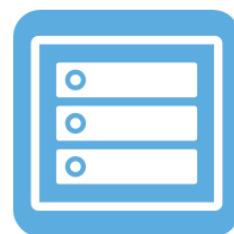


OpenMediaVault, mucho más que un servidor NAS

openmediavault/ **openmediavault**



openmediavault is the next generation network attached storage (NAS) solution based on Debian Linux. Thanks to the modular design of...

58

Contributors

74

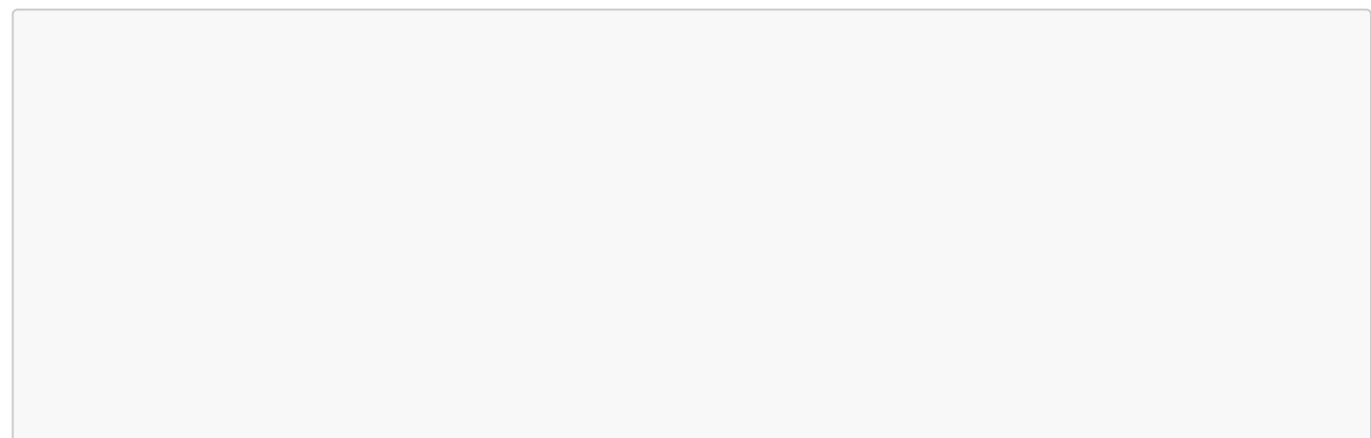
Issues

5k

Stars

453

Forks



Alumno: Jesús Marchante Meco

Ciclo: Administración de Sistemas Operativos y Redes

IES La Senia. Curso 2022/2024

18 de Junio de 2024

Tutor individual: Ángel Berlanas

Índice

1. [Introducción, justificación y objetivos](#) pag. 3
2. [Planificación del proyecto](#) pag. 4
3. [Recopilación de hardware](#) pag. 5
4. [Instalación Debian 11 LVM](#) pag. 8
5. [Instalación OpenMediaVault 6](#) pag. 10
6. [Instalación plugin lvm2](#) pag. 11
7. [Añadir nuevo disco](#) pag. 12
8. [Instalación plugin sharerootfs](#) pag. 15
9. [Instalación docker y docker-compose](#) pag. 16
10. [Instalación nginx-proxy-manager](#) pag. 19
11. [Sitio web](#) pag. 21
12. [Nube privada NextCloud](#) pag. 27
13. [Servidor multimedia Jellyfin](#) pag. 30
14. [Pruebas de seguridad](#) pag. 33
15. [VPN](#) pag. 43
16. [Conclusiones y ampliación](#) pag. 47
17. [Referencias](#) pag. 48

Introducción, justificación y objetivos

Si eres una PYME/autónomo que acabas de iniciar tu actividad, o incluso un particular, es seguro que necesitarás visibilidad en internet mediante tu sitio web, una nube privada sin restricciones no te vendrá mal, y seguro que le puedes sacar partido a un servidor de archivos multimedia.

Todo esto se podría implementar en empresas externas como [Amazon Web Services](#) o [Microsoft Azure](#), pero dado que no son gratuitas y no tenemos por qué creernos que garantizan nuestra privacidad, decidimos montarlo en un equipo propio con la conexión a internet de nuestro domicilio.

Tal y como se indica en la portada, si buscamos información acerca de OpenMediaVault encontraremos que es la nueva generación [NAS](#) basada en Debian; pero si rascamos un poco más nos daremos cuenta que nos va a permitir llevar a cabo todo lo anterior de una forma relativamente sencilla.

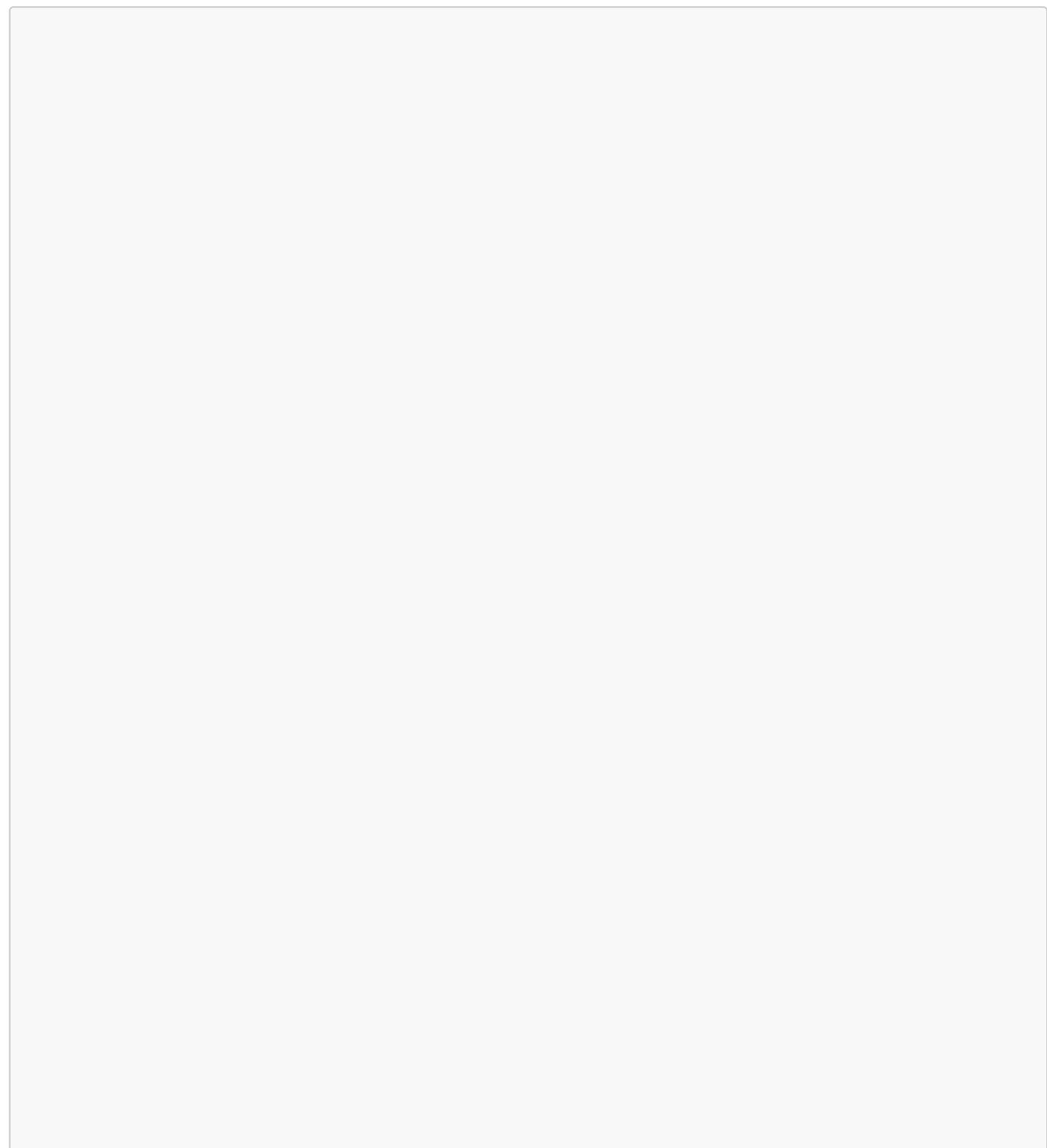
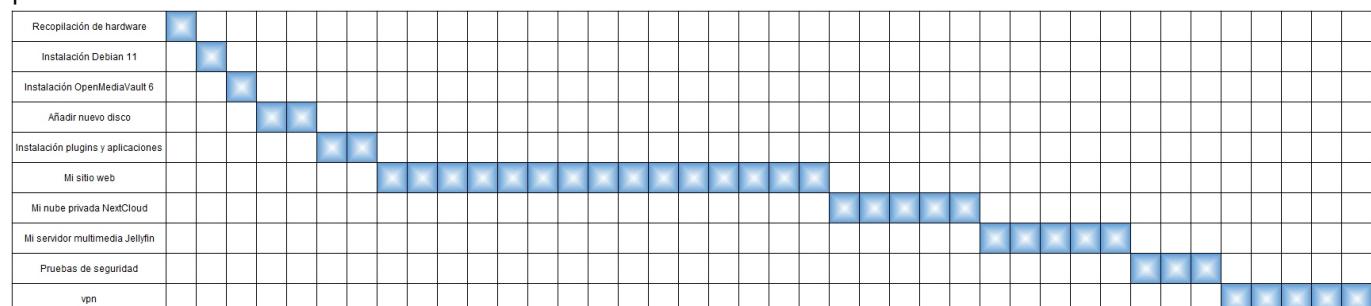
Para este proyecto se implementará mediante OpenMediaVault 6 el sitio web de películas marchantemeco.duckdns.org (con su CRUD y su base de datos), la nube privada NextCloud marchantemeco-nextcloud.duckdns.org y el servidor multimedia Jellyfin marchantemeco-jellyfin.duckdns.org, todo mediante certificados SSL autorenovables, accesibles a través de internet desde cualquier parte, y **abriendo sólo 2 puertos en el router** gracias al proxy inverso Nginx Proxy Manager.

Como extra y para poder acceder desde cualquier parte a nuestra red local como un equipo más, se pondrá en marcha el servidor VPN más rápido, Wireguard, que además se integrará con PiHole (servidor DNS que resuelve dominios y subdominios asociados a ads a 0.0.0.0) para bloquear la publicidad, a costa de abrir un puerto más en el router.

En un mundo hiperconectado, tener en cuenta la seguridad es a día de hoy una obligación, y más si estamos exponiendo a internet ciertos servicios abriendo puertos en el router, por lo que se realizarán ciertas pruebas de seguridad.

Planificación del proyecto

Diagrama de Gantt para mostrar cual ha sido el desarrollo del proceso, así como el tiempo destinado a cada parte:



Recopilación de hardware

Preciosa placa base [Asus P5K3 Deluxe/WiFi-AP LGA 775](#) modificada para reconocer la CPU de servidor [Intel Xeon X5460](#) (si nos fijamos se le ha aplicado un ligero overclock para alcanzar los 3.8GHz)

```
OpenSSH SSH client
root@omv:~# dmidecode --type 2
# dmidecode 3.3
Getting SMBIOS data from sysfs.
SMBIOS 2.4 present.

Handle 0x0002, DMI type 2, 15 bytes
Base Board Information
    Manufacturer: ASUSTeK Computer INC.
    Product Name: P5K3 Deluxe
    Version: Rev 1.xx
    Serial Number: MS1C75B60100787
    Asset Tag: To Be Filled By O.E.M.
    Features:
        Board is a hosting board
        Board is replaceable
    Location In Chassis: To Be Filled By O.E.M.
    Chassis Handle: 0x0003
    Type: Motherboard
    Contained Object Handles: 0

root@omv:~# dmidecode --type 4
# dmidecode 3.3
Getting SMBIOS data from sysfs.
SMBIOS 2.4 present.

Handle 0x0004, DMI type 4, 35 bytes
Processor Information
    Socket Designation: LGA775
    Type: Central Processor
    Family: Other
    Manufacturer: Intel
    ID: 76 06 01 00 FF FB EB BF
    Version: Intel(R) Xeon(R) CPU X5460 @ 3.16GHz
    Voltage: 1.2 V
    External Clock: 333 MHz
    Max Speed: 3800 MHz
    Current Speed: 3166 MHz
    Status: Populated, Enabled
    Upgrade: Socket LGA775
    L1 Cache Handle: 0x0005
    L2 Cache Handle: 0x0006
    L3 Cache Handle: 0x0007
    Serial Number: To Be Filled By O.E.M.
    Asset Tag: To Be Filled By O.E.M.
    Part Number: To Be Filled By O.E.M.
```

