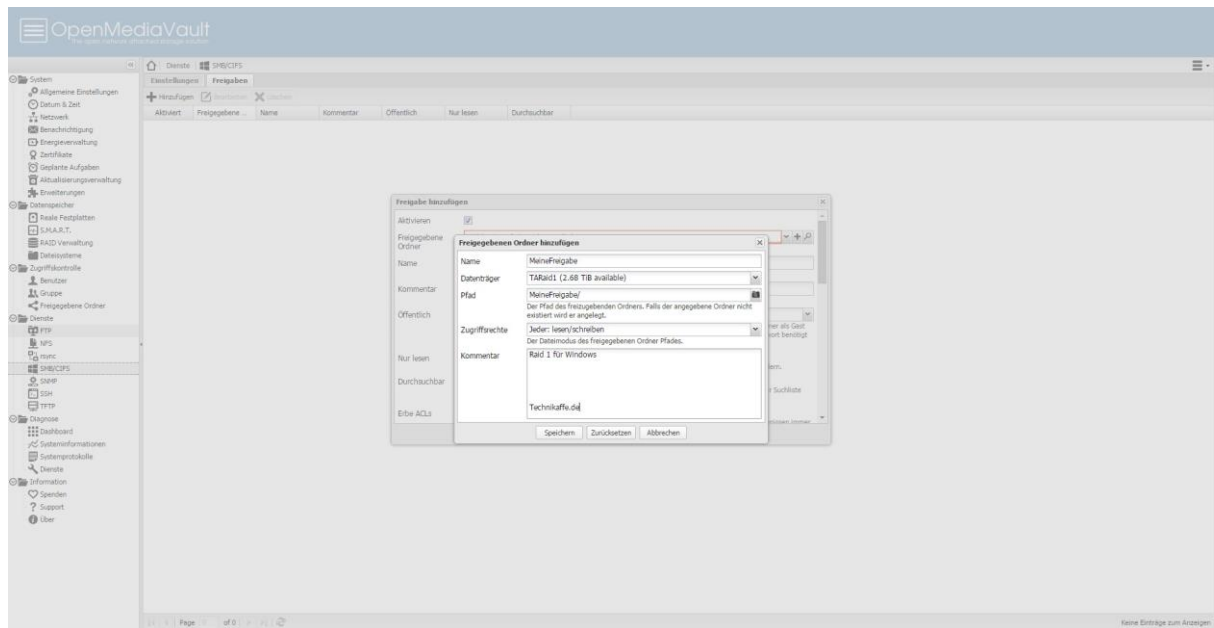
Hinweis: Nachdem ihr die gewünschten Änderungen vorgenommen habt, müsst ihr diese speichern und danach das NAS neustarten. Erst nach einem Neustart werden die Einstellungen auch korrekt beachtet.

Sollte trotz aller Tipps AutoShutDown noch nicht richtig laufen, solltet ihr euch die Log-Datei unter dem Punkt Systemprotokolle - "AutomatischHerunterfahren" anschauen und auf eventuelle Fehler / Meldungen prüfen.

