

---

# **openmediavault Documentation**

*Release 5.x.y*

**Volker Theile**

**Aug 25, 2021**



---

## Contents:

---

<b>1</b>	<b>Releases</b>	<b>3</b>
<b>2</b>	<b>Prerequisites</b>	<b>5</b>
<b>3</b>	<b>Installation</b>	<b>7</b>
<b>4</b>	<b>Features</b>	<b>9</b>
4.1	System . . . . .	9
4.2	General settings . . . . .	9
4.3	Storage . . . . .	10
4.4	Access Right Management . . . . .	10
4.5	Services . . . . .	10
4.6	Diagnostics . . . . .	10
<b>5</b>	<b>New User Guide</b>	<b>13</b>
5.1	Introduction to Openmediavault . . . . .	14
5.2	About this Guide . . . . .	16
5.3	Hardware . . . . .	17
5.4	Installing on Single Board Computers (SBC's) . . . . .	21
5.5	Installing on i386 32-bit Platforms . . . . .	21
5.6	amd64 (64-bit) Platforms . . . . .	21
5.7	Initial Configuration . . . . .	37
5.8	Quick Start Guide for Advanced Users: . . . . .	39
5.9	Basic Configuration . . . . .	40
5.10	Creating A Network Share . . . . .	53
5.11	The Flash Memory Plugin - amd64 users only . . . . .	60
5.12	Hard Drive Health and SMART . . . . .	65
5.13	Final Installation Notes: . . . . .	69
5.14	Utilities to Help With openmediavault Management . . . . .	70
5.15	Backups and Backup-strategy . . . . .	76
5.16	Full Disk Mirroring / Backup with Rsync . . . . .	78
5.17	Second Level Backup – Replication to a Second Host . . . . .	86
5.18	Operating System Backup . . . . .	87
5.19	Add-on's – Adding Value to Your OMV server . . . . .	90
5.20	When things go wrong . . . . .	96
5.21	A Closing Note . . . . .	100

<b>6 Administration</b>	<b>101</b>
6.1 General . . . . .	101
6.2 Storage . . . . .	109
6.3 Access Rights Management . . . . .	115
6.4 Services . . . . .	120
6.5 Custom Configuration . . . . .	129
<b>7 Plugins</b>	<b>133</b>
7.1 Benefits . . . . .	133
7.2 Overview . . . . .	133
7.3 3rd party . . . . .	134
<b>8 FAQ</b>	<b>135</b>
<b>9 Troubleshooting</b>	<b>139</b>
<b>10 Development</b>	<b>141</b>
10.1 Coding Guideline . . . . .	141
10.2 Contribute . . . . .	144
10.3 How it works . . . . .	145
10.4 Internal Tools . . . . .	148
<b>11 Support</b>	<b>155</b>
<b>12 Press releases, reviews and external references</b>	<b>157</b>
<b>13 Contributors</b>	<b>159</b>
<b>14 Copyright</b>	<b>163</b>

openmediavault is a complete network attached storage (NAS) solution based on Debian Linux.

- It's available for x86-64 and ARM platforms.
- Features a full Web Administration interface.
- Can be controlled via SSH, if enabled.
- Access to file storage is possible with a variety of different protocols such as FTP, SMB/CIFS or NFS and can be controlled with Access Right Management for users and groups.

openmediavault is primarily designed to be used in home environments or small home offices, but is not limited to those scenarios. It is a simple and easy to use out-of-the-box solution that everyone can install and administer without needing expert level knowledge of Networking and Storage Systems.

The system is built on a modular design and can be easily extended with plugins available right after installation of the base system. Additional 3rd-party plugins are available via the [OMV-Extras repository](#).



# CHAPTER 1

---

## Releases

---

Table 1: openmediavault historical releases

Version	Codename	Base Distro	Status	Date Released
0.2	Ix	Debian 6	EOL	Oct 2011
0.3	Omnious	Debian 6	EOL	Jul 2012
0.4	Fedaykin	Debian 6	EOL	Sep 2012
0.5	Sardoukar	Debian 6	EOL	Aug 2013
1.0	Kralizec	Debian 7	EOL	Sept 2014
2.0	Stoneburner	Debian 7	EOL	Jun 2015
3.0	Erasmus	Debian 8	EOL	Jun 2016
4.0	Arrakis	Debian 9	EOL	Apr 2018
5.0	Usul	Debian 10	Stable	Mar 2020
6.0	Shaitan	Debian 11	In Development	est. Q4/2021





## CHAPTER 2

---

### Prerequisites

---

Before installing openmediavault make sure your hardware is supported.

- **CPU:** Any x86-64 or ARM compatible processor
- **RAM:** 1 GiB capacity
- **HDD:**
  - **System Drive:** min. 4 GiB capacity (but more than the capacity of the RAM)
  - **Data Drive:** capacity according to your needs

---

**Note:** The whole disc will be occupied by the system and swap space<sup>1</sup>, so size doesn't matter so much. Data storage on the system disc is not supported.

---

Spinning Harddisk, SSD<sup>2</sup>, Disk-on-Module<sup>3</sup>, CompactFlash<sup>4</sup> or USB thumb drive<sup>5</sup> type drives can be used as system drive.

If you use a Flash Drive, select one with static wear leveling<sup>6</sup>, without this the drive will have a very short lifetime. It is also recommended to install and activate the *Flash Memory plugin*. The entire disk is used as system disk and can not be used to store user data.

---

<sup>1</sup> <https://en.wikipedia.org/wiki/Paging>

<sup>2</sup> [https://en.wikipedia.org/wiki/Solid-state\\_drive](https://en.wikipedia.org/wiki/Solid-state_drive)

<sup>3</sup> [https://en.wikipedia.org/wiki/Solid-state\\_drive#DOM](https://en.wikipedia.org/wiki/Solid-state_drive#DOM)

<sup>4</sup> <https://en.wikipedia.org/wiki/CompactFlash>

<sup>5</sup> [https://en.wikipedia.org/wiki/USB\\_flash\\_drive](https://en.wikipedia.org/wiki/USB_flash_drive)

<sup>6</sup> [https://en.wikipedia.org/wiki/Wear\\_leveling](https://en.wikipedia.org/wiki/Wear_leveling)



### Before you begin:

- Check if your hardware is supported on the system [requirements page](#).
- [Download](#) an installation image file for your system. openmediavault provides ISO installers for x86 architecture and several preconfigured images for ARM devices.
- Disconnect all disk devices except the one for the system drive. This way you avoid an accidental install on a storage drive (which will be configured after installation anyway).

**Installation variants:** Choose your installation variant and follow the instructions.

- Dedicated drive - Advised method via ISO image. This runs OMV from its own drive.
- USB flash drive - This runs openmediavault from a USB flash drive.
- Debian Operating System - This runs openmediavault as a services on top of a Debian OS.
- [Debian Operating System via debootstrap](#). Use this as a last resort in case the installer does not recognize a specific essential hardware component like hard disk (NVME) or a network card that needs a higher kernel (backport).
- SD card - This runs openmediavault from a SD card.

**First time use:** If you have a screen attached, KVM or IMPI console the login screen will display the current IP address assigned for the web interface. Open your browser and type that IP address. The default web interface login credential is `admin:openmediavault`, the `root` password is the one you setup during installation.

For ARM images the root password is the same as admin password.

---

**Note:** openmediavault will enable SSH access for the user `root` by default to be able to access a headless system in case of a broken installation or other maintenance situations. You can disable this behaviour in the [Services | SSH page](#).

To still get `root` access you need to create a non-privileged user and add them to the `ssh` and `sudo` groups. After that you can SSH into the system with this non-privileged user and run `sudo su`.

---



### 4.1 System

### 4.2 General settings

**General settings:** Change web interface listening port, SSL and force SSL. Change admin password.

**Notification system:** Integrated into several services in the form of email using Postfix<sup>1</sup> backend as MTA, these include scheduled tasks, services monitoring, S.M.A.R.T., MDADM and cron-apt. Since openmediavault 3.0 is possible to add also third party notification systems by using scripts, more information [here](#) and real example on how to use it [here](#).

**Network configuration:** The web interface provides configuration options for ethernet, WiFi (only WPA/WPA2 supported), bond and vlan interfaces. This also includes a panel for firewall configuration.

**Certificates:** Create or import existing SSL and SSH certificates. This certificates can be used for securing the web interface or SSH access. Plugins can use the backend framework to select the available certificates.

**Power Management:** Scheduled power management for hibernation (S5), suspend (S3), shutdown and/or reboot.

**Service Discovery:** Using avahi-daemon<sup>2</sup> is possible to announce the following services Samba, NFS, AFP, FTP, web admin panel, to any Linux desktop with file browser that supports it (GNOME, KDE or XFCE for example). OS X can recognise AFP and Samba services in the Finder sidebar. To announce SMB to windows clients, samba uses NetBios, not avahi.

**Scheduled Tasks:** Based on cron the webUI can define tasks for running specific commands or custom scripts at certain time or regular intervals.

**Update Manager:** Displays all available packages for upgrade.

---

<sup>1</sup> <http://postfix.org>

<sup>2</sup> <https://www.avahi.org/>

## 4.3 Storage

**S.M.A.R.T.:** Based on smartmontools<sup>3</sup>, It can display advanced information of S.M.A.R.T values in the webUI. It can also schedule health tests as well as send notifications when S.M.A.R.T. attributes values change.

**RAID Management:** Based Linux RAID<sup>4</sup>, create arrays in 6 different configurations. Levels available are linear, 0, 1, 10, 5 and 6. The array can have disks removed or expanded using the web interface.

**File Systems:** Volume format, device mount and unmount. More information in the *filesystem section*.

**LVM:** Enhanced by the LVM2 plugin, the system has the capability of formatting disks or partitions as LVM that can be used in volume groups to create logical partitions.

## 4.4 Access Right Management

**Users:** User and group managing. Using privileges is possible to restrict access/login to shares on network sharing services (FTP, Samba and AFP) without interfering Unix permissions.

**Groups:** Create and manage custom groups. System groups cannot be manipulated here.

**Shared Folders:** Simple shared folder administration. Within this section is also possible to assign ACLs and/or privileges to the shared folders.

## 4.5 Services

**SMB/CIFS:** SMB sharing protocol using Samba<sup>5</sup> as standalone server by default.

**FTP:** Service based on proftpd<sup>6</sup>. Intended for accessing shares from remote or local.

**RSync:** Server daemon. Shared folders can be defined as rsyncd modules. With scheduled tasks, rsync client can be configured for push or pull jobs.

**NFS:** Network file system protocol<sup>7</sup>.

**SSH:** Remote shell access using openssh<sup>8</sup>.

**TFTP:** A basic configuration panel is provided. This can complement a PXE server to deploy local network installations.

---

**Note:** In openmediavault version 4 the TFTP has been removed from core, and now it can be installed as an official plugin.

---

## 4.6 Diagnostics

**Dashboard:** By default the server comes with four information widgets. Network interfaces, System, Filesystem and service/daemon status. The dashboard panel can have widgets added using the plugin framework.

---

<sup>3</sup> <https://www.smartmontools.org/>

<sup>4</sup> [https://raid.wiki.kernel.org/index.php/RAID\\_setup](https://raid.wiki.kernel.org/index.php/RAID_setup)

<sup>5</sup> <https://www.samba.org/>

<sup>6</sup> <http://www.proftpd.org/>

<sup>7</sup> <http://nfs.sourceforge.net/>

<sup>8</sup> <https://www.openssh.com/>

**System information:** The panel displays four tabs with system information and statistics graphs.

**System Logs:** Interface to view and download logs from syslog, journalctl, message, auth, ftp, rsync and samba. Plugins can attach their logs here using the framework.

**Services:** View status (enabled/disabled and running/not running) of services. Detailed information is provided by default for Samba, FTP and SSH. Plugins can use this tab to integrate their service information also.





## CHAPTER 5

---

New User Guide

---

# Getting Started with



## Openmediavault 5

---

This document can be converted to a PDF file, at the bottom left side corner of this page. Click the drop down arrow next to **Read the Doc's v: 5.x**

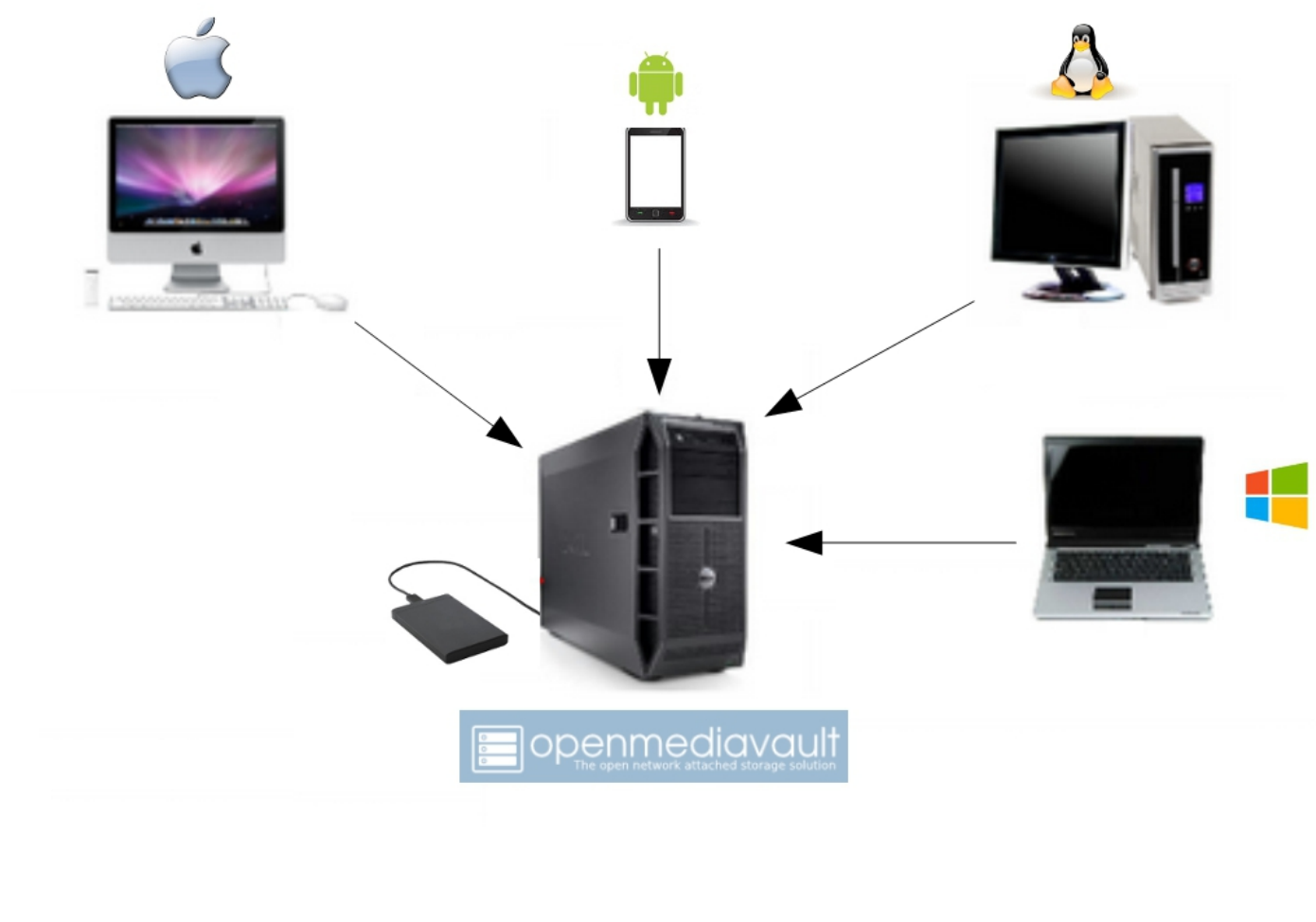
- [Google Translate](#) kann Wiki-Dokumente in Ihre Sprache übersetzen. Fügen Sie die Wiki-URL in das linke Fenster ein und öffnen Sie den übersetzten Link rechts.
  - [Google Translate](#) puede traducir documentos wiki a su idioma. Pegue la URL de la wiki en la ventana izquierda y abra el enlace traducido a la derecha.
  - [Google Translate](#) peut traduire des documents wiki dans votre langue. Collez l'url du wiki dans la fenêtre de gauche et ouvrez le lien traduit sur la droite.
  - [Google wiki wikiURL](#)
- 

### 5.1 Introduction to Openmediavault

Openmediavault is a File Server / NAS system designed to work on most modern IBM compatible PC systems, to include typical amd64 or i386 PC's and select ARM devices. Openmediavault can be thought of as filling a role similar to Microsoft's Server Essentials, but extends far beyond the role of a basic File Server with additional functionality

added VIA plugin's and Dockers. Openmediavault is designed to work with popular client operating systems and multiple filesystem types, utilizing proven data sharing techniques on small and medium sized Local Area Networks.

In meeting the needs of it's intended users, individuals and small-to-medium-sized businesses, openmediavault is designed for flexibility.



---

### 5.1.1 History

Openmediavault's history began with Volker Theile, who was the only active developer of the FreeNAS project by the end of 2009. Volker became interested in completely rewriting FreeNAS, for use on Linux. Initially, he named the rewritten package **coreNAS**. Shortly thereafter, Volker discarded the name **coreNAS** in favor of **openmediavault**. Openmediavault's initial release was on 17 October 2011. It's built upon very mature and proven software layers and is under constant development. Openmediavault relies on the Debian project and uses their system and repositories as a base. The project focus is on creating and maintaining a stable and extensible NAS system that is intuitive and easy to use.

## 5.1.2 Purpose

The purpose of openmediavault, is to provide a NAS system that is highly “extensible” with value added plugin’s and access to numerous Dockers that are desirable and beneficial to home users and small businesses at little to no cost.

One of the ambitions of the openmediavault project is to make advanced NAS technologies and features available to inexperienced users in an easy to use web interface, thereby making it possible for people, without extensive knowledge of Linux, to gain easy access to advanced technologies.

## 5.1.3 Getting Involved

If businesses and home users find openmediavault to be beneficial, please consider supporting the project with a modest donation. While openmediavault is free, donations to cover Web site costs, hardware for testing, and other unavoidable expenses are needed and very much appreciated.

[Donate to openmediavault](#) (Main project development)

[Donate to omv-extras.org](#) (Support for Single Board Computers and Development of Plugins.)

The openmediavault project is looking for coding talent and contributors. If one has developer experience, (BASH, PHP, Python, Javascript) the project would like to hear from you. Users with Linux experience are invited to help out on the [openmediavault Forum](#).

---

## 5.2 About this Guide

In computing, generally speaking, there are several ways to do the same thing. By extension, methods and methodology become progressively more advanced as a user’s skill level increases. With these notes in mind, methods found in this guide may not be considered as “Best Practice”, especially from a hardened security perspective. The purpose and intent of this guide is to provide a walk-through to get users up and running as quickly and easily as possible.

- This guide contains links to external sources of information and software. It’s best used on a PC connected to the Internet.
- This is a community document and a work in progress. Input and feedback are welcome and can be sent to: [omvguide@gmail.com](mailto:omvguide@gmail.com)

### 5.2.1 Beginners:

This document is intended for beginners who will, primarily, be using the openmediavault’s GUI. Beginners are assumed to have basic knowledge of computers and their LAN systems, and a Windows or Apple PC. The focus of this guide will be to take a technically easy route, for the widest possible cross section of new users, toward accomplishing basic tasks using methods and processes that are easy to understand and duplicate.

### 5.2.2 Advanced Users:

Openmediavault was designed to be intuitive for advanced users and beginners alike. After the installation is complete, for a streamlined setup, see the [Quick Start Guide](#) .

### A Cautionary Note for Advanced Users:

Many of the configuration files traditionally used to customize Debian Linux are controlled by the openmediavault system database. As a result, manual edits of configuration files may be overwritten as of the next, “on-demand”, configuration change in the openmediavault GUI. Further, it is possible to “break” openmediavault with alterations and permissions changes to the files of the boot drive, on the command line. In the beginning it’s best to rely, primarily, on the GUI for configuration and control. Otherwise, before attempting to customize the operating system, backing up the boot drive is highly recommended.

---

## 5.3 Hardware

Hardware requirements to run openmediavault are very modest, however, actual hardware requirements for specific “use cases” vary widely. The following is intended only as general guidance.

### 5.3.1 Compatibility:

Openmediavault 5.X is currently supported by Debian 10, “Buster”. Compatible hardware and other requirements of Debian Linux are available at [Debian.org](http://Debian.org)

### 5.3.2 64 bit hardware (amd64):

The openmediavault project maintains convenient, fully integrated, openmediavault/Debian installation ISO’s. This is the best method for getting openmediavault up and running quickly.

### 5.3.3 32 bit Hardware (i386):

While openmediavault is supported by 32 bit Debian installations, it’s a two step scripted process referenced in; *Installing on i386 32-bit Platforms* . The openmediavault project does not provide integrated 32 bit installation ISO’s.

### 5.3.4 ARM Hardware:

The openmediavault project provides scripted installation support for ARM Single Board Computer (SBC) platforms. Supported platforms are the Raspberry Pi, models 2B and higher, and various ARM platforms supported by the [Arm-bian Project](#) .

### 5.3.5 Minimum Hardware requirements

Openmediavault/Debian will run on I386, AMD64, and select ARM platforms with 1GB of ram or less, but performance expectations should be adjusted accordingly. The system boot drive should have a minimum of 8GB capacity.

### 5.3.6 Recommended Minimum requirements

For basic File Server operations - 1 or 2 users:

- Intel Core 2 Duo or equivalent AMD processor and 1GB of RAM.
- Any of the ARM Single Board Computers supported by openmediavault.

If flash media is used, (USB thumb-drives, SD-cards, etc.) the system boot drive should have at least 16GB capacity, for longer life.

### 5.3.7 Recommended Hardware and Considerations for a good use experience

#### amd64

- Intel i3 (or equivalent AMD processor), 4GB ram or better (ECC preferred) and a 16GB system boot drive will provide good performance in home or small business use cases.
- As the number of NAS users increase and server processes are added, processing power and memory requirements increase.
- For file caching, in support of normal file system operations, performance is better with more RAM.
- The number of a Motherboard's SATA or SAS ports can be a factor if future storage expansion is needed.
- A case design that accommodates the physical installation of additional hard drives can be helpful.
- Integrated video is preferred over add-on Video cards. With openmediavault's headless server design, add-on Video cards are an excessive and unnecessary power drain, with no performance benefit. Installing a high end, high powered Video card in a headless server is analogous to installing a 65 to 200 watt light bulb in a closet, without a switch, and closing the door.

#### ARM - Single Board Computers:

Performance levels vary greatly among the various models of **Single Board Computer** (hereafter referred to as an "SBC") that are supported by Armbian, Raspbian, and openmediavault. While most will support file server operations for a few users, if running server add-on's or Dockers is a requirement, research supported SBC's carefully before buying. *Armbian's or openmediavault's forums may be of assistance, along with Internet product reviews. When considering an SBC as a primary NAS server for home use, note that support for SBC's is for the current openmediavault release only. Accordingly, SBC users should read the ending cautionary note in *Operating System Backup**

#### Raspberry PI's

(Hereafter referred to as **R-PI's**.) Given the current market for SBC's, the majority of SBC users will likely be owners of R-PI's.

Openmediavault runs well on the R-PI 4. While openmediavault will run on an R-PI model 2B and the various models of the R-PI 3, performance is poor. What exactly does "poor performance" mean? In this context, if the R-PI's CPU is running at 100%, openmediavault may not show up on the network and / or network shares may not open. This may give the false impression that there's a software or permissions problem. In other instances, the web interface login page may not respond.

These issues may appear to be software related, but that's not always the case. Older R-PI's are very easily over stressed and, during periods where the CPU is running at 100%, they may not respond to external input. With this performance limitation in mind, earlier versions of the R-PI (2B and 3X models) should be used only as a basic file

server for 1 or 2 user home environments, where multitasking is less likely. If running automated tasks, it's best to schedule them to run in the early morning hours when user access would not be affected. In addition, R-PI's suffer from USB under powering in models 2B and 3X. See notes regarding this issue in *USB Power - A Common Raspberry PI problem* .

### 5.3.8 Where CPU Power may be Needed – “Transcoding”

If a users' primary consideration is setting a up a media server, CPU selection may need careful consideration. Transcoding is a process for translating media file formats into types that mobile devices understand. Since mobile devices are low powered, they're not capable of re-processing high resolution media files smoothly so the processing burden is often transferred to the media server.

---

#### Pre-2011 Intel and AMD CPU's

Plex, a popular media server, recommends at least 2000 on the CPU's [PassMark](#) score for each concurrent 1080p transcoded stream. See the advice article → [here](#) . However note that this advice applies to pre-2011 Intel and AMD CPU's.

Look up an older CPU here → [PassMark CPU Benchmarks](#) .

#### 2011 and Newer Intel CPU's

As of the beginning of the Sandy Bridge CPU series in 2011 and later, a core has been added to Intel CPU's for the sole purpose of video transcoding. CPU's with [Quick Sync](#) , to include Celeron and Atom models that are relatively low powered, do a good job of transcoding for portable devices.

If NAS administrators have numerous smart phone users, in their homes or businesses, who will be watching transcoded video on the small screen, CPU loading and Video processing features may require some additional thought and research.

Additional reading: [Intel Quick Sync versus similar AMD technology](#)

---

### 5.3.9 Selecting a Boot Drive

Nearly any type of hard drive, SSD, or flash device (USB thumb-drives and SD-cards) 8GB or larger, will function as an openmediavault boot drive.

However, some notions of achieving a “Faster” or a “Better Performing NAS server” by using certain types of fast boot media should be dispelled.

Server booting requirements and considerations are different when compared to desktop and business workstation requirements.

- Given openmediavault's lean configuration, boot times can be fast. Boot times of 1 minute and Shutdown times of 20 seconds are common, even when using relatively slow flash media such as USB thumb-drives and SD-cards. (Recent models can be quite fast – check their benchmarks.)
- Typically servers are rebooted no more than once a week. When automated, a reboot event is usually scheduled after-hours when users are not affected.
- After the boot process is complete, most of openmediavault's file server functions are running from RAM.

**Conclusion – for Linux file server operations, fast boot media is not important.**

- “The WEB/GUI is more responsive with fast media.”

This is the single instance where an SSD or a spinning hard drive may create the illusion of higher performance. In the traditional role of a NAS as a File Server, when the server boots, the Linux kernel and most of the necessary processes required to act as a File Server are loaded into RAM - the fastest possible media for execution.

Navigating openmediavault’s WEB/GUI interface is another matter. Loading WEB pages may call files from the boot drive, which may make the server appear to be slower, when using slow media. However, the speed of the boot drive has little impact on overall file server function and actual NAS file serving performance.

*The above assumes that adequate RAM has been provisioned.*

---

### Final Notes on Choosing a Boot Drive

Openmediavault’s boot requirements are very modest: While some users prefer traditional hard drives or SSD’s, the boot requirement can be served with USB thumb-drives and SD-cards, 8GB or larger.

With USB connections on the *outside* of a PC case, cloning USB drives for *operating system backup* is an easy process. Given this consideration, some users prefer USB thumb-drives and other external flash media to internal drives. Further, given the ease of operating system recovery in the event of a boot drive failure, beginners are encouraged to consider using flash media.

If flash media is used:

**New** name brand drives are recommended such as Samsung, SanDisk, etc. While not absolutely essential for the purpose; USB3 thumb-drives are preferred, due to their more advanced controllers, and SD-cards branded A1 for their improved random read/write performance. **USB3** thumb-drives and **A1** spec’ed SD-cards are faster and, generally speaking, more reliable than similar items with older specifications.

While boot drive size matters, bigger is not always better. An acceptable size trade off for wear leveling and speed of cloning is between 16 and 32GB. (“**Wear leveling**” will be explained during the installation and configuration of the flash-memory plugin.)

The flash-memory plugin is required for flash media. It’s purpose and installation is detailed in [The Flash Memory Plugin](#) .

**Use-case exceptions where boot media larger than 32GB may be useful:**

- Running applications that utilize WEB interfaces, such as Plex, Emby, etc.
- Hosting Web or Media Servers with extensive content.
- Hosting Virtualized Guest operating systems with desktops. (Does not apply to ARM platforms. ARM platforms can not virtualize i386 or amd64 operating systems. )

(There’s no penalty for starting with a smaller boot drive. Moving to a larger drive, if needed, can be done later.)

---

**Note:** Buying flash devices on-line, even from reputable retailers, comes with the substantial risk of buying fakes.

---

Buying flash drives, in sealed packaging, from walk-in retail stores with liberal return policies is recommended. The use of cheap generics, fakes or knockoffs is highly discouraged. They tend to have a short life and they’re known to cause problems, even if they initially test error-free. In addition, to detect fakes or defective media *even when new*; all SD-cards and USB thumb-drives, should be formatted and tested in accordance with the process outlined under [Format and Test Flash Media](#) .

---



### 5.3.10 Hardware - The Bottom Line

Again, openmediavault/Debian's hardware requirements are modest. Nearly any IBM compatible PC or Laptop produced in the last 10 years could be re-purposed as an openmediavault server.

However, it should be noted that newer hardware is, generally speaking, more power efficient and it's higher performing. The power costs of running older equipment that is on-line, 24 hours a day, can easily pay for newer, more power efficient equipment over time.

Further, the supported ARM platforms are both power efficient and capable of providing file server functions in a home environment. (Again, performance expectations should be adjusted in accordance with the capabilities of the hardware.)

---

## 5.4 Installing on Single Board Computers (SBC's)

Installation guides for SBC installations are available in [PDF's](#) or in a [Wiki](#) .

---

## 5.5 Installing on i386 32-bit Platforms

An installation guide for 32-bit installations is available in [PDF](#) or in a [Wiki](#) .

---

## 5.6 amd64 (64-bit) Platforms

This guide assumes the user will be installing from a CD, burned from an image found in openmediavault's files repository [openmediavault's files repository](#) , using 64 bit hardware. Information for creating a bootable USB thumb-drive, as a software source, is provided as well.

## 5.6.1 Downloading

Beginners should download **the latest stable version** from [Sourceforge.net](https://sourceforge.net) and copy or download the SHA or MD5 checksums for the ISO. The checksum value will be used with the MD5 SHA checksum utility.

---

**Note:** Windows Notepad can open MD5 files by selecting “**All Files**”, next to the file name drop down.

---

**Warning:** If users install Beta versions of openmediavault, they are agreeing to be a “tester”. As part of being a tester, users may experience issues or bugs that can not be resolved which may result in **lost data**. Plan accordingly, with full data backup.

### Verify the download

After the download is complete, verify the download with a [MD5 & SHA checksum utility](#). MD5 and SHA hashes check for image corruption that may have occurred during the download.

---

**Note:** Beginners - DO NOT SKIP THIS STEP. The chance of image corruption is high when downloading and it's pointless to build a server with flawed software. Even the **slightest** corruption of the installation ISO may ruin your installation and the effects may not be noticed until well after your server is built and in use. Headaches can be avoided by checking the image.

---

## 5.6.2 Installing - amd64 Platforms

### Burning a source CD

Assuming a CD/DVD drive is installed; in most cases, double clicking an installation file, with an **.ISO** extension, will trigger a CD burning utility on a Windows Computer or a MAC. If help is needed for this process, see the following link.

[How to burn an ISO image in Windows 7, 8, 10](#)

### Creating a Bootable ISO Thumb-drive

For PC's without an Optical drive; the openmediavault ISO can be installed using a Thumbdrive as the ISO source, and install the Debian/openmediavault system to a second thumb drive.

For assistance in creating a bootable ISO thumb-drive, see the following link.

[How to install an ISO file on a USB drive](#)

**Before creating an ISO thumb-drive consider checking the drive, to be used as a software source, using the utilities and process described below in, [Preparing Flash Media](#) .**

---

**If installing to a standard hard drive or SSD, skip to → [openmediavault installation](#) .**

---

## Preparing Flash Media

To use flash media as a boot drive, a couple utilities are recommended:

SDFormatter (get the latest version), and h2testw1.4 .

- SDFormatter installs in the same manner as a typical Windows program.
- h2testw1.4 is stand-alone “portable” application. Simply unzip h2testw\_1.4 onto the desktop, open the folder, and double click the executable.

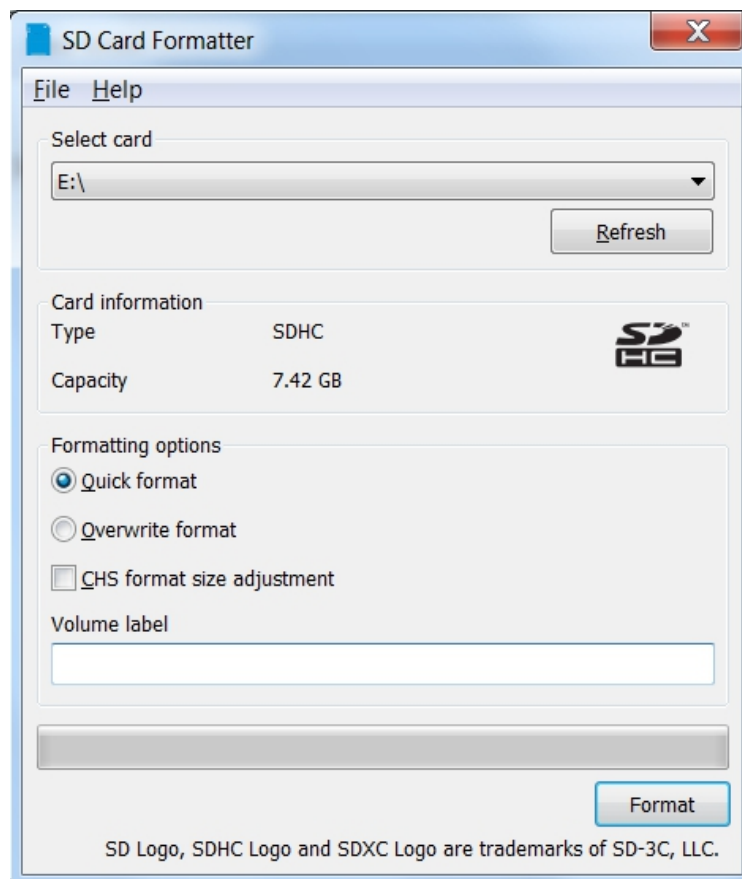
Due to the rise in counterfeit media and media that reports a fake size, it’s recommended that all USB thumb-drives, new or used, be formatted with SDFormatter and tested with h2testw1.4 before using them.

## Format and Test Flash Media

Using SDFormatter, do a clean format:

(While SDFormatter was designed for SD-cards, it can format USB thumb-drives for error testing. For those who would prefer a formatter specifically for a USB thumb-drive; HPUSBDISK.EXE )

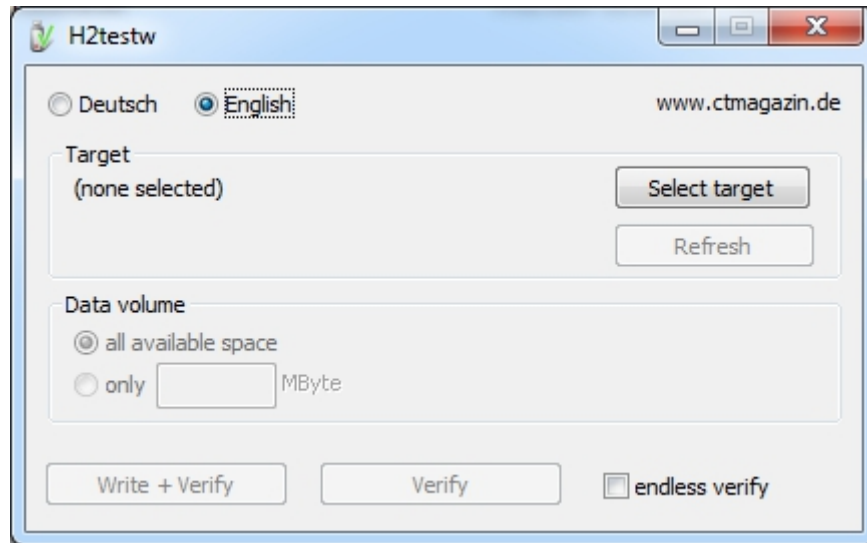
SDFormatter will detect a USB thumb-drive. A volume label is optional and the default options are fine.



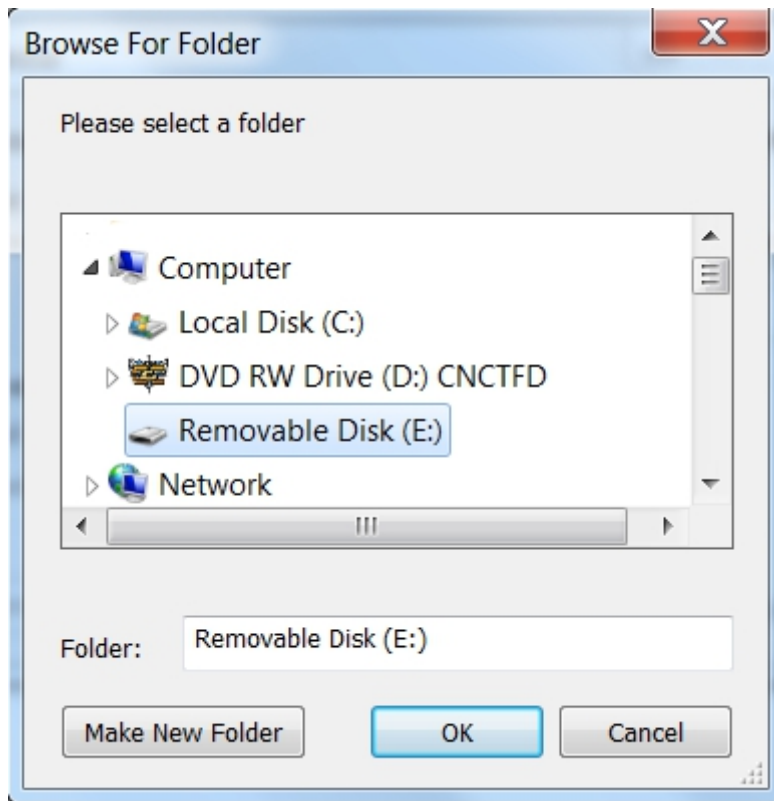
Click on **Format**

After the drive format is completed, open h2testw and select your language.

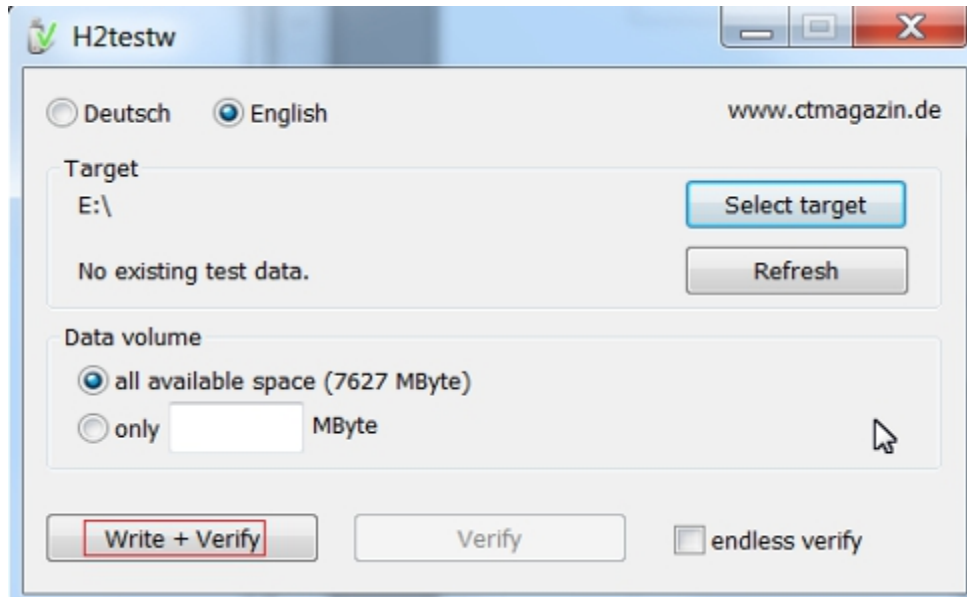
Then, click on **Select target**



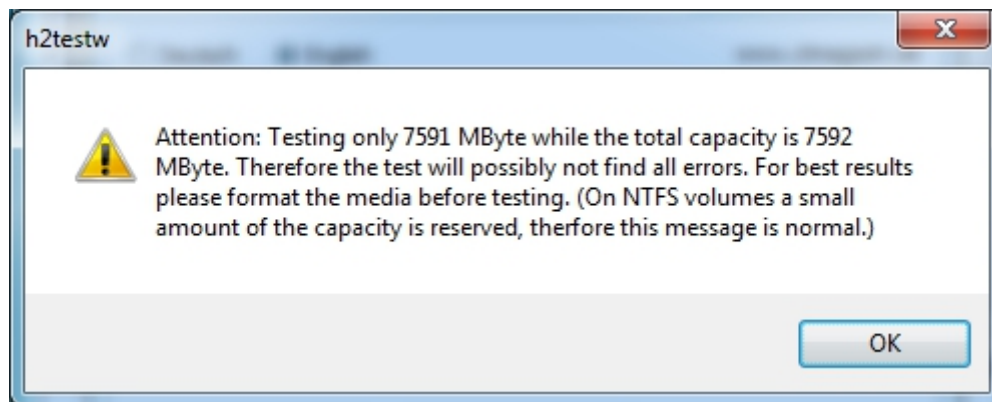
Under **Computer**, select the flash media previously formatted.



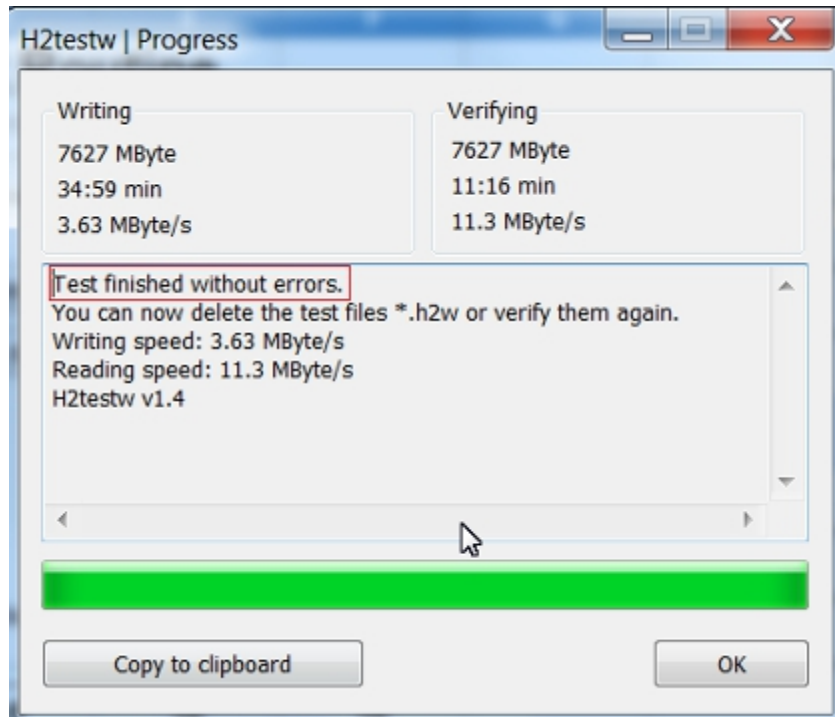
Select **Write+Verify**. (Do not check endless verify)



A dialog box similar to the following may pop up, drawing attention to a **1\*\*MB difference**. **Ignore it and click on \*\*OK.**



“**Without errors**” is the desired outcome. (If media tests with errors or is much smaller than is indicated by it’s labeled size, don’t use it.)



After H2testw verifies the USB thumb-drive, do one more clean format, using SDFormatter, before using the thumb-drive.

---

### 5.6.3 amd64 – Openmediavault Installation

If your PC platform won't boot onto a CD or USB thumb-drive with the installation ISO, it may be necessary to change the boot order in BIOS, to set the CD/DVD drive or USB boot to the top of the boot order. This link may provide assistance on this topic. → [How To Enter BIOS](#)

If difficulties are encountered during the ISO installation, consider the → [Alternate 64bit installation guide](#) Or use the [Wiki](#) .