4x2Gb de memoria RAM DDR3

```
OpenSSH SSH client
root@omv:~# dmidecode --type 6
# dmidecode 3.3
Getting SMBIOS data from sysfs.
SMBIOS 2.4 present.

Handle 0x0009, DMI type 6, 12 bytes
Memory Module Information
    Socket Designation: DIMM0
    Bank Connections: 0 1
    Current Speed: 15 ns
    Type: DIMM
    Installed Size: 2048 MB (Double-bank Connection)
    Enabled Size: 2048 MB (Double-bank Connection)
    Error Status: OK

Handle 0x000A, DMI type 6, 12 bytes
Memory Module Information
    Socket Designation: DIMM1
    Bank Connections: 2 3
    Current Speed: 15 ns
    Type: DIMM
    Installed Size: 2048 MB (Double-bank Connection)
    Enabled Size: 2048 MB (Double-bank Connection)
    Error Status: OK

Handle 0x000B, DMI type 6, 12 bytes
Memory Module Information
    Socket Designation: DIMM2
    Bank Connections: 4 5
    Current Speed: 15 ns
    Type: DIMM
    Installed Size: 2048 MB (Double-bank Connection)
    Enabled Size: 2048 MB (Double-bank Connection)
    Error Status: OK

Handle 0x000C, DMI type 6, 12 bytes
Memory Module Information
    Socket Designation: DIMM3
    Bank Connections: 6 7
    Current Speed: 15 ns
    Type: DIMM
    Installed Size: 2048 MB (Double-bank Connection)
    Enabled Size: 2048 MB (Double-bank Connection)
    Error Status: OK
```

Tarjeta gráfica dedicada AMD HD5850

```
OpenSSH SSH client
root@omv:~# lspci | grep -i vga
01:00.0 VGA compatible controller: Advanced Micro Devices, Inc. [AMD/ATI] Cypress PRO [Radeon HD 5850]
```

2 discos mecánicos IDE

```
OpenSSH SSH client

root@omv:~# fdisk -l
Disk /dev/sda: 298.09 GiB, 320072933376 bytes, 625142448 sectors
Disk model: MAXTOR STM332082
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xdffb5b022

Device      Boot   Start     End   Sectors   Size Id Type
/dev/sda1    *       2048   999423   997376   487M 83 Linux
/dev/sda2          1001470 625141759 624140290 297.6G  5 Extended
/dev/sda5          1001472 625141759 624140288 297.6G 8e Linux LVM

Disk /dev/sdb: 232.89 GiB, 250059350016 bytes, 488397168 sectors
Disk model: WDC WD2500BB-22G
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

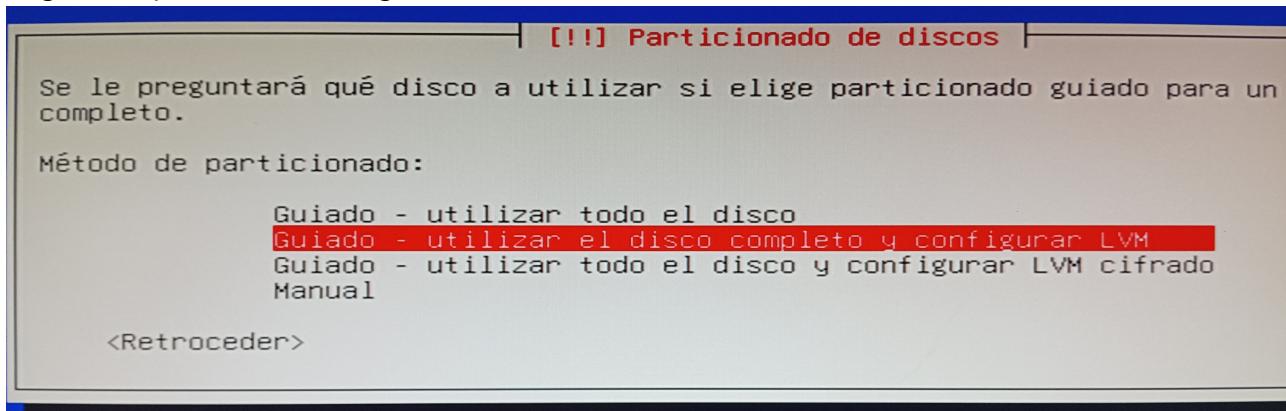
Disk /dev/mapper/omv--vg-root: 529.54 GiB, 568584044544 bytes, 1110515712 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/mapper/omv--vg-swap_1: 980 MiB, 1027604480 bytes, 2007040 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

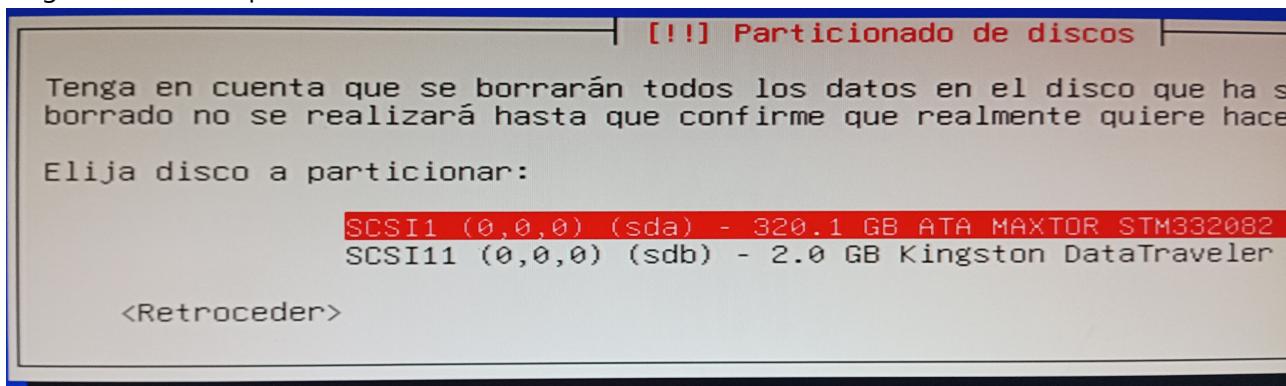
Instalación Debian 11 LVM

Instalamos Debian 11 a partir de la [iso netinst para PC de 64 bits](#)

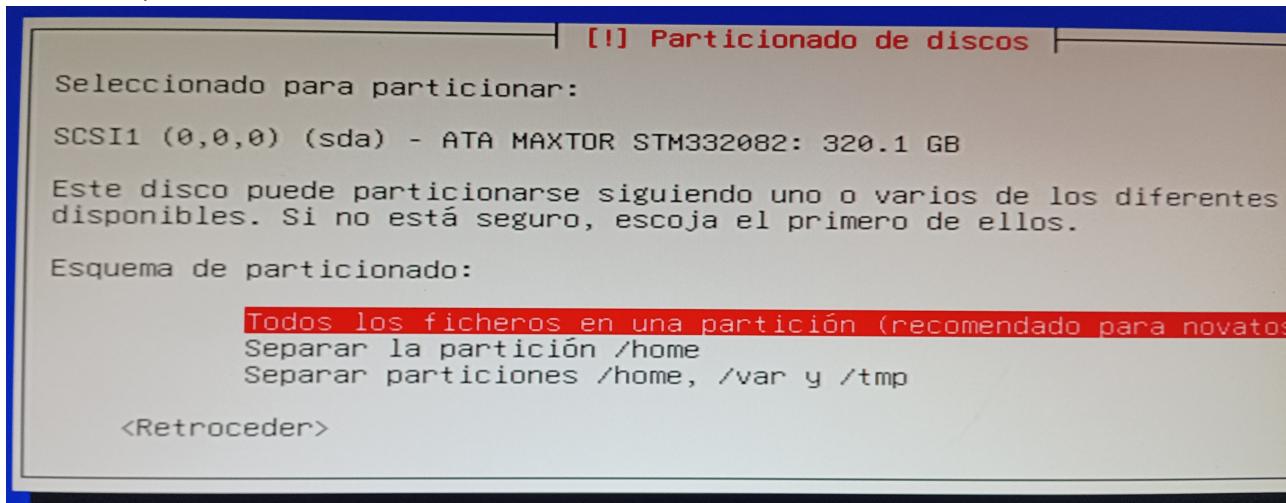
- Llegados al particionado se elige LVM



- Elegimos el disco a particionar



- Todo en la partición raíz /



- Creará los volúmenes lógicos **root** (para el sistema de archivos /) y **swap_1** (para el área de intercambio) y los meterá en el grupo de volúmenes **omv-vg**

```

[!] Particionado de discos

Este es un resumen de las particiones y puntos de montaje que tiene configurados
actualmente. Seleccione una partición para modificar sus valores (sistema de ficheros
puntos de montaje, etc.), el espacio libre para añadir una partición nueva o un
dispositivo para inicializar la tabla de particiones.

Particionado guiado
Configurar RAID por software
Configurar el Gestor de Volúmenes Lógicos (LVM)
Configurar los volúmenes cifrados
Configurar los volúmenes iSCSI

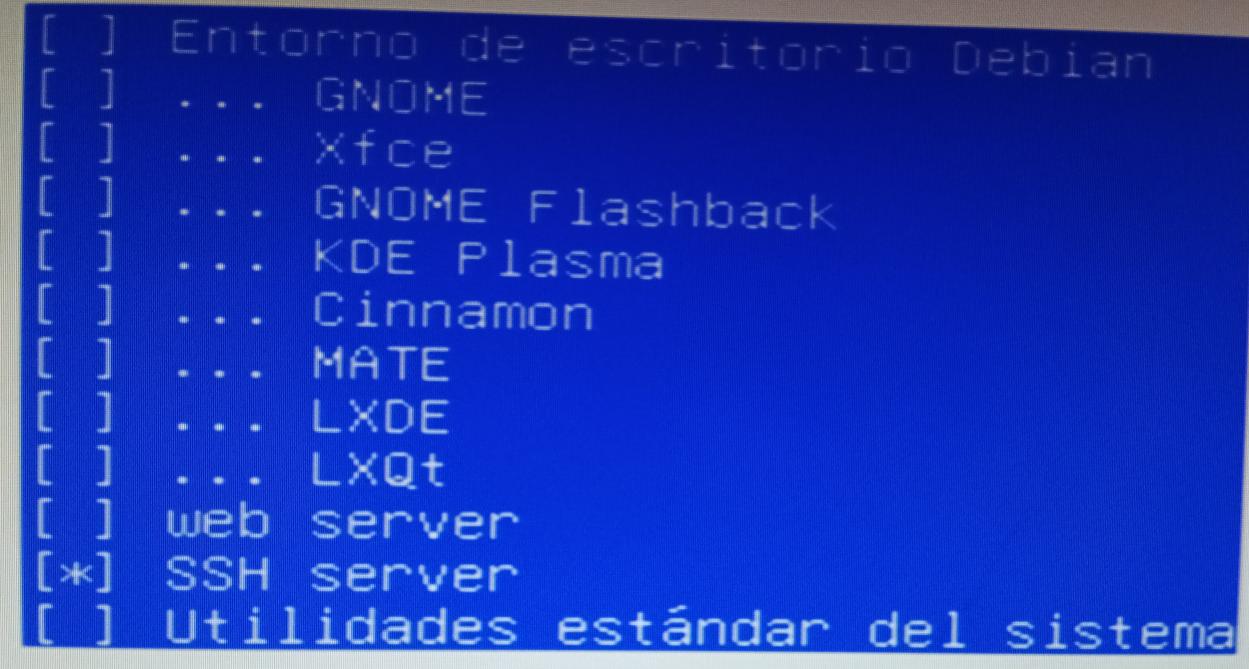
LVM VG omv-vg, LV root - 318.5 GB Linux device-mapper (linear)
#1 318.5 GB f ext4 /
LVM VG omv-vg, LV swap_1 - 1.0 GB Linux device-mapper (linear)
#1 1.0 GB f intercambio intercambio
LVM VG ventoy, LV ventoy - 658.5 MB Linux device-mapper (linear)
SCSI1 (0,0,0) (sda) - 320.1 GB ATA MAXTOR STM332082
#1 primaria 510.7 MB f ext2 /boot
#5 lógica 319.6 GB K lvm
SCSI11 (0,0,0) (sdb) - 2.0 GB Kingston DataTraveler 2.0
#1 primaria 2.0 GB B
#2 primaria 33.6 MB fat16

Deshacer los cambios realizados a las particiones
Finalizar el particionado y escribir los cambios en el disco

