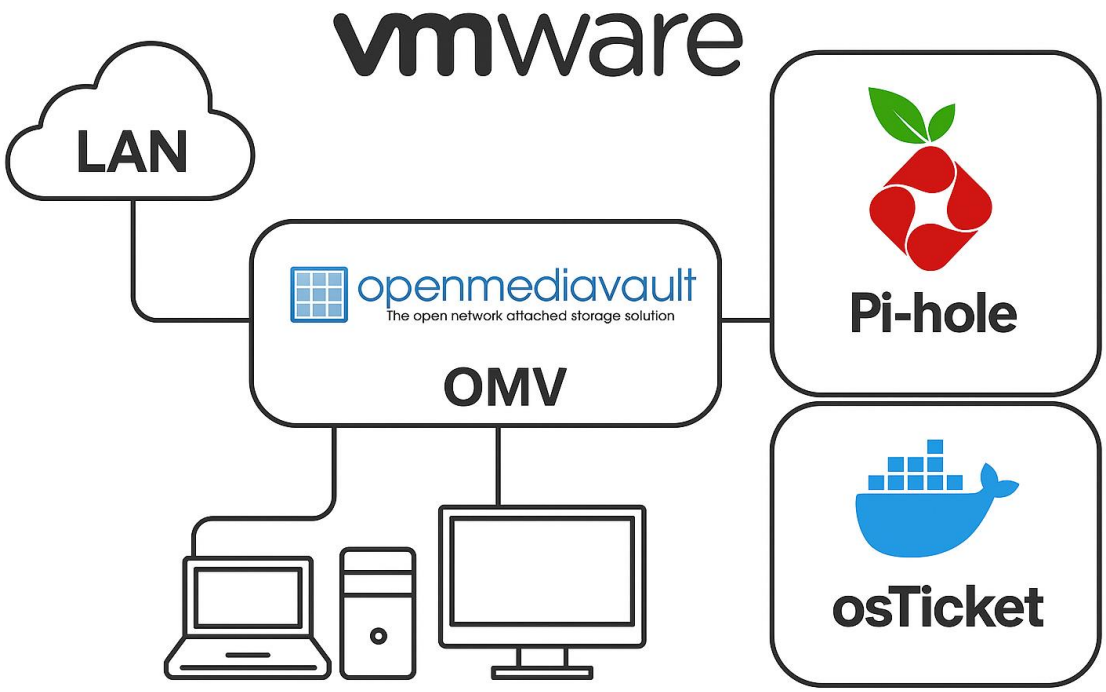
Introduction to infrastructures

Assignments 2025 - 2026



SAXION
UNIVERSITY OF
APPLIED SCIENCES

Version: 20250709.1449.MSI11

Contents

0 Business Case: Transition to a Linux-Based IT Infrastructure – Municipality of Enschede

This chapter presents the business case and helps with the preparation for the assignment.

0.1 The business case

Several cities and regions in Northern Europe are successfully adopting open-source software to reduce costs, increase control over their data, and improve efficiency. For instance, Copenhagen and Aarhus in Denmark have migrated many of their services away from proprietary software, achieving significant cost savings. Similarly, Schleswig-Holstein in Germany has replaced Windows and Office with Linux, LibreOffice, and Nextcloud to enhance security and data privacy. Inspired by these examples, the Municipality of Enschede should explore the possibility of moving to a Linux-based infrastructure to modernize its IT systems.

Objective

To explore the feasibility of transitioning to a Linux-based server and client infrastructure for the Municipality of Enschede, with a focus on reducing reliance on proprietary software vendors, improving digital sovereignty, and enabling cost-effective, scalable IT management.

Background

Public organizations in the Netherlands, including municipalities, are encouraged to embrace open-source technologies in alignment with national and EU digital autonomy strategies. Proprietary software can be costly, restrictive, and opaque, while open-source alternatives offer greater flexibility, transparency, and control.

Proposal

This initiative proposes the development of a **virtualized proof of concept** that demonstrates the core components of a Linux-based IT environment:

- **Server**: **Open Media Vault (OMV)** will serve as the municipality's **Network Attached Storage (NAS) system,** providing file services, user management, and Docker-based application hosting.
- **Containerization**: Deploy key apps (e.g., osTicket, Pi-hole) via **Docker containers** inside OMV to show modular service deployment.
- **Client**: A Linux-based desktop (e.g., Ubuntu or Linux Mint) will connect to the OMV server to access services and resources.
- **Nextcloud**: The Municipality is also interested in exploring Nextcloud as a collaboration platform. To assess its suitability and capabilities, Nextcloud will be first deployed and tested on an **Azure Virtual Machine**. This cloud-based test will help understand scalability, integration options, and performance before considering local deployment.

Proof of Concept (PoC) – Virtualized Setup

To be developed within **VMware Workstation Pro** as a controlled and reproducible environment:

- One virtual machine (VM) running **Open Media Vault** as the server.
- One or more VMs running a **Linux desktop OS** as client systems.
- Docker containers deployed within OMV for key services.
- Nextcloud deployed on an Azure Linux VM to test collaboration capabilities.
- Network configuration and access simulated within VMware to mimic real-world use.

Benefits for the Municipality of Enschede

- **Cost Savings**: No license fees for OS and core services.
- **Vendor Independence**: Reduced lock-in with proprietary platforms.
- **Modular Scalability**: Easily expand functionality via Docker containers.
- **Data Control**: Full ownership and visibility over municipal data.
- **Eco-Friendly**: Efficient software enables longer hardware lifespans.

Next Steps

1. Build and document the Proof of Concept(PoC) using VMware Workstation Pro.
2. Test client-server interaction, container deployment, and usability.
3. Deploy Nextcloud on an Azure VM and evaluate its capabilities.
4. Analyse performance, manageability, and potential for scaling.
5. Present recommendations for future pilot programs or phased implementation.

Transitioning to a Linux-based IT infrastructure offers the Municipality of Enschede a strategic opportunity to reduce costs, increase control over its digital assets, and improve operational flexibility. By leveraging proven open-source solutions such as Open Media Vault and Nextcloud that have already been successfully adopted by leading municipalities in Northern Europe, Enschede can modernize its IT environment in alignment with national and EU objectives for digital sovereignty. The proposed proof of concept will provide valuable insights into the technical feasibility and benefits of this approach and lay the groundwork for a sustainable, scalable, and cost-effective IT future for the municipality.

0.2 Download the required ISOs

- Debian 12: https://www.debian.org/CD/netinst/
- Ubuntu 24.04 Desktop: https://cdimage.ubuntu.com/noble/daily-live/current/

0.3 Install VMware

- Read this blogpost: https://www.mikeroysoft.com/post/download-fusion-ws/
- Register at www.broadcom.com
- Download & Install the newest version of VMware Workstation Pro or VMware Fusion Pro

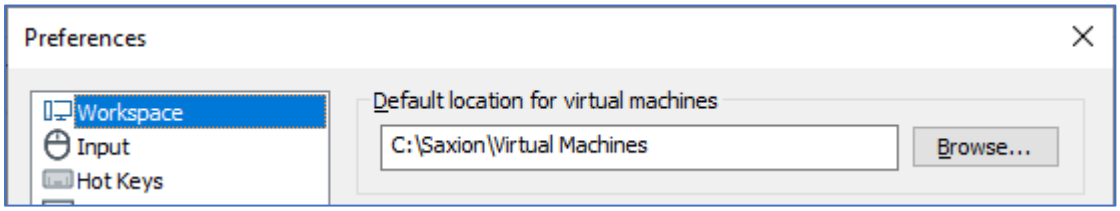
0.4 Folders

- Create a folder called **Saxion** on your biggest and fastest(ssd) hard drive
- Create a subfolder called **ISO** in the Saxion folder
    - Copy the downloaded ISOs into the **ISO** folder
- Create another subfolder called **Virtual Machines** in the Saxion folder

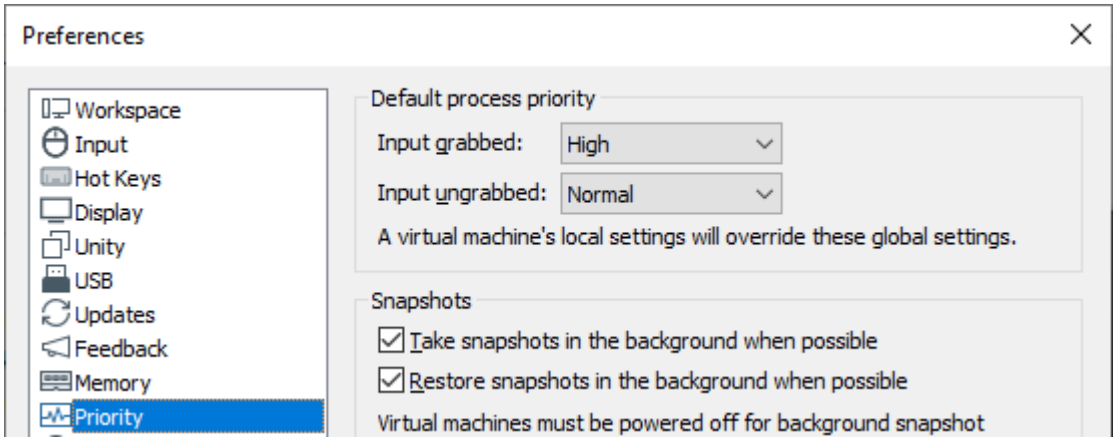
0.5 VMware Preferences

Once VMware is installed edit the preferences of VMware.

Set Default location for virtual machines to the **Virtual Machines** folder you've created.



Set priority on High if the Input is grabbed.



Click on the OK button.

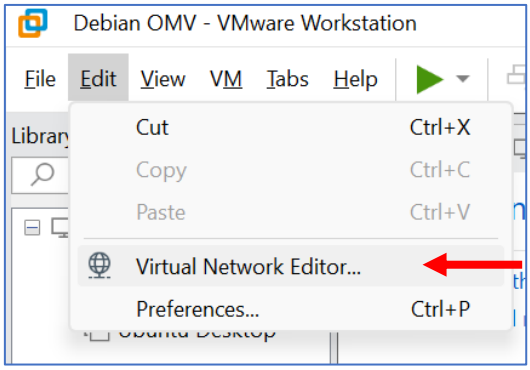
0.6 What is the Open Media Vault?

Do research and find out what the Open Media Vault is. Focus specifically on file sharing. We want to implement this system for the municipality of Enschede. Then fill in the quality requirements table in the template report. What do you think the quality requirements should be for this system. Fill in the **Requirement** and **Explanation** columns.

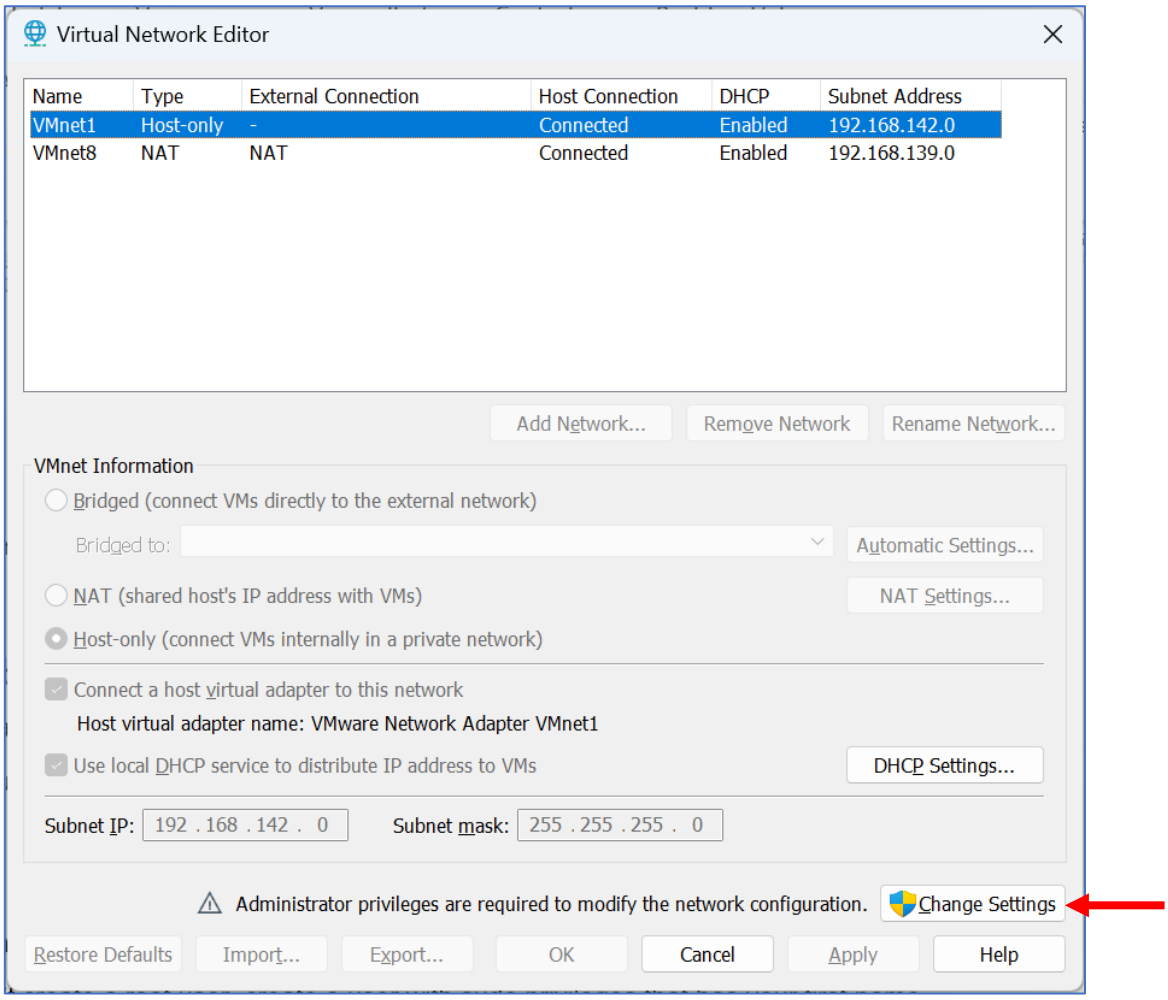
1 Week 1: Setting up a client/server architecture

Prerequisite: You have successfully installed VMware Workstation Pro.

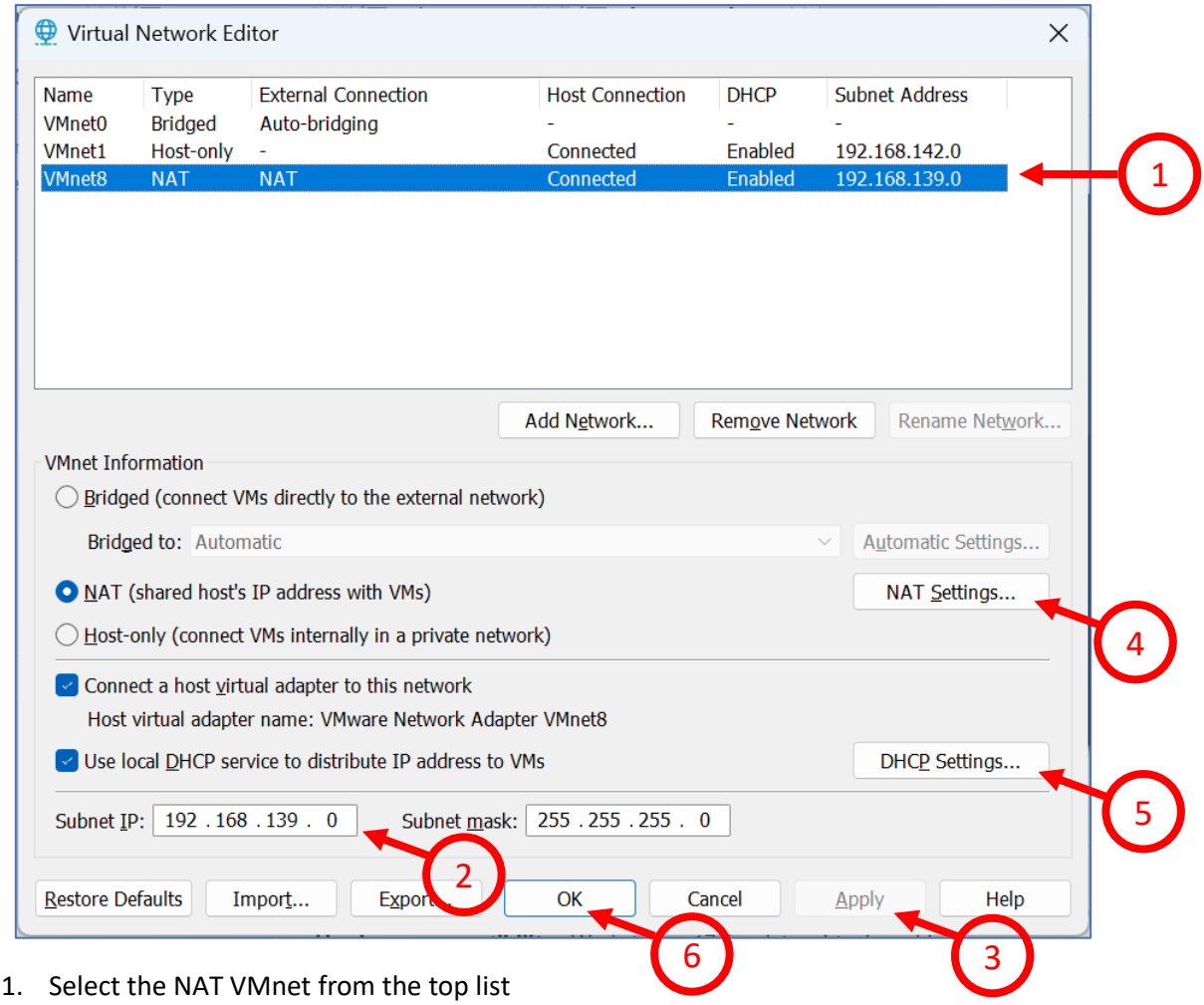
1.1 VMware Workstation Pro network settings



Open the Virtual Network Editor in VMware Workstation



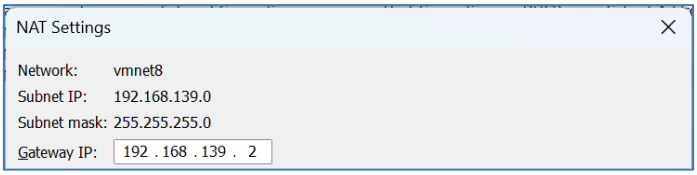
Click on Change Settings.



1. Select the NAT VMnet from the top list
2. Change the Subnet IP to **192.168.139.0**
3. Click on the button Apply
4. Click on the button NAT Settings.

Here you can see what your **Gateway** IP address is. It should now be set to:

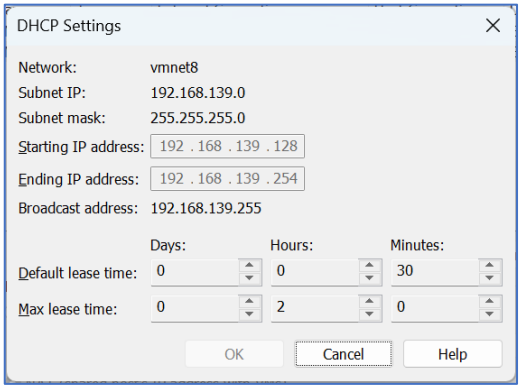
192.168.139.2



Click on the OK button in the NAT Settings window.

Back in the Virtual Network Editor window:

5. Click on the DHCP settings button.



Here you can see that the NAT VMnet network will distribute IP addresses in the range of:

192.168.139.128 – 192.168.139.254

Click on the OK button in the DHCP Settings Window.

6. Click on the OK button in the Virtual Network Editor window.

Now your NAT VMnet is configured.

1.2 Debian 12 Server in VMware

Install a Debian 12 Server VM

1cpu, 4cores, 4GB ram, 32GB hard disk, NAT network adapter, CD/DVD drive.

ISO: https://www.debian.org/CD/netinst/

Use hostname: omv<your student number>

Domain: local

Don't create a root user, create a user with sudo privileges that has your first name.

Don't install a Graphical desktop environment

Select SSH server and standard system utilities only!

Finish the Debian 12 installation and let it reboot.

1.3 Open Media Vault

1.3.1 Installation

Install Open Media Vault 7 on Debian12 (bookworm) server.

Log in to your Debian 12 server.

In the terminal execute the following commands:

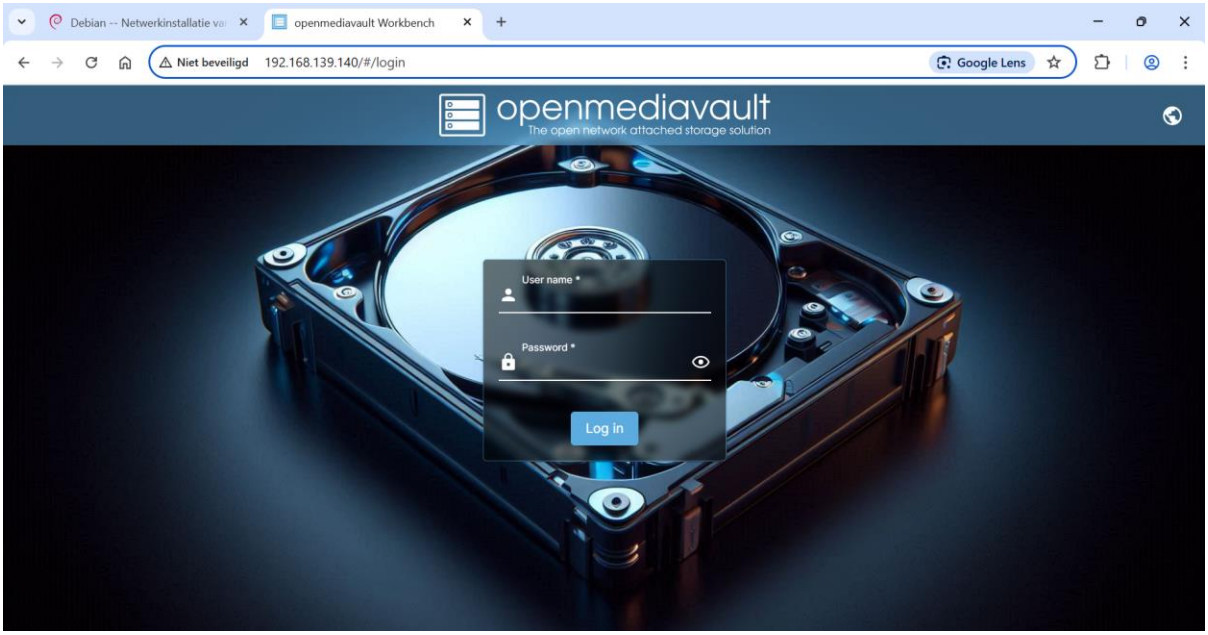
```
sudo apt update && sudo apt upgrade -y
wget -O - https://github.com/OpenMediaVault-Plugin-Developers/installScript/raw/master/install | sudo bash
```

Reboot the system after the installation of Open Media Vault.

The IP address of the web gui is displayed in the terminal.

It can take a couple of minutes before the web gui is accessible in your web browser.

Use your host machine's web browser to access the web gui of Open Media Vault.



1.3.2 Access Web Gui

Go to: http://<your-server-ip>

User name: **admin**

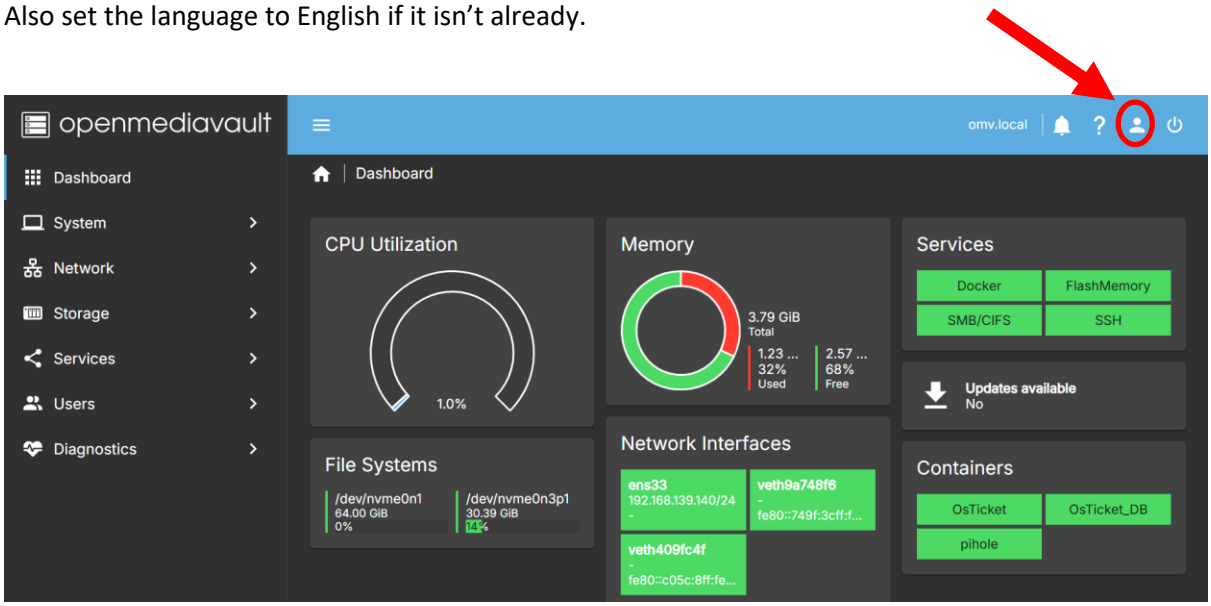
Password: **openmediavault**

Keep the default password for now.

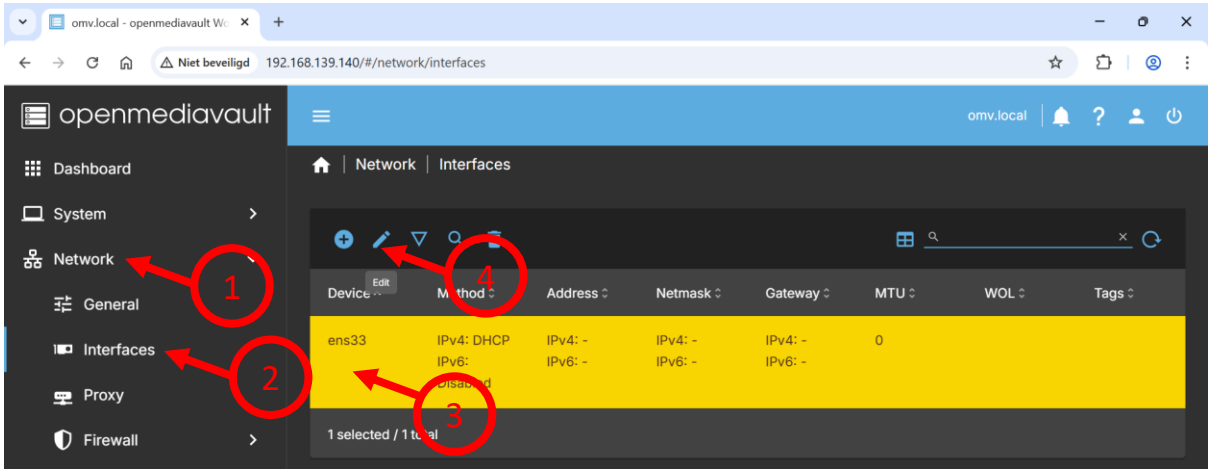
In a production environment it is prudent to change the password immediately after the installation.

Log in to your Open Media Vault server via the web gui and setup your Dashboard.

Also set the language to English if it isn't already.