---

An installation walk through:

**Boot Menu:** Select **Install**

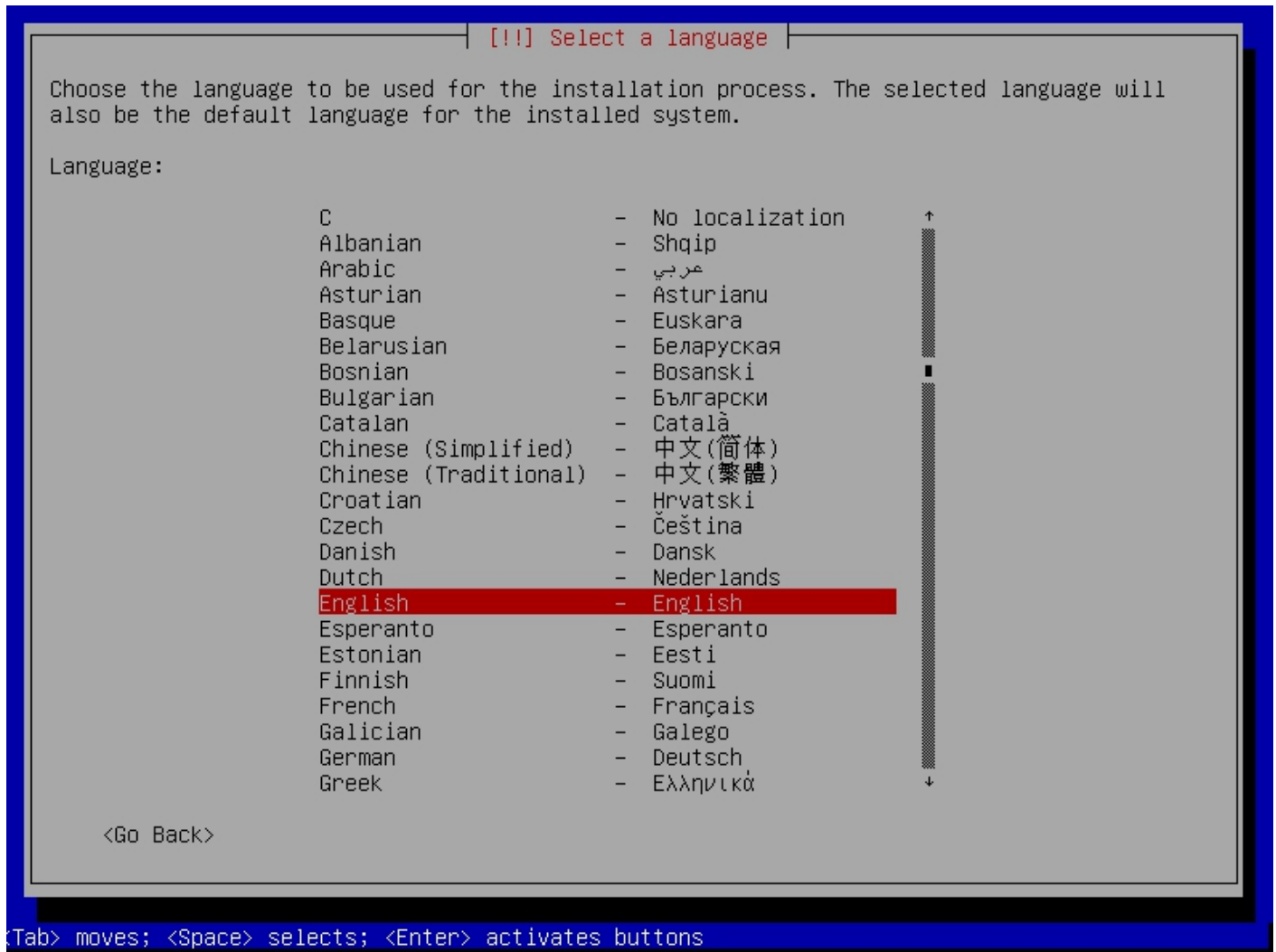


Boot menu

- Install
- Install (serial console)
- Advanced options >

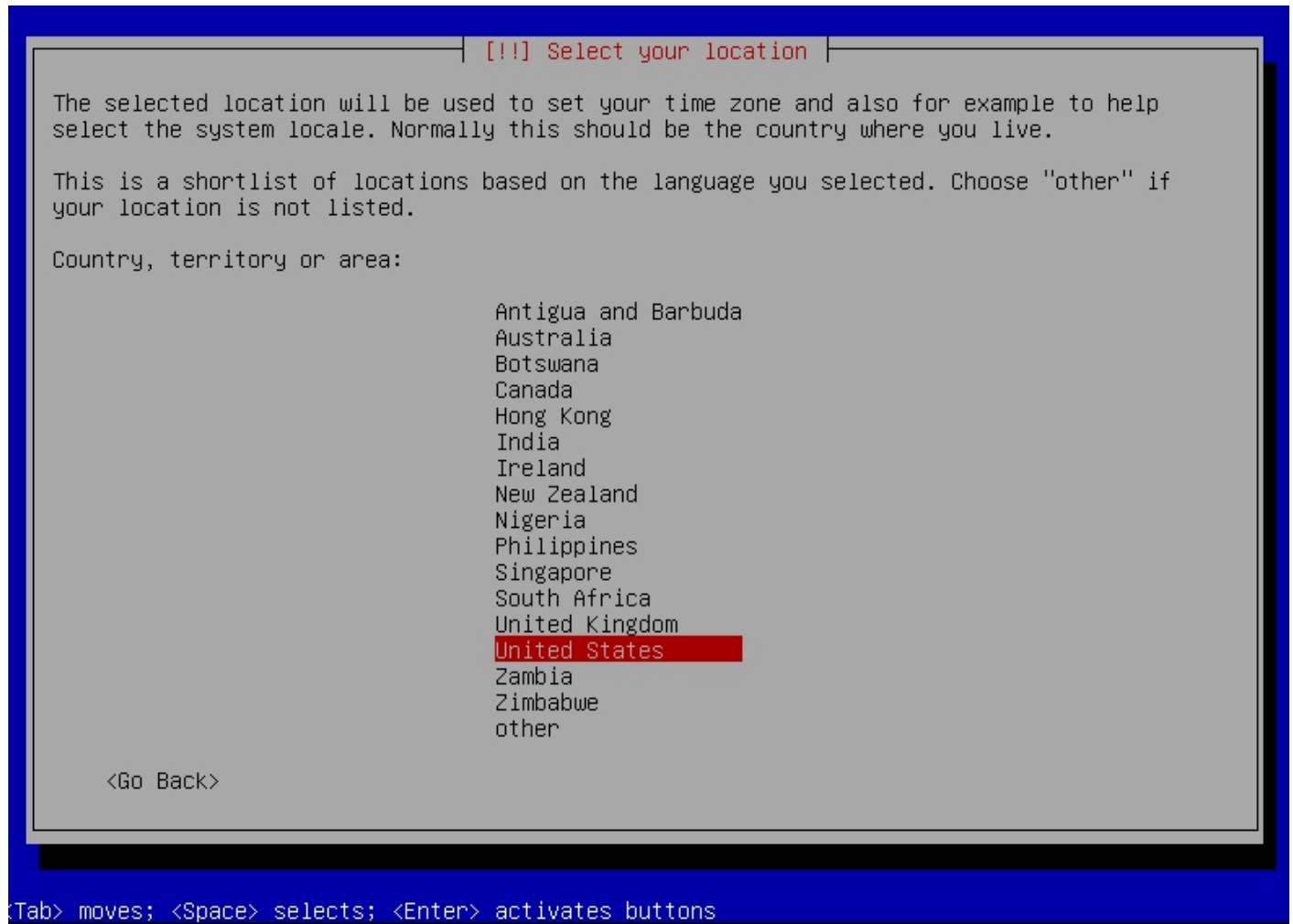
Press ENTER to boot or TAB to edit a menu entry

Select a Language: (As needed)

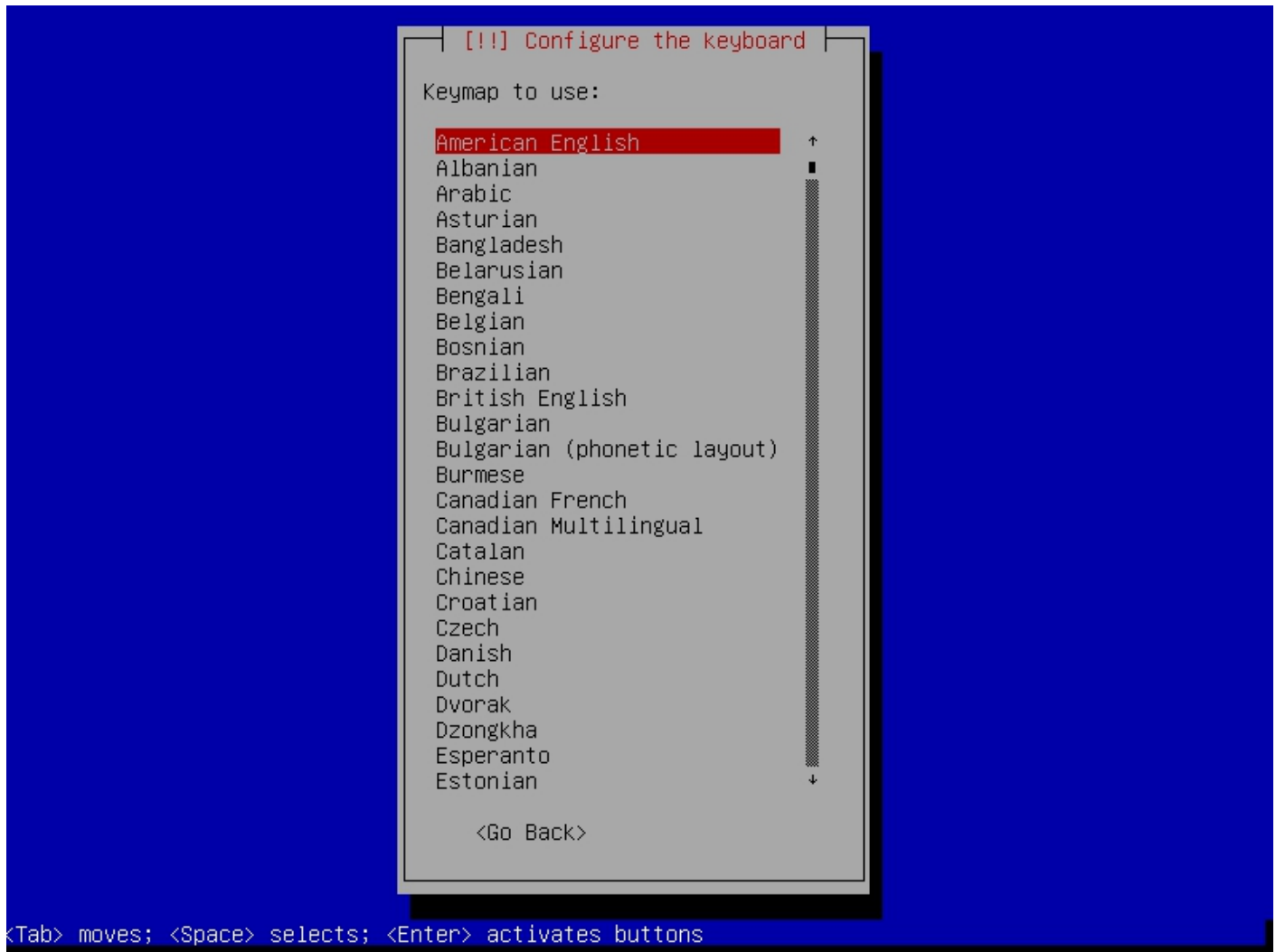


Select your Location: (As appropriate.)



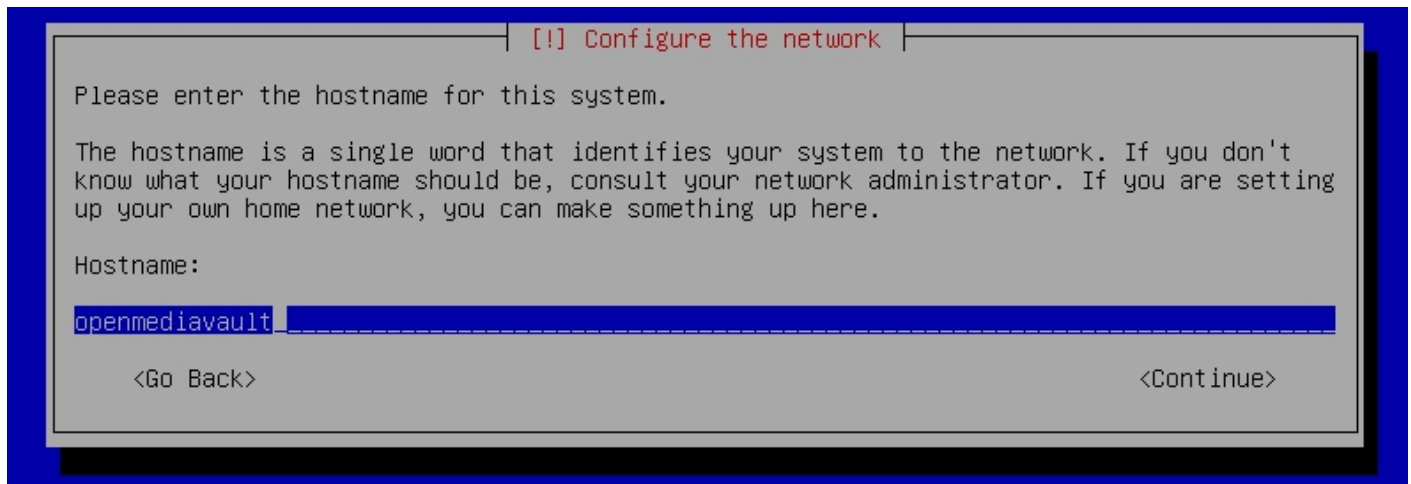


**Configure the Keyboard: (Select as appropriate)**



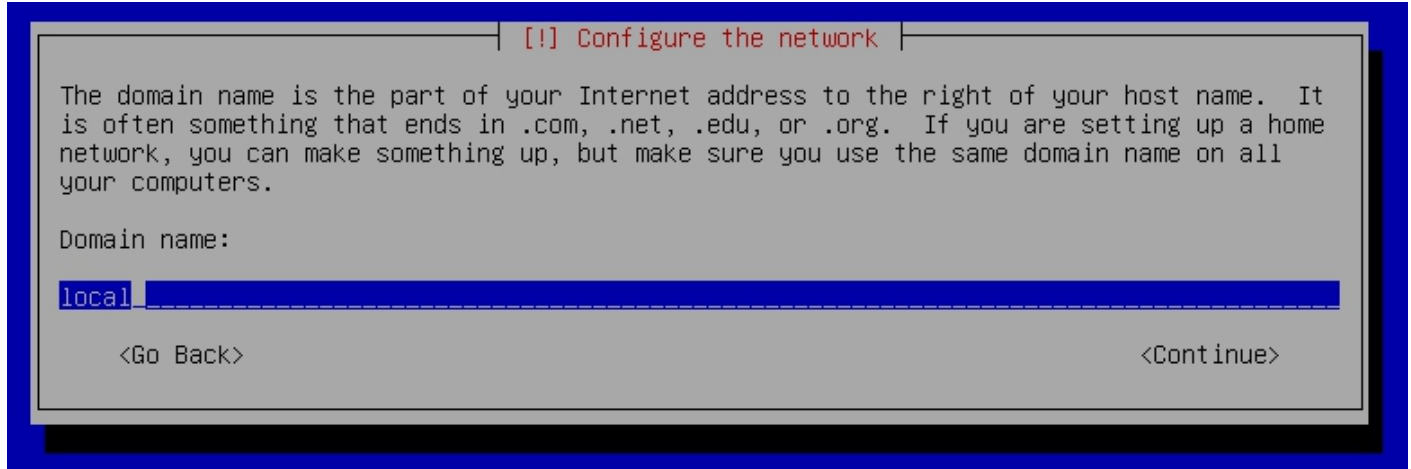
### Configure the Network:

While the default hostname is fine, a server name that is a bit shorter might be easier to work with later on. (Something like **OMV1**).



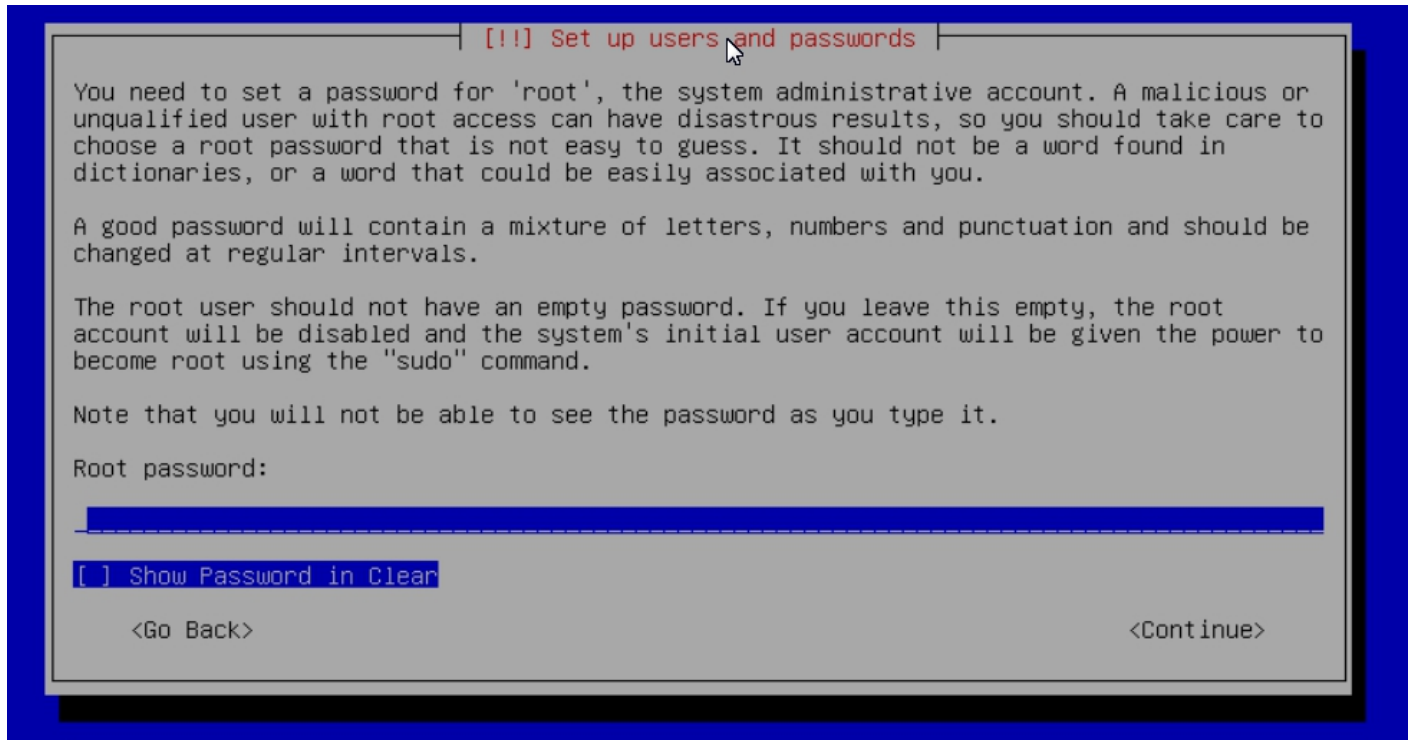
### Configure the Network:

If applicable, enter your domain name suffix. Otherwise, for home users and businesses with peer to peer networks, the default entry is fine.



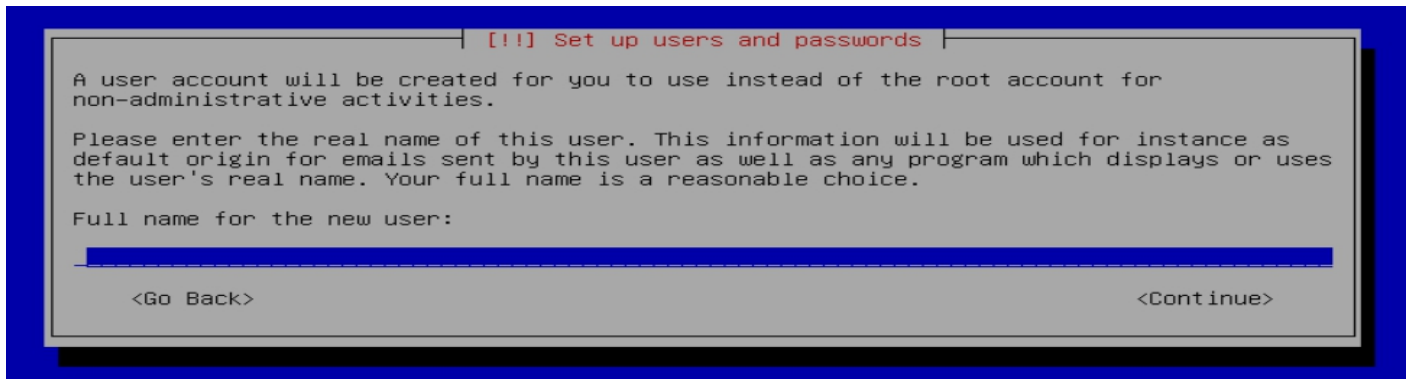
### Set up users and passwords:

Follow the on screen guidance for setting the **root password**. While not recommended, it would be better to write down the root password, then to forget it.



### Set up users and passwords:

Follow the on screen guidance for setting up a new admin user and password.



---

### Configure the Clock:

Select your time zone.

(NO PIC)

---

### Partition Disks 1:

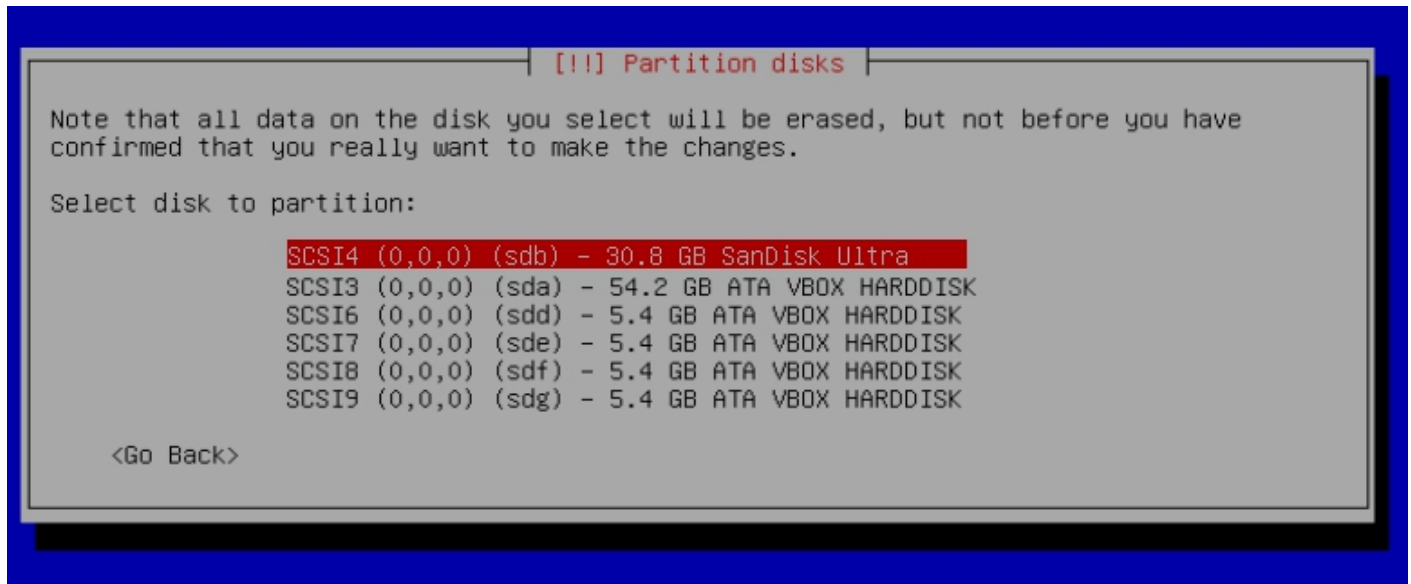
If two storage devices are available for installation, this screen is displayed.



---

### Partition Disks 2:

If installing to a single internal drive, there will be only one selection available. In this particular example, the installation is placed on a USB thumb-drive



Partition Disks 3:

(No Pic)

A 3rd window asks for confirmation of partition selections. Select Yes.

**Note:** If installing to a USB drive, at this point, it is possible to an error may pop-up regarding partitioning the drive, and recommend a reboot. Follow the recommendation. After the reboot, the partition operation should succeed the 2nd time around.

**The system installs.....**

**Configure the Package Manager: Debian Archive Mirror Country**

(NO PIC)

While the advice given in this screen is true, without testing, there's no way to know which Debian archive mirror is best. Without testing, picking your country or the closest location to your country would be the logical choice.

**Configure the Package Manager: Debian Archive Mirror**

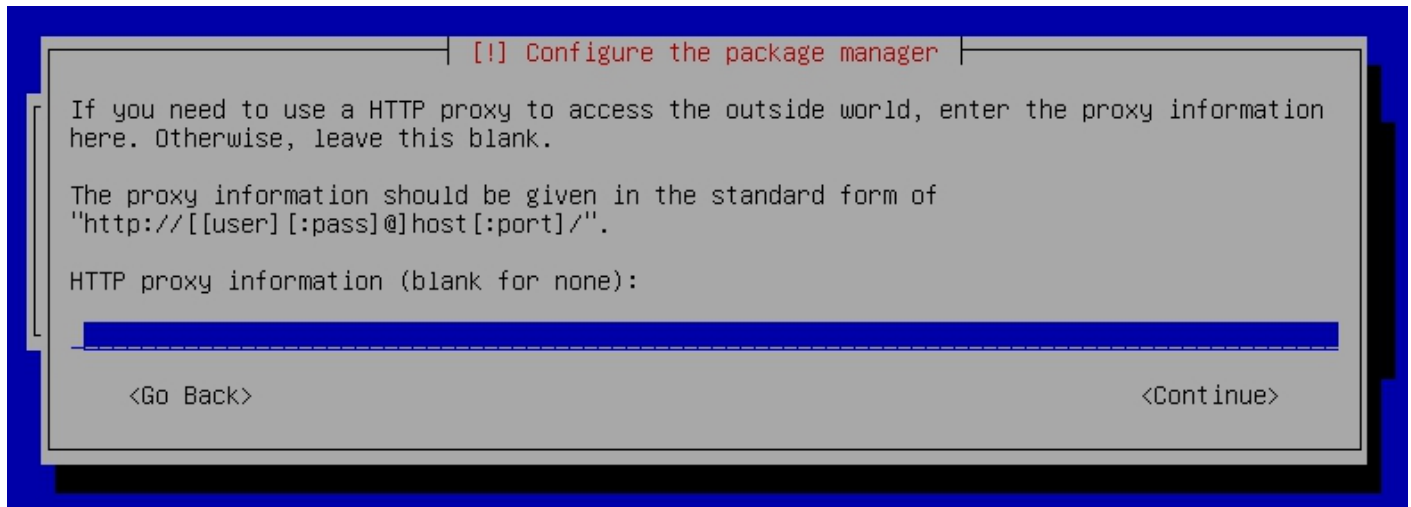
(NO PIC)

The default choice is usually best.

**Configure the Package Manager: HTTP proxy**

In most cases this entry will be blank.

(If a proxy is required, note the form of entry required in the dialog box.)



---

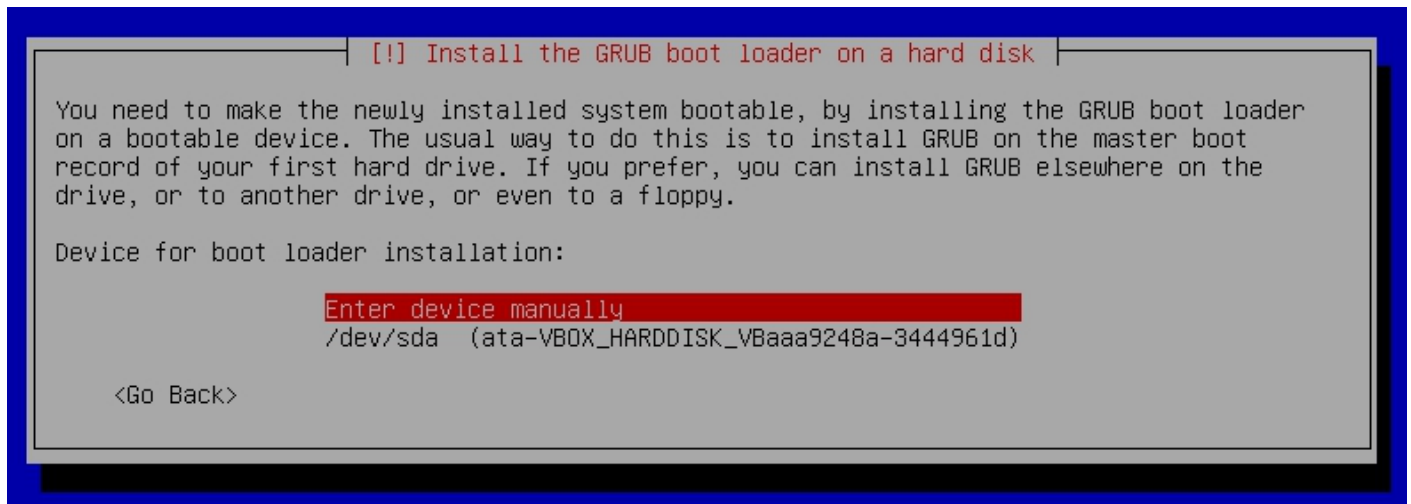
**Note:** If installing to a hard drive, the following screen may or may not appear.

---

#### Install the GRUB Boot Loader on a Hard Disk:

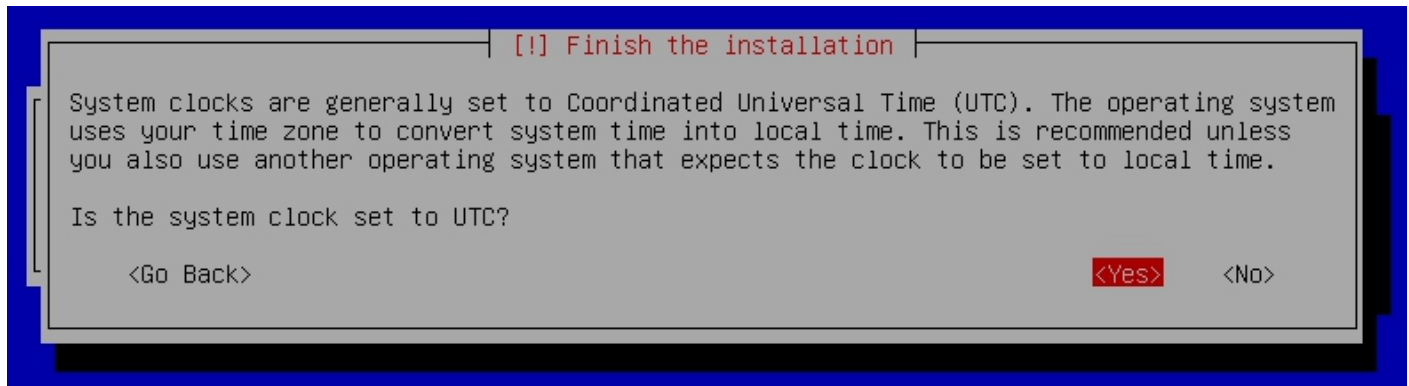
Select the appropriate boot disk in your server.

Generally the boot drive will be `/dev/sda` which is, in most cases, the first sata port.



---

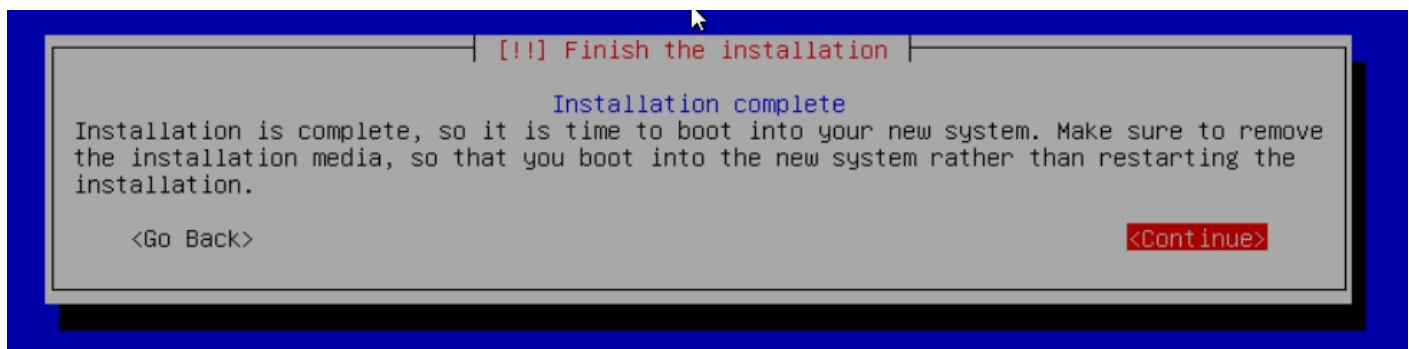
**Finish the Installation:** Accept the default.



### Installation Complete:

Remove the CD or USB installation source, then hit ENTER.

(Otherwise, the installation process may re-start.)



## 5.6.4 First Boot

Allow the installation to boot. Normally, the text above the login prompt will provide an **IP address** to be used for opening the console in a web browser. If an IP address is available, skip the following and proceed to *Initial Configuration*.

**Note:** There are two exception cases on the first boot that users should be aware of.

### 1.) No address from the DHCP server:

Normally, DHCP will assign an IP address to openmediavault and the address will be printed to the screen. However, on odd occasions the following issue may be observed.

```
openmediavault 3.0.94 (Erasmus) openmediavault tty1
Copyright (C) 2009-2017 by Volker Theile. All rights reserved.

To manage the system visit the openmediavault web control panel:
No network interface(s) available

By default the web control panel administrator account has the
username 'admin' and password 'openmediavault'.
It is recommended that you change the password for this account
within the web control panel or using the 'omv-firstaid' CLI
command.

For more information regarding this appliance, please visit the
web site: http://www.openmediavault.org

openmediavault login: _
```

This is usually due to a slow response from your DHCP server, during a fast boot process.

---

#### An easy method of finding the IP address is:

At the login prompt type `root`

Enter your previously set root password.

At the # prompt type: `ip addr`

```
root@OMV-Server:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eno1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
oup default qlen 1000
    link/ether 6c:0b:84:de:b4:59 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.55/24 brd 192.168.1.255 scope global eno1
        valid_lft forever preferred_lft forever
```

To access the WEB control panel, the IP address for the wired Ethernet interface is needed. In this case it's **192.168.1.55** (/24, the subnet mask, can be ignored.)

---

#### 2.) An odd IP address is assigned, that is not in the user's network:

In the following example, the actual network is 192.168.\*\*1\*\*.0/24



```
openmediavault 5.0.5-1 (Usul) openmediavault tty1
Copyright (C) 2009-2019 by Volker Theile. All rights reserved.

To manage the system visit the openmediavault web control panel:

enp5s0: 192.168.178.4
enp5s0: fe80::d99e:4b57:61a8:b72
virbr0: 192.168.122.1

By default the web control panel administrator account has the
username 'admin' and password 'openmediavault').
It is recommended that you change the password for this account
within the web control panel or using the 'omv-firstaid' CLI
command.

For more information regarding this appliance, please visit the
web site: https://www.openmediavault.org
openmediavault login:
```

This is usually a one time event where the fix is simple – simply login as root and type `reboot` on the command line. The address will be correct the second time around.

With a known IP address, proceed to *Initial Configuration*.

## 5.7 Initial Configuration

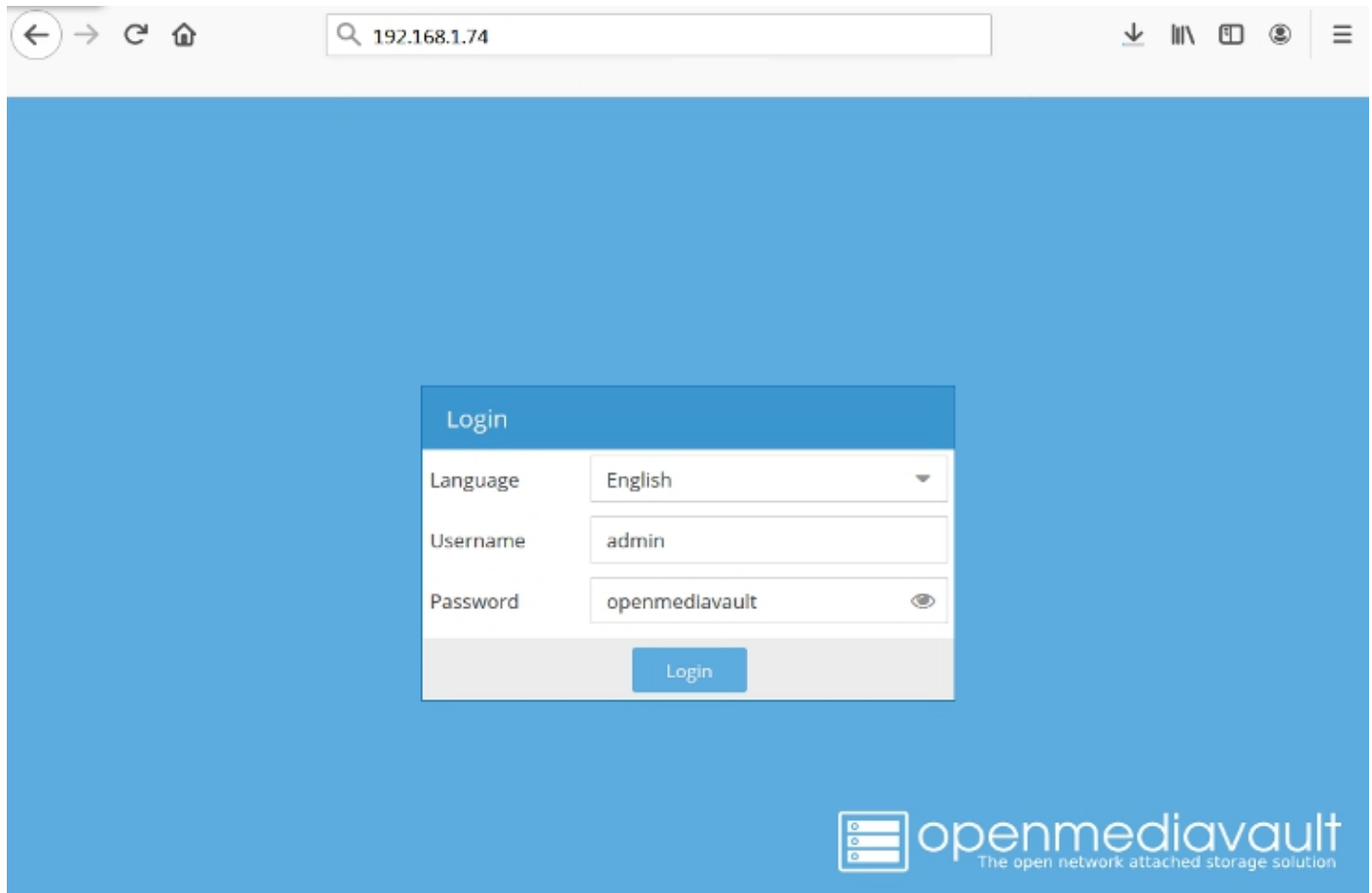
### 5.7.1 Web console login

In a web browser, type in the IP address provided by the first boot screen:

Set the language of your choice.

The user name is `admin` and default password is `openmediavault`

(In the following, by clicking on the **eye icon**, the default password is shown unmasked.)



---

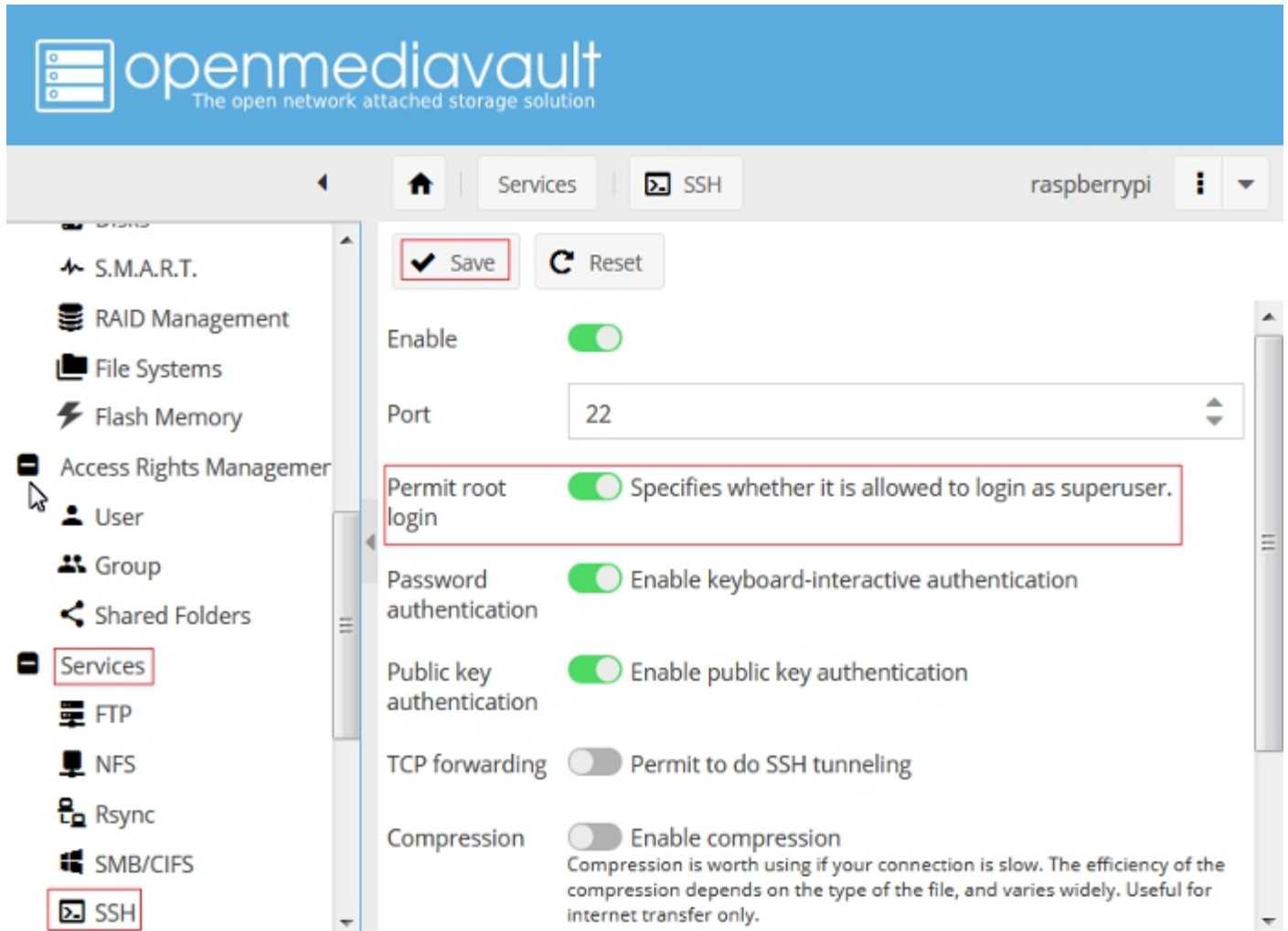
### SSH Login:

Under Services, SSH, check that the toggle switch for “**Permit root login**” is **ON** (Green) . If necessary, make the change and **Save**. After clicking on “**Save**” a yellow banner “**The configuration has been changed**” will appear. For the change to be applied, the **Apply** button must be clicked.

---

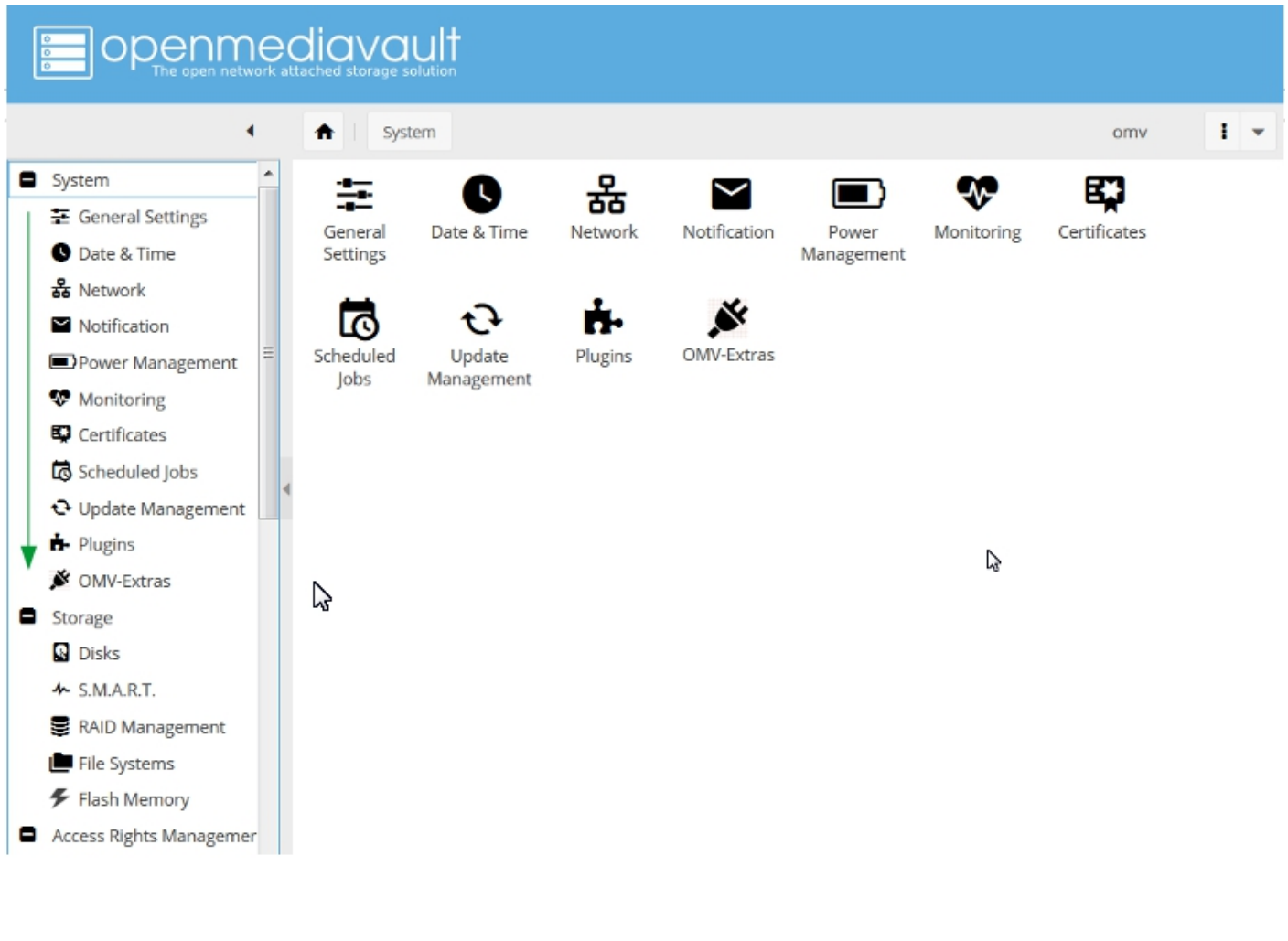
**Note:** The yellow confirmation banner is a final “SANITY” check and, in most cases, is required to finalize changes.)

---



## 5.8 Quick Start Guide for Advanced Users:

- In the left hand column, start at the top with **General Settings**, and work your way down, choosing and activating the services and features you need for your use case.
- For amd64 and i386 users, a static address for the openmediavault server and setting the address of a [public DNS server](#) is recommended. (SBC users, see the section, *Network Interfaces – SBC Users* .) As an example: Google's servers 8.8.8.8 and 8.8.4.4 support **DNSSEC** for better security, and “**Anycast**” which will direct DNS queries to a nearby server with low network latency. There are several choices for Public servers that support these features. [List of Public DNS Servers](#) .
- For a browsable network share, a minimum of one shared folder would need to be configured and that folder would need to be added to SMB/CIF to be visible on the network.



## 5.9 Basic Configuration

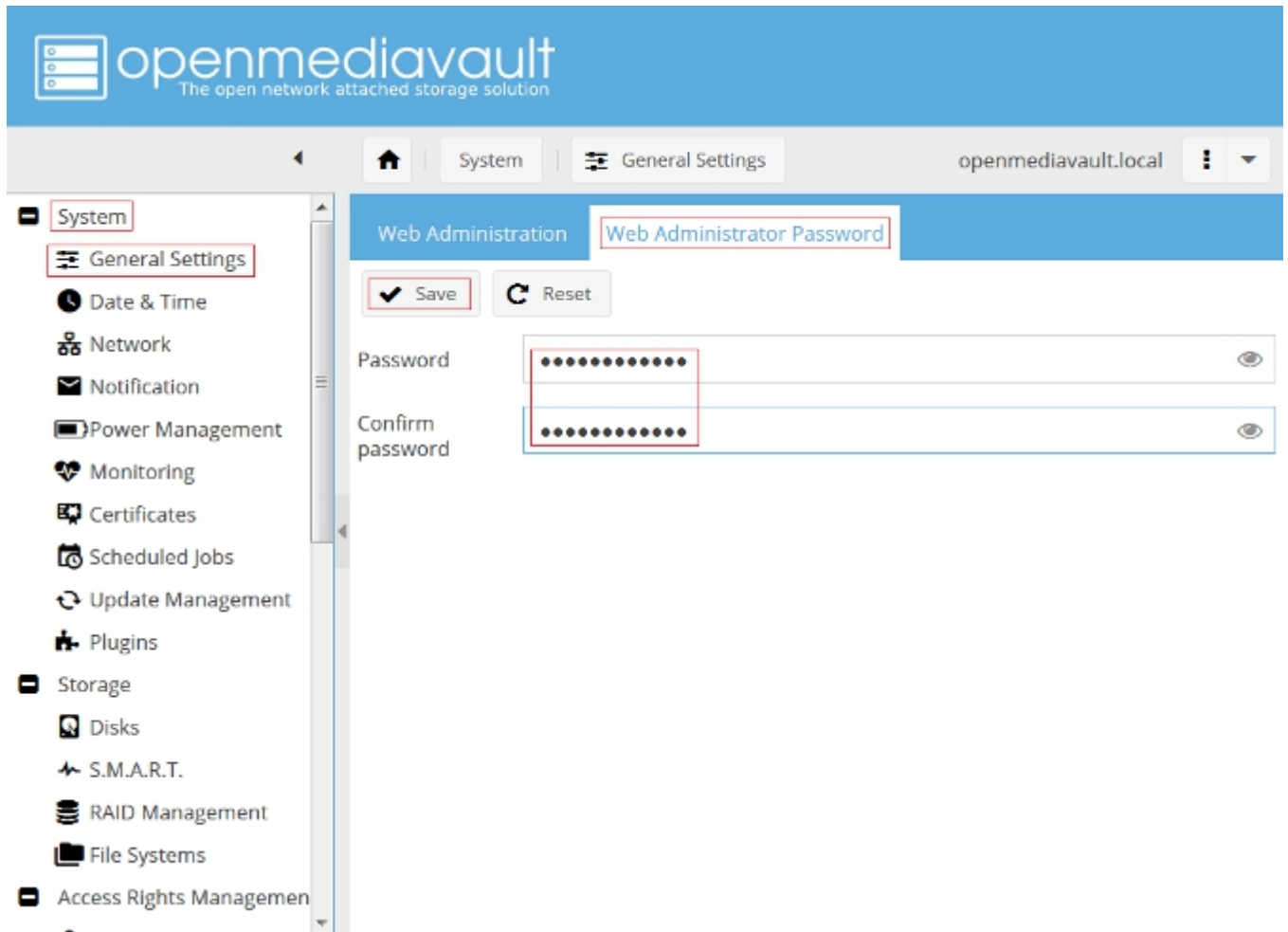
This section will guide new users through the initial setup of openmediavault. It addresses how to add a plugin, enabling OMV-Extras, how to setup a shared folder and make it browsable on the network with an SMB/CIF share.

