

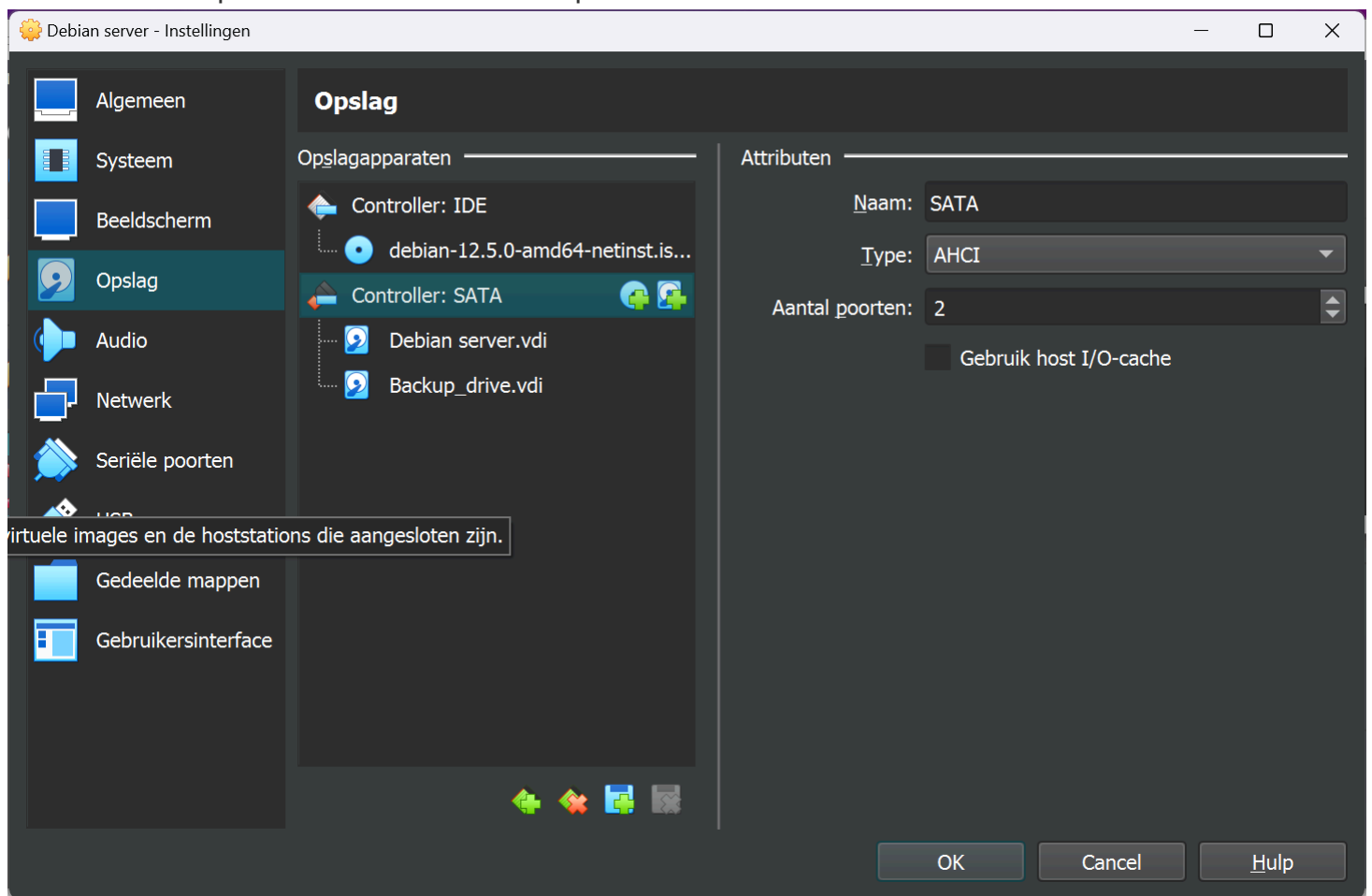
# Linux network services Documentation

## Server

## Virtual Machine Configuration

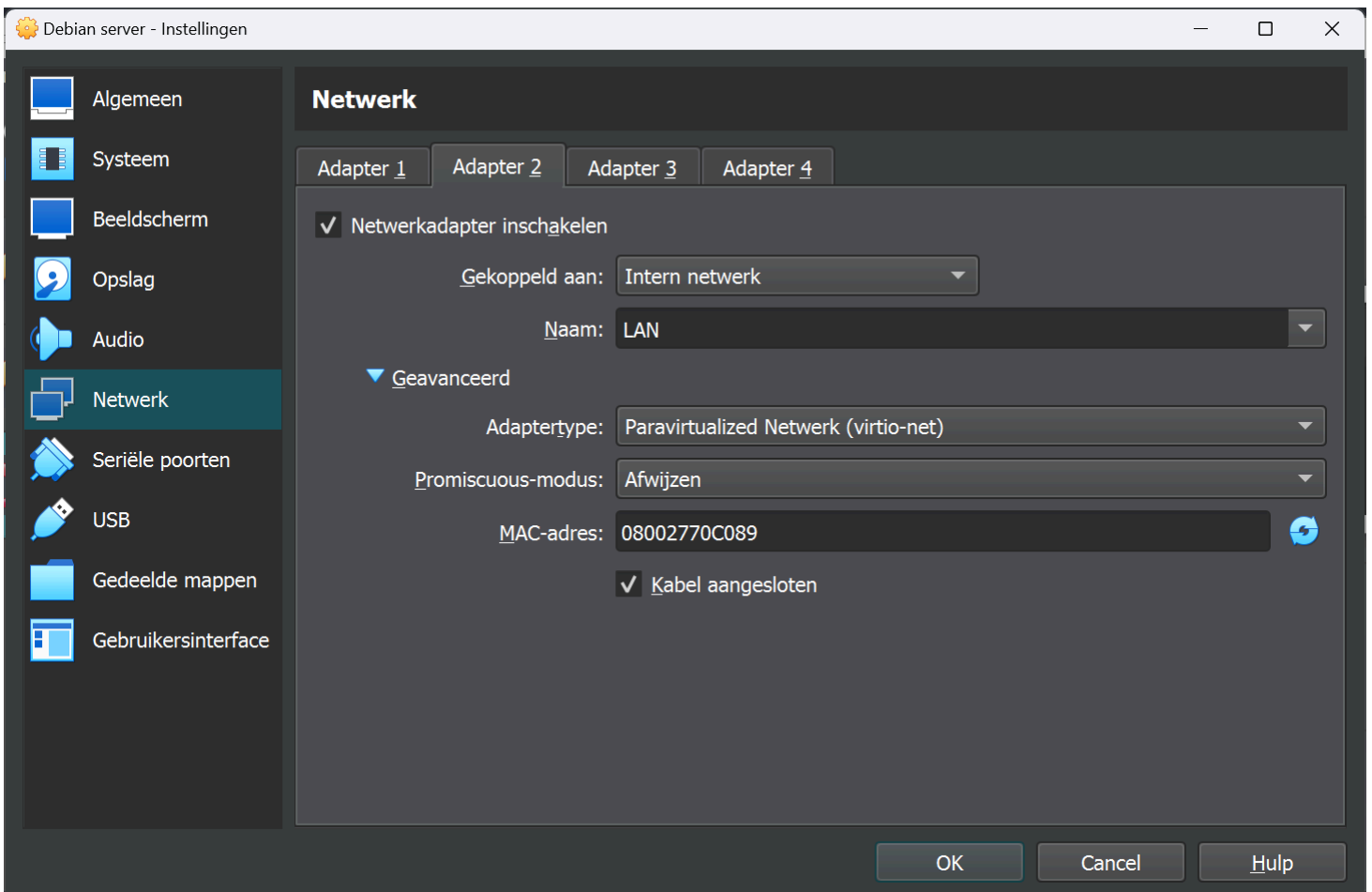