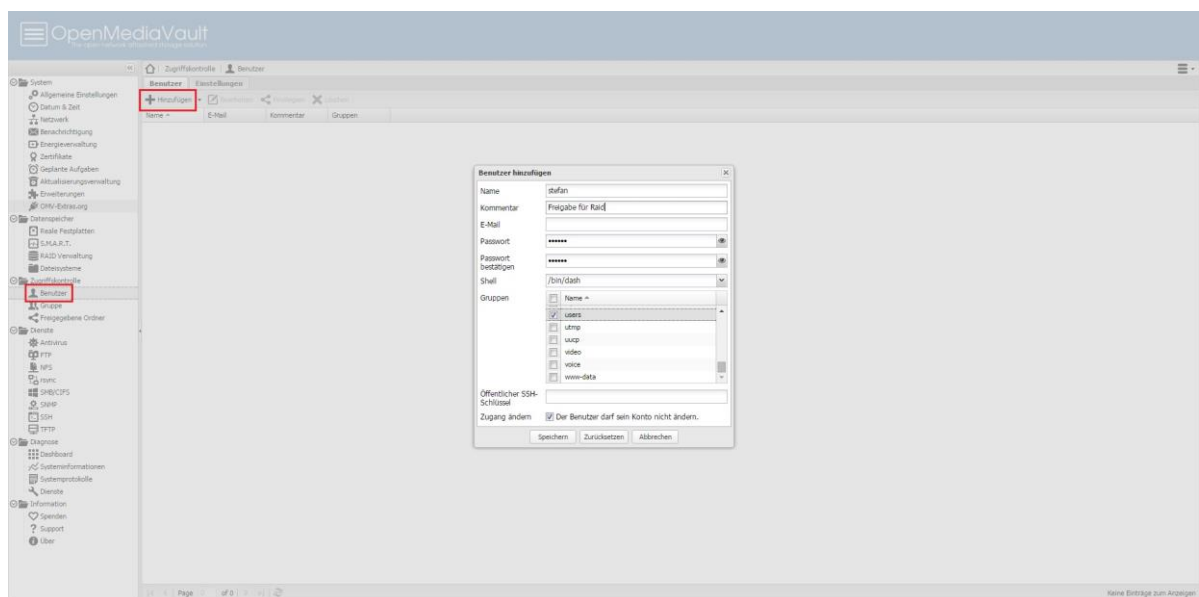
Generell geht das Script wie folgt vor: Nach dem Start des Systems wartet das Script 1 Minute und ermittelt dann die IP-Adresse des NAS. Danach wartet das Script weitere 5 Minuten bevor die eigentliche Prüfung auf aktive Geräte laut euren Einstellungen erfolgt.

9 - Erstellen einer Freigabe für andere Computer

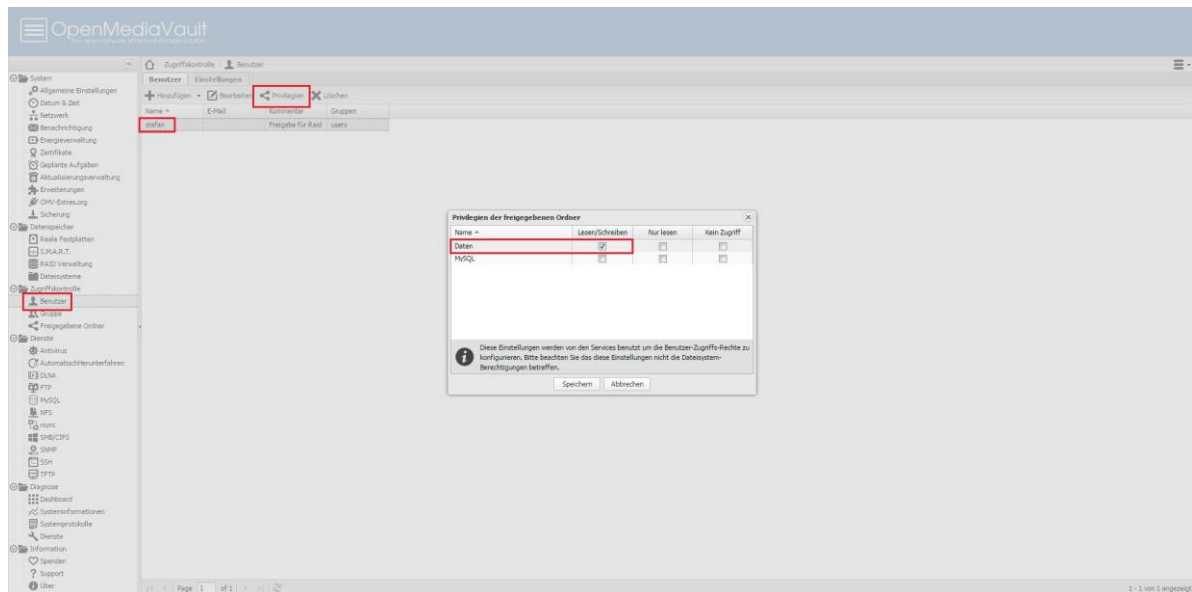
Zunächst müsst ihr euch entscheiden ob ihr eine SMB/CIFS oder eine NFS Freigabe erstellen möchtet. Die meisten werden sich aufgrund der Windows-Kompatibilität sicher für SMB entscheiden. Klickt auf den Menüpunkt SMB/CIFS und aktiviert diesen Dienst. Danach könnt ihr über den Reiter **Freigaben** eine Freigabe erstellen. Ich nenne meine Freigabe als Beispiel **Daten**.



