openmediavault Documentation

Release 4.0.0

Volker Theile

Jul 30, 2019

Contents:

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	Ago 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	Current	Apr 2018
5.0	Usul	Debian 10	In Development	est. 2019

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
  - **Data Drive**: capacity according to your needs

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

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

If you use a Flash Drive, select one with static wear leveling[6], 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.

[1] https://en.wikipedia.org/wiki/Paging
[2] https://en.wikipedia.org/wiki/Solid-state_drive
[3] https://en.wikipedia.org/wiki/Solid-state_drive#DOM
[4] https://en.wikipedia.org/wiki/CompactFlash
[5] https://en.wikipedia.org/wiki/USB_flash_drive
[6] https://en.wikipedia.org/wiki/Wear_leveling

CHAPTER 3

Installation

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 harddisks except the future 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 deboostrap. Use this as a last resource 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.

CHAPTER 4

Features

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[1] 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[2] 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.

[1] http://postfix.org
[2] https://www.avahi.org/

4.3 Storage

S.M.A.R.T.: Based on smartmontools[3], 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[4], 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[5] as standalone server by default.

FTP: Service based on proftpd[6]. 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[7].

SSH: Remote shell access using openssh[8].

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.

[3] https://www.smartmontools.org/
[4] https://raid.wiki.kernel.org/index.php/RAID_setup
[5] https://www.samba.org/
[6] http://www.proftpd.org/
[7] http://nfs.sourceforge.net/
[8] 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

Administration

5.1 General

5.1.1 Network

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

General

Hostname and domain settings.

Interfaces

The grid only displays configured interfaces done through the web interface. If you see this panel empty and your default interface was configured by DHCP or static during install is normal. The installer does not setup the network using openmediavault, it just configures `/etc/network/interfaces`. The dashboard contains a network widget that displays current status of 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 as you already know the IP address assigned to the server NIC.

When using static configuration be aware that the configuration window does not expand completely, scrolling down are the IPv6 fields and DNS fields. The DNS setting is essential for fetching updates, do not leave empty. 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

Support for wireless network was added in openmediavault 3.0. The configuration window displays the same IP configuration fields as ethernet, plus the relevant wireless values: SSID (the wireless network name) and the password. Please be aware wireless should not be used in a production server. This feature is intended for extreme cases. Whenever is possible please always use ethernet for a NAS server.

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 ammount of nics) in a single client using LACP. Even if the client also has a LACP bonded nic or 10Gbit card as there is no multipath support in samba or other openmediavault services like 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 phisical media is capable (SSD or RAID array) of reaching the speed of the bonded nic.

Advanced Interface Configuration

Proxy

This panel configures the server proxies using system wide enviromemtal variables. Every software that obbeys 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 appropiatly 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 avahi-daemon announce services. You can disable selectively by service and/or change the common name announce. Plugins can add their service here also. Avahi announces are recognized by Linux file browsers by default. Mac OSX only recognizes SMB and AFP protocol in their sidebar.

Windows does not understand avahi announces. Samba announces to windows client using the NetBIOS daemon (nmbd). If windows network section does not display the samba server this settings do not change that behaviour.

Firewall

This is grid panel for adding iptables rules. This can be useful if you need to secure access in your local network. At the moment 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 located in this file `/etc/network/if-pre-up.d/openmediavault-iptables`. The mkconf openmediavault script uses a run-parts folder `/usr/share/mkconf/iptables.d` where is possbile to store custom scripts to add rules to the NAT and RAW table or the FORWARD chain,

---

Tip:

- To avoid locking yourself out while testing, create a cron command to run every five minutes that flushes the OUTPUT/INPUT chain.

```
*/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.

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

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

If you have no problems with sensitive information in the ruleset then you can create a text link:

```
$ iptables-save | curl -F 'sprunge=<-' http://sprunge.us
```

5.1.2 Notifications

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

[1] http://www.postfix.org

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 his 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.
- Summary of locked users by pam_tally2[2]. 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]

[2] http://www.linux-pam.org/Linux-PAM-html/sag-pam_tally2.html

- 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 selectivly. 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

```
SMTP Server: smtp.gmail.com
SMTP Port: 587
SSL/TLS: Yes
Sender email: rootthe@gmail.com (include domain)
Authentication: 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`

SSL

If the remote SMTP server uses port 465, openmediavault will reconfigure the MTA to use the corresponding directives as documented in postfix for wrapper mode.