<Retroceder>

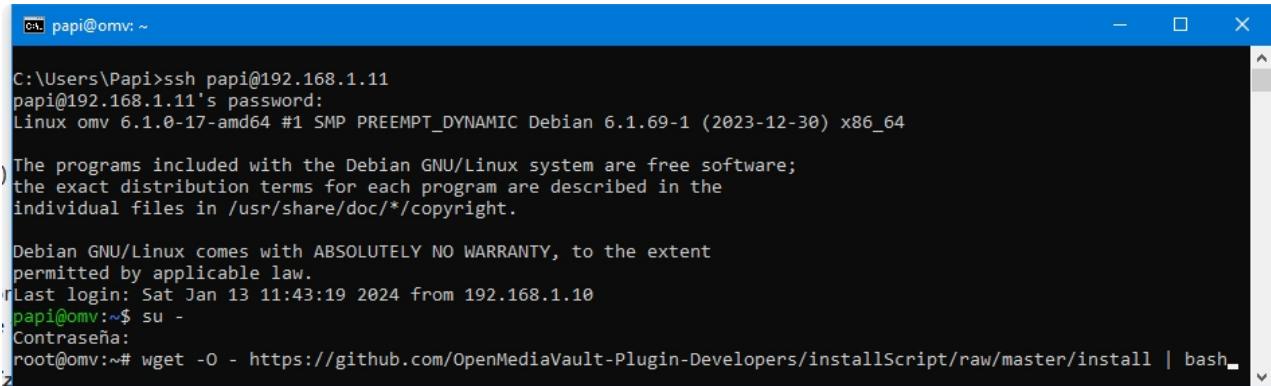
```

- No debemos instalar entorno gráfico, sólo el servidor SSH, ésto es importante



Instalación de OpenMediaVault 6

- Nos conectamos mediante SSH al servidor (la dirección IP 192.168.1.11 es dinámica pero está reservada en el servidor DHCP) y lanzamos como superusuario según la [guía wget -O -](#)
<https://github.com/OpenMediaVault-Plugin-Developers/installScript/raw/master/install | bash> para instalar OpenMediaVault junto con los plugins OMV-Extras y Flashmemory

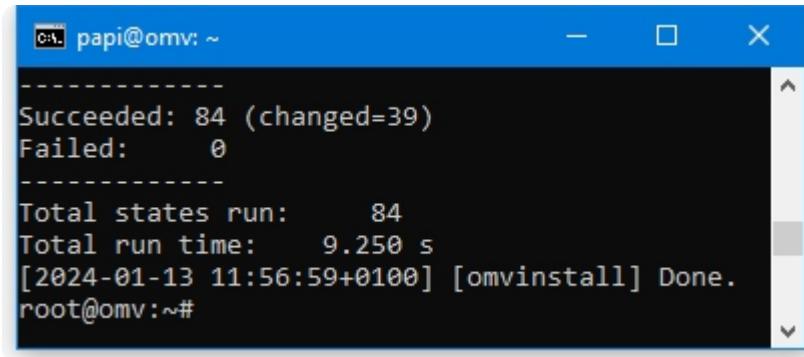


```
papi@omv: ~
C:\Users\Papi>ssh papi@192.168.1.11
papi@192.168.1.11's password:
Linux omv 6.1.0-17-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.69-1 (2023-12-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Jan 13 11:43:19 2024 from 192.168.1.10
papi@omv:~$ su -
Contraseña:
root@omv:~# wget -O - https://github.com/OpenMediaVault-Plugin-Developers/installScript/raw/master/install | bash
```

- Si todo ha ido bien nos mostrará un bonito Done

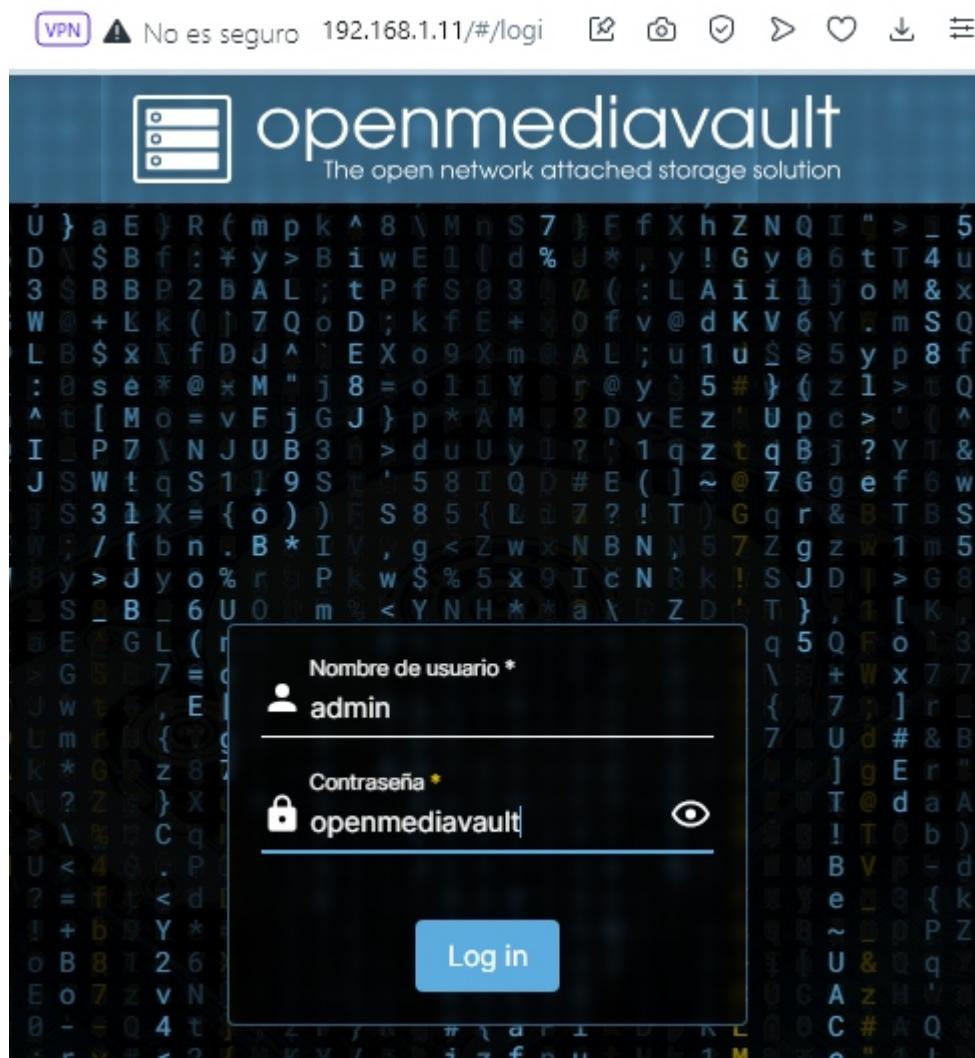