### 5.9.1 System Settings

Under **System**, **General Settings**, in the **Web Administration** tab:

To allow a bit more time for configuration in the GUI, **beginners should consider lengthening the automatic log out time**. When the yellow banner appears, click **Apply**.

In the **Web Administrator Password** tab, enter a **strong password**, confirm it and Save. (This is one of a few instances where the yellow “confirmation” banner does not appear.) This setting changes the GUI login password. The user “**admin**” will remain the same.



### Under **System, Date & Time**

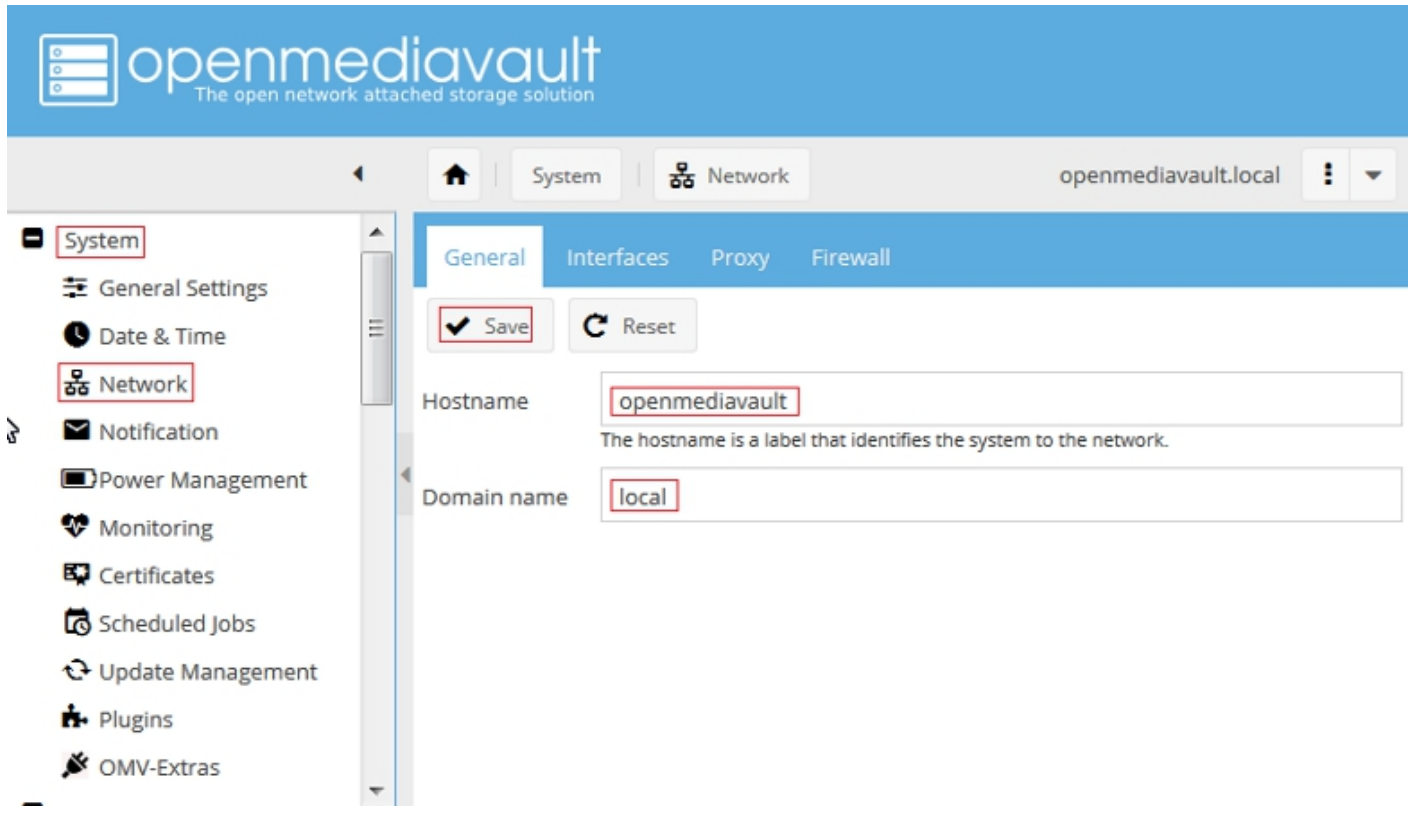
(No Pic)

Select your **Time Zone** and “toggle ON” **Use NTP Server**. When openmediavault toggle switches are **ON**, they’re green. **OFF** is gray.

### Under, **System, Network, General** tab.

**Hostname:** The hostname is the name that will appear on your network and on the command line. While the default is fine, the hostname can be changed here.

**Domain name:** If needed, the Domain suffix can be changed here. (Very few users will use Fully Qualified Domain Names.)



### Network Interfaces – SBC Users

Part of the **SBC** installation process is setting the wired interface to DHCP. SBC users should consider leaving their wired network interface set to DHCP, until [Docker](#) and [Portainer](#) are installed.

If a static IP address is needed:

Note that your SBC has been assigned an IP address by your LAN's DHCP server. (Typically, a router.) See your router's documentation for information on setting a "Static", or "Reserved" DHCP lease.

### Network Interfaces – i386/amd64 Users

Under, **System, Network, Interfaces** tab: Highlight / click on the **interface** found under the **Name** column, and click the **Edit** button. (As of the release of *\*\*Debian 9/OMV4\**, the interface name might not be the traditional **eth0**. A variety of names may be found, such as **eno1** or others. Use the first interface line/name found.\*)

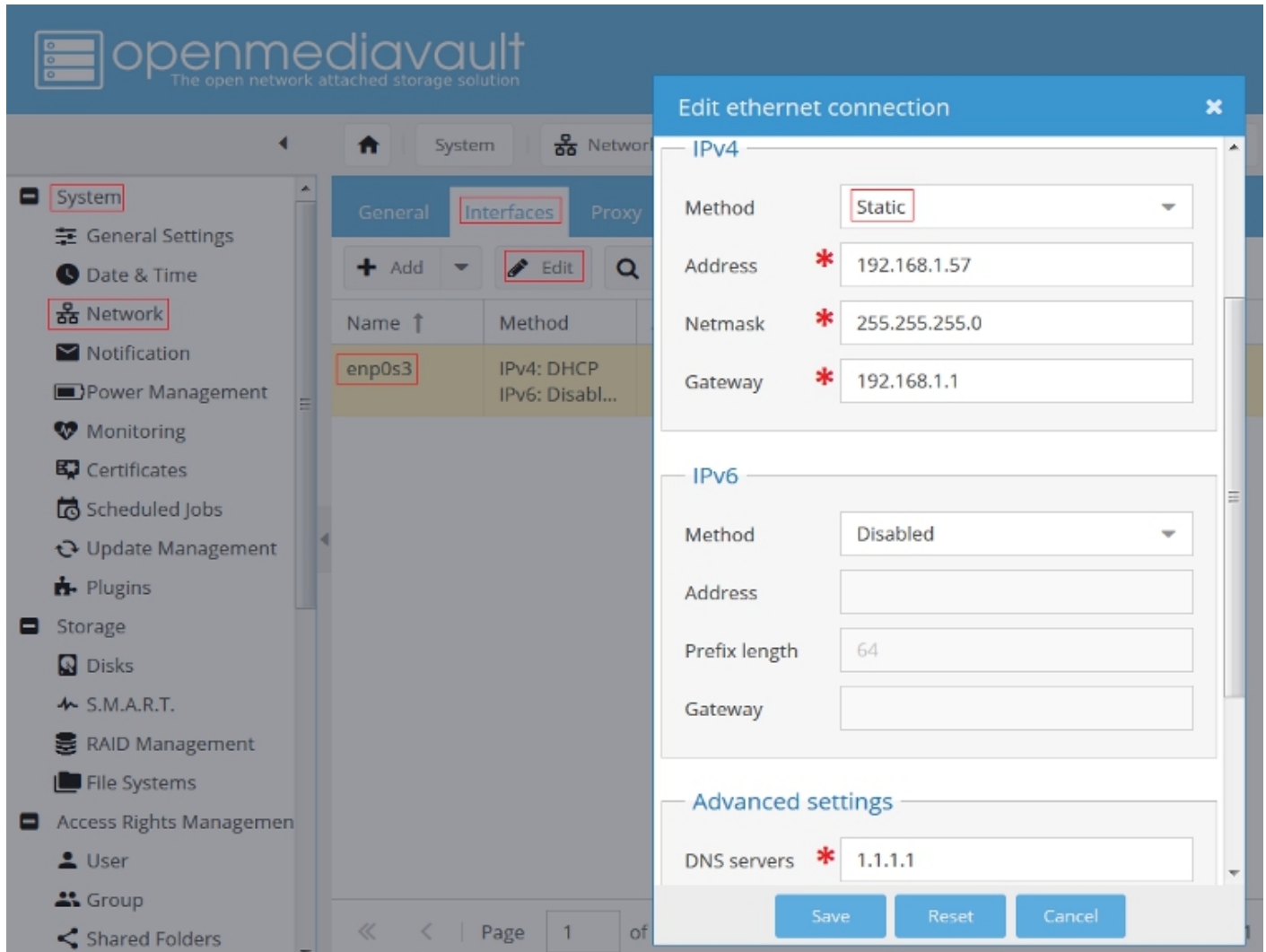
- It is recommended that users assign a static IP address to the new openmediavault server that is outside the range of the network's DHCP server.
- It is also recommended that users consider using a public DNS address. A list of public DNS servers is available → [here](#) . Use a server that supports **DNSSEC**, for better security, and **Anycast**, for low latency end point servers that are closer to user locations.
- The Netmask will be as shown, in most cases, and the Gateway address will be the address of the user's router.

---

**Note:** When saving a new static IP address, the user will be "going out on a limb and cutting it off".

---

Since the address provided by the network DHCP server is different from the static IP address chosen by the user, when the new address is changed, saved and applied, the GUI web page will stop responding. This is normal and expected. Type the new address, entered in the dialog box, into the URL line of your Web browser to reconnect.



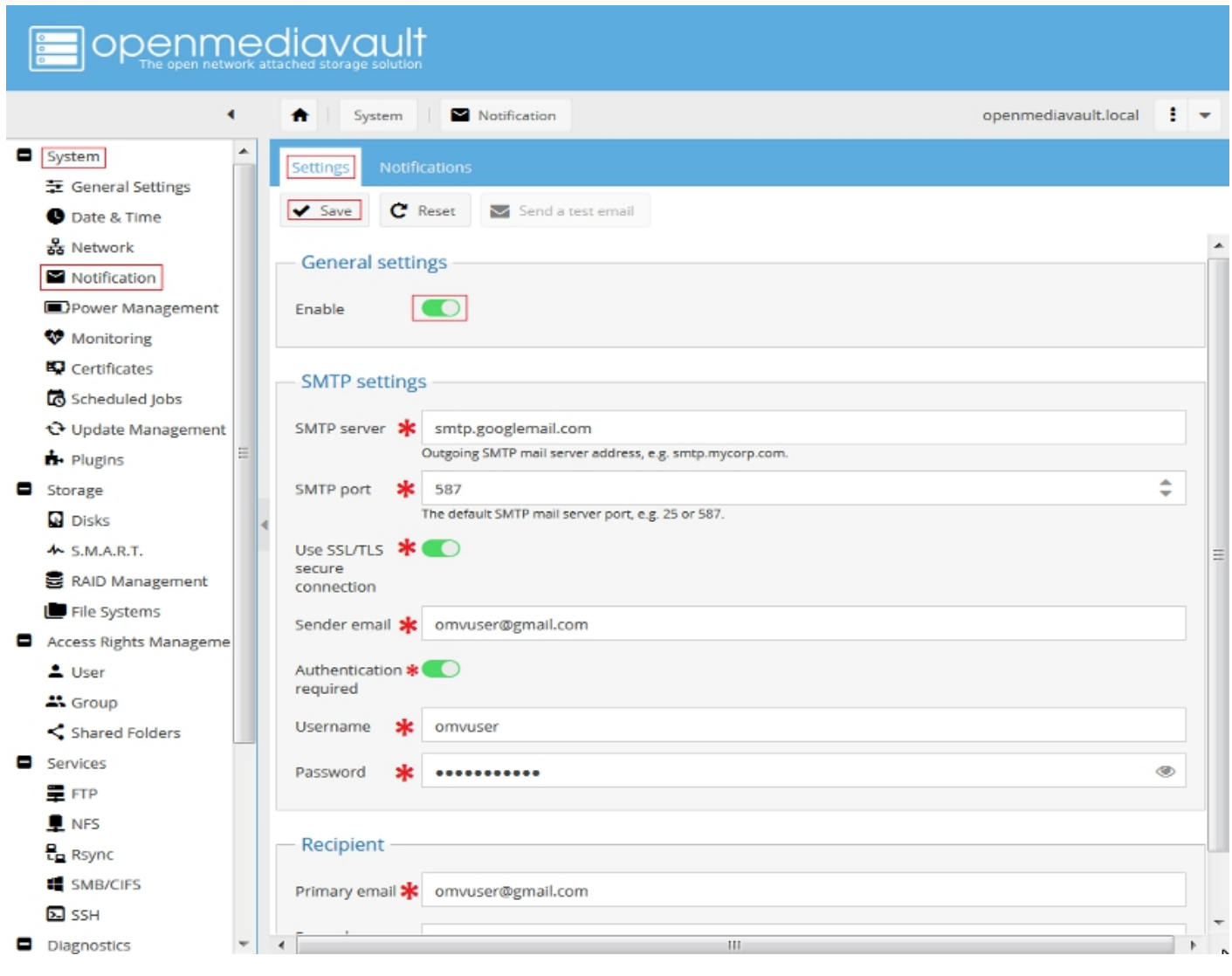
## Server Notifications

Under **System, Notification, Settings**:

If enabled, E-mail entries in the **Settings** Tab are required if users want to take advantage of automated server notifications and reports. Other actions and scripts, in **Scheduled Jobs** for example, can use this information to E-mail a report of task execution or status, as users may deem necessary.

To gather the required information for entry in the **Settings** Tab, users should refer to the settings for their E-mail clients. Note that most ISP's are using **SSL/TLS** secured E-mail connections.

**Fill in fields with user E-mail requirements and settings.**



The **Notifications** tab allows the selection of various functions for monitoring and error reporting.

If using a minimalist platform, such as older hardware or SBC's, E-mail's regarding system resources, memory, etc., may become bothersome. Unchecking **Enabled** boxes under **System** would eliminate excess E-mails, while maintaining **Storage reports** on hard drive health and file system errors.



The screenshot shows the OpenMediaVault web interface. The top navigation bar includes 'System' and 'Notification' tabs. The left sidebar shows the 'System' menu expanded, with 'Notification' selected. The main content area shows the 'Notifications' settings page. The 'Storage' section is expanded, showing 'Filesystems' and 'S.M.A.R.T.' both checked. The 'System' section shows 'Software updates' checked. The 'Save' button is highlighted.

Notification ↑	Enabled
Storage	
Filesystems	<input checked="" type="checkbox"/>
S.M.A.R.T.	<input checked="" type="checkbox"/>
Software RAID	<input type="checkbox"/>
System	
CPU usage	<input type="checkbox"/>
Load average	<input type="checkbox"/>
Memory usage	<input type="checkbox"/>
Process monitoring	<input type="checkbox"/>
Software updates	<input checked="" type="checkbox"/>

**Note:** Using Storage Notifications is *highly* recommended.

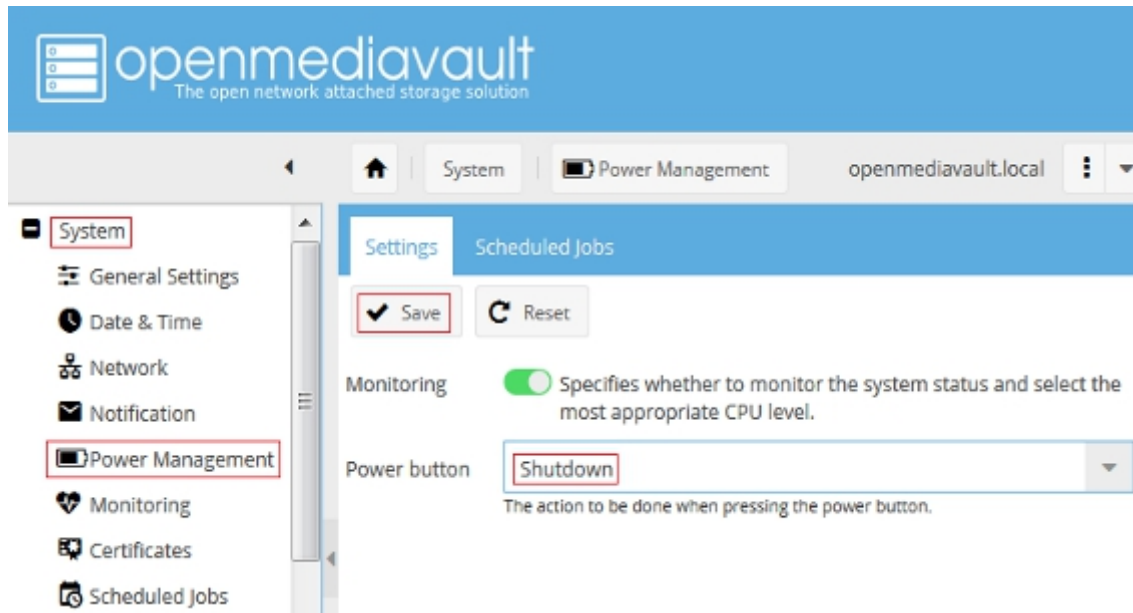
If SMART is **enabled**, under **Storage, SMART**, and short drive self-tests are enabled on spinning drives in the **Scheduled Tests** tab, the system may notify the user of hard drive errors *before* a hard drive fails completely.

For an explanation of drive self-tests and an example of how to set up a drive self-test, see the section; *Drive Self-Tests*

(Optional)

Under **System, Power Management**

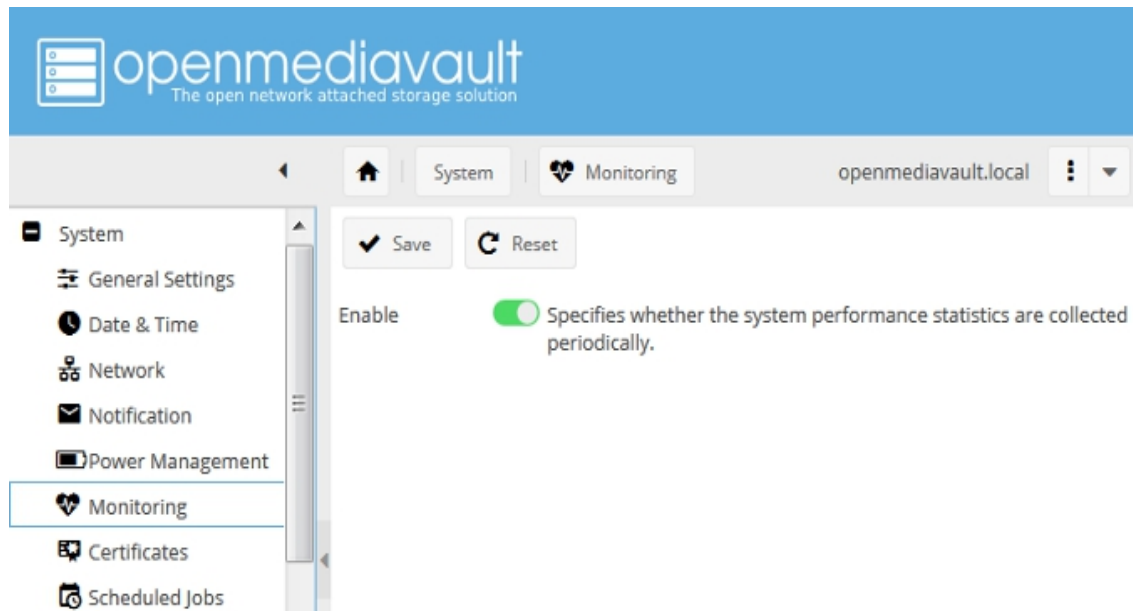
- In the **Settings** Tab, toggle **monitoring on** (recommended).
- In the Power button drop down, amd64 and i386 users should select the action preferred. Since power buttons are not available on some SBC installations, SBC users may chose to select “Nothing”.
- The **Scheduled Jobs** tab allows for the automation of a various power related tasks, such as an scheduled reboot.



(Optional)

Under **System, Monitoring**:

The initial recommended setting is **Enabled**. (Information gathered may be of use in diagnosing potential problems.)



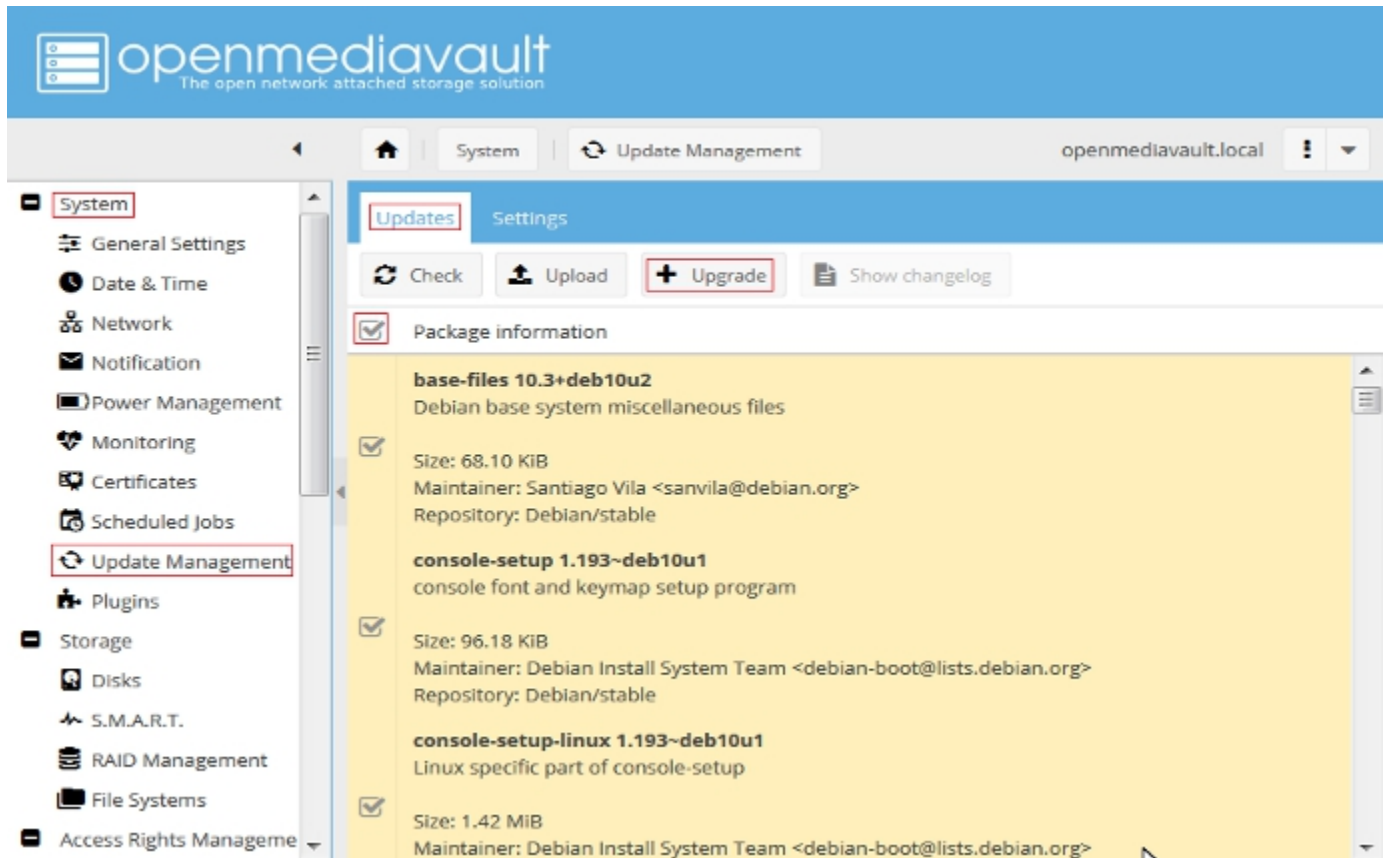
Under **System, Update Management**:

First, click on the **Check** button, to refresh available updates for your platform. (This may take a few minutes)

Checking the box by **Package information** will update all packages at once. (Recommended for beginners.) Otherwise, individual packages may be selected as desired or needed.

**amd64** and **i386** users may be offered a list of “firmware updates”. Select firmware updates that apply to your specific hardware. However, there’s no “penalty” for selecting firmware updates that do not apply.

Beginners should leave the 2nd Tab, **Settings**, with default settings.



## 5.9.2 OMV-Extras

**Note:** The following does not apply to SBC or i386 users. When using the scripted install, OMV-Extras is installed with OMV by default.))

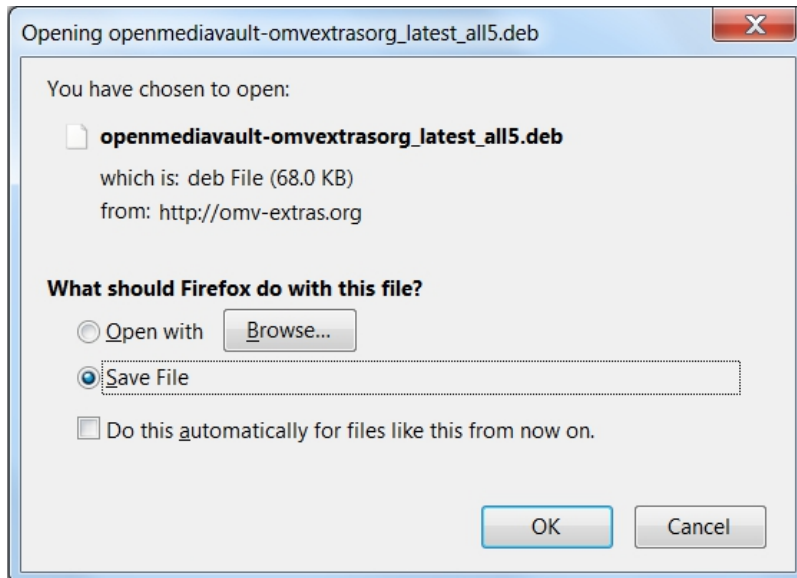
amd64 users will have a basic set of plugin's appropriate for a basic NAS / File Server. To enable the full range of plugin's available on openmediavault, the installation of OMV-Extras is required. For a preview of what is available visit [omv-extras.org](http://omv-extras.org) and select the version of openmediavault that's being installed.

**Note:** For **amd64** users who installed openmediavault on **SD-cards** or **USB thumb-drives**; The flash-memory plugin is **required** for flash media boot drives. Installing **OMV-Extras** is a prerequisite for installing the **flash-memory plugin**.

### Installing OMV-Extras

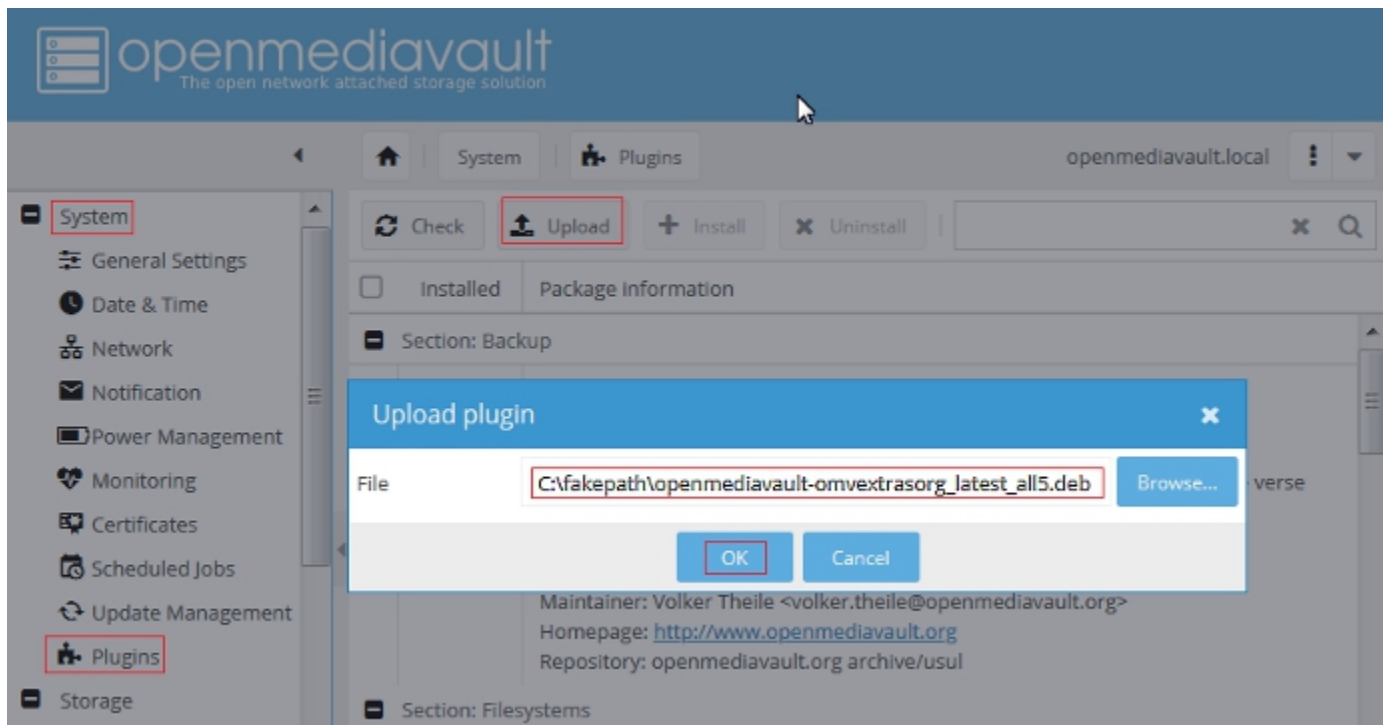
To enable OMV-Extras, a file is downloaded that will be used in the server console. Select the following link and download the associated file for OMV5.

→ [OMV-extras for OMV5](#)



Save the file.

Under **System, Plugins**: Click on the **Upload** button. **Browse** to the file downloaded, above. Select it and click **OK**.



A dialog window will popup that says, “Checking for Plugins”. (OMV-Extras is being added to the default plugin list.)

In the same window (**System, Plugins**) scroll to the bottom.

Select **openmediavault-omvextrasorg** and click the **Install** button.

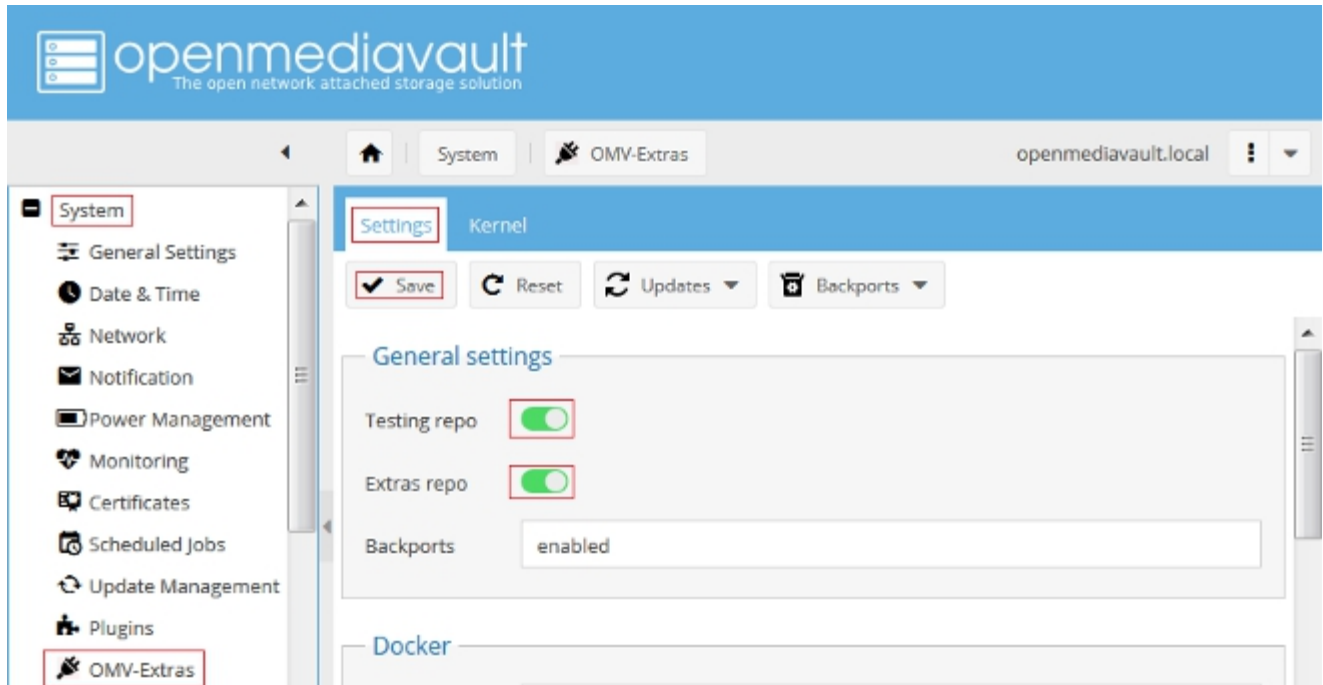
The screenshot shows the OpenMediaVault web interface. The top navigation bar includes 'System' and 'Plugins'. The left sidebar has 'System' and 'Plugins' highlighted with red boxes. The main content area shows a table of installed packages. The 'OMV-Extras.org Package Repositories for OpenMediaVault' package is highlighted in yellow, and its checkbox is checked. A mouse cursor is pointing at the 'http://omv-extras.org/' link.

Installed	Package information
<input type="checkbox"/>	<p>Network UPS Tools (NUT) is a client/server monitoring system that allows computers to share uninterruptible power supply (UPS) and power distribution unit (PDU) hardware.</p> <p>Size: 30.06 KiB  Maintainer: Volker Theile &lt;volker.theile@openmediavault.org&gt;  Homepage: <a href="http://www.openmediavault.org">http://www.openmediavault.org</a>  Repository: openmediavault.org archive/usul</p>
<input checked="" type="checkbox"/>	<p><b>openmediavault-omvextrasorg 5.1.11</b>  OMV-Extras.org Package Repositories for OpenMediaVault</p> <p>Allows enabling of multiple repositories hosted by omv-extras.org. The plugin allows installation of the backports kernel for increased compatibility with newer hardware. An apt cleaning function is also available for fixing repository cache problems and saving hard drive space in some instances.</p> <p>Size: 67.98 KiB  Maintainer: OpenMediaVault Plugin Developers &lt;plugins@omv-extras.org&gt;  Homepage: <a href="http://omv-extras.org/">http://omv-extras.org/</a>  Repository: /</p>

(Optional, but recommended)

Under **System**, **OMV-Extras**:

In the **Settings** Tab, highlight **OMV-Extras.org Testing** and click **Edit**. **Enable** and **Save**.



To insure that all plugins are available, go back to **System, Plugins**, and click the **Check** button. This will refresh the page and fully populate it with plugins that may be missing.

### 5.9.3 A Basic Data Drive

#### General

Openmediavault is capable of setting up basic Linux file systems in the GUI up to, and including, modern “Copy on Write” file systems such as ZFS which combine check summed files, RAID functions, and Logical Volume Management into a single package. However, advanced file systems add complexity which can make administration of a NAS server more challenging for a beginner.

Until some experience is gained, it is recommended that Linux/NAS beginners use single disks with a native Linux file system. In the processes described in the following, EXT4 will be used with a single data drive.

Some Windows users will want to use USB attached hard drives that are formatted NTFS by Windows. While this is possible, there are technical limitations to consider that are beyond the scope of this guide.

A far easier and better approach would be to format all server connected drives, using openmediavault’s GUI, and create a Samba share (SMB/CIF) for Windows clients, as described in [‘Setting up a Shared Folder’](#) and [‘Creating a SMB/CIF “Samba” share’](#). A Samba (SMB/CIF) network share understands the Windows file format and can be configured to accommodate DOS and extended file attributes. Samba serves as a transparent “translator” for Windows data storage.

#### RAID+USB = Potential Problems

Setting up RAID of any type using “USB to drive” connections is discouraged. RAID over USB has known problems. The USB interface (there are several flavors) may filter some the characteristics of hard drives, fail to pass SMART stat’s and ATA drive commands, delay the assembly of a RAID array, etc. While USB may work in some RAID cases,

it's not as reliable as using a standard hard drive interface. If RAID of any type is considered to be a requirement, drives should be connected with SATA or SAS ports.

If users choose to use RAID over USB connections, it is done at their own risk with the potential for the total loss of stored data. RAID issues involving SBC's, USB connected hard drives, or USB RAID enclosures are not supported on the forum.

RAID is often confused with backup which is far more important. For more information, see the explanation of backup, in *Backups and Backup-strategy* .

## Data Storage - Size matters

In general terms, beginners should do a rough calculation of their storage requirement. When selecting a data drive, the initial fill rate should be between 25 and 50%. As an example, if the calculated data to be stored on the NAS is 1TB, the selected drive should be between 2 and 4TB. With 50%+ drive free space (2 to 3TB) additional data can be accommodated, without the need to expand in the immediate future. When the fill percentage reaches 75%, it's time to plan for more storage.

---

## Data Drive Set Up

---

**Note:** Note for Beginners and SBC users: Openmediavault is designed to separate the Operating System (the boot drive) from data storage. This is "best practice" when setting up a server. Accordingly, openmediavault reserves the drive it is installed on exclusively for the OS. By default, the GUI will not allow the boot drive to be selected when creating a data share. A second hard drive or SSD is required for data storage.

---

With a data drive installed or connected.

Under **Storage, Disks:**

**Highlight the data disk** and click on **Wipe**. When prompted, click **Quick** and **Yes**. (*Reformatting a disk with GPT formatting present may result in an error. Simply re-run the wipe operation a 2nd time.*)

The screenshot shows the OpenMediaVault web interface. The top navigation bar includes 'Storage' and 'Disks' tabs. The left sidebar has 'Storage' and 'Disks' highlighted. The main content area displays a table of disks:

Device ↑	Model	Serial Num...	Vendor	Capacity
/dev/sda	VBOX HARDDI...	VB4c04b07...	n/a	50.52 GiB
/dev/sdb	VBOX HARDDI...	VBa74a38...	n/a	248.27 GiB
/dev/sr0	CD-ROM	VB2-01700...	n/a	7.70 GiB

At the bottom of the interface, there is a pagination control showing 'Page 1 of 1' and 'Displaying items 1 - 3 of 3'.

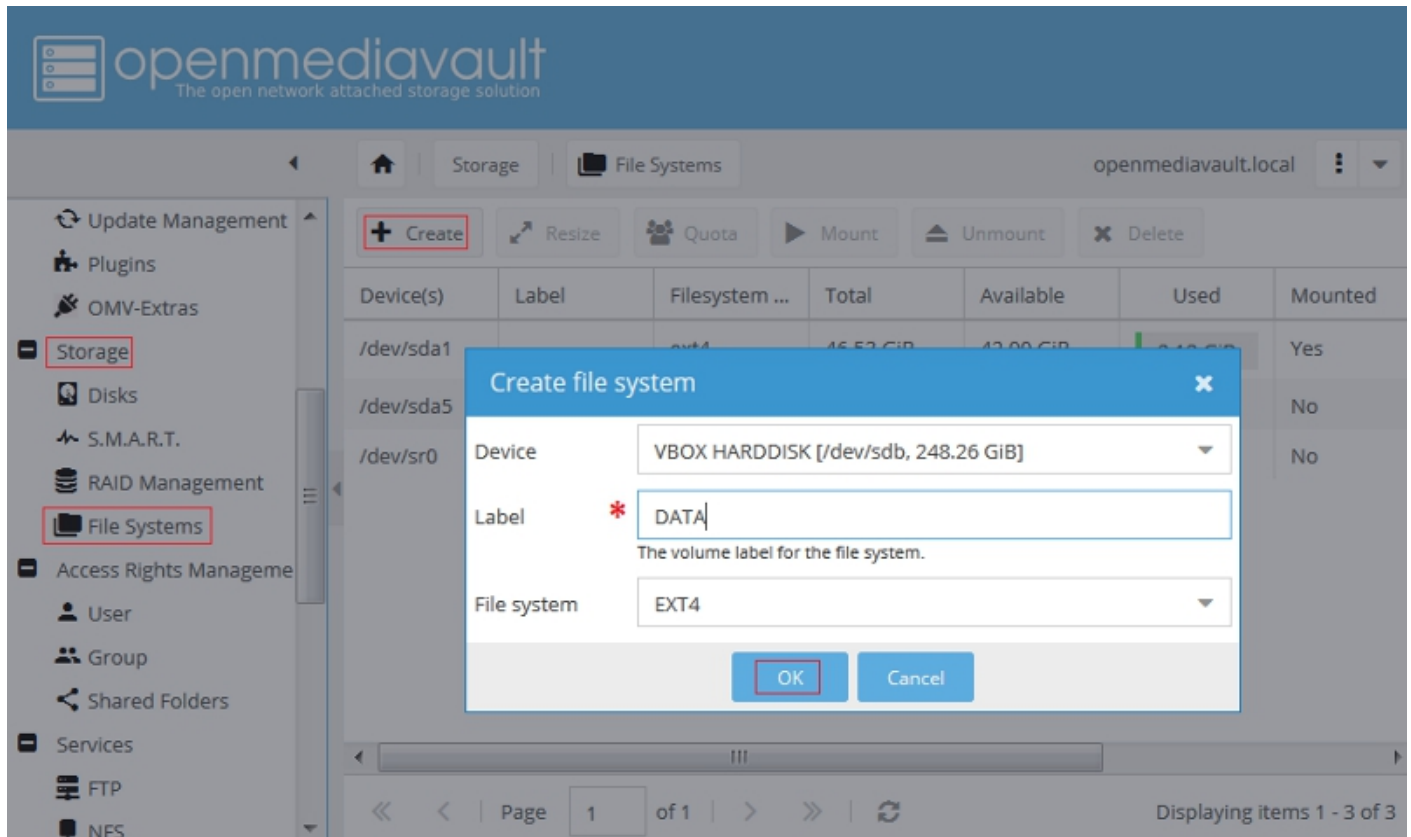
((The first device in the above list **/dev/sda** is the boot drive.))

#### Under **Storage**, **File Systems**:

Click on **Create**. In the Popup Window use the **drop down** to **select the drive** previously wiped. Provide a **Label** of your choice, accept the default File System **EXT4** and click on **OK**. Confirm the “format device” warning.

Allow a few minutes for the format to complete. When the message “**File system creation has completed successfully**” is displayed, click on **Close**.





#### In the same Window:

Click on the newly created **file system line**, and click on the **Mount** button. When the yellow confirmation banner appears, click on **Apply**.

The Data Drive is now prepared for a shared folder.

## 5.10 Creating A Network Share

Network shares are the primary reason for setting up and running a NAS. While easy access to data provides convenience to users, storing and backing up data in a centralized location makes it much more manageable.

### 5.10.1 Setting up a shared folder

The majority of the files and folders in a new openmediavault installation are controlled by the root user. One of the purposes of a **Shared Folder** is to set permissions that will allow regular users access to folders and files used for data storage. A shared folder could also be called a “base share”. The shared folder created in the following will be the foundation for creating a “**Network Share**”, covered later.

Under **Access Rights Management**, click on **Shared Folders**, then click on the **Add** button.

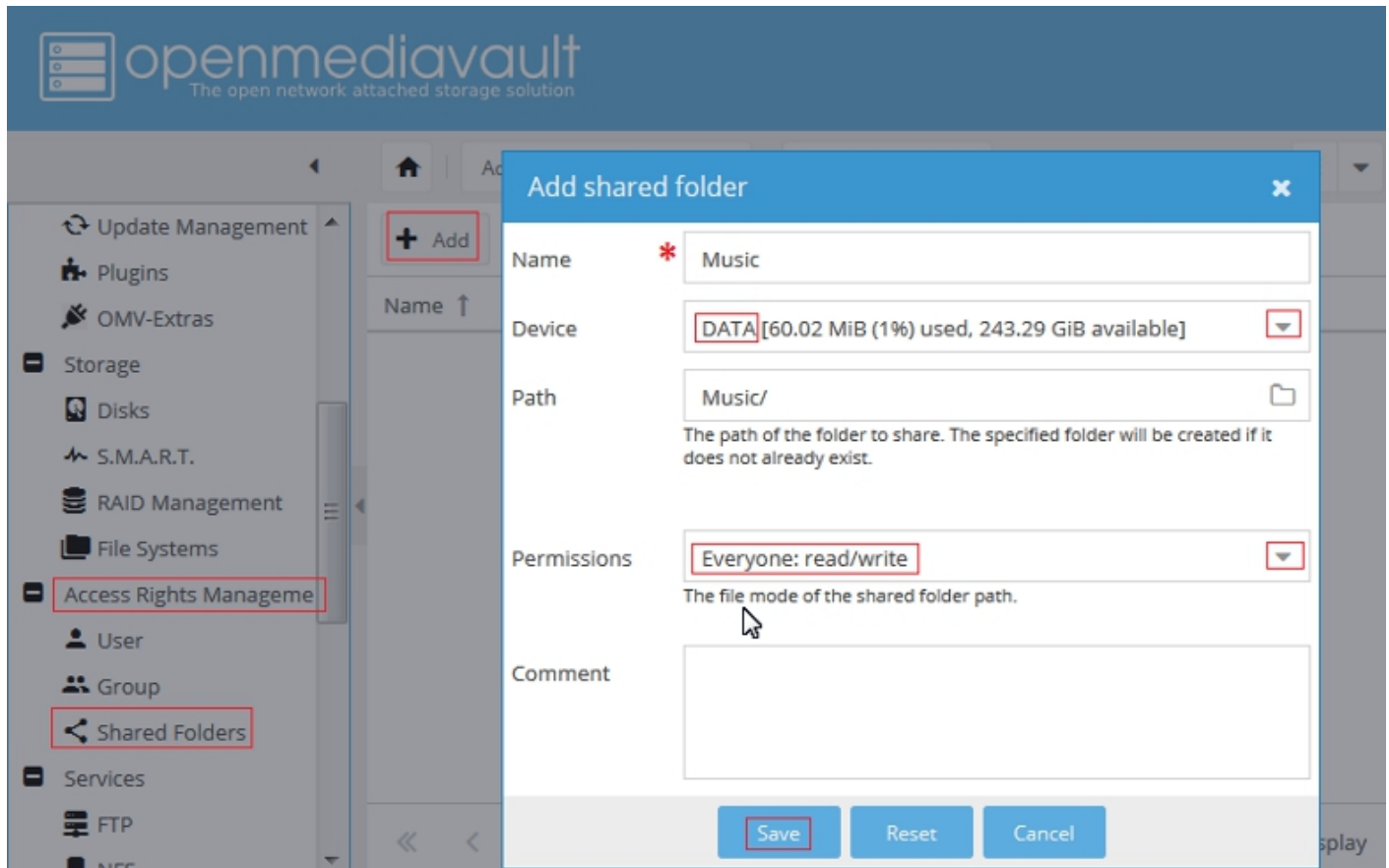
In the following example, next to:

**Name:** Add your new shared folder's **name**.

**Device:** Click on the drop down and select the drive that was previously added and formatted.

**Path:** Accept the default

**Permissions:** Click on the drop down and select **Everyone: read/write**



Click the **Save** button.