1.3.3 Static IP Address

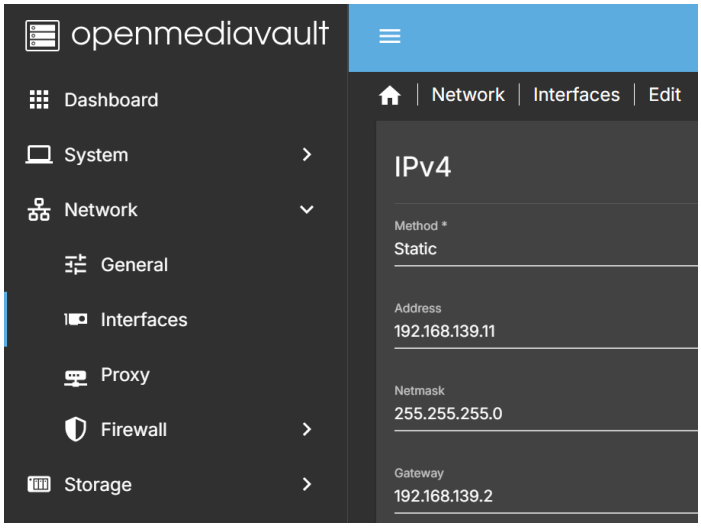


In the Open Media Vault web gui:

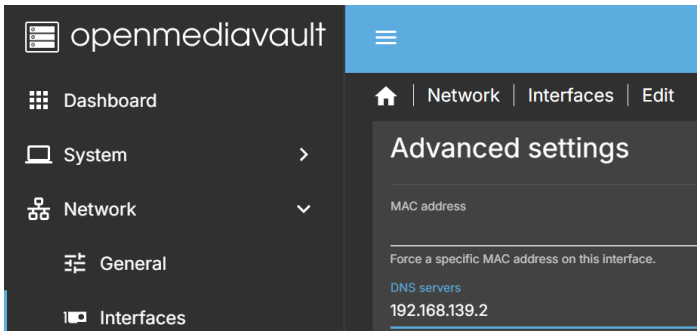
1. Select Network
2. Select Interfaces
3. Select your network interface in the list
4. Click on the pencil symbol ✎ to edit its properties

A server needs to have a static IP address:

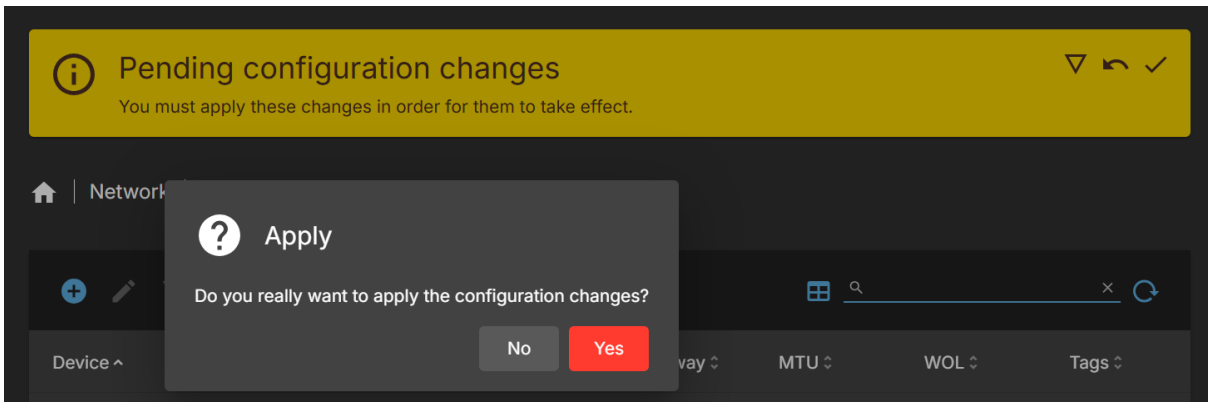
Scroll down a bit and copy the information in the picture into the IPv4 section.



Scroll down further to the Advanced settings. Set the DNS servers IP address on 192.168.139.2

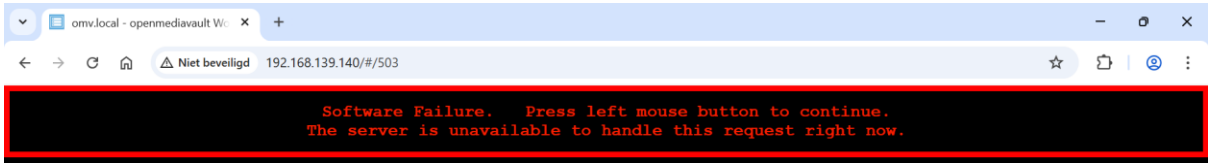


Scroll down even further and click on the Save button. 

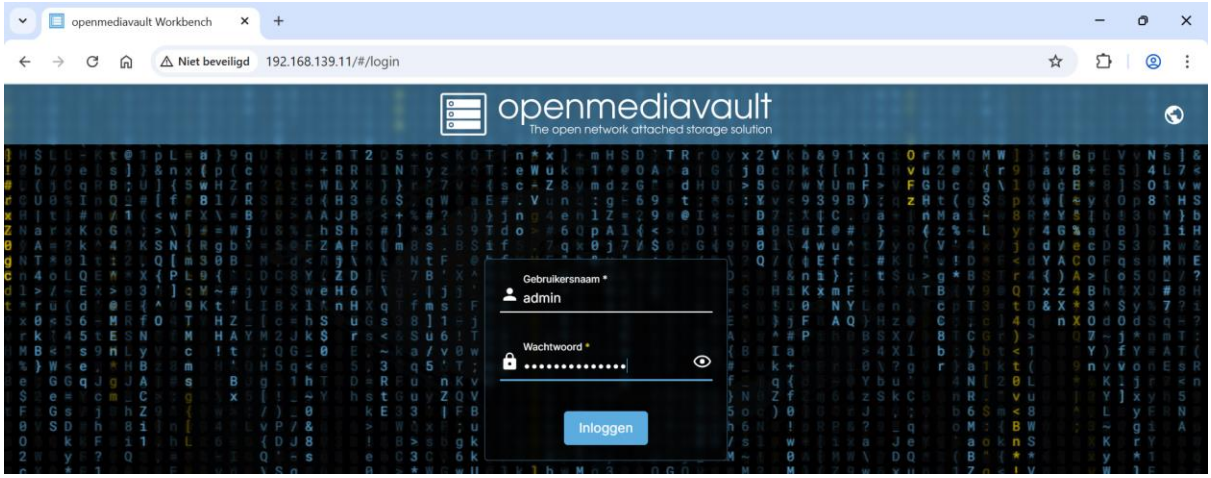


Then click on the check mark in the yellow bar. Select Yes to apply the changes.

Now you will lose the connection to the Open Media Vault server in the web gui because you have changed its IP address to 192.168.139.11.



Go to http://192.168.139.11 in your web browser.



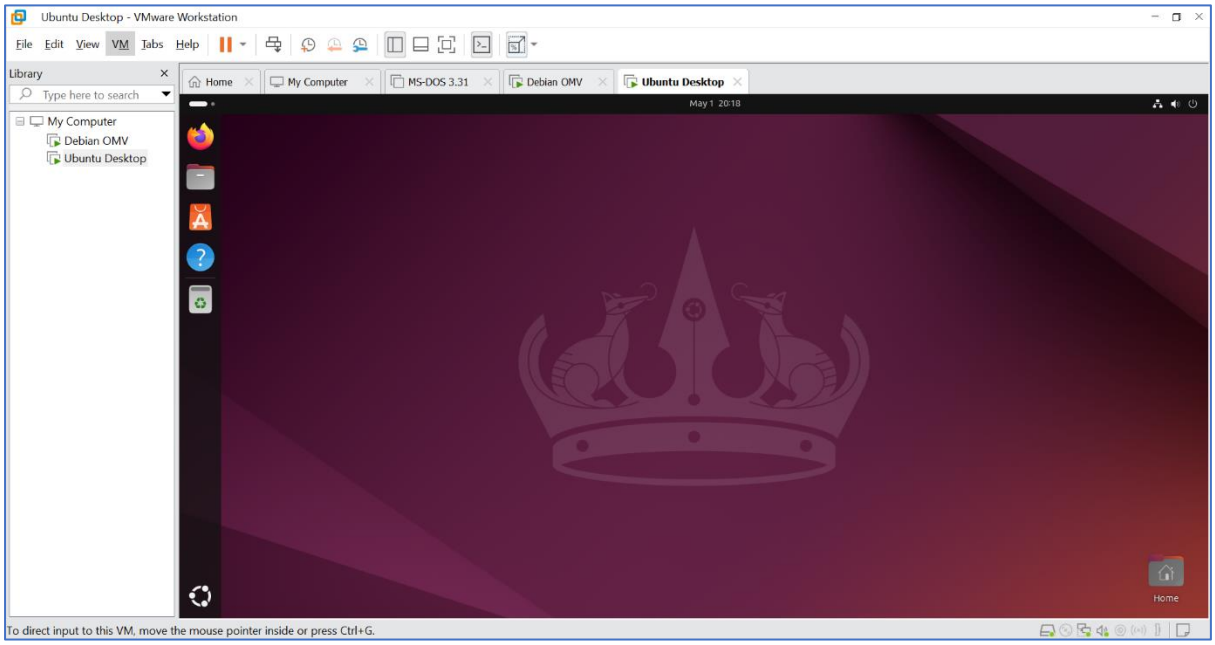
Log in to Open Media Vault.

1.4 Ubuntu 24.04 Desktop in VMware

Install an Ubuntu 24.04 Desktop VM

1cpu, 4cores, 2GB ram, 64GB hard disk, NAT network adapter, CD/DVD drive.

ISO: https://cdimage.ubuntu.com/noble/daily-live/current/



1.5 What is Nextcloud?

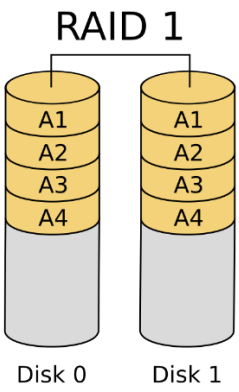
Do research and find out what Nextcloud is. Focus specifically on the office collaboration tools of Nextcloud. We want to implement this system for the municipality of Enschede. Then fill in the quality requirements table in the template report. What do you think the quality requirements should be for this system. Fill in the **Requirement** and **Explanation** columns.

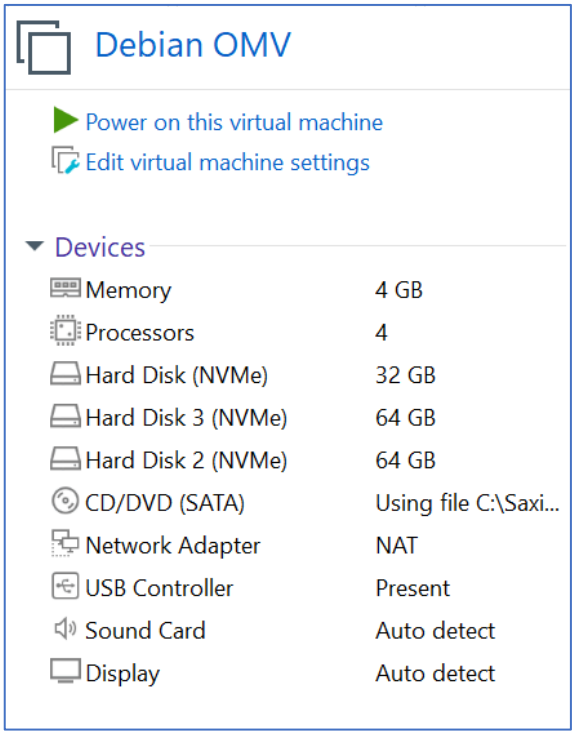
2 Week 2: Adding disks and setting up file shares

You need to add two more hard disks to your Open Media Vault NAS running on Debian 12 VM. These hard disks will store our data. The other hard disk that is already in the VM contains the operating system. That way we separate the operating system from the data. So, if anything happens to the operating system our data is still safe.

2.1 Adding two more hard disks

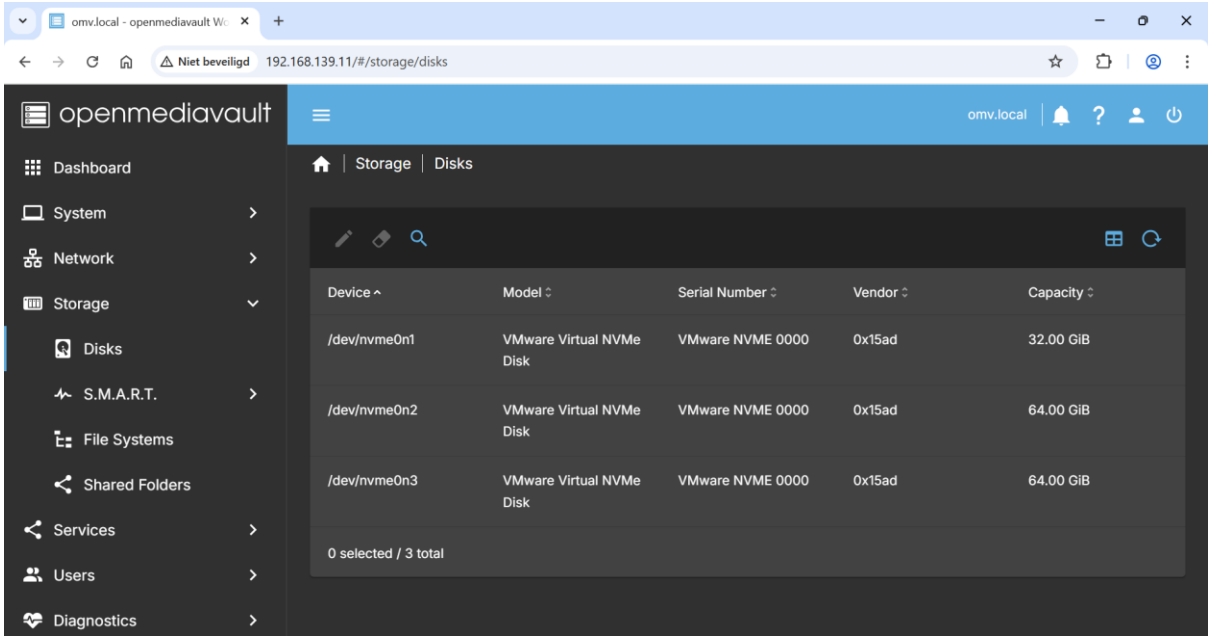
We choose to add two more 64GB hard disks so we can configure a RAID 1 array. RAID 1 is a storage configuration that **mirrors** data across two or more drives, meaning the same data is written to each drive simultaneously. This setup provides redundancy, so if one drive fails, the data remains safe and accessible on the other. The file system we are choosing for this is BTRFS. It is suitable for RAID 0, 1 and 10. But don't use it for RAID 5 or 6.





Once you have added the two additional hard disks you can start the Debian 12 VM.

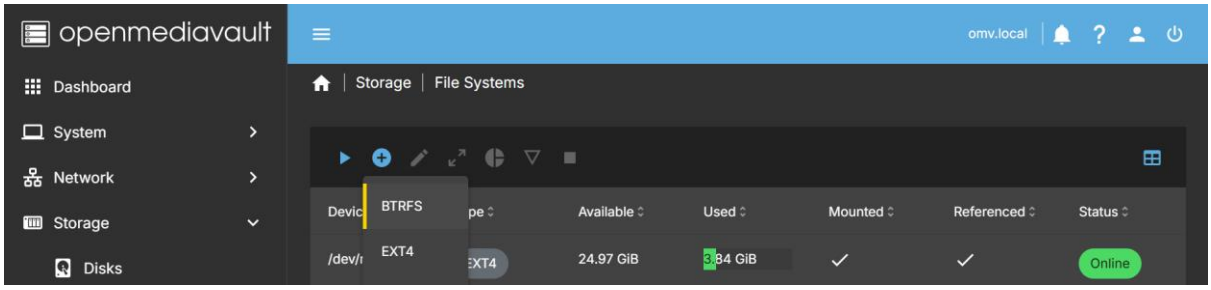
2.2 Open Media Vault file system setup



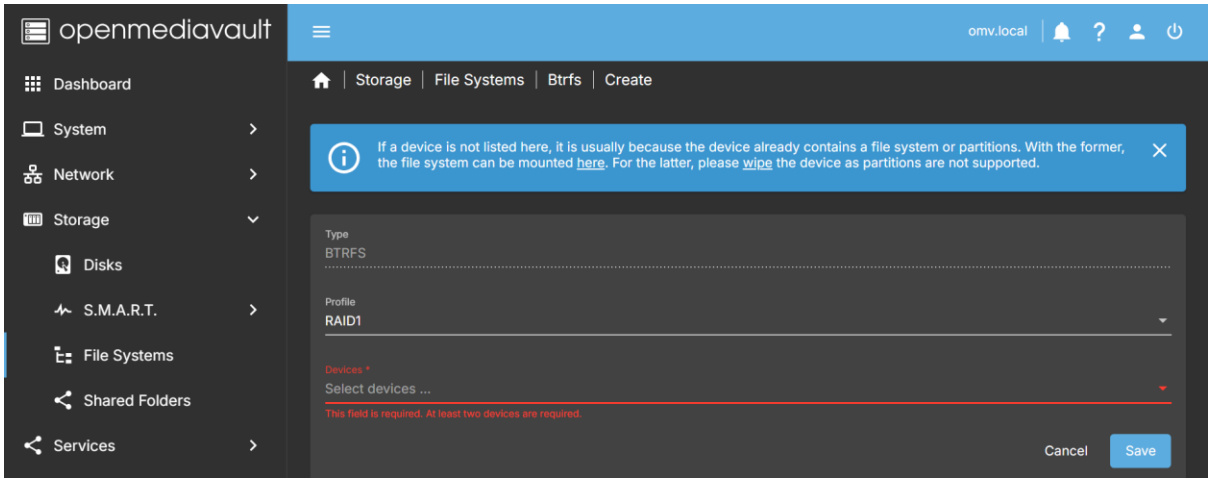
1. Select Storage and click on Disks

You should now see the two added disks of 64GB.

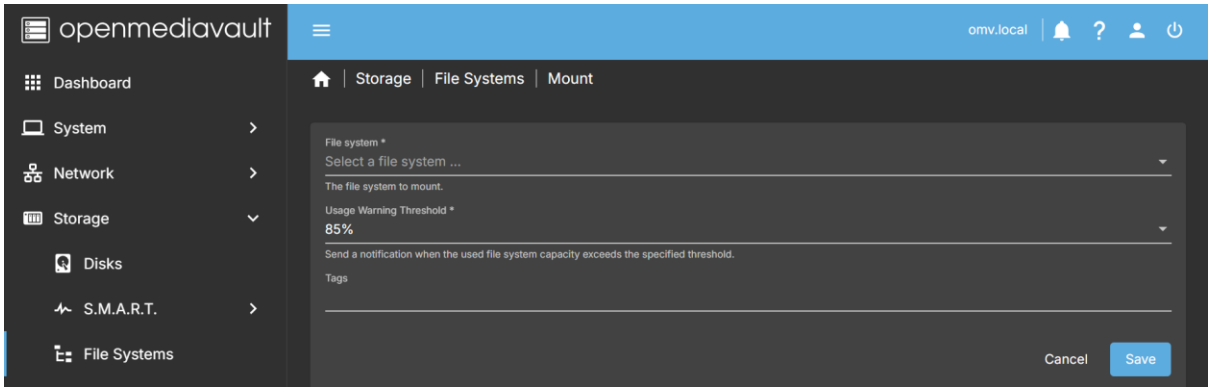
2. Select File Systems



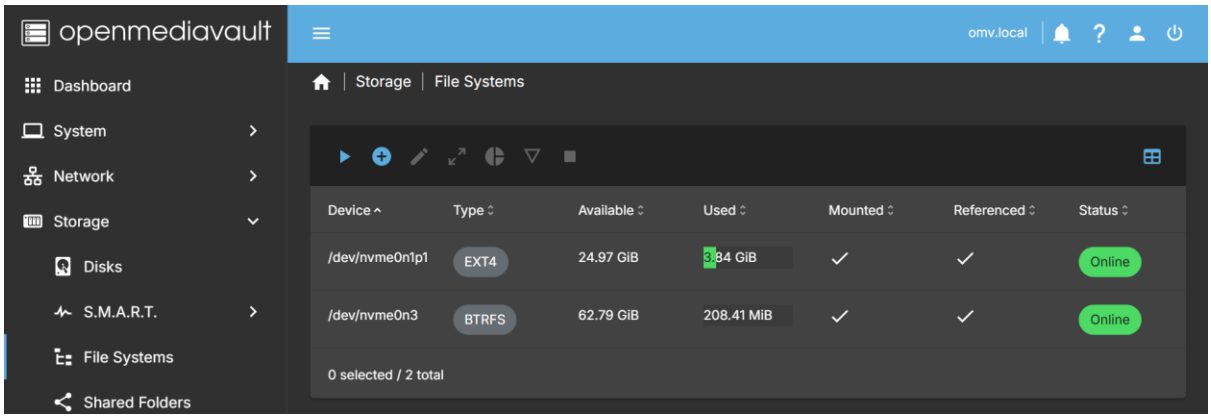
3. Click on the + symbol and choose BTRFS



4. Set Profile to RAID1 and Select the two available hard disks
5. Click on the Save button



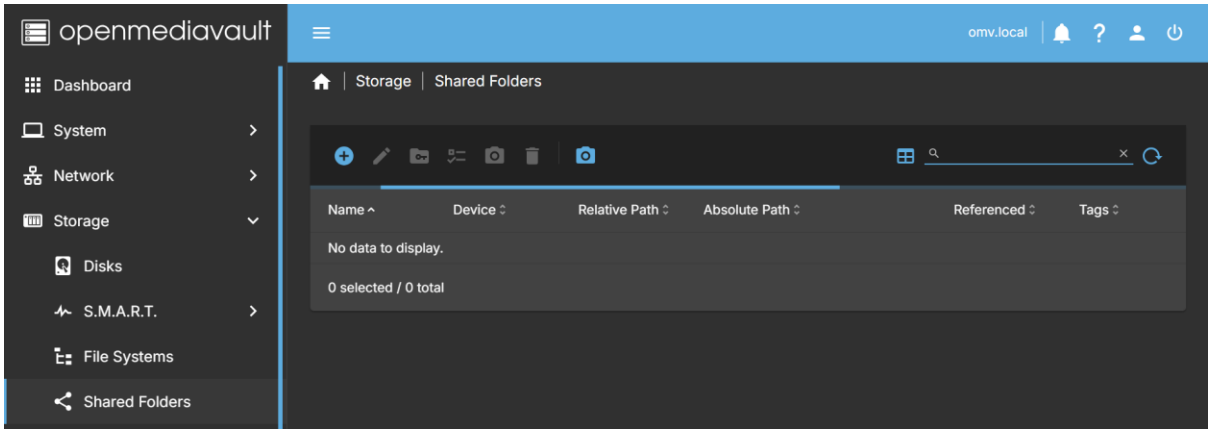
6. Now select the newly created file system to mount it
7. Click on the Save button
8. You may have to apply the pending configuration changes



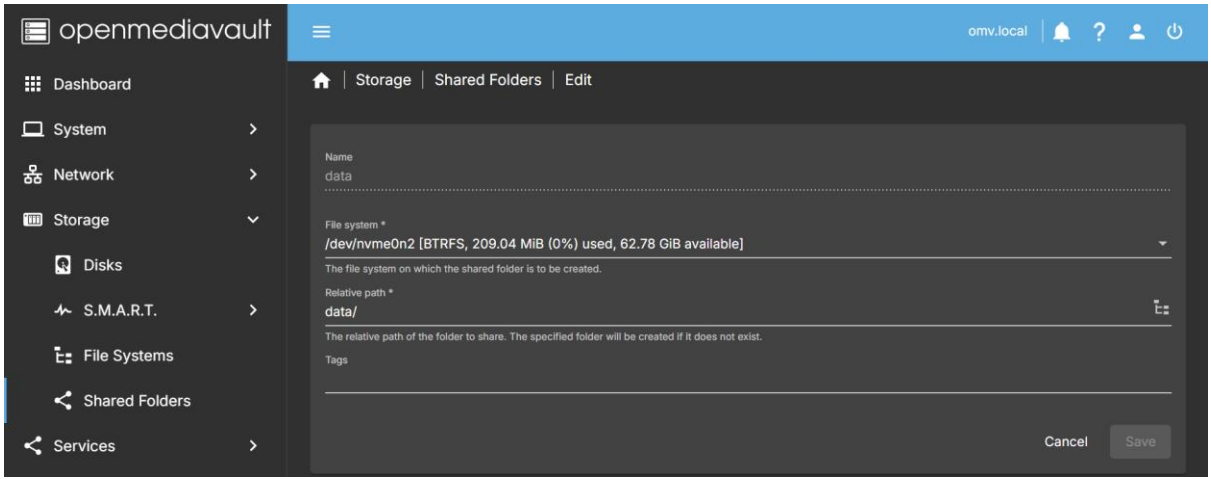
The BTRFS file system is now created and operates as a RAID1 array. The available size could be incorrectly shown as double its size. Later on it will correct itself when it realises that it is a RAID1 array that mirrors data across two drives.

2.3 Shared folders

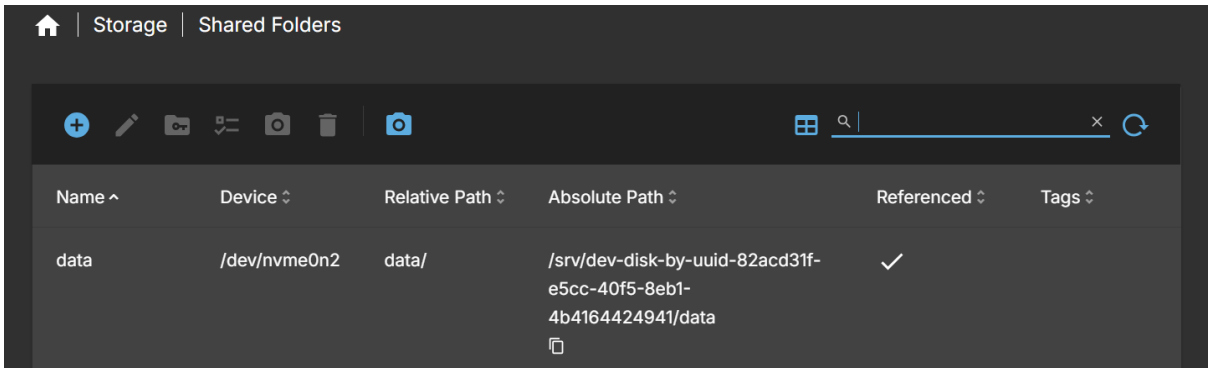
Now it is time to create a shared folder.



1. Click on Storage
2. Click on Shared Folders
3. Click on the + symbol to create a shared folder



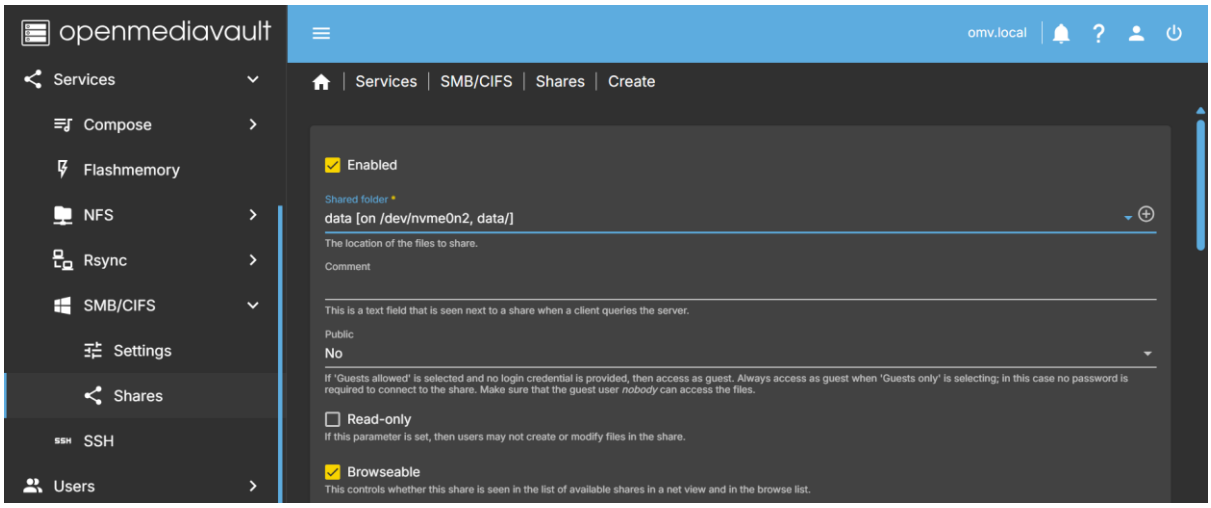
4. Name the shared folder **data**
5. Select the BTRFS RAID1 array for the file system
6. The relative path name should automatically be filled
7. Click on the Save button
8. You may have to apply the pending configuration changes



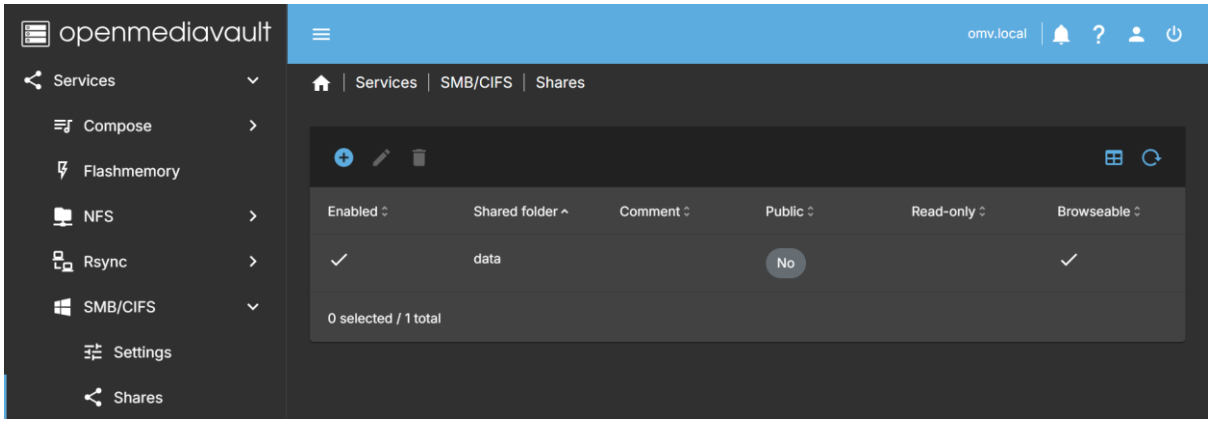
The shared folder is now created but nobody can access it.