Im nächsten Schritt legen wir nun einen neuen Benutzer an. Mit diesem Benutzer können sich Clients mit der Freigabe auf dem NAS verbinden. Ich nenne den Benutzer in meinem Beispiel **stefan**.



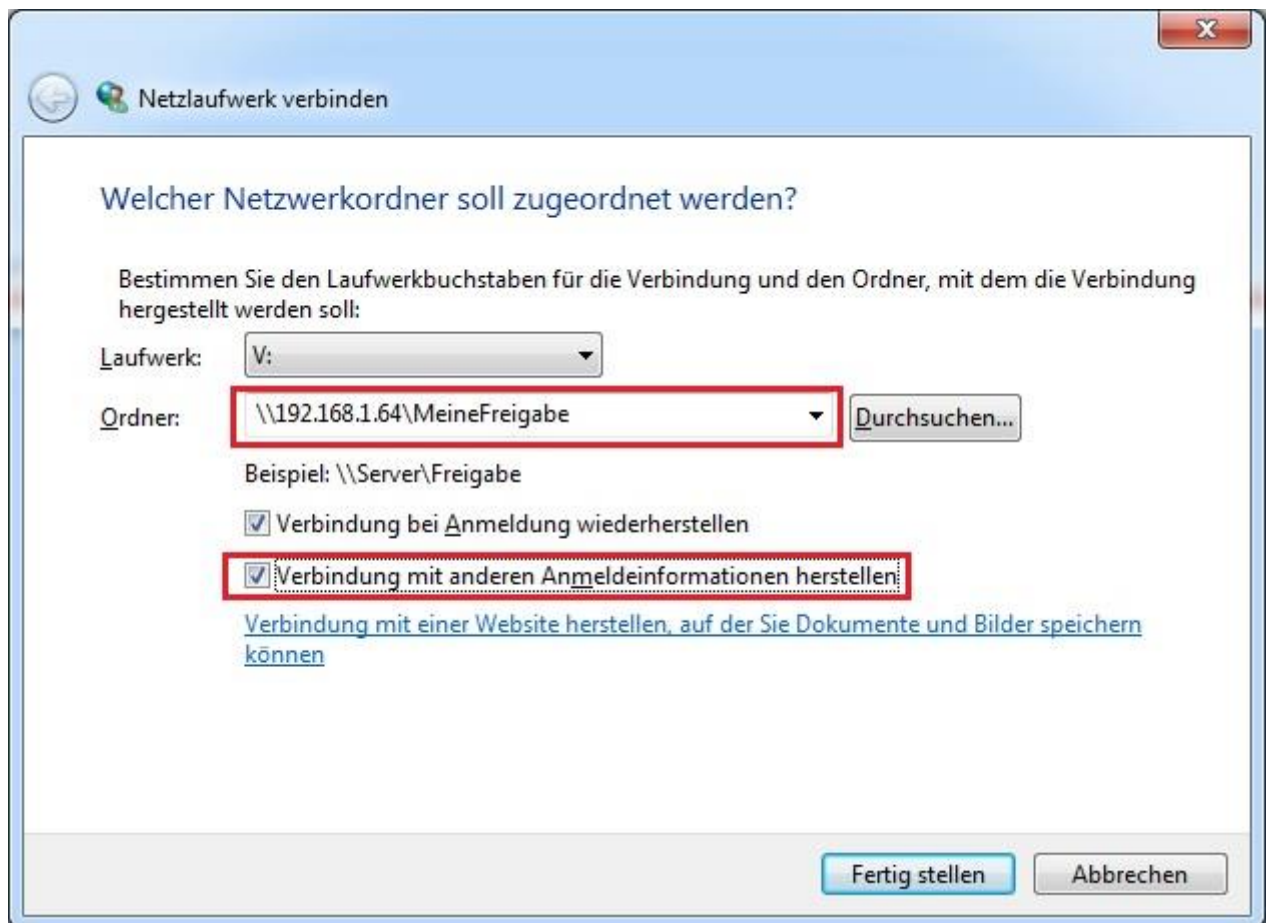
Nachdem der Benutzer angelegt ist, wählt ihr diesen aktiv aus und klickt auf die Schaltfläche Privilegien. Hier erscheinen nun alle von euch zuvor erstellten Freigaben. Wählt nun aus worauf der Benutzer Zugriff haben soll.