```
papi@omv: ~
-----
Succeeded: 84 (changed=39)
Failed:    0
-----
Total states run:      84
Total run time:      9.250 s
[2024-01-13 11:56:59+0100] [omvinstall] Done.
root@omv:~#
```

Instalación plugin lvm2

Nos permitirá añadir nuevos discos al volumen lógico sin tirar un sólo comando:

- Introducimos en el navegador web la dirección ip del servidor; por defecto el usuario es **admin** y la contraseña es **openmediavault**



- Instalamos este plugin

openmediavault-lvm2 7.0-1

openmediavault Logical Volume Manager (LVM2) plugin

Instaladas

LVM supports enterprise level volume management of disk and disk subsystems as regular block devices.

Sección: Filesystems

Mantenedor: Volker Theile <volker.theile@openmediavault.org>

Página de inicio: <http://www.openmediavault.org>

Repositorio: [openmediavault.org archive/sandworm](http://openmediavault.org/archive/sandworm)

Tamaño: 24.61 KiB

Añadir nuevo disco

Añadimos un nuevo disco al equipo y extendemos el volumen lógico

- Ya que es un disco usado, primero vamos a borrarle la tabla de particiones

Dispositivo ^	Modelo ^	Número de Serie ^	Vendedor ^	Capacidad ^
/dev/sda	WDC	WD- WD2500BB- 22GUC0	ATA	232.89 GiB
/dev/sdb	MAXTOR	9QF7RK36 STM3320820A	ATA	298.09 GiB

- Creamos un volumen físico

Almacenamiento | Gestión de volúmenes lógicos | Volúmenes físicos

Dispositivo *
WDC WD2500BB-22GUC0 [/dev/sda, 232.88 GiB]

Cancelar Salvar

- Extendemos el grupo de volúmenes con el nuevo volumen físico

Almacenamiento | Gestión de volúmenes lógicos | Grupos de volúmenes

Nombre ^	Disponible ^	Libre ^	Volúmenes físicos ^	Volúmenes lógicos ^
omv-vg	297.61 GiB	0.00 B	• /dev/sdb5	• root • swap_1

[Home](#) | Almacenamiento | Gestión de volúmenes lógicos | Grupos de volúmenes | Ampliar

Nombre

omv-vg

Nombre del grupo de volúmenes.

Dispositivos *

LVM physical volume [/dev/sda, 232.88 GiB]

Seleccionar los discos usados para extender el grupo de volúmenes.

Cancelar

Salvar

- Extendemos el volumen lógico /dev/omv-vg/root al 100% del espacio

[Home](#) | Almacenamiento | Gestión de volúmenes lógicos | Volúmenes lógicos



Nombre	Capacidad	Grupo de volúmenes	Activo
root	296.65 GiB	omv-vg	✓
swap_1	980.00 MiB	omv-vg	✓

[Home](#) | Almacenamiento | Gestión de volúmenes lógicos | Volúmenes lógicos | Ampliar

Nombre

root

Nombre del volumen lógico.

Grupo de volúmenes

LVM volume group omv-vg [/dev/omv-vg, 530.49 GiB, 232.88 GiB free]

Capacidad

296.65 GiB

Size

100

The percentage of the total space in the volume group to use by the logical volume.

Cancelar

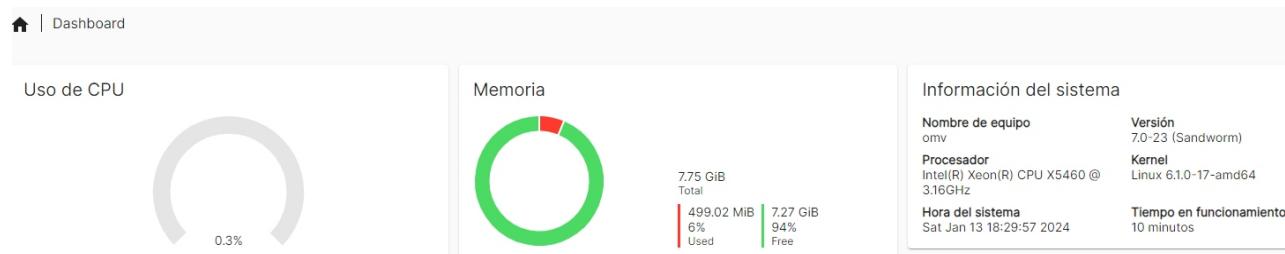
Salvar

Una maravilla, con el nuevo disco hemos pasado de tener casi 300GB de almacenamiento a más de 500GB (varios volúmenes físicos como un único volumen lógico).

Almacenamiento | Gestión de volúmenes lógicos | Volúmenes lógicos

Nombre	Capacidad	Grupo de volúmenes	Activo
root	529.54 GiB	omv-vg	✓
swap_1	980.00 MiB	omv-vg	✓

Resumen del sistema:



Instalación plugin sharerootfs

Necesitamos instalar el siguiente plugin para que OpenMediaVault pueda trabajar con el sistema de archivos raíz:

openmediavault-sharerootfs 6.0.3-1 Instaladas
openmediavault share root filesystem plugin

By default the root filesystem is hidden in openmediavault and cannot be used to create shared folders on it. This is by design to separate the operating system from user data. This plugin allows creating shared folders in the root file system.

Sección: Admin
Mantenedor: Volker Theile <volker.theile@openmediavault.org>
Página de inicio: <https://www.openmediavault.org>
Repositorio: openmediavault.org archive/shaitan
Tamaño: 3.20 KIB

Una vez instalado ya nos aparece en Sistema de Archivos, si no **no aparecerá**

⌂ | Almacenamiento | Sistema de Archivos

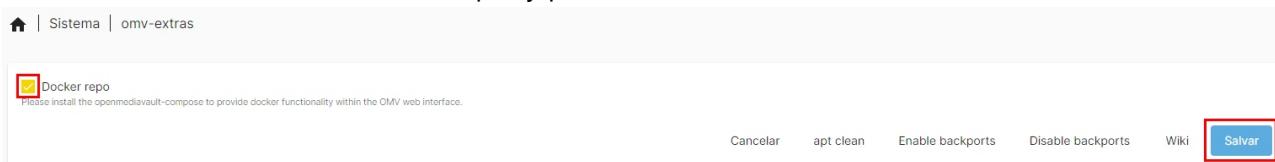
The screenshot shows the 'Sistema de Archivos' (Filesystem) section of the OpenMediaVault web interface. A single partition is listed:

Dispositivo	Tipo	Disponible	Usado	Montados	Referenciado	Estado
/dev/dm-0	EXT4	491.70 GiB	1.96 GiB	✓		Online

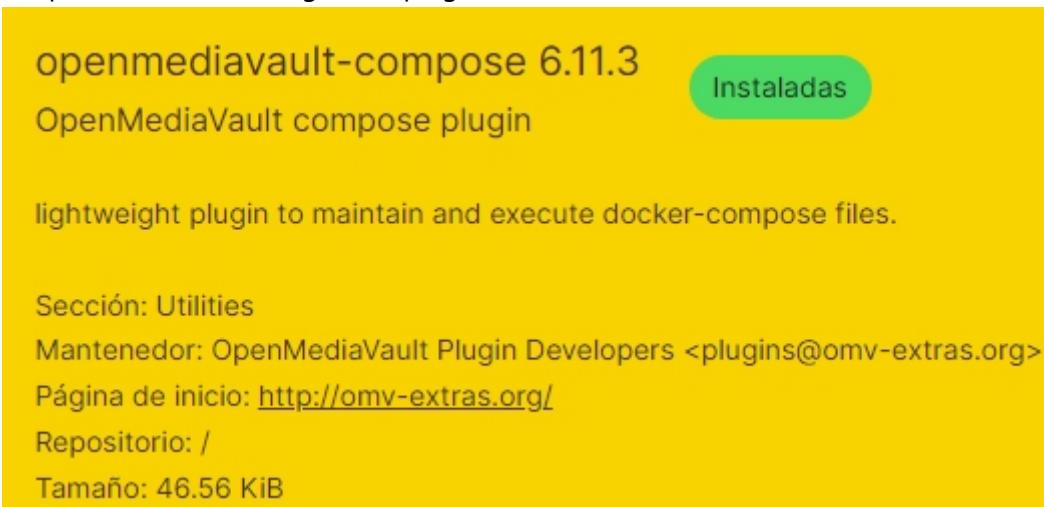
Instalación docker y docker-compose

Quizás se me haya pasado, pero aquí todo funciona mediante contenedores, por lo que hemos de hacer los siguientes paso:

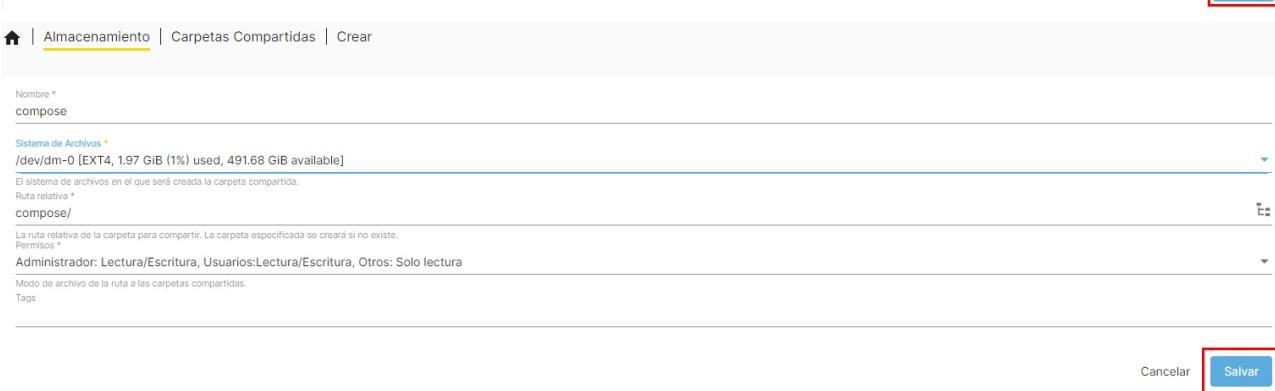
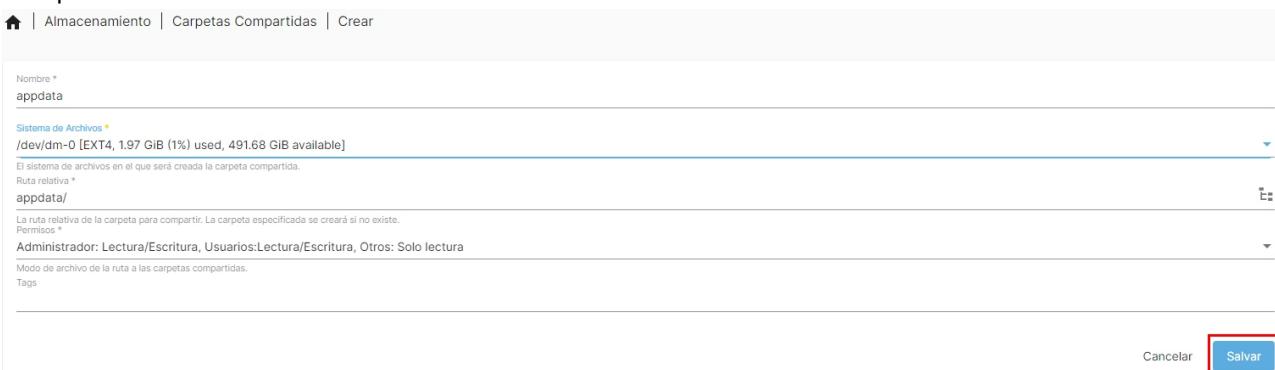
- Primero activamos el check "Docker repo" y pulsamos en "Salvar"



- Después instalamos el siguiente plugin



- Compartimos las carpetas appdata, compose, compose_backup, docker y configuramos docker-compose con ellas



Almacenamiento | Carpetas Compartidas | Crear

Nombre *
compose_backup

Sistema de Archivos *
/dev/dm-0 [EXT4, 1.97 GiB (1% used, 491.68 GiB available)]

El sistema de archivos en el que será creada la carpeta compartida.

Ruta relativa *
compose_backup/

La ruta relativa de la carpeta para compartir. La carpeta especificada se creará si no existe.

Propietario *
Administrador: Lectura/Escritura, Usuarios:Lectura/Escritura, Otros: Solo lectura

Modo de archivo de la ruta a las carpetas compartidas.

Tags

Cancelar **Salvar**

Almacenamiento | Carpetas Compartidas | Crear

Nombre *
docker

Sistema de Archivos *
/dev/dm-0 [EXT4, 1.97 GiB (1% used, 491.68 GiB available)]

El sistema de archivos en el que será creada la carpeta compartida.

Ruta relativa *
docker/

La ruta relativa de la carpeta para compartir. La carpeta especificada se creará si no existe.

Permisos *
Administrador: Lectura/Escritura, Usuarios:Lectura/Escritura, Otros: Solo lectura

Modo de archivo de la ruta a las carpetas compartidas.

Tags

Cancelar **Salvar**

Almacenamiento | Compose | Configuración

Archivos compose

Shared folder
compose [on /dev/mapper/omv--vg-root, compose/]

Location of compose files
Propietario de los directorios y archivos *

Grupo de directorios y archivos *
root

Permisos de los directorios y archivos
Administrador: lectura/escritura, Usuarios: sin acceso, Otros: sin acceso

Datos

Shared folder
appdata [on /dev/mapper/omv--vg-root, appdata/]

Optional - Location of persistent container data
Only used to substitute CHANGE_TO_COMPOSE_DATA_PATH in compose and env files with this shared folder path.

Backup

Shared folder
compose_backup [on /dev/mapper/omv--vg-root, compose_backup/]

Location of backups
Max Size *
1

Units in GB. Backup will skip volumes larger than this size.
Set to 0 for unlimited.

Docker

Almacén de dockers
/docker

Dejar en blanco para usar /etc/docker/daemon.json personalizado

Estado
Not installed

Versión de Docker
n/a

Versión de Compose
n/a

Cancelar Reinstalar Docker Reiniciar Docker **Salvar**

- Si todo ha ido bien, reinstalamos docker con la nueva configuración

Home | Servicios | Compose | Configuración

Archivos compose

Shared folder
compose [on /dev/mapper/omv--vg-root, compose/]

Location of compose files
Propietario de los directorios y archivos *
root

Grupo de directorios y archivos *
root

Permisos de los directorios y archivos
Administrador: lectura/escritura, Usuarios: sin acceso, Otros: sin acceso

Datos

Shared folder
appdata [on /dev/mapper/omv--vg-root, appdata/]

Optional - Location of persistent container data
Only used to substitute CHANGE_TO_COMPOSE_DATA_PATH in compose and env files with this shared folder path.

Backup

Shared folder
compose_backup [on /dev/mapper/omv--vg-root, compose_backup/]

Location of backups
Max Size *
1

Units in GB. Backup will skip volumes larger than this size.
Set to 0 for unlimited.

Docker

Almacenamiento de docker
/docker

Dejar en blanco para usar /etc/docker/daemon.json personalizado
Estado
Instalado y ejecutando

Versión de Docker
docker-ce 5:24.0.7-1~debian.12~bookworm

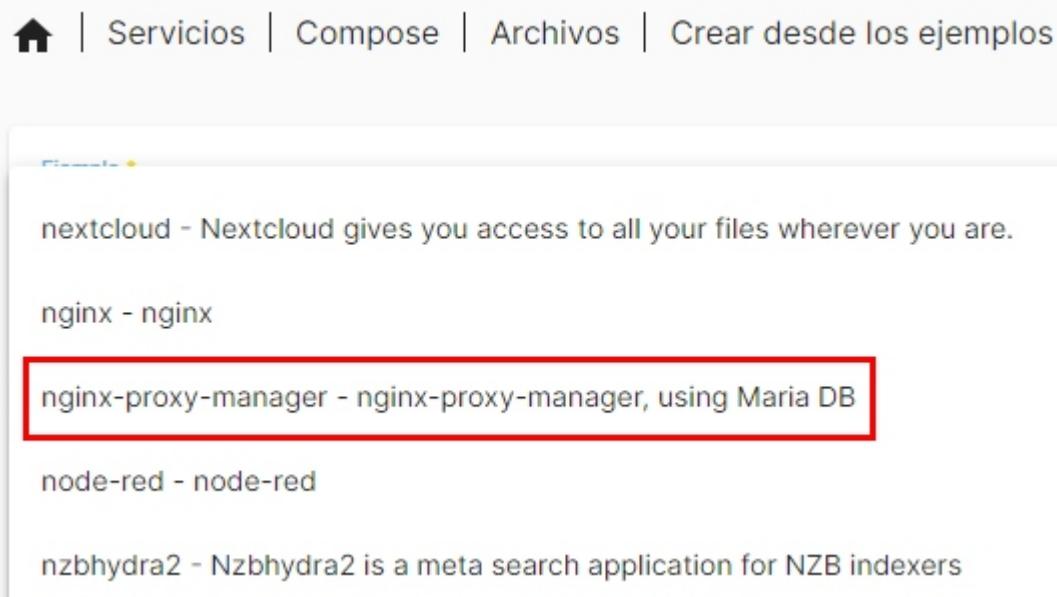
Versión de Compose
docker-compose-plugin 2.21.0-1~debian.12~bookworm

Instalación nginx-proxy-manager

Este proxy inverso es la aplicación que nos va a permitir tener cuantas aplicaciones deseemos, cada una trabajando en un puerto diferente, pero accediendo a ellas desde internet sin tener abiertos en el router todos esos puertos, sino sólo los puertos 80 y 433.

Además nos permitirá disponer de certificados SSL para cada una de esas aplicaciones y que éstos se renueven automáticamente, atentificación Digest, etc.

Dicha aplicación también la podemos instalar fácilmente desde los ejemplos (recomiendo la versión 2.9.19)

A screenshot of a web-based Docker Compose interface. At the top, there's a navigation bar with icons for Home, Services, Compose, Archives, and Create from Examples. Below the navigation, a list of services is shown: nextcloud, nginx, nginx-proxy-manager (which is highlighted with a red border), node-red, and nzbhydra2. Each service name is followed by a brief description.

Como nos explican en la documentación, los puertos 80 y 443 han de ser públicos (NAT en el router), y el puerto 81 es que utilizaremos para administrar la aplicación localmente