2.4 SMB/CIFS Services

You need to setup a SMB/CIFS share so users can access your shared folder on the NAS.



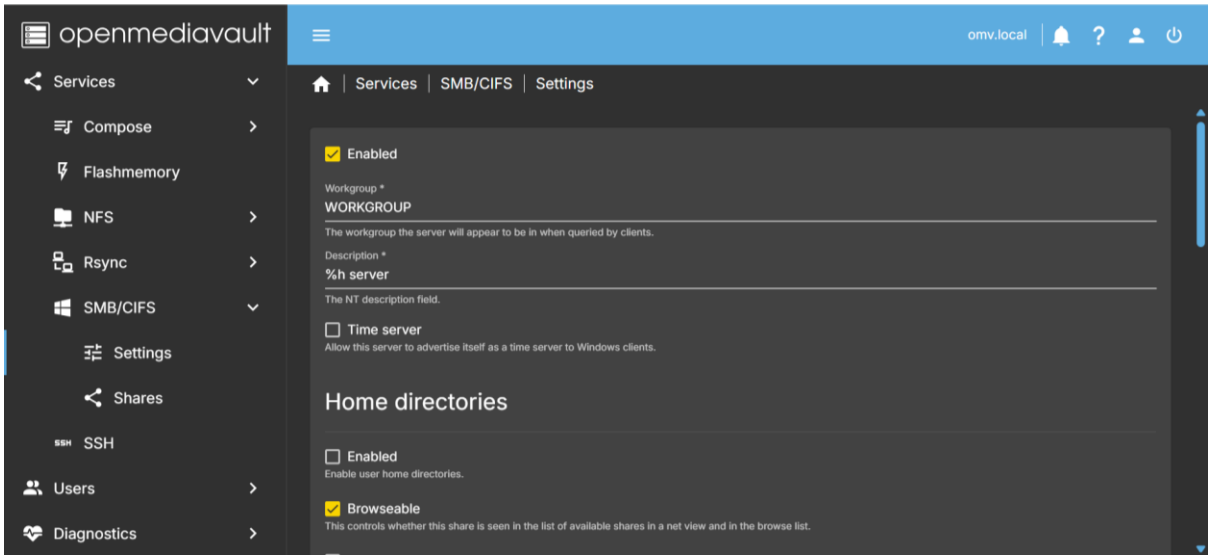
1. Go to Services and select SMB/CIFS
2. Select Shares and click on the + symbol to create a SMB/CIFS share.
3. Click on Enabled and select the **data** shared folder you've created earlier
4. Scroll down to the bottom of the page and click on the Save button
5. You may have to apply the pending configuration changes



Your SMB/CIFS share named **data** is now created.

But users still can't access it.

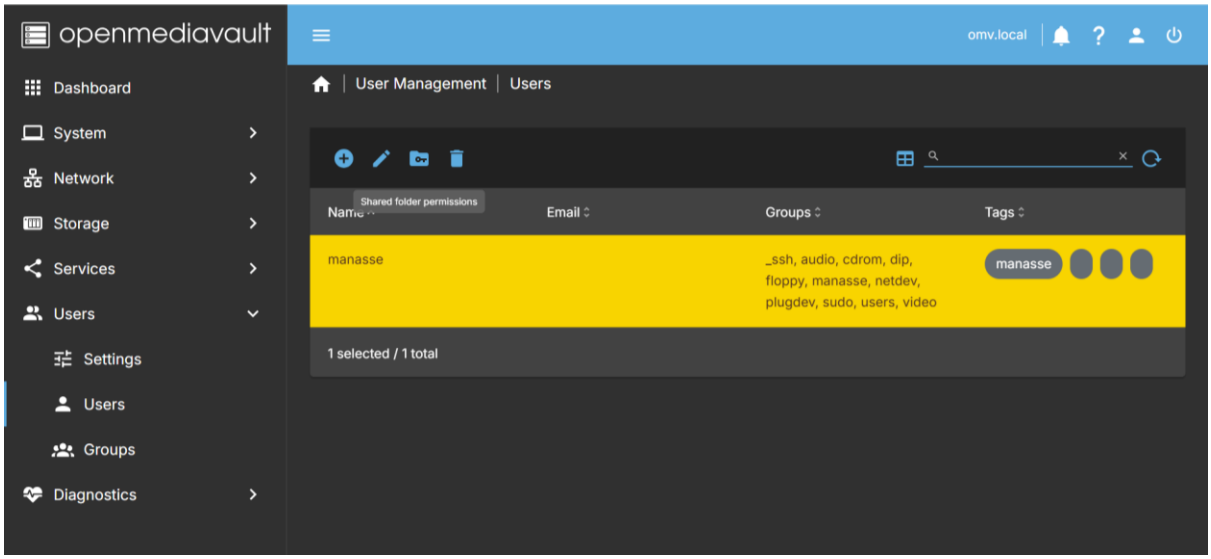
Go to Services > SMB/CIFS > Settings



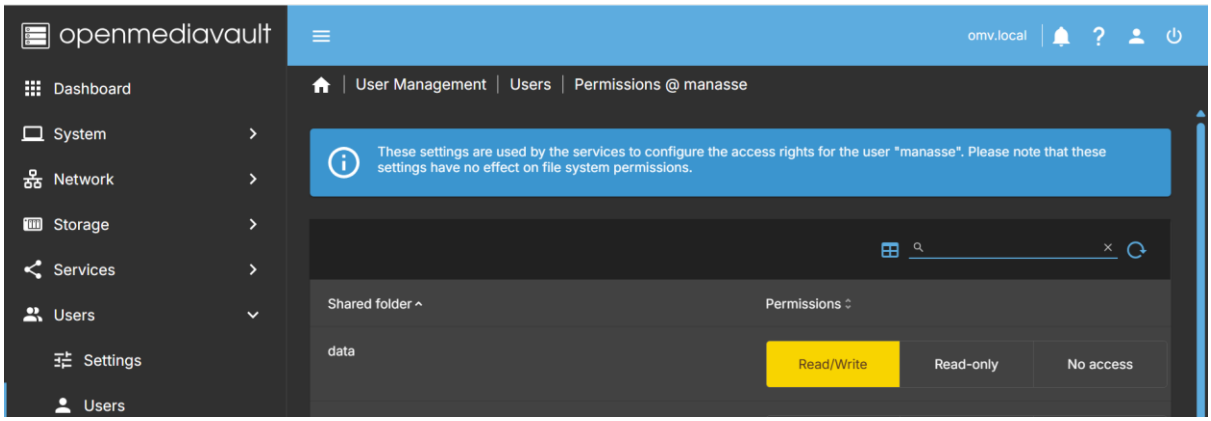
1. Click on Enabled
2. Scroll to the bottom of the page and click on the save button.
3. You may have to apply the pending configuration changes

2.5 User access rights

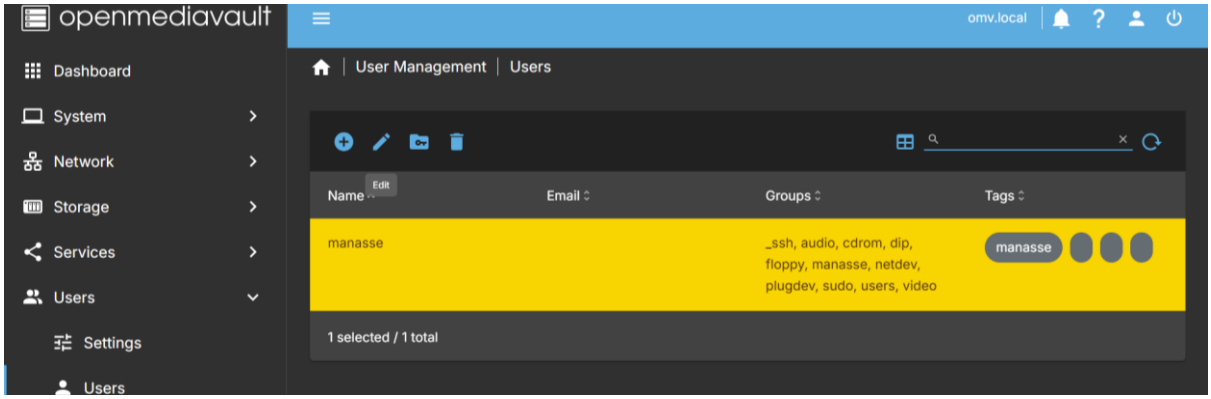
Your users need read/write permissions to access the shared folder.



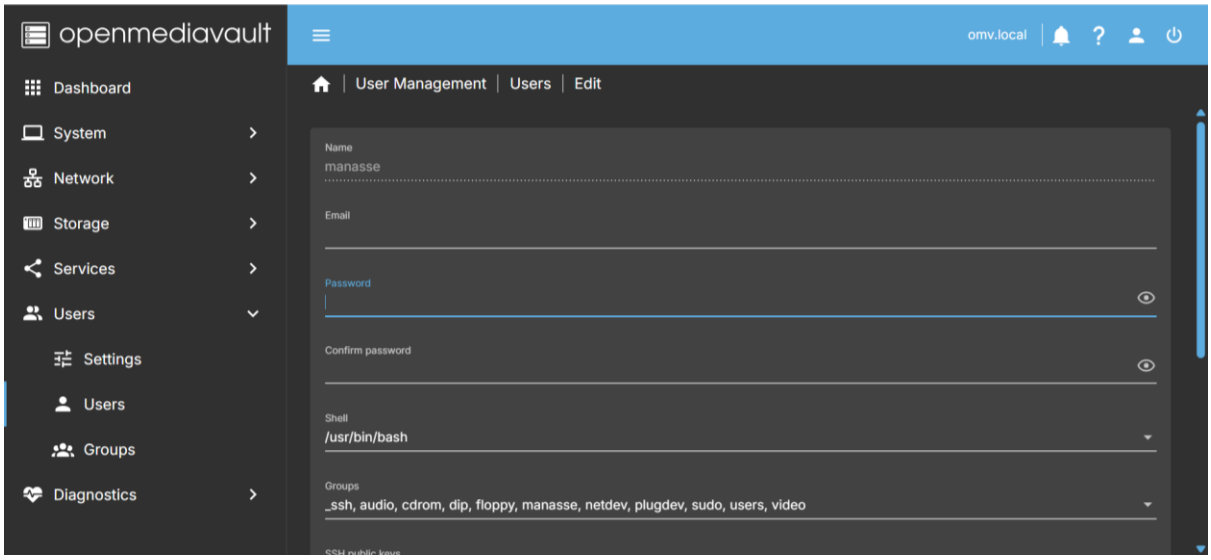
- Go to Users > Users
- Select your only user there
- Click on the Shared folder permissions button



- Give your user Read/Write permissions on the **data** shared folder.
- Click on the Save button
- You may have to apply the pending configuration changes
- Go back to Users > Users



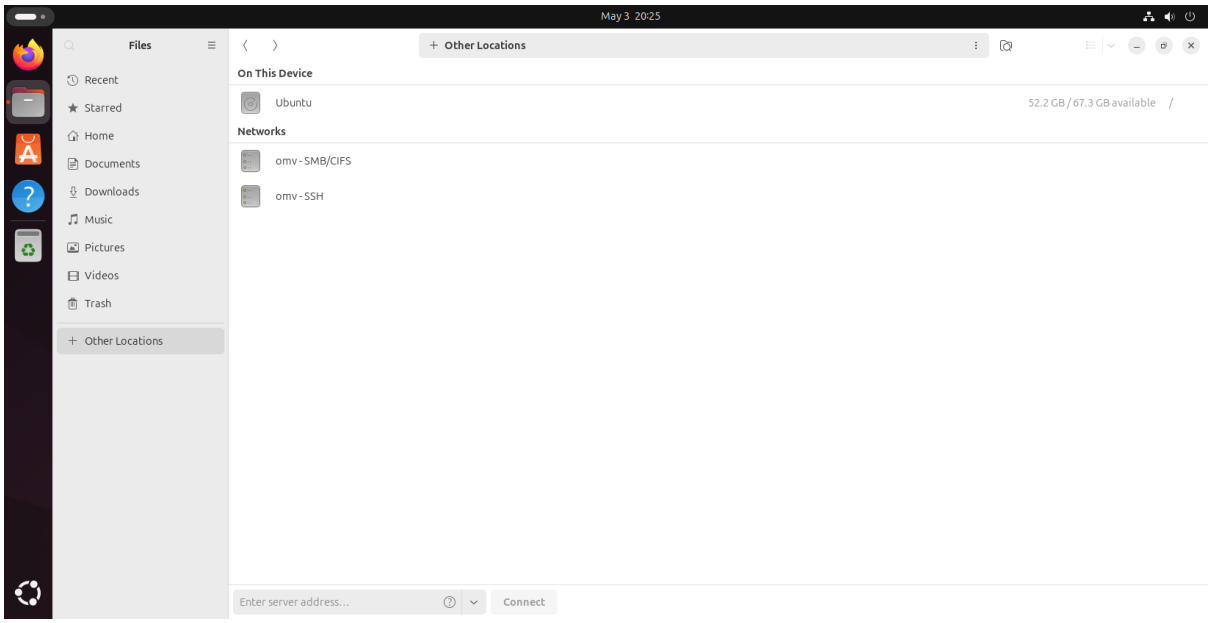
Now click on the pencil button to edit your user



- Enter your Debian login password for your user in the Password text field and Confirm
- Scroll down and click on the Save button
- You may have to apply the pending configuration changes

2.6 Testing shared folder access

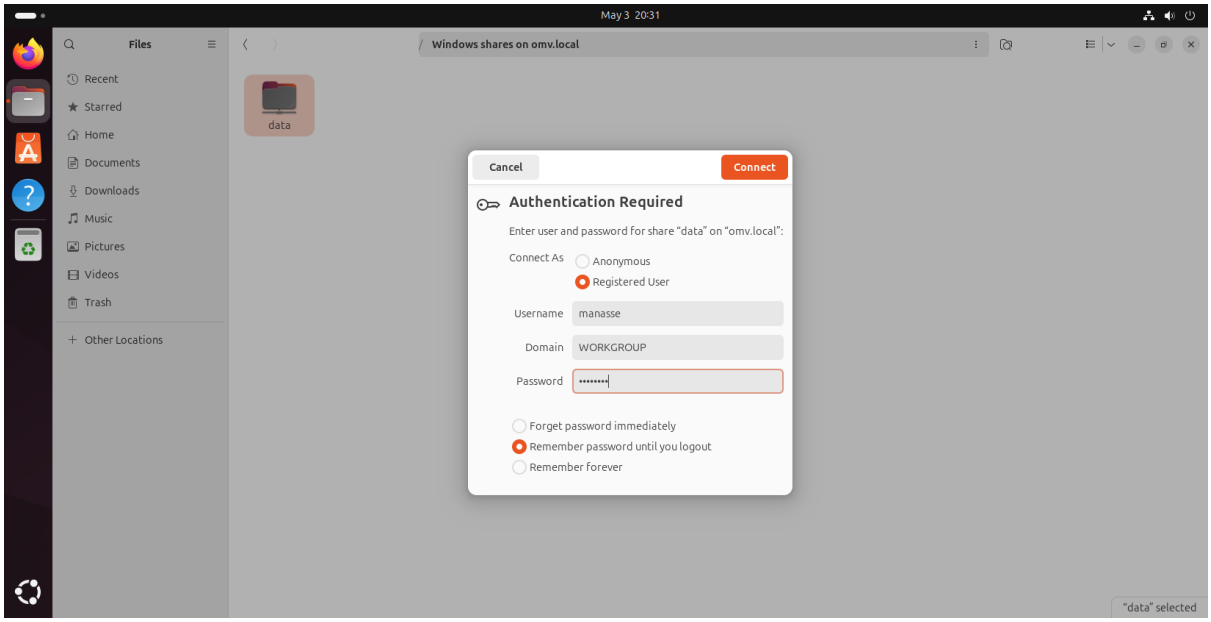
- Boot up the Ubuntu Desktop VM
- Select Files
- Select Other Locations



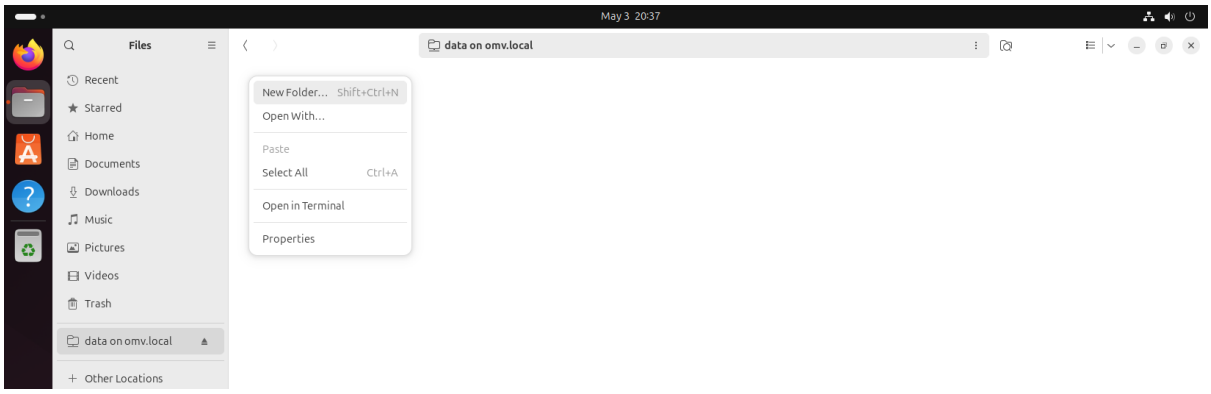
- If the omv – SMB/CIFS share is not visible here, you can enter a server address and click on the Connect button. The static IP address of the Open Media Vault server is 192.168.139.11.
    - **smb://192.168.139.11/data** on Linux/Mac/Unix systems
    - **\\192.168.168.11\data** on Windows systems

- If the omv – SMB/CIFS share is visible, click on it.

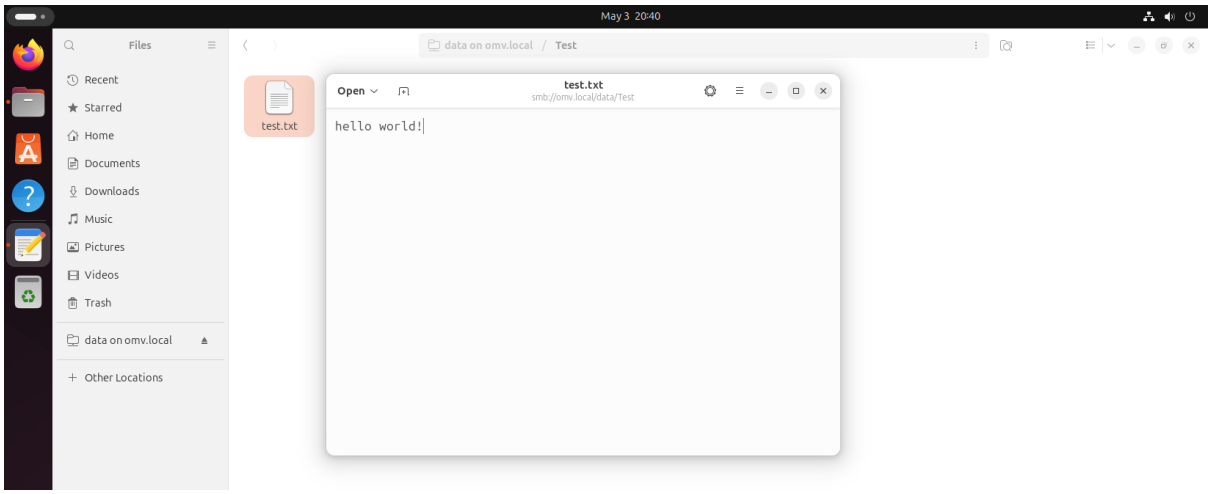
- Click on the **data** folder



- Enter your login credentials
- Click on the Connect button



- Try if you can create a folder here, named **Test**.
- Enter the folder **Test**.



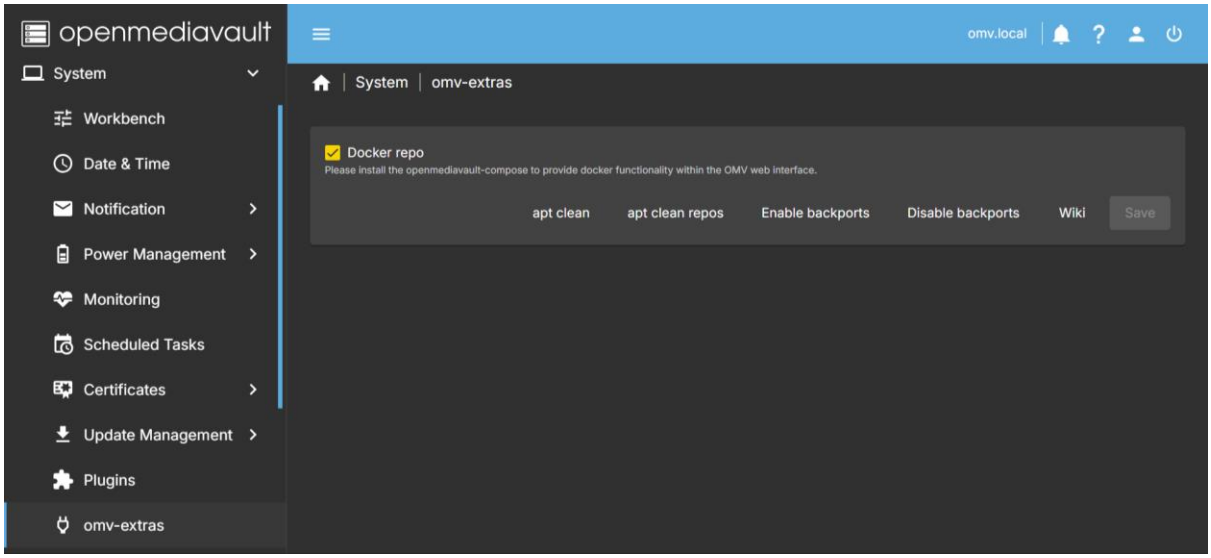
- Place a text file inside the **Test** folder named **test.txt**.
- If you can save the text file, then all the read/write permissions are working correctly.
- Put your first name and student number in this text file.

3 Week 3 – Deploying docker applications

On the Open Media Vault server you can deploy docker applications. To make this possible, you need to enable docker.

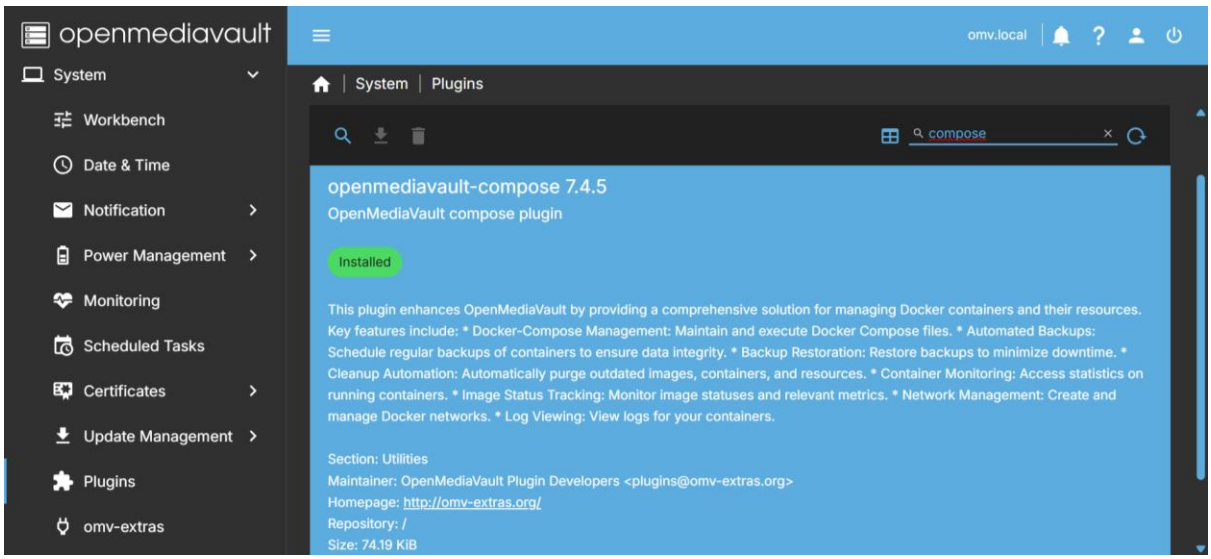
3.1 Docker setup

3.1.1 Enable docker



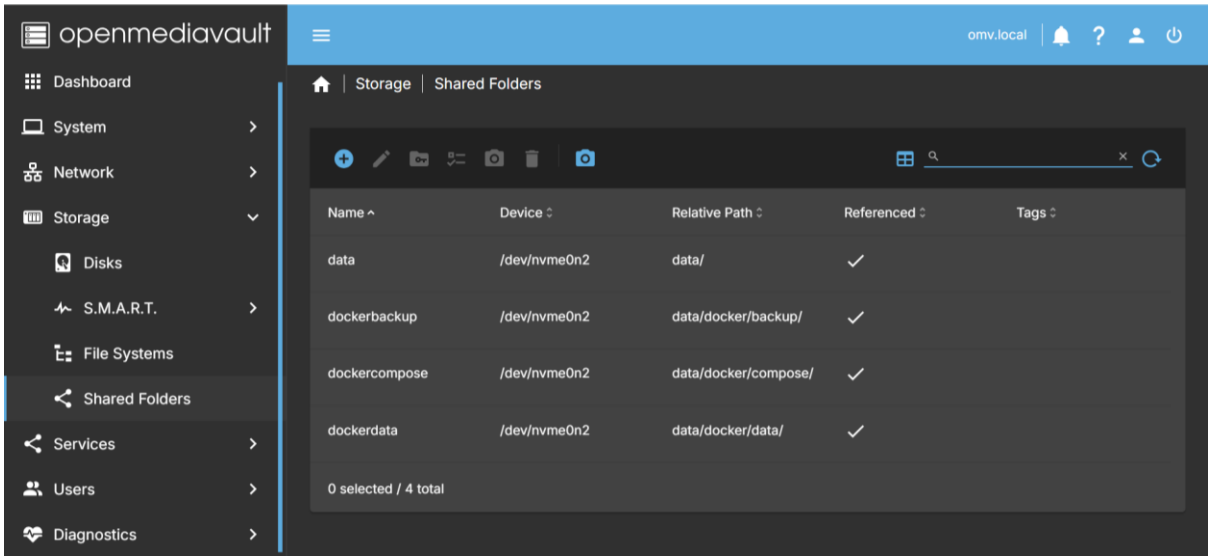
- Go to System > omv-extras
- Enable Docker repo
- Click on the Save button
- You may have to apply the pending configuration changes