---

**The End Result:**

The screenshot shows the OpenMediaVault web interface. The top navigation bar includes a home icon, 'Access Rights Management', 'Shared Folders', and the URL 'openmediavault.local'. The left sidebar contains a menu with items: RAID Management, File Systems, Access Rights Management (highlighted with a red box), User, Group, Shared Folders (highlighted with a red box), Services, and FTP. The main content area displays a table with the following data:

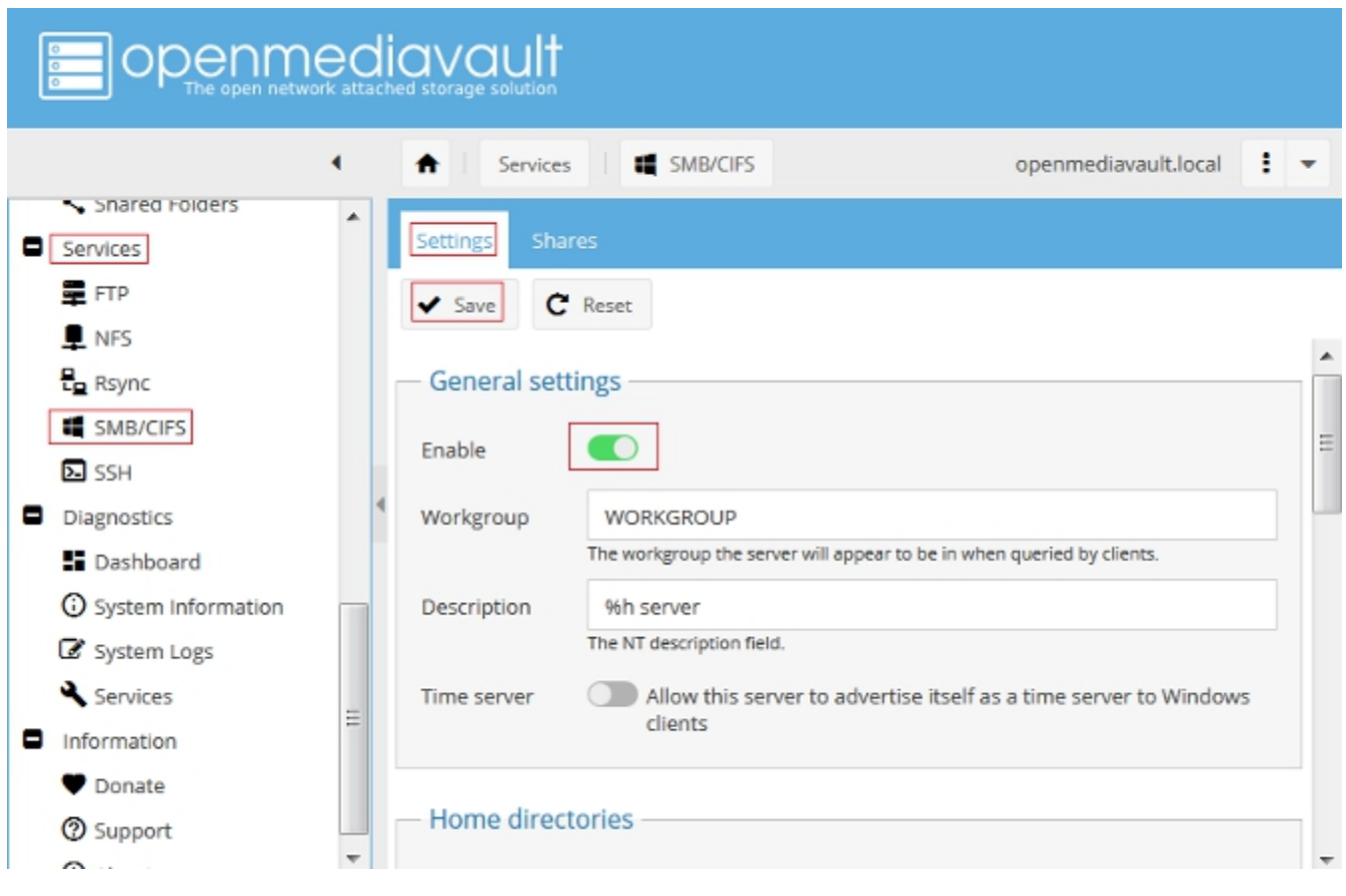
Name	Device	Relative Pa...	Comment	Referenced
Music	DATA	Music/		No

Below the table, there are navigation controls: '<< < | Page 1 of 1 | > >>' and a refresh icon. The text 'Displaying items 1 - 1 of 1' is shown on the right.

### 5.10.2 Creating a SMB/CIF “Samba” Network Share

In order to make your shared folder viewable in **Windows Explorer**, under **Network**, it’s necessary to make it a Samba share using the SMB (Server Messaging Block) protocol. Openmediavault makes setting up a Samba network share an easy task.

Under **Services**, click on **SMB/CIF**. In the **Settings** tab toggle **Enable** to **On** (green) and set your workgroup name. (In Windows, the default workgroup name is, WORKGROUP.) Leave the remainder of settings in this tab at their defaults, and click on Save. (Confirm with “**Apply**” when the yellow banner pops up.)



Click on the **Shares** Tab and the **+Add** button.

In the popup dialog box, set the following:

**Shared folder:** Click on the drop down and select **Music** (or the name for the shared folder previously created.)

**Public:** Click on the drop down and select the **Guests Allowed**

Scroll down with the right scroll bar and toggle **ON** (green), **Extended attributes** and **Store DOS attributes**.

(Leave the remaining settings at defaults.)

Click **Save** and confirm with **"Apply"** when the yellow banner appears. The final result should appear as follows.

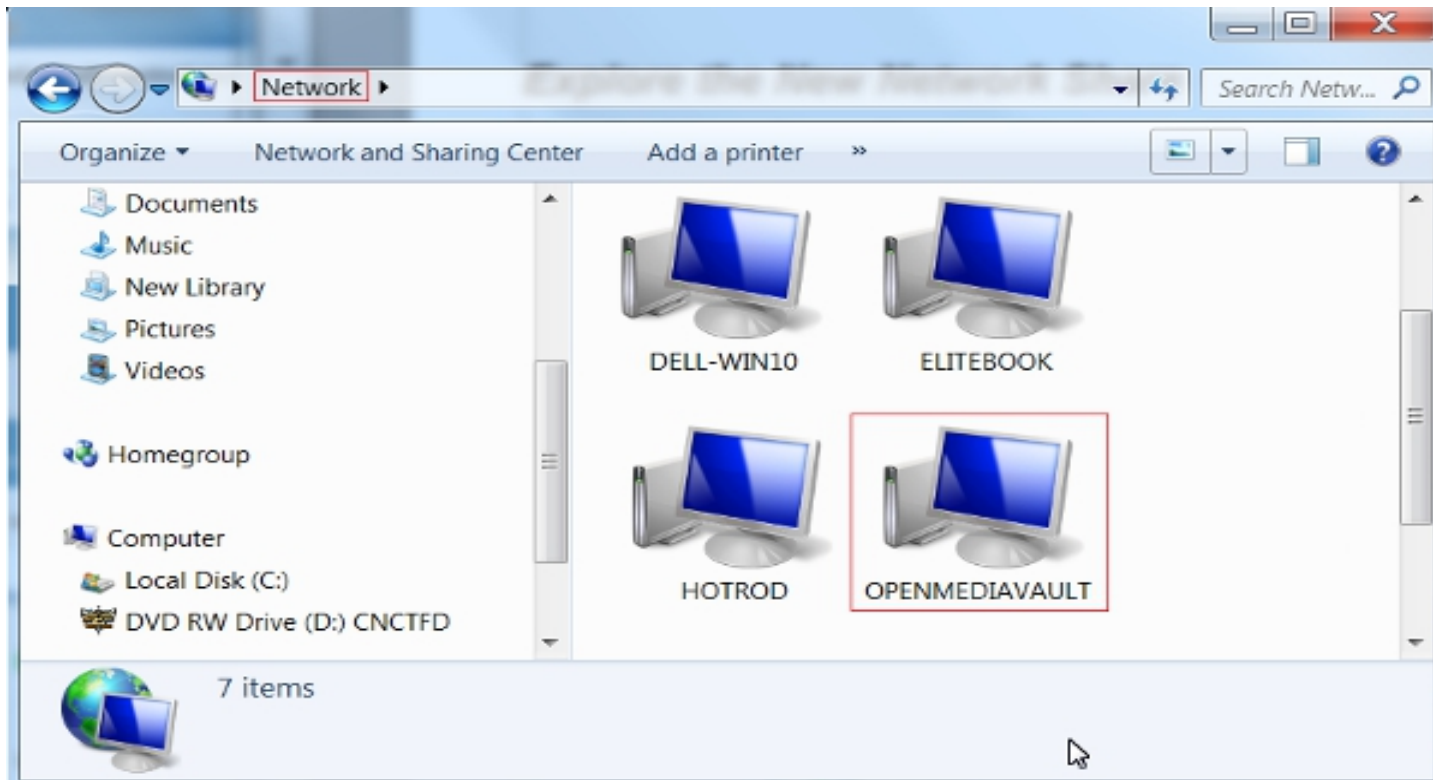
The screenshot shows the OpenMediaVault web interface. The top header features the OpenMediaVault logo and the tagline "The open network attached storage solution". The navigation menu on the left includes "Shared Folders", "Services", "FTP", "NFS", "Rsync", "SMB/CIFS", "SSH", "Diagnostics", "Dashboard", "System Information", "System Logs", and "Services". The "Services" menu item is highlighted. The main content area shows the "Shares" configuration page for "SMB/CIFS". The page has a "Settings" tab and a "Shares" tab. Below the tabs are "Add", "Edit", and "Delete" buttons. A table lists the shares:

Enabled	Shared fol...	Comment	Public	Read only	Browseable
<input checked="" type="checkbox"/>	Music		Guest allowed	No	Yes

At the bottom of the page, there is a pagination control showing "Page 1 of 1" and a refresh button. The text "Displaying items 1 - 1 of 1" is also visible.

### 5.10.3 Explore the New Network Share

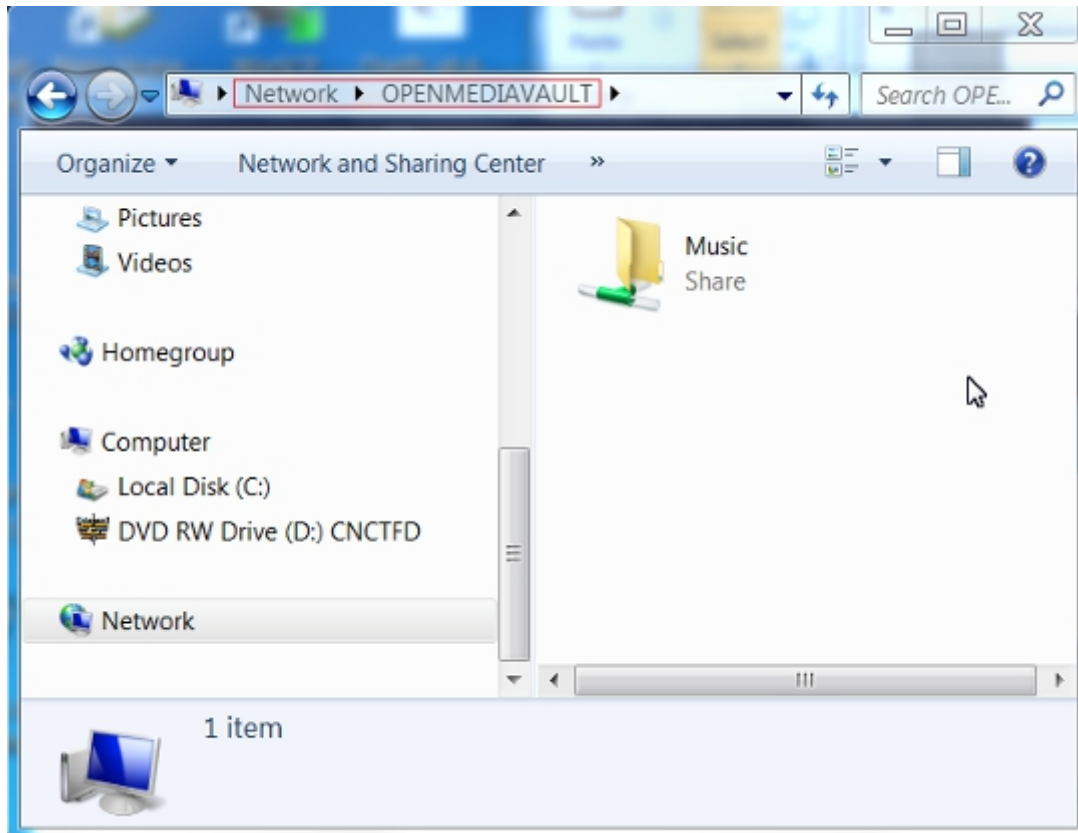
You should now have a browsable Server with a Network share named Music, so let's take a look. Open Windows explorer, scroll down to Network and click on it. There's the new server OPENMEDIAVAULT.



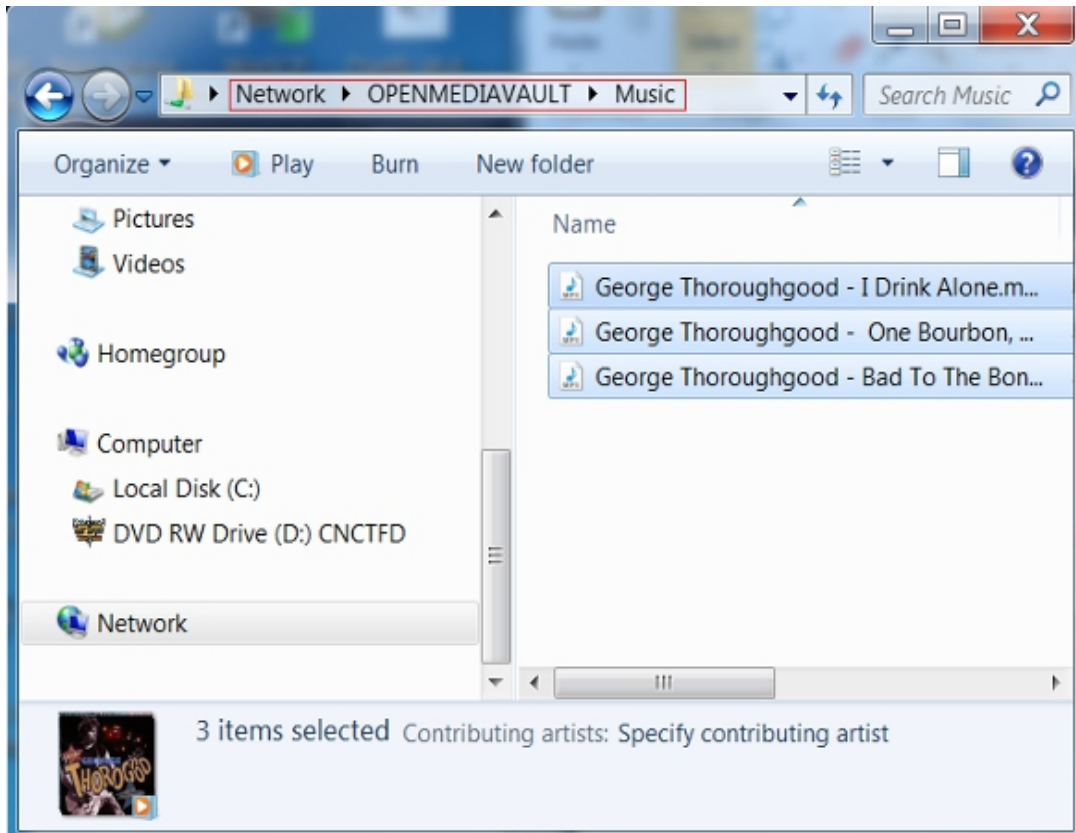
A few minutes may be required for the Windows Network to “Discover” the new server. If users are using **Windows 10 PC’s** and the server and share does not appear at a client, see this networking [How To](#) .

---

Now let’s look at the server’s new Samba share. It’s there and browsable.



This share is “writable” with a standard “Copy and Paste”, from a client PC.



Congratulations! You now have a functional NAS that can be expanded to accommodate additional network shares. Simply repeat the processes in *Creating A Network Share* to create and make additional shares visible on your network.

## 5.11 The Flash Memory Plugin - amd64 users only

**amd64** users who installed openmediavault **on flash media** will need to install the flash memory plugin.

### 5.11.1 Flash Media and Wear Leveling

While modern flash media drive is solid state, it's life is limited by the number of write cycles it can withstand before it goes "read only". When a specified number of flash memory blocks refuse to erase, the device's controller will set it "read only". At that point, the device's useful life is over.

To extend the life of flash media, most modern flash devices have **wear leveling** built into their controllers. If blocks are written, but not erased, they experience no wear. If blocks are erased, the next new write is set on adjacent blocks that have never been written before. As data is erased and written, blocks are used starting at the beginning of the device's addressable storage range and proceeding, in sequence, working toward the end. When the end of the range is reached, the process starts at the beginning and cycles through again. This wear leveling process avoids writing a single location to failure, and spreads wear evenly throughout.



With wear leveling and two drives of the same type, a drive that is twice the size will last roughly two times longer than the smaller drive. This may seem like is a strong vote for using a larger flash drive. However, when backups are considered, drives of twice the size also take twice as long to image and their image files are twice as large. (When using flash media as a boot drive, a practical trade-off should be considered in the suggested 16 to 32GB range.)

### 5.11.2 The Purpose of the Plugin

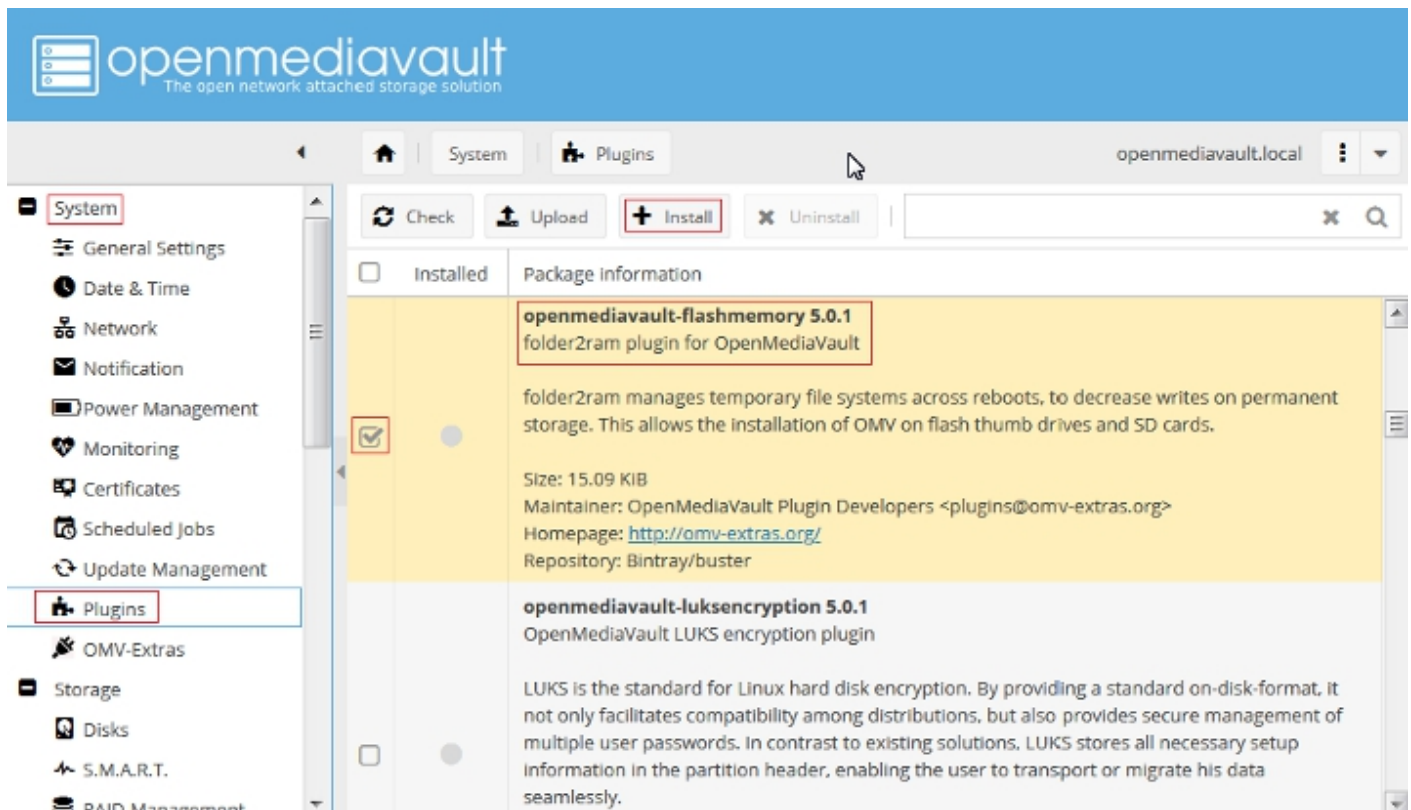
The primary purpose of the Flash Memory Plugin is to reduce the frequency of writes to flash media by consolidating very small writes into one, larger, bulk write. This reduces the number of blocks physically written to the Flash Device being used as the boot drive. The plugin can reduce the number of blocks written to the Flash drive by an order of magnitude or, potentially, 1/10th the amount that would otherwise be written. By extension, a drive of a given size might last up to 10 times longer than it would without the Flash Media plugin.

### 5.11.3 Installing the Plugin

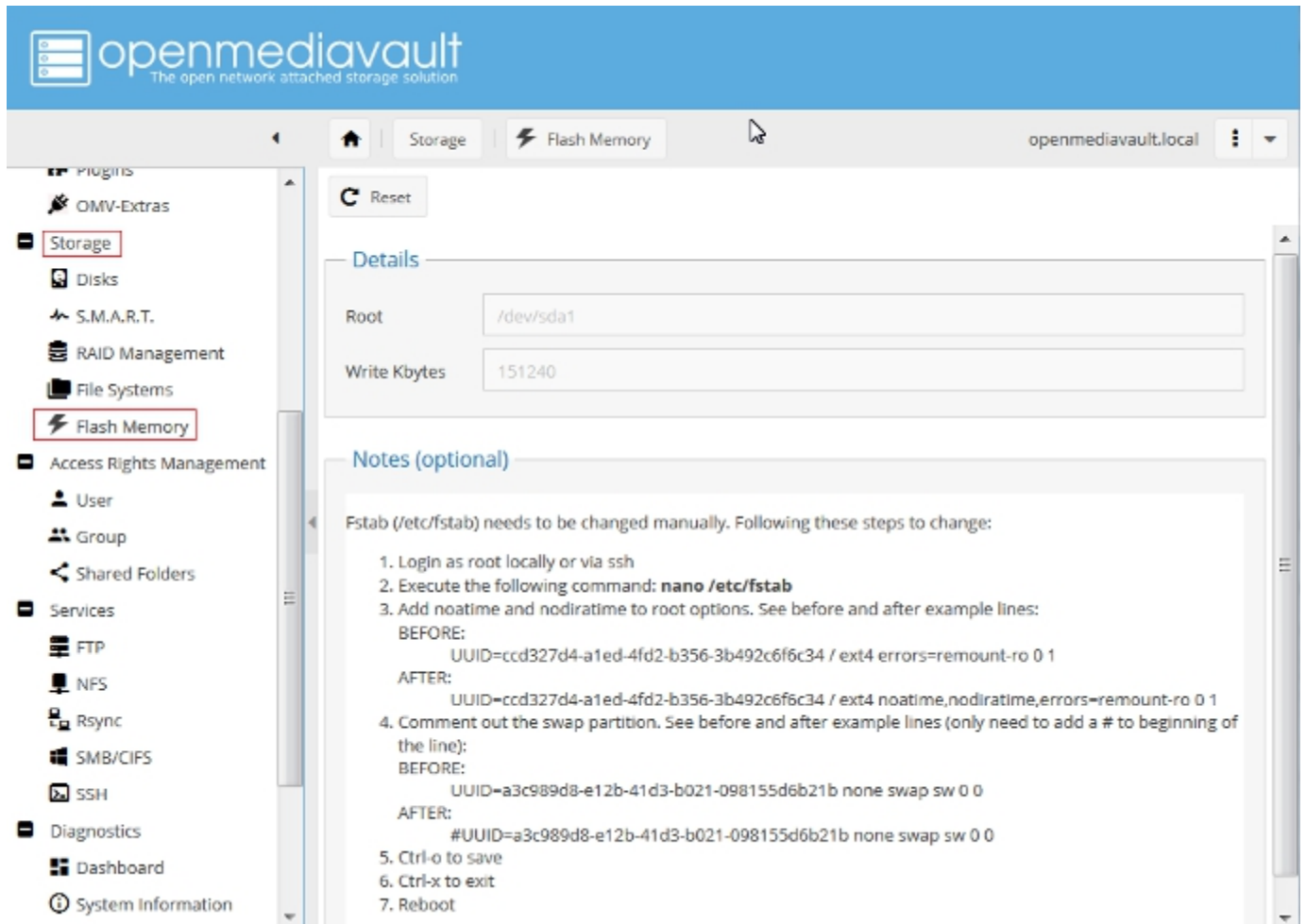
The prerequisite for installing this plugin is the installation of *OMV-Extras* . If *OMV-Extras* is not installed, it is required to proceed.

Under **System, Plugins**, scroll down to Section: **Filesystems**.

Select **openmediavault-flashmemory** and click the **Install** button.



Under **Storage, Flash Memory**, the following screen is now available.



The plugin will work as is, but it will be more effective if the guidance under **Notes (optional)** is followed. While this guidance shows steps for nano, following are options with guidance that beginners may find easier to implement.

## Flash Memory Plugin – Editing /etc/fstab

There are two options for editing /etc/fstab

- (Option 1) A Linux command line text editor
- (Option 2) WinSCP and Windows Notepad can be used if [WinSCP](#) is installed

### Option 1: Editing /etc/fstab with nano

The first example will use **nano**. This option requires the installation of PuTTY which is detailed [here](#).

Using PuTTY, SSH into the server. Log in as root and enter the root password.

On the command line, type the following and hit enter. `nano /etc/fstab`

**Note:** In nano, the mouse does not move the cursor. The cursor is moved by the keyboard's arrow keys to the insertion point. Type to insert text and use the backspace key to erase text if need. If a mistake is made, exit without saving and go back in again.

From the plugin's **Notes, Step 3:**

- First: We're going to add two statements **,noatime,nodiratime** to the / partition (the root partition) exactly as shown. The text addition is highlighted in green.
- Second: Note the partition with **swap** in it. Per Step 4, we're going to comment this line out using a **#** at the beginning of the line. The **#** is an addition, and is highlighted in green.

```

192.168.1.88 - PuTTY
GNU nano 2.2.6 File: /etc/fstab

/etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point> <type> <options> <dump> <pass>
# / was on /dev/sdb1 during installation
UUID=5111ffd4-47bd-4586-9077-edd65d21dae7 / ext4 noatime,nodiratime,errors=remount-ro 0 1
# swap was on /dev/sdb5 during installation
#UUID=c91cfa5d-f4ca-45e8-92f5-6357840f9c54 none swap sw 0 0
# Use a # to comment out this partition
# >>> [openmediavault]
/dev/disk/by-label/data /srv/dev-disk-by-label-data ext4 defaults,nofail,user_xattr,noexec,usrjquota=aguota.user,$
# <<< [openmediavault]

^G Get Help      ^O WriteOut     ^R Read File    ^Y Prev Page    ^K Cut Text     ^C Cur Pos
^X Exit          ^J Justify     ^W Where Is    ^V Next Page    ^U UnCut Text   ^T To Spell

```

Use **Ctrl+o** to save, then **Ctrl+x** to exit

Reboot the server. On the command line, the following command can be used: `reboot` **Done**.

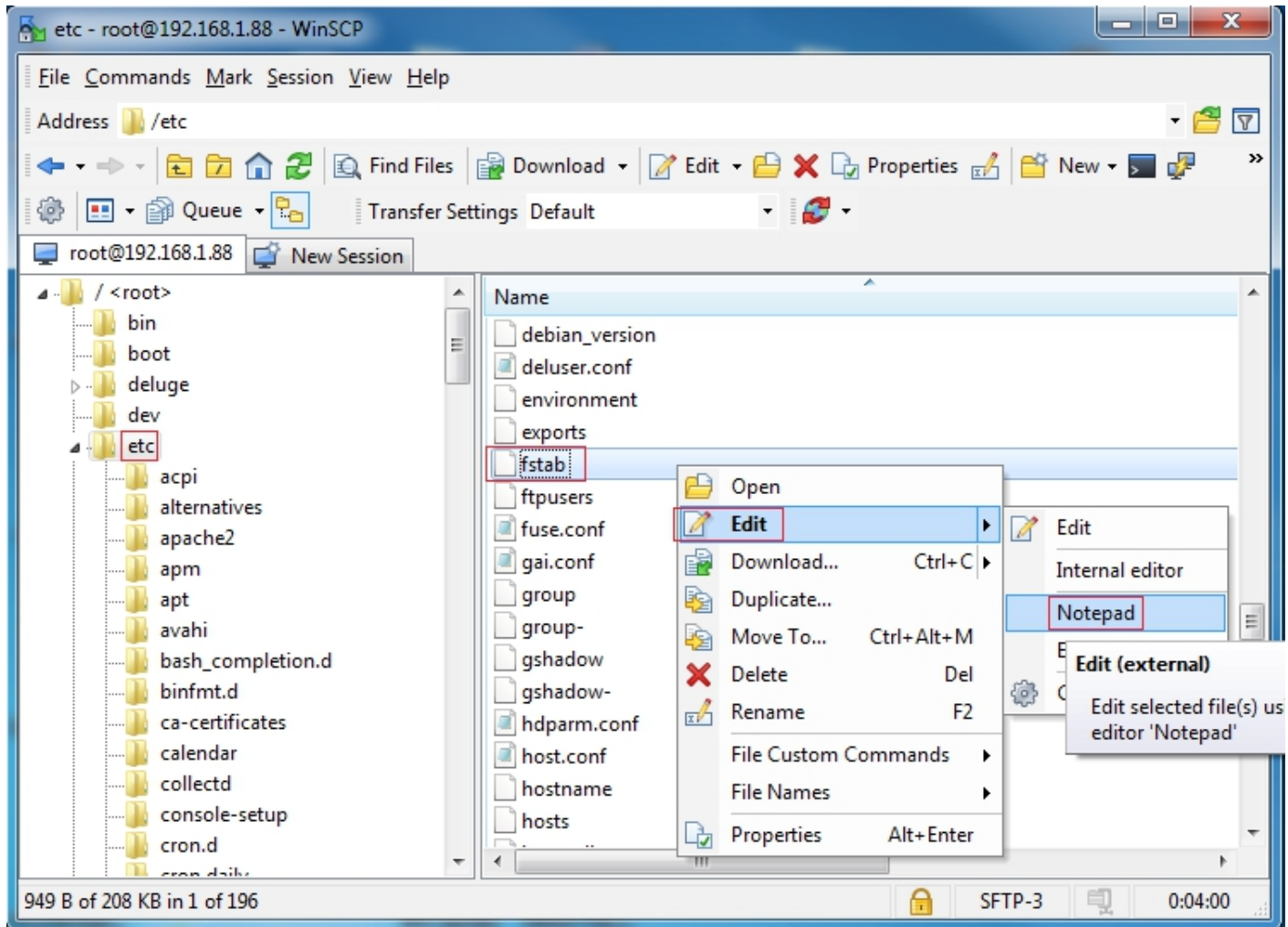
**Note:** In the latest version of the Flash Memory plugin, there are extended instructions that go beyond editing `/etc/fstab`. Those instructions apply to mdadm RAID and are NOT for beginners.

## Option 2: Editing `/etc/fstab` with WinSCP and Notepad

This option requires the installation of [WinSCP](#).

Users who are not comfortable with editing `fstab` using nano can use WinSCP and Windows Notepad to make the needed changes. If WinSCP is not installed, this doc-link to → [WinSCP](#) will describe the process for installing WinSCP and logging into the openmediavault server for the first time.

When logged in, click on `/etc` in the left pane. In the right pane, “right” mouse click on `fstab`, select **Edit** and **Notepad**.



Notepad will open the `fstab` file.

First: Find the root partition - it's the line with `/` and insert **noatime,nodiratime**, after **ext4** and **one space** as shown.

Second: Find the swap partition – it's the line with **swap** and insert a **#** at the beginning of the line as shown below.

```

# /etc/fstab: static file system information.
#
# use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point> <type> <options> <dump> <pass>
# / was on /dev/sdb1 during installation
UUID=5111ffd4-47bd-4586-9077-edd65d21dae7 ext4 noatime,nodiratime,errors=remount-ro 0 1
# swap was on /dev/sdb5 during installation
#UUID=c91cfa5d-f4ca-45e8-92f5-6357840f9c54 none swap sw 0 0
/dev/sr0 /media/cdrom0 udf,iso9660 user,noauto 0 0
tmpfs /tmp tmpfs defaults 0 0
# >>> [openmediavault]
/dev/disk/by-label/data /srv/dev-disk-by-label-data ext4
defaults,nofail,user_xattr,noexec,usrjquota=aquota.user,grpjquota=aquota.group,jqfmt=vfsv0,ac1 0 2
# <<< [openmediavault]

```

Do **File, Save**. Close Notepad.  
Exit WinSCP.  
Reboot the server, from the GUI.

## Done

---

**Note:** In the latest version of the Flash Memory plugin, there are extended instructions that go beyond editing `etc/fstab`. Those instructions apply to mdadm RAID and are NOT for beginners.

---

## 5.12 Hard Drive Health and SMART

Hard drives are the hardware component most likely to fail, in a server, over time. With continuous use, spinning hard drives last roughly 4 to 7 years, but there are notable exceptions where hard drive life may be significantly shorter or longer.

Given that storage failure is inevitable, the best overall strategy to avoid losing data is 100% backup of the entire data store. Further, it is equally important to monitor the condition of a server's storage media to prevent silent data corruption and, unknowingly, replicating corrupted data to a backup device.

Another characteristic of hard drives is that they rarely fail all at once. While it is possible for a drive to fail abruptly, and without notice, it is a fairly rare occurrence. Typically hard drives begin to fail slowly, gradually accelerating

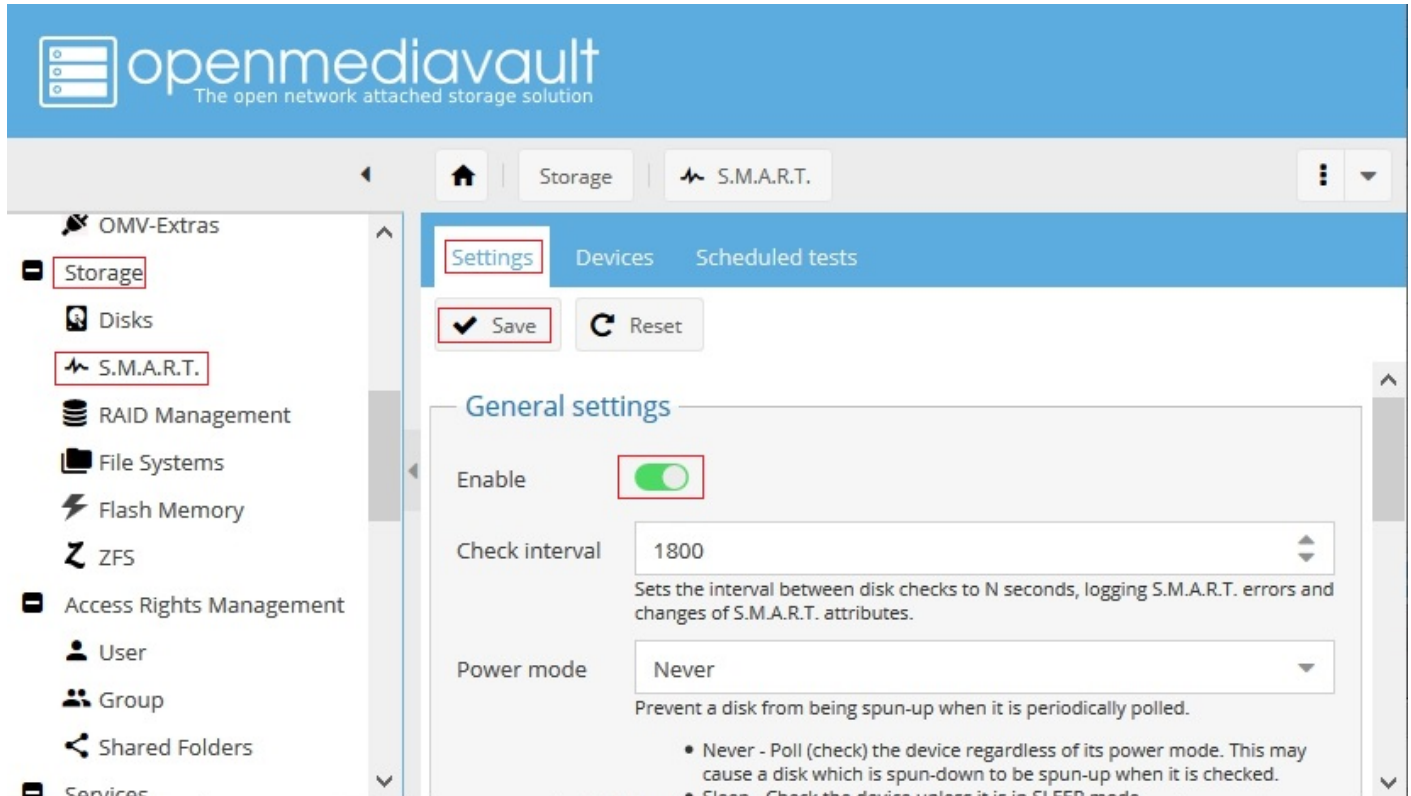
toward a point in time where they become unreadable. This unfortunate circumstance, where data lost to a corrupted or completely unreadable hard drive, might be avoidable with automated testing and monitoring.

To protect the server's data, enabling SMART is strongly recommended.

---

### 5.12.1 Enable SMART

In **Storage, S.M.A.R.T.**, in the **Settings** tab, **enable** SMART.

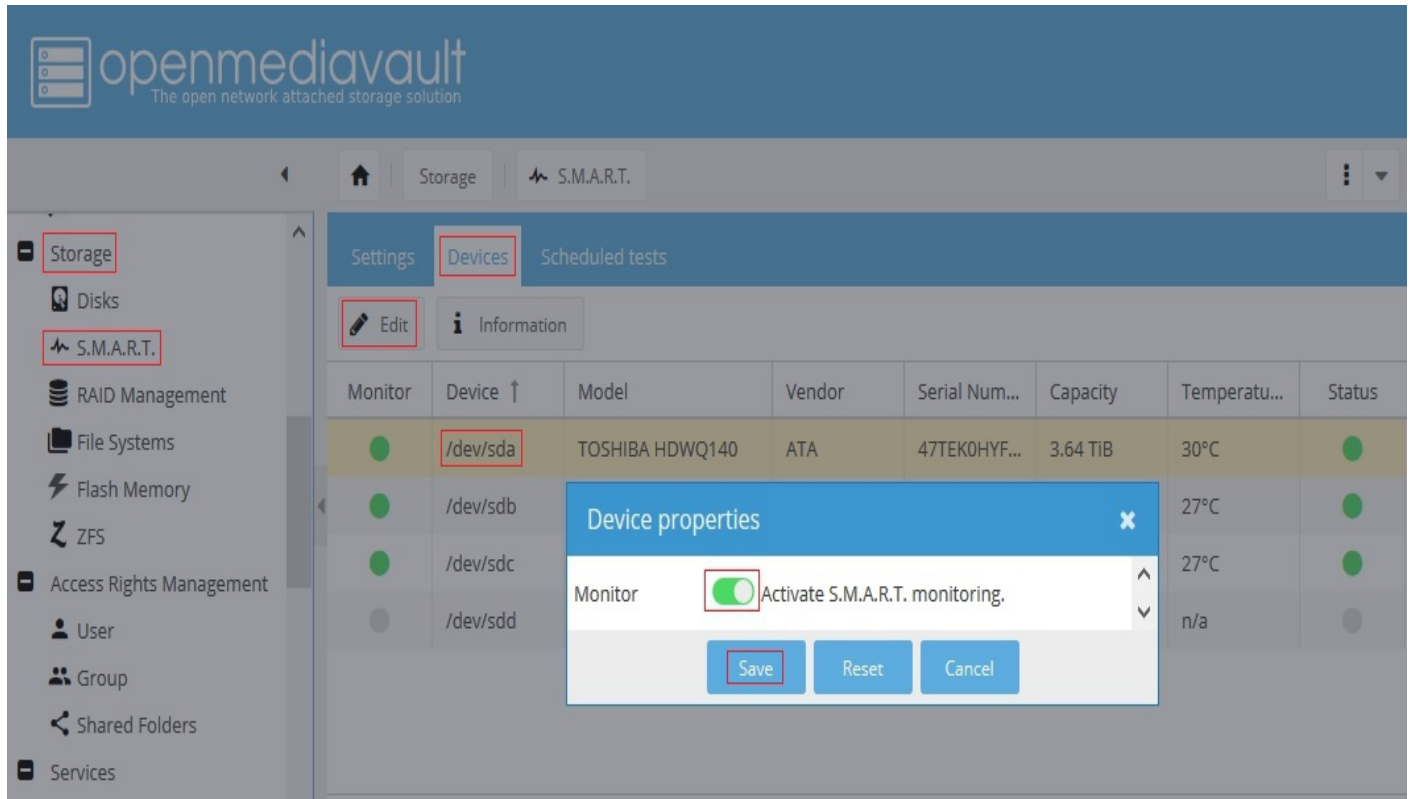


In **Storage, S.M.A.R.T.**, in the **Devices** tab:

Click on a drive, then the **Edit** button.

Activate monitoring and **Save**.

Do this for each drive. Note that some types of flash devices (thumbdrives and SD-cards) may not be monitored.



### 5.12.2 Drive Self-Tests

Drive self-tests are a tool for early discovery of hard drive issues. Periodic testing of hard drives will uncover the majority of hard drive issues as they begin to develop and, hopefully, before a drive fails completely. The following illustration shows the setup for automated short tests, for an individual hard drive. (Each hard drive will require its own scheduled tests.) In this example, a short self-test is run every Saturday at 1:00AM)

The screenshot shows the OpenMediaVault web interface. The left sidebar contains a navigation menu with 'Storage' and 'S.M.A.R.T.' highlighted. The main content area is titled 'S.M.A.R.T.' and has a sub-tab 'Scheduled tests'. Below the sub-tab are buttons for '+ Add', 'Edit', 'Run', and 'Delete'. A table lists three existing tests, each with a green 'Enabled' status and details for the device (e.g., /dev/sda, /dev/sdb, /dev/sdc). A modal window titled 'Add scheduled test' is open, showing a form with the following fields:

Field	Value
Enable	<input checked="" type="checkbox"/>
Device	TOSHIBA HDWQ140 [/dev/sda, 3.63 TIB]
Type	Short self-test
Hour	1
Day of month	*
Month	*
Day of week	Saturday
Comment	

At the bottom of the modal are 'Save', 'Reset', and 'Cancel' buttons. The main table below the modal has columns: Enabled, Device, Type, Hour, Day of month, Month, Day of week, and Comment. The existing tests in the table are:

Enabled	Device	Type	Hour	Day of month	Month	Day of week	Comment
<input checked="" type="checkbox"/>	Device: /dev/sda Model: TOSHIBA HDWQ140 S/N: 47TEK0HYFPBE Capacity: 3.64 TIB					Saturday	
<input checked="" type="checkbox"/>	Device: /dev/sdb Model: ST4000DM005-2DP1 S/N: ZDH18HML Capacity: 3.64 TIB					Saturday	
<input checked="" type="checkbox"/>	Device: /dev/sdc Model: ST4000DM004-2CV1 S/N: ZFN062B4 Capacity: 3.64 TIB					Saturday	

A **Short** self-test runs for a few minutes and is an “on-line” procedure, meaning that drives are still accessible during the test. A **Long** self-test is an “off-line” test, meaning drives are not accessible during the test. While a Short test does a quick check of a drive’s components, a Long test does everything in a Short test then checks the media (platters) for bad sectors and other imperfections. Repairs are made, if possible, such as reallocating bad sectors.

The down side of a Long test is that it is L-O-N-G, where drive size and spindle speed are factors in the length of the test. Long tests are off-line and, since entire platter surfaces are scanned, it may push a drive that’s beginning to fail closer to an actual failure as the test detects and attempts to repair problems.

There are many opinions on which tests to use and the frequency of testing.

- Some data center admins schedule short self-tests once a week and a long test once every 30 to 60 days. (Remember, when scheduling a Long self-test, schedule it for after-hours periods where the server is not in use.)
- Some home NAS admin’s schedule a short test, once a week, skipping Long tests altogether.

There’s no exact right or wrong but the self-test tool should be used as an aid to monitor drive health, in avoiding data corruption and loss.



### 5.12.3 SMART Attributes

There are numerous SMART attributes to consider. Unfortunately, only a handful are standardized among the various drive OEM's and many have little to no practical meaning to the end user. Given the variation between drive OEM's, the interpretation of a specific SMART stat may require going to the drive OEM's support site.

A good explanation of individual SMART attributes, and a brief explanation for each, can be found → [here](#) .

Where spinning drives are concerned, thanks to the ongoing [BackBlaze drive study](#) , a correlation has been made between impending drive failure and specific SMART stat's.

---

#### SMART stats loosely related to drive failure

**SMART 5 – Reallocated\_Sector\_Count**

**SMART 187 – Reported\_Uncorrectable\_Errors**

**SMART 188 – Command\_Timeout**

**SMART 197 – Current\_Pending\_Sector\_Count**

**SMART 198 – Offline\_Uncorrectable**

Any one count of the above stats may be meaningless, but it should be noted and closely monitored. If any of the above begin to increment upward, as of the 3rd or 4th count, home or small business admins might want to consider ordering a replacement drive.

**SMART 199 - UltraDMA CRC errors**

While not directly linked to drive failure, it's worth noting that counts on SMART stat 199 are usually hardware or cable related. This may be due to loose or a bad SATA / SAS cable, a connectivity problem, or an interface issue of some kind with the motherboard or the drive interface board.

### 5.12.4 Drive Failure - The Bottom Line

When using scheduled drive self-tests in conjunction with SMART E-mail notifications (see *Server Notifications* ), server admin's and home users will be afforded better protection against the data corruption and data loss due to a failing hard drive.

---

## 5.13 Final Installation Notes:

1. Permissions for the shared folder created in this guide, and the SMB network share layered on top of it, are completely open. While these permission settings are OK for home environments, the server should not be exposed to the Internet by port forwarding. (Ports 80 or 443, for example.) As users gain knowledge and experience, they should consider tightening up permissions on the underlying Shared Folders and SMB/CIFS network shares.

Help with permissions in openmediavault, along with some practical examples, can be found here → *Wiki* <[https://wiki.omv-extras.org/doku.php?id=nas\\_permissions\\_in\\_omv](https://wiki.omv-extras.org/doku.php?id=nas_permissions_in_omv)> .

2. **Important:** Put your new server on a good surge suppression power strip, at the absolute minimum. An **UPS** system is **preferred** and is best practice. In consumer electronics, the majority of failures are related to power supplies and adverse conditions created by line power. The prime causes of power issues and failures are short duration surges, high voltage spikes, brown-outs, and sustained over-volt or under-volt conditions. A good UPS system is designed to counteract these problems. Further, the file system on the boot drive is at risk of corruption from sudden (dirty) shutdowns due to power loss. An UPS minimizes these risks.

---

## 5.14 Utilities to Help With openmediavault Management

Being able to work from the command line would be very useful to users, who may need to gather detailed information on the OS and platform hardware, for troubleshooting and for an occasional edit to a configuration file. Much can be learned with the following utilities that allow users to look at openmediavault “under the hood”.