```
version: '3.8'  
services:  
  app:  
    image: 'jc21/nginx-proxy-manager:2.9.19'  
    restart: unless-stopped  
    ports:  
      # These ports are in format <host-port>:<container-port>  
      - '80:80' # Public HTTP Port  
      - '443:443' # Public HTTPS Port  
      - '81:81' # Admin Web Port  
      # Add any other Stream port you want to expose  
      # - '21:21' # FTP  
      -
```

Cuando ingresemos por primera vez el usuario es admin@example.com y la contraseña es changeme, los cuales después deberíamos cambiar

Default Administrator User login:
Email: admin@example.com
Password: changeme

Prácticamente no tenemos que configurar casi nada, salvo la zona horaria, la ruta a los volúmenes

```
volumes:
  - /appdata/nginxproxymanager/data:/data
  - /appdata/nginxproxymanager/letsencrypt:/etc/letsencrypt
depends_on:
  - db
db:
  image: 'jc21/mariadb-aria:latest'
  restart: unless-stopped
  volumes:
    - /appdata/nginxproxymanager/mysql:/var/lib/mysql
```

ment

```
###  
# Nginx Proxy Manager variables  
###  
TZ=Europe/Madrid
```

Ahora crearemos un certificado SSL/Proxy Host para cada uno de nuestros dominios/aplicaciones

Sitio web

Creo el sitio web marchantemeco.duckdns.org con la siguiente configuración (escucha en el puerto **8080**)

```
version: "3.1"
services:
  db:
    image: mysql
    ports:
      - "8306:3306"
    command: --default-authentication-plugin=mysql_native_password
    environment:
      MYSQL_DATABASE: peliculastmdb
      MYSQL_PASSWORD: test
      MYSQL_ROOT_PASSWORD: test
    volumes:
      - /appdata/dump:/docker-entrypoint-initdb.d
      - /appdata/conf:/etc/mysql/conf.d
      - /appdata/persistent:/var/lib/mysql
    networks:
      - default
    restart: unless-stopped
  www:
    image: php:8.0.0-apache
    ports:
      - "8080:80"
    volumes:
      - /appdata/www:/var/www/html
    links:
      - db
    environment:
      - DEBIAN_FRONTEND=noninteractive
    command: >
      bash -c "apt update && apt install -y sendmail libpng-dev libzip-dev zlib1g-dev libonig-dev && apt install -y nodejs && docker-php-ext-install mysqli pdo pdo_mysql && a2enmod rewrite && apache2-foreground"
    networks:
      - default
    restart: unless-stopped
  phpmyadmin:
    image: phpmyadmin/phpmyadmin
    links:
      - db:db
    ports:
      - 8000:80
    environment:
      MYSQL_USER: root
      MYSQL_PASSWORD: test
      MYSQL_ROOT_PASSWORD: test
    restart: unless-stopped
volumes:
  persistent:
```

Como no queremos que nadie no autorizado pueda crear nuevas películas, creamos una lista de control de acceso

Edit Access List

[X](#)

[Details](#) [Authorization](#) [Access](#)

Name *

Satisfy Any Pass Auth to Host

Edit Access List

[X](#)

[Details](#) [Authorization](#) [Access](#)

Basic Authorization via [Nginx HTTP Basic Authentication](#)

Username	Password
profe	p*****

Y ya por último indicamos al proxy que toda petición a nuestro dominio se redirija a nuestra dirección IP local y puerto **8080**, asignando la lista de control de acceso anteriormente creada y el certificado SSL

Edit Proxy Host X

↳ Details ↳ Custom locations ↳ SSL ↳ Advanced

Domain Names *

marchantemeco.duckdns.org

Scheme *

http

Forward Hostname / IP *

192.168.1.11

Forward Port *

8080

Cache Assets

Block Common Exploits

Websockets Support

Access List

web

Edit Proxy Host X

↳ Details ↳ Custom locations ↳ SSL ↳ Advanced

SSL Certificate

marchantemeco.duckdns.org

Force SSL

HTTP/2 Support

HSTS Enabled (?)

HSTS Subdomains

Y dado que ni el proyecto web ni la base de datos apuntan a localhost, y tenemos un proxy de por medio ¿se habrán tenido que modificar ciertos archivos? Por supuesto, los siguientes, y saber cuales son puede requerir muuuuchoo tiempo:

- /config/livewire.php

```
'asset_url' => 'https://marchantemeco.duckdns.org/public',
```

- /.env

```
APP_URL=https://marchantemeco.duckdns.org  
DB_HOST=db  
DB_PASSWORD=test
```

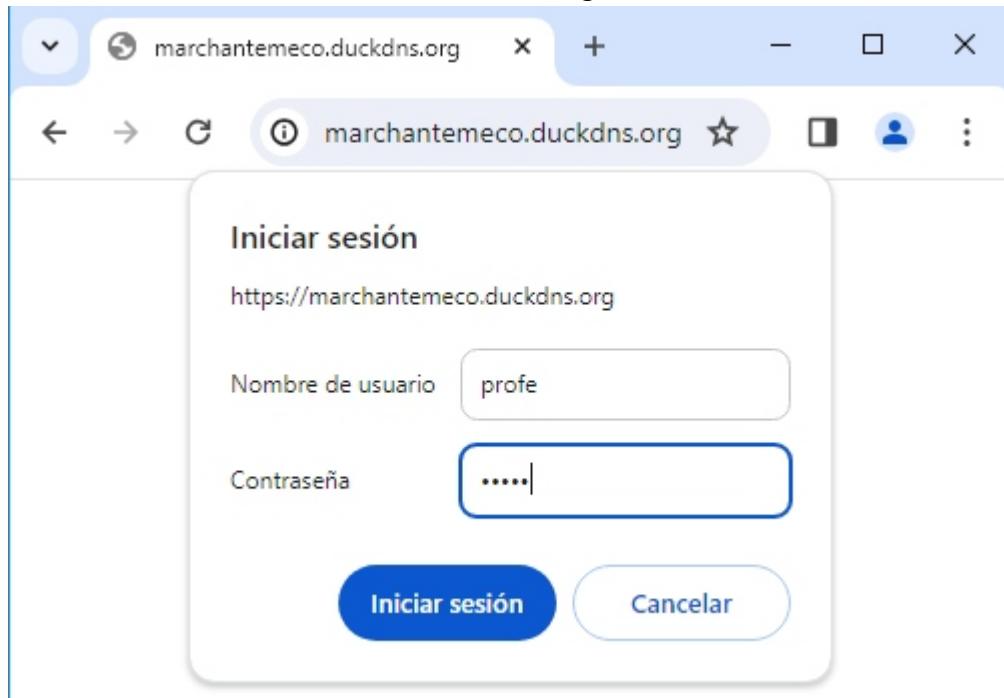
- /resources/js/insertar_con_api.js

```
"host"      : "db",  
"password"  : "test",
```

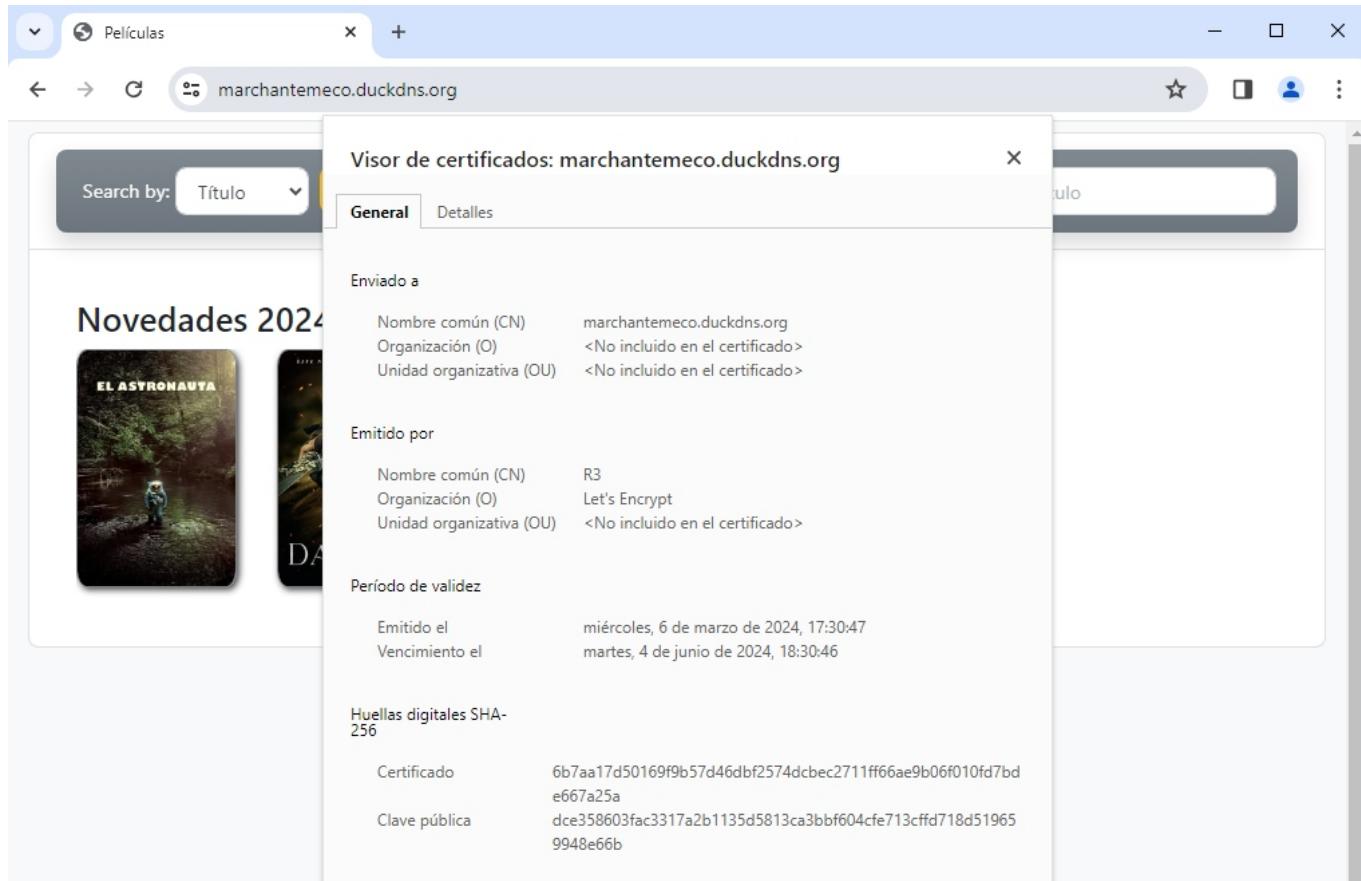
- /app/Http/Middleware/TrustProxies.php

```
protected $proxies = '*';
```

Entrando en el sitio web con autentificación Digest



Sitio web seguro mediante certificado SSL firmado por Let's Encrypt



No podía faltar un CRUD con su paginación para buscar películas en la base de datos, aunque ya veremos en

la defensa que la página es capaz de hacer muchas más cositas

Screenshot of a web browser showing a movie database interface. The URL is marchantemeco.duckdns.org/public.

The search bar includes dropdowns for "Search by:" (set to "Año"), "Nueva peli", "Nueva saga", and the total count "31 pelis". A date input field shows "1981".

The main table lists 31 movies from 1981, each with an "Actions" button, ID, year, title, and a "Saga" link. The "Caratula" column shows small thumbnail images.

ACTIONS	Id	Año	Título	Saga	Caratula
Actions	1103	1981	1997: Rescate en Nueva York	Rescate_en	
Actions	10540	1981	Atmósfera cero		
Actions	26444	1981	Caza salvaje		
Actions	387	1981	Das Boot		
Actions	23668	1981	Distrito apache: El Bronx		
Actions	46445	1981	Dos granujas en el Oeste		
Actions	44247	1981	El asesino de Rosemary		
Actions	11027	1981	El cartero siempre llama dos veces		
Actions	60794	1981	El crack	Españolas	
Actions	848	1981	El dragón del lago de fuego		
Actions	10768	1981	El final de Damien	La_profecía	
Actions	32047	1981	El príncipe de la ciudad		
Actions	48773	1981	El último combate (Game of Death II)	Bruce_Lee	
Actions	17360	1981	Evasión o victoria		
Actions	11527	1981	Excalibur		
Actions	10323	1981	Furia de titanes	Furia_de_titanes	
Actions	21610	1981	Halcones de la noche		
Actions	11281	1981	Halloween 2: Sanguinario	Halloween	

Pagination controls at the bottom left show pages 1 and 2.

Nube privada NextCloud

NextCloud también está disponible desde los ejemplos, lo cual es suficiente para un ámbito doméstico (si nuestras necesidades son más serias instalaríamos la versión oficial copiando la configuración "Base version - apache" de la página de [github](#))

 | Servicios | Compose | Archivos | Crear desde los ejemplos

mysql+phpmyadmin - mysql+phpmyadmin

navidrome - enjoy music collection from anywhere

netdata - netdata

nextcloud - Nextcloud gives you access to all your files wherever you are.

nginx - nginx

Tampoco tenemos que configurar mucho, sólo la zona horaria y la ruta a los volúmenes (escucha en el puerto **8443**)