3.1.2 Install docker compose plugin



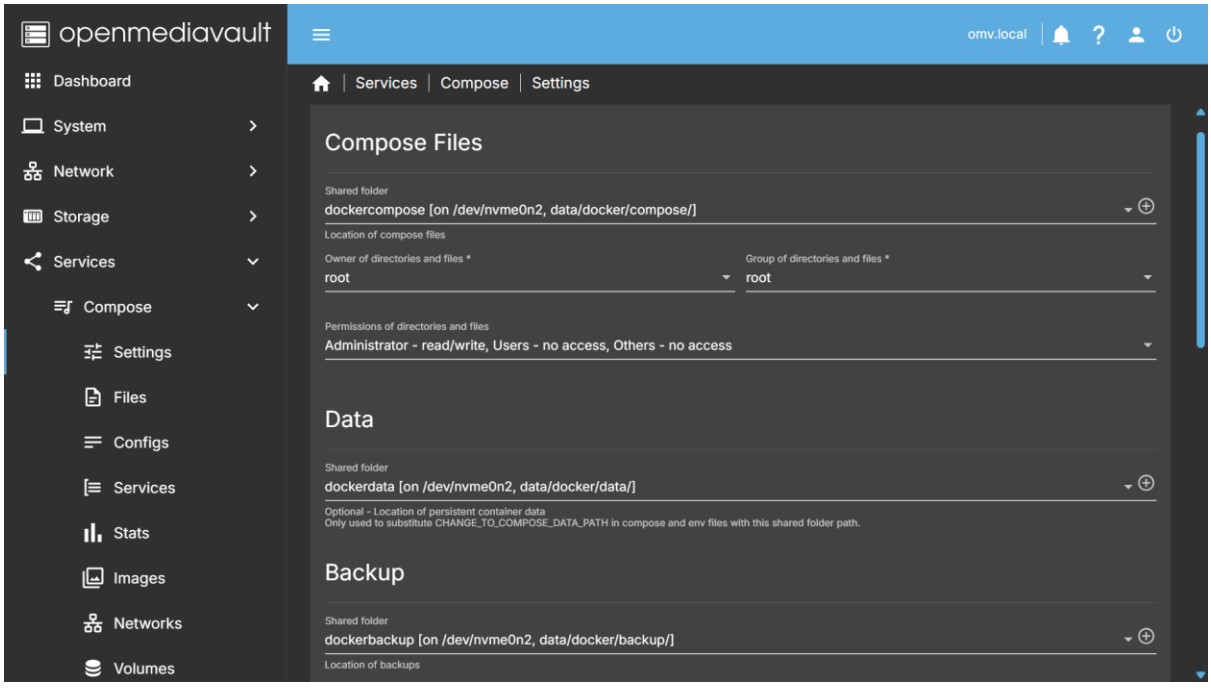
- Then go to System > Plugins
- Search for the docker compose plugin
- Select the plugin and click on the install button (download icon)
- You may have to apply the pending configuration changes

3.1.3 Setup shared folders for docker



- Go to Storage > Shared Folders
- Create three additional shared folders:
  - dockercompose
  - dockerdata
  - dockerbackup
- Look at the picture for the Relative Paths

3.1.4 Docker compose setup

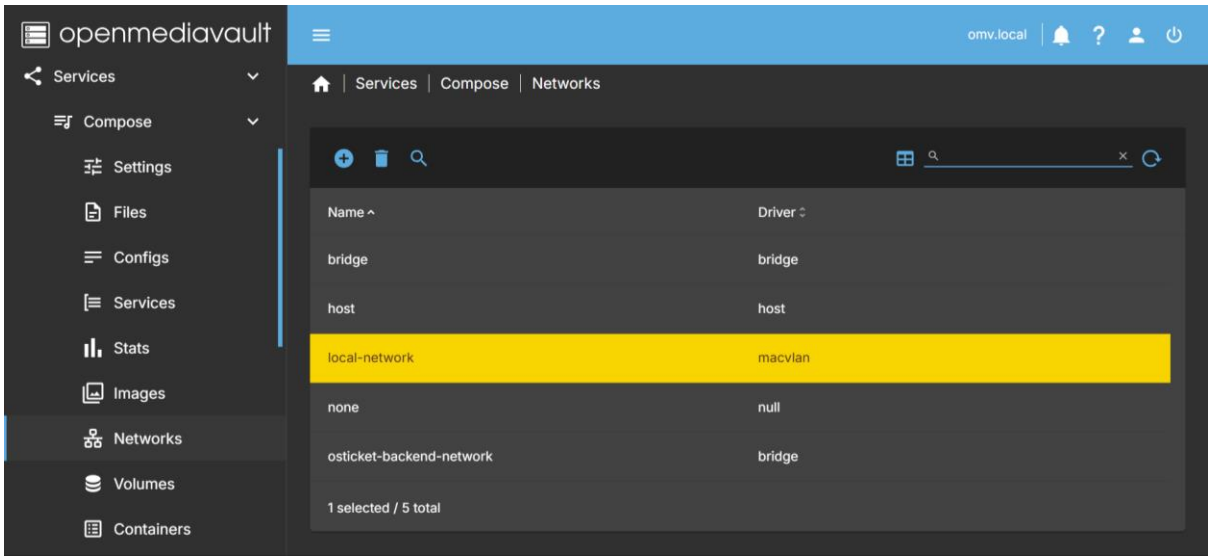


- Go to Services > Compose > Settings
- Select the three created shared folders in the Compose Files, Data and Backup sections:
  - dockercompose
  - dockerdata
  - dockerbackup

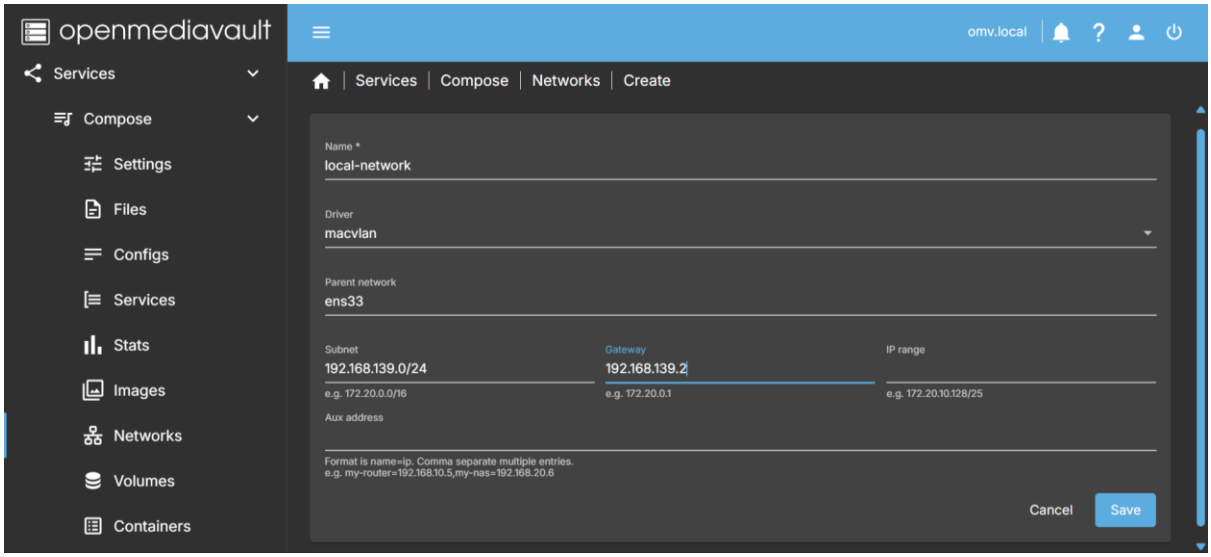
- Scroll down and click on the Save button
- You may have to apply the pending configuration changes
- Docker will be installed automatically now

3.2 Creating a macvlan network for our docker apps

A macvlan network lets Docker containers get their own LAN IPs, enabling direct access without port forwarding, as if they were separate physical devices on the network.

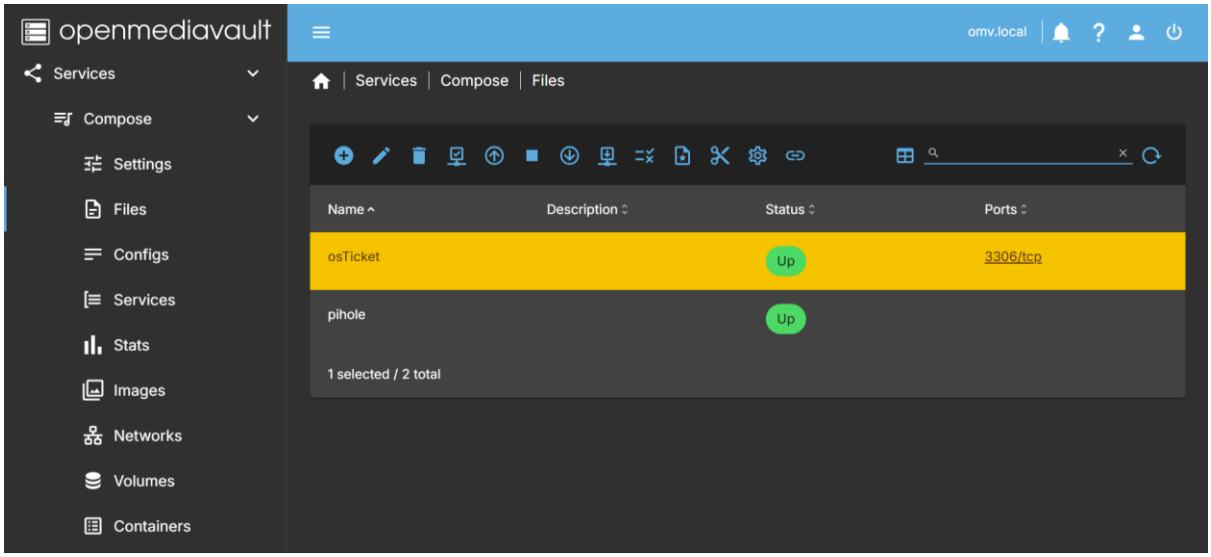


- Go to Services > Compose > Networks
- Click on the + symbol to create a network

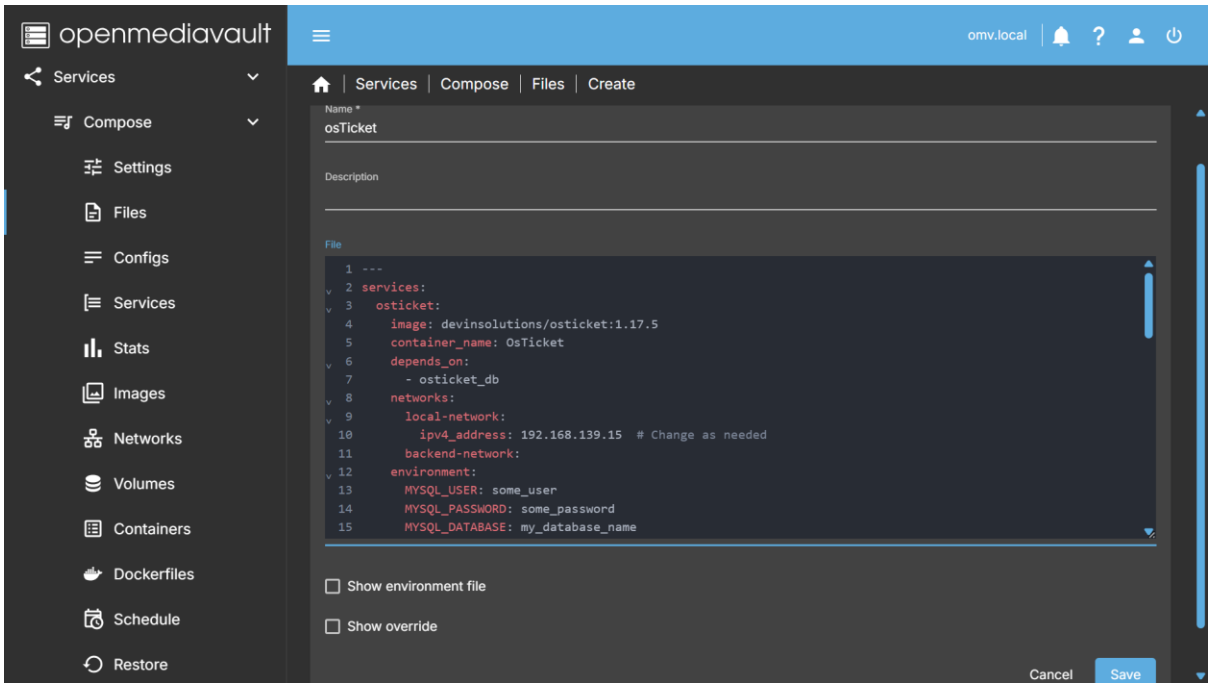


- Fill in the form:
  - Name: local-network
  - Driver: macvlan
  - Subnet: 192.168.139.0/24
  - Gateway: 192.168.139.2
- Click on the Save button
- You may have to apply the pending configuration changes

3.3 Installing osTicket app via docker compose



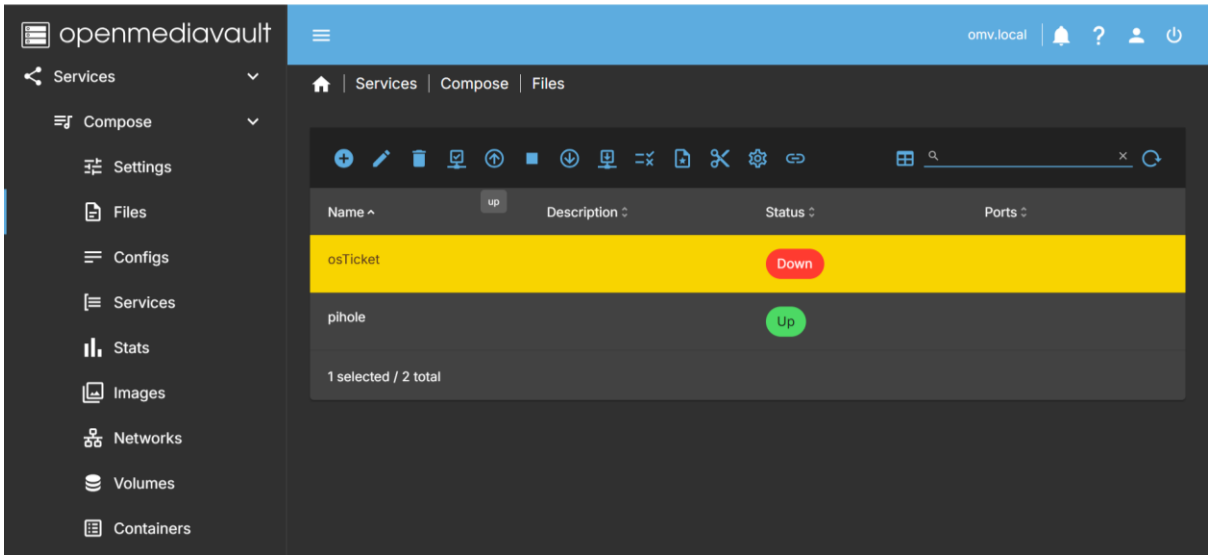
- Go to Services > Compose > Files
- Click on the + symbol to create a new docker compose yaml file



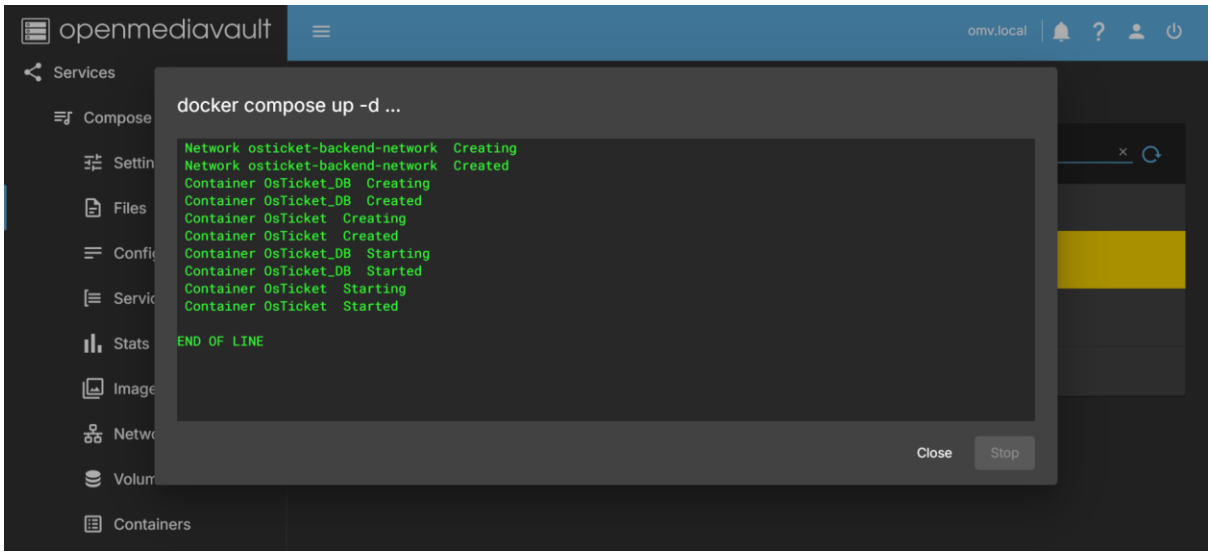
- Fill in the form:
  - Name: osTicket
  - File: See source code on next page, copy and paste it in the text area.
- Click on the Save button
- You may have to apply the pending configuration changes

osTicket docker compose yaml file:

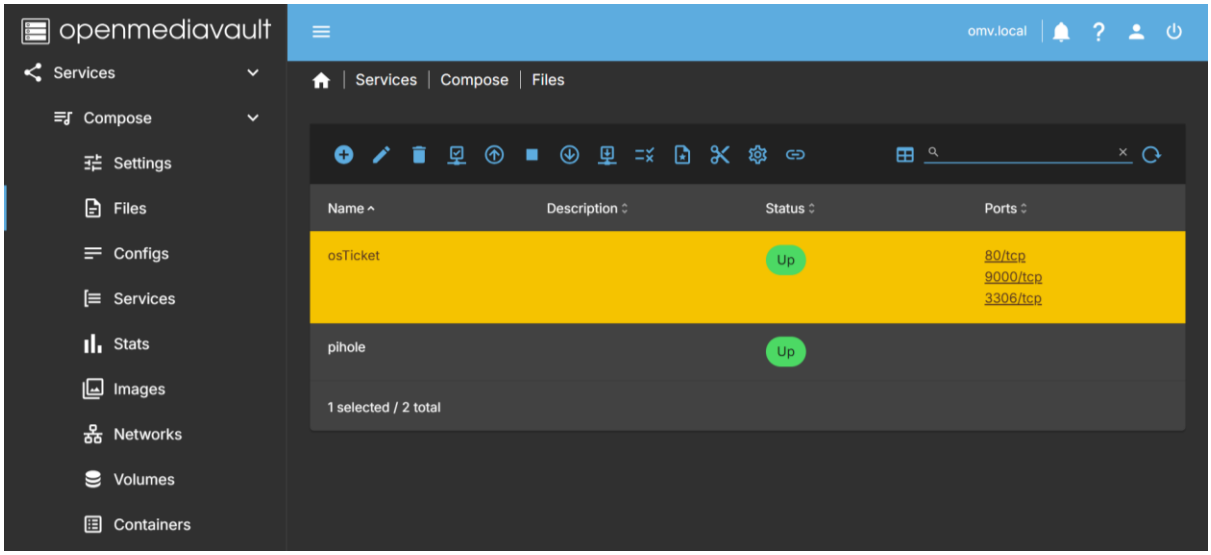
```
---
services:
  osticket:
    image: devinsolutions/osticket:1.17.5
    container_name: OsTicket
    depends_on:
      - osticket_db
    networks:
      local-network:
        ipv4_address: 192.168.139.15  # Change as needed
      backend-network:
    environment:
      MYSQL_USER: some_user
      MYSQL_PASSWORD: some_password
      MYSQL_DATABASE: my_database_name
      MYSQL_HOST: osticket_db
      INSTALL_SECRET: mysecret
      INSTALL_URL: http://osticket.local
      INSTALL_NAME: Helpdesk
      ADMIN_USERNAME: mike
      ADMIN_PASSWORD: Welkom#01
      ADMIN_FIRSTNAME: Mike
      ADMIN_LASTNAME: Sierra
      ADMIN_EMAIL: yourown@email
      CRON_INTERVAL: 1
      #SMTP_USER: Your-own-gmail-address
      #SMTP_PASSWORD: Your-own-app-password
      #SMTP_HOST: smtp.gmail.com
      #SMTP_PORT: 587
      #SMTP_FROM: Your-own-gmail-address
      #SMTP_TLS: 1
    volumes:
      - CHANGE_TO_COMPOSE_DATA_PATH/osticket/config:/usr/local/apache2/htdocs
    restart: unless-stopped

  osticket_db:
    image: mariadb:11.3-jammy
    container_name: OsTicket_DB
    security_opt:
      - no-new-privileges:true
    environment:
      MYSQL_ROOT_PASSWORD: root_password
      MYSQL_USER: some_user
      MYSQL_PASSWORD: some_password
      MYSQL_DATABASE: my_database_name
    volumes:
      - CHANGE_TO_COMPOSE_DATA_PATH/osticket/db:/var/lib/mysql:rw
    networks:
      - backend-network
    restart: unless-stopped

networks:
  backend-network:
    name: osticket-backend-network

  local-network:
    external: true
```



- Select the osTicket docker compose yaml file
- Click on the up ↑ button

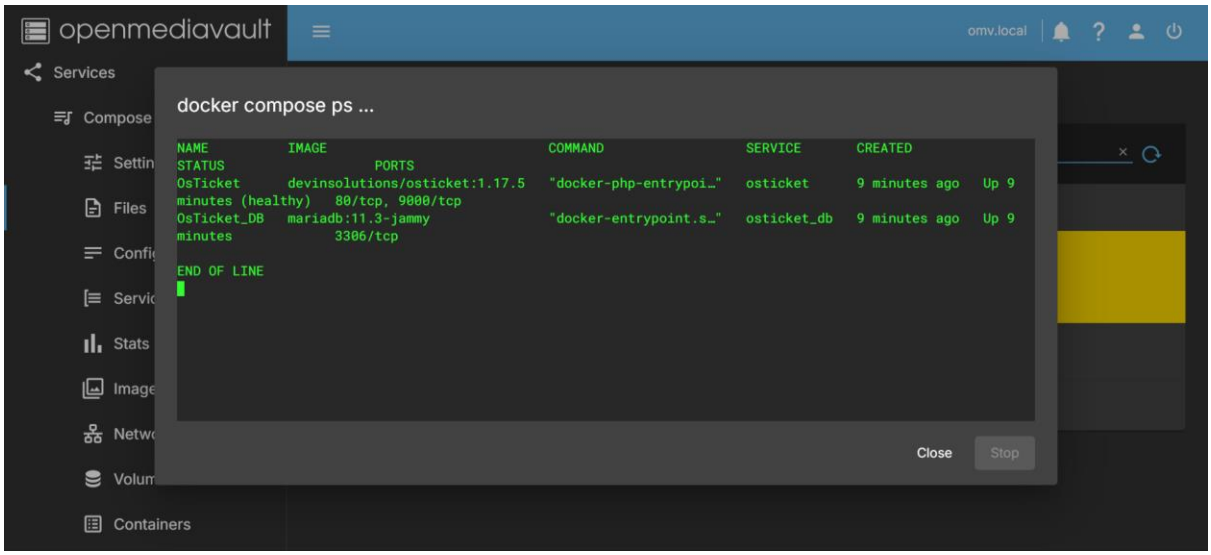


- Docker compose will pull all the needed images:
  - Create the entire infrastructure for the osTicket app
  - Start a mariaDB database server
  - Start the osTicket app
- You can close the docker compose up -d window when it says END OF LINE



Now you should see that osTicket is up and running!

- Select osTicket and click on the ps button 



Here you can check if all docker containers are up and running.

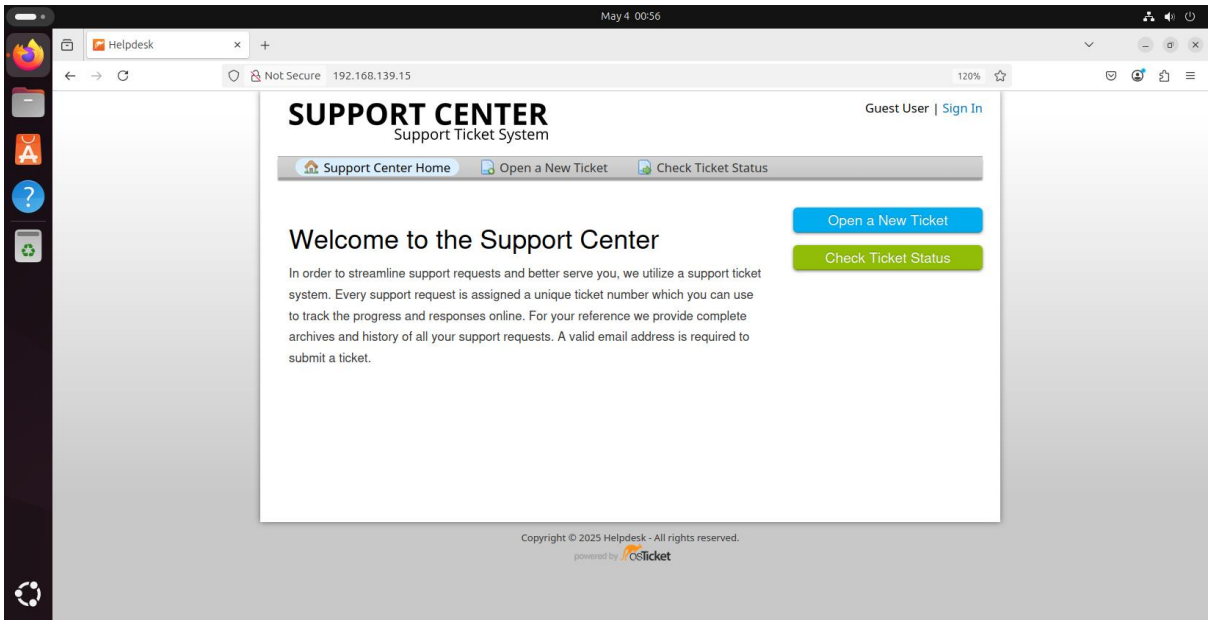
Now if everything checks out you can access osTicket in your Ubuntu Desktop VM.

If you examine the docker compose yaml file for osTicket you can see that the osTicket app is using:

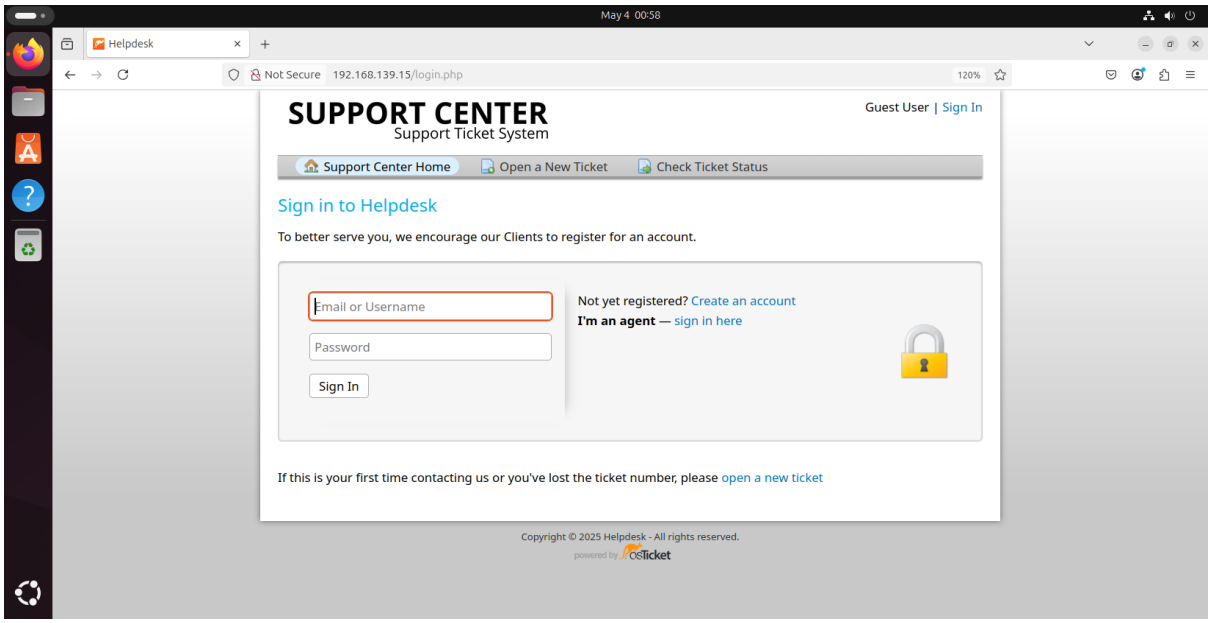
- IP address 192.168.139.15.
- Also the ADMIN username is: mike
- And the ADMIN password is: Welkom#01

Let’s check that out in the Ubuntu Desktop VM.