---

### 5.14.1 WinSCP

WinSCP allows users, beginners and experienced alike, to visualize the Linux file structure in a manner similar to Windows Explorer. WinSCP installs on a Window Client and connects to Linux servers, allowing users to work with their server remotely.

One of the more useful features of WinSCP is that it gives users the ability to edit Linux configuration files with a familiar editor like Notepad. For experienced Linux Desktop users who would like to use WinSCP, it will run from **WINE** (in Linux Mint, Ubuntu and others)

WinSCP can be downloaded here. → [WinSCP](#)

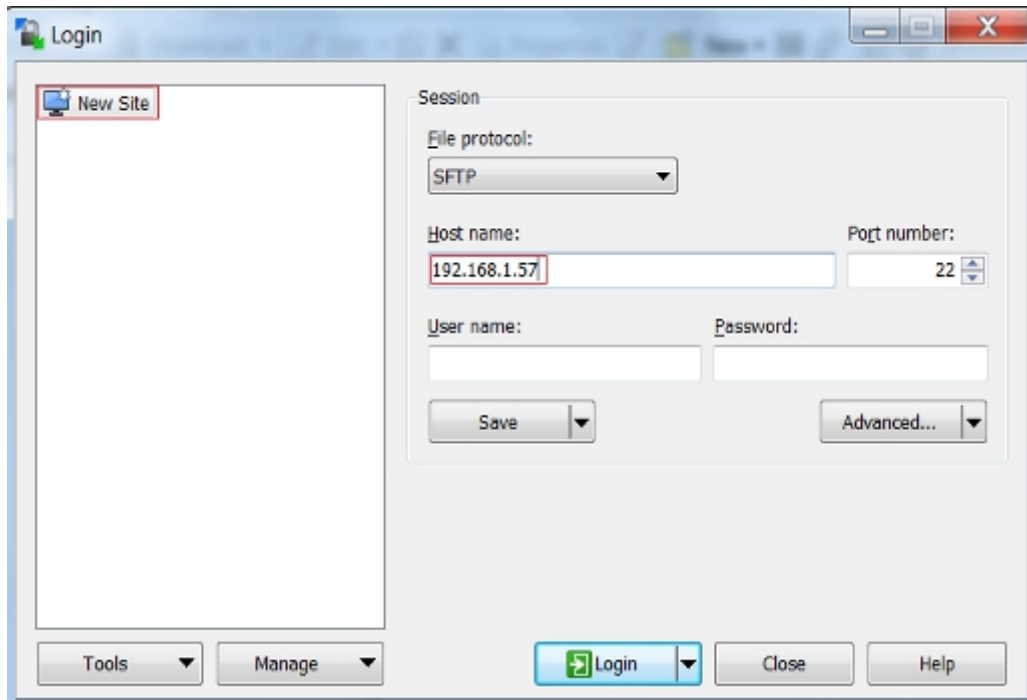
---

#### Installing WinSCP

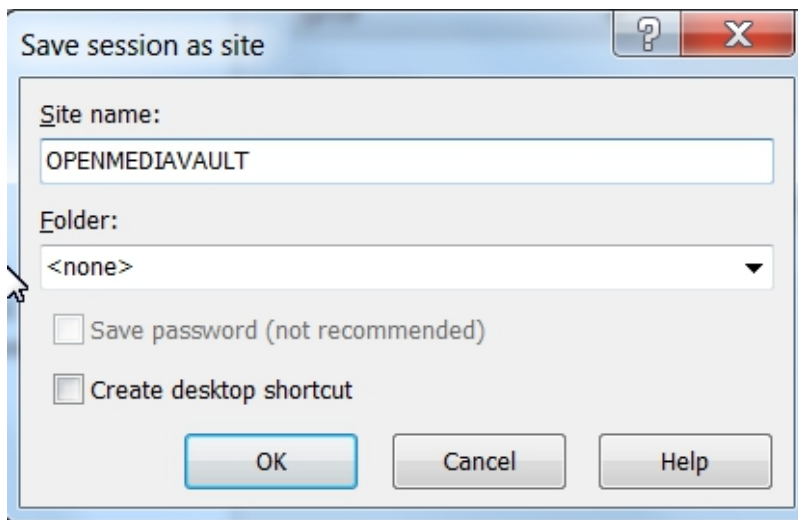
During the installation process, if prompted, select the **Explorer Interface**. This display shows the remote file system only. If the Explorer Interface is not offered it can be selected after the installation, under View, **Preferences, Environment, Interface**.

---

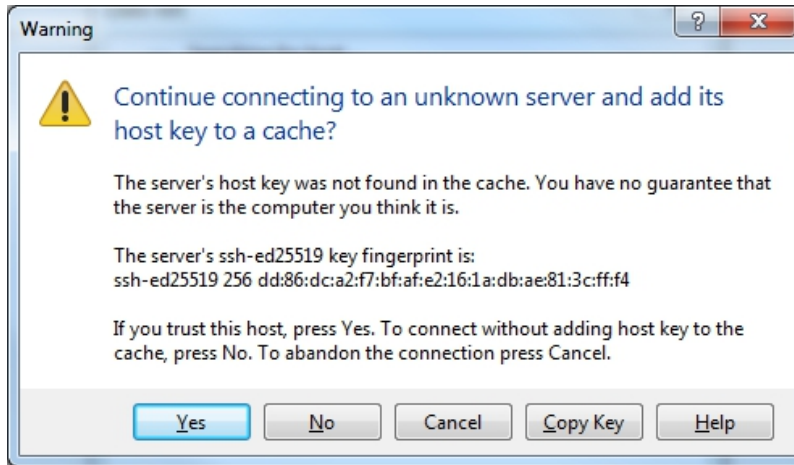
On the first run, the login screen is presented. Click on **New Site** and type in the **IP address** of the new server. Click on **Save**.



In Site name: The server's IP address is displayed. Optionally, the site name can be changed. If using WinSCP for a single server, a desktop short cut may be useful. Click on **OK**.



The **login** screen will come back. Double click on the new site name. The following is normal for the first SSH connection to any client or server. Click **Yes**.



The first prompt is for the username. Enter `root`

The second prompt is for the root password. Enter the root `password`.

---

**Note:** R-PI users would enter the user `pi` and the `pi password` or a previously added user with admin privileges. Due to the restrictions of a non-root “sudo” environment, WinSCP will be restricted from root functions. This restriction can be mitigated, but it’s beyond the scope of this guide.

---

The following link may of assistance: [Connect as root \(sudo\) using WINS SCP](#)

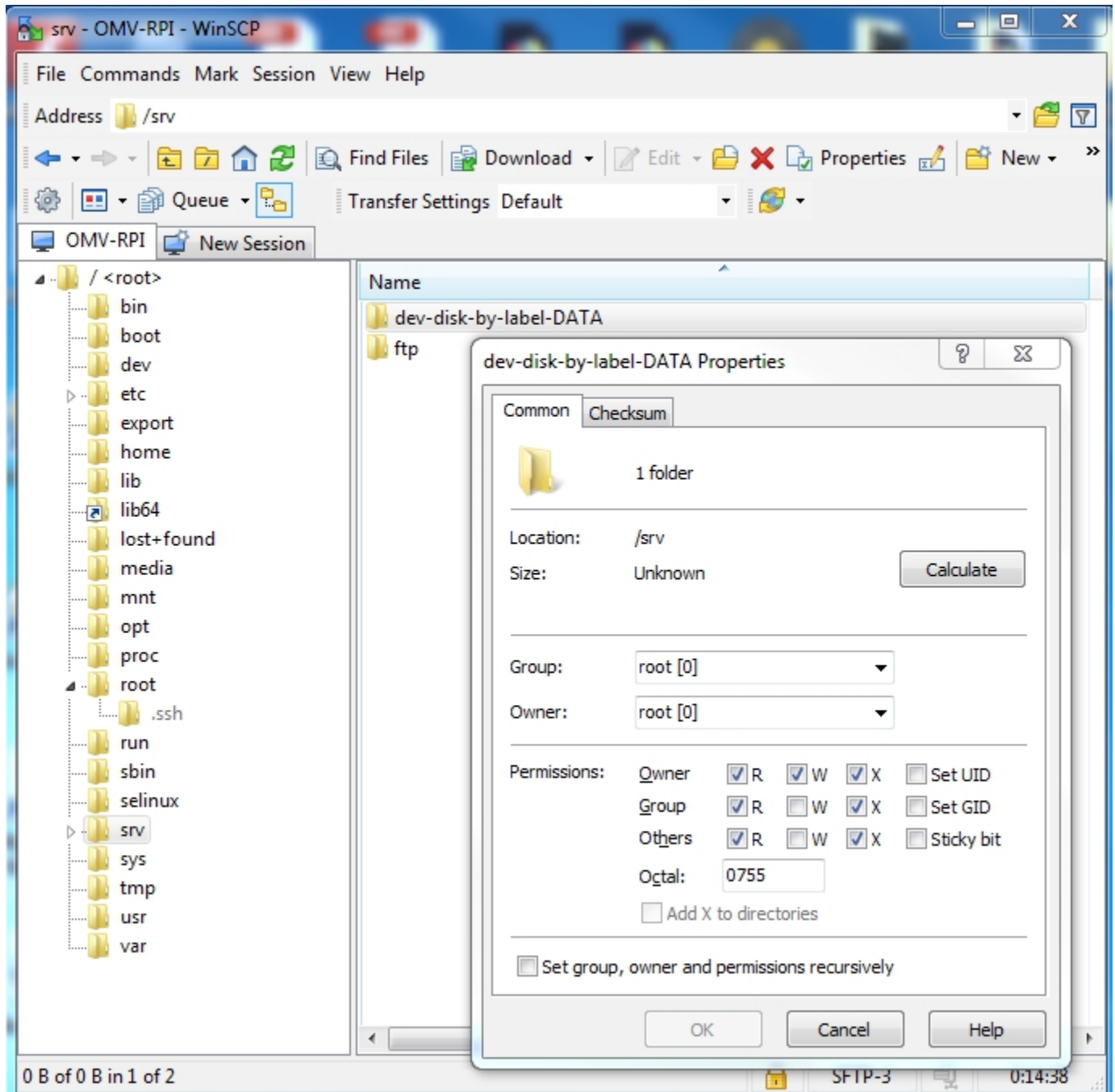
---

WinSCP opens with a two pane window. Selections are made in the left pane; operations are done on the right. The folder `srv` was selected on the left. **dev-disk-by-label-DATA** was highlighted on the right. A right click of the mouse brings up an operations menu. **Properties** was selected. In this particular popup, permissions could be changed. (Without backup, this is **NOT** a recommended action for beginners. **Backup** is covered later.)

---

**Note:** As of **OMV 5.5.20**, data drives are mounted using **UUID** (Universally Unique Identifier). In WinSCP, the same path might appear as: `/srv/dev-disk-by-uuid-f188c8ad-74d3-443a-a23e-89711270367d` (This is an example only – all disks will have a unique identifier.)

---



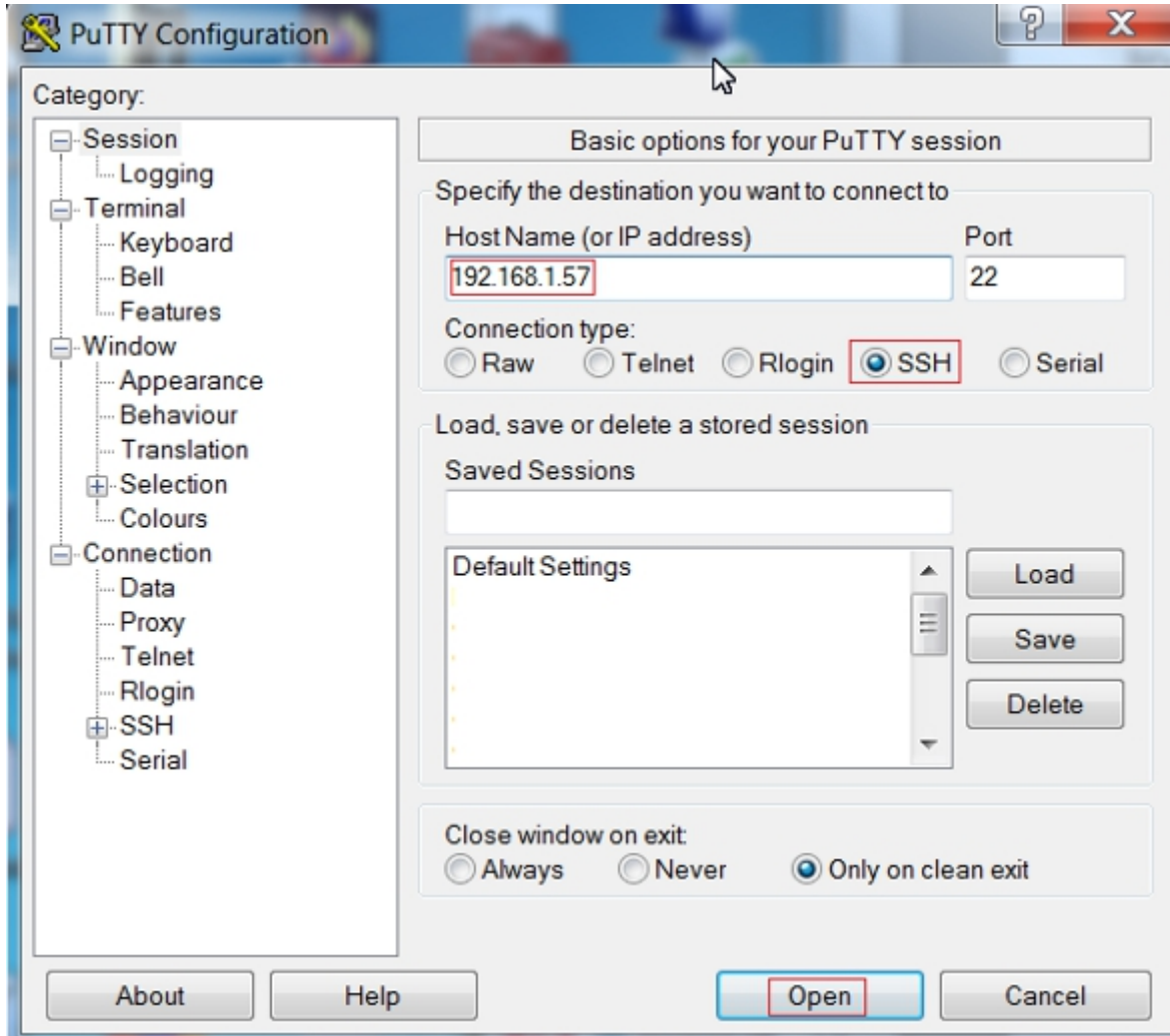
In a similar manner, a configuration file can be highlighted in the right pane. A right click of the mouse brings up the menu, select **EDIT** and Windows notepad, or the internal editor can be used for editing configuration files. Beginners will find either choice to be easier than using **nano** or **vi** on the Linux command line.

While they can be done in WinSCP, very large file copies, moves, or deletes are best done using [Midnight Commander](#).

### 5.14.2 PuTTY

PuTTY is similar to a Window's command prompt, but it allows users to work on openmediavault's command line from a remote PC. If PuTTY was not installed as part of your installation process, install it on a Windows PC. It's available here. → [PuTTY](#)

Using PuTTY is as simple as typing in the server's IP address in the **Host Name** field and clicking on open. There will be a warning for a first time connection – click **OK**. Then, login on the command line.



### 5.14.3 MC (Midnight Commander)

Midnight Commander is a command line file utility that utilizes a very cleverly created graphical interface. It's very useful for navigating through openmediavault's directory structure. It excels in efficient copying, moving, and deleting folders and files.

The installation process:

- Use **PuTTY** to get to openmediavault's command line.
- Log in as `root`.

- On the command line type the following; `apt-get install mc`
- When prompted continue with “Y”

(R-PI users will log in as `pi` and use `sudo apt-get install mc`)

When the installation finishes, on the command line, type `mc`

Midnight Commander is a two pane window where the source is the left pane and the destination is the right pane. Copies and moves are done, left to right. Since it's possible to navigate to any location on the openmediavault host, in either pane, the source and destination can be set for any location.

A mouse works in MC. Click on the various menu items at the top and bottom, to select them. Similarly, files or folders can be selected by clicking on them. To level up, click on the `./.` at the top left of either window.

```

mc [root@openmediavault]:~
Left      File      Command  Options  Right
<- ~     <- ~     <- ~     <- ~     <- ~
~         ~         ~         ~         ~
.n      Name      Size      Modify time  .n      Name      Size      Modify time
./..    UP--DIR   Dec 16 11:37  ./..    UP--DIR   Dec 16 11:37
./cache 4096      Dec 18 21:26  ./cache 4096      Dec 18 21:26
./config 4096      Dec 18 21:26  ./config 4096      Dec 18 21:26
./local 4096      Dec 18 21:26  ./local 4096      Dec 18 21:26
./ssh   4096      Dec 13 18:49  ./ssh   4096      Dec 13 18:49
.bash_history 14      Dec 16 11:26  .bash_history 14      Dec 16 11:26
.bashrc   446      Aug 16 03:11  .bashrc   446      Aug 16 03:11
.inputrc 278      Aug 16 03:11  .inputrc 278      Aug 16 03:11
.profile 161      Dec 16 11:40  .profile 161      Dec 16 11:40
.profile.bak 148     Aug 17 2015  .profile.bak 148     Aug 17 2015
.wget-hsts 180     Dec 13 19:14  .wget-hsts 180     Dec 13 19:14

UP--DIR                                     UP--DIR
44G/47G (95%)                               44G/47G (95%)

Hint: Want your plain shell? Press C-o, and get back to MC with C-o again.
root@openmediavault:~#
1Help 2Menu 3View 4Edit 5Copy 6RenMov 7Mkdir 8Delete 9PullDn 10Quit

```

**Warning:** Beginners - Midnight Commander is powerful and potentially dangerous. MC does not have “Undo”. A careless operation on the boot drive, such as accidental file “Move” or “Delete”, can ruin your installation.

Work with MC carefully and before doing anything extensive with it, the appropriate backups are recommended. *Operating System Backup – Data Backup* .

#### 5.14.4 Win32DiskImager

Win32DiskImager is a utility that's designed to write raw image files to SD-cards and USB drives. What makes it stand out from similar utilities is that it can “read” a flash drive and create an image file from the contents of the

device. If users decide to use an SD-card or a USB thumb-drive as a boot drive; the ability to read flash media devices makes [Win32DiskImager](#) useful for cloning flash boot drives.

**There is a known bug in Win32DiskImager V1.0.0** While the exact cause of the bug has not been determined, the number of affected users is very small. However, this bug requires the use of the Verify Only button after every operation. If the Verification hash is successful, the operation is good. If Verification fails, the read or write has failed and the image file or flashed drive cannot be used.

Details for using Win32DiskImager are found in *Operating System Backup* , under *Cloning Flash Media* .

---

### 5.14.5 Etcher

[Etcher](#) is a utility similar to Win32DiskImager that installs on a Windows client. It's designed to write an image files to flash media. In addition to the write operation, Etcher verifies the the image has been written correctly as part of the write operation. With two available USB ports, the latest version of Etcher will clone flash media in an all-in-one operation.

---

### 5.14.6 Virtual Box

Virtual Box is a cross platform virtualization platform that will work with both servers and clients. For learning about openmediavault, there simply is no better tool than working with an openmediavault Virtual Machine (VM). An openmediavault VM can be built, configured, and put on the local network complete with shares, in the same manner as real hardware. VM's can be created, cloned, used for test beds, and destroyed without consequence. Many advanced openmediavault users fully test upgrades, Docker's, plugin's, server add-ons and changes in configuration, in openmediavault VM's before upgrading or reconfiguring their real-world servers.

If users have a Windows client with at least 6GB RAM and plenty of hard disk space, installing Virtual Box on the client to host test VM's of openmediavault is highly recommended. → [Virtual Box](#)

---

## 5.15 Backups and Backup-strategy

It's important to understand the concept of backup and why backup is important. In understanding the concept of backup, an automotive analogy may be helpful.

If one has a car and that car has a spare tire, is the "car" backed up? The answer is "No". There are a great number of things that can happen to a car that can disable it, until parts are replaced or the car is otherwise repaired. These items would include the battery, alternator, any component of the ignition system, the transmission, the cooling system, etc., etc. To backup the car, **a second car is needed**. This is why using RAID of any type is not backup. At best, RAID could be thought of as a "spare tire" for a PC.

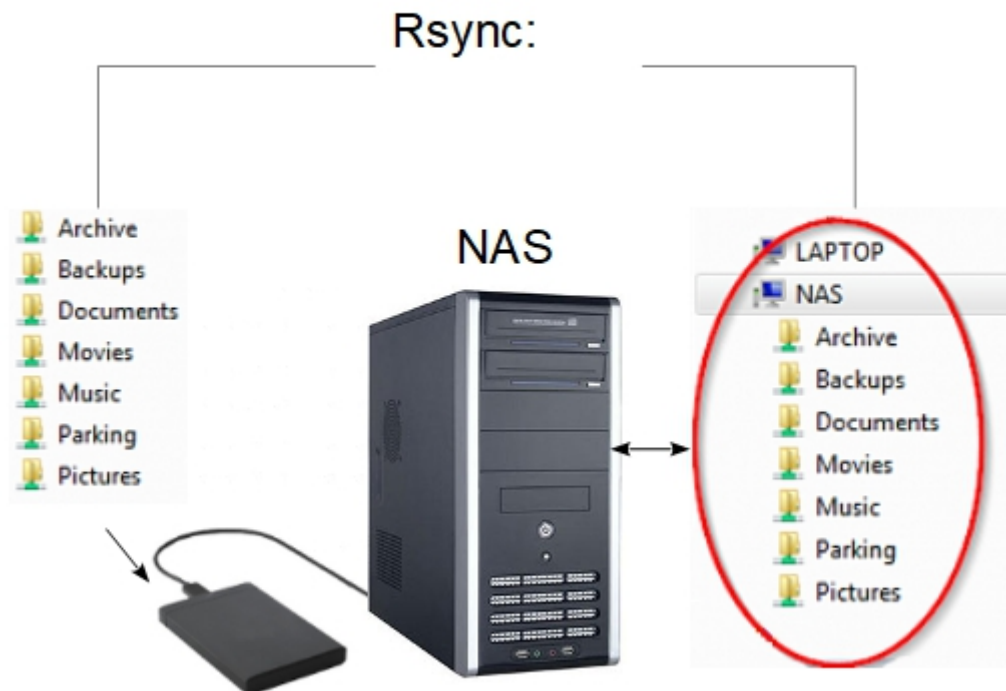
Where the automotive analogy fails, generally speaking, is that when a car fails it can be repaired. In computing, if a user's personal data is lost without backup, it's permanently lost. There are many possible events where data may be corrupted beyond recovery (viruses, ransomware) or is completely lost due to drive failures, a failing drive controller,



or other hardware failures. This is why real data back up is far more important than the computing equivalent of a spare tire (RAID).

### 5.15.1 Backing Up Data

#### First Level Backup: Replication To an External Drive



The scenario depicted in this graphic represents true backup. There are two full copies of data. With two separate copies, this backup strategy is superior to traditional RAID1 for home or small business use cases for a couple reasons.

- Rsync can be used with most USB connected hard drives where RAID1, when used with USB connected drives, is notably unreliable.
- If there's a drive error, an accidental deletion, a virus, or other data related issue; in RAID1 the effects are instantly replicated to the second drive. With Rsync, both drives are independent and, in most cases, the second disk will be available after the source disk fails. In any case, the Rsync replication interval allows time for admin intervention before the second disk is affected.

## 5.16 Full Disk Mirroring / Backup with Rsync

While individual shared folders can be replicated using Services, Rsync, a more efficient approach is using an Rsync Command line, in a scheduled job, under System, Scheduled Jobs to mirror a drive. This method allows for replicating the file and folder contents of an entire data drive, to an external drive or a second internal drive of adequate size.

- To implement something similar to the following example; it's necessary to add and mount a destination drive, in accordance with the section labeled A Basic Data Drive.
- When formatted, the hard drives used in this example were labeled to indicate their function. This is a good practice that will help new users to easily identify drives and avoid admin mistakes.
- Dissimilar sized drives can be used, provide that the destination drive is large enough to hold the source drive's data.

---

The following Rsync command line is an example of how a data drive can be mirrored onto a second drive.

```
rsync -av --delete /srv/dev-disk-by-label-DATA/ /srv/dev-disk-by-label-RSYNC/
```

The source drive is on the left (ending with **DATA**) and the destination is on the right (ending with **RSYNC**). In this example, the entire contents of dev-disk-by-label-**DATA** would be copied to dev-disk-by-label-**RSYNC**

The switches are:

-a **Archive Mode**. Archive mode adds an array of options to an Rsync command. It's the equivalent of switches -r -l -p -t -g -o and -D which copies files and folders recursively, copies links and devices, preserves permissions, groups, owners and file time stamps.

-v **Increase Verbosity**. This can be useful when examining Rsync command output or log files.

--delete **Deletes files in the destination drive that are not in the source**. If accidental deletion protection is desired, this switch could be left out of the command line. However, from time to time, it would necessary to be temporarily re-added the --delete switch to purge previously deleted and unwanted files from the destination drive.

---

To find the appropriate Rsync command line entries for the user's server, under **Storage, File Systems** click on **down arrow** at the top right edge of a column. On the pop down menu, select **Columns** and check the **Mount Point** box.

Under the **Mount Point** column (red boxes) are the full paths needed for the source drive (in this example **/srv/dev-disk-by-label-DATA**) and the destination drive (in this example **/srv/dev-disk-by-label-RSYNC**).

Device(s)	Label	Filesystem Type	Used	Mounted	Mount Point	Referenced	Status
/dev/mmcb	Sort Ascending		21.62 MiB	Yes	/boot	No	Online
/dev/mmcb	Sort Descending		1.26 GiB	Yes	/	Yes	Online
/dev/sda1	Columns		515.00 MiB	Yes	/srv/dev-disk-by-label-DATA	Yes	Online
/dev/sda2	RSYNC	ext4	514.99 MiB	Yes	/srv/dev-disk-by-label-RSYNC	No	Online

**Note:** As of OMV 5.5.20, data drives are mounted using **UUID** (Universally Unique Identifier). The path under the **Mount Point** will be similar to: `/srv/dev-disk-by-uuid-f188c8ad-74d3-443a-a23e-89711270367d` (This is an example only – all disks will have a unique identifier.) To avoid source and destination drive confusion when using UUID's: The **Mount Point** Column, above, can be moved by “left clicking” the column head, holding and dragging it to the **Devices** and **Label** columns.

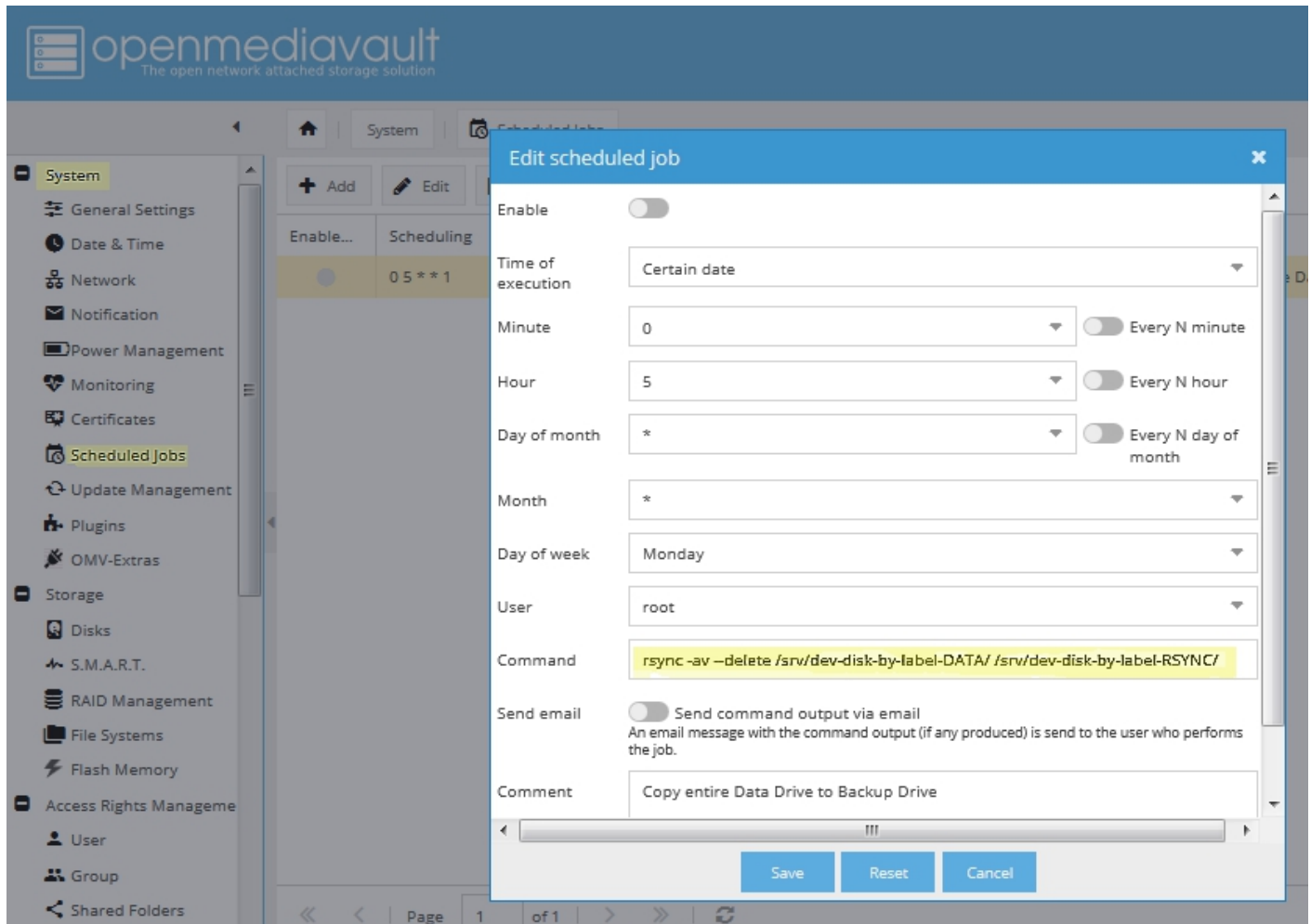
To construct the appropriate command line, add a slash “/” after each drive path, in the full command line as follows:

```
rsync -av --delete /srv/dev-disk-by-label-DATA//srv/dev-disk-by-label-RSYNC/
```

#### Warning: Beginners Warning, Note and Sanity Check

- Getting the source (left) and destination (right) in the correct order, in the command line, is **CRUCIAL**. If they're accidentally *reversed*, the **empty** source drive will delete all data on the **destination** drive.
- The safest option would be to leave the switch `--delete` out of the command line until it is confirmed that two full copies exist.

As previously mentioned, this Rsync operation can be manually run or automated under: **System, Scheduled Jobs**, as shown in the illustration. Copy and paste the Rsync command line into the command box and select scheduling parameters as desired.



User Options for Backup:

- **Automated:**

As configured above, and if **ENABLED** (green), this Scheduled Job will run the Rsync command line once a week, on Monday, at 05:00AM. After the first run of the command, which may take an extended period to complete, a week or more would be a good backup interval. Generally speaking, the backup interval should be long enough to allow for the discovery of a data disaster (drive failure, a virus, accidentally deleted files, etc.), with some time to intervene before the next automated backup replicates the problem to the 2nd drive. This is also a drawback of using automation; if data loss or corruption is not noticed by the user, those problems will be replicated to the back up drive during the next Rsync event. Longer automated backup intervals, such as two weeks or even a month, allow more time to discover issues and disable replication.

- **Manual Run:**

If the job is **disabled** (the **ENABLED** toggle switch is gray), the job won't run automatically. However, the job can be run manually, at any time, by clicking on the job and the **Run** button. This may be the best option for users who do not check their server regularly.

- **Delete Protection:**

Removing the `--delete` switch from the command adds delete protection, and may allow the retrieval of files accidentally deleted from the source drive. As previously noted, to clean up the destination drive of intentionally deleted and unwanted files, the `--delete` switch could be manually entered into the command line, from time to time, as may be deemed necessary.

**Keep in mind:** In the event of a failing or failed data drive it is **crucial** that the drive-to-drive Rsync job is turned **OFF**, if automated. Similarly, after noting a problem, **DO NOT** run the job manually.\*\*

The Bottom Line:

The additional cost for full data backup using Rsync is the cost of an external drive, or an additional internal drive, of adequate size. For the insurance provided, the additional cost is very reasonable.

**Note:** If errors occur when running the command line, see the following:

→ *Rsync Drive Copy Errors*

## 5.16.1 Recovery from a Data Drive failure - Using an Rsync'ed backup

### General:

*Again, as a reminder, when the NAS primary drive is failing or has failed, it's crucial to turn **\*\*OFF\*\*** an automated drive-to-drive Rsync command line.\**

There are two basic options for restoring data with an Rsync'ed backup drive - they are “with” or “without” a replacement for the source data drive.

### Restoration Without a Replacement Drive:

Without a replacement drive on site, which would be the most likely case for most home users and small businesses, the backup Rsync'ed “destination” disk can become the data source for network shares. This involves repointing existing shared folders, from the old drive location, to the backup drive. All simple services layered on top of the shared folder, to include SMB/CIF shares and other shared folder services, will follow the shared folder to the new location on the back up drive.

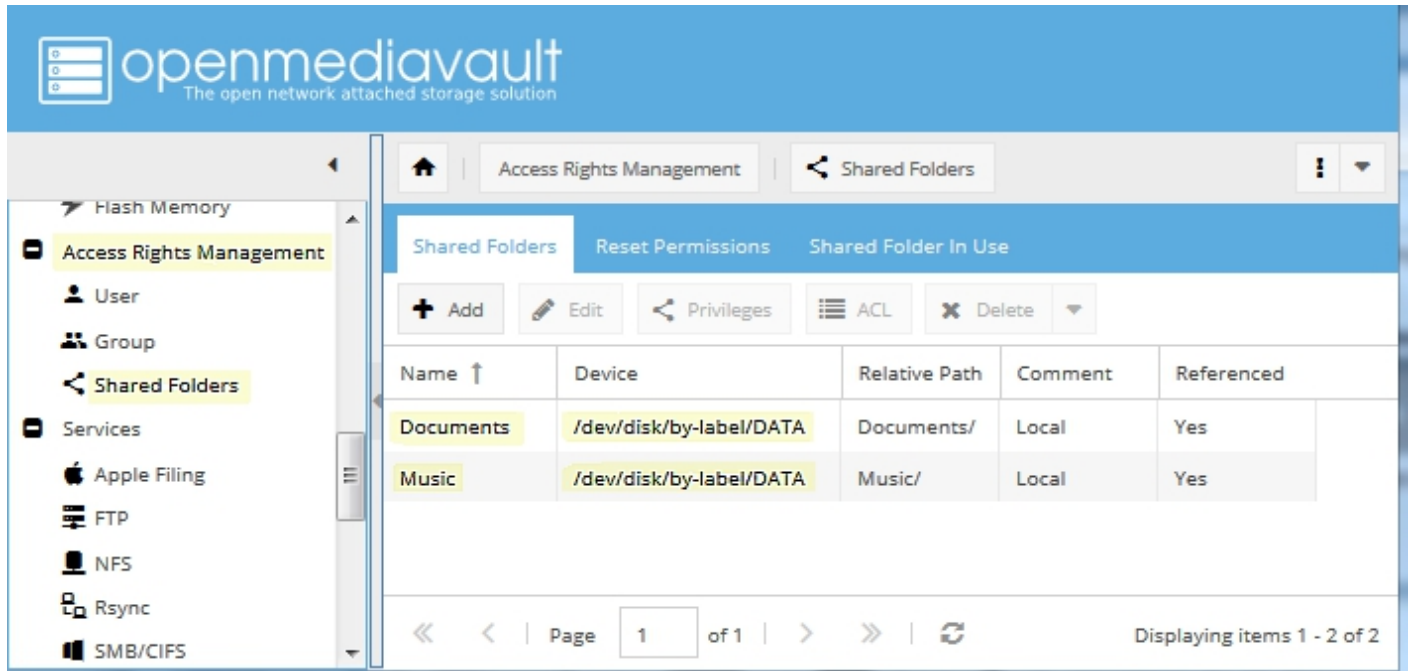
### Repointing a Shared Folder:

In the following example, the data drive has failed and it's been determined that it's not repairable. Under **Storage**, **File Systems** we have a **missing** source drive (labeled DATA) that's **referenced**.

Device(s)	Label	Filesy...	Total	Available	Used	Mounted	Mount Point	Referenced	Status
/dev/disk/by-label/DATA		ext4	n/a	n/a	n/a	No	/srv/dev-disk-by-label-DATA	Yes	Missing
/dev/mmcblk0p1	boot	vfat	62.01 MiB	40.39 M...	21.52 MiB	Yes	/boot	No	Online
/dev/mmcblk0p2		ext4	7.15 GiB	5.77 GiB	1.26 GiB	Yes	/	Yes	Online
/dev/sda2	RSYNC	ext4	83.66 GiB	78.84 GiB	514.99 MiB	Yes	/srv/dev-disk-by-label-RSYNC	No	Online

**Note:** There may be ERROR dialog boxes regarding the failed mount of existing shared folders. With a missing but referenced drive, this is to be expected. When all shares are redirected, these error messages will stop.

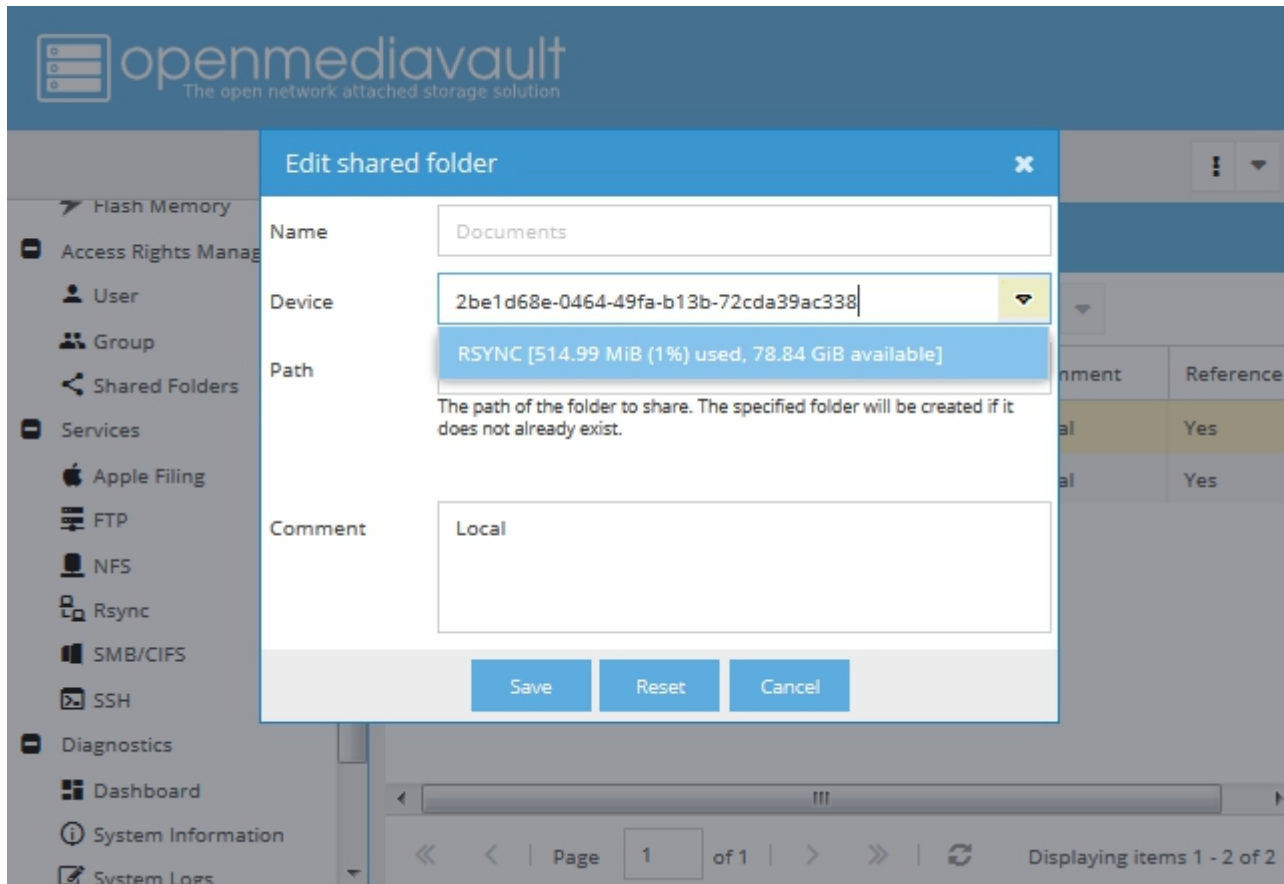
The actual references to the failed DATA drive are the **Shared Folders** assigned to the drive, named **Documents** and **Music** as follows:



Since the DATA drive no longer exists and there's an *exact duplicate* of all folders and files on the backup drive, we'll repoint the shared folder named **Documents** to the RSYNC backup. Click on the **Documents** Shared Folder, above, and the **Edit** button.

In the **Edit Shared Folder** Dialog Box, click the **drop down button** on the **Device** Line and select the destination / backup drive. (In this example the drive with **RSYNC** in the label is the backup.) A confirmation dialog box will prompt "**Do you really want to relocate the shared folder?**" Click "**Yes**" and "**Save**".

(Remember that *all* contents of the now missing source drive and the destination drive were *identical* as of the last backup, to include the path statement. Changes are not necessary. Repointing the share is just a matter of selecting **the backup drive**.)

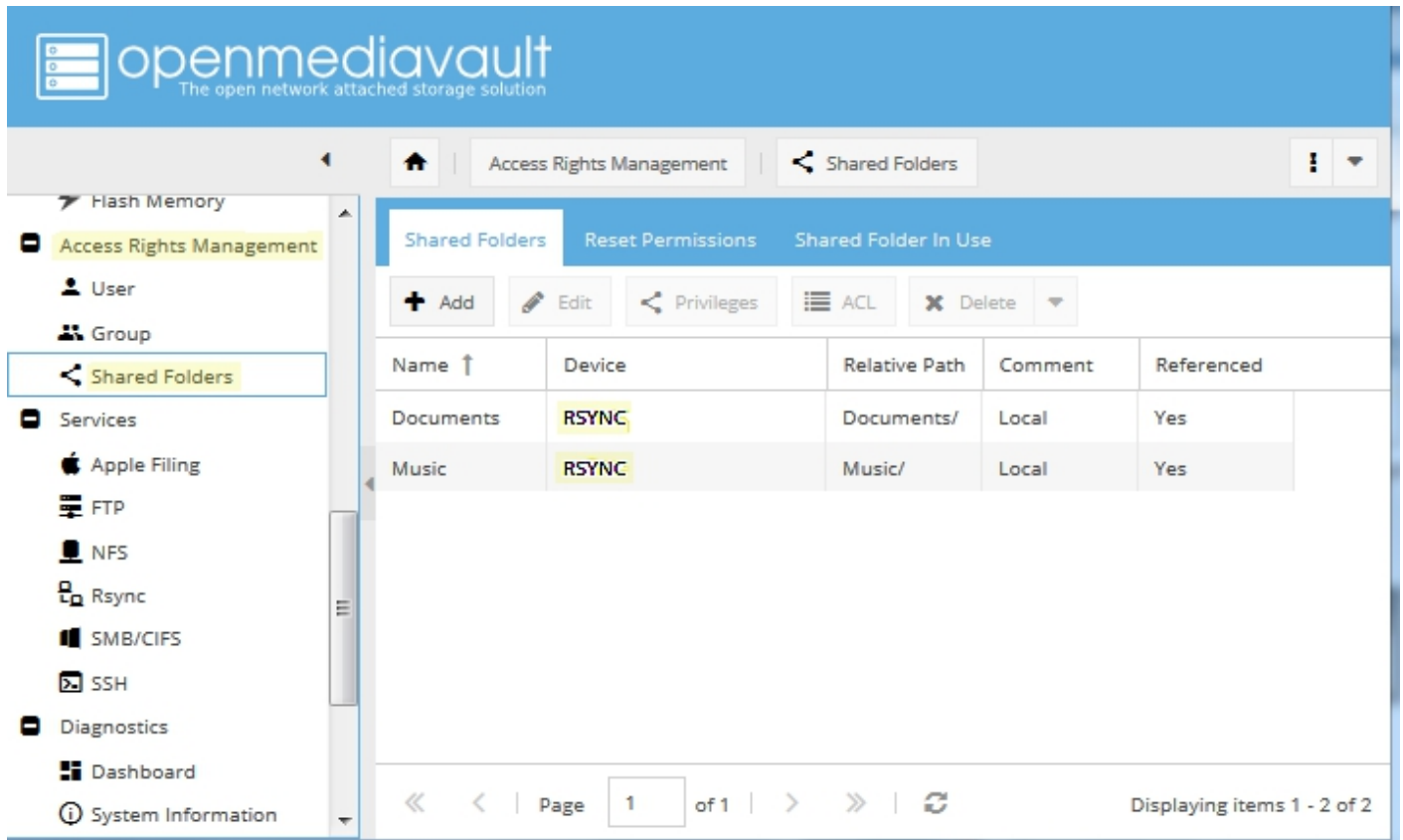


Click on **Save**, confirm the change, and it's done.

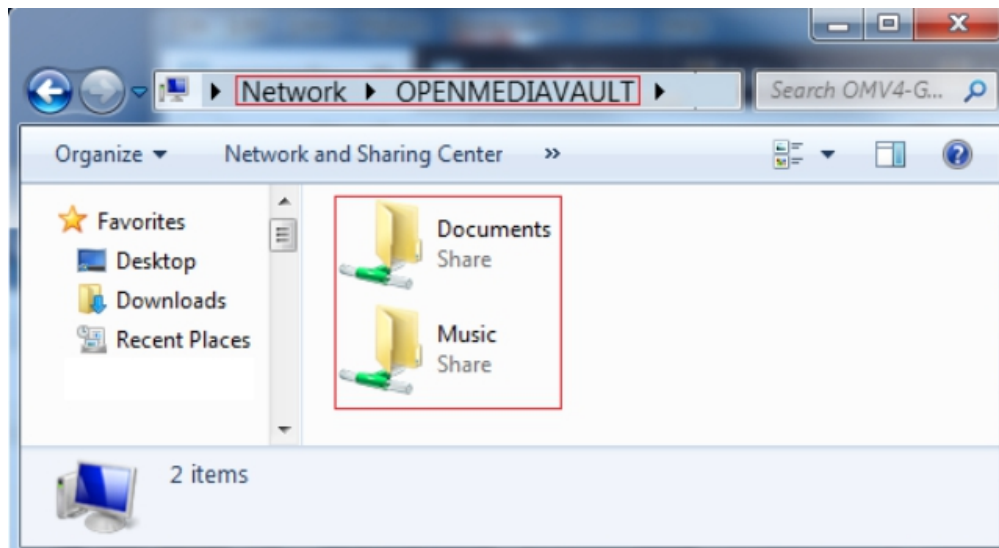
Do the same process for all remaining Shared Folders. (In this example, Music was repointed as well, but not shown.) Again, error dialog boxes may appear during the process. Acknowledge them (with **OK**) but do not revert, or back out of change confirmations. When all Shared Folders are redirected to the backup drive and saved, the error dialog boxes will end.

In the final result:

With one operation per shared folder, all shared folders have been redirected to the backup drive labeled RSYNC.