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:

```
$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 adresses (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 MESSAGE_FILE variable only in your script.

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.

5.1.3 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[1]. 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 his *profile* the notification will be sent to that mail address.

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:

[1] https://linux.die.net/man/5/crontab

- 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[1].

5.1.4 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

5.1.5 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 appropiate 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 from to his certificate pair.

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

When importing existing ssl certificates make sure they are formated/converted appropiatly.

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.

5.2 Storage

5.2.1 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 `DiskMgnt::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"
```


(continues on next page)

(continued from previous page)


```
            ],
            "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]",
            "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[1]. 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-mkconf 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 inmediatly 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:

```
$ 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
```

5.2.2 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 assest 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 bests for assesing health[1].

There are several tools for accessing those attributes. openmediavault reads and monitors hard drives smart values using smartmontools[2].

[1] https://linux.die.net/man/8/hdparm
[1] https://www.backblaze.com/blog/what-smart-stats-indicate-hard-drive-failures/
[2] https://www.smartmontools.org/

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[3].

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 tooltup 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
- 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 inmediate

These tests and what they do are explained here and here.

SMART only realloactes a bad sector on write. A manual method to force reallocating the pending(s) sector(s) is decribed here.

[3] https://www.backblaze.com/blog/hard-drive-temperature-does-it-matter/

5.2.3 RAID

openmediavault uses linux software RAID driver (MD) and the mdadm utility to create arrays[1]. Arrays created in any other linux distro should be recognized inmmediatly 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.

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 in 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:

[1] https://raid.wiki.kernel.org/index.php/Linux_Raid

```
$ 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, Pogoplugs and any low entry ARM SBC.

5.2.4 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 is better that you delete all fstab lines execept 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 mounted entry inside config.xml <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,noexec,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, mkconf fstab script writes the appropiate line in `/etc/fstab`. You can indentify entries in `/etc/fstab` created by the web interface by looking at «openmediavault» tags. Is important to mention to not alter the information in bewteen 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, the mkconf will pipe 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 ocurr if you decide to resize a disk partition or you have grown a RAID array by adding one or more disks.

Warning:

Filesystems greater than 16TB in ext4 The default mkfs.ext4 of Debian Wheezy does not use the 64bit flag for filesystems under 16TB, this is a serious problem since RAID arrays without that flag won't be able to expand and there is no workaround more than reformat. Version 1.8 introduced the flag as default for newly created ext4 filesystems, independant of the size. However the current resize2fs tool in Debian Wheezy cannot handle the flag for expanding the size. To overcome this a newer version of e2fsprogs is necessary. For avoiding recompiling the package, you can boot systemrescuecd and perform the expansion using gparted.

Delete The delete button actually deletes filesystems, using **`wipefs -a`**. This will flush filesystem, raid or partition-table 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 asociated 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.

5.3 Access Rights Management

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

5.3.1 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 him 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 his own profile information. Depending if the adminstrator has setup the username account to allow changes, they can change their password and mail account.

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 his account.

Paste the contents into the import dialog.

Privileges

The button opens a window that displays all current exisiting 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.

5.3.2 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`.

5.3.3 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[1][2].

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.

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`**[3] and read with **`getfacl`**[4].

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.

5.4 Services

5.4.1 Samba

Samba server comes from Debian software repositories. openmediavault developer does not mantain 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

[1] https://help.ubuntu.com/community/FilePermissionsACLs
[2] http://vanemery.net/Linux/ACL/linux-acl.html
[3] https://linux.die.net/man/1/setfacl
[4] https://linux.die.net/man/1/getfacl

```
[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
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"
```

Is possible to add extra options in the general and share configuration at the bottom with a multi line text field. This options are hardcoded in the mkconf script but they can be changed using 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 username changes his) 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 his 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 mkconf regenerates the `/etc/samba/smb.conf` file.

Note:

- The guest account is mapped to system account nobody, he doesn't belong to group users, thus he 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 adecuate 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.

5.4.2 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
  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 certficate 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_PROFTPD_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
```

5.4.3 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,nroot_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.[1][2]

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`.[3]
- **Extra options:** Add options according the exports manual. If squash options are not specified, the mkconf script will add `root_squash` by default which is not displayed in the text field.

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`:

[1] https://help.ubuntu.com/community/NFSv4Howto#NFSv4_without_Kerberos
[2] https://www.centos.org/docs/5/html/5.1/Deployment_Guide/s3-nfs-server-config-exportfs-nfsv4.html
[3] This is not standard openmediavault privileges as in the shared folder section

```
$ 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.

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 `anonuid=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.