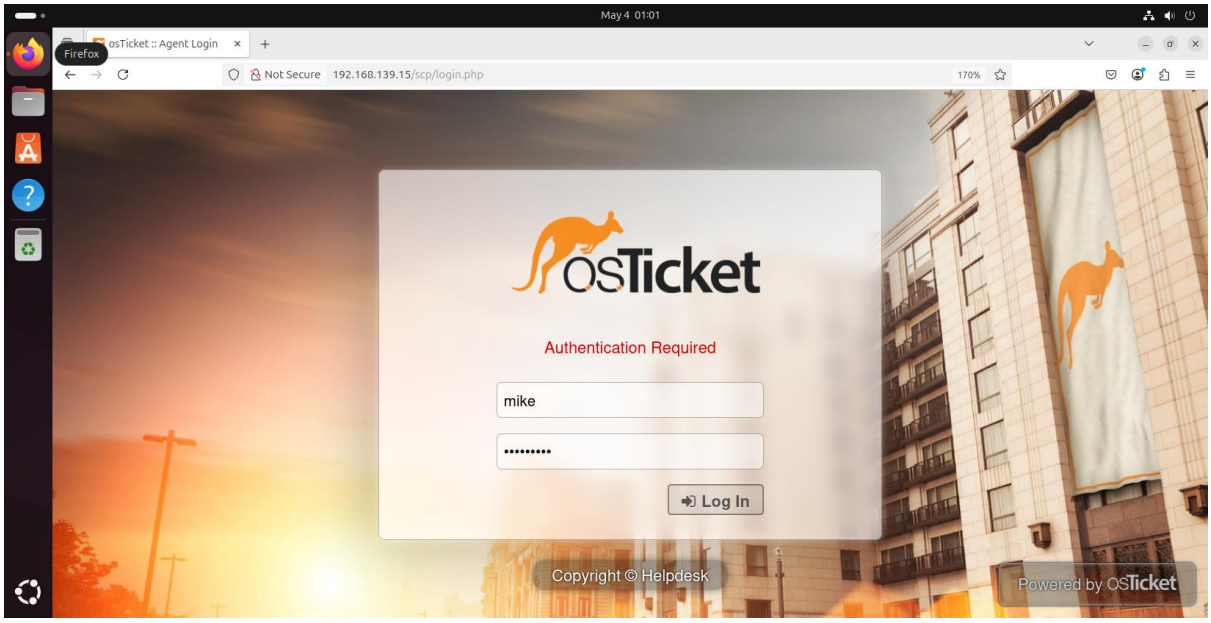
3.4 Using osTicket



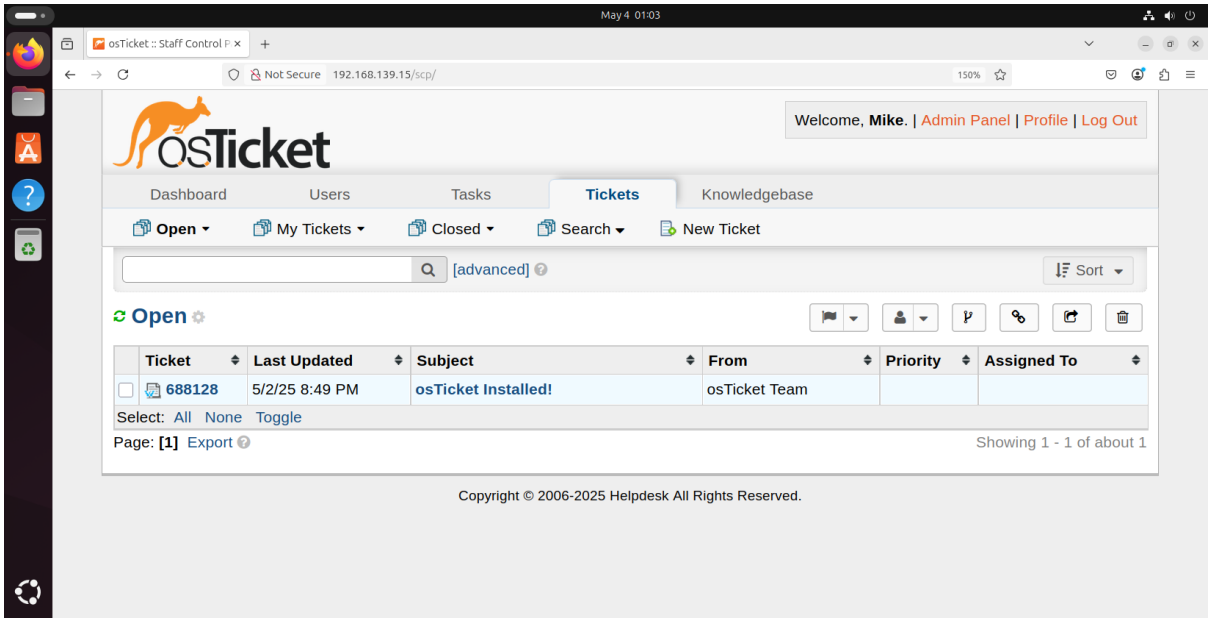
- Go to http://192.168.139.15 in Firefox
- Click on Sign In



- Go to **I'm an agent**
- Click on sign in here



- Here you can log in to osTicket with the admin account:
  - mike
  - Welkom#01
- Click on the Log In button



In here you can go to:

- The Admin Panel to setup the system
- The Agent Panel to manage the tickets

4 Week 4 – Setting up Pi-hole as local DNS server

Pi-hole is a network-wide ad blocker and local DNS server that filters ads, trackers, and malicious domains at the DNS level for all devices on your network. In addition to blocking unwanted traffic, it can also serve as a local DNS server by allowing you to define custom A records, enabling local hostname resolution (e.g., helpdesk.enschede.nl → 192.168.139.15)

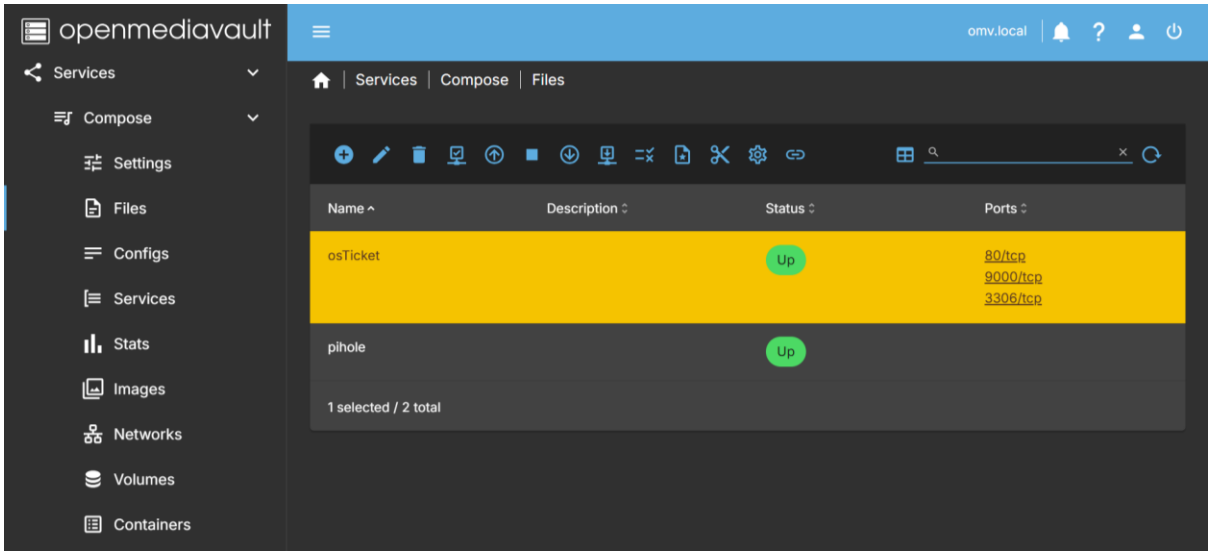
Pi-hole will run as a docker container on the Open Media Vault server with IP address: 192.168.139.3

4.1 Pi-hole docker compose yaml file

```
---
services:
  pihole:
    container_name: pihole
    image: pihole/pihole:latest    #2024.07.0
    hostname: pihole
    networks:
       pihole-network:
          ipv4_address: 192.168.139.3  #Change if necessary
    environment:
       TZ: Europe/Amsterdam
       WEBPASSWORD: Welkom#01    #Does not work anymore
    volumes:
      - CHANGE_TO_COMPOSE_DATA_PATH/pihole/etc-pihole:/etc/pihole
      - CHANGE_TO_COMPOSE_DATA_PATH/pihole/etc-dnsmasq.d:/etc/dnsmasq.d
    #   https://github.com/pi-hole/docker-pi-hole#note-on-capabilities
#    cap_add:
#      - NET_ADMIN # Required if you are using Pi-hole as your DHCP server
    restart: unless-stopped

networks:
  pihole-network:
     name: local-network
     external: true

# After this script, run these commands in the terminal:
# sudo docker exec -it pihole bash
# pihole setpassword 'Welkom#01'
```

This Docker Compose YAML file defines a single service named pihole, which runs the latest Pi-hole image in a container named pihole. It sets the hostname to pihole, assigns it a static IP address (192.168.139.3) on an externally defined Docker network named local-network, and configures environment variables such as the timezone (Europe/Amsterdam) and a web interface password (although the comment suggests the password is no longer effective).

The container mounts two volumes, one for Pi-hole configuration and one for DNSMasq settings. Open Media Vault will store these volumes in the docker shared folders you've created earlier, see section **3.1.3**. The container is configured to restart unless manually stopped. The cap_add section for NET_ADMIN is commented out but noted as required if using Pi-hole for DHCP services. What we are not planning to use now.



- Go to Services > Compose > Files
- Click on the + symbol to create a new docker compose yaml file named pihole
- Use the docker compose script for pihole and start this app with the up ↑ button
- If pihole is up and running it is accessible via IP address 192.168.139.3
- The admin panel for pihole is available via http://192.168.139.3/admin
- However we need to set an admin password before we can log in.

4.2 Going into the Pi-hole docker container via the terminal

```
omv login: manasse
Password:
Linux omv 6.12.22+bpo-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.22-1~bpo12+1 (2025-04-25) 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: Fri May  2 22:56:59 CEST 2025 on tty1
manasse@omv:~$ sudo docker exec -it pihole bash
[sudo] password for manasse:
pihole:/#
pihole:/# pihole setpassword 'Welkom#01'
  [✓] New password set
pihole:/#
pihole:/# exit
exit
manasse@omv:~$ _
```

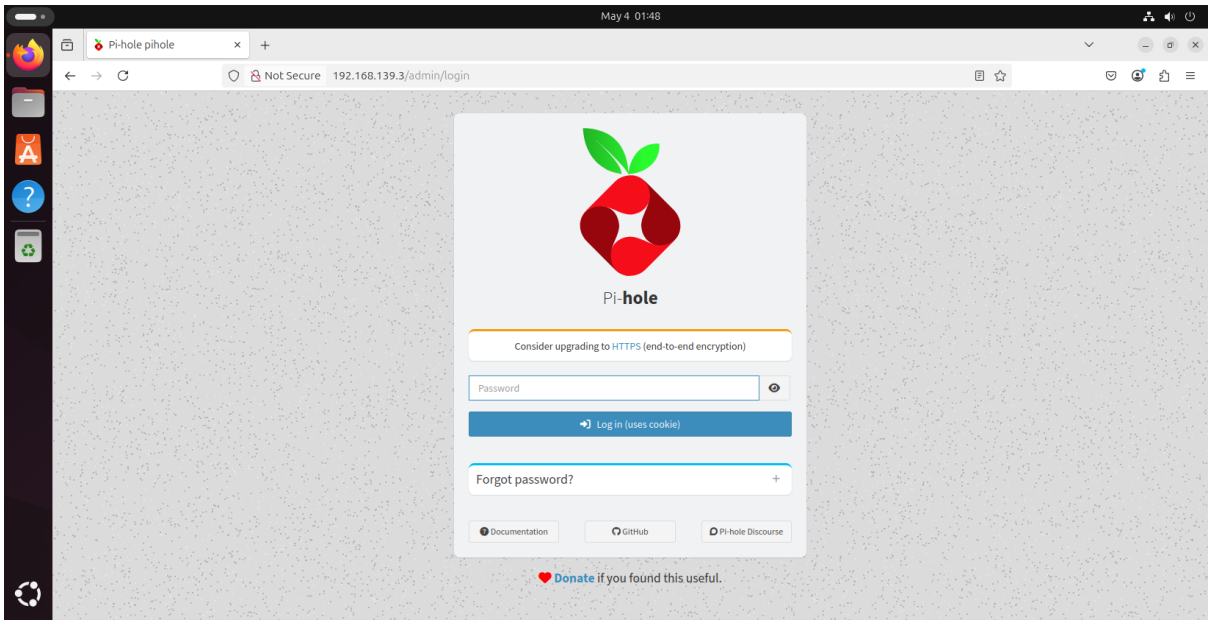
On the server where Open Media Vault is installed, open the Debian 12 terminal and log in.

In the terminal we need to run the following commands:

```
sudo docker exec -it pihole bash
pihole setpassword 'Welkom#01'
exit
exit
```

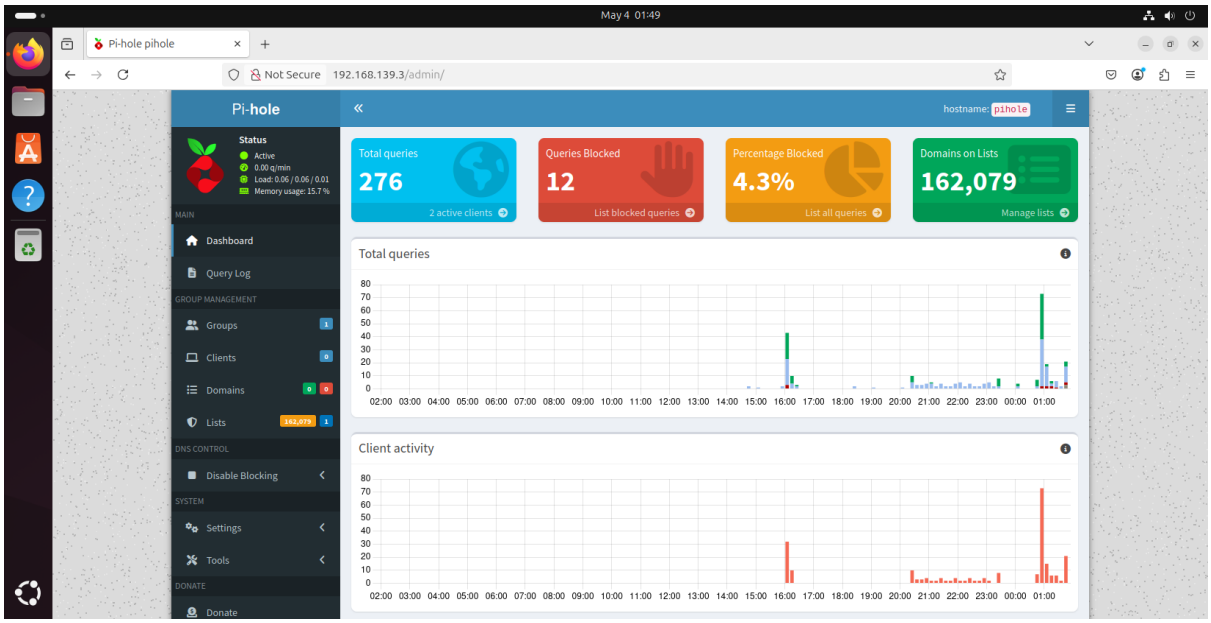
This will set the Pi-hole admin password to **Welkom#01**

4.3 Pi-hole Web Gui setup



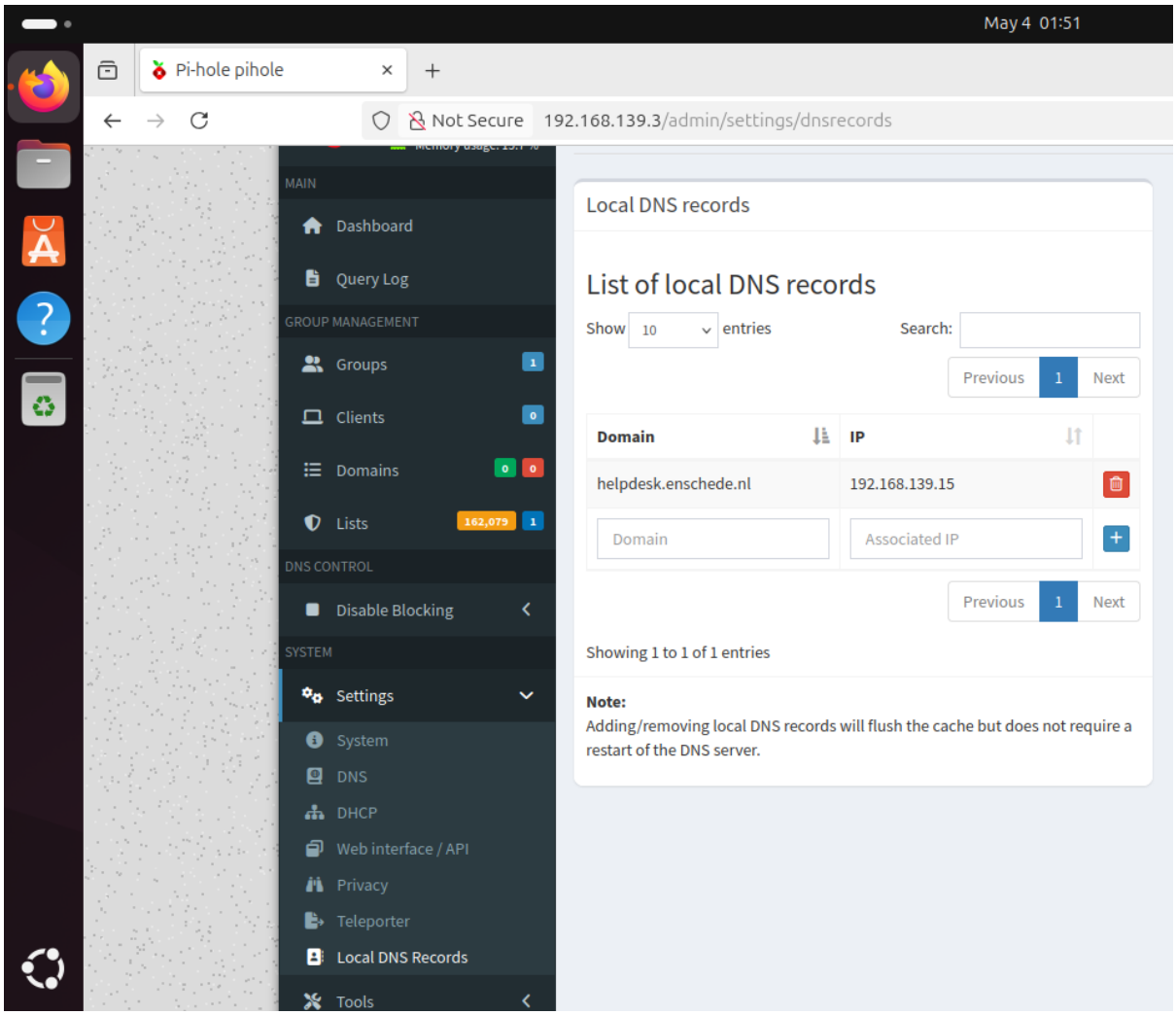
In the Ubuntu Desktop VM we can now use Firefox to access the Web Gui of Pi-hole:

- Go to http://192.168.139.3/admin
- Use the password **`Welkom#01`** and click on the Log in button



Pi-hole is used to block ads and trackers across your entire network by filtering DNS requests, the system that turns website names into IP addresses. When a device on your network tries to load an ad or connect to a tracking service, Pi-hole blocks the request before it ever reaches the internet. This makes browsing faster, safer, and more private. In addition, Pi-hole can act as a local DNS server, allowing you to create custom domain names for devices on your network (like printer.local). It can even serve as a DHCP server, assigning IP addresses to devices, which is useful if your router doesn't offer advanced network control. In our setup, we'll use Pi-hole to manage local DNS in our LAN network, giving us better control and easier access to our local devices.

We are going to create a custom domain name for the osTicket app which is using IP 192.168.139.15



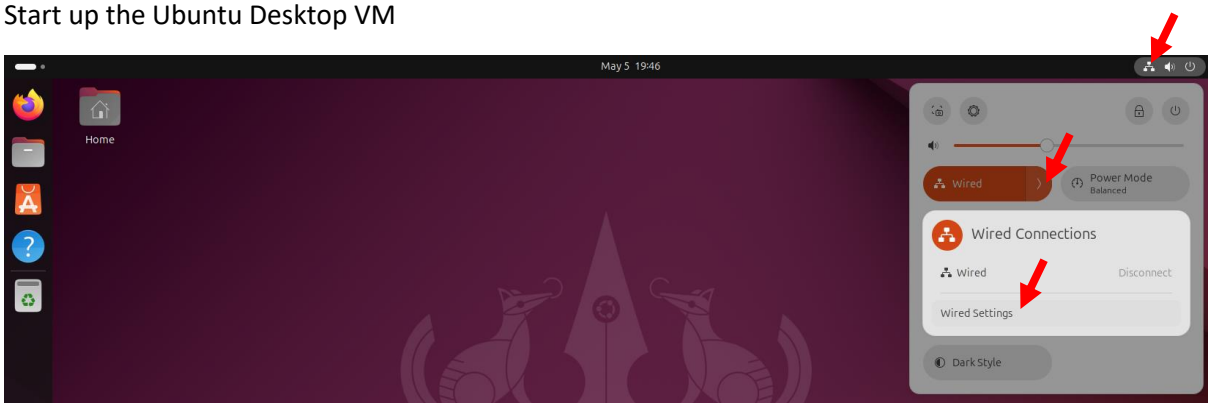
- Go to Settings > Local DNS Records
- Add the Domain **helpdesk.enschede.nl** and IP **192.168.139.15**
- Click on the + button

Pi-hole is now configured.

Now we need to configure the desktop clients so that they will use Pi-hole as their DNS server.

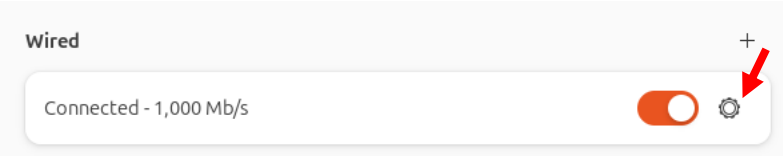
4.4 Network settings for clients using Pi-hole

Start up the Ubuntu Desktop VM

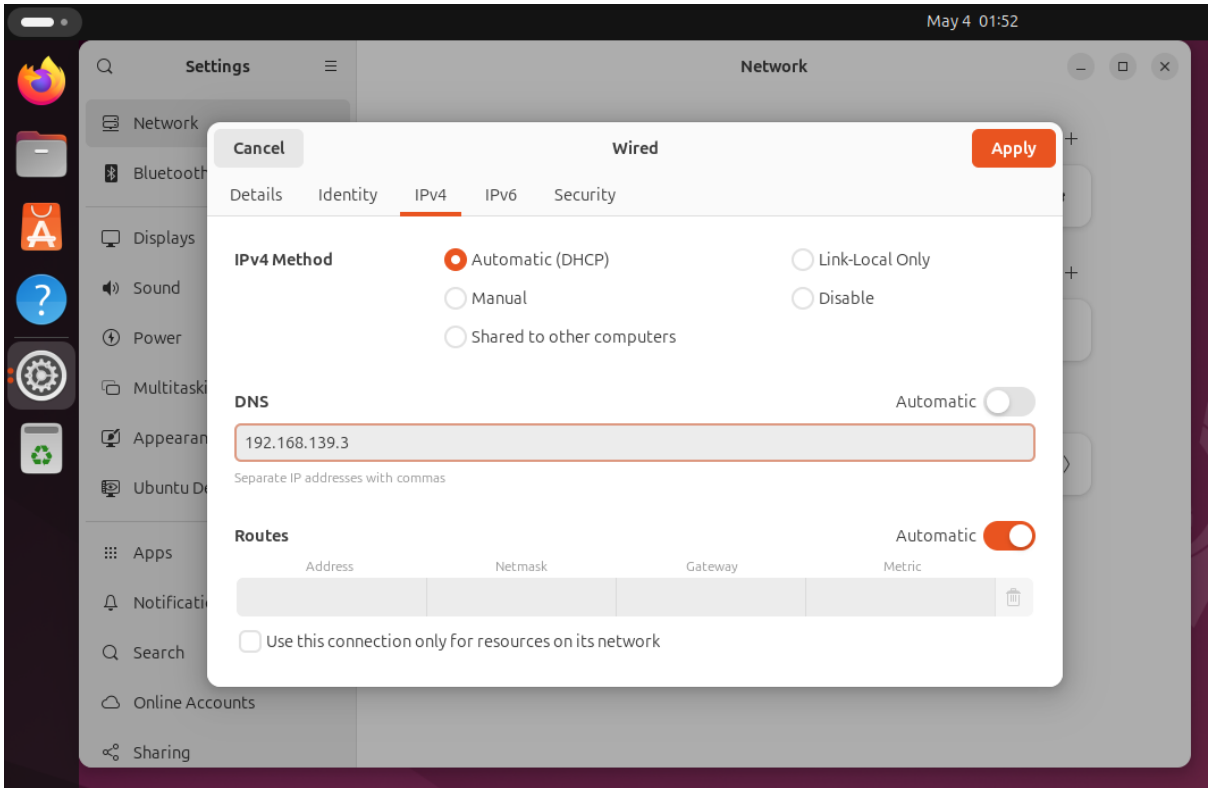


Click on the network settings in the top right corner

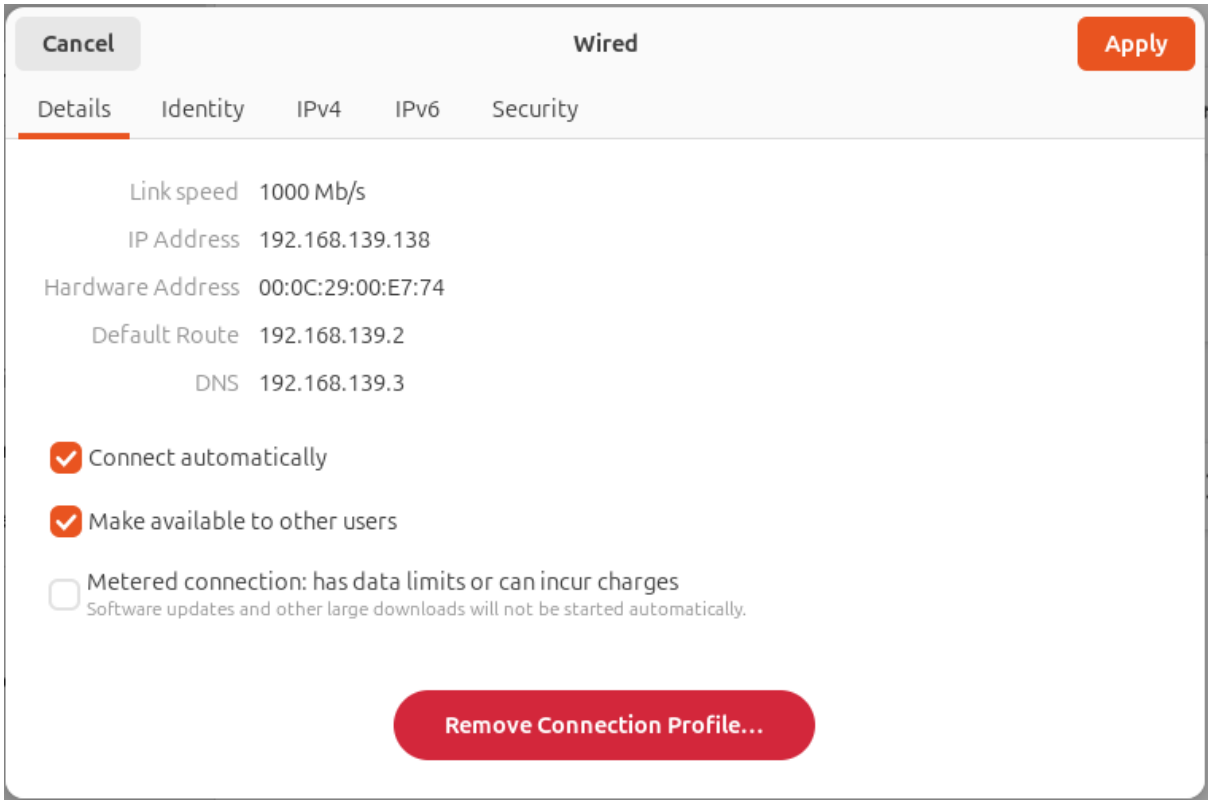
Choose the Wired Settings



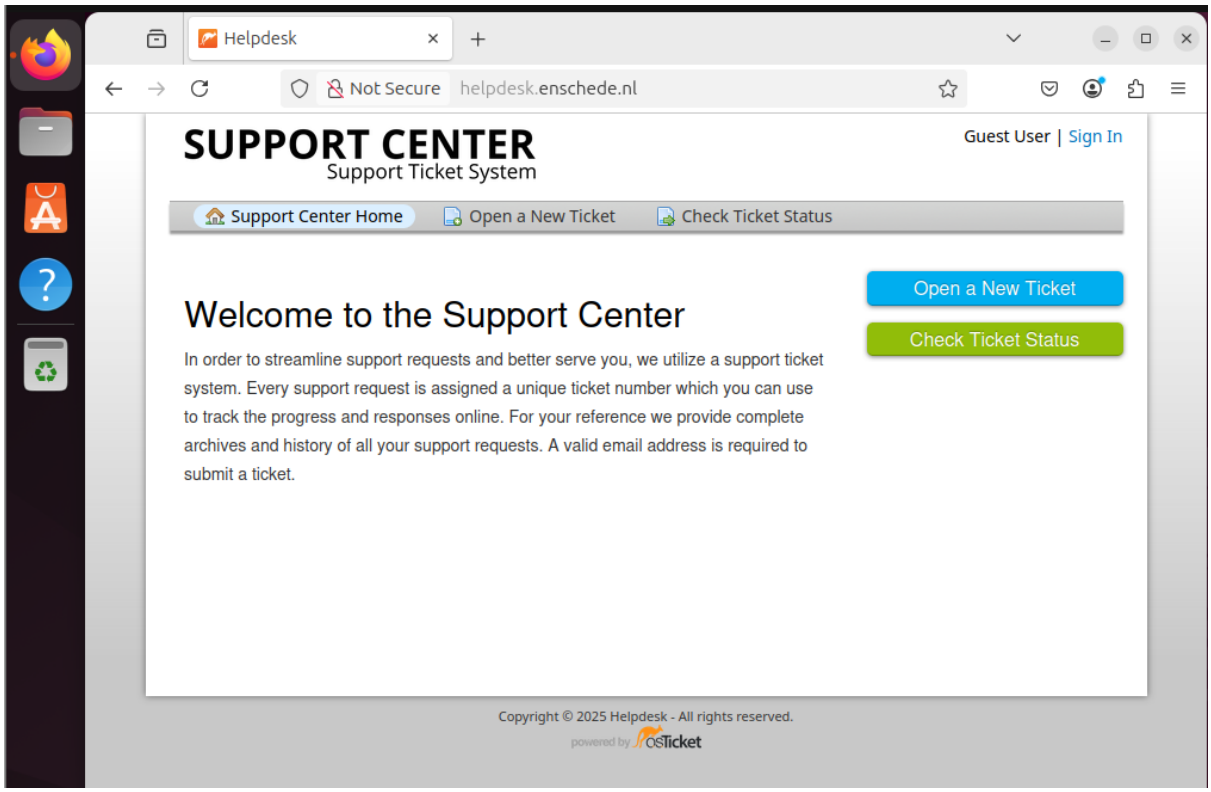
Click on the cog wheel to open the network configuration for the Wired network interface.