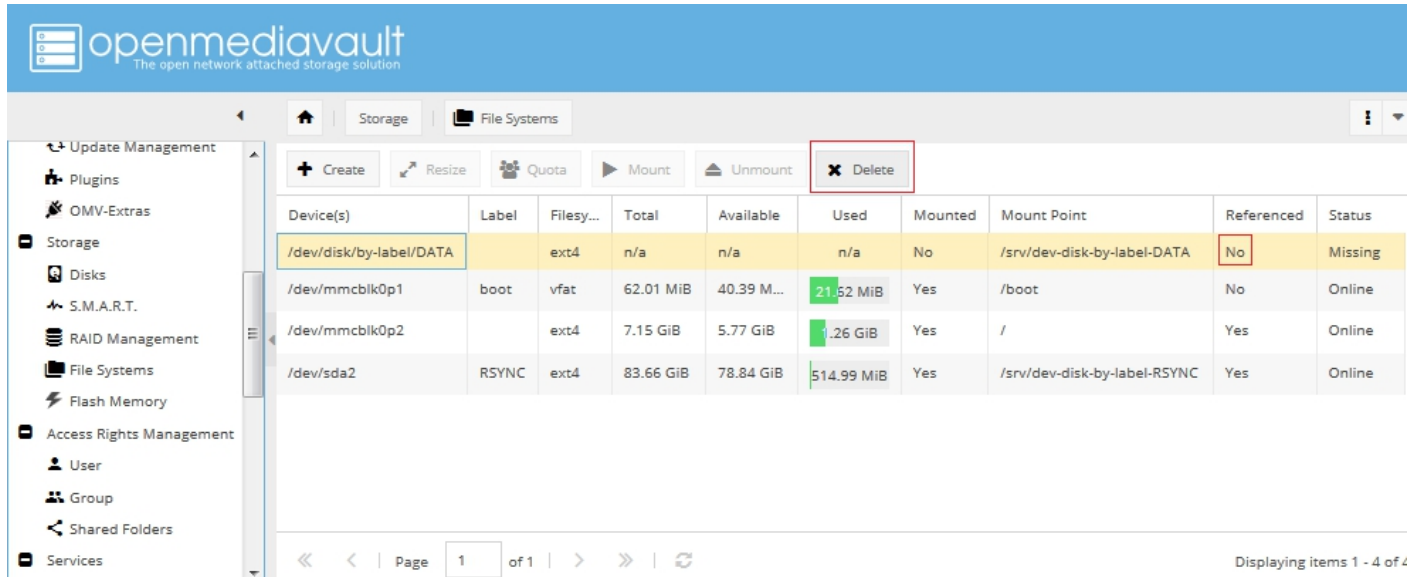
In this case there were SMB network shares layered on top of the Shared Folders above. The SMB network shares followed their associated Shared Folders, without additional configuration, so SMB shares are up and running on the Network.



In addition, most simple services that are applied to these shared folders, would follow the shared folder when it is repointed to the backup drive.



One last operation is needed to completely remove the failed DATA drive. Go to **Storage, File Systems** and note that missing drive DATA is no longer referenced. When clicking on the failed drive, the **Delete** button is now active. **Delete** the drive.



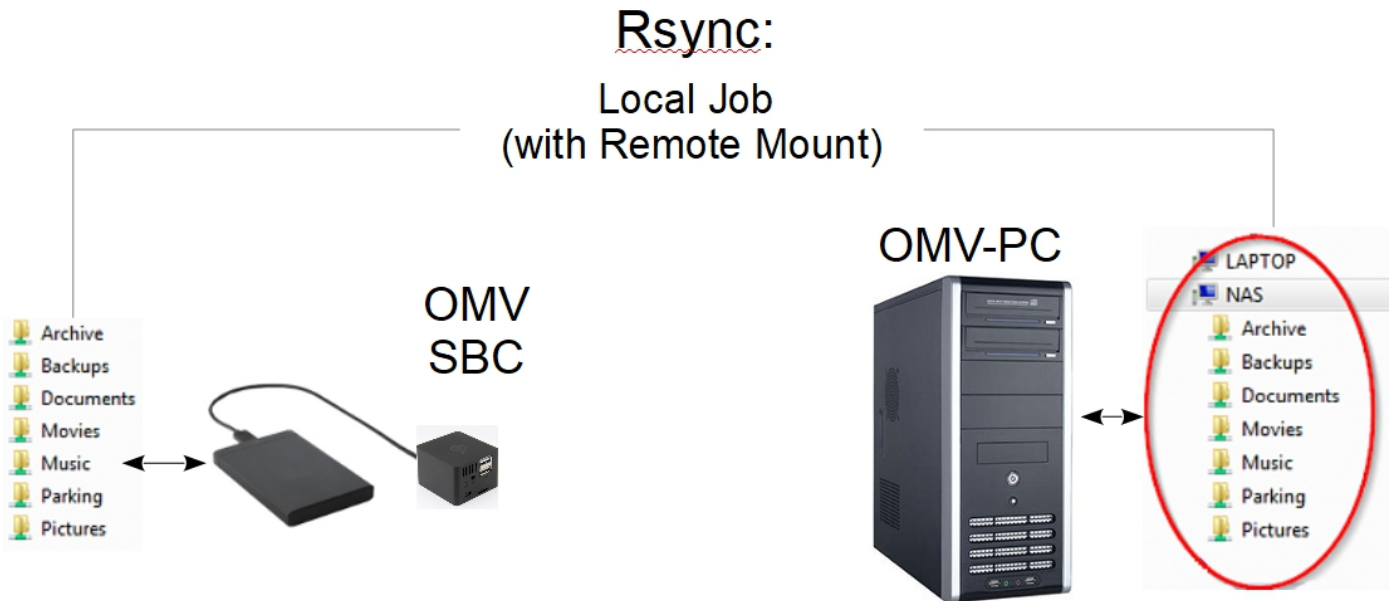
The screenshot shows the OpenMediaVault web interface. The left sidebar contains navigation options: Update Management, Plugins, OMV-Extras, Storage, Disks, S.M.A.R.T., RAID Management, File Systems, Flash Memory, Access Rights Management, User, Group, Shared Folders, and Services. The main content area is titled 'File Systems' and includes a toolbar with buttons for Create, Resize, Quota, Mount, Unmount, and Delete. The 'Delete' button is highlighted with a red box. Below the toolbar is a table listing file systems:

Device(s)	Label	Filesy...	Total	Available	Used	Mounted	Mount Point	Referenced	Status
/dev/disk-by-label/DATA		ext4	n/a	n/a	n/a	No	/srv/dev-disk-by-label-DATA	No	Missing
/dev/mmcblk0p1	boot	vfat	62.01 MiB	40.39 M...	21.52 MiB	Yes	/boot	No	Online
/dev/mmcblk0p2		ext4	7.15 GiB	5.77 GiB	1.26 GiB	Yes	/	Yes	Online
/dev/sda2	RSYNC	ext4	83.66 GiB	78.84 GiB	514.99 MiB	Yes	/srv/dev-disk-by-label-RSYNC	Yes	Online

At the bottom of the interface, there is a pagination control showing 'Page 1 of 1' and a refresh icon. The text 'Displaying items 1 - 4 of 4' is visible in the bottom right corner.

At this point, all shares in this example have been successfully redirected to the backup drive and the server is fully functional again.

## 5.17 Second Level Backup – Replication to a Second Host



The first item to note, is that this scenario can be accomplished using a LAN client, as the second host, and it could be a Windows client. The additional cost would be the price of a second drive of sufficient size (internal or external) to house the second copy of data, attached to a remote host. The Remote Mount Plugin can mount a Windows network share (a user name and password with write access is required) and Rsync can be configured to replicate NAS data to the Windows share.

As illustrated above, the second host could be a low cost SBC. This scenario can be designed with a number of desirable features.

- First, if backing-up to a second server platform, two fully independent copies of data are possible.
- When using an SBC with openmediavault installed:

If the primary server failed completely, the second platform can be configured to take over as a backup file server. With all data backed up and resident on the SBC, this data can be made available to the network with SMB shares.

- Other than re-homing clients to the shares on the backup device, there's no recovery time and no "crisis" involved in getting data back on-line. It's already there.

The costs for this level of backup are very reasonable, with the cost of a hard drive of adequate size and an SBC. Good performing SBC's are a low cost option. Older PC platforms or laptops could be configured as a backup server as well.

The Practical details for setting up Primary Server to Backup Server share replication, using Remote Mount and Local Rsync Jobs are covered here → [Wiki](#) or [PDF](#) .

While replication to an independent host is an excellent method of avoiding data loss catastrophes, there are other potential events which can threaten irreplaceable data. Fires, roof or plumbing leaks and other unforeseen events can result in the loss of data, even on two independent hosts. For these reasons, backup professionals and experienced server administrators recommend an off-site copy. While this may seem extreme, it's actually fairly easy to accomplish. It can be done with an SBC or an old laptop, connected wirelessly, and housed in a utility shed with AC power. Some users set up a backup host in a family members' house, and replicate changed data over the internet.

In the bottom line, if users want to keep their irreplaceable data, an absolute minimum of two full copies is recommended, with a 3rd off-site copy preferred. As previously noted, effective backup strategies do not have to be expensive and are relatively easy to set up.

For further information on Backup concepts and best practices, an excellent explanation of Backup is provided by [Backblaze.com](https://www.backblaze.com).

---

## 5.18 Operating System Backup

By design, the OMV/Debian operating system installs on its own partition, segregated from data. This makes copying or cloning the openmediavault boot/OS drive an easy process. So, one might ask, why is a clone or a copy of the operating system important?

Building openmediavault, from scratch, using the installer ISO is a 15-minute proposition, give or take. While it takes longer, roughly 30 to 45 minutes, the actual hands-on portion of an SBC build is even less.

As users configure their servers, add services, reconfigure shares, move their data around, tweak access controls, etc., servers tend to become “works in progress”. Configuring a server to the user’s preferences can be an evolution that may take weeks or even months. If a complete server rebuild is required, the customization, add-ons, and the collection of various user tweaks may take several hours to recreate. It is this time and effort that Operating System Backup will preserve.

There are several ways to duplicate an operating system boot drive, but many can be technically involved; requiring network access to remote servers, bootable utilities and somewhat complex processes.

Given the low cost of flash media and with sockets mounted on the outside of a PC case, SD-cards and USB thumb-drives lend themselves to cloning and very quick recovery.

---

### 5.18.1 The Benefits of Maintaining Operating System Backup

In accordance with “Murphy’s Law”, users may encounter issues where things go wrong. As examples, users may test software on their active server or try new settings. On occasion, installing an add-on may have unintended consequences. Trying new settings or working on the command line, may break openmediavault in a way that might not be recoverable. In other cases, there may be instances where a software update goes south – the source repository may go off-line in the middle of an update resulting in broken packages.

In all of these cases, having a confirmed working clone of the boot drive will allow users to “drop back” to a known good state. The “FIX” would be as simple as shutting down and booting the server on a known working clone.

The advantages of maintaining operating system backup are obvious. Beginners, with very little knowledge of Linux, can work with their servers without fear, which facilitates learning. If a Linux update causes ill effects, it’s possible to drop back and selectively install packages to isolate the exact cause of the problem. If an add-on update doesn’t work (direct installed software, a plugin, Docker, etc.), the user can gracefully back out of the update and leave the older (but working) software package in place.

It’s the easiest, quickest, and most effective fix, for resolving problems with openmediavault and the underlying Debian Operating System.

**The practical issues of maintaining boot drive clones – when to update and rotate?**

1. It makes sense to apply Linux Operating System updates and wait a week or so, to insure that all is working and that there are no ill effects. If all is well, update the backup and rotate.
  2. The above would also apply to add-on packages, Docker, or plugin upgrades. (Plex, Urbackup, Pi-Hole, etc.)
  3. If a network share is added, deleted, or any aspect of the NAS is reconfigured that changes the operation of the NAS; the backup would need to be updated. (Otherwise, the configuration of the previously cloned boot drive would not mesh with the configuration and contents of data storage drives.)
  4. If a cloning mistake is made (let's respect Murphy's Law), a 3rd clone could become a "fallback of last resort". Given that Linux package upgrades and openmediavault sub-version upgrades have little to no effect on network shares or the high level configuration of the NAS, a 3rd clone can be maintained that is updated only when the NAS configuration is changed.
- 

### A Last Important Note About Backing Up your OS

Just as it is in the commercial world, where support for a product may be discontinued, the open source community is constantly moving forward as well.

Users may believe that an ISO file, or image, contains all the software needed for a build. In some current build cases, that assumption would be incorrect. Linux distro's, during the initial build and to finalize the installation, may depend on on-line software repositories. After the installation is complete, patches and updates may be applied which rely on on-line repositories as well.

Can it be assumed that those same software repositories and resources will be available on some future date, exactly as they were at the time of a current build? The answer is "No". Distributions of a specific Linux version, complete with specific applications, fully patched and updated, can be built for a **limited time**.

Therefore, if users have extensively configured builds, are using specialty hardware (such as SBC's) or are using openmediavault to serve a critical function; it would be wise to backup the boot drive to an image file, or Clone the fully configured working installation to separate media, and save one or more copies for future use.

---

## 5.18.2 Cloning Flash Media

To avoid issues that can result from dissimilar sizes, it's best to clone images from/to identical SD-cards or USB thumb-drives. Otherwise, it's easier to clone if a new drive is slightly larger than the working drive.

(And while it's an intermediate level technique, [Gparted](#) can be used to slightly shrink flash drive partitions, to fit on the smaller of the two flash drives.)

### The Cloning Process for USB thumbdrives and SD-Cards

- Install [Win32Diskimager](#) on a Windows PC.
- Format the new SD-Card or USB thumb-drive with [SDFormatter](#)
- Test the new card or USB drive with [h2testw1.4](#) . One test is enough. (Do not select endless verify.)

If the device registers errors, or if the capacity is significantly different from what is that's marked on the label (a fake), return it for refund or throw it away.

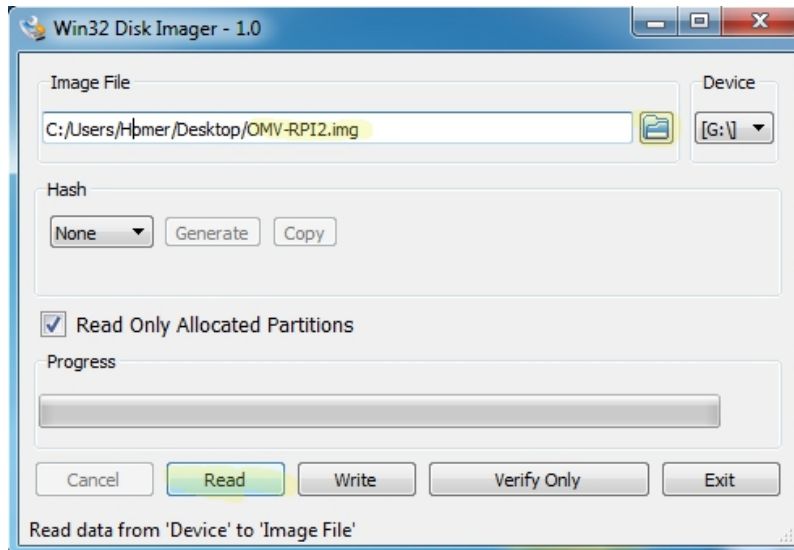
**At this point you should consider marking your working SD-card (with permanent marker?) to make sure you don't mix it up with the blank card. Otherwise, it is possible to read a "blank card" and use the blank image to "overwrite" the working card.**

- Insert the working card and start [Win32Diskimager](#)

**Warning:** SANITY Check, make sure you inserted your working SD-card / USB thumb-drive at this point.

**Note:** Windows will not be able to read the format of the partitions on the working boot drive and offer to format it for you. **DO NOT** format the drive. Close the dialog box with the **X**.

- In most instances, Win32Diskimager will detect USB thumb-drives and SD-cards, and set the Device drive letter. However, it would be prudent to check the letter Windows assigns to the drive with Windows Explorer.
- First click on the folder ICON and navigate to the location where you'll store your image file. Type a name in the file line. (OMV-RPI2.img was used for this example, but users can add a date to the name as well, such as OMV-RPI2-04-30-2018.img)
- Check the box for "**Read Only Allocated Partition**". (With larger drives, this option avoids imaging unused space which saves significant time when reading a drive to a new image and, later, when writing the image to another drive.)
- Click **Read**.



When the **read** is done, this is **crucial**, click the **Verify Only** button. This will compare the image file just created, to the boot drive. **DO NOT SKIP Verification**. (Win32Diskimager has a known bug which may affect a very small number of use cases.)

- If verification passes, pull the working boot drive and store it close by. If verification FAILS, the image file is corrupt and cannot be used.

**If the user/admin is running a business or is in another time sensitive scenario, where the NAS server can not be out of service for an extended period; the server can be booted on the source drive while the clone is being written. Thereafter, the drive swap could be accomplished during a low use period.**

While the resultant image file may be quite large, if the file is retained, it can be used to write another thumbdrive at a later date. In such a case, the image file itself can be saved as a dated backup and archived. The size of the image can be reduced significantly, by using 7zip to compress it before storage.

The last process uses [Etcher](#) to burn the image file and verify it in one pass. Etcher is a free utility that installs on Windows.

- Insert the **new** flash drive and start [Etcher](#) . (Etcher typically auto detects flash drives as well.)

- Select the image file previously created, verify the destination flash media drive, and click the FLASH! button.

One of Etcher's features is that it writes the image and verifies it in a single operation. If the operation is successful, the working boot drive has been cloned. Insert the new clone into the server and boot it up. With a successful boot up on the clone, user/admin's will have two verified working copies of their server's boot drive.

**Note** – Win32diskimager will write an SD-Card or USB drive, but verification is required and it's a second operation. Etcher combines the write and verification in a single process. If users walk away, during the write operation, which can take a long of time, Etcher is the best choice for writing flash media.

---

## 5.19 Add-on's – Adding Value to Your OMV server

### 5.19.1 General

The [openmediavault Forum](#) has an extensive [Guides](#) section. Whether a user's preference is videos or printed text, there's something for everyone among the numerous "How-To's". Beginners and Advanced users alike should take a few minutes to familiarize themselves with the content in the Guides section of the Forum.

### 5.19.2 Openmediavault's Plugins

Openmediavault has numerous plugin's. Some are integrated into the base package by openmediavault's developer Volker Theile. Examples are iSCSItarget, usbbackup, among others.

Still more were created by openmediavault plugin developers, such as Remote Mount, the flash-memory plug-in, backup plugins, and more.

Many plugins are integrations of third party packages such as SNAPRAID, MergerFS, etc. While questions or issues regarding the **integration of plugin's**, into openmediavault, are of interest to openmediavault's developers, questions regarding the **operation** of the base software package are best directed to the application's supporting web site.

### 5.19.3 Dockers - General

While Dockers are an avenue toward adding *extensive* functionality to openmediavault, they are an advanced topic that may prove to be frustrating for beginners. To get started, beginners should consider installing Docker, then Portainer, as found under System, OMV-Extras. While it's command line oriented, this [Docker Tutorial](#) is very helpful for understanding basic concepts. User authored [Docker - How To's](#) can be found on the openmediavault forum.

#### So, What is a "Docker"?

Dockers are a type of Virtual Machine (VM) that share the Linux kernel and memory spaces with the host. A Docker is spawned from a Docker image. The resultant VM equivalent, that's built from a Docker image, is referred to as a "container". A container is fully self-sufficient, bare-bones, Linux operating system. The idea behind a Docker image is to create a Linux installation, that is as small and as lean as possible, that includes all necessary dependencies required to run the Docker application and nothing more. Since these containers tend to be very small, they can be constructed and destroyed in rapidly. (After downloading, usually, in a matter of seconds.)

Dockers are more resource efficient when compared to running a full VM in a hypervisor, due to direct allocation of hardware resources. Typically, VM hypervisors provision fixed blocks of memory and may require access to dedicated hard disk space or block device partitions. Whether these dedicated resources are used by the VM or not, they're no longer available to the Host operating system or other VM's. A Docker, on the other hand, uses the needed memory space to run its processes and the host's hard drive for storage, without wasted resources. Resource management is lean and tight, allowing more Docker containers to run concurrently with much greater efficiency.

---

## Installing Docker

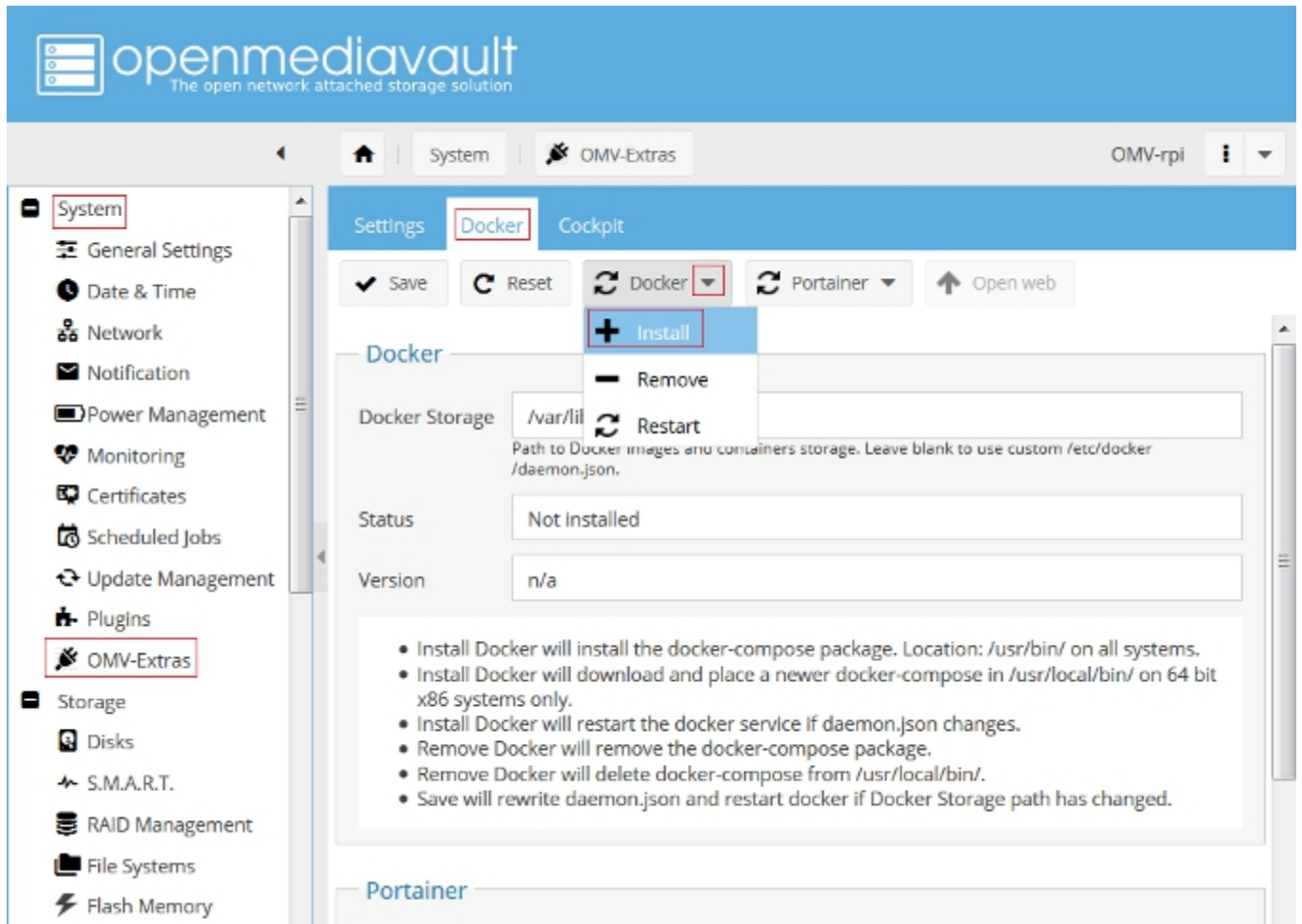
Installing *OMV-Extras* is a **prerequisite** to installing Docker.

---

Under **System, OMV-Extras**, select the **Docker** tab.

**Before installing Docker**, take note of the Docker Storage location. `/var/lib/docker` is on the **boot drive**. This location is not an issue for hard drives and SSD's of medium capacity (notionally, 128GB or larger.) However, when using flash media to boot (8 to 16GB), the boot drive is not a good location for media servers or downloader type Dockers. There are two possible solutions:

- The easiest solution is to change the Docker Storage path to a data drive. If the default path is changed, downloader output and metadata created by media servers (Plex and others) will be stored on a data drive by default.
- A more advanced solution would be to leave the default storage location in place (`var/lib/docker`) and configure the Downloaders and media servers to store their output and metadata on a data drive, but this requires individual configuration of each Docker.



To install Docker, click the **Docker Button** and select **Install**.

An install dialog box will popup and scroll as files are downloaded and installed. At the end, **Done** will be displayed. Click the **Close** button.

The **Status** line will report: **Installed and running**.

## Installing Portainer

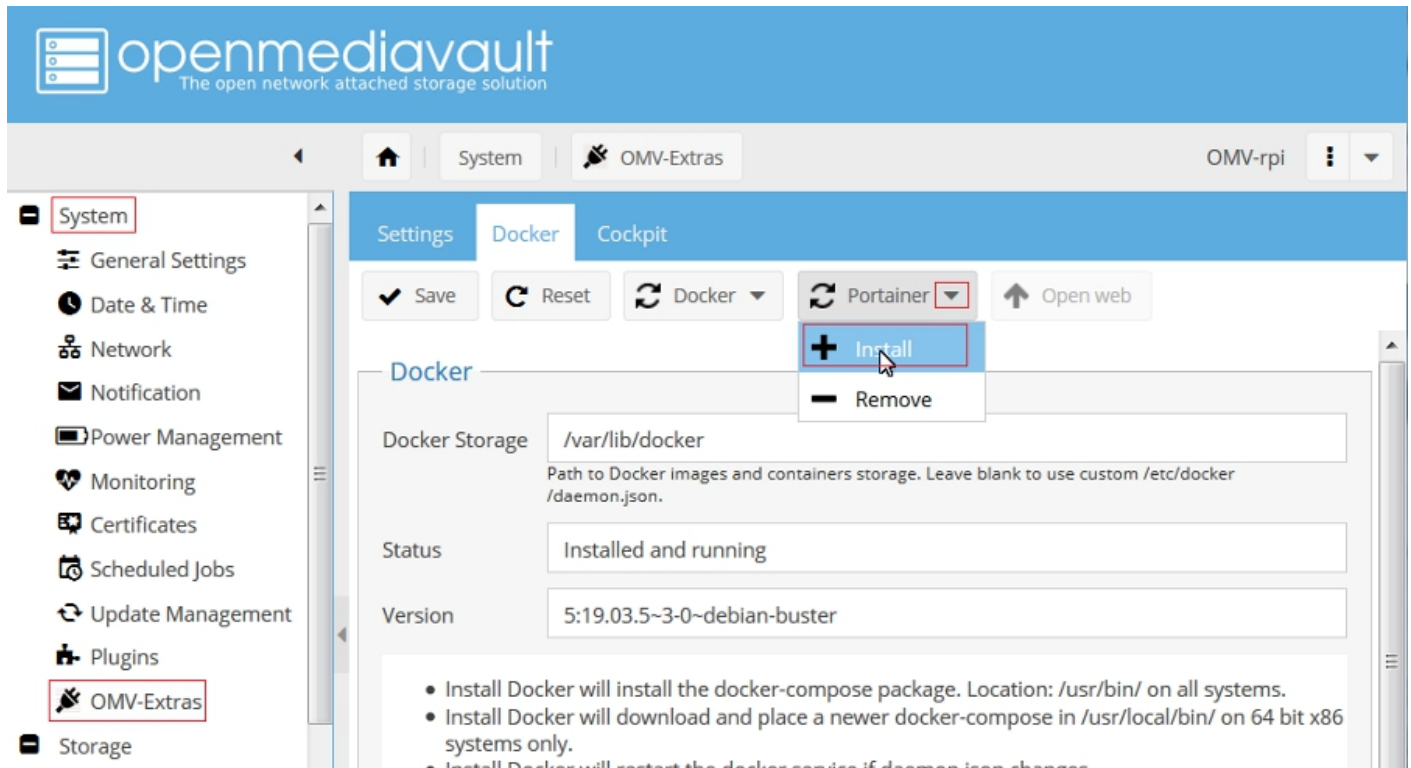
Under **System, OMV-Extras**, in the **Docker** tab, scroll down to the **Portainer** section.

### General:

While Portainer is a Docker itself, it is the control interface through which Dockers are downloaded and configured in openmediavault.

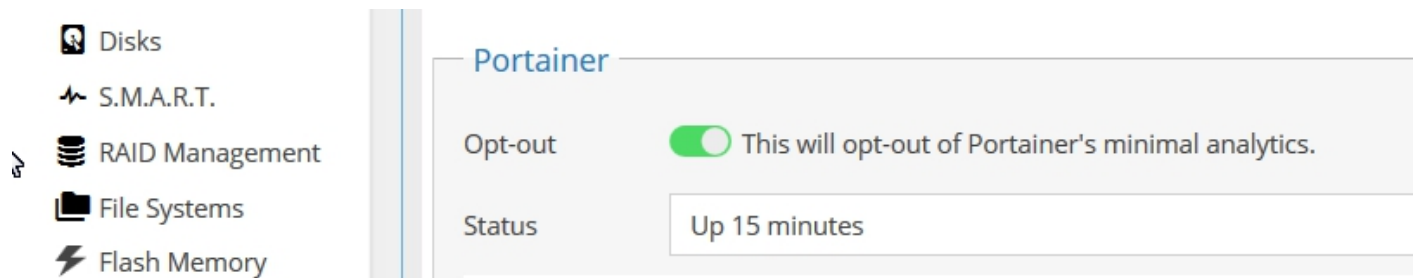
Click the **Install Portainer** button.





An install dialog box will popup and scroll as files are downloaded and installed. At the end, **Done** will be displayed. Click the **Close** button.

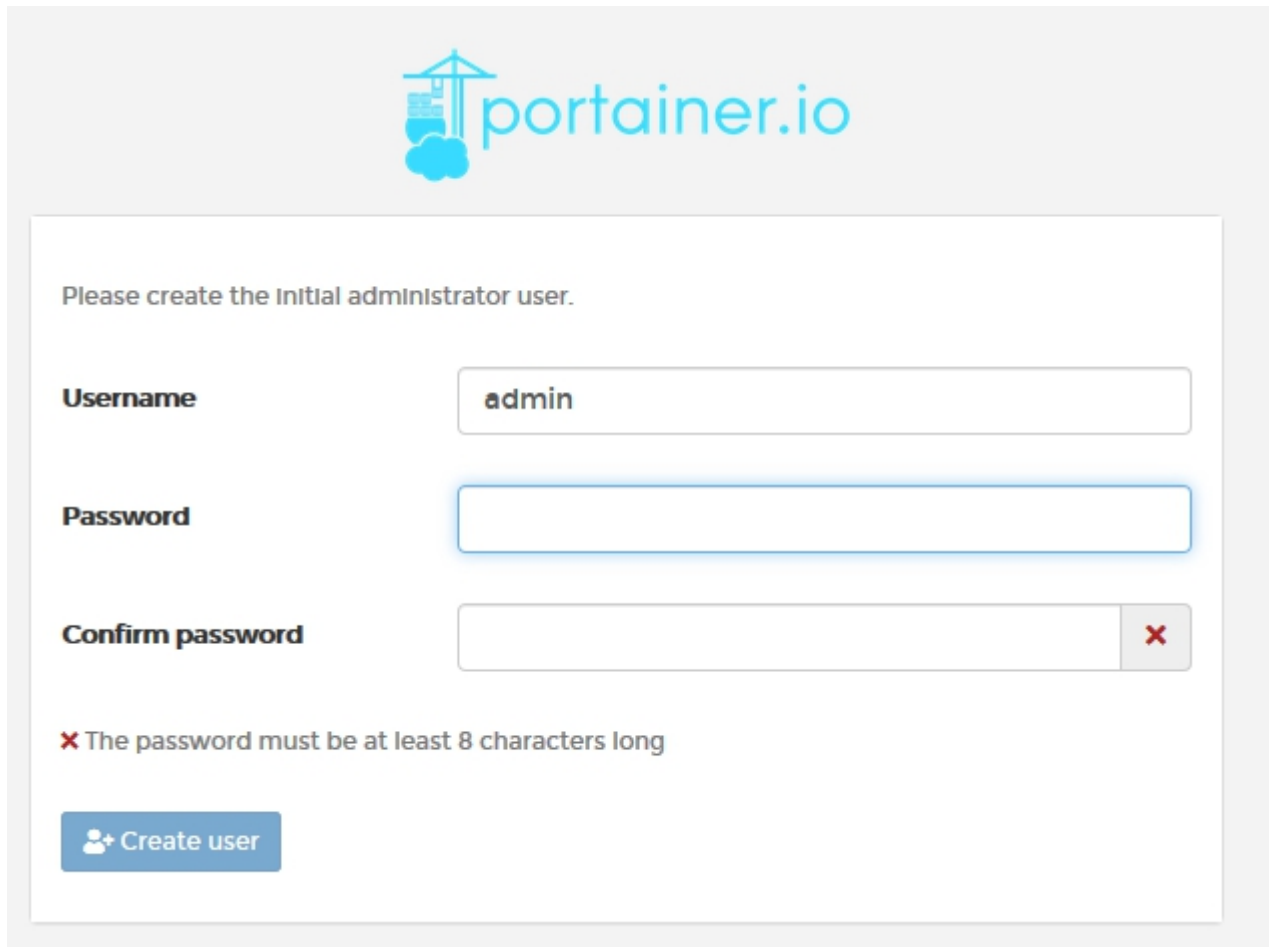
With a successful install, the **Status** line will change to reflect “**up**” time:



Finally, click on the **Open Web** button.

At this point, Portainer is completely unconfigured. The first configuration requirement is setting a password for the Admin user. Take note of this password. It will be needed to log into Portainer again.

Click on **Create User**



Please create the initial administrator user.

**Username**

**Password**

**Confirm password**  ✖


✖ The password must be at least 8 characters long


In the next log in, there will be a login dialog with two empty fields. Enter the username **admin** in the top field and the **password** in the bottom field.


---


When this screen pops up, Click on **Local**, then **Connect**

Connect Portainer to the Docker environment you want to manage.

  
**Local**  
 Manage the local Docker environment

  
**Remote**  
 Manage a remote Docker environment

  
**Agent**  
 Connect to a Portainer agent

  
**Azure**  
 Connect to Microsoft Azure ACI

---

**Information**

Connect Portainer to a remote Docker environment using the Docker API over TCP.

**i** The Docker API must be exposed over TCP. You can find more information about how to expose the Docker API over TCP in the [Docker documentation](#).

---

**Environment**

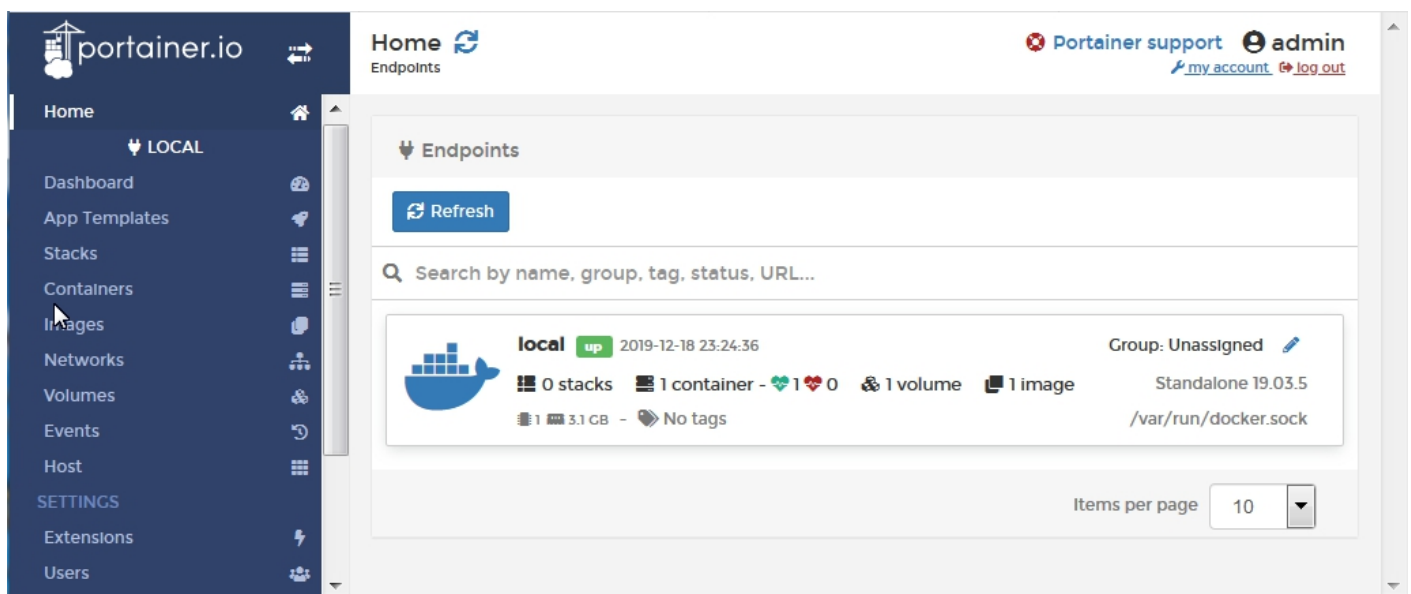
**Name**

**Endpoint URL**

**TLS**

### Dismiss the News and Click on Local

The following screen will now be the “**Home**” screen. Using “Local” menu selections on the left, this is where Docker Images are downloaded, containers are created, etc.



The screenshot shows the Portainer interface. On the left is a dark blue sidebar with the Portainer logo and a navigation menu including Home, LOCAL, Dashboard, App Templates, Stacks, Containers, Images, Networks, Volumes, Events, Host, SETTINGS, Extensions, and Users. The main content area is titled 'Home Endpoints' and shows a list of endpoints. The first endpoint is 'local', which is 'up' and was created on '2019-12-18 23:24:36'. It has a status of 'Group: Unassigned' and is located on 'Standalone 19.03.5' with the socket path '/var/run/docker.sock'. Below the endpoint details, there is a search bar and a table showing 0 stacks, 1 container (with 1 heart icon), 1 volume, and 1 image. The total size is 3.1 GB and there are no tags. At the bottom right, there is a pagination control showing 'Items per page' set to 10.

This concludes the installation of Docker and Portainer.

## 5.19.4 Dockers - It's about choices

While there are 100,000+ Dockers, available on the [Docker Hub](#), all are not created equal. The offerings, from Docker authors, range from a one-off experiment with no documentation (users are on their own) to organizations like [Linuxserver.io](#) that specialize in building first-rate Docker images. Linuxserver.io offers Dockers that have been thoroughly tested, they support multiple architectures, they provide detailed container setup instructions, their offerings are “Tagged” and they retain inventories of their older images.

---

### Selecting a Docker - Primary Considerations

#### First:

When installing a Docker, for the greatest chance of success, it is suggested that users follow the guidance provided in [Guides Section](#) of the openmediavault forum.

#### Second:

Potential Docker users must use Dockers that support their **architecture**. The three primary architectures supported by openmediavault are **ARMHF or ARM64, i386\*\* (32 bit), and \*\*amd64\* (64 bit)**. **In most cases, 32bit Dockers will run on 64bit hardware. \*\*While there may be exceptions, i386 and amd64 Docker images may not run on ARM platforms.** “\*\*Multi-arch” (multiple architecture) Docker images are more platform flexible.\*\*

#### Third:

To increase the chance of success, when attempting to install a Docker without a guide, look for the more popular Dockers with the highest number of “pulls” on the Docker Hub. ([hub.docker.com](http://hub.docker.com)) There are good reasons why these Dockers are broadly popular – they tend to work.

#### Forth:

In the *vast majority* of cases, Dockers that fail to work won't have anything to do with openmediavault or Portainer. Their issues tend to originate from selecting the **wrong architecture**, selecting the **wrong network mode** (host, bridged, macvlan) for the application, other configuration issues (such as port 80 OMV/Docker conflicts), permissions problems or the Dockers themselves.

Since most Dockers share Network ports with the host (openmediavault), it's important to use ports that are not currently in use. To get a better understanding of network ports and for commands that will reveal ports that are in use, refer to this forum post for more information:

[How-To] [Define exposed ports in Docker which do not interfere with other services/applications](#)

## 5.20 When things go wrong

First take note of any error dialog boxes. On most Windows and Linux machines it's possible to copy and paste the text out of a dialog box by holding down the left mouse button and dragging the mouse pointer over text, to highlight

it. Then use the keys with Ctrl+c (to copy), then click in a Notepad document and use Ctrl+v (to paste). This basic information will be helpful, in searching out the details related to the problem.

### 5.20.1 The First Resource – The Internet

Users should search the internet first. The solutions for many generic problems can be found with [google](#) , [yippy](#) , [duckduckgo](#) , and other search engines. When searching on key words that match error message or the problem users may be having, in some cases, answers can be found quickly in real time. This is the fastest and often the best way to learn how to fix server problems. Since openmediavault is based on “**Debian**”, it may be a useful search term.

While the search function of the openmediavault forum site will produce “hits” on search criteria, it is by no means all inclusive. If **OMV** is included in search criteria, a Google search may generate more result hits on information found on the openmediavault forum, than the forum’s integrated search function.

With information from searches, users should make an effort to address their own issues. This approach tends to be the path to the fastest answers and greatly facilitates the learning process.

### 5.20.2 The Openmediavault Forum

→ [Forum](#)

When coming to the forum for help:

First search the forum. In many cases, user problems can be resolved with a few searches and a bit of reading. However, look at the dates of posts and the version of openmediavault referenced. Posts that are 3 or more years old may not apply to the current openmediavault version.

If posting a problem on the forum, start at the [forum index](#) , and look for the category that looks to be appropriate for the post. Along with an explanation of the the issue, the openmediavault version, the appropriate logs and command line output, if known, and the hardware platform in use are the absolute minimums required. Realize that, without information, even the most experienced users, Moderators, and / or Developers will not be able to provide assistance.

- Ask the right questions. For beginners, this can be deceptively difficult. There’s some “straight forward” guidance on this topic here → [Ask the right questions](#) .
- While openmediavault’s forum is known for responsiveness, it’s unrealistic to expect answers in real time. It may be a matter of days before a forum member, who is familiar with the described problem, will read and respond to a post.
- When looking at answers, try to focus on the information presented, not the perceived tone. Remember that support is provided “**gratis**”, so act accordingly.
- Be open-minded. The reason why users post on the forum should be because they couldn’t solve a problem on their own. With that in mind, when an experienced forum user replies, taking the time to make a suggestion or requesting more information, forum users should follow up and post the result. Whether the issue is fixed or not, user posts help other users with the same or a similar problem.
- If a forum post or a “How To” fixes your problem, or gets you through a configuration issue, consider giving the author a “Like” or “Thanks”. The gesture is free and it’s an indicator to other users who may have the same problem. In essence, you’d be saying “I agree” or “this worked for me”.
- When users are experiencing problems with their data store (a file system issue, a hard drive, array, etc.) the working assumption on the part of experienced forum users and moderators will be that **users have full data backup**. Accordingly, recommendations for correcting filesystems, hard drives, and RAID array issues may result in the loss of data. **Keep this in mind.**

### 5.20.3 Solutions to Common Problems

Follow this link to the maintained list on the forum. → [Solutions to Common Problems](#)

#### USB RAID

**Problem:** I have an SBC and I'm having trouble with RAID. (OR) I have a USB connected drives that I want to configure as a RAID array.

**N/A:** USB RAID is not supported.

---

#### Rsync Drive Copy Errors

**Problem:** Rsync shows errors “Operation not permitted (1)” or “renaming” with regard to the files `aquota.user` and `aquota.group`. These files are found at the root of data drives.

In a very small number of instances, the quota service may interfere with an Rsync drive-to-drive copy.

##### Solution 1:

Add the following exclude statements to the rsync command line: `--exclude='aquota.group'`  
`--exclude='aquota.user'`

A full command line example:

```
rsync -av --delete --exclude='aquota.group' --exclude='aquota.user' /srv/  
dev-disk-by-label-DATA/ /srv/dev-disk-by-label-RSYNC/
```

---

**Note:** As of **OMV 5.5.20**, data drives are mounted using **UUID** (Universally Unique Identifier). Under **Storage, File Systems**, the path under the *Mount Point* column might appear as: `/srv/dev-disk-by-uuid-f188c8ad-74d3-443a-a23e-89711270367d` (This is an example only – all disks will have a unique identifier.) Check the Mount Point Column in File Systems for the appropriate path for `aquota` commands.

---

##### Solution 2:

Turn the quota service off.

```
sudo /etc/init.d/quota stop
```

(In the following examples, substitute the appropriate labels for the source and destination drives.)

```
sudo quotaoff --user --group /srv/dev-disk-by-label-DATA sudo quotaoff --user  
--group /srv/dev-disk-by-label-RSYNC
```

Optionally, delete the files `aquota.group` and `aquota.user` from the source and destination drives.

---

#### USB Power - A Common Raspberry PI problem

##### General:

Many problems with R-PI's, in versions prior to the R-PI4, are related to under-powering. While the R-PI4 is much improved, depending on the power requirements of connected peripherals, it is not exempt from power problems. The issues caused by under-powering can range from bizarre behavior to data corruption on storage devices.

## Do I have a problem?

With all peripherals attached that are normally used – use the command `dmesg` on the CLI and scroll through the output. If an **undervoltage** situation exists, it will be noted in the output.

## What is the problem?

Beyond using a power supply with the appropriate current rating for the R-PI model, it should be noted that a USB power source must meet certain voltage specifications “at the socket”. In essence, the output voltage of a USB power supply can’t be increased to compensate for external voltage losses typical when using a long USB cable with small gauge wire.

Making matters worse is, models prior to the R-PI4 use a micro USB plug as the power connection. The tiny contacts of a micro USB connection, combined with cables for micro USB that have small gauge wires, drop power supply voltage significantly.

## Consider the following chart of voltage losses, versus wire length and gauge

(Note that voltage drops increase as current draw requirements rise.)

Voltage Drop at 1000mA						
AWG	15cm	50cm	1m	2m	3m	5m
20	0.129993	0.15331	0.18662	0.25324	0.31986	0.4531
22	0.135888	0.17296	0.22592	0.33184	0.43776	0.6496
24	0.145266	0.20422	0.28844	0.45688	0.62532	0.9622
26	0.16017	0.2539	0.3878	0.6556	0.9234	1.459
28	0.18387	0.3329	0.5458	0.9716	1.3974	2.249

Voltage Drop at 2000mA						
AWG	15cm	50cm	1m	2m	3m	5m
20	0.259986	0.30662	0.37324	0.50648	0.63972	0.9062
22	0.271776	0.34592	0.45184	0.66368	0.87552	1.2992
24	0.290532	0.40844	0.57688	0.91376	1.25064	1.9244
26	0.32034	0.5078	0.7756	1.3112	1.8468	2.918
28	0.36774	0.6658	1.0916	1.9432	2.7948	4.498

## Potential Remedies:

- Use a power supply that meets at least the minimum recommended current rating for the R-PI model being used.
- Use the shortest possible USB cable. Cables that are 1 foot / 30cm or less, made of thick gauge wire are preferred. If a short USB cable is not long enough to place an R-PI in a convenient location, use an AC extension cord rather than a long USB cable.
- Avoid using direct connected USB powered hard drives. The additional current load will drop voltage and may stress a weak power supply. A self powered USB hub or a drive dock is preferred.
- Avoid leaving peripherals attached, such as a monitor, keyboard or a mouse. Even when they’re not used, they consume power.

## 5.21 A Closing Note

We, who support the openmediavault project, hope you've found this guide to be useful and that you'll find your openmediavault server to be efficient, easy to use, and enjoyable.



Configuration changes are not applied immediately, instead you can determine when this happens. This enables several changes to be activated at the same time, which reduces unnecessary waiting times.

---

**Note:** openmediavault does not display the submodules that are affected by the configuration changes. If you still want to know which submodules are affected, simply run `cat /var/lib/openmediavault/dirtymodules.json` in the CLI.

---

## 6.1 General

### 6.1.1 Network

In this section you can set several system network related settings.

#### General

Hostname and domain settings.

#### Interfaces

Only network interfaces that have been configured via the web interface are displayed in the data table. If this panel is empty right after the installation the automatic synchronisation of the interface configuration that was done by the installer. In this case simply start to configure the interfaces via the web interface.