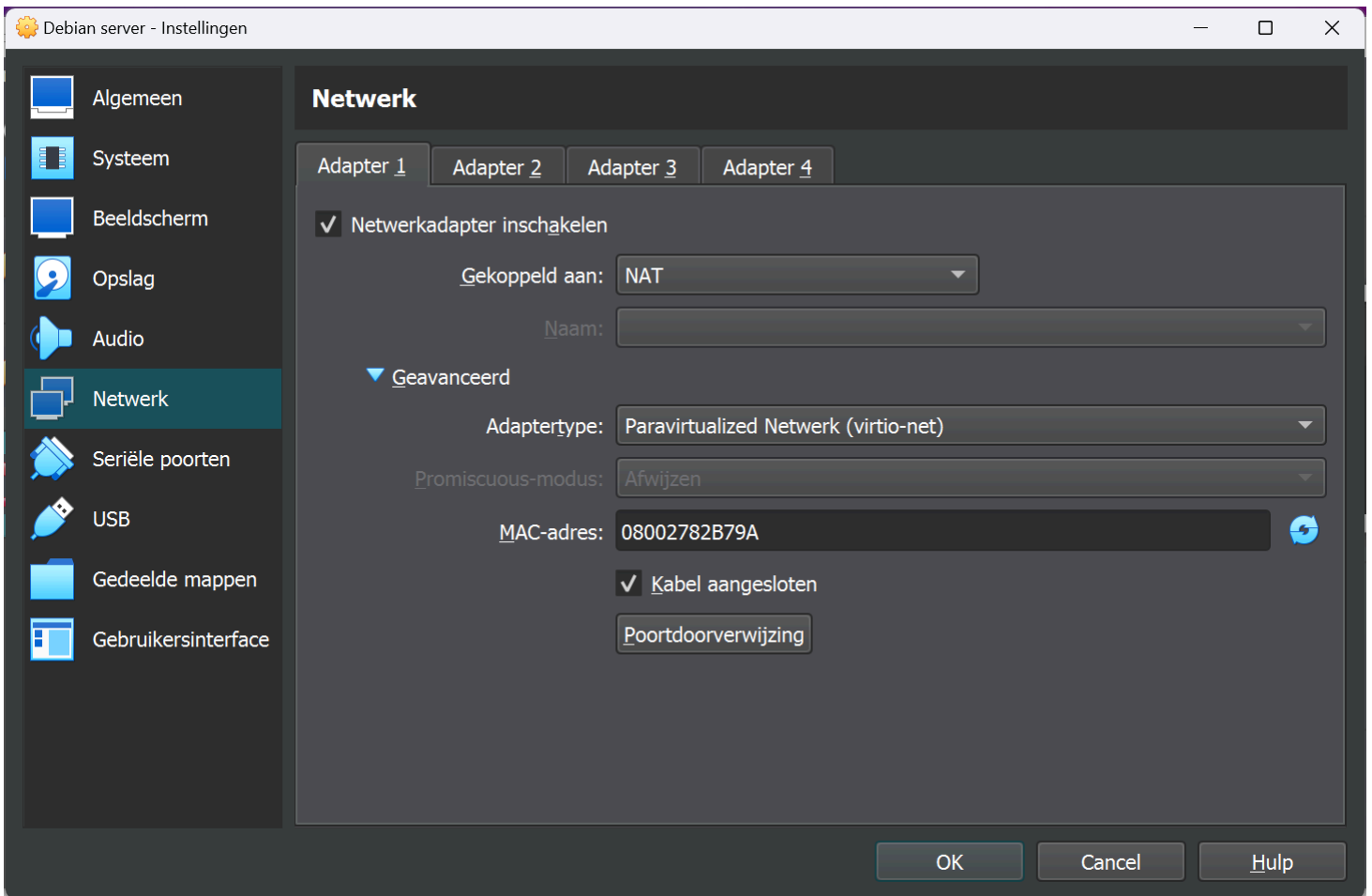
### Hard drives

we will use a separate hard drive for backups



### Network Adapters

we will use 2 network adapters, 1 connected to the internet, one for the internal network



# OS

we will use Debian as the server OS as it's a very reliable, trusted linux distribution with minimal system requirements.