- Select IPv4
- Turn automatic DNS off
- Put the Pi-hole IP address in the text field.
- Click on the Apply button



- Select Details
- The DNS should now read 192.168.139.3



- Open Firefox
- Try if you can reach the domain name: http://helpdesk.enschede.nl/

4.5 Hardware advice

a) Eventually, Open Media Vault (OMV) needs to be installed on a bare metal server to serve as a reliable and efficient network-attached storage (NAS) solution. Considering the intended use in a municipal setting, with requirements for data integrity, uptime, scalability, and future-proofing provide the municipality of Enschede with a well-justified recommendation on which server hardware they should purchase. Your advice should take into account the performance needs of OMV and hardware compatibility. The municipality of Enschede only purchases servers from reliable well-known brands like **Dell**, **HP** or **Lenovo**. Clearly explain why your chosen bare metal server is an adequate and well-suited choice to run OMV for the municipality of Enschede.

b) The Municipality of Enschede is migrating to a Linux desktop environment and will be using either Ubuntu 24.04 Desktop or Linux Mint 22. There are 1500 employees, divided into three distinct groups:

- Office Users (1000 employees): These employees mainly use standard office applications such as word processing, spreadsheets, email, and web browsing.
- GIS Users (400 employees): These users regularly work with large 3D drawings related to buildings and underground infrastructure (e.g., pipelines). They edit and save these drawings using GIS and CAD applications.
- Mobile Users (100 employees): This group includes aldermen and city councillors who frequently travel and work without a fixed workstation. They require access to documents, email, and centrally stored files while on the move.

The municipality only purchases desktops, laptops, or tablets from reliable, well-known brands such as **Dell**, **HP**, or **Lenovo**.

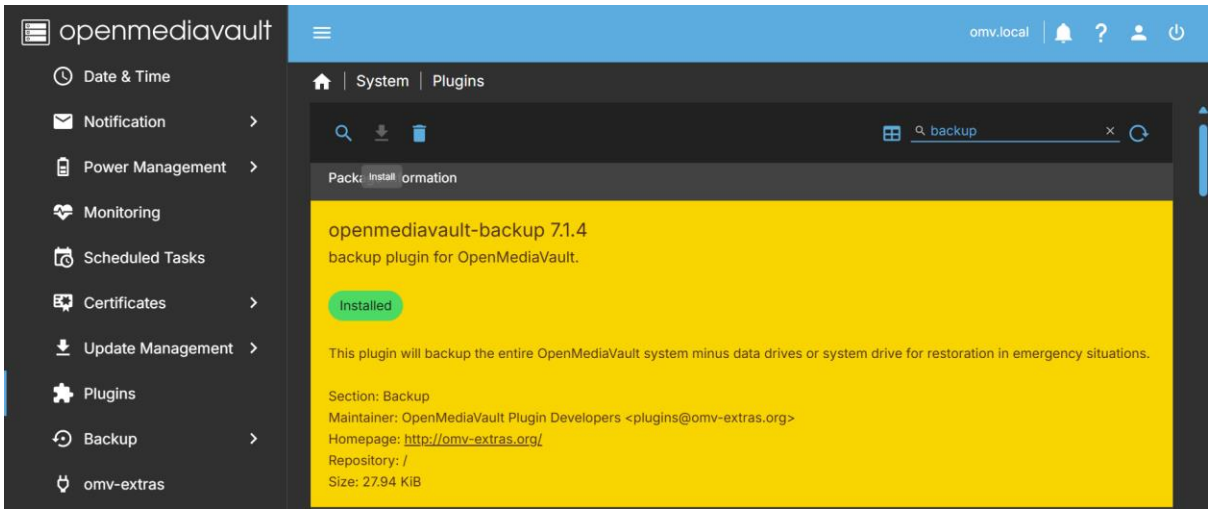
What hardware would you recommend for each of these three groups? Use the **SMART** criteria (**S**pecific, **M**easurable, **A**chievable, **R**elevant, **T**ime-bound) to describe your hardware choices for each group.

5 Week 5 – Backups & Security

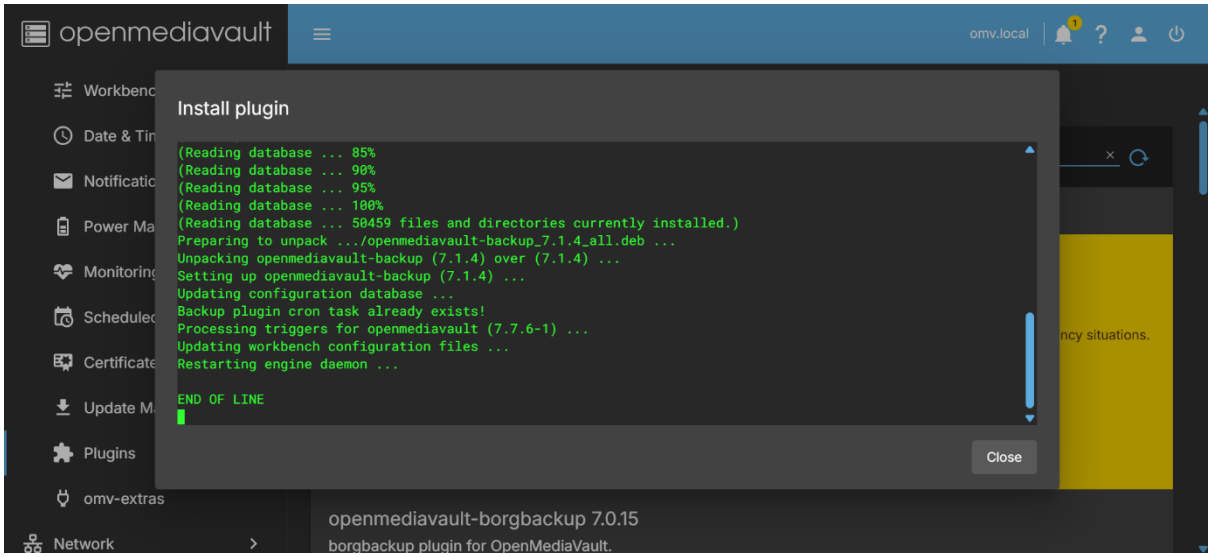
Backups and security are essential in IT infrastructure to protect critical data from loss, corruption, or cyberattacks. They ensure business continuity and safeguard sensitive information against unauthorized access or system failures.

5.1 Backup OS drive of Open Media Vault

Install the backup plugin in open media vault

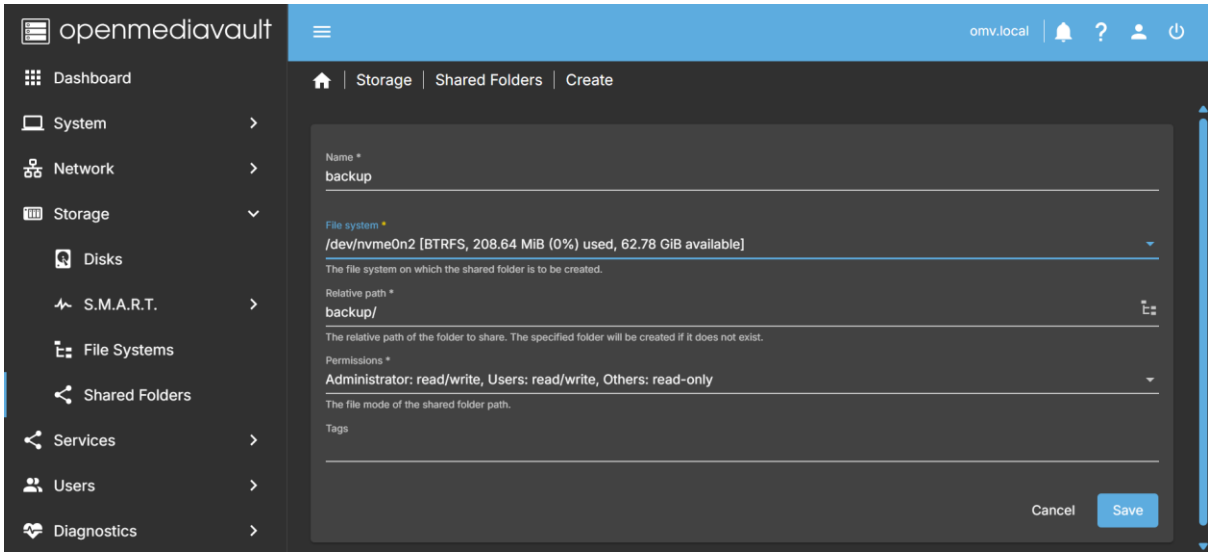


Select the openmediavault-backup plugin and install it

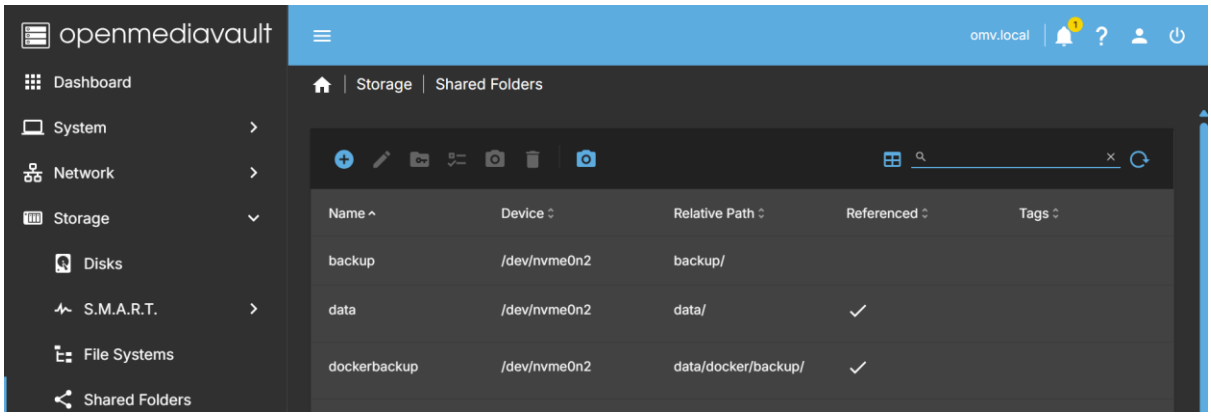


If the installation fails you can restart it

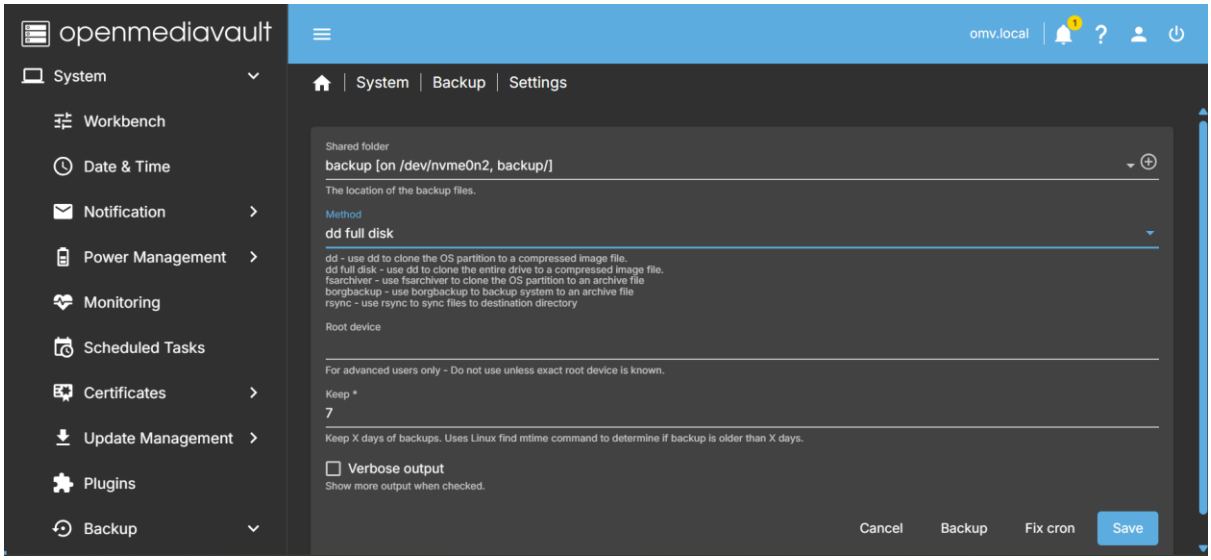
The above image shows a successful installation of the backup plugin



- Go to Storage > Shared Folders
- Create a new shared folder named backup on the BTRFS RAID1 array
- Click on the Save button
- Apply the pending configuration changes



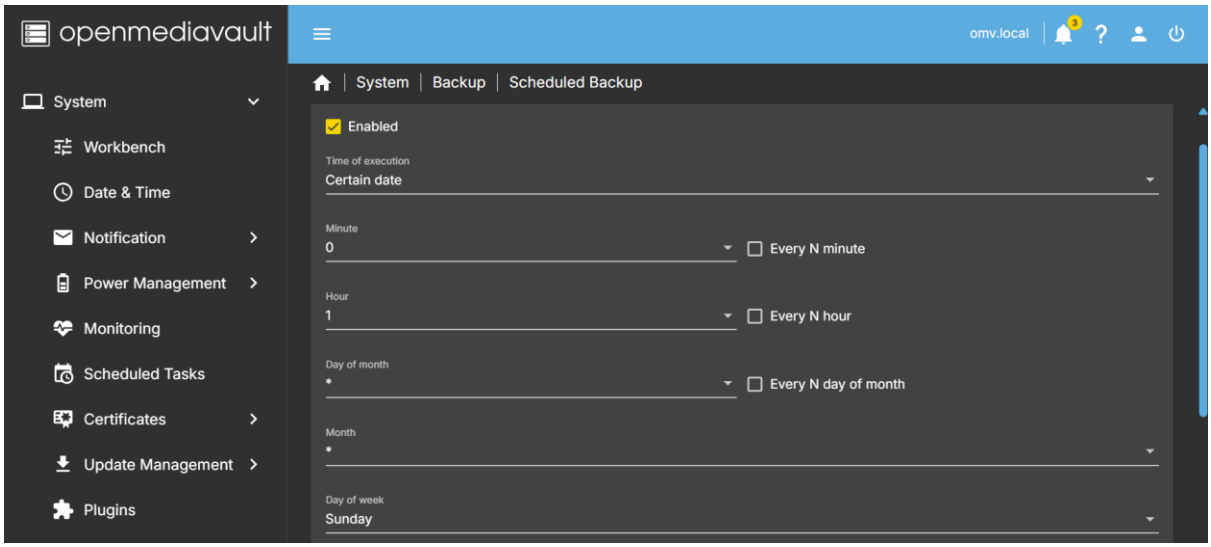
The backup shared folder should now be available for our backup plugin.



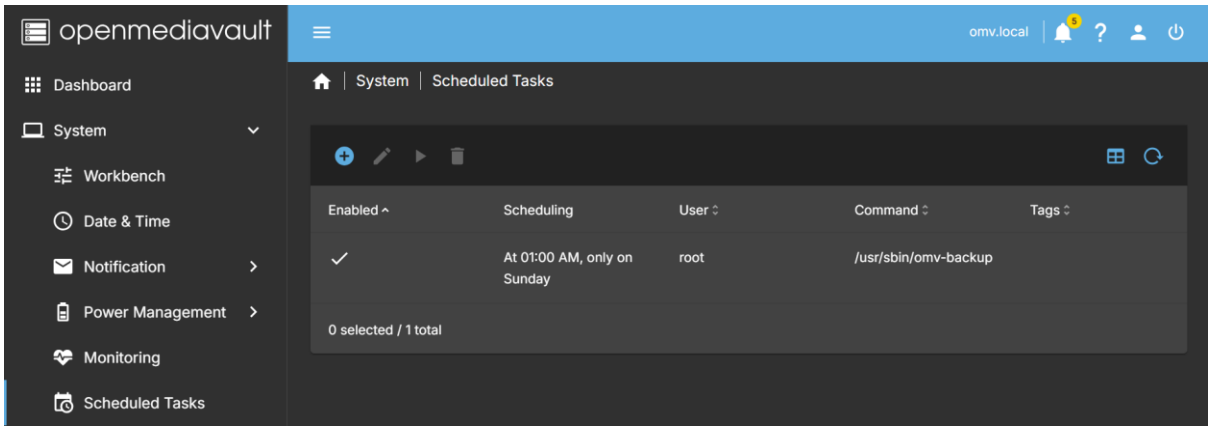
- Go to System > Backup > Settings

- Fill in the form:
    - Shared Folder: backup
    - Method: dd full disk
    - Keep: 7
    - Verbose output enabled is optional
- Click on the Save button

If you click on the Backup button the backup process will start and this will take some time.

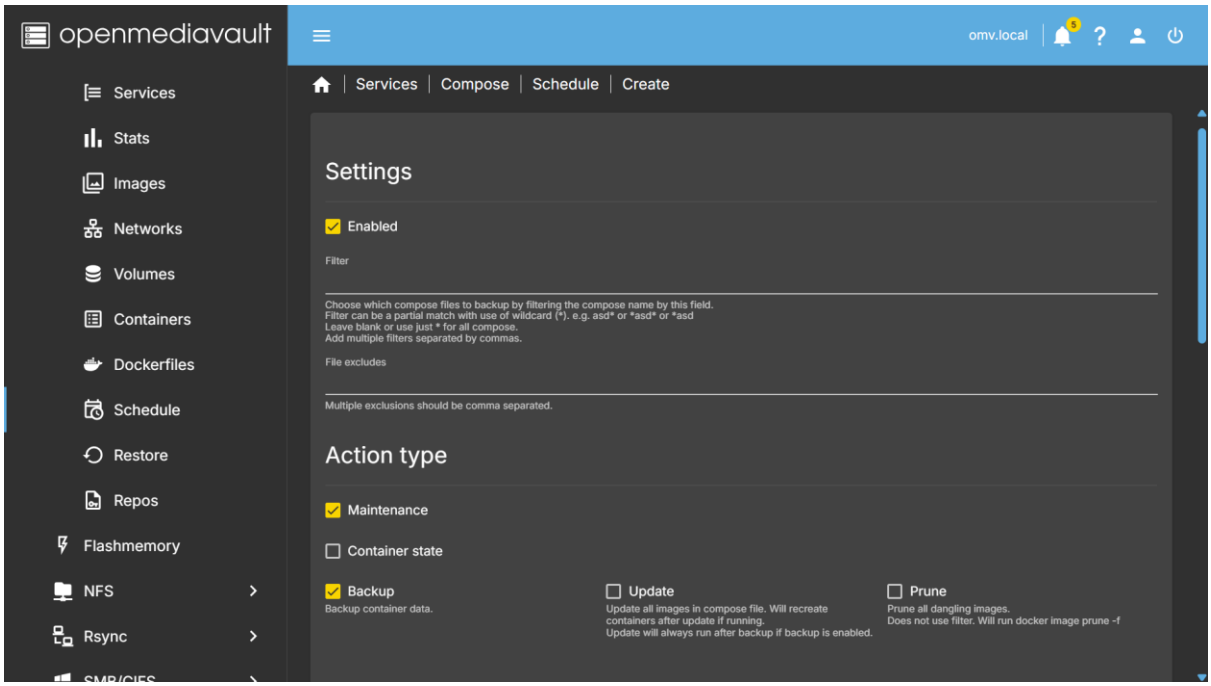


- Go to System > Backup > Schedule
- We want a weekly back up on Sunday
- Click on Enabled
- Set the appropriate time
- Click on the Save button
- Apply the pending configuration changes

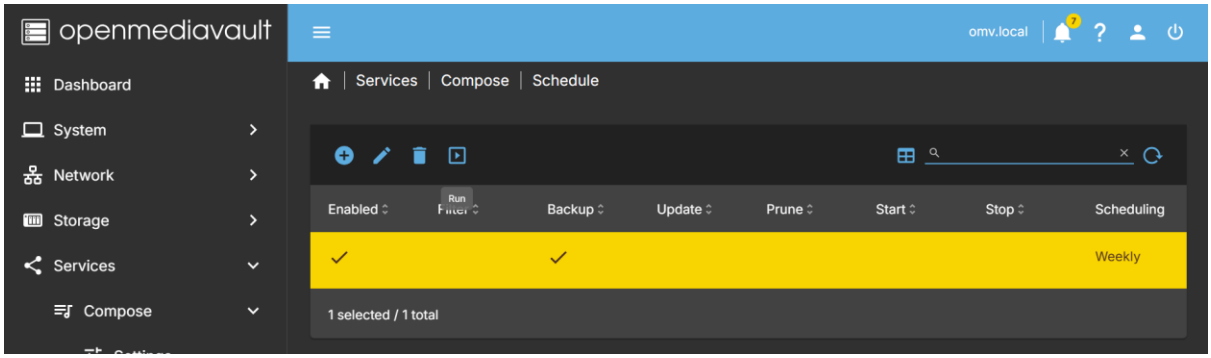


If you go to System > Scheduled Tasks you can see the planned backup cron job.

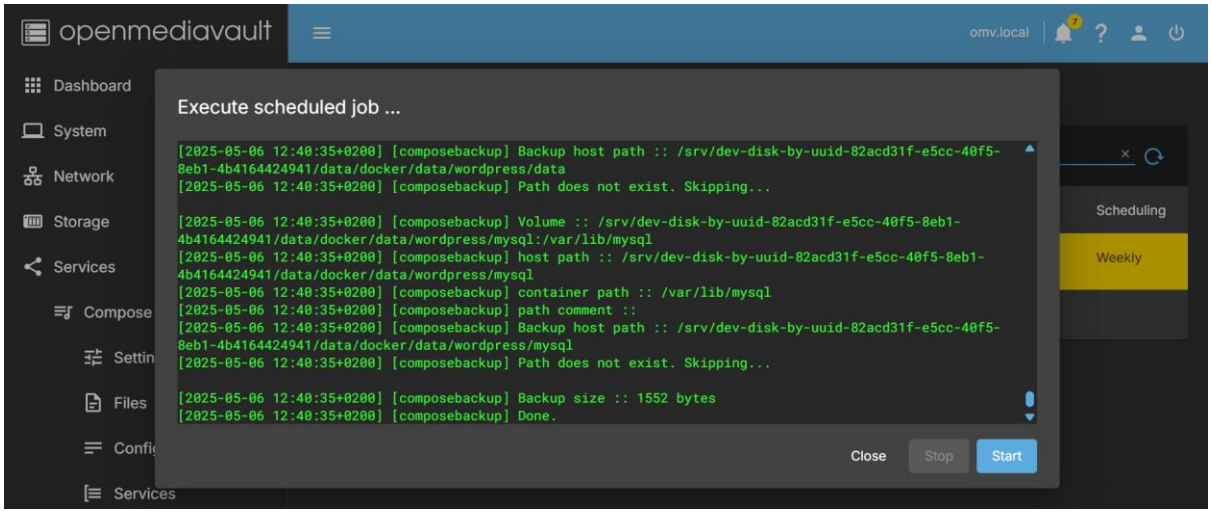
5.2 Back up docker applications



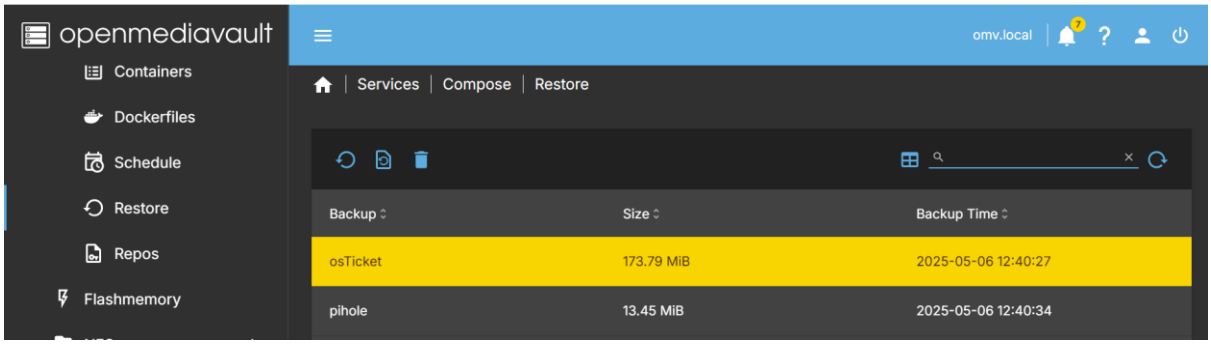
- Go to Services > Compose > Schedule
- Click on the + symbol to create a new backup job
- Click on Enabled
- Action type: select Maintenance and Backup.
- Do a weekly backup of the docker apps
- Click on the save button
- Apply the pending configuration changes



- You can now also choose to run this task manually
- Select the Scheduled task and click on the run button 



- Click on the Start button
- Close this screen if the backups are completed
- This will back up your docker apps



- Go to Services > Compose > Restore
- Here you can find your backups for the docker apps

5.3 Scanning for open ports

Open the terminal and Install **nmap** on the Ubuntu Desktop with the following commands:

```
sudo apt update
sudo apt install nmap
```

Run the following command in the terminal to scan the open ports on the Open Media Vault:

```
sudo nmap -p0- -v -A -T4 helpdesk.enschede.nl
```

- Make screenshots of the results.
- What would you advise to secure the Open Media Vault based on the scan results?