The dashboard contains a network widget that displays the current status of the interfaces.

## Ethernet

Just select DHCP or static. openmediavault is a server so the recommended setting is to have static IP address, if you have a proper network infrastructure (separate router and switch). In a reboot, if the router fails to boot you can still access the web interface through the switch bridge. If the switch also fails you can use a direct Ethernet connection with the static IP address assigned to the server NIC.

Do not leave DNS setting empty; it is essential for fetching updates. A common value is to use the same IP address as the gateway. If unsure, just use google DNS 8 . 8 . 8 . 8.

**Wake on LAN (WOL)** This enables WOL in the kernel driver, make sure the NICs supports this and the feature is enabled in BIOS.

## Wireless

The configuration window displays the same IP configuration fields as Ethernet, plus the relevant wireless values: SSID (the wireless network name) and the password.

Whenever possible, use Ethernet for a NAS server. Wireless should not be used in a production server; this feature is intended for extreme cases only.

## VLAN

If your network supports VLAN, just add the parent interface and the VLAN id.

## Bond

The configuration window provides all available **modes** for the bond driver. To configure bonding, is necessary at least two physical network interfaces. The web interface allows the selection of less than two. This is by design for configuration purposes. The workflow is as follow for dual NICs:

- If the primary NIC is already working either by the installer, configure it through the web interface as static. If set as static using the same IP address given by DHCP, it should not be necessary to re-login to the web interface.
- Click **Network | Interfaces | Add | Bond**, select the second available NIC, select the bond mode, fill the IP field and subnet mask values, leave gateway and DNS empty. Save and hit apply.
- Log out and access the web interface using the new IP address assigned to the bond interface created.
- Now select the primary interface configured through web interface in the first step, and delete it. Save and hit apply.
- Select the newly created bond interface, click edit add now the physical nic that was deleted from the step before should be available to select. Save and hit apply.
- The dashboard should now report the bond interface information (including speed).

---

### Note:

- 802.3ad LACP (Link Aggregation) mode only works if physical interfaces are connected to a managed switch that supports aggregation.
- Is not possible to achieve 2Gbit bandwidth (or more depending on the number of NICs) in a single client using LACP, even if the client also has a LACP-bonded NIC or 10Gbit card; there is no multipath support in Samba or other openmediavault services in the way Windows Server has for file sharing using SMB.

- Higher speeds using link aggregation are limited by disk speed. When serving simultaneous clients make sure the physical media is capable of reaching the speed of the bonded NIC (e.g. SSD or RAID array).
- 

## Advanced Interface Configuration

### Proxy

This panel configures the server proxies using system wide environmental variables. All software that obeys Linux proxy environmental variables should be able to use the proxy. This is useful for example if there are many Debian servers in the network, when performing **apt** operations, packages can be cached in the proxy if this configured appropriately to reduce download bandwidth.

The variables name are:

```
http_proxy
https_proxy
ftp_proxy
```

This settings do not configure openmediavault to act as a proxy server.

### Service Discovery

This panel configures the Zeroconf/mDNS announce service. You can disable selectively by service and/or change the common name announce. openmediavault plugins can add their service here. Zeroconf/mDNS announces are recognized by Linux file browsers by default. Mac OSX only recognizes SMB and AFP protocol in their sidebar. Windows does not understand Zeroconf/mDNS announces.

### Firewall

This data table is for adding iptables rules. This can be useful if you need to secure access in your local network. Currently it is only possible to add rules to the OUTPUT and INPUT chains in the filter table. The configuration to load the rules at boot or network restart is done by the systemd unit called *openmediavault-firewall*.

---

#### Tip:

- To avoid locking yourself out while testing, create a cron command to run every five minutes that flushes the OUTPUT/INPUT chain. Don't forget to delete the cron job after testing.:

```
*/5 * * * * root /sbin/iptables -F INPUT && /sbin/iptables -F OUTPUT
```

- Before adding the last rule to reject all, add a rule before the reject all, to LOG everything. This will help understand why some rules do not work. The log is saved in dmesg or syslog.
- 

**Tip:** When seeking support please avoid posting screenshots of the data table, this is useless because it does not give the full overview of your firewall ruleset. Instead use:

```
$ iptables-save > /tmp/file.txt
```

---

## 6.1.2 Notifications

Notifications work in the form of email. The backend software used here is postfix<sup>1</sup> configured as a MTA in satellite mode. The options allow to configure to send mail via SMTP servers using the standard port or use SSL/TLS. The web interface allows the configuration of two recipient addresses. Both are assigned to the root user.

### Configuration

The central MTA configuration is stored in `/etc/postfix/main.cf`

openmediavault creates the `/etc/postfix/recipient_canonical` to define the root (admin) and normal users mail addresses when added via the web interface. Example:

```
root rootthe@gmail.com
mike mikeadmin@themailco.com
@server.lan rootthe@gmail.com
```

When a scheduled task is defined to run as a certain user the output generated from that task, will be sent to that user defined mail.

The last line is the catch all address. For example a scheduled task set to be run as user with no mail defined in their profile will get the output generated sent to the catch all address (`rootthe@gmail.com`). The same will happen with any other mail action intended for an undefined user (not in that list).

Mails can be sent from terminal also with mail command. `mail` receives from `stdin`.

Examples 1:

```
$ echo "Message body" | mail -s "Test subject" mike
```

Mail will be delivered to `mikeadmin@themailco.com` as it is defined in `canonical_recipients`. The delivery address can be explicit also:

```
$ echo "Message body" | mail -s "Test subject" mikeadmin@themailco.com
```

Examples 2:

```
$ echo "Message body" | mail -s "Test subject" john
```

Mail will delivered to `rootthe@gmail.com` because user **john** does not have an email address defined in `canonical_recipients`, so it goes to the catch all address.

**Warning:** openmediavault stores the configuration values in the database (including the password). Before posting information for support please sanitize the values.

### Events

The server will send notifications for this events:

- Log in from browser (If cookies are allowed, then it just sends once).
- Use of sudo by a user not in allowed group.

---

<sup>1</sup> <http://www.postfix.org>

- Summary of locked users by pam\_tally<sup>2</sup>. This happens when a user or admin attempts fails to log in for more than three times.
- MD RAID events: degraded, reshape, etc. [D]
- Monit software: php-fpm, nginx, netatalk, rrdcached, collectd and omv-engined. [D]
- Monit filesystem: usage and mount points. [D]
- Monit system: CPU, Load and memory usage. [D]
- Scheduled tasks. [D]
- Rsync jobs. [D]
- Cron-apt: Summary of upgrade packages available. [D]
- SMART: Report of attribute changes. [D]

Options marked with [D] can be disabled selectively. The rest only when the whole notification backend is disabled.

## Gmail

Gmail can be used in notifications. If you have 2FA enabled for the account, then is necessary to create an [app password](#). Please use the following settings:

```
SMTP Server: smtp.gmail.com
SMTP Port: 587
Encryption mode: STARTTLS
Sender email: rootthe@gmail.com (include domain)
Authentication required: Yes
Username: rootthe@gmail.com (include domain)
Password: <the app password here>
Primary email: rootthe@gmail.com
Secondary email: optional
```

---

**Note:** Aliases are allowed. This is good for filtering later in gmail. `rootthe@gmail.com` can be `rootthe+server1@gmail.com` or `rootthe+whatever@gmail.com`.

---



---

**Note:** Gmail requires “access for less secure applications” to be enabled, in order for openmediavault to send notifications using `smtp.gmail.com`. [Enable access for less secure applications](#).

---

## Third Party Notifications

Whenever a mail is dispatched by the MTA, postfix will execute a run-parts of this directory `/usr/share/openmediavault/notification/sink.d`, passing the following environmental variables:

```
OMV_NOTIFICATION_FROM
OMV_NOTIFICATION_RECIPIENT
OMV_NOTIFICATION_SUBJECT
OMV_NOTIFICATION_DATE
OMV_NOTIFICATION_MESSAGE_FILE
```

Also the following positional arguments are passed:

<sup>2</sup> [http://www.linux-pam.org/Linux-PAM-html/sag-pam\\_tally2.html](http://www.linux-pam.org/Linux-PAM-html/sag-pam_tally2.html)

```
$1 The path of the file containing the message text (OMV_NOTIFICATION_MESSAGE_FILE)
$2 The FROM email address (OMV_NOTIFICATION_FROM)
$3 The TO recipient email addresses (OMV_NOTIFICATION_RECIPIENT)
```

Most modern non mail notifications systems have a documented API, where you can send text using curl payloads with a secret *TOKEN*. So most common case would be to use *OMV\_NOTIFICATION\_MESSAGE\_FILE* variable only in your script.

Your script's filename must adhere to the following standards:

- Must belong to one or more of the following namespaces:
  - The LANANA-assigned namespace (`^[a-z0-9]+$`)
  - The LSB hierarchical and reserved namespaces (`^_?([a-z0-9_]+)+[a-z0-9]+$`)
  - The Debian cron script namespace (`^[a-zA-Z0-9_-]+$`)
- Start with a number like this: `<##>pushnotification`

---

**Note:**

- Do not add an extension to your script in the run-parts directory, otherwise it will get excluded.
  - Make sure the script file is executable. In this case also make sure the script is not a symlink to a mounted filesystem with *noexec* flag.
- 

## 6.1.3 Scheduled Jobs

### Overview

You can configure common and repetitive command(s) or scripts in this section. Is based on cron using the `minute hour day Week month crontab syntax`<sup>1</sup>. Due to web framework limitation, ranges are not supported. If you need a range you can configure a task for each day or simply use terminal with:

```
$ crontab -e
```

The grid panel reflects all current created cron jobs done via the web interface. The second field reflects the schedule in crontab language.

### Options

**Username:** Under what user should the command/script be executed. You can select root, system accounts and openmediavault users.

**Mail Notification:** Send all the command/script output to the mail defined in the username profile. If the task is running as root, the mail recipient will be the one defined in notifications for primary and secondary delivery. If openmediavault user is defined in the task and has an email configured in their *profile* the notification will be sent to that mail address.

---

<sup>1</sup> <https://linux.die.net/man/5/crontab>

## Configuration

The server configures all tasks done in the web interface creating this file `/etc/cron.d/openmediavault-userdefined` on demand as single lines per job.

```
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
# m h dom mon dow user  command
12 18 * * * root /var/lib/openmediavault/cron.d/userdefined-04dc9701-881f-4440-93e2-
↳66c385df4068 | mail -E -s "Cron - Movies" -a "From: Cron Daemon <root>" root >/dev/
↳null 2>&1
50 18 * * * root /var/lib/openmediavault/cron.d/userdefined-69a1cf21-3099-4d37-bb8f-
↳df3fecfac988 >/dev/null 2>&1
@daily root /var/lib/openmediavault/cron.d/userdefined-f04f0bbb-03d3-4d45-9efb-
↳e1e980cbbaf3 >/dev/null 2>&1
```

First is the cron time or interval, then username finally the command. The actual command is wrapped in a shell script located in this folder `/var/lib/openmediavault/cron.d/`. All files in there are prefixed with username and the internal database uuid.

### Warning:

- When using a single command to be executed, make sure this does not have any bashism. This because the cron wrapper script gets executed in pure shell `#!/bin/sh`. If you need to use something in bash wrap your command(s) in a bash script.
- `@hourly`, `@daily`, `@weekly` and `@monthly` are just nicknames. If you select `@daily` and your computer is shutdown at midnight the task will not run<sup>1</sup>.

## 6.1.4 Power Management

### Monitoring

Configures `cpufrequtils` and sets the default options for the governor to be **conservative** by default in x86 architectures if enabled. If architecture is different then governor is set as **ondemand**.

`/etc/default/cpufrequtils`

```
ENABLE="true"
GOVERNOR="conservative"
MAX_SPEED="0"
MIN_SPEED="0"
```

`/etc/default/loadcpufreq`

```
ENABLE="true"
```

All values above can be changed via *environmental variables*.

### Power button

Configures the action to take when pressing the mechanical power button of the server.

## Scheduled

Based on cron, is possible to define shutdown, hibernation or suspend times for the server.

## 6.1.5 Certificates

This section allows you to create or import SSH keys or SSL certificates.

### SSH (Secure Shell)

The public/private pair keys created or imported here are for using in the *RSync client (jobs)* service section. Plugins can use the internal database if they want to use these keys using the SSH certificates combo class. The key pair will be stored in the internal database, but only the public key will be available for display just by clicking edit. Not displaying the private key is basic ssh security as it never has to leave the host where it was created. The public key can be copied to clipboard or any other transport to be added to a remote server. Add a comment as this will be appended to the public key, this is important if you need to revoke the key pair in the remote server in case the server that generated the pair is compromised. The keys are stored beside the database in these two files:

- **Public key:** `/etc/ssh/openmediavault-<uuid_suffix>.pub`
- **Private key:** `/etc/ssh/openmediavault-<uuid_suffix>`

The `<uuid>` suffix is the internal openmediavault reference number.

---

**Note:** The public key is not displayed in RFC 4716. In case the remote server is also openmediavault based, you need to *convert* it the appropriate format.

---

### SSL (Secure Socket Layer)

The SSL certificates created or imported here can be used by the web interface or FTP server. Plugins can also use them by adding the SSL certificate combo class. The create window has the most common SSL certificates fields. The certificate/private pair is stored in the internal database and as files in the Linux standard SSL location. Certificate file with a `<uuid>` suffix, which is the internal database number:

```
/etc/ssl/certificates/openmediavault-<uuid>.cert
```

Private key file with the same `<uuid>` suffix as their certificate pair.

```
/etc/ssl/private/openmediavault-<uuid>.key
```

When importing existing ssl certificates make sure they are formatted/converted appropriately.

The command that creates the certificate runs in the PHP backend and is documented [here](#). This certificates are self signed, without root CA.

### LetsEncrypt

Lets Encrypt certificates can be imported directly, just locate your `/etc/letsencrypt/live/<mydomain.com>/fullchain,privkey.pem` files and copy their contents in their respective field. No need to convert.



## 6.2 Storage

### 6.2.1 Disks

An overview of all physical disks attached to the server. Displays basic information to identify disks, such as: manufacturer, model, serial number and capacity. A hidden column also displays the linux block device identification symlinks `/dev/disk/by-id,by-path,by-uuid`.

Be aware that when attaching disks via USB (a docking station, cage, adapter, etc.) the internal disk information will not pass, the backend will display probably the USB-SATA controller information. The capacity should remain the same. This is a response given by the backend with `DiskMgmt::getList` service-method using a rock64 SBC board with a docking station attached via the USB 3.0 port:

```
{
  "response": {
    "total": 3,
    "data": [
      {
        "devicename": "mmcblk1",
        "devicefile": "/dev/mmcblk1",
        "devicelinks": [
          "/dev/disk/by-id/mmc-SL16G_0x0091d901",
          "/dev/disk/by-path/platform-ff500000.dwmmc"
        ],
        "model": "",
        "size": "15931539456",
        "description": "n/a [/dev/mmcblk1, 14.83 GiB]",
        "vendor": "",
        "serialnumber": "",
        "israid": false,
        "isroot": true
      },
      {
        "devicename": "sda",
        "devicefile": "/dev/sda",
        "devicelinks": [
          "/dev/disk/by-path/platform-xhci-hcd.8.auto-usb-0:1:1.0-scsi-0:0:0:0",
          "/dev/disk/by-id/usb-USB_3.0_HDD_Docking_Station_2017101701E0-0:0"
        ],
        "model": "",
        "size": "500107862016",
        "description": "n/a [/dev/sda, 465.76 GiB]",
        "vendor": "USB 3.0",
        "serialnumber": "2017101701E0",
        "israid": false,
        "isroot": false
      },
      {
        "devicename": "sdb",
        "devicefile": "/dev/sdb",
        "devicelinks": [
          "/dev/disk/by-id/usb-USB_3.0_HDD_Docking_Station_2017101701E0-0:1",
          "/dev/disk/by-path/platform-xhci-hcd.8.auto-usb-0:1:1.0-scsi-0:0:0:1"
        ],
        "model": "",
        "size": "2000398934016",
        "description": "n/a [/dev/sdb, 1.81 TiB]",

```

(continues on next page)

(continued from previous page)

```

        "vendor": "USB 3.0",
        "serialnumber": "2017101701E0",
        "israid": false,
        "isroot": false
    }
]
},
"error": null
}

```

Notice here `sdb` and `sda` both disks show same serial number and that is incorrect. There is no vendor and model shows as “USB 3.0”.

In this cases you can access the disk information in the SMART section, not the grid but the information button. External portable USB hard drives should display information normally.

## Power Options

Pressing the edit button with a selected disk will give the following options available to set:

- Advanced power management (APM)
- Automatic accoustic management (Not all drives support this)
- Spindown time (ST)
- Write cache

All the above options are configured using `hdparm`<sup>1</sup>. The APM values from the interface are resumed in seven steps with a small description to make it easier for the user to select. If you want to experiment with intermediate values then you can edit `/etc/openmediavault/config.xml` find this xpath `/storage/hdparm`, change the values for the disk, finally run:

```
$ omv-salt deploy run hdparm
```

Reboot, check if APM has been set with:

```
$ hdparm -I /dev/sdX
```

When setting a spindown time make sure APM is set bellow 128, otherwise it will not work. The web framework does not narrow the APM options if spin down time is set, or disables the spindown menu when a value higher than 128 is selected.

---

**Note:** For changes to be permanent, settings are stored in this file `/etc/hdparm.conf`, however those settings are applied using a UDEV `ADD+` that executes `/lib/udev/hdparm` which parses that file. For changes to be applied immediatly server needs to be suspended/resumed or rebooted.

---

## Wipe

If you need to erase data from your disks, you can use this button. It gives the secure or quick option.

The quick option basically erases the partition table and signatures (MBR or GPT) by using this command:

<sup>1</sup> <https://linux.die.net/man/8/hdparm>

```
$ sgdisk --zap-all /dev/sdX
```

After that it ensures is clean by using dd:

```
$ dd if=/dev/zero of=/dev/sdX bs=4M count=1
```

Which erases the beginning of the disk.

The secure mode will rewrite the block device entirely. This process takes a long time and is only one iteration. It uses this command:

```
$ shred -v -n 1 /dev/sdX
```

## 6.2.2 SMART

Modern hard disks drives (and SSD's) have firmware inside that reports several attributes (usually called S.M.A.R.T values) through sensors that are relevant to assess the device condition. Those values and what they mean are explained by [here](#). Not all drives report the same amount of attributes, but all of them report some common ones which are known to be the best for assessing health<sup>1</sup>.

There are several tools for accessing those attributes. openmediavault reads and monitors hard drives smart values using smartmontools<sup>2</sup>.

Notifications are integrated with smartmontools. Changes in S.M.A.R.T values are reported via mail.

### General

This enables smartd (SMART daemon). The daemon will periodically check disks attributes and compare them with previous check. You can select the daemon not to poll information if the disks are in certain power state.

Temperature is a very critical attribute. Select the desired limits for smart monitoring to report on changes<sup>3</sup>.

### Devices

The grid displays all current block devices in the system with SMART capabilities. From this grid by selecting a drive you can configure if you want smartmontools to watch and inform for any SMART attributes changes during uptime using the edit button.

Smartmontools is configured in this file `/etc/smartd.conf`.

The information button displays several tabs which provide friendly parsed information about the drive. The last tab has all the information in raw text.

The grid columns shows different identification values for the drive, the last one (Status) reports a green icon if drive is in good condition or red if drive needs some attention, if you hover on the icon a tooltip that will report more details. The code that reports the red icon is based on this function [here](#) and [here](#), so basically the red icon will be triggered only on attributes with the prefailure (P) flag when:

- Any attribute (P) current value is equal or less than threshold → Bad attribute now
- The attribute (P) worst value is equal or less the threshold value → Bad attribute in the past

<sup>1</sup> <https://www.backblaze.com/blog/what-smart-stats-indicate-hard-drive-failures/>

<sup>2</sup> <https://www.smartmontools.org/>

<sup>3</sup> <https://www.backblaze.com/blog/hard-drive-temperature-does-it-matter/>

- `Reallocated_Sector_Ct (id=5)` and `Current_Pending_Sector (`id=197)` raw attributes values report more than 1 → Bad sector

---

**Note:** Do not enable SMART for a virtual block device (Virtualbox, Proxmox or ESXi) and expect to get reports of SMART values.

---

### Scheduled tests

Gives an option to select four different scheduled tests:

- Short self-test
- Long self-test
- Conveyance self-test
- Offline immediate

These tests and what they do are explained [here](#) and [here](#).

SMART only reallocates a bad sector on write. A manual method to force reallocating the pending(s) sector(s) is described [here](#).

## 6.2.3 RAID

openmediavault uses linux software RAID driver (MD) and the `mdadm` utility to create arrays<sup>1</sup>. Arrays created in any other linux distro should be recognized immediately by the server. In most cases you can skip to the filesystem array and proceed to mount to integrate the filesystem into the database.

### Overview

The grid panel shows all currently available MD arrays. There is no internal database section for RAID arrays, so every array that is assembled in the server should be displayed here.

**Create** The following table displays levels available in the web interface:

Table 1: RAID

Level	Name	Min. Disks	Redundancy	Growable
Linear	JBOD	2	No	No
0	Stripe	2	No	No
1	Mirror	2	Yes	Yes
5	RAID5	3	Yes	Yes
6	RAID6	4	Yes	Yes
10	Stripped Mirror	4	Yes	No

---

**Note:**

- RAID4 and FAULTY levels are not supported in the web interface.
- RAID1+0 is possible by stripping two mirrors. The create window should display both mirrors if they do not have any filesystem signatures yet.

---

<sup>1</sup> [https://raid.wiki.kernel.org/index.php/Linux\\_Raid](https://raid.wiki.kernel.org/index.php/Linux_Raid)

**Detail** Displays extended information of the array, the output comes from `mdadm -detail /dev/mdX`

**Grow** Add disk(s) into the array.

**Recover** If the array comes from another linux server you can use this button to reassemble the array in the current server

**Remove** This is used to remove failed disks, in case one needs be replaced.

**Delete** Stop the array and zero the superblock of all devices conforming the array (script `/usr/sbin/omv-rmraid`). Use with caution.

Mdadm works better with unpartitioned disks, plain raw block devices. Before creating MD RAID in your system make sure disks are clean before. In the physical disk section you can perform a quick or full wipe. Quick wipe is enough to delete partition tables.

Degraded array creation is not possible in the web interface, however the array can be created in terminal using mdadm if you want for example to convert a RAID from level 1 to 5 or 6.

Mail notifications are integrated for mdadm, these are sent everytime an array enters degraded state.

## Growing

Before growing array is better to clean the partition table of the new disk, specially if the disk was used before in another mdadm array, erase also the superblock:

```
$ mdadm --zero-superblock /dev/sdX
```

After adding a disk to the array, the re-synching process will begin immediately. Depending on the size of the disks this process can take several hours or even days, this is because mdadm tries to balance resources and keep usability of the system not using high CPU and RAM. To speed the process:

```
$ echo ${value} > /proc/sys/dev/raid/speed_limit_min #value is interpreted as kbytes/  
↪seconds
```

After synching is finish is necessary to expand the filesystem using the resize button.

### Warning:

- If your MD array and filesystem was created with openmediavault or Debian before December 2014, then please read [here](#).
- Do not use RAID arrays in production with drives connected via USB, neither hubs or different ports. This includes low power devices that do not have a SATA controller, e.g. Raspberry Pi, Pogoplug and any low entry ARM SBC.

## 6.2.4 Filesystems

**Overview** The filesystem section of the openmediavault web interface is where you integrate disk volumes to be part of the server. Drives/filesystems that are not mounted through the web interface are not registered in the backend database, this means you cannot use volumes to create shared folders if they were not mounted properly. *This is very important*, users that come from an existing debian installation with filesystems already present in their fstab file will see that no volumes will be available for creating shared folders even if they are mounted. For the disks to be properly integrated it is better to delete all fstab lines except rootfs and swap, reboot your server and start mounting the disks through the web interface.

The mount process acts like many other services in openmediavault, first it writes a database entry in `config.xml`, this entry contains essential information:

- UUID of the database object `<uuid>`
- Predictable device path of the filesystem `<fsname>`
- Target mount directory `<dir>`
- Filesystem options `<opts>`
- Filesystem type (EXT3, EXT4, etc.) `<type>`

You can inspect a `mntent` entry in `config.xml` it should look like this:

```
<mntent>
  <uuid>f767ee54-eb3a-44c5-b159-1840a289c84b</uuid>
  <fsname>/dev/disk/by-label/VOLUME1</fsname>
  <dir>/srv/dev-disk-by-label-VOLUME1</dir>
  <type>ext4</type>
  <opts>defaults,nofail,user_xattr,usrjquota=aquota.user,grpjquota=aquota.
↔group,jqfmt=vfsv0,acl</opts>
  <freq>0</freq>
  <passno>2</passno>
  <hidden>0</hidden>
</mntent>
```

With the `mntent` entry in `config.xml`, `omv-salt deploy run fstab` script writes the appropriate line in `/etc/fstab`. You can identify entries in `/etc/fstab` created by the web interface by looking at «openmediavault» tags. It is important to mention to not alter the information in between these tags. If you delete or modify a `fstab` option (`noexec` or `quota` for example) the next time you mount a new disk into the server, `omv-salt deploy run fstab` will deploy the original value there again. If you need persistent change use environmental variables. Finally the backend will proceed to mount the filesystem. After this the volume is ready for creating shared folders.

**Resize** The resize button is used for expanding filesystems. This can occur if you decide to resize a disk partition or you have grown a RAID array by adding one or more disks.

**Delete** The delete button actually deletes filesystems, using `wipefs -a`. This will flush filesystem, raid or partitionable signatures (magic strings). Be careful using this. The button is disabled until the filesystem is actually unmounted.

**Unmount** Disabled until you have deleted all shared folders associated with that volume. Unmount will remove the entry from `config.xml` and `/etc/fstab`.

**Supported Filesystems** openmediavault supports the following filesystems that can be mounted through the web interface:

Table 2: openmediavault supported filesystems

Type	Format	Mount
ext4	yes	yes
ext3	yes	yes
jfs	yes	yes
xfs	yes	yes
btrfs	yes	yes
zfs	no	no
ntfs	no	yes
hfsplus	no	yes
ufs	no	yes
vfat	no	yes

**Note:****BTRFS**

- Creating multi device filesystems is not supported in the web interface. However you can add devices to your btrfs array in CLI and it will not present any problems.
- No extra features of btrfs are available in the webui like snapshots or subvolumes. Additional subvolumes will have either be mounted outside of the OMV fstab tags or manually add mntent entries to config.xml or use advanced configuration

**Note:**

**ZFS** Support for zfs is available through [ZoL](#) an uses a third party plugin provided by omv-extras. The development of the plugin was done in conjunction with core of openmediavault, so new code was added in the filesystem backend to improve support for zfs. The plugin registers datasets and pools in the internal database so you can create shared folders for zfs volumes. The creation of zvols is automatically recognized by openmediavault so you can format them and mount them in the web interface. The iscsiplugin can also use these zvols block devices to export LUN's.

## 6.3 Access Rights Management

In this section you can create, edit and access information of openmediavault users, groups and shared folders.

### 6.3.1 User

Create or modify users information and configuration of home folders.

**Add**

**Information** The configuration panel gives you options to add, edit or remove users. The grid displays all openmediavault current users.

When a user is created openmediavault backend executes `useradd` in non-interactive mode with all the information passed from the web text fields, this command also creates an entry in `/etc/passwd`, a hashed

password in `/etc/shadow`. Samba service is watching any changes in users database section so it also sets the password in the samba tdbsam storage backend.

The mail field is used for cron jobs when the task is selected to run as specific user. By default users are created with `/bin/nologin` shell, this will prevent local and remote console access.

**Group** Add or remove users from specific groups. In linux groups can be used to control access to certain features and also for permissions.

Adding a user to the `sudo` group will give them root privileges, adding a user to `saned` will give access to scanners, etc. By default all users created using the web interface are added to the `users` group (`gid=100`).

**Public Key** Add or remove *public keys* for granting remote access for users.

---

### Note:

- The user profile information (except password) is also stored in the internal openmediavault database, along with the public keys.
  - The grid shows information from internal database and also parses information from `/etc/passwd` lines with a `UID` number higher than 1000. A user created in terminal is not in the internal database. This causes trouble with samba, as there is no `user/password` entry in the `tdbsam` file. Just click edit for the user, enter the same or new password, now the user has the linux and samba password synced.
  - A user can log into the web interface to see their own profile information. Depending if the administrator has setup the username account to allow changes, they can change their password and mail account.
  - A non-privileged user can become a web interface administrator by adding them to the `openmediavault-admin` group.
- 

## Import

Designed for bulk user creation. Create a spreadsheet with the corresponding data as described in the import dialog window, save it as CSV (make sure the field separator is semicolon `;`), then just simply:

```
$ cat usersfile.csv
```

Example outputs:

```
# <name>;<uid>;<comment>;<email>;<password>;<shell>;<group,group,...>;  
↪<disallowusermod>  
user1;1001;user1;user1@myserver.com;password1;/bin/bash;sudo;1  
user2;1002;user2;user2@my.com;password2;/bin/sh;;0  
user3;1003;user3;user3@example.com;password3;/bin/false;;1  
user4;1004;user4;user4@test.com;password4;;;1
```

### Note:

- `/etc/shells` will give you a list of valid shells.
  - The last field is a boolean for allowing the user to change their account.
- 

Paste the contents into the import dialog.



## Privileges

The button opens a window that displays all current existing shared folder and their privileges for selected user from the grid. How the privileges are stored is described further down in the *shared folder* section.

## Settings

Option to select a shared folder as root for home folders for new users created in the web interface. Previously existing users created before enabling this setting will not have their home folders moved to this new location. You can manually edit `/etc/passwd` to point them to the new location. Also existing users data in default linux location `/home` has to be moved manually.

## 6.3.2 Group

### Add

Create groups and select the members. You can select current openmediavault users and system accounts. Information is stored in `config.xml` and `/etc/group`.

### Import

Bulk import works in similar as user account import. Just a csv text, delimited with a semicolon `;`. The dialog displays the necessary fields.

### Edit

Just to add or remove members from groups. Default groups created in the web interface have a GID greater than 1000. Same as usernames, groups created in terminal are not stored in the internal database. Just edit, insert a comment and their information should now be stored in `config.xml`.

## 6.3.3 Shared Folder

Shared folder in openmediavault is an internal database object configuration that has been created using the web interface.

### Add

When a shared folder is created using the add button, the window form displays the following options:

- **Name:** The logical name. This can override the path name. Typing a name here will fill the path with the same string.
- **Device:** The parent filesystem associated with the shared folder.
- **Path:** The relative path to the mounted device. To share the whole disk just type `/`.
- **Permissions:** The default descriptive text will create the shared folder with `root:users` ownership and `775` permission mode.

#### Available modes

Logical name	Octal mode
Administrator: read/write, Users: no access, Others: no access	700
Administrator: read/write, Users: read only, Others: no access	750
Administrator: read/write, Users: read/write, Everyone: no access	770
Administrator: read/write, Users: read only, Everyone: read-only	755
Administrator: read/write, Users: read/write, Everyone: read-only	775 (Default)
Everyone: read/write	777

This is how a shared folder looks inside the `config.xml` database:

```
<sharedfolder>
  <uuid>9535a292-11e2-4528-8ae2-e1be17cf1fde</uuid>
  <name>videos</name>
  <comment></comment>
  <mntentref>4adf0892-cf63-466f-a5aa-80a152b8dea6</mntentref>
  <reldirpath>data/videos/</reldirpath>
  <privileges>
    <privilege>
      <type>user</type>
      <name>john</name>
      <perms>7</perms>
    </privilege>
    <privilege>
      <type>user</type>
      <name>mike</name>
      <perms>5</perms>
    </privilege>
  </privileges>
</sharedfolder>
```

Some of the elements explained:

- **uuid**: Internal database reference number.
- **name**: logical name given to the shared folder.
- **mntent**: the associated filesystem reference. The number is in the `uuid` format, the `fstab` section in `config.xml` should contain a `<mntent>` reference with this number.
- **reldirpath**: Path relative to the parent filesystem.
- **privileges**: Users associated with the shared folder and their access level.

When a plugin or a service uses a shared folder it stores the `uuid` value only. Later on using helper scripts or internal openmediavault functions the full path can be obtained just by using the `uuid`. An example in shell:

```
$ . /usr/share/openmediavault/scripts/helper-functions && omv_get_sharedfolder_path_
↪ 9535a292-11e2-4528-8ae2-e1be17cf1fde
```

This returns:

```
$ /srv/dev-disk-by-label-VOLUME1/data_general/videos
```

More information about [helper functions](#).

A shared folder can be used across all over the system backend. Is available to select it in sharing services (FTP, Samba, RSync, etc.) at the same time. Plugins can use them also just by using the shared folder combo class.

**Note:**

- A shared folder belongs to an internal openmediavault database filesystem entry. Is not possible to unmount the filesystem without deleting the folder configuration from the web interface.
  - If a shared folder is being used by a service (FTP, plugins, etc.) is not possible to delete it. Is necessary to disengage the shared folder from the service(s) or section(s) that is holding it before proceeding with removal. This will also prevent to unmount a device from the web interface in the filesystem section if there is still a shared folder associated with it.
  - Due to the design of the software is not possible at the moment to know what section or service is holding which shared folder.
- 

**Edit**

Edit shared folder is possible, but it has some limitations. You can only change the parent device volume. Once the parent device is changed the backend will reconfigure every service that is using a shared folder and stop/start daemons accordingly.

Be aware that changing the parent device volume will not move the data from one filesystem to another.

**Warning: NFS Server:** Editing the parent device will not descent into `/etc/fstab`. Make sure you edit the share in the NFS section so the bind can be remounted.

**Privileges**

Same as in the user section, the window here is relative to the shared folder. It will display for the selected shared folder all the openmediavault users/groups and their corresponding privileges.

As you can see from the code block in the [add section](#) privileges are expressed in the internal database in the same manner as permissions in Linux, simplified using the octal mode: *read/write(7)*, *read-only(5)* and *no access(0)*.

If a privilege is changed, it means a change in the shared folder database section. This database event will trigger a reconfiguration of SMB, FTP and AFP, it will also restart all the above daemons. A plugin using shared folder, but not the privilege information from the database entry should not get reconfigured/restarted if a change occurs just in privileges.

Privileges can be edited from *shared folder* or *users* section. But it is also possible to edit privileges from the shared folder combo selection, just click the  to left side of the drop down menu.

**ACL (Access Control List)**

Provides fine grained permission control besides the standard POSIX permissions. The usage of ACL is not recommended for the average home user. If a server is using an extensive list of users then ACL could suit better<sup>1</sup>.

The expanded ACL window displays three panels. Left one is a browser of the selected shared folder, so you can see the apply ACL to the current folder or a subdirectory and so on.

The left panel displays all current openmediavault users and system accounts and their current ACL of the selected folder. This panel actually reads ACL from the selected folder.

---

<sup>1</sup> <https://help.ubuntu.com/community/FilePermissionsACLs>

<sup>2</sup> <http://vanemery.net/Linux/ACL/linux-acl.html>

The bottom panel displays the standard POSIX permission of the selected folder or subfolders in a user friendly interface.

If you want just to reset linux permissions, just use the recursive checkbox and change options only in the bottom panel, and not selecting any ACL user/group in left panel.

The ACL is applied using `setfacl`<sup>3</sup> and read with `getfacl`<sup>4</sup>.

---

**Note:**

- openmediavault mounts all Linux filesystems with ACL enabled. Only native linux POSIX filesystems support ACL. The button gets disabled for HFS+, NTFS, FAT, etc.
  - ZFS provides ACL support, just need to enable the pool/dataset property.
- 

## 6.4 Services

### 6.4.1 Samba

Samba server comes from Debian software repositories. openmediavault developer does not maintain this package, all bug, hotfixes and features come from Debian. Advanced features like spotlight server or time machine support is not available because they have not reach yet stable Debian or the Debian developers have not made it available in their build.

#### General

The server configures Samba as standalone mode. The default global section

```
[global]
workgroup = HOME
server string = %h server
dns proxy = no
log level = 0
syslog = 0
log file = /var/log/samba/log.%m
max log size = 1000
syslog only = yes
panic action = /usr/share/samba/panic-action %d
encrypt passwords = true
passdb backend = tdbsam
obey pam restrictions = no
unix password sync = no
passwd program = /usr/bin/passwd %u
passwd chat = *Enter\snew\s*\spassword:* %n\n *Retype\snew\s*\spassword:* %n\n
↳*password\supdated\ssuccessfully* .
pam password change = yes
socket options = TCP_NODELAY IPTOS_LOWDELAY
guest account = nobody
load printers = no
disable spoolss = yes
printing = bsd
```

(continues on next page)

---

<sup>3</sup> <https://linux.die.net/man/1/setfacl>

<sup>4</sup> <https://linux.die.net/man/1/getfacl>

(continued from previous page)

```
printcap name = /dev/null
unix extensions = yes
wide links = no
create mask = 0777
directory mask = 0777
use sendfile = yes
aio read size = 16384
aio write size = 16384
null passwords = no
local master = yes
time server = no
wins support = no
```

A default share example:

```
[MyDocuments]
path = /media//dev/disk/by-label/VOLUME1/Documents/
guest ok = no
read only = no
browseable = yes
inherit acls = yes
inherit permissions = no
ea support = no
store dos attributes = no
printable = no
create mask = 0755
force create mode = 0644
directory mask = 0755
force directory mode = 0755
hide dot files = yes
valid users = "john"
invalid users =
read list =
write list = "john"
```

It is possible to add extra options in the general and share configuration page. Options that are managed by openmediavault can be customized via *environmental variables*.

## Privileges

The login access in Samba is configured using privileges. This means they will not act in the file system layer, they will run in the Samba authentication layer. From there the access can be controlled to be read only or read/write access and guest account access. This is done with the PRIVILEGES button in the shared folder section, not the ACL. Privileges only gets login access and from there determines if user can read or write. If write access is enabled but files/folders have restricted permissions then write access is not possible using Samba.

---

**Important:** Samba does not use PAM for login, it has a different password database. When the admin changes a username password (or the user changes their own) using the web interface what openmediavault does is that it changes both the linux login password and the Samba internal database. If a username changes their password using shell, this will not be reflected in Samba log in.

---

## Share types

**Non-public (Private):** *Login always required, Guest Allowed denied*

```
guest ok = no
valid users = User1, User2, @Group1, @Group2   this will deny all none authorized_
↳users
read list = User1, @Group1
write list = User2, @Group2
```

This means that every user will have to provide valid OMV credentials to access that share. Also this type of shares requires at least one definition of a valid user, otherwise the directive would be empty.

---

**Note:** This will allow every user to log into the share.

---

**Semi-public:** *When login is not provided, the guest user is used. This is the “guest allowed” option from the Samba share option*

```
guest ok = yes
read list = User1, @Group1
write list = User2, @Group2
```

Notice here if users are not set up privileges (that means blank tick boxes) anyone will be able to login anyway and have write access.

**Public only:** *The guest user is always used. This is the Guest Only option in the Samba share configuration.*

```
guest ok = yes
guest only = yes
```

With these options valid, read only and write user directives will be ignored when the `/etc/samba/smb.conf` is deployed by openmediavault.

---

**Note:**

- The guest account is mapped to system account nobody, it doesn't belong to group users, thus it has, by default, NO WRITE ACCESS just READ. This can be reverted modifying the POSIX permissions of the share to 777.
  - These directives are NOT ACL.
- 

## Questions

**How do I enter credentials in a semi-public share?** In most cases the user will always be logged as guest. Use Windows map network drive feature to provide other login credentials different from guest. In Mac OS X use CMD+K (if using Finder)

**Why the login keeps saying access denied?**

**This is more likely caused by two things:**

- Permission issue (ACL or non default POSIX permission mode/ownership). Fix the permissions in the shared folder. Samba runs as privileged (root) user, even so if parts of path don't have adequate permissions, it will still respond access denied.
- Out of sync password in between linux and Samba. This is very rare but it has happened. Test in ssh the following `[tt]smbpasswd username[/tt]` enter password and try and login again.

**Why I can't edit files that other users have created?** The default umask in Samba is 644 for files. To enable flexible sharing check *Enable permission inheritance* in the Samba share settings, this will force 664 creation mode. Files created previously need to change their permission mode. Check also that you don't have read only enabled. This option overrides privileges and POSIX.

## 6.4.2 FTP

### Overview

On top of the proftpd debian package, openmediavault uses the vroot module by Castaglia. The server is configured using a DefaultRoot for this folder `/srv/ftp`. Adding folders to the chroot is done by using vroot aliases. This is the default behaviour of the FTP server and cannot be changed. The vroot default path can be changed with environmental variables. The chroot also prevents symlinks from escaping that path, however you can use symlinks that point inside the chroot. So any time you add a shared folder to the FTP, OMV will create first a vroot alias:

```
<IfModule mod_vroot.c>
  VRootAlias "/media/dev-disk-by-label-VOLUME1/videos" "Videos"
</IfModule>
```

Then that alias will have privileges assigned:

```
<Directory /Videos>
  <Limit ALL>
    AllowUser OR omvUser
    DenyAll
  </Limit>
  <Limit READ DIRS>
    AllowUser OR omvUser
    DenyAll
  </Limit>
</Directory>
```

By default you're not allowed to write in there when you login, this means you cannot create folders in the landing directory, you have to enter one of the shared folders. Also due to the nature of the chroot, creating top level folders is pointless since they will be actually stored in `/srv/ftp` and not in the media disks.

### Remote Access

FTP is a protocol intended for use in LAN and WAN. For accessing WAN it is required to forward the server port (default 21) and the passive range to the openmediavault server.

### Anonymous Login

Disabled by default, the anonymous user is mapped to the system user ftp and nogroup. There is no write access for anonymous and this is configured in the `/etc/proftpd/proftpd.conf` file and cannot be changed as is hard coded into the default configuration script of the server. In this case there is no environmental variable to change that behaviour:

```
<Anonymous ~ftp>
  User ftp
  Group nogroup
  UserAlias anonymous ftp
  DirFakeUser on ftp
```

(continues on next page)

(continued from previous page)

```
DirFakeGroup on ftp
RequireValidShell off
<Directory *>
  HideFiles (welcome.msg)
  HideNoAccess on
  <Limit WRITE>
    DenyAll
  </Limit>
</Directory>
</Anonymous>
```

## FTP(S/ES)

openmediavault provides two SSL/TLS modes for encrypting the FTP communication, implicit and explicit FTPS. The differences and features are explained [here](#) and [here](#). Enabling FTP over SSL/TLS requires first that you create or import a certificate in the corresponding section. Once the certificate is there you can choose it from SSL/TLS section in FTP. The default FTPS of the server is explicit, you can click the checkbox to enable implicit. If you choose implicit make sure you forward port 900 in your router to port 21 in your NAS server if you're accessing from WAN, otherwise the client will probably display ECONREFUSED.

## Tips

**Login Group** By default all openmediavault users created in the web interface can log into FTP. You can restrict to read only or read write, there is no deny access, but a user without privileges would not see that folder. If you want to add a layer of extra security for the login, you can create a control group to restrict login to FTP. You first create a group, for example ftp\_users, then at the end of the general extra options of the server we add:

```
<Limit LOGIN>
  DenyGroup !ftp_users
</Limit>
```

Only users members of that particular group will be able to log into the FTP server.

**Home Folders** There is no straightforward way of doing this in the web interface, but if you really need home folders for FTP, you can change the default vroot path with environmental variable `OMV_PROFPTPD_MODAUTH_DEFAULTROOT=~"`. What will happen here is users will log in straight into their home folders. If you add shared folders to the server they will be displayed inside the user home folder plus any other folder present in their home folder.

**LetsEncrypt** Just import your LE certificate in the [General | Certificates | SSL section](#). Then in the TLS/SSL tab, select the imported cert from the dropdown menu. Do not enable implicit ssl. You need also to add the chain file. So in the extra option field text add:

```
TLSCACertificateFile <yourpathtoLE>/etc/letsencrypt/live/<yourdomain>/
chain.pem
```

## 6.4.3 NFS

### Overview

The configuration of the server is done using the common [NFS guidelines](#). Shared folders are actually binded to the /export directory. You can check by examining the `/etc/fstab` file after you have added a folder to the server. All NFS server configured folders are in `/etc/exports` as follows:



```
/export/Shared_1 (fsid=1,rw,subtree_check,secure,root_squash)
/export/Videos 10.10.0.0/24 (fsid=2,rw,subtree_check,secure,root_squash)
/export (ro,fsid=0,root_squash,no_subtree_check,hide)
```

The first two lines are examples, the last line is the NFSv4 pseudo file system.<sup>12</sup>

## Server Shares

The following options are available to configure from the web interface:

- **Shared folder:** Select a folder, the system will add an bind entry to fstab, mount that bind and add it to /etc/exports file
- **Client:** Enter a single ip, host or network CIDR notation. Only one entry is allowed at the moment. You can leave it empty if you do not want network security.
- **Privilege:** This will append read write (rw) or read-only (ro) to /etc/exports.<sup>3</sup>
- **Extra options:** Add options according the [exports manual](#).

The server also shares by default the pseudo root filesystem of /exports as NFSv4.

## Clients

To access NFS shares using any debian derived linux distro:

- Mount as NFSv4 all folders in /export/ in /mnt/nfs:

```
$ mount 172.34.3.12:/ /mnt/nfs
```

- Mount as NFSv3 all folders inside /export in /mnt/nfs:

```
$ mount 172.34.3.12:/export /mnt/nfs
```

- Mount as NFSv3 the folder /export/Videos in /mnt/nfs:

```
$ mount 172.34.3.12:/export/Videos /mnt/nfs
```

- Mount as NFSv4 the folder /export/Videos in /mnt/nfs:

```
$ mount 172.34.3.12:/Videos /mnt/nfs
```

Check your distro on how to proceed with different NFS versions.

## NFSv4 Pseudo filesystem

The default /export folder is shared with this default options `ro,wdelay,root_squash,no_subtree_check,fsid=0` only available to change via environmental variables, so be aware that mounting this path you will encounter permission problems.

<sup>1</sup> [https://help.ubuntu.com/community/NFSv4Howto#NFSv4\\_without\\_Kerberos](https://help.ubuntu.com/community/NFSv4Howto#NFSv4_without_Kerberos)

<sup>2</sup> [https://www.centos.org/docs/5/html/5.1/Deployment\\_Guide/s3-nfs-server-config-exports-nfsv4.html](https://www.centos.org/docs/5/html/5.1/Deployment_Guide/s3-nfs-server-config-exports-nfsv4.html)

<sup>3</sup> This is not standard openmediavault privileges as in the shared folder section

## Permissions

NFS relies on uid/gid matching at the remote/local filesystem and it doesn't provide any authentication/security at all. Basic security is provided by using network allow, and squash options. If you want extra security in NFS, you will need to configure it to use kerberos ticketing system.

## Tips

**Macos/OSX** If you want to mount your NFS exports, add `insecure` in extra options or use `resvport` in the command line.

Example:

```
$ sudo mount -t nfs -o resvport,rw 192.168.3.1:/export/Videos /private/nfs
```

**Debian** Debian distributions (and many others) always include the group users with `gid=100` by default, if you want to resolve permissions easily for all users of a PC using linux add `anongid=100` in extra options. This will force all mounts to use that gid.

**Symlinks** This are not followed outside of their export path, so they have to be relative.

**Remote access** NFS was designed to be used as a local network protocol. Do not expose the NFS server to the Internet. If you still need access use a VPN.

## 6.4.4 SSH

### Overview

Secure shell comes disabled by default in openmediavault, when installing openmediavault on top a Debian installation, the systemd unit will be disabled after the server packages are installed. Just login into web interface to re-enable the ssh service.

The configuration options are minimal, But is possible to:

- Disable the root login
- Disable password authentication
- Enable public key authentication (PKA)
- Enable compression
- Enable tunneling (for SOCKS and port forward)

An extra text field is provided to enter more options. Examine first the file `/etc/ssh/sshd_config` before adding extra options otherwise the option will not be applied. In that case is necessary change the environmental variable.