Freigabe in Windows einbinden

Nachdem ihr die Freigabe in OpenMediaVault erstellt hab, könnt ihr diese auf unbegrenzt vielen Computern im Netzwerk einbinden. In meinem Beispiel möchte ich von einem **Windows 7** Computer auf das NAS zugreifen.

Wählt dazu im Computer / Arbeitsplatz die Option Netzwerklaufwerk verbinden aus. Hier könnt ihr euch einen Laufwerksbuchstaben aussuchen sowie den Ordner aussuchen den ihr verbinden möchtet. Benutzt hierzu die IP-Adresse des OpenMediaVault NAS und den Namen euer eben erstellten Freigabe.



Im nächsten Fenster müsst ihr nun angeben mit welchem Benutzernamen und Passwort ihr auf die Freigabe zugreifen möchtet. Wählt hier erst einmal den Hostnamen eures NAS aus (in meinem Fall omv). Ihr findet den Namen in OpenMediaVault unter dem Punkt Netzwerk - Allgemein - Hostname.

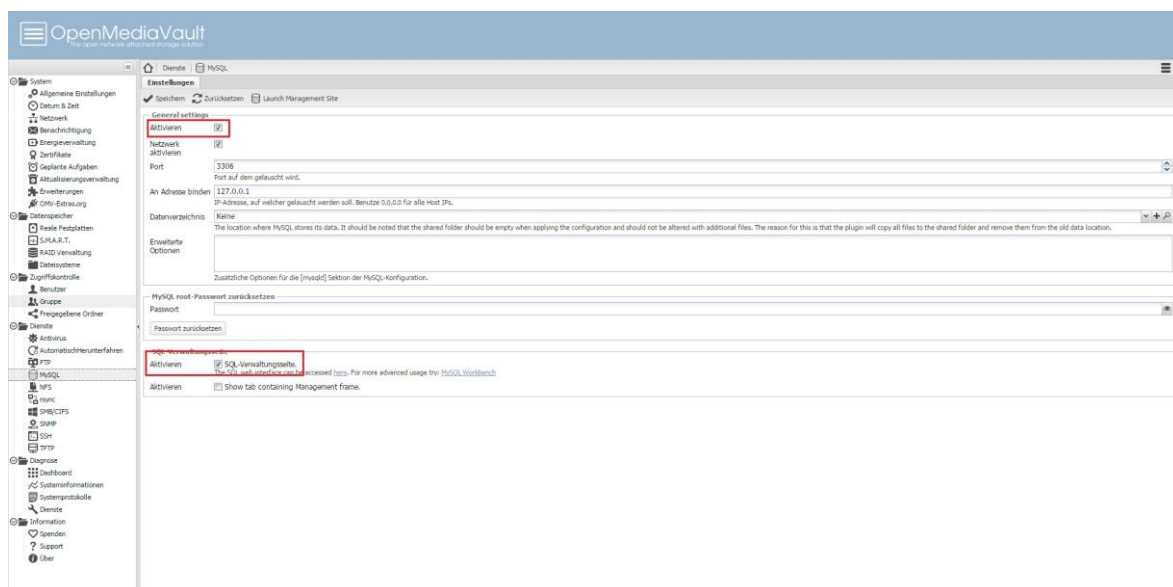
Nach dem Hostnamen gebt ihr noch den Benutzernamen an, den wir vorher auf dem NAS erstellt haben. Gebt als letztes euer Passwort ein und bestätigt den Dialog. Nun solltet ihr in eurem Arbeitsplatz ein neues Laufwerk sehen können.