## Installation steps

- choose a non graphical install



- choose your language, country, locale and keyboard map

## [!!] Select a language

Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.

Language:

C	- No localization
Albanian	- Shqip
Arabic	- عربي
Asturian	- Asturianu
Basque	- Euskara
Belarusian	- Беларуская
Bosnian	- Bosanski
Bulgarian	- Български
Catalan	- Català
Chinese (Simplified)	- 中文(简体)
Chinese (Traditional)	- 中文(繁體)
Croatian	- Hrvatski
Czech	- Čeština
Danish	- Dansk
Dutch	- Nederlands
<b>English</b>	<b>- English</b>
Esperanto	- Esperanto
Estonian	- Eesti
Finnish	- Suomi
French	- Français
Galician	- Galego
Georgian	- ქართული
German	- Deutsch

<Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons

- choose the external network adaptor.

### [!!] Configure the network

Your system has multiple network interfaces. Choose the one to use as the primary network interface during the installation. If possible, the first connected network interface found has been selected.

Primary network interface:

enp0s3: Unknown interface  
enp0s8: Unknown interface

<Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons

- Enter a hostname and domain name(Server1 and [library.be](https://library.be) respectively in this case)

### !!! Set up users and passwords

You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.

Note that you will not be able to see the password as you type it.

Root password:

ydQtf@Y5

[\*] Show Password in Clear

<Go Back>

<Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons

- Choose a root password: ydQtf@Y5
- create a new user by following the prompts
- for partitioning choose guided - use entire disk -> all files in one partition

### [[!]] Partition disks

The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.

If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.

Partitioning method:

Guided - use entire disk  
Guided - use entire disk and set up LVM  
Guided - use entire disk and set up encrypted LVM  
Manual

<Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons

- write changes to disk

### [[!]] Partition disks

If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.

The partition tables of the following devices are changed:  
SCSI3 (0,0,0) (sda)

The following partitions are going to be formatted:  
partition #1 of SCSI3 (0,0,0) (sda) as ext4  
partition #5 of SCSI3 (0,0,0) (sda) as swap

Write the changes to disks?

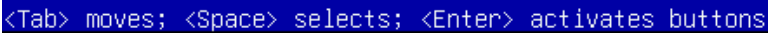
<Yes>

<No>

<Tab> moves; <Space> selects; <Enter> activates buttons

- don't scan extra installation media





- choose a mirror (any belgian one will work fine)
- don't participate in the package survey

### [!] Configuring popularity-contest

The system may anonymously supply the distribution developers with statistics about the most used packages on this system. This information influences decisions such as which packages should go on the first distribution CD.

If you choose to participate, the automatic submission script will run once every week, sending statistics to the distribution developers. The collected statistics can be viewed on <https://popcon.debian.org/>.

This choice can be later modified by running "dpkg-reconfigure popularity-contest".

Participate in the package usage survey?

<Yes>

<No>

<Tab> moves; <Space> selects; <Enter> activates buttons

- uncheck the desktop environment, check the ssh server in software selection

## [!] Software selection

At the moment, only the core of the system is installed. To tune the system to your needs, you can choose to install one or more of the following predefined collections of software.

Choose software to install:

```
[ ] Debian desktop environment
[ ] ... GNOME
[ ] ... Xfce
[ ] ... GNOME Flashback
[ ] ... KDE Plasma
[ ] ... Cinnamon
[ ] ... MATE
[ ] ... LXDE
[ ] ... LXQt
[!] web server
[*] SSH server
[*] standard system utilities
```

<Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons

- install grub on /dev/sda

[!] Configuring grub-pc

It seems that this new installation is the only operating system on this computer. If so, it should be safe to install the GRUB boot loader to your primary drive (UEFI partition/boot record).