5.4.4 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"
AAAAB3NzaC1yc2EAAAADAQABAAABAQDfSQulxffUktx2P6EikkjVxDw0tT8nCW8LHLx/kl
8t37xFQ5/OoL9m6rVzYy5CFGYt+l7DffWjL0Av7AqaM0ykZVmv2VEM6TmMo56LTlmyZdlz
X5+GEJgCQNtDxcIYAVuPXKpLtlB/uAGzwHdZWpAen+mHgWIi4va8N5QNn4rXpkREcvM1q4
snyAi+gyjAS2Dn4pm8zzrd9qQFnoRYzidbp5e2Rs3brOkwUco0ZkOME2Ff6SpLGaXz4DHH
qgdTqZwHaTXEwm6kDmglCQrauIPI/ggNqz9mVEspYkskR2PM4CAty8RkZD4MQe5K3EMAFR
aFobBSlhQ3ESCYWNXTS3bF
---- 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.

5.4.5 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
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`.

5.4.6 Netatalk

Overview

Netatalk software was expected to reach version 3.x with Debian Jessie. Unfortunatly due to some unresolved issue with the maintainers, Debian team opted to leave it out of Jessie and future releases. Debian Wheezy was the latest release with netatalk. To avoid loosing netatalk as a plugin openmediavault uses a debianized source of netatalk 3.x maintained by Adrian Knoth[1]. Openmediavault does not maintain this software.

[1] https://github.com/adiknoth/netatalk-debian

Configuration

The server panel provides minimal options to the server, but it has an extra field in case you need more directives. The default configuration file is located in `/etc/netatalk/afp.conf`. This is the default global section:

```
[Global]
max connections = 20
mac charset = MAC_ROMAN
unix charset = LOCALE
guest account = nobody
uam list = uams_dhx.so,uams_dhx2.so
save password = no
```

Netatalk provides PAM modules, so a change of password in terminal or web interface should be reflected inmediately in AFP login.

Shared Folders

The plugin uses the privileges database, so in the same way openmediavault configures Samba shares, the login is controlled using valid, read and write directives in the software layer, not the filesystem. This is an example of a share in netatalk with default options:

```
[Documents]
path = /media/dev-disk-by-label-VOLUME1/documents
read only = no
unix priv = yes
file perm = 0664
directory perm = 0775
umask = 0002
invisible dots = no
time machine = no
valid users = "mike"
invalid users =
rolist =
rwlist = "mike"
```

Password In case you don't want to use privileges you can assign a single password (no username) to the share.

Time Machine Support for the Apple backup software was added in netatalk 2.x, and improved in 3.x. Just check the box in the share options to make announce an individual share as a time machine server.

Guest Access You can select guest access which by default is read only. A second checkbox is provided for giving write access to guest.

Quota You can define a size limit, in case you have multiple time machine volumes and want to prevent them to fill up the data drives.

CHAPTER 6

Plugins

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 prefered way to extend your NAS. It is still possible to install regular software or containerized software like Docker. Plugins only exist for your convenience.

6.1 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.

6.2 Overview

The following is the list of official plugins by openmediavault.

- **ClamAV**: Provides antivirus scan for folders.
- **Route**: Add static routes.
- **Forked-daap**: Provides a daap protocol music server.
- **LDAP**: Integrates the user management panel with a LDAP server.
- **LVM2**: LVM managing. Create volume groups and logical partitions.
- **Netatalk**: Provides AFP sharing protocol used mainly in Mac OS X environments.
- **Diskstats**: Complementary plugin to extend current system statistics collection by adding iostats graphs.
- **NUT**: Controlling and configuring UPS. The driver support is based on NUT.

- **USB Backup**: Backup internal data to external disks on scheduled basis or on plug drive event.

6.3 3rd party

An overview of the third party plugin list can be found at omv-extras.org.

CHAPTER 7

FAQ

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.

Can I give access to non-admin users to the web control panel? No. By default non-admin users can only access their account profile, they can change password and their email address if the admin 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-admin users to their plugin. An example is in the openvpn plugin by omv-extras.

What is the file `/etc/openmediavault/config.xml` for? 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. If this is a save change, then mkconf passes the value to the service configuration file and reloads the daemon in case is necessary.

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 and existing openmediavault configuration? No. 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 of `/etc/network/interfaces` with some custom options the web interfa The interfaces file is controlled by openmediavault. To add network interfaces that are not configurable through the web interface or other options not present, use advanced settings.

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 /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 omv 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 acommodate 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.

Why are my filesystems mounted as noexec? This is a security measure to avoid the placement of malicious scripts in the shared folders. This will prevent any script execution in those paths, including compiling packages and binaries.

If you need to remove the noexc flag, use advanced settings as decribed here.

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-mkconf` command for? **`omv-mkconf`** 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-mkconf accepts are related to the name of the service it configures. Type **omv-mkconf** 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.