10 - MySQL Datenbank unter OpenMediaVault

Sofern ihr die OMV-Extras Erweiterung installiert habt (siehe Erweiterungen), habt ihr Zugriff auf das MySQL Plugin für OpenMediaVault. Installiert dieses Plugin und klickt im Anschluss auf den nun neuen Menüpunkt **MySQL** unter **Dienste**.

Hier könnt ihr die MySQL Datenbank aktivieren und auch die Verwaltungsseite, auf der sich neue Benutzer oder Datenbanken anlegen lassen.



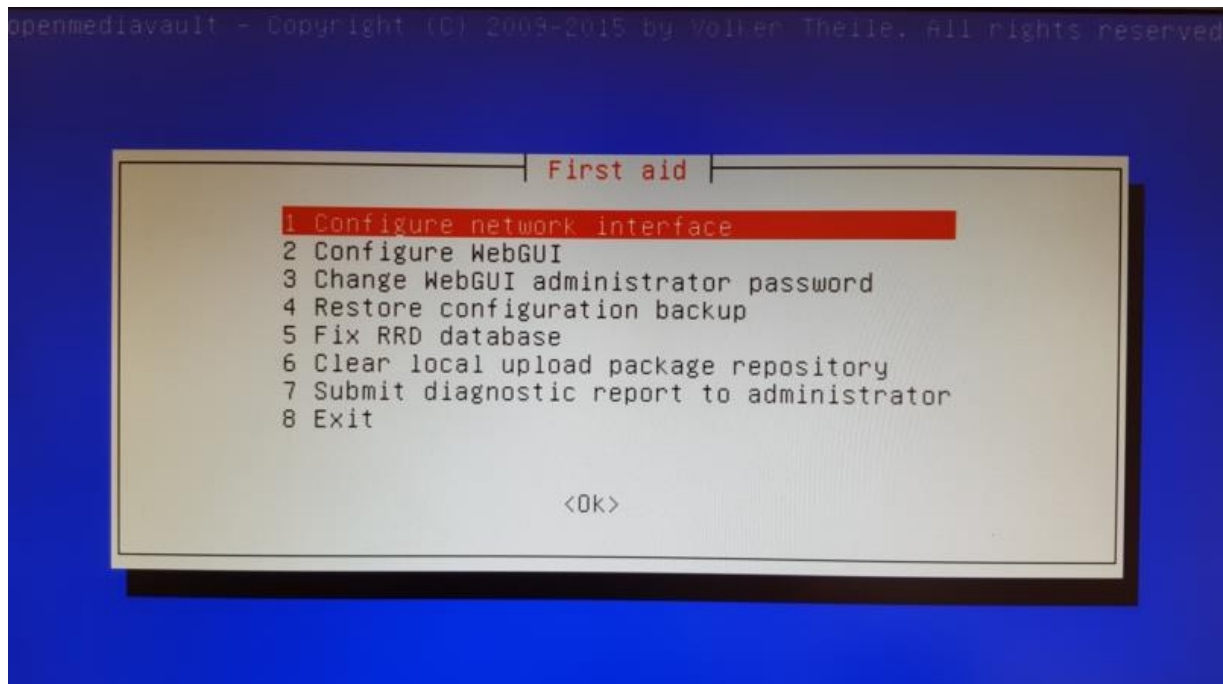
11 - Backup des Systemdatenträgers

Wie ihr in dieser Anleitung festgestellt habt, kann eine Ersteinrichtung von OpenMediaVault gerne mal 1-2 Stunden dauern, vor allem für Einsteiger. Daher empfiehlt sich ein regelmäßiges Backup des Systemdatenträgers. Im Falle eines Defektes des Systemdatenträgers lässt sich OpenMediaVault inkl. aller Einstellungen sehr einfach wiederherstellen. Auch hierfür reicht es ein Plugin zu installieren, welches wieder der OMV-Extras Erweiterung beiliegt.

Sofern ihr OpenMediaVault auf einem USB-Stick installiert habt, ist eine zweite Möglichkeit für ein manuelles Backup die Erstellung eines [1:1 Images des USB-Sticks](#).