Warning: If your computer has another operating system that the installer failed to detect, this will make that operating system temporarily unbootable, though GRUB can be manually configured later to boot it.

Install the GRUB boot loader to your primary drive?

<Go Back>

<Yes>

<No>

<Tab> moves; <Space> selects; <Enter> activates buttons

### [!] Configuring grub-pc

You need to make the newly installed system bootable, by installing the GRUB boot loader on a bootable device. The usual way to do this is to install GRUB to your primary drive (UEFI partition/boot record). You may instead install GRUB to a different drive (or partition), or to removable media.

Device for boot loader installation:

Enter device manually

/dev/sda (ata-VBOX\_HARDDISK\_VBe779364f-7d43100c)

/dev/sdb (ata-VBOX\_HARDDISK\_VBbcf68b33-9fe9935e)

<Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons

- reboot the server

## Post Installation

- we install tailscale to facilitate working on the vm together

login as root and then:

```
apt install curl
```

```
curl -fsSL https://tailscale.com/install.sh | sh
```

```
tailscale up
```

- add subnet routing to tailscale

```
echo 'net.ipv4.ip_forward = 1' | sudo tee -a /etc/sysctl.d/99-tailscale.conf
```

```
echo 'net.ipv6.conf.all.forwarding = 1' | sudo tee -a /etc/sysctl.d/99-tailscale.conf
```

```
sudo sysctl -p /etc/sysctl.d/99-tailscale.conf
```

```
sudo tailscale up --advertise-routes=10.0.10.0/24
```

- add sudo

```
apt install sudo
```

```
usermod -a -G sudo <username>
```

- partition second hard drive

- install parted

```
apt install parted
```

- partition the disk

```
sudo parted /dev/sdb
```

```
mklabel gpt
```

```
mkpart primary ext4 1MB
```

```
quit
```

- add a filesystem to /dev/sdb1

```
mkfs.ext4 /dev/sdb1
```

# Configure the internal network adaptor

- find your network interface names

ip a

```
gregory@Server1: ~  
valid_lft forever preferred_lft forever  
gregory@Server1:~$ sudo  
-bash: sudo: command not found  
gregory@Server1:~$ su -  
Password:  
root@Server1:~# ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:82:b7:9a brd ff:ff:ff:ff:ff:ff  
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3  
        valid_lft 85189sec preferred_lft 85189sec  
    inet6 fe80::a00:27ff:fe82:b79a/64 scope link  
        valid_lft forever preferred_lft forever  
3: enp0s8: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000  
    link/ether 08:00:27:70:c0:89 brd ff:ff:ff:ff:ff:ff  
4: tailscale0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1280 qdisc fq_codel state UNKNOWN group default qlen 1000  
    link/none  
    inet 100.94.244.53/32 scope global tailscale0  
        valid_lft forever preferred_lft forever  
    inet6 fd7a:115c:a0e::4301:f435/128 scope global  
        valid_lft forever preferred_lft forever  
    inet6 fe80::2a0e:e91a:8109:39b7/64 scope link stable-privacy  
        valid_lft forever preferred_lft forever  
root@Server1:~# ~
```

- open /etc/network/interfaces and add the following changing enp0s8 with the internal network card interface

```
auto enp0s8  
iface enp0s8 inet static  
    address 10.0.10.100  
    netmask 255.255.255.0  
    network 10.0.10.0  
    broadcast 10.0.10.255
```

```
gregory@Server1: ~  
GNU nano 7.2 /etc/network/interfaces *  
# This file describes the network interfaces available on your system  
# and how to activate them. For more information, see interfaces(5).  
  
source /etc/network/interfaces.d/*  
  
# The loopback network interface  
auto lo  
iface lo inet loopback  
  
# The primary network interface  
auto enp0s3  
iface enp0s3 inet dhcp  
  
# Secondary network interface  
auto enp0s8  
iface enp0s8 inet static  
    address 10.0.10.100  
    netmask 255.255.255.0  
    network 10.0.10.0  
    broadcast 10.0.10.255  
    gateway 10.0.10.1  
  
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo  
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/_ Go To Line  M-E Redo
```