```
version: "2.1"
services:
  nextcloud:
    image: lscr.io/linuxserver/nextcloud:latest
    container_name: nextcloud
    environment:
      - PUID=1000
      - PGID=1000
      - TZ=Europe/Madrid
    volumes:
      - /appdata/nextcloud/config:/config
      - /appdata/nextcloud/data:/data
    ports:
      - 8443:443
    restart: unless-stopped
```

Al igual que hicimos con el sitio web, indicamos al proxy que toda petición a nuestro dominio se redirija a nuestra dirección IP local y puerto **8443**, asignando el certificado SSL

Edit Proxy Host

Details Custom locations SSL Advanced

Domain Names *

merchantemeco-nextcloud.duckdns.org

Scheme *

https

Forward Hostname / IP *

192.168.1.11

Forward Port *

8443

Cache Assets

Block Common Exploits

Websockets Support

Access List

Publicly Accessible

Edit Proxy Host

Details Custom locations SSL Advanced

SSL Certificate

merchantemeco-nextcloud.duckdns.org

Force SSL

HTTP/2 Support

HSTS Enabled

HSTS Subdomains

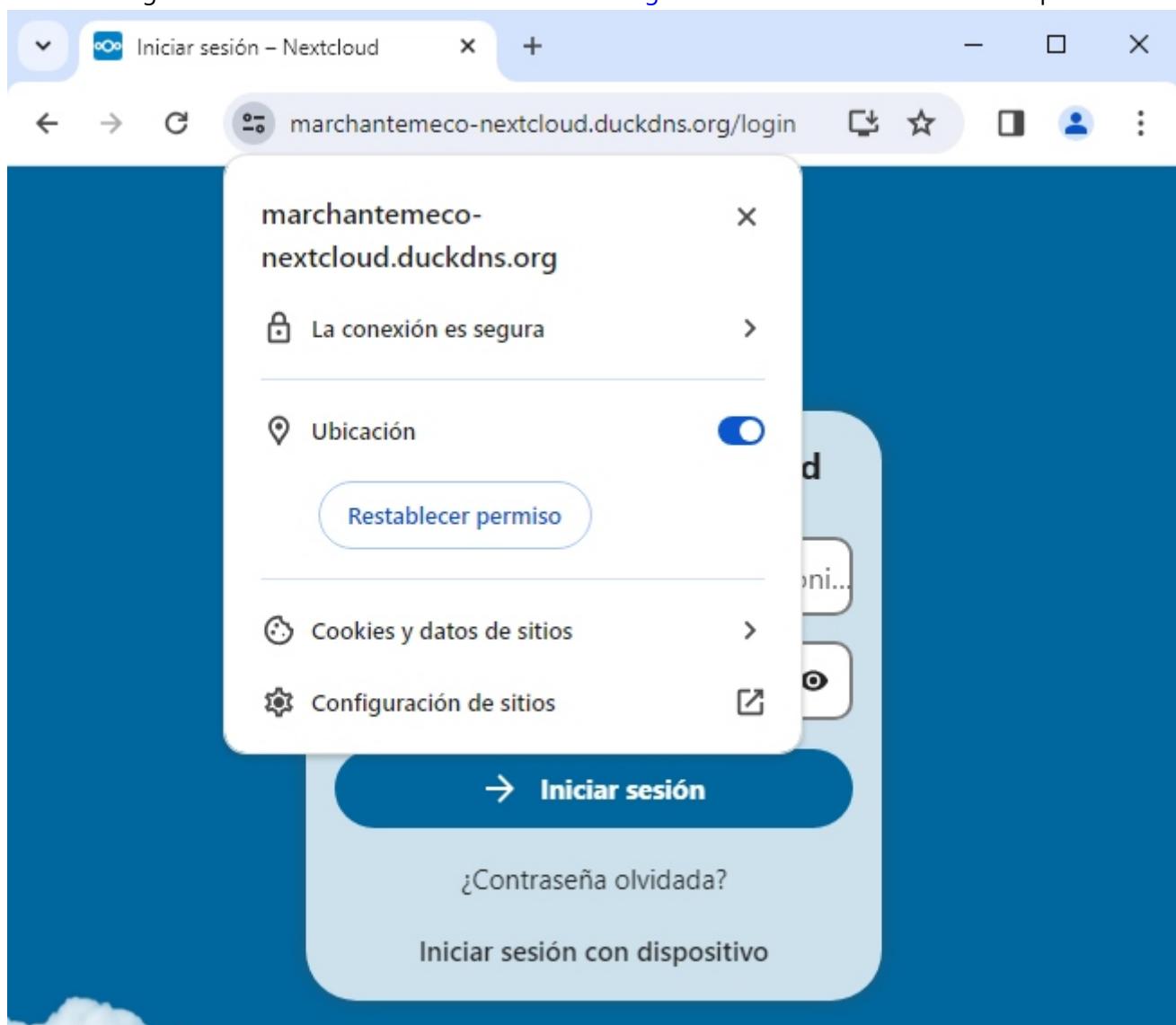
Puede que cuando accedamos con nuestro nombre de dominio nos aparezca un cartelito informándonos que no se confía en él y que editemos la configuración "trusted_domains" en config/config.php.



Para ello editaremos el archivo /appdata/nextcloud/config/www/nextcloud/config/config.php y añadimos al array trusted_domains nuestro dominio marchantemeco-nextcloud.duckdns.org

```
'trusted_domains' =>
array (
    0 => 'marchantemeco-nextcloud.duckdns.org',
),
```

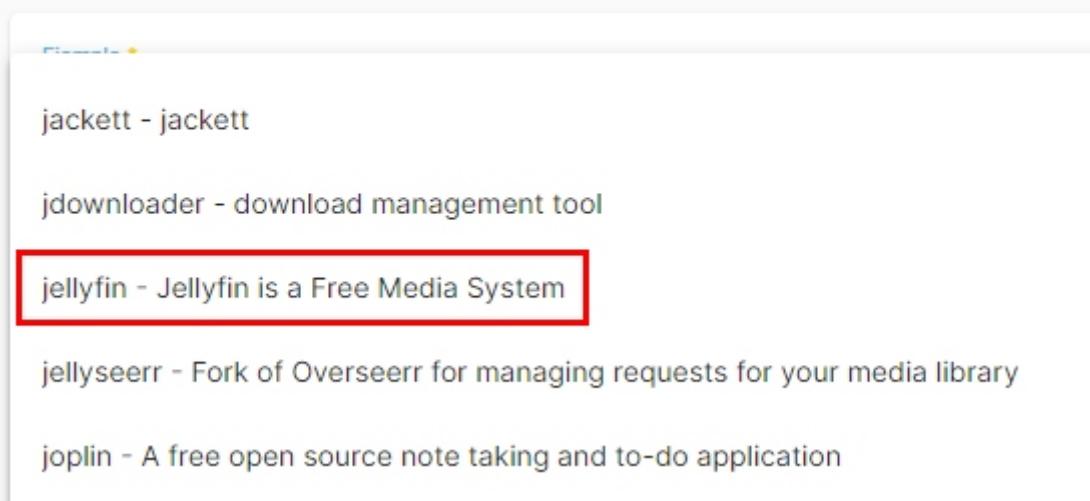
Conexión segura a marchantemeco-nextcloud.duckdns.org mediante certificado SSL firmado por Let's Encrypt



Servidor multimedia Jellyfin

Jellyfin también está disponible desde los ejemplos

 | Servicios | Compose | Archivos | Crear desde los ejemplos



Tampoco tenemos que configurar mucho, sólo la zona horaria y la ruta a los volúmenes (escucha en el puerto **8096**)

```
- PUID=1000
- PGID=100
- TZ=Europe/Madrid
#- JELLYFIN_PublishedServerUrl=192.168.0.5 #optional
volumes:
- /appdata/jellyfin/library:/config
- /appdata/jellyfin/pelis:/data/pelis
- /appdata/jellyfin/musica:/data/musica
ports:
- 8096:8096
#- 8920:8920 #optional
#- 7359:7359/udp #optional
#- 1900:1900/udp #optional
restart: unless-stopped
```

Indicamos al proxy que toda petición a nuestro dominio se redirija a nuestra dirección IP local y puerto **8096**, asignando el certificado SSL

Edit Proxy Host

Details Custom locations SSL Advanced

Domain Names *

marchantemeco-jellyfin.duckdns.org

Scheme *

http

Forward Hostname / IP *

192.168.1.11

Forward Port *

8096

Cache Assets

Block Common Exploits

Websockets Support

Access List

Publicly Accessible

Edit Proxy Host

Details Custom locations SSL Advanced

SSL Certificate

marchantemeco-jellyfin.duckdns.org

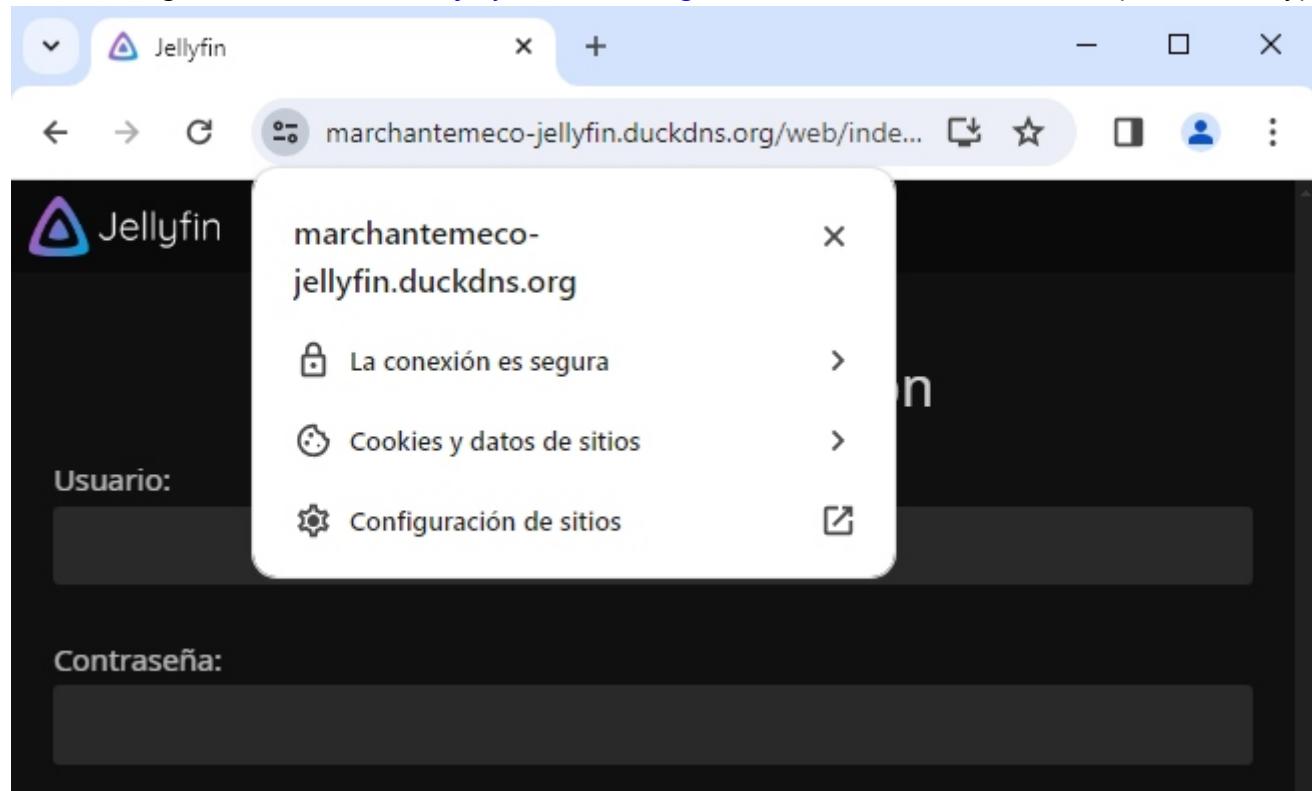
Force SSL

HTTP/2 Support

HSTS Enabled

HSTS Subdomains

Conexión segura a marchantemeco-jellyfin.duckdns.org mediante certificado SSL firmado por Let's Encrypt



Pruebas de seguridad

Vemos que a los dominios marchantemeco.duckdns.org, marchantemeco-nextcloud.duckdns.org y marchantemeco-jellyfin.duckdns.org responde nuestra dirección IP pública 188.79.149.152, la cual si introdujésemos en el navegador web y por seguridad, nos redirigiría a https://google.es