12 - OpenMediaVault First Aid - Erste Hilfe

Sollte keine Verbindung zum Webinterface hergestellt werden können, kann man mit einem an das NAS angeschlossenen Monitor in ein kleines Hilfemenü gelangen. Dazu melden man sich nach dem Start des NAS mit dem Benutzer **root** und seinem während der OMV Installation vergebenen Passwort an.



Anschließend lässt sich das Hilfemenü von OpenMediaVault mit dem Befehl **omv-firstaid** aufrufen. Dieses bietet unter anderen die Möglichkeit die Netzwerkschnittstelle neu zu konfigurieren sowie das Passwort oder den Port der Weboberfläche neu zu setzen. Mit dem Befehl **ifconfig** lässt sich der Status und die IP-Adressen der Netzwerkschnittstelle anzeigen. Manuell lässt sich diese mit **dhclient -r** und dann mit **dhclient eth0** neu zuweisen.

13 - Installation des Backports Kernels

OpenMediaVault basiert aktuell auf Debian 7 "Wheezy" und nutzt den Kernel 3.2.0 aus dem Jahr 2012. Durch die manuelle Installation eines Backports Kernels mit neueren Treibern lässt sich der Energieverbrauch nochmal etwas reduzieren.

Eine vollständige [Schritt-für-Schritt Anleitung für die Installation des Backports Kernels](#) gibt es auch bei uns.

14 - SnapRAID

SnapRAID ist eine Mischung aus Backup und Raid und überwiegend für den privaten Gebrauch gedacht. Es kann eine interessante Alternative zu einem klassischen Raid Verbund sein. Eine [vollständige Anleitung](#) findet ihr auch bei uns.

15 - Wissenswertes

Hier haben wir Tipps und Antworten zu häufigen Fragen rund um OpenMediaVault gesammelt. Wenn ihr der Meinung seid, dass hier ein guter Hinweis fehlt, lasst es uns wissen!

15.1 - Tausch vom Mainboard

Möchtet ihr euer Mainboard inkl. Prozessor und Arbeitsspeicher tauschen, könnt ihr das tun denn OpenMediaVault nutzt den normalen Linux Software-Raid. Auch nach einer kompletten Neuinstallation der Software (OpenMediaVault) sowie einem Austausch der Hardware (bis auf die Datenfestplatten) bleiben alle Daten auf eurem Raid erhalten.

15.2 - Reihenfolge und Anschluss der Datenfestplatten

Bei vielen Raid-Systemen (z.B. dem Intel Fake-Raid) ist es immens wichtig, dass alle Datenfestplatten auf einen ganz bestimmten SATA-Port angeschlossen werden. Einmal initialisiert, dürfen die Festplatten nicht mehr vertauscht oder an einen anderen SATA-Port angeschlossen werden. Daher werden in solchen Raid-Systemen die Festplatten meist mit einer Port-Nummer beschriftet.

Bei OpenMediaVault könnt ihr euch diesen Stress sparen. Die Festplatten können beliebig vertauscht oder an andere SATA-Ports angeschlossen werden - allerdings muss das System dazu heruntergefahren werden.

15.3 - Nachträgliche Partitionierung des Systemdatenträgers

In der Standardeinstellung benutzt OpenMediaVault immer den kompletten

Datenträger, egal wie viel Kapazität dieser besitzt. Da OpenMediaVault locker mit 4 GB auskommt ist dies unter Umständen eine ziemliche Verschwendung. Daher kann man den Systemdatenträger nachträglich mit GParted partitionieren und kann den restlichen Systemdatenträger dann für Daten nutzen.

Die nachträgliche Partitionierung mit GParted haben wir [hier gesondert beschrieben](#).

15.4 - Braswell Mainboard ohne Monitor

Einige Braswell Mainboards verweigern den OpenMediaVault start, so lange kein Monitor angeschlossen ist. Da man ein NAS meistens ohne Monitor betreibt ist dies natürlich störend. Abhilfe schafft unser [OpenMediaVault Braswell Fix](#).