Why there is no iscsitarget plugin in openmediavault 4? The iscsitarget software is divided in two parts. The user-land tools and the kernel modules both are provided by Debian repository system. Kernel modules come in the form of DKMS. The upstream software is maintained in sourceforge. Debian only provides packages up to Jessie, this is because the DKMS modules do not built in kernels higher than 4.x. The last commit upstream was in 2010, right now iscsitarget is abandoned software.

It is possible to use iscsitarget plugin in openmediavault 3 or lower versions by using kernels lower than 4.x.

The intention is to migrate core underlaying software from iscsitarget to LIO targetcli

What is the omv-update and omv-release-upgrade for? Information about those commands are in the software section.

CHAPTER 8

Troubleshooting

Problem Web interface has missing fields and/or items showing that have been uninstalled.

Solution Clear your browser cache.

P I mounted the drive using the command line or GUI tool and I can't pick that drive in the shared folder device dropdown.

S Never mount a drive with anything other than the openmediavault web interface. This creates the necessary database entries to populate the device dropdown.

P I only see a few items in the web interface like the user section of Access Rights Management.

S You did not login as the admin user. This is the only user that can access everything.

P 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.

S 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.

P Samba is slow.

S Read these threads - Tuning Samba for more speed and Tuning Samba for more speed 2

P Samba share password is refused from Windows 10.

S To fix the problem you need to change the Network Security LAN Manager authentication level.

P The web interface keeps rejecting my admin/user password.

S 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 /`**

P I have problem accessing the web interface with Firefox.

S Try the solution mentioned in the Sencha ExtJS forum or the Mozilla bugtracker.

CHAPTER 9

Development

9.1 Coding Guideline

These standards for code formatting and documentation must be followed by anyone contributing to the openmediavault project. Any contributions that do not fullfill these guidelines will not be accepted.

9.1.1 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.

9.1.2 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"]';
```

9.1.3 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);
```

9.1.4 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();
}
```

9.1.5 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) {
    ...
}
```

9.2 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.

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

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.

Code contributions 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 in a GitHub pull request must be signed via `Signed-off-by: Frank Mustermann <frank.mustermann@xxx.yyy>`.
- You have to subscribe the CLA online via GitHub.

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.

9.3 Internal Tools

openmediavault software comes with several terminal command line tools that can be used by developers and/or advanced users. Also it can be used to gather support information.

9.3.1 omv-confdbadm (Database)

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[1] 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,
        "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,
```

(continues on next page)

[1] https://stedolan.github.io/jq/manual/v1.5/

(continued from previous page)

```
        "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:

```
# omv-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:

```
# omv-confdbadm read conf.system.filesystem.mountpoint  | jq -r '.[]|select(.type==
↪"ext4")'
```

Output returns:

```
{
  "opts": "defaults,noauto,user_xattr,usrjquota=aquota.user,grpjquota=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,
  "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"}'
```

(continues on next page)

(continued from previous page)

Remove a filesystem from the database, this time we pass only the corresponing uuid of the object:

```
# omv-confdbadm delete --uuid 567c2bd4-3d82-45b2-b34b-a6d38e680ed3 conf.system.
↪filesystem.mountpoint
```

9.3.2 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"
   ]
 },
 {
   "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,
```


(continues on next page)

(continued from previous page)


```
    "description": "dfa (875.00 MiB available)",
    "propposixacl": 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)",
    "propposixacl": 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:


```
[
  {
    "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]"
  },
```


(continues on next page)

(continued from previous page)

```
 {
   "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 tools is used to prettify the output in json.

9.3.3 helper-functions (Shell)

openmediavault ships with this file `/usr/share/openemdiavault/scripts/helper-functions` that contains several POSIX shell functions. This are intended to make it easier for developers to create mkconf or postinst/postrm scripts. 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-b761-1ddfabde2d2a
```

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 is purged. This is from omvextras 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"
```

(continues on next page)

(continued from previous page)

```
omv_config_add_key "${SERVICE_XPATH}" "loglevel" "error"
omv_config_add_key "${SERVICE_XPATH}" "extraoptions" ""
```

Notice in the postint file how it sources at the beginning `helper-functions`. The same happens in mkconf scripts .

Note: What each function do and the parameters it accepts is documented in the helper-functions file .

CHAPTER 10

Support

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.

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.

CHAPTER 11

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 12

Contributors

Founder and project manager

Volker Theile

Forum

- area3o
- Cpoc
- davidh2k
- Dennis
- donh
- i814u2
- jensk
- jhmiller
- KM0201
- knumsi
- PhantomSens
- ryecoaaron
- 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 Grünewald (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)

Code

- Stefan Seidel
- Don Harpell

- Ralf Lindlein
- Tony Guepin
- Ian Grant

More code contributers can be found here.

CHAPTER 13

Copyright