```
papi@papi-PC7176:~/Escritorio$ ping -c 1 marchantemeco.duckdns.org
PING marchantemeco.duckdns.org (188.79.149.152) 56(84) bytes of data.
64 bytes from 152.149.79.188.dynamic.jazztel.es (188.79.149.152): icmp_seq=1 ttl=63 time=1.70 ms

--- marchantemeco.duckdns.org ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.702/1.702/1.702/0.000 ms
papi@papi-PC7176:~/Escritorio$ ping -c 1 marchantemeco-nextcloud.duckdns.org
PING marchantemeco-nextcloud.duckdns.org (188.79.149.152) 56(84) bytes of data.
64 bytes from 152.149.79.188.dynamic.jazztel.es (188.79.149.152): icmp_seq=1 ttl=63 time=1.68 ms

--- marchantemeco-nextcloud.duckdns.org ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.680/1.680/1.680/0.000 ms
papi@papi-PC7176:~/Escritorio$ ping -c 1 marchantemeco-jellyfin.duckdns.org
PING marchantemeco-jellyfin.duckdns.org (188.79.149.152) 56(84) bytes of data.
64 bytes from 152.149.79.188.dynamic.jazztel.es (188.79.149.152): icmp_seq=1 ttl=63 time=1.68 ms

--- marchantemeco-jellyfin.duckdns.org ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.675/1.675/1.675/0.000 ms
papi@papi-PC7176:~/Escritorio$
```

- Primero vamos a escanear la dirección IP pública:

```
sudo nmap -v -A 188.79.149.152
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-02 14:07 CEST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:07
Completed NSE at 14:07, 0.00s elapsed
Initiating NSE at 14:07
Completed NSE at 14:07, 0.00s elapsed
Initiating NSE at 14:07
Completed NSE at 14:07, 0.00s elapsed
Initiating Ping Scan at 14:07
Scanning 188.79.149.152 [2 ports]
Completed Ping Scan at 14:07, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:07
Completed Parallel DNS resolution of 1 host. at 14:07, 0.00s elapsed
Initiating Connect Scan at 14:07
Scanning 152.149.79.188.dynamic.jazztel.es (188.79.149.152) [1000 ports]
Discovered open port 80/tcp on 188.79.149.152
Discovered open port 443/tcp on 188.79.149.152
Completed Connect Scan at 14:07, 4.05s elapsed (1000 total ports)
Initiating Service scan at 14:07
Scanning 2 services on 152.149.79.188.dynamic.jazztel.es (188.79.149.152)
Completed Service scan at 14:07, 17.41s elapsed (2 services on 1 host)
NSE: Script scanning 188.79.149.152.
Initiating NSE at 14:07
Completed NSE at 14:07, 0.54s elapsed
Initiating NSE at 14:07
```

```
Completed NSE at 14:07, 0.19s elapsed
Initiating NSE at 14:07
Completed NSE at 14:07, 0.00s elapsed
Nmap scan report for 152.149.79.188.dynamic.jazztel.es (188.79.149.152)
Host is up (0.0077s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    OpenResty web app server
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: openresty
|_http-title: Did not follow redirect to https://google.es
443/tcp   open  ssl/http OpenResty web app server
|_http-server-header: openresty
|_http-title: 400 The plain HTTP request was sent to HTTPS port
| ssl-cert: Subject: commonName=localhost/organizationName=localhost
| Issuer: commonName=localhost/organizationName=localhost
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-03-15T11:17:22
| Not valid after:  2034-03-13T11:17:22
| MD5:   5f42 84de 6ef7 8aa2 1d29 49f4 2f19 26af
|_SHA-1: 236c 8839 99bd 76eb 9086 d7ea 5948 e2ce ac2e f76e
```

```
NSE: Script Post-scanning.
Initiating NSE at 14:07
Completed NSE at 14:07, 0.00s elapsed
Initiating NSE at 14:07
Completed NSE at 14:07, 0.00s elapsed
Initiating NSE at 14:07
Completed NSE at 14:07, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.38 seconds
```

```
sudo nmap -Pn -n -sV -O 188.79.149.152
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-02 14:15 CEST
Nmap scan report for 188.79.149.152
Host is up (0.0019s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    OpenResty web app server
443/tcp   open  ssl/http OpenResty web app server
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (93%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway
```

(93%)

No exact OS matches for host (test conditions non-ideal).

No ha conseguido sacar la versión del servidor web ni el sistema operativo que lo aloja, sólo que por el puerto 80 redirige a https://google.es, y por el puerto 443 devuelve un error 400 Bad Request (o sea, no responde).

Los hackers lo van a tener difícil.

- Ahora vamos a escanear los servicios:
 - marchantemeco.duckdns.org

```
sudo nmap -v -A marchantemeco.duckdns.org
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-02 14:39 CEST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:39
Completed NSE at 14:39, 0.00s elapsed
Initiating NSE at 14:39
Completed NSE at 14:39, 0.00s elapsed
Initiating NSE at 14:39
Completed NSE at 14:39, 0.00s elapsed
Initiating Ping Scan at 14:39
Scanning marchantemeco.duckdns.org (188.79.149.152) [4 ports]
Completed Ping Scan at 14:39, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:39
Completed Parallel DNS resolution of 1 host. at 14:39, 0.00s elapsed
Initiating SYN Stealth Scan at 14:39
Scanning marchantemeco.duckdns.org (188.79.149.152) [1000 ports]
Discovered open port 80/tcp on 188.79.149.152
Discovered open port 443/tcp on 188.79.149.152
Increasing send delay for 188.79.149.152 from 0 to 5 due to
max_successful_tryno increase to 4
Completed SYN Stealth Scan at 14:40, 51.81s elapsed (1000 total ports)
Initiating Service scan at 14:40
Scanning 2 services on marchantemeco.duckdns.org (188.79.149.152)
Completed Service scan at 14:40, 17.31s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against marchantemeco.duckdns.org
(188.79.149.152)
Retrying OS detection (try #2) against marchantemeco.duckdns.org
(188.79.149.152)
Initiating Traceroute at 14:40
Completed Traceroute at 14:40, 0.02s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 14:40
Completed Parallel DNS resolution of 2 hosts. at 14:40, 0.10s elapsed
NSE: Script scanning 188.79.149.152.
Initiating NSE at 14:40
Completed NSE at 14:40, 0.51s elapsed
Initiating NSE at 14:40
Completed NSE at 14:40, 0.15s elapsed
Initiating NSE at 14:40
Completed NSE at 14:40, 0.00s elapsed
```

```
Nmap scan report for marchantemeco.duckdns.org (188.79.149.152)
Host is up (0.0020s latency).
rDNS record for 188.79.149.152: 152.149.79.188.dynamic.jazztel.es
Not shown: 993 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   OpenResty web app server
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: openresty
|_http-title: Did not follow redirect to https://marchantemeco.duckdns.org/
443/tcp   open  ssl/http OpenResty web app server
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_ Basic realm=Authorization required
|_http-server-header: openresty
|_http-title: 401 Authorization Required
| ssl-cert: Subject: commonName=marchantemeco.duckdns.org
| Subject Alternative Name: DNS:marchantemeco.duckdns.org
| Issuer: commonName=R3/organizationName=Let's Encrypt/countryName=US
| Public Key type: ec
| Public Key bits: 384
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-03-06T16:30:47
| Not valid after:  2024-06-04T16:30:46
| MD5:   f72b f7b9 fb9c be82 b5a2 89b2 4988 9d7c
|_SHA-1: e7ff 765e 331c 594e b9d5 1f6d 6494 26cc 96c8 abfd
2006/tcp closed invokator
2007/tcp closed dectalk
2323/tcp closed 3d-nfsd
8000/tcp closed http-alt
8443/tcp closed https-alt
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (97%), QEMU (93%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (97%), QEMU user mode network
gateway (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=17 (Good luck!)
IP ID Sequence Generation: Incremental

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  0.40 ms _gateway (10.0.2.2)
2  0.48 ms 152.149.79.188.dynamic.jazztel.es (188.79.149.152)

NSE: Script Post-scanning.
Initiating NSE at 14:40
Completed NSE at 14:40, 0.00s elapsed
Initiating NSE at 14:40
Completed NSE at 14:40, 0.00s elapsed
Initiating NSE at 14:40
Completed NSE at 14:40, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
```

```
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 75.83 seconds
    Raw packets sent: 6066 (269.876KB) | Rcvd: 126 (5.612KB)
```

```
sudo nmap -Pn -n -sV -O marchantemeco.duckdns.org
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-02 14:43 CEST
Nmap scan report for marchantemeco.duckdns.org (188.79.149.152)
Host is up (0.0030s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    OpenResty web app server
443/tcp   open  ssl/http OpenResty web app server
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (93%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network
gateway (93%)
No exact OS matches for host (test conditions non-ideal).
```

```
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.43 seconds
```

- marchantemeco-nextcloud.org

```
sudo nmap -v -A marchantemeco-nextcloud.duckdns.org
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-02 16:06 CEST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:06
Completed NSE at 16:06, 0.00s elapsed
Initiating NSE at 16:06
Completed NSE at 16:06, 0.00s elapsed
Initiating NSE at 16:06
Completed NSE at 16:06, 0.00s elapsed
Initiating Ping Scan at 16:06
Scanning marchantemeco-nextcloud.duckdns.org (188.79.149.152) [4 ports]
Completed Ping Scan at 16:06, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:06
Completed Parallel DNS resolution of 1 host. at 16:06, 0.01s elapsed
Initiating SYN Stealth Scan at 16:06
Scanning marchantemeco-nextcloud.duckdns.org (188.79.149.152) [1000 ports]
Discovered open port 443/tcp on 188.79.149.152
Discovered open port 80/tcp on 188.79.149.152
Completed SYN Stealth Scan at 16:06, 5.00s elapsed (1000 total ports)
Initiating Service scan at 16:06
```

```
Scanning 2 services on marchantemeco-nextcloud.duckdns.org (188.79.149.152)
Completed Service scan at 16:06, 17.45s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against marchantemeco-nextcloud.duckdns.org
(188.79.149.152)
Retrying OS detection (try #2) against marchantemeco-nextcloud.duckdns.org
(188.79.149.152)
Initiating Traceroute at 16:06
Completed Traceroute at 16:06, 0.03s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 16:06
Completed Parallel DNS resolution of 2 hosts. at 16:06, 0.01s elapsed
NSE: Script scanning 188.79.149.152.
Initiating NSE at 16:06
Completed NSE at 16:06, 0.37s elapsed
Initiating NSE at 16:06
Completed NSE at 16:06, 0.15s elapsed
Initiating NSE at 16:06
Completed NSE at 16:06, 0.00s elapsed
Nmap scan report for marchantemeco-nextcloud.duckdns.org (188.79.149.152)
Host is up (0.00096s latency).
rDNS record for 188.79.149.152: 152.149.79.188.dynamic.jazztel.es
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    OpenResty web app server
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: openresty
|_http-title: Did not follow redirect to https://marchantemeco-
nextcloud.duckdns.org/
443/tcp   open  ssl/http OpenResty web app server
|_http-server-header: openresty
|_http-title: 502 Bad Gateway
| ssl-cert: Subject: commonName=marchantemeco-nextcloud.duckdns.org
| Subject Alternative Name: DNS:marchantemeco-nextcloud.duckdns.org
| Issuer: commonName=R3/organizationName=Let's Encrypt/countryName=US
| Public Key type: ec
| Public Key bits: 384
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-03-06T16:39:54
| Not valid after: 2024-06-04T16:39:53
| MD5: 39d7 f017 90ec 678f d62b a9e3 8291 2897
|_SHA-1: 022a 8d5e 0f3d 425f e878 185e 3551 80d7 643e 6b5a
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (93%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network
gateway (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=17 (Good luck!)
IP ID Sequence Generation: Incremental

TRACEROUTE (using port 80/tcp)
```

```
HOP RTT      ADDRESS
1  0.58 ms _gateway (10.0.2.2)
2  0.48 ms 152.149.79.188.dynamic.jazztel.es (188.79.149.152)

NSE: Script Post-scanning.
Initiating NSE at 16:06
Completed NSE at 16:06, 0.00s elapsed
Initiating NSE at 16:06
Completed NSE at 16:06, 0.00s elapsed
Initiating NSE at 16:06
Completed NSE at 16:06, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.92 seconds
```

```
sudo nmap -Pn -n -sV -O marchantemeco-nextcloud.duckdns.org
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-02 16:09 CEST
Nmap scan report for marchantemeco-nextcloud.duckdns.org (188.79.149.152)
Host is up (0.0015s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    OpenResty web app server
443/tcp   open  ssl/http OpenResty web app server
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (93%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network
gateway (93%)
No exact OS matches for host (test conditions non-ideal).