5.4 Backup tools for Ubuntu Desktop

Backups are necessary to protect user and system data on the Ubuntu desktop.

5.4.1 Install Déjà Dup and Timeshift

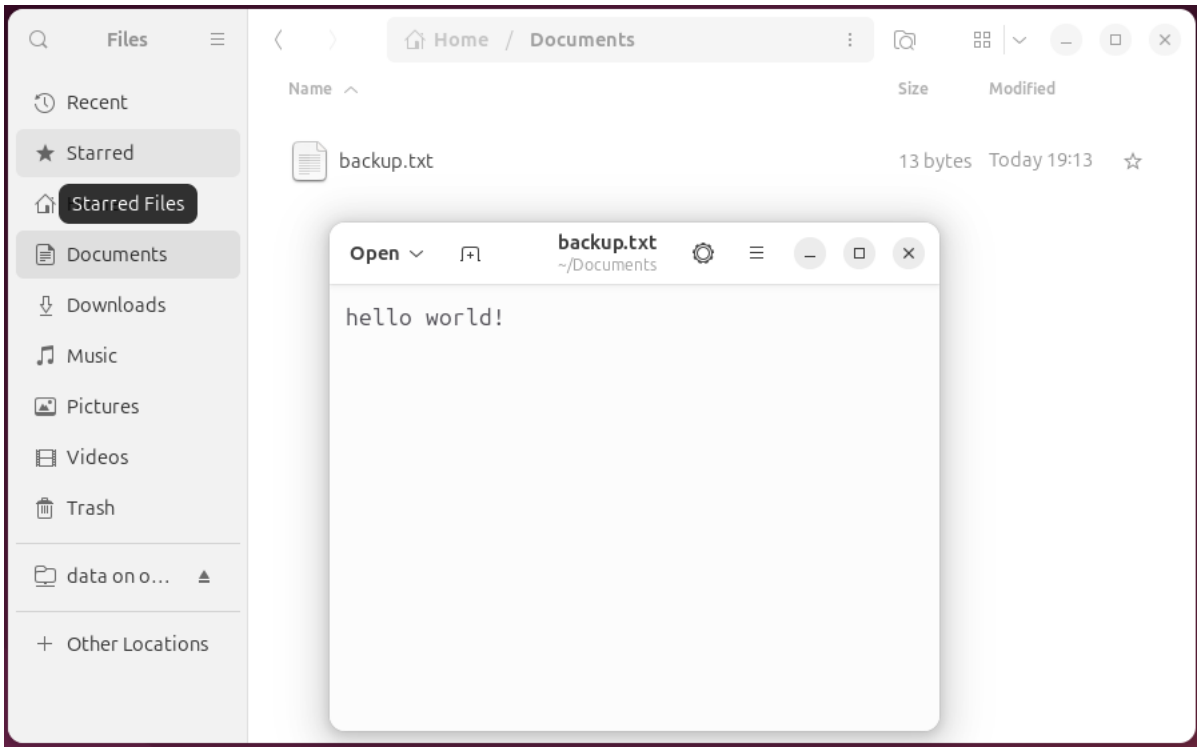
Open the terminal and Install **Déjà Dup** and **Timeshift** on the Ubuntu Desktop with the following commands:

```
sudo apt update
sudo apt install deja-dup
sudo apt install timeshift
```

Déjà Dup is a simple and user-friendly backup tool for Linux systems. It provides an easy way to back up and restore your important files, offering features like scheduled backups, encryption, and support for cloud storage services. Designed to be intuitive, Déjà Dup helps users protect their data without the complexity of advanced backup software. You can also use this tool to back up your files to an Open Media Vault server via SMB, making it easy to store backups on a network-attached storage device.

Timeshift is a powerful backup tool focused mainly on creating and restoring system snapshots, allowing you to quickly recover your entire system to a previous state after problems like failed updates or system crashes. Unlike Déjà Dup, which is designed primarily for backing up personal files and data, Timeshift works at the system level, protecting system files and settings rather than individual user documents. This makes Timeshift ideal for system recovery, while Déjà Dup is better suited for personal file backups.

5.4.2 Create sample user data for backup testing

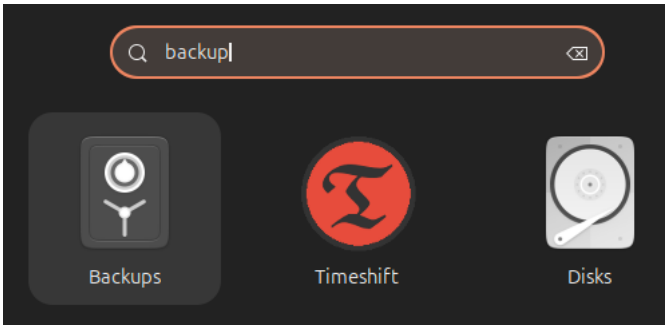


Place a text file in the user's Documents folder.

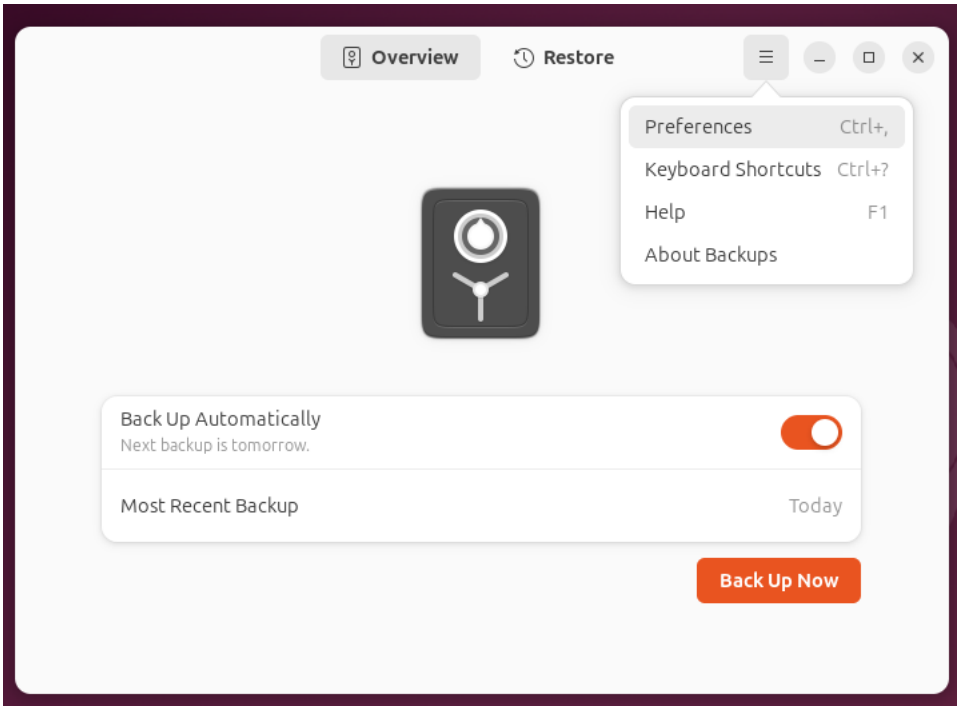
5.4.3 Backup user data with Déjà Dup

Click on the show apps button  .

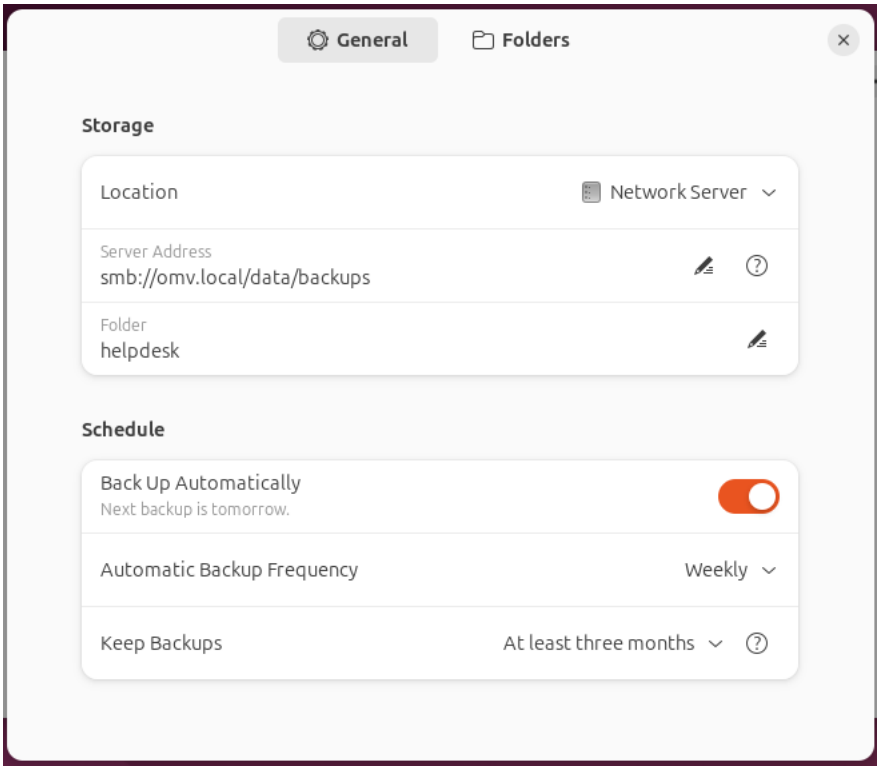
Search for backup. This will find the applications Backups(Déjà Dup) and Timeshift.



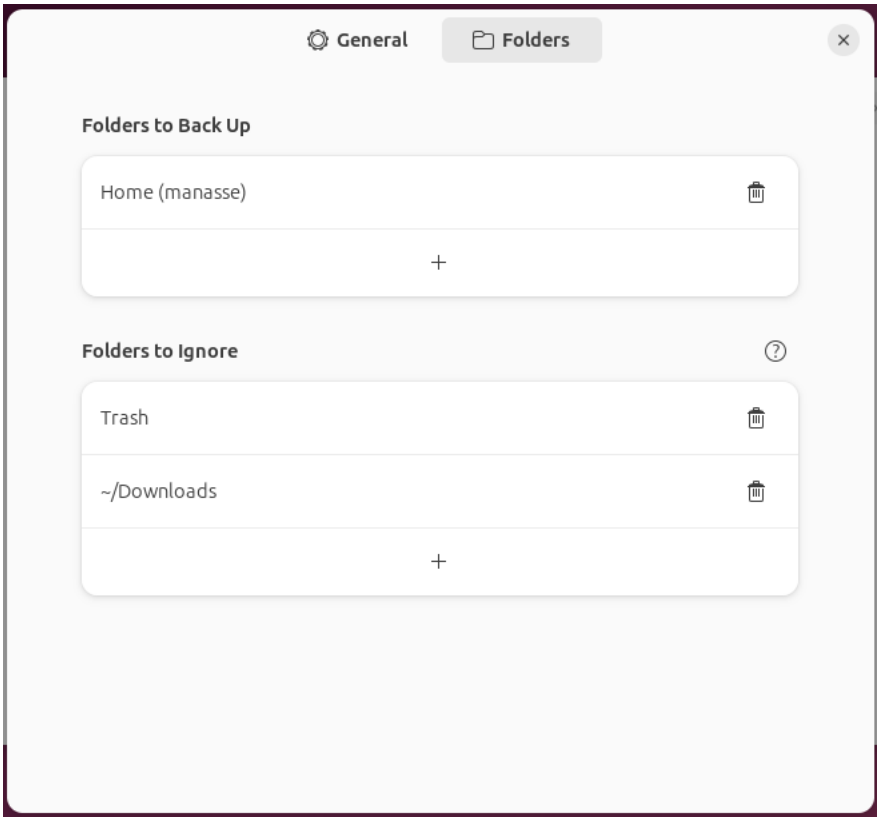
Select Backups to start the Déjà Dup application.



First you need to edit the Preferences to setup your first Backup.

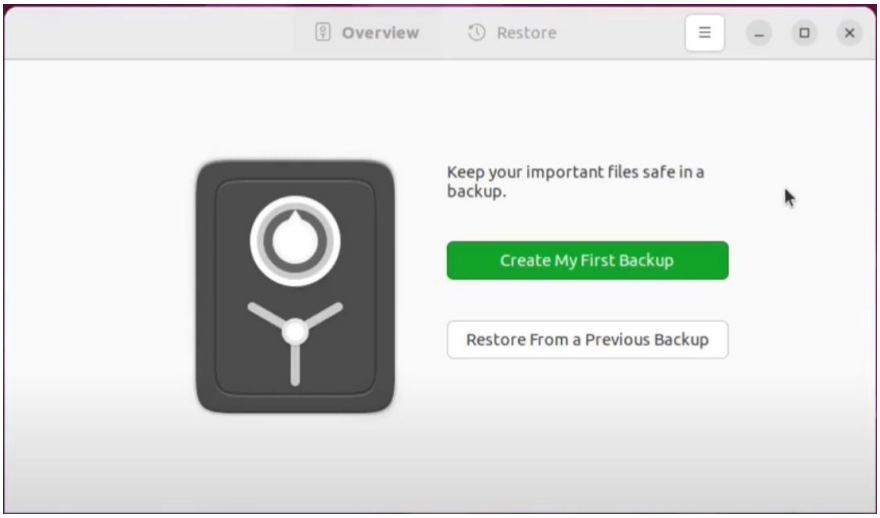


The backup of your home folder should be stored on the open media vault NAS. We are going to use the SMB protocol for this to access the shared data folder. Schedule weekly automatic backups and keep these backups at least three months.



If you select Folders you can see which folders will be in the backup.

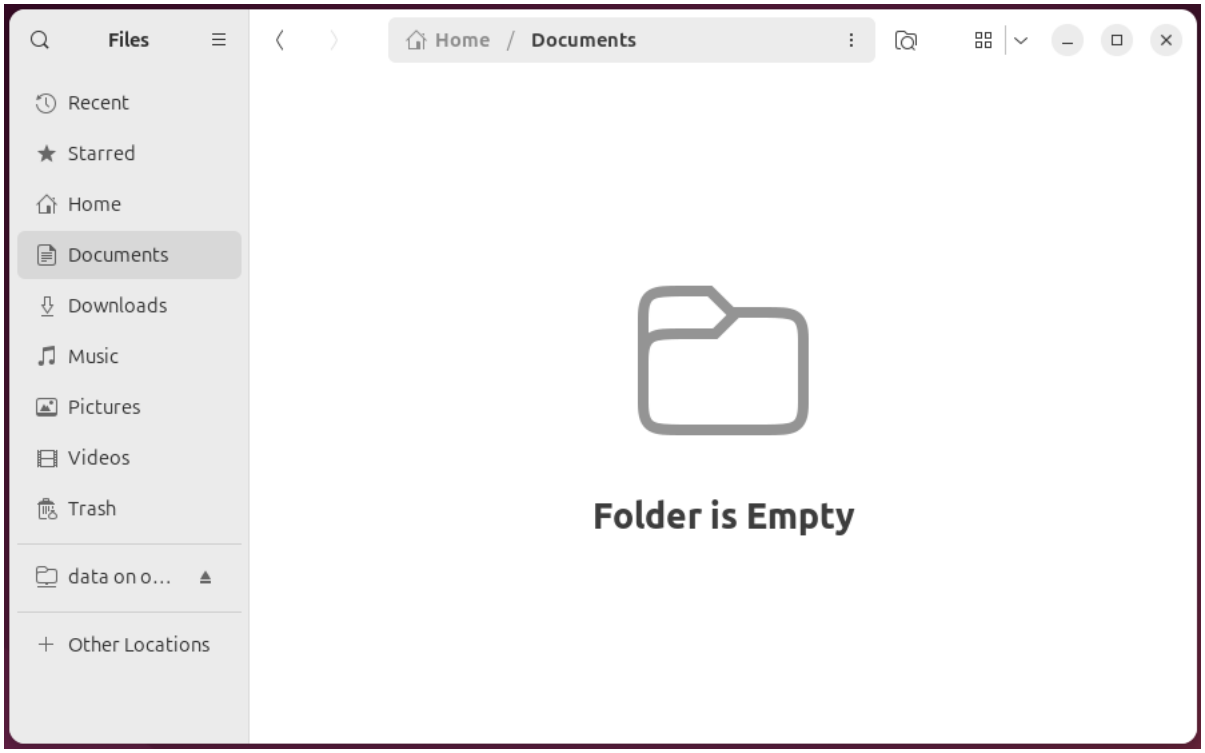
Close this preferences window by clicking on the x in the top right corner.



Now click on the **Create My First Backup** button and make a Backup of the user's home folder.

Also use encryption when making this backup. Don't forget to write down the encryption password.

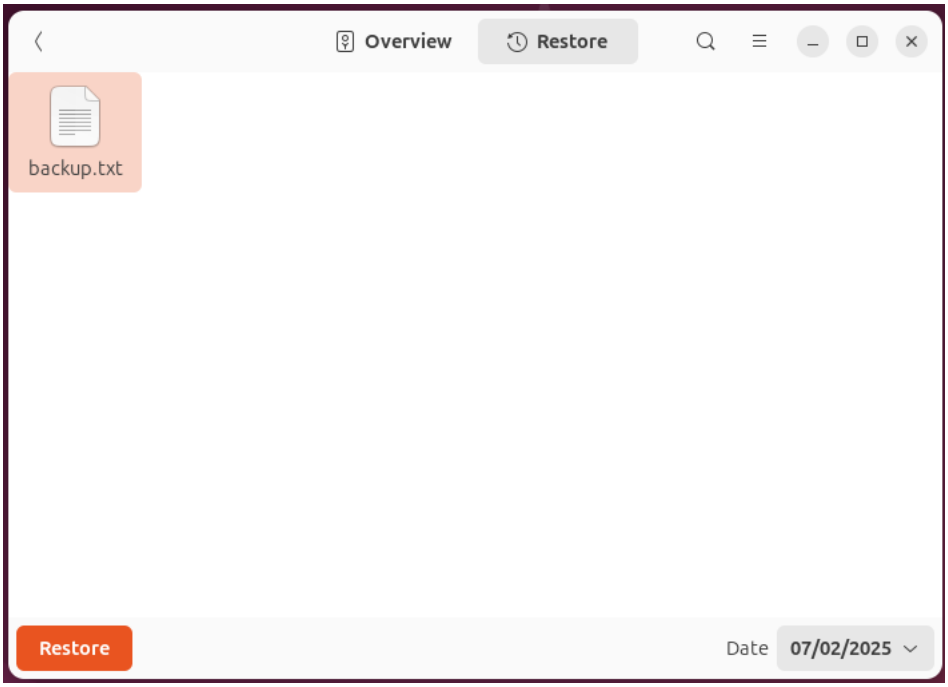
5.4.4 Delete user data



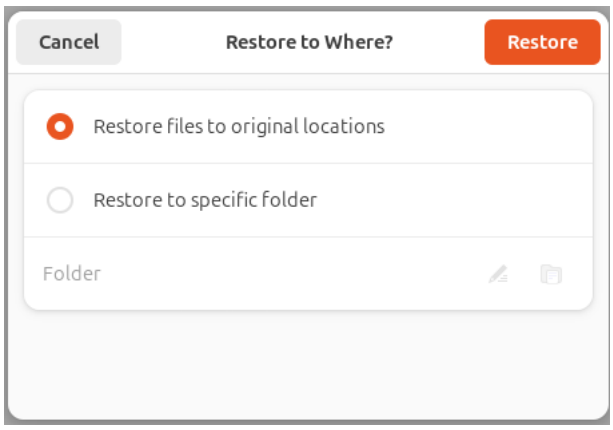
Delete the created text file. So, now you should have an empty Documents folder.

5.4.5 Restore user data with Déjà Dup

Start Backups(Déjà Dup)



- Click on Restore at the top of the window.
- Find the text file in the backup in the Documents folder and select it.
- Click on the Restore button.



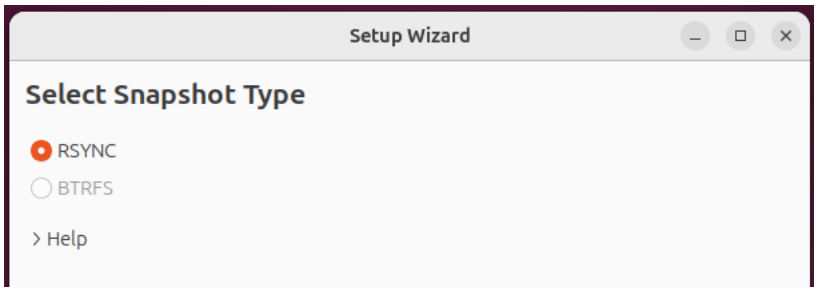
- Select Restore files to original locations
- Click on the Restore button.

Check the user's Documents folder if the text file has been restored.

5.4.6 Using Timeshift for system backups

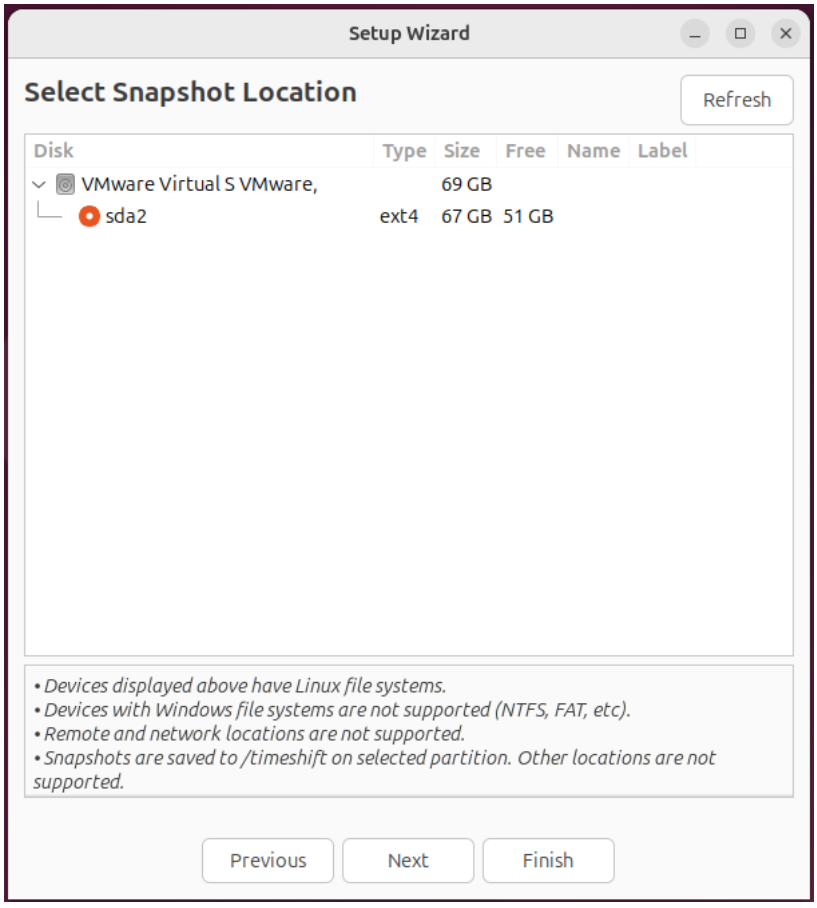
Timeshift is a tool designed for creating system backups, allowing you to easily restore your Ubuntu system to a previous state in case of problems. It focuses on backing up system files and settings rather than personal user data, so it's not intended for backing up documents, photos, or other personal files. For backing up personal data, we use Déjà Dup, which is designed specifically to protect user files and folders. Timeshift is especially useful when something goes wrong during system updates or software installations, allowing you to quickly roll back your system to a stable state.

- Start the Timeshift application.

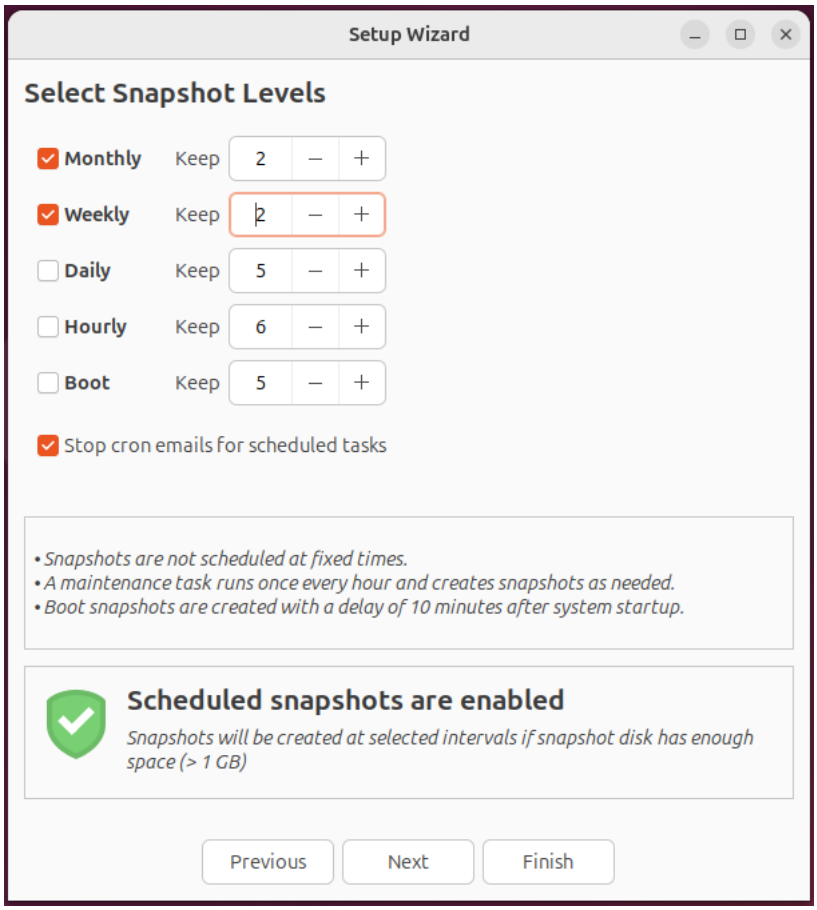


We need to configure the application before we can make system snapshots.