Normal openmediavault users created in the web interface can access the remote shell by adding them to the ssh group. Using PKA for users requires keys to be added to their profile, this is done in the Users section. The key has to be added in [RFC 4716](#) format. To do that run:

```
$ ssh-keygen -e -f nameofthekey.pub
```

Paste the output in the users profile at Access Right Management | Users | <USERNAME> | Edit | Public Keys.

The number of keys per user is unlimited. A public key in RFC 4716 looks like this:

```

---- BEGIN SSH2 PUBLIC KEY ----
Comment: "iPhone user1"
AAAAB3NzaC1yc2EAAAADAQABAAQDfSQuLx2P6EikkjVxDw0tT8nCW8LHLx/k1
8t37xFAQ5/OoL9m6rVzYy5CFGYt+17DdfWjL0Av7AqaM0ykZVmv2VEM6TmMo56LTlmyZdlz
X5+GEJgCQntDxcIYAVuPXXkPlt1B/uAGzwHdZWpAen+mHgWIi4va8N5QNn4rXpkREcvM1q4
snyAi+gyjAS2Dn4pm8zzrd9qQFnoRYzidbp5e2Rs3brOkwUco0ZkOME2Ff6SpLGaXz4DHH
qgdTqZwHaTXEwm6kDmg1CQrauIPI/ggNqz9mVEspYkskR2PM4CAty8RkZD4MQe5K3EMAFR
aFobBS1hQ3ESCYWNXTS3bF
---- END SSH2 PUBLIC KEY ----

```

The comment string is very important. This will help track down when is necessary to revoke the key in case it gets lost or stolen.

## Admin Tasks

If root login has been disabled and need to perform administrative tasks in the terminal, swap to root by typing:

```
$ su
```

To use sudo for root operations add the user to the sudo group.

The SFTP server comes enabled by default for root and ssh group. So POSIX folder permissions apply to non-root users accessing via SFTP.

---

### Note:

#### Remote WAN access

- Forward in router/firewall a port different than 22. This will minimize bots fingering the ssh server.
  - Always use PKA.
  - Disable password login.
  - Disable root login.
- 

## 6.4.5 RSync

The server can be configured to act as a client to pull and push data to remote locations as well as act an RSync daemon server, where other clients can retrieve or store data from/to the server. In RSync language, the shared folders are called modules. Since openmediavault version 3.0 is possible now to create remote RSync jobs using ssh as transport shell. The RSync is divided in two tabs:

### Jobs (client)

Based on cron, the tasks can be configured to run at certain time or make it repetitive. A few of the options explained:

#### Type

- Local: This will run an RSync in between two internal folders of the server. For example you can use this to move data across different disks in your system
- Remote: This will deactivate destination folder, and instead you'll need to place a destination server address. You can select here:

#### Mode (remote)

- Push: store contents to a remote server
- Pull: Retrieve contents from a remote server

Selecting one or the other will invert the folder as source or destination, the same as the server address.

**Destination/Source Shared Folder** Choose a shared folder where you want the contents to be stored (pull) or you want the contents from that folder to be sent to a remote server (push).

**Destination/Source Server** You need to put address server host or ip.

Examples:

If you are targeting the job against an RSync daemon server:

```
rsync://10.10.10.12/ModuleName
username@10.10.10.12::ModuleName
rsync://username@10.10.10.12:873/ModuleName
```

If you are going to connect to another server just using SSH with public key:

```
username@10.10.0.12:/srv/dev-disk-by-label-VOLUME1/Documents
```

**Warning:** When the RSync task is configured using ssh with PKA, the script that runs the jobs is non-interactive, this means there cannot be neither a passphrase for the private key nor a login password. Make sure your private key is not created with a password (in case is imported). Also make sure the remote server can accept PKA and not enforce password login.

### Authentication (remote)

- **Password:** For the remote RSync daemon module. Is not the username login password defined in the Rights Management section of the server. Read ahead in server tab.
- **Public Key:** Select a key. These are created/imported from General | Certificates | SSH *section*.

These are the options most commonly used in RSync. At the end there is an extra text field where you can add more options.

**Configuration** openmediavault makes the tasks run by placing them in `/etc/cron.d/openmediavault-rsync` one line per job. The cron time at the beginning, then user (root) and the target file that holds the actual RSync file with the final command, is configured in the same way as *scheduled tasks*. The files are stored in `/var/lib/openmediavault/cron.d/`, prefixed with `rsync` and a `<uuid>`. A default SSH RSync job looks like this:

```
#!/bin/sh
# This configuration file is auto-generated.
# WARNING: Do not edit this file, your changes will be lost.
. /usr/share/openmediavault/scripts/helper-functions
cleanup() {
    omv_kill_children $$
    rm -f /var/run/rsync-05260f23-5098-4f07-9250-0b38b923ac7f
    exit
}
[ -e /var/run/rsync-05260f23-5098-4f07-9250-0b38b923ac7f ] && exit 1
if ! omv_is_mounted "/srv/dev-disk-by-label-VOLUME1/" ; then
    omv_error "Source storage device not mounted at </srv/dev-disk-by-label-VOLUME1>!"
    exit 1
fi
```

(continues on next page)

(continued from previous page)

```

trap cleanup 0 1 2 5 15
touch /var/run/rsync-05260f23-5098-4f07-9250-0b38b923ac7f
omv_log "Please wait, syncing </srv/dev-disk-by-label-VOLUME1/backupdir/> to
↳<username@backupserver.com:/opt/backup> ...\\n"
eval $(ssh-agent) >/dev/null
ssh-add /etc/ssh/openmediavault-484a6837-5170-468c-aa8f-0e3cb92a641e >/dev/null
rsync --verbose --log-file="/var/log/rsync.log" --rsh "ssh -p 22" --recursive --times_
↳--archive --perms '/srv/dev-disk-by-label-VOLUME1/backupdir/'
↳'username@backupserver.com:/opt/backup' & wait $!
omv_log "\\nThe synchronisation has completed successfully."

```

## Server

This is the place for configuring the RSync daemon and its modules (shared folders).

**Settings** Change listening port of the daemon and add extra configurations `directives` text field.

**Modules** This is where you add shared folders to be available to the daemon. The options are explained in the module web panel. If you want to protect the modules you can select the next tab and choose a server username and establish a password. Be aware the password is only for the modules, is not the linux password. Documentation for the extra options for the modules is provided by `rsyncd` manual.

The above server settings are sent to this file `/etc/rsyncd.conf`.

## 6.5 Custom Configuration

openmediavault is not a replacement for webmin, where you can configure all options in the web interface. Options are already preconfigured to make it easier for the average user to install and start using the NAS server.

As mentioned before in the [FAQ](#) openmediavault takes full control of some services, making it difficult to intervene configuration files. Changes manually added to configuration files will eventually overwritten at some stage by the openmediavault system.

To overcome this there are some options available to modify some of the default openmediavault configuration options and values, like the use of environmental variables.

### 6.5.1 Environmental Variables

The web interface does not provide access to ALL the configuration aspects of a complex system like openmediavault. However, the system allows to change some advanced settings through the use of environment variables.

#### List environment variables

A list of available environment variables can be collected via:

```
# omv-env list
```

To get a list of all configured environment variables use the following command:

```
# omv-env get
```

To get the value of a specific environment variable use:

```
# omv-env get <VARIABLE_NAME>
```

The list of environmental variables used for `/etc/fstab` filesystem with the defaults options and how to use them is described here.

### Modify environment variables

To set or change these variables, run the following command:

```
# omv-env set <VARIABLE_NAME> <VALUE>
# omv-env set OMV_SSHD_SUBSYSTEM_SFTP "/usr/lib/openssh/sftp-server"
```

The configured environment variables are located in the file `/etc/default/openmediavault`.

### Apply changes

To apply the custom settings you need to execute the following commands as root:

```
# monit restart omv-engined
# omv-salt stage run prepare
# omv-salt stage run deploy
```

## 6.5.2 The SaltStack states

If you want to deploy custom configuration settings, then you could add additional Salt states. Please check out the [SaltStack documentation](#) for more information about how it works and how to use it.

The openmediavault SLS files are located at `/srv/salt/omv/`.

### Add custom states

If you want to customize the configuration of a service or any other application that is managed by openmediavault, then you need to know where to add your custom state file first. Start searching the location on [GitHub](#). You will find the corresponding location below `/src/salt/omv/deploy` in the root file system of your system. If there are no files starting with a number, e.g. `90cron.sls`, then this service is not customizable. It is still possible, but is beyond the scope of this introduction. The states are executed in ascending order.

Choose the order when your state needs to be executed and create a file like `<N>xxxx.sls`, where N is between 0 and 100.

To append something to an already existing configuration file use this YAML:

```
<UNIQUE_IDENTIFIER>:
  file.append:
    - name: "<PATH_OF_THE_FILE>"
    - text: |
      <LINE1>
      <LINE2>
      <...>
```

Example:

```
customize_postfix_main:
  file.append:
    - name: "/etc/postfix/main.cf"
    - text: |
        mynetworks = 127.0.0.0/8 168.100.189.0/28
```

For more file modifications please have a look into the [file module](#).

Finally you need to deploy your changes by running:

```
# omv-salt deploy run <SERVICE_NAME>
```





You can add more features & apps by simply selecting the software you need, we call this plugins. Plugins are possible due to the modular design of openmediavault and are the preferred way to extend your NAS. It is still possible to install regular software or containerized software like Docker. Plugins only exist for your convenience.

### 7.1 Benefits

Compared to adding regular software, plugins offer the following benefits:

- Easier to install - You just click on what you want.
- Easier to configure - it is often preconfigured so you don't have to.
- Automatic updates - ensure Stability & Security.
- A Webinterface - is added when needed for your ease of use.

### 7.2 Overview

The following is the list of official plugins by openmediavault.

- **ClamAV:** Provides Clam AntiVirus (ClamAV). It is a free software, cross-platform and open-source antivirus software toolkit able to detect many types of malicious software, including viruses
- **Diskstats:** Complementary plugin to extend system statistics collection by adding I/O statistic graphs.
- **Forked-daap:** Provides a daap protocol music server.
- **LVM2:** LVM managing. Create volume groups and logical partitions.
- **NUT:** Controlling and configuring UPS. The driver support is based on NUT.
- **Shairport:** Provides Airtunes emulator. Stream music wirelessly to your iPod/iPad/iPhone/iTunes.
- **ShareRootFs:** Provides shared directories on root file system.

- **SNMP**: Provides Simple Network Management Protocol (SNMP). SNMP is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks.
- **TFTP**: Provides Trivial File Transfer Protocol (TFTP). TFTP is a simple lockstep File Transfer Protocol which allows a client to get a file from or put a file onto a remote host.
- **USB Backup**: Backup internal data to external disks on scheduled basis or on plug drive event.

## 7.3 3rd party

An overview of the third party plugin list can be found at [omv-extras.org](http://omv-extras.org).

### Frequently Asked Questions

**What is OMV?** OMV is an abbreviation of openmediavault.

**Is openmediavault a fork of FreeNAS?** No

**Does openmediavault have drivers for my hardware?** All module drivers are provided by the Debian standard kernel of oldstable release 8.9 (aka Jessie). This distribution ships with kernel 3.16 by default. Optionally is possible to install the backport kernel 4.9. If hardware is supported under Debian Jessie then is supported under openmediavault. The Jessie backport kernel 4.9 is the default kernel used by Stretch (Debian 9.3) at the moment, so it provides support for newer hardware.

**Can I use a usb flash drive (stick) for installing the system?** Yes, but the installation does not have any optimizations to reduce writes into the OS disk. The usb media will most likely start failing within a few weeks of usage. Most common symptom is basic command execution does not work, denied login, etc. More information [here](#).

**What are the default credentials for the UI?** Use the user ‘admin’ and the password ‘openmediavault’ for the first login.

**Can I give administrator privileges to non-privileged users to access the web control panel?** Yes. By default non-privileged users can only access their account profile, they can change password and their email address if the administrator has allowed changes on their account. However the current web interface framework is designed for developers to create plugins where they can give limited or full access to non-privileged users. An example is the [openvpn plugin](#) by [omv-extras.org](#). A non-privileged user can become a web interface administrator by adding them to the `openmediavault-admin` group.

**What is the file `/etc/openmediavault/config.xml` for?** It is the database configuration store file for openmediavault. When a change is performed in the web interface, the config value is stored and/or retrieved by RPC to/from this file.

**Can I upgrade to Debian Testing/Unstable (Debian Testing/Sid) or use Ubuntu as a base distribution?** Yes. But the end is most likely a broken web interface and possibly broken system. openmediavault releases are heavily tight to their Debian base distribution.

**I’ve lost the web interface password. How do I reset it?** Simply connect via ssh into the server or login locally on the machine and type in: `omv-firstaid`. There is an option to reset the web interface password.

**Can I backup or restore an existing openmediavault configuration?** There is no regular backup/restore procedure, but yes, in some way: keep the file `/etc/openmediavault/config.xml` for references purposes if the option is to go for a clean re-install.

**What is the default HTTP engine of openmediavault?** NGINX. The last version of openmediavault with Apache was 0.5 Sardoukar.

**Can I use Apache as HTTP engine?** Yes, but is not supported. Eventually every openmediavault package upgrade will activate NGINX again leaving the web interface broken. A parallel Apache instance next to Nginx is possible, just make sure the ports are different otherwise the openmediavault web interface will not work.

**How can use the default HTTP engine to hold my own web page?** Do not modify openmediavault default NGINX files. Place the website configurations in `/etc/nginx/sites-available` and enable it with `nginx_ensite <SITE>`. Read more information in the [NGINX documentation](#).

**Why does the system rewrites a configuration file(s) that I have manually edited?** OMV takes full control of some system services. This services include `monit`, `ntp`, `samba`, `network`, `proftpd`, `nginx`, `php5-fpm`, etc. Read [here](#).

**How can I modify an internal value of some service openmediavault has control over?** Read [here](#) for advanced configurations.

**How can I modify or add a network configuration with some custom options the web interface does not provide?** Starting with openmediavault 5 `systemd-networkd` is used to configure the network. The interfaces file `/etc/network/interfaces` is controlled by openmediavault but not used anymore. To add network interfaces that are not configurable through the web interface or other options not present, use [advanced settings](#). Alternatively write your own `systemd-networkd` configuration files.

**Why my disks mount paths have a long alphanumeric number?** The long number is called UUID, it is used by `fstab` to mount disks. This number is unique per filesystem (or at least unlikely possible that another filesystem comes with an identical one). This helps maintaining the mount points. The old linux way (`sda1`, `sdb1`, etc.) is not guaranteed that `/dev/sda1` is the same disk on next reboot. If having trouble identifying them in terminal, create a pool with symlinks to each file system with easy to remember names.

This behaviour has been deprecated now in current openmediavault releases including stable (Jessie). The default creation of mount paths is documented [here](#).

**I don't have a data disk, and I want to use my OS disk for storing data?** The default behaviour of openmediavault is to act as NAS server, that means OS files are separated from data disks.

However if the OS disk is partitioned the system will recognise the extra partitions besides rootfs if is formatted. You can mount it and use it for shared folders.

The current installer does not provide access to the partition manager, use a plain Debian iso then install openmediavault on top and accommodate the partitions, or resize the partition after installing using `Gparted` or `SystemRescueCd`.

**Can I install openmediavault on top a running Debian system?** Yes, but it is recommended that the current running OS not to have a desktop environment installed.

**What is the permissions/ownership of folders in openmediavault created by shared folders?** The default is folders in `2775` mode, with `root:users` ownership. This means all users created in the web interface can read, write to folders created by the system in the data drives using the default. The `setgid` allows group inheritance, meaning new files/folders below will always have the group users (`GID=100`) membership.

**I need to delete a shared folder, why the delete button is greyed/disabled?** Shared folder configurations can be used across different services. When removing a shared folder configuration is necessary to unlink it from every service is attached to, before the delete button becomes available. At the moment there is no internal database backend that can display information about which service is holding which shares.

**What is the `omv-salt` command for?** `omv-salt` is a terminal console command that is used by the backend of openmediavault to pipe directives and values to service configuration files. The arguments that `omv-salt` accepts are related to the name of the service it configures. Type `omv-salt` in terminal, press TAB key, and the terminal will display all available arguments.

**I want to experiment with openmediavault or make changes to the code** As a true open source system everything is possible. The recommendation is do not test with the production server to avoid breaking the web interface. The best thing to do is to use a Virtual Machine. On [Sourceforge](#) there are preconfigured openmediavault images with virtual disks ready to launch. Alternatively checkout the openmediavault [GIT repository](#) and use [Vagrant](#) to create a virtual machine.

**What is the `omv-update` and `omv-release-upgrade` for?** Information about those commands are in the software section.



- **The web interface has missing fields and/or items showing that have been uninstalled.**

Clear your browser cache.

- **The web interface keeps rejecting my admin/user password.**

If the password is correct then this is most likely caused by the rootfs partition being full. This command can help track which folders are the biggest `df -hx --max-depth=1 /`

- **I have problem accessing the web interface with Firefox.**

Try the solution mentioned in the [Sencha ExtJS forum](#) or the [Mozilla bugtracker](#).

- **I only see a few items in the web interface interface like the user section of Access Rights Management.**

You did not login as the admin user. This is the only user that can access everything.

- **I get an error every time I post in the forum especially if it is a long post and/or has links to external pages.**

The error is deceiving. Please don't keep trying to post. The spam filter has flagged your post and it will need to be approved. Please be patient.

- **I mounted the drive using the command line or GUI tool and I can't pick that drive in the shared folder device dropdown.**

Never mount a drive with anything other than the openmediavault web interface. This creates the necessary database entries to populate the device dropdown.

- **Samba is slow.**

Read these threads

- [read/write performance for SMB shares hosted on RPi4](#)
- [Tuning Samba for more speed \(note: written for OMV 2.x\)](#)
- [Tuning Samba for more speed 2 \(note: written for OMV 2.x\)](#)

- **Samba share password is refused from Windows 10.**

To fix the problem you need to change the [Network Security LAN Manager authentication level](#).

- **How to troubleshoot an error caused by an “Option” parameter passed to a plug-in**

To find the root cause, run the faulty systemd unit file yourself by executing: `# systemd restart <plug-in-daemon>`

If output of `<plug-in>` is now more verbose, then you will get a hint on STDOUT. If not, then you need to run `journalctl -f` in parallel to get the syslog output. Admittedly, not really novice friendly, but it’s really not possible to do it any other way. OMV always tries to be as error/debug friendly as possible; by default.

- **I am using JMicron drive enclosures and some of my drives are not appearing.**

This is likely because JMicron controllers incorrectly report identical serial numbers and other data which confuses various systems. openmediavault provides an [UDEV rules database](#) which will fix that issue for several USB PATA/SATA bridge controllers. If your hardware still does not work, then please provide the information mentioned in that pull request and open a new tracker issue.

Alternatively you can manually “fix” this by adding a rule to `/lib/udev/rules.d/60-persistent-storage.rules` after the entry for “Fall back usb\_id for USB devices”:

```
# JMicron drive fix
KERNEL=="sd*", ENV{ID_VENDOR}=="JMicron", SUBSYSTEMS=="usb", PROGRAM=
↳"serial_id %N", ENV{ID_SERIAL}="USB-%c", ENV{ID_SERIAL_SHORT}="%c"
```

This will ensure that unique paths are created based on the serial number of the actual drives and not the enclosures.



## 10.1 Coding Guideline

These standards for code formatting and documentation must be followed by anyone contributing to the openmediavault project. Any contributions that do not fulfill these guidelines will not be accepted.

### 10.1.1 File Formatting

**Indentation** Use 4 space tabs for writing your code. If you are modifying someone else's code, try to keep the coding style similar.

**Line Length** Lines shouldn't be longer than 80 characters.

**Line Endings** Line endings should be Unix-style LF.

**Encoding** Files should be saved with UTF-8 encoding.

### 10.1.2 Naming Conventions

**Classes** PHP classes should use the OMV namespace.

```
namespace OMV\System;

/**
 * @ingroup api
 */
class Process {
    use \OMV\DebugTrait;
    ...
}
```

**Functions/Methods** Functions/Methods must use camel case syntax, this convention capitalizes the first character of each word except the first one.

```
public function getGecos() {
...
}

public function getHomeDirectory() {
...
}
```

**Variables** Variables must use camel case syntax, this convention capitalizes the first character of each word except the first one.

```
$fsName
$outputFileName
```

**Constants** Constants should start with OMV\_ and should be all upper case.

```
$OMV_DEFAULT_FILE = "/etc/default/openmediavault";
$OMV_JSONSCHEMA_SORTFIELD = '"type":["string","null"]';
```

### 10.1.3 Multiline parameters

Functions with many parameters may need to be split onto several lines to keep the 80 characters/line limit. The first parameters may be put onto the same line as the function name if there is enough space. Subsequent parameters on following lines are to be indented using 1 tab.

```
throw new OMVException(OMVErrorMsg::E_EXEC_FAILED,
    $cmd, implode("\n", $output));

$dispatcher->notify(($data['uuid'] == $GLOBALS['OMV_UUID_UNDEFINED']) ?
    OMV_NOTIFY_CREATE : OMV_NOTIFY_MODIFY,
    "org.openmediavault.system.storage.hdparm", $object);
```

### 10.1.4 Control Structures

```
for (i = 0; i < 10; i++) {
    if (foo(i)) {
        bar();
    }
}

switch (x) {
case 'a':
    ...
    break;
case "b":
    ...
    break;
default:
    ...
    break;
}

if (a) {
```

(continues on next page)

(continued from previous page)

```

    foo();
} else {
    bar();
}

if (TRUE === $result)
    break;

foreach ($output as $outputk => $outputv) {
    foo();
}

```

## 10.1.5 Comments

**Single line comments** You should use the `//` comment style to “comment out” code. It may be used for commenting sections of code too. Single line comments must be indented to the indent level when they are used for code documentation.

**Block comments** Block comments should usually be avoided. For descriptions use the `//` comments.

```

// Parse output:
// shadow:x:42:openmediavault
// snmp:x:112:
// sambashare:x:113:
// openmediavault:x:999:
// nut:x:114:
foreach ($output as $outputv) {
    ...
}

```

**Documentation comments** Use the `doxygen` syntax where possible.

```

/**
 * Get the filesystem label.
 * @return string The filesystem label, otherwise FALSE.
 */
public function getLabel() {
    ...
}

/**
 * Enumerate all disk devices on the system.
 * @return array An array containing physical disk device objects with
 * the fields \em devicename, \em devicefile, \em model, \em size,
 * \em description, \em vendor, \em serialnumber, \em israid and
 * \em isrootdevice.
 */
public function enumerateDevices() {
    ...
}

/**
 * Enumerate all disk devices on the system. The field \em hdparm will
 * be added to the hard disk objects if there exists additional hard
 * disk parameters (e.g. S.M.A.R.T. or AAM) that can be defined

```

(continues on next page)

(continued from previous page)

```
* individually per hard disk.
* @param array data An array containing the following fields:
*   \em start The index where to start.
*   \em limit The number of objects to process.
*   \em sortfield The name of the column used to sort.
*   \em sortdir The sort direction, ASC or DESC.
* @return array An array containing the requested objects. The field
*   \em total contains the total number of objects, \em data contains
*   the object array. An exception will be thrown in case of an error.
*/
public function getList($data) {
    ...
}
```

## 10.2 Contribute

If you want to contribute to the openmediavault project you have to subscribe a [Contributor License Agreement](#).

Note that the CLA is not a transfer of copyright ownership, this simply is a license agreement for contributions. You also do not change your rights to use your own contributions for any other purpose.

### 10.2.1 Why do i have to subscribe a CLA when contributing to the openmediavault project?

- <http://oss-watch.ac.uk/resources/cla>
- <http://www.golem.de/1107/85208.html>
- [Rechtliche Sicherheit bei Open-Source-Beiträgen](#)
- [Django's CLA FAQ](#)
- [Karl Fogel's Producing Open Source Software on CLAs](#)
- [The Wikipedia article on CLAs](#)
- [Gemeinsame Durchsetzung der Rechte](#)

### 10.2.2 Can I submit patches without having signed the CLA?

No. All contributors and patch submitters must sign the CLA before they submit anything substantial. Trivial patches like spelling fixes or missing words won't require an agreement, since anybody could do those. However, almost anything will require a CLA.

### 10.2.3 Contribution rules

Code contributions must satisfy the following conditions. Contributions that do not fulfill these conditions will not be accepted.

- The *coding guidelines* must be followed.
- The feature/improvement must be implemented as generic as possible.
- The code/feature/improvement must not affect existing functionality.

- Each commit message in a [GitHub pull request](#) must be signed via Signed-off-by: Frank Mustermann <frank.mustermann@xxx.yyy>.
- If the PR fixes a [GitHub issue](#), then the line Fixes: [https://github.com/openmediavault/openmediavault/issues/<ISSUE\\_NR>](https://github.com/openmediavault/openmediavault/issues/<ISSUE_NR>) must be included.
- You have to sign the CLA online via GitHub.
- Make sure your PR has only one commit.

### 10.2.4 How to become a translator?

If you want to help translating the openmediavault web interface please do the following:

- Subscribe the [CLA](#) and send it to the given email address.
- Create an account at Transifex and join the openmediavault project as translator.
- You will get notified when your request has been approved. You will be listed as contributor here.

## 10.3 How it works

openmediavault is a complex piece of software. Developers can easily understand how it works by looking at the source code and developing plugins. For the average user it is a little bit more complicated. Some of the mechanics on how it works are explained ahead.

**Essential elements: Frontend** The web interface, is written in JavaScript using the ExtJS Sencha framework. The page is delivered using the nginx web server.

**Backend** PHP code, executes several tasks.

**config.xml** Database file in XML format, located in `/etc/openmediavault` We will refer in this explanation just as config.xml

**omv-salt** Tool to *deploy* the configuration and services.

**omv-engined** RPC daemon that runs all the PHP backend code. The nginx web server connects to this daemon through the FastCGI PHP socket. If an error appears in the web interface that indicates no connection to the PHP socket means the daemon is not running.

**Listeners** PHP backend code that listens to changes in the database. They are located in the modules section of the code `/usr/share/openmediavault/engined/modules`.

**/var/lib/openmediavault/dirtymodules.json** File that enumerates all sections that need to be reconfigured after the database has been written.

### 10.3.1 web interface values to/from the database

#### Read

When a user clicks on a panel, the JavaScript code retrieves values from config.xml using a RPC call. The RPC call has two main components usually the service name of the section (is in the js code) and the method. Press F12 in your favorite browser to open the developer console and go to Samba section in the web interface. In the browsers developer tools network section you will see several rpc.php calls. Find the one related to Samba, right click and select copy as cURL.

This is the json payload sent to omv-engined:

```
{
  "service": "SMB",
  "method": "getSettings",
  "params": null,
  "options": null
}
```

and the response:

```
{
  "response": {
    "enable": true,
    "workgroup": "HOME",
    "serverstring": "%h server",
    "loglevel": 0,
    "usesendfile": true,
    "aio": true,
    "nullpasswords": false,
    "localmaster": false,
    "timeserver": false,
    "winssupport": false,
    "winsserver": "",
    "homesenable": false,
    "homesbrowseable": true,
    "extraoptions": ""
  },
  "error": null
}
```

Just after the one before, another call, this time to get the Samba share list:

```
{
  "service": "SMB",
  "method": "getShareList",
  "params": {
    "start": 0,
    "limit": 25,
    "sortfield": "sharedfoldername",
    "sortdir": "ASC"
  },
  "options": null
}
```

And the response:

```
{
  "response": {
    "total": 1,
    "data": [
      {
        "uuid": "9e4c8405-b01c-40b6-8c46-af6be17a1ff6",
        "enable": true,
        "sharedfolderref": "7ee2e4d0-8173-442b-88b9-63b4c731f920",
        "comment": "",
        "guest": "no",
        "readonly": true,
        "browseable": true,

```

(continues on next page)

(continued from previous page)

```

        "recyclebin":false,
        "recyclemaxsize":0,
        "recyclemaxage":0,
        "hidedotfiles":true,
        "inheritacls":true,
        "inheritpermissions":false,
        "easupport":false,
        "storedosattributes":false,
        "hostsallow":"","
        "hostsdeny":"","
        "audit":false,
        "extraoptions":"","
        "sharedfoldername":"sfl"
    }
}
},
"error":null
}

```

## Write

A user can do a simple task as to create a shared folder or change some settings in a service section. Whenever the user hits the save button, all fields from the section are submitted from the frontend via RPC to the internal database in `config.xml`, even the ones that are not changed. This is similar on what happens when reading values however the method here is named differently when saving: `setSettings`.

Stopping here, examining `config.xml` in terminal will see all the new stored values, what follows is that usually a yellow notification bar will appear in the web interface to indicate that it is necessary to apply changes. The yellow notification bar happens for one reason only: the `dirtymodules.json` file.

So the save button does two things actually, sends information to `config.xml` and what is called mark the relevant module as dirty. As an example: Making a change in general Samba or its shares will create a `dirtymodules.json` file like this:

```

[
  "samba",
  "zeroconf"
]

```

## Reconfiguring services

When the apply button is pressed, this very long PHP function gets executed.

In the following order, this will happen in background:

**omv-salt deploy run samba** -> `/etc/samba/smb.conf` will be completely rewritten -> Samba daemon is restarted

**omv-salt deploy run zeroconf** -> All files at `/etc/avahi/services/ftp, smb, web, ssh, nfs.` service will be rewritten -> Avahi daemon is restarted

That PHP function also performs checks for dependencies, in case a configuration needs to be reconfigured or reloaded before/after another one.

**Why is Zeroconf marked dirty?** Because the Samba openmediavault code indicates that whenever a change is performed in this section, Zeroconf must be marked dirty. This is by design, Avahi is configured to announce Samba

server if is enabled, so needs to know if openmediavault Samba server is enabled or disabled. If the database shows it is disabled the Avahi service file will be removed. The module backend is something all plugins can use. For example, a plugin that wants to use the privilege database model will have to listen to any changes in the shared folder database so it can reconfigure its files accordingly.

**What can break the web interface?** As explained, the web interface depends on several third party software components.

1 - Nginx HTTP engine. The web server software is very sensitive to any syntax mistakes in `sites-available` folder. Any files there that do not pass syntax check will result in a fail to restart/reload nginx daemon. Also editing the `openmediavault-webui` nginx file improperly will result in failure. Nothing will be displayed by the browser, it will just say “Connection refused”, as there is no software running on the HTTP port.

2 - `omv-engined` not running. Whenever the RPC daemon is not running, an error will pop in web interface “Failed to connect to socket: No such file or directory”.

3 - The `php-fpm` socket is not running. Uncommon error, but if fiddling around with the PHP socket configuration or `systemd` to make it not start the web interface will display “502 Bad gateway”.

All of the above errors should be able to be corrected with `omv-firstaid`. Offending files in `sites-available` should be removed from there to start the nginx server.

---

**Note:** As noticed how openmediavault works, the software does not parse configuration files. Any changes users add manually to `smb.conf` or any other configuration file will not be reflected in the web interface. This is why some hardcoded values are suggested to be customized via environmental variables. It can happen that a plugin marks Samba as dirty by design then the apply button will rewrite everything and restart it also.

---

Not every component in openmediavault is executed in the way described above. For example the filesystem backend has a much more complex mechanism.

## 10.4 Internal Tools

openmediavault software comes with several command line tools that can be used by developers and/or advanced users. Also it can be used to gather support information.

### 10.4.1 `omv-salt`

This tool is used to deploy the configuration of services and to start or stop them.

To get a list of all available deployment states:

```
# omv-salt deploy list
```

To deploy one or more states run the following command:

```
# omv-salt deploy run <NAMES>...
# omv-salt deploy run avahi monit systemd
```

The tool also supports stages that bundle various tasks. To get a list of them, run the command:

```
# omv-salt stage list
```

The following stages are available:



- **setup** This stage is being run only once after the openmediavault Debian package has been installed on the system. It is used to set up the system to the desired requirements.
- **prepare** This stage takes care that the pillar and grains are up to date and all modules/states are being synced to the minions.
- **deploy** Deploy the configuration of various services like SMB, FTP, ...
- **all** This stage contains the stages prepare and deploy.

If you want to deploy all states in one bunch, then you need to execute the following command:

```
# omv-salt stage run deploy
```

## 10.4.2 omv-confdbadm

Most users tend to access/modify the database by using nano:

```
$ nano /etc/openmediavault/config.xml
```

This is a problem as sometimes a wrong pressed key can add strange chars out of the xml tags and make the database unreadable by the backend.

**omv-confdbadm** is a tool written in python for retrieving, storing or deleting values from/to the database. This tool combined with **jq**<sup>1</sup> provides an easier method for interacting with the database using Shell/BASH.

To read values in the database the tool needs as last argument the datamodel path. You can find all data models path here `/usr/share/openmediavault/datamodels/` prefixed with `conf`. Or list them with **omv-confdbadm list-ids**

Lets read all the registered filesystems that have been mounted through the web interface. Type the following command as root:

```
# omv-confdbadm read --prettify conf.system.filesystem.mountpoint
```

Output returns:

```
[
  {
    "dir": "/srv/dev-disk-by-label-ironwolf_3TB_1",
    "freq": 0,
    "fsname": "/dev/disk/by-label/ironwolf_3TB_1",
    "hidden": false,
    "opts": "defaults,noauto,user_xattr,usrjquota=aquota.user,grpjquota=aquota.
↪group,jqfmt=vfsv0,acl",
    "passno": 2,
    "type": "ext4",
    "uuid": "567c2bd4-3d82-45b2-b34b-a6d38e680ed3"
  },
  {
    "dir": "/media/a448c5e9-7a50-4d48-b73d-48cadbe0326e",
    "freq": 0,
    "fsname": "a448c5e9-7a50-4d48-b73d-48cadbe0326e",
    "hidden": true,
    "opts": "noauto,",
    "passno": 0,
  }
]
```

(continues on next page)

<sup>1</sup> <https://stedolan.github.io/jq/manual/v1.5/>

(continued from previous page)

```

    "type": "fuse.mergerfs",
    "uuid": "4adf0892-cf63-466f-a5aa-80a152b8dea6"
  },
  {
    "dir": "/export/videos",
    "freq": 0,
    "fsname": "/media/a448c5e9-7a50-4d48-b73d-48cadbe0326e/data_general/videos",
    "hidden": false,
    "opts": "bind,noauto",
    "passno": 0,
    "type": "none",
    "uuid": "4457831c-309e-4693-8b0d-5db6b257194d"
  },
  {
    "dir": "/export/PVR",
    "freq": 0,
    "fsname": "/media/a448c5e9-7a50-4d48-b73d-48cadbe0326e/data_general/videos/pvr
↪",
    "hidden": false,
    "opts": "bind,noauto",
    "passno": 0,
    "type": "none",
    "uuid": "dce89b85-f1e1-42e2-8d46-986de599abff"
  },
]

```

The first one is a native ext4 filesystem, the second object is storage pool, the last two are NFS binds.

**Filtering:** Get all filesystem mountpoints:

```
# ovmv-confdbadm read conf.system.filesystem.mountpoint | jq -r '[]|.dir'
```

Output returns:

```
/media/dev-disk-by-label-ironwolf_3TB_1
/media/a448c5e9-7a50-4d48-b73d-48cadbe0326e
/export/videos
/export/PVR
```

**Selecting:** Get all filesystem objects that are registered as ext4:

```
# ovmv-confdbadm read conf.system.filesystem.mountpoint | jq -r '[]|select(.type==
↪"ext4")'
```

Output returns:

```

{
  "opts": "defaults,noauto,user_xattr,usrjquota=aquota.user,grpquota=aquota.group,
↪jqfmt=vfsv0,acl",
  "uuid": "567c2bd4-3d82-45b2-b34b-a6d38e680ed3",
  "passno": 2,
  "dir": "/media/dev-disk-by-label-ironwolf_3TB_1",
  "fsname": "/dev/disk/by-label/ironwolf_3TB_1",
  "freq": 0,
  "hidden": false,

```

(continues on next page)

(continued from previous page)

```
"type": "ext4"
}
```

**Write:** This tool can also modify values in the database.

Add the `noexec` flag to this filesystem object `567c2bd4-3d82-45b2-b34b-a6d38e680ed3`, we need to pass the whole json object as argument:

```
# omv-confdbadm update conf.system.filesystem.mountpoint '{"freq":0,"hidden":false,
↪ "passno":2,"opts":"defaults,noexec,noauto,user_xattr,usrjquota=aquota.user,
↪ grpjquota=aquota.group,jqfmt=vfsv0,acl","dir":"/media/dev-disk-by-label-ironwolf_
↪ 3TB_1","uuid":"567c2bd4-3d82-45b2-b34b-a6d38e680ed3","fsname":"/dev/disk/by-label/
↪ ironwolf_3TB_1","type":"ext4"}'
```

Remove a filesystem from the database, this time we pass only the corresponding uuid of the object:

```
# omv-confdbadm delete --uuid 567c2bd4-3d82-45b2-b34b-a6d38e680ed3 conf.system.
↪ filesystem.mountpoint
```

### 10.4.3 omv-rpc

This tool can execute RPC commands. This is identical of what the web frontend uses to set/get information. It accepts service, method and parameters. RPC services can be found listed in `engined/rpc` folder

**Example 1:** Get all mounted filesystems, including rootfs:

```
# omv-rpc -u admin 'FileSystemMgmt' 'enumerateMountedFilesystems' '{"includeroot":_
↪ true}'
```

Output returns:

```
[
{
  "devicefile": "/dev/sda1",
  "parentdevicefile": "/dev/sda",
  "uuid": "752dee88-11a3-4524-848e-d50baf0211a2",
  "label": "",
  "type": "ext4",
  "blocks": "9738548",
  "mountpoint": "/",
  "used": "5.44 GiB",
  "available": "3595554816",
  "size": "9972273152",
  "percentage": 62,
  "description": "/dev/sda1 (3.34 GiB available)",
  "propposixacl": true,
  "propquota": true,
  "propresize": true,
  "propfstab": true,
  "propcompress": false,
  "propautodefrag": false,
  "hasmultipledevices": false,
  "devicefiles": [
    "/dev/sda1"
  ]
}
```

(continues on next page)

(continued from previous page)

```

},
{
  "devicefile": "dfa",
  "parentdevicefile": null,
  "uuid": null,
  "label": "dfa",
  "type": "zfs",
  "blocks": 901386.24,
  "mountpoint": "/dfa",
  "used": "5.26 MiB",
  "available": 917504000,
  "size": 923019509.76,
  "percentage": 0,
  "description": "dfa (875.00 MiB available)",
  "proposixacl": true,
  "propquota": false,
  "propresize": false,
  "propfstab": false,
  "propcompress": false,
  "propautodefrag": false,
  "hasmultipledevices": false,
  "devicefiles": "dfa"
},
{
  "devicefile": "/dev/sdg1",
  "parentdevicefile": "/dev/sdg",
  "uuid": "b50987a4-f111-4e94-a52e-9e6b204ac227",
  "label": "vol3",
  "type": "ext4",
  "blocks": "2030396",
  "mountpoint": "/srv/dev-disk-by-label-vol3",
  "used": "6.01 MiB",
  "available": "2056044544",
  "size": "2079125504",
  "percentage": 1,
  "description": "vol3 (1.91 GiB available)",
  "proposixacl": true,
  "propquota": true,
  "propresize": true,
  "propfstab": true,
  "propcompress": false,
  "propautodefrag": false,
  "hasmultipledevices": false,
  "devicefiles": [
    "/dev/sdg1"
  ]
}
]

```

**Example 2:** Get all block devices with no filesystem signatures. This is used by the RAID creation window:

```
# omv-rpc -u admin 'RaidMgmt' 'getCandidates' | jq
```

Output returns:

```
[
{
```

(continues on next page)

(continued from previous page)

```

    "devicefile": "/dev/mapper/vg-lv1",
    "size": "1296039936",
    "vendor": "",
    "serialnumber": "",
    "description": "LVM logical volume lv1 [/dev/mapper/vg-lv1, 1.20 GiB]"
  },
  {
    "devicefile": "/dev/mapper/vg-lv1",
    "size": "1296039936",
    "vendor": "",
    "serialnumber": "",
    "description": "LVM logical volume lv1 [/dev/mapper/vg-lv1, 1.20 GiB]"
  },
  {
    "devicefile": "/dev/sde",
    "size": "1610612736",
    "vendor": "QEMU",
    "serialnumber": "drive-scsi5",
    "description": "QEMU HARDDISK [/dev/sde, 1.50 GiB]"
  },
  {
    "devicefile": "/dev/sdf",
    "size": "2147483648",
    "vendor": "QEMU",
    "serialnumber": "drive-scsi4",
    "description": "QEMU HARDDISK [/dev/sdf, 2.00 GiB]"
  },
  {
    "devicefile": "/dev/sdj",
    "size": "1073741824",
    "vendor": "ATA",
    "serialnumber": "QM00009",
    "description": "QEMU HARDDISK [/dev/sdj, 1.00 GiB]"
  }
]

```

The `jq` tool is used to prettify the output in JSON.

#### 10.4.4 Shell helper-functions

openmediavault ships with this file `/usr/share/openmediavault/scripts/helper-functions` that contains several POSIX shell functions. To test them just run in terminal:

```
$ source /usr/share/openmediavault/scripts/helper-functions
```

Type `omv_`, press tab key to autocomplete, this will show all functions and a small description in the name.

**Example 1:** Shared folders objects in the database do not have their complete absolute path, it has to be constructed from the relative directory and the parent filesystem. If we know the shared folder database object `<uuid>` then:

```
$ omv_get_sharedfolder_path 2a8b04de-4e6c-4675-b761-1ddfabbde2d2a
```

Returns:

```
/media/dev-disk-by-label-VOLUME1/Videos/Unsorted
```

**Example 2:** Database nodes need to be created when a plugin is installed and removed when it is purged. This is from omv-extras MiniDLNA plugin postinst file

```
omv_config_add_node "/config/services" "${SERVICE_XPATH_NAME}"
omv_config_add_key "${SERVICE_XPATH}" "enable" "0"
omv_config_add_key "${SERVICE_XPATH}" "name" "MiniDLNA Server on OpenMediaVault"
omv_config_add_key "${SERVICE_XPATH}" "port" "8200"
omv_config_add_key "${SERVICE_XPATH}" "strict" "0"
omv_config_add_key "${SERVICE_XPATH}" "tivo" "0"
omv_config_add_key "${SERVICE_XPATH}" "rootcontainer" "."
omv_config_add_node "${SERVICE_XPATH}" "shares"
omv_config_add_key "${SERVICE_XPATH}" "loglevel" "error"
omv_config_add_key "${SERVICE_XPATH}" "extraoptions" ""
```

Notice in the postinst file how it sources at the beginning helper-functions.

---

**Note:** What each function do and the parameters it accepts is documented in the [helper-functions file](#) .

---

At present there are many ways of getting support, many of them are done by the community. The current support channels are:

**Code**

<https://scm.openmediavault.org/>

**Bugtracker**

<http://bugtracker.openmediavault.org/>

**Forum**

<https://forum.openmediavault.org/>

**IRC**

We have a support IRC channel at freenode servers, just type `/join #openmediavault` in your favourite IRC client, type your question and wait for someone available to help you.

**Facebook**

<https://www.facebook.com/openmediavault/>

**Twitter**

<https://twitter.com/OpenMediaVault/>

**Discord**

Since last year there is also a discord group. You can get access by clicking [here](#).

---

**Note:** Make sure you provide as much information as you can when posting in the forum or bugtracker and describing your problem. If you have an error in the web interface make sure you take screenshots of the backtrace, to identify properly what's failing.

---





---

### Press releases, reviews and external references

---

- Dec 2008, FreeNAS: BSD Line and Linux Fork [Linux magazine](#)
- October 2011 “First version of the NAS distribution openmediavault” [pro-linux.de](#) (German)
- September 2014, “Community Choice” Project of the Month – openmediavault [Sourceforge](#)
- April 2015, Interview openmediavault developer Volker Theile [Canox](#)
- August 2015 LinuxVoice Magazine issue #9, Distrohopper [LinuxVoice Magazine](#)
- November 2014, openmediavault Open source network attached storage for Debian/GNU Linux [ODROID Magazine](#)
- January 2014 “How to build your own NAS box” [APC Magazine Australia](#)
- August 2015 “The open-source NAs distro for media lovers” [ACP Magazine Australia](#)
- Distribution Release: openmediavault 2.1 [Distrowatch](#)
- September 2014, openmediavault 1.0 review [Linuxbsdos.com](#)



# CHAPTER 13

---

## Contributors

---

### **Founder and project manager**

Volker Theile

### **Forum**

- area3o
- Cpoc
- davidh2k
- Dennis
- donh
- i814u2
- jensk
- jhmiller
- KM0201
- knumsi
- PhantomSens
- ryecoaron
- SerErris
- Solo0815
- spyalelo
- subzeroin
- SVS
- tekkbebe
- WastlJ

- The Master

### Documentation

- area3o
- Davidh2k
- GreenBean
- i814u2
- Reddy
- witopi
- subzero79

### Testing

- Falk Menzel

### Translators

- Alexandr aka azlk (Russian)
- Andrey Chapalda (Ukrainian)
- Antonio Pelaez Redondo (Spanish)
- Babchuk Volodymyr Romanovych (Ukrainian)
- Balajti Ádám (Hungarian)
- Bocquet Stéphane (French)
- Cyryl Sochacki (Polish)
- Gábor Majoros (Hungarian)
- Harry Stoker (Dutch)
- Helge Philipp (German)
- Henrik Sandström (Swedish)
- Jacek Niedziółka (Polish)
- Jakub Górny (Polish)
- Jonathan Weber (German)
- José Manuel Caínzos Sánchez (Spanish)
- Kochin Chang (Chinese (Taiwan))
- Kostas Gounaris (Greek)
- Marcel Beck (German)
- Mario Varelli (Italian)
- Mathias Grünwald (German)
- Mauro Rulli (Italian)
- Miguel Anxo Bouzada (Galician)
- Milan Toet (Dutch)
- Ming Song (Chinese)

- Nahir Mohamed (French)
- Nelson Rosado (Portuguese)
- Paolo Velati (Italian)
- Raul Fernandez Garcia (Spanish)
- Rune Bystrøm (Norwegian)
- Seba Kerckhof (Dutch)
- Serhat SUT (Turkish)
- Stefan Thrane Overby (Danish)
- Stephan Steiner (German)
- Szanyi Szabolcs (Hungarian)
- Tim Debie (Dutch)
- Tobias Brechle (German)
- Toshihiro Kan (Japanese)
- Volker Theile (German)
- Wei Ding (Chinese)
- (Russian)
- (Russian)
- (Russian)
- Maliar Benoit (French)
- Ji-Hyeon Gim (Korean)
- Sergio Rius Rodriguez (Spanish/Portuguese)
- Chang-Eon Byeon (Korean)
- Jan Štourač (Czech)
- Sungjin Kang (Korean)
- Pavel Borecki (Czech)
- Joaquim Farriol (Catalan)
- Plamen Vasilev (Bulgarian)
- Gábor Sári (Hungarian)
- Jonatan Nyberg (Swedish)
- Gyuris Gellért (Hungarian)
- Miha Bezjak (Slovenian)
- Jérémy D (French)
- Herald Yu (Chinese)
- Axel Cantenys (French)
- Abo Khalid (Arabic)
- Kevin Leclercq (French)

- Rudy ten Kate (Dutch)

#### Code

- Stefan Seidel
- Don Harpell
- Ralf Lindlein
- Tony Guepin
- Ian Grant

More code contributors can be found [here](#).

## CHAPTER 14

---

### Copyright

---

openmediavault is Copyright © 2009-2021 by Volker Theile ([volker.theile@openmediavault.org](mailto:volker.theile@openmediavault.org)). All rights reserved.

openmediavault is free software: you can redistribute it and/or modify it under the terms of the [GNU General Public License v3](#) as published by the Free Software Foundation. The documentation is licensed under Creative Commons Attribution Share Alike 3.0 ([CC-BY-SA-3.0](#)).

openmediavault is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with openmediavault. If not, see <http://www.gnu.org/licenses>.