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.46 seconds
```

- [marchantemeco-jellyfin.org](#)

```
sudo nmap -v -A marchantemeco-jellyfin.duckdns.org
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-02 16:11 CEST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:11
Completed NSE at 16:11, 0.00s elapsed
Initiating NSE at 16:11
Completed NSE at 16:11, 0.00s elapsed
Initiating NSE at 16:11
Completed NSE at 16:11, 0.00s elapsed
```

```
Initiating Ping Scan at 16:11
Scanning marchantemeco-jellyfin.duckdns.org (188.79.149.152) [4 ports]
Completed Ping Scan at 16:11, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:11
Completed Parallel DNS resolution of 1 host. at 16:11, 0.00s elapsed
Initiating SYN Stealth Scan at 16:11
Scanning marchantemeco-jellyfin.duckdns.org (188.79.149.152) [1000 ports]
Discovered open port 80/tcp on 188.79.149.152
Discovered open port 443/tcp on 188.79.149.152
Completed SYN Stealth Scan at 16:11, 5.15s elapsed (1000 total ports)
Initiating Service scan at 16:11
Scanning 2 services on marchantemeco-jellyfin.duckdns.org (188.79.149.152)
Completed Service scan at 16:11, 17.41s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against marchantemeco-jellyfin.duckdns.org
(188.79.149.152)
Retrying OS detection (try #2) against marchantemeco-jellyfin.duckdns.org
(188.79.149.152)
Initiating Traceroute at 16:11
Completed Traceroute at 16:11, 0.03s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 16:11
Completed Parallel DNS resolution of 2 hosts. at 16:11, 0.00s elapsed
NSE: Script scanning 188.79.149.152.
Initiating NSE at 16:11
Completed NSE at 16:11, 0.50s elapsed
Initiating NSE at 16:11
Completed NSE at 16:11, 0.16s elapsed
Initiating NSE at 16:11
Completed NSE at 16:11, 0.00s elapsed
Nmap scan report for marchantemeco-jellyfin.duckdns.org (188.79.149.152)
Host is up (0.00066s latency).
rDNS record for 188.79.149.152: 152.149.79.188.dynamic.jazztel.es
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    OpenResty web app server
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: openresty
|_http-title: Did not follow redirect to https://marchantemeco-
jellyfin.duckdns.org/
443/tcp   open  ssl/http OpenResty web app server
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: openresty
| http-title: Jellyfin
|_Requested resource was /web/index.html
| ssl-cert: Subject: commonName=marchantemeco-jellyfin.duckdns.org
| Subject Alternative Name: DNS:marchantemeco-jellyfin.duckdns.org
| Issuer: commonName=R3/organizationName=Let's Encrypt/countryName=US
| Public Key type: ec
| Public Key bits: 384
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-04-01T17:51:00
```

```
| Not valid after: 2024-06-30T17:50:59
| MD5: 7872 8072 2724 f947 50ab c690 0845 838e
|_SHA-1: 6e1b d2d7 c8ff 6f3b f8f1 57b8 cf9e d0e3 3b2a 5138
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (93%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network
gateway (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=17 (Good luck!)
IP ID Sequence Generation: Incremental

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  0.30 ms  _gateway (10.0.2.2)
2  0.37 ms  152.149.79.188.dynamic.jazztel.es (188.79.149.152)

NSE: Script Post-scanning.
Initiating NSE at 16:11
Completed NSE at 16:11, 0.00s elapsed
Initiating NSE at 16:11
Completed NSE at 16:11, 0.00s elapsed
Initiating NSE at 16:11
Completed NSE at 16:11, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.28 seconds
    Raw packets sent: 2059 (93.748KB) | Rcvd: 58 (2.892KB)
```

```
sudo nmap -Pn -n -sV -O marchantemeco-jellyfin.duckdns.org
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-02 16:16 CEST
Nmap scan report for marchantemeco-jellyfin.duckdns.org (188.79.149.152)
Host is up (0.0015s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    OpenResty web app server
443/tcp   open  ssl/http OpenResty web app server
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (93%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network
gateway (93%)
No exact OS matches for host (test conditions non-ideal).

OS and Service detection performed. Please report any incorrect results at
```

```
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.72 seconds
```

Por el puerto 80 redirigen a la conexión segura https, y por el puerto 443 tenemos la conexión segura mediante certificado SSL firmado por Let's Encrypt.

Sigue sin conseguir sacar la versión del servidor web ni el sistema operativo que lo aloja, por lo que va a ser difícil que un hacker sepa por dónde meterle mano.

VPN

Para probar la VPN conectaremos el cliente a internet (sería absurdo hacerlo a través de nuestro propio router, por lo que lo haremos a través de una red WIFI pública), y activaremos la conexión VPN Wireguard para poder ser un equipo más de nuestra red local (192.168.1.0/24).

La publicidad será bloqueada mediante PiHole, por lo que si además configuramos los equipos de nuestra red local como servidor DNS al equipo OpenMediaVault (192.168.1.11) estaremos bloqueando la publicidad para todos ellos de manera fácil y transparente.

- Wireguard + PiHole:

```
version: "3.8"
services:
  wg-easy:
    environment:
      - LANG=es
      # Change this to your host's public address
      - WG_HOST=marchantemeco.duckdns.org
      # Web UI Password:
      - PASSWORD=test
      - WG_DEFAULT_ADDRESS=10.8.0.x
      - WG_DEFAULT_DNS=10.8.1.3
      - WG_PERSISTENT_KEEPALIVE=25
      # - WG_MTU=1420
      - WG_ALLOWED_IPS=192.168.1.0/24, 0.0.0.0/1, 128.0.0.0/1
    image: ghcr.io/wg-easy/wg-easy
    container_name: wg-easy
    volumes:
      - /appdata/wireguard:/etc/wireguard
    ports:
      # Abrir en el router
      - "51820:51820/udp"
      # Puerto de administración localmente
      - "51821:51821/tcp"
    restart: unless-stopped
    cap_add:
      - NET_ADMIN
      - SYS_MODULE
    sysctl:
      - net.ipv4.ip_forward=1
      - net.ipv4.conf.all.src_valid_mark=1
    networks:
      wg-easy:
        ipv4_address: 10.8.1.2
  pihole:
    image: pihole/pihole
    container_name: pihole
    environment:
      # Web UI Password:
      - WEBPASSWORD=test
    volumes:
      - '/appdata/pihole/etc-pihole:/etc/pihole'
```

```

- '/appdata/pihole/etc-dnsmasq.d:/etc/dnsmasq.d'
ports:
- "53:53/tcp"
- "53:53/udp"
# Puerto administración localmente
- "5353:80/tcp"
restart: unless-stopped
networks:
wg-easy:
    ipv4_address: 10.8.1.3
networks:
wg-easy:
    ipam:
    config:
        - subnet: 10.8.1.0/24

```

- Creamos el cliente en el servidor:

WireGuard

Cerrar sesión ↗

Clients

+ Nuevo

vpn_portatil	10.8.0.2	↓ 0 B/s · ↑ 0 B/s · hace 1 minuto				
--------------	----------	-----------------------------------	--	--	--	--

- Instalamos la aplicación Wireguard en el cliente, cargamos la configuración y activamos la conexión VPN:

Túneles Registro

vpn_portatil

Interfaz: vpn_portatil
Estado: Activo
Clave pública: konDoyRC6zxdq2l6AHWO+y5zFtVp10iEvSP9Q2RaST8=
Puerto de escucha: 58668
Direcciones: 10.8.0.2/24
Servidores DNS: 10.8.1.3

Desactivar

Pares

Clave pública: MpARTxNSh0wakl3KAc8j5kZfMB1gJX8M/8QQ2CPFzTM=
Clave compartida: activado
IPs permitidas: 0.0.0.0/1[EnumerationSeparator]128.0.0.0/1[EnumerationSeparator]192.168.1.0/24
Endpoint: 188.79.149.152:51820
Persistent keepalive: 25
Último saludo: hace 36 segundos
Transferir: 2,11 MiB received, 600,81 KiB sent

- Comprobamos en el cliente las conexiones y que llegamos al equipo de nuestra red local OpenMediaVault (192.168.1.11):

Windows PowerShell

PS C:\Users\Papi> ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

Estado de los medios. : medios desconectados
Sufijo DNS específico para la conexión. . . : home

Adaptador desconocido vpn_portatil:

Sufijo DNS específico para la conexión. . .
Dirección IPv4. : 10.8.0.2
Máscara de subred : 255.255.255.0
Puerta de enlace predeterminada :

Adaptador de LAN inalámbrica Wi-Fi:

Sufijo DNS específico para la conexión. . . : home
Dirección IPv4. : 192.168.1.128
Máscara de subred : 255.255.255.0
Puerta de enlace predeterminada : 192.168.1.1

Adaptador de túnel Teredo Tunneling Pseudo-Interface:

Sufijo DNS específico para la conexión. . .
Dirección IPv6 : 2001:0:2851:782c:3c76:43b0:6a67
Vínculo: dirección IPv6 local. : fe80::3458:3c76:43b0:6a67%2
Puerta de enlace predeterminada :

Adaptador de túnel isatap.home:

Estado de los medios. : medios desconectados
Sufijo DNS específico para la conexión. . . : home

Adaptador de túnel isatap.{3B9746CF-9A1C-B240-BA9F-FC7000D56BA3}:

Estado de los medios. : medios desconectados
Sufijo DNS específico para la conexión. . . :

PS C:\Users\Papi> Invoke-WebRequest ifconfig.me/ip

```
StatusCode : 200
StatusDescription : OK
Content : 188.79.149.152
RawContent : HTTP/1.1 200 OK
access-control-allow-origin: *
Content-Length: 14
Content-Type: text/plain
Date: Tue, 09 Apr 2024 14:11:09 GMT
Server: fasthttp
Via: 1.1 google
188.79.149.152
Forms : {}
Headers : {[access-control-allow-origin, *], [Content-Length, 14], [Content-Type, text/plain], [Date, Tue, 09 Apr 2024 14:11:09 GMT]...}
Images : {}
InputFields : {}
Links : {}
ParsedHtml : System.__ComObject
RawContentLength : 14
```

PS C:\Users\Papi> ping -n 1 192.168.1.11

Haciendo ping a 192.168.1.11 con 32 bytes de datos:
Respuesta desde 192.168.1.11: bytes=32 tiempo=25ms TTL=63

Estadísticas de ping para 192.168.1.11:
Paquetes: enviados = 1, recibidos = 1, perdidos = 0
(0% perdidos).
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 25ms, Máximo = 25ms, Media = 25ms

- Comprobamos en el equipo OpenMediaVault que su dirección IP pública es 188.79.149.152 y que se están bloqueando los ads:

The screenshot shows a terminal window titled "Seleccionar OpenSSH SSH client". The terminal output is as follows:

```
root@omv:~# curl ifconfig.me
188.79.149.152root@omv:~#
root@omv:~# dig @192.168.1.11 ads.google.com

; <>> DiG 9.16.48-Debian <>> @192.168.1.11 ads.google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4944
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;ads.google.com.           IN      A          0.0.0.0

;; ANSWER SECTION:
ads.google.com.        2       IN      A          0.0.0.0

;; Query time: 0 msec
;; SERVER: 192.168.1.11#53(192.168.1.11)
;; WHEN: Tue Apr 09 17:12:08 CEST 2024
;; MSG SIZE  rcvd: 59
```

Conclusiones y ampliación

Proyecto desde mi punto de vista interesante en el que se pone en práctica casi todo lo aprendido en el ciclo y se nos da a conocer esa fantástica aplicación llamada Nginx Proxy Manager.

Ante rotura de los discos sería fácil volver a crear los contenedores pero, ¿qué pasa con los datos?

Se me queda en el tintero probar la aplicación de backup [duplicati](#)

Referencias

[Creo una Nube para mi Amigo con una PC antigua y con Discos Duros Viejos | OpenMediaVault SERVER](#)

[Creo una Nube de MÁS de 2 Terabyte con una PC antigua y con Discos Duros Viejos | CasaOS SERVER](#)

[Le demos SEGURIDAD a nuestra NUBE PRIVADA para acceder desde cualquier parte mundo OpenMediaVault](#)

[Creo una Nube Casera con pc viejo](#)

[INSTALA tu VPN personal SIN ADS! con Wireguard + PiHole](#)