- restart networking

```
systemctl restart networking
```

## DHCP

### installation

```
apt install isc-dhcp-server
```

### configure

- change /etc/dhcp/dhcpd.conf to:



```
default-lease-time 600;
max-lease-time 7200;

subnet 10.0.10.0 netmask 255.255.255.0 {
    range 10.0.10.2 10.0.10.99;
    option routers 10.0.10.254;
    option domain-name-servers 10.0.10.100;
    option domain-name "library.be";
}
```

- in /etc/default/isc-dhcp-server make the following change

```
INTERFACESv4="enp0s8"
```

- restart dhcp with `sudo systemctl restart isc-dhcp-server.service`

# GLPI

## Installation

- install a web server

```
apt install nginx
```

create /etc/nginx/sites-enabled/glpi and add the following

```

server {
    listen 80;
    listen [::]:80;

    server_name gpli.library.be;

    root /var/www/glpi/public;

    location / {
        try_files $uri /index.php$is_args$args;
    }

    location ~ ^/index\.php$ {
        # the following line needs to be adapted, as it changes depending on OS distributions ar
        fastcgi_pass unix:/run/php/php-fpm.sock;

        fastcgi_split_path_info ^(.+\.php)(/.*)$;
        include fastcgi_params;

        fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
    }
}

```

- install mariadb

```

apt install mariadb-server
mysql_secure_installation

```

- configure root user
  - set root password for mariadb to b4#9etCY

```
gregory@Server1: /var/www/ | X + -
gregory@Server1:/var/www/glpi$ sudo mysql_secure_installation

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
haven't set the root password yet, you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password or using the unix_socket ensures that nobody
can log into the MariaDB root user without the proper authorisation.

You already have your root account protected, so you can safely answer 'n'.

Switch to unix_socket authentication [Y/n]
Enabled successfully!
Reloading privilege tables..
... Success!

You already have your root account protected, so you can safely answer 'n'.

Change the root password? [Y/n] |
```

- o disallow anonymous users

```
gregory@Server1: /var/www/ | X + -
Enabled successfully!
Reloading privilege tables..
... Success!

You already have your root account protected, so you can safely answer 'n'.

Change the root password? [Y/n]
New password:
Re-enter new password:
Sorry, passwords do not match.

New password:
Re-enter new password:
Sorry, passwords do not match.

New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
... Success!

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] n
```

- o disallow root remote login

```
gregory@Server1: /var/www/ x + ~
Change the root password? [Y/n]
New password:
Re-enter new password:
Sorry, passwords do not match.

New password:
Re-enter new password:
Sorry, passwords do not match.

New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
... Success!

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] n
... skipping.

Normally, root should only be allowed to connect from 'localhost'. This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y/
```

- add user and database for glpi

```
sudo mysql -u root -p
```

```
CREATE DATABASE glpi;
CREATE USER 'glpi'@localhost IDENTIFIED BY '!HD9M&s#';
GRANT ALL PRIVILEGES ON glpi.* TO 'glpi'@localhost;
FLUSH PRIVILEGES;
```

- install php for nginx

```
apt install php-fpm
apt install php-xml
apt install php-mysql
apt install php-gd
apt install php-curl
apt install php-intl
```

- enable php extensions

in /etc/php/8.2/fpm/php.ini uncomment add the following lines:

```
extension=mysqli
extension=fileinfo
extension=dom
extension=simplexml
extension=xmlreader
extension=xmlwriter
```

extension=curl

extension=gd

extension=intl

also set session.cookie\_httponly=1

- restart php-fpm

```
systemctl restart php8.2-fpm.service
```
- install glpi

```
wget https://github.com/glpi-project/glpi/releases/download/10.0.14/glpi-10.0.14.tgz
```

```
tar -xf glpi-10.0.14.tgz --directory=/var/www/
```

```
rm glpi-10.0.14.tgz
```

```
cd /var/www/glpi
```