- Select RSYNC
- Click on Next

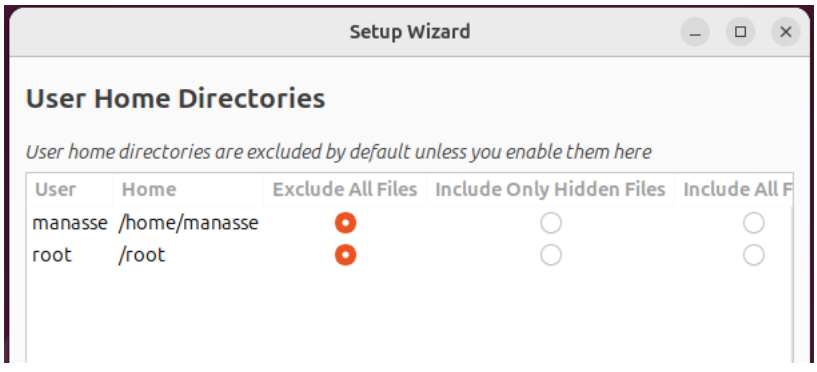


- **Note:** It's more prudent to store snapshots on a dedicated USB hard drive separate from the main system.
- Select Next

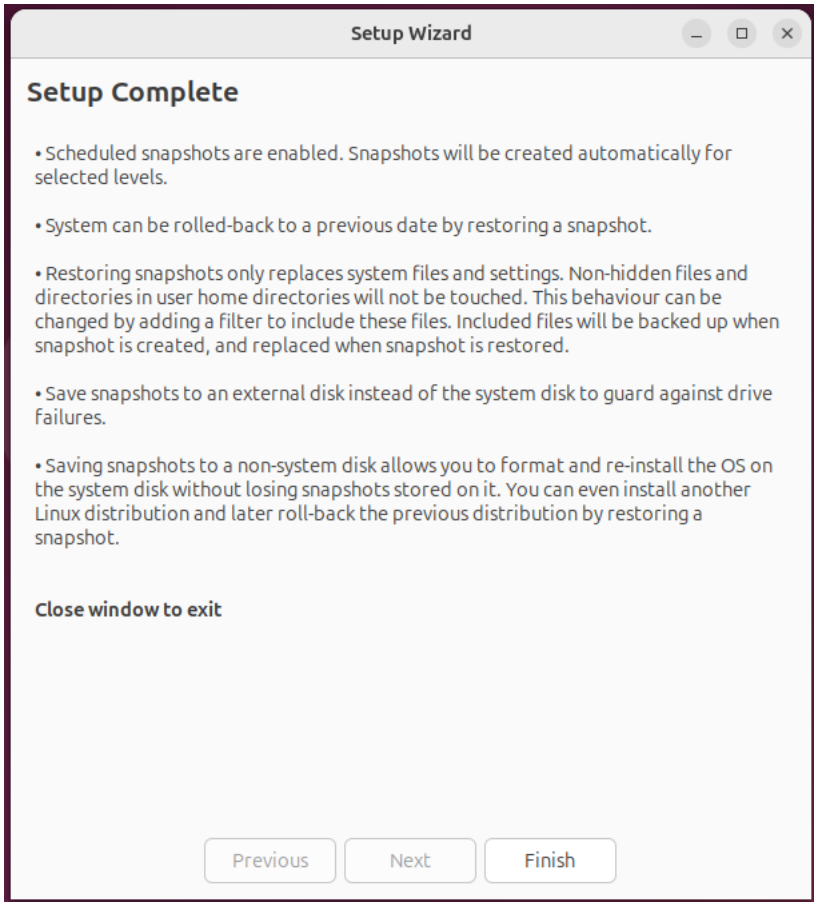


Set monthly and weekly RPO snapshots:

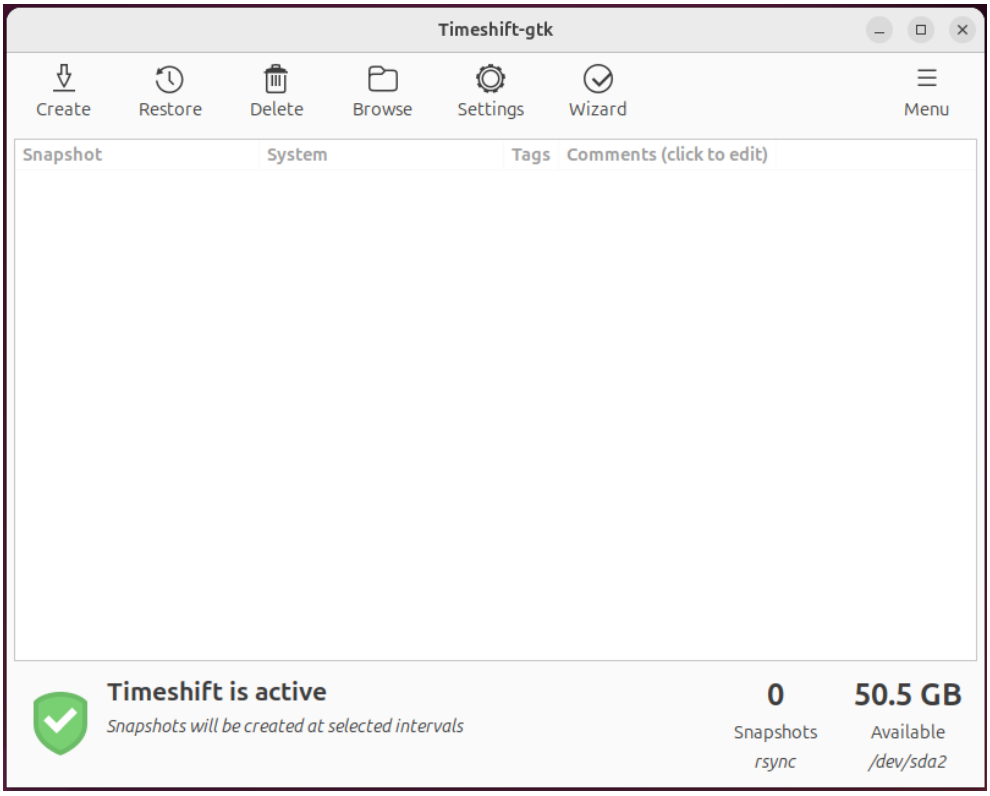
- 1 monthly and 1 weekly snapshot should be enough for testing purposes.
- Click on Next.



- Exclude user Home directories and root
- Click on Next.

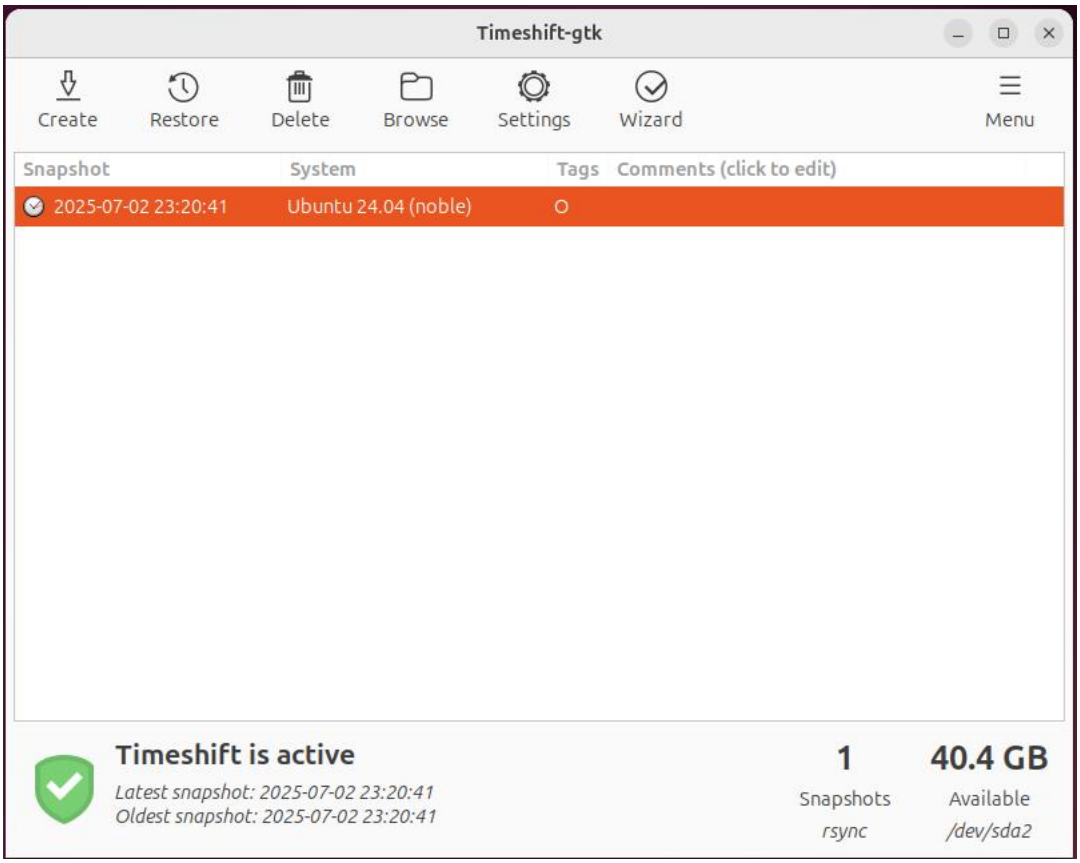


Click on Finish.



Click on Create.

This will create the first System Snapshot. Wait for the process to complete.



5.4.7 Final thoughts on backups

Using Timeshift with Déjà Dup is a smart backup strategy. Timeshift protects your system by creating snapshots of system files, allowing quick recovery from updates or configuration issues. Déjà Dup complements this by backing up your personal files, supporting encryption and cloud storage. Together, they provide full coverage: Timeshift for system stability, and Déjà Dup for safeguarding your data.

5.5 Cyberattack Eindhoven University of Technology (TU/e)

Recently the Eindhoven University of Technology (TU/e) was hit by a cyberattack. The municipality of Enschede wants to learn from this incident. Read the following article and the management summary compiled by Fox-IT. Then complete the following assignment.

Link to article: here

The NIST Cybersecurity Framework (NIST CSF) is organized into five core functions:

Identify, Protect, Detect, Respond, Recover.

Something went wrong during the hack. Which NIST functions, must the TU/e improve?

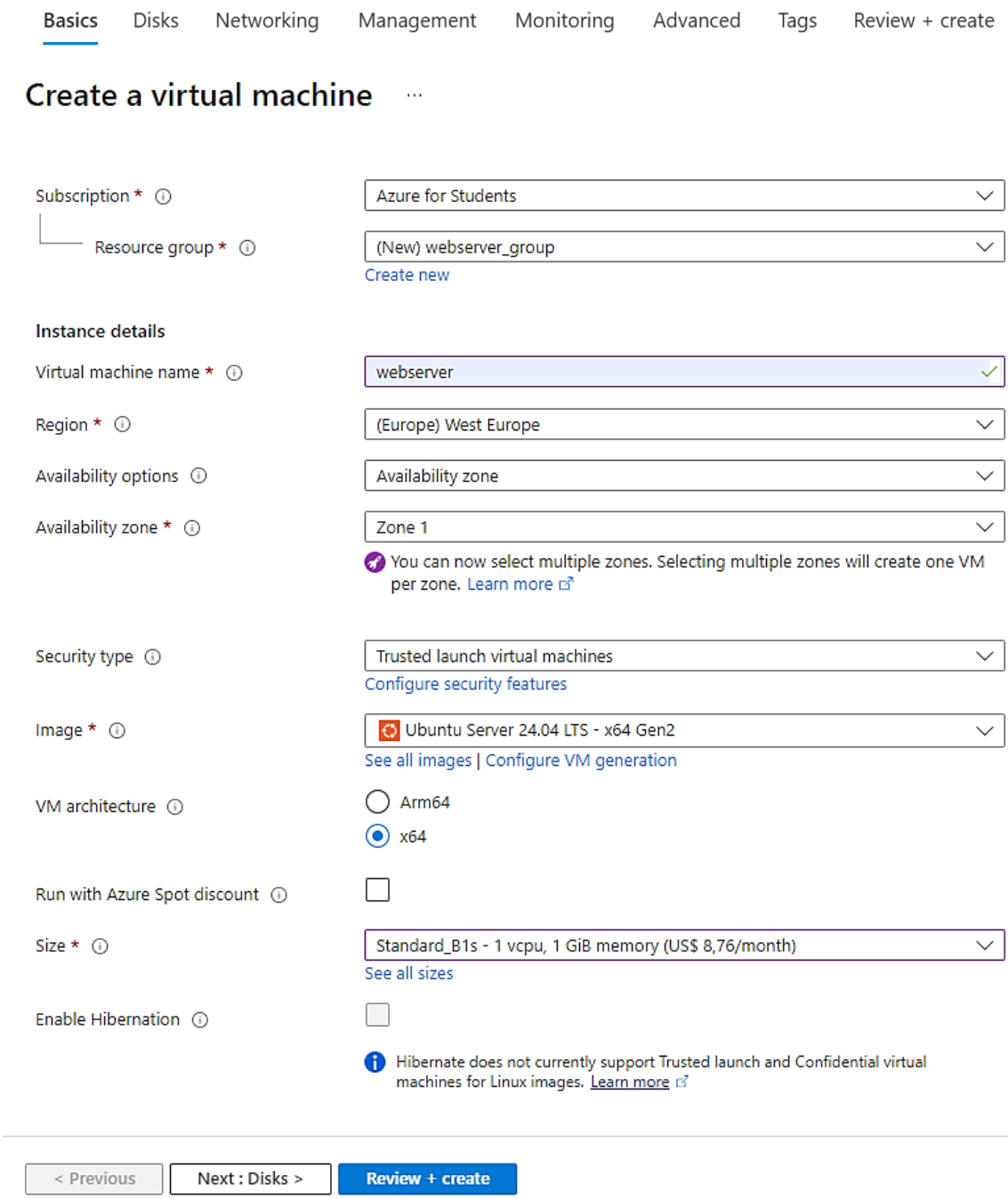
6 Week 6 – Cloud

This week you will deploy a virtual machine on Azure and install **Nextcloud** on it. First go to: https://azure.microsoft.com/en-us/free/students and get $100 Azure credit.

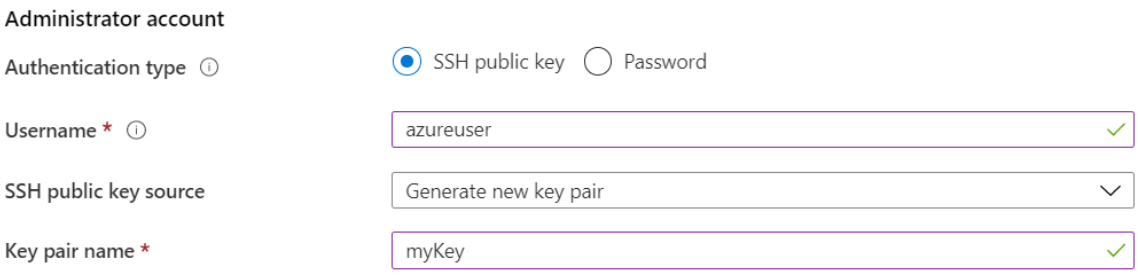
6.1 Nextcloud as Azure VM

Steps in the Azure Web Portal (GUI)

1. **Open**: https://portal.azure.com
   Go to: *Azure Portal > Virtual Machines > Create > Azure virtual machine*
2. **Fill out the basics**:



3. **Create SSH public key:**



4. **Finish the rest of the wizard**:
    - On the "Networking" tab, make sure you:
        - Allow **HTTP (port 80)**, **HTTPS(port 443)** and **SSH (22)**
    - Push on the button Review + Create 

    - Download the private key to your host machine's Downloads folder

After Deployment

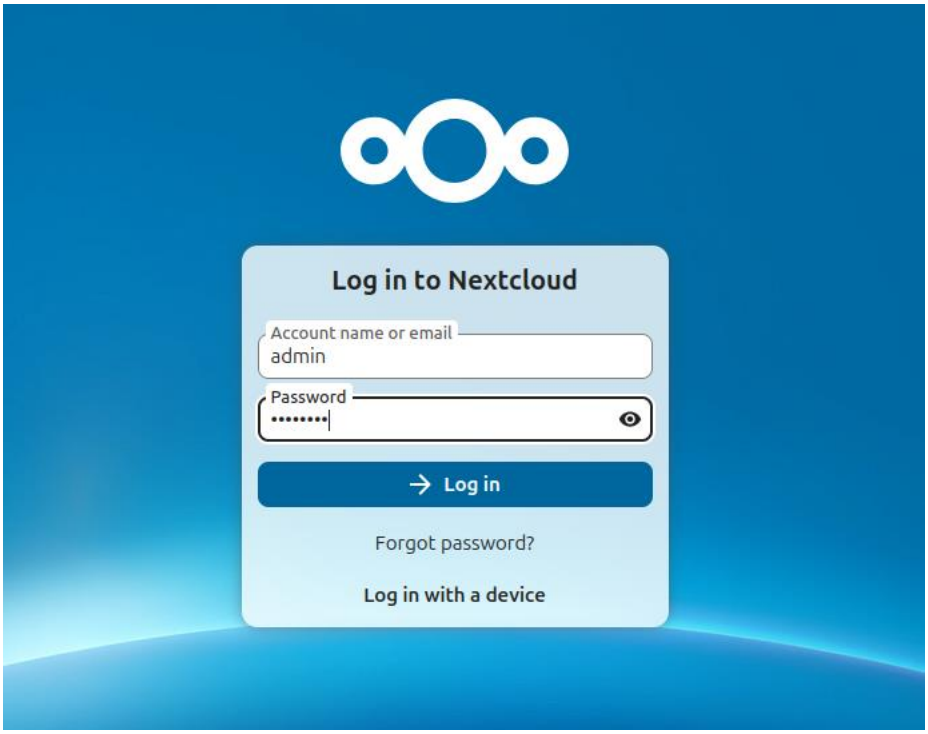
- Wait for the VM to boot (~2–3 minutes).
- Look up your public IP address of this VM
- Connect to your Azure VM with SSH:
    - If you are on a Mac or Linux machine, open a Bash prompt and set read-only permission on the .pem file using `chmod 400 ~/Downloads/myKey.pem`. If you are on a Windows machine, open a PowerShell prompt.
    - At your prompt, open an SSH connection to your virtual machine. Replace the IP address with the one from your VM, and replace the path to the .pem with the path to where the key file was downloaded.
    - `ssh -i ~/Downloads/myKey.pem azureuser@123.123.123.123`
- Finish the Nextcloud installation with the bash commands below

You need your actual public IP address of the Azure VM for these commands to work.
NOTE: Replace IP address 123.123.123.123 with your actual public IP address.
Type these lines one by one in the terminal once you are logged in to the Azure VM via SSH:

```
sudo snap install nextcloud
sudo nextcloud.manual-install admin password
sudo nextcloud.occ config:system:set trusted_domains 1 --value=123.123.123.123
sudo nextcloud.occ config:system:set trusted_domains 2 --value=cloud.enschede.nl
sudo nextcloud.enable-https self-signed
```

Fire up your favourite web browser

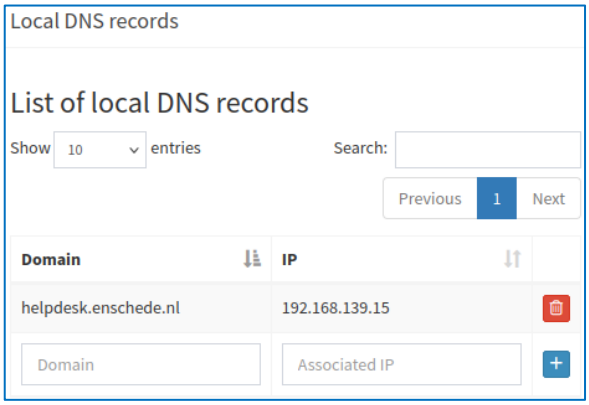
- Go to https://<public-ip-nextcloud> in your browser.
- You'll see the **Nextcloud login Web Gui: Username: admin, Password: password**
- Log in to Nextcloud



6.2 Include the public IP of Nextcloud in the Pi-hole local DNS

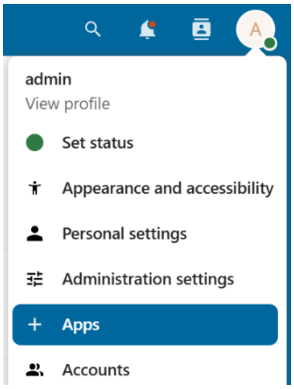
We are going to create a custom domain name for the Nextcloud Azure VM.

- Log in to Pi-hole
- Go to Settings > Local DNS Records
- Add the Domain **cloud.enschede.nl** and the public IP of the Nextcloud VM
- Click on the + button

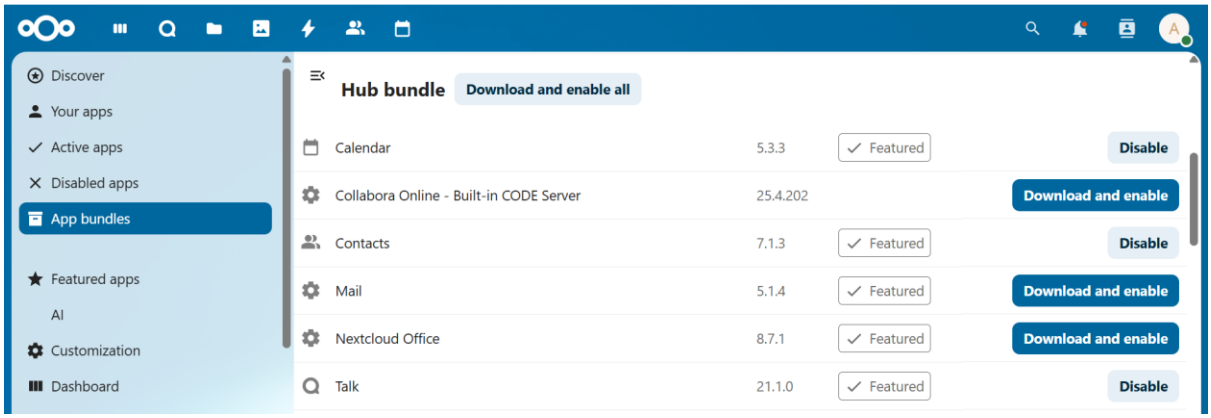


Test the DNS configuration on your Ubuntu Desktop VM.

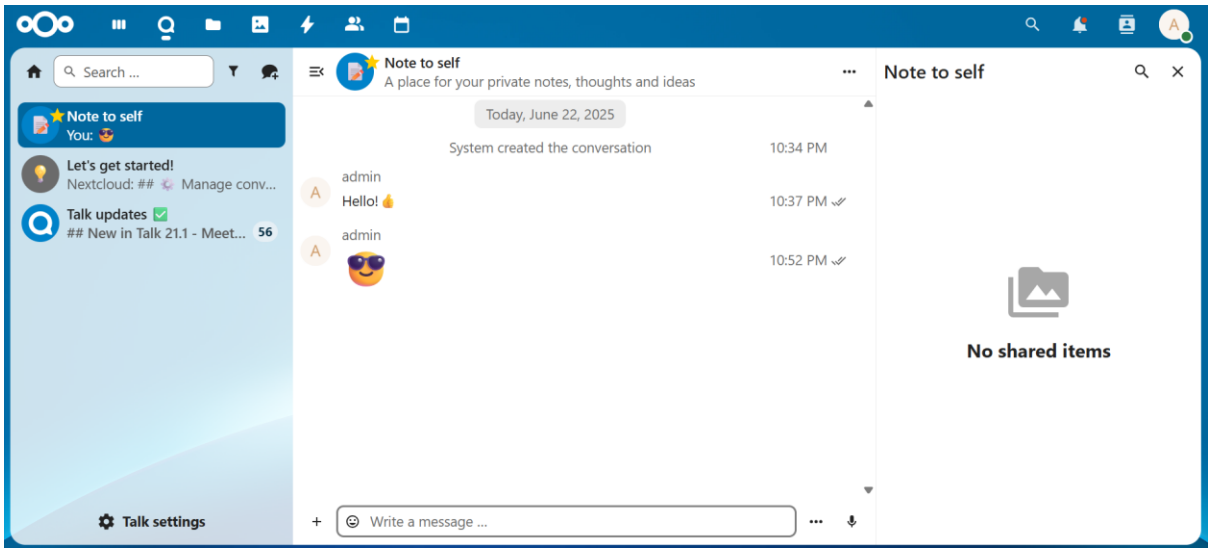
6.3 Install Apps in Nextcloud



For testing purposes on our lightweight 1 GB RAM Azure VM, you can install selected collaboration apps from the Nextcloud Hub bundle without installing the entire suite. After logging into the Nextcloud web interface as an admin, go to **+ Apps** from the user menu. Under the **Hub Bundle** category, locate and install only the essential apps: **Calendar**, **Contacts**, and **Talk**. These applications enable basic scheduling, contact management, and text-based communication. Avoid installing heavier apps like Nextcloud Office or Mail. This keeps the VM stable for lightweight, individual or small-group use.

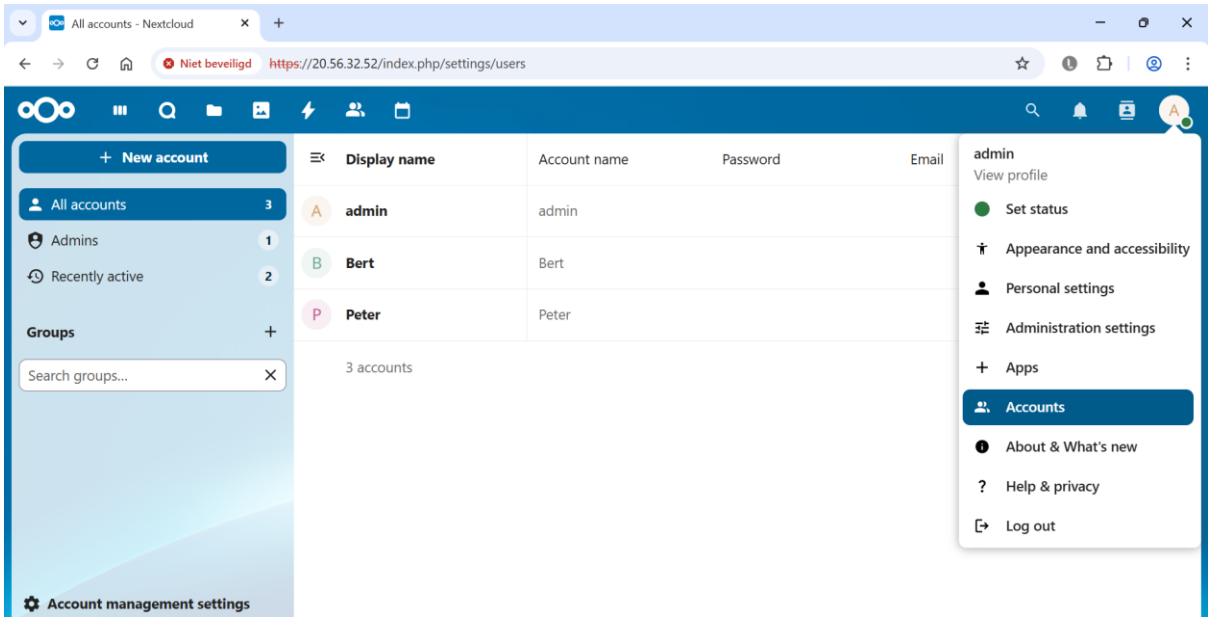


Try if the chat function in the **Talk** application works:



6.4 Add users to Nextcloud

Select accounts in the admin user menu.



Add multiple users(fellow students) to the Nextcloud server. Fill in the following details:

- Display name
- Account name
- Password

!!! Do not make these new users admins !!!

6.5 Nextcloud stress test

Invite at least three other students to your Nextcloud server. Do the stress test together as a group of four. Share the results among the group.

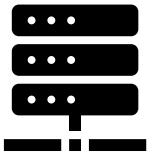
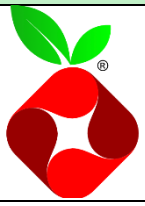
- Test with how many users you can text chat in the Talk application before the Nextcloud server stops working.
- Test with how many users you can video conference in the Talk application before the Nextcloud server stops working.
- Write a recommendation how the municipality of Enschede can improve the usability of the collaboration application Talk.

6.6 Draw the created infrastructure diagram

Draw the infrastructure that you have created during the past six weeks.

- Use lines to connect all components (e.g., routers, switches, servers, clients).
- Label each component clearly with its name and IP address(IPv4).
- Use the drawing tools in Microsoft Word to create your diagram.
- Use the provided icons from the table below.

Your final diagram should be neat, complete, and accurately reflect your implemented setup.

Router/Switch/Firewall	Server	Internet/Cloud	User laptop
			
User desktop	**osTicket**	**Pi-hole**	**Docker**
			

6.7 Azure VM calculator

Use the Azure pricing calculator to estimate how much the Nextcloud VM would cost per month. The Azure Linux VM is of size B1s and it is an Ubuntu Server 24.04 LTS.

Azure pricing calculator: https://azure.microsoft.com/en-us/pricing/calculator/

Bibliography

Canonical Ltd. (2024). *Ubuntu 24.04 LTS "Noble Numbat" release notes*.
Retrieved May 5, 2025, from https://ubuntu.com/download/desktop

Debian Project. (2023). *Debian 12 "Bookworm" release notes*.
Retrieved May 5, 2025, from https://www.debian.org/releases/bookworm/

Docker, Inc. (n.d.). *Docker Compose overview*.
Retrieved May 5, 2025, from https://docs.docker.com/compose

Docker, Inc. (n.d.). *Docker networking overview*.
Retrieved May 5, 2025, from https://docs.docker.com/network

Gordon Lyon. (n.d.). *Nmap: Network Mapper - Free Security Scanner*. Insecure.Org.
Retrieved May 5, 2025, from https://nmap.org

Microsoft. (n.d.). *Microsoft Azure portal*.
Retrieved May 5, 2025, from https://portal.azure.com

Nextcloud GmbH. (n.d.). *Nextcloud – The self-hosted productivity platform*.
Retrieved May 5, 2025, from https://nextcloud.com/

OpenMediaVault. (n.d.). *OpenMediaVault documentation*.
Retrieved May 5, 2025, from https://docs.openmediavault.org

OMV-Extras.org. (n.d.). *OMV-Extras plugin repository*.
Retrieved May 5, 2025, from https://omv-extras.org

osTicket. (n.d.). *osTicket open source support ticket system*.
Retrieved May 5, 2025, from https://osticket.com

osTicket GitHub. (n.d.). *osTicket support ticketing system* [GitHub repository].
Retrieved May 5, 2025, from https://github.com/osTicket/osTicket

Pi-hole Team. (n.d.). *docker-pi-hole* [GitHub repository].
Retrieved May 5, 2025, from https://github.com/pi-hole/docker-pi-hole

Pi-hole Team. (n.d.). *Pi-hole documentation*.
Retrieved May 5, 2025, from https://docs.pi-hole.net

Wikimedia Commons. (2007, October 29). *RAID 1.svg – RAID 1 layout diagram* [SVG image].
Retrieved May 5, 2025, from https://commons.wikimedia.org/wiki/File:RAID_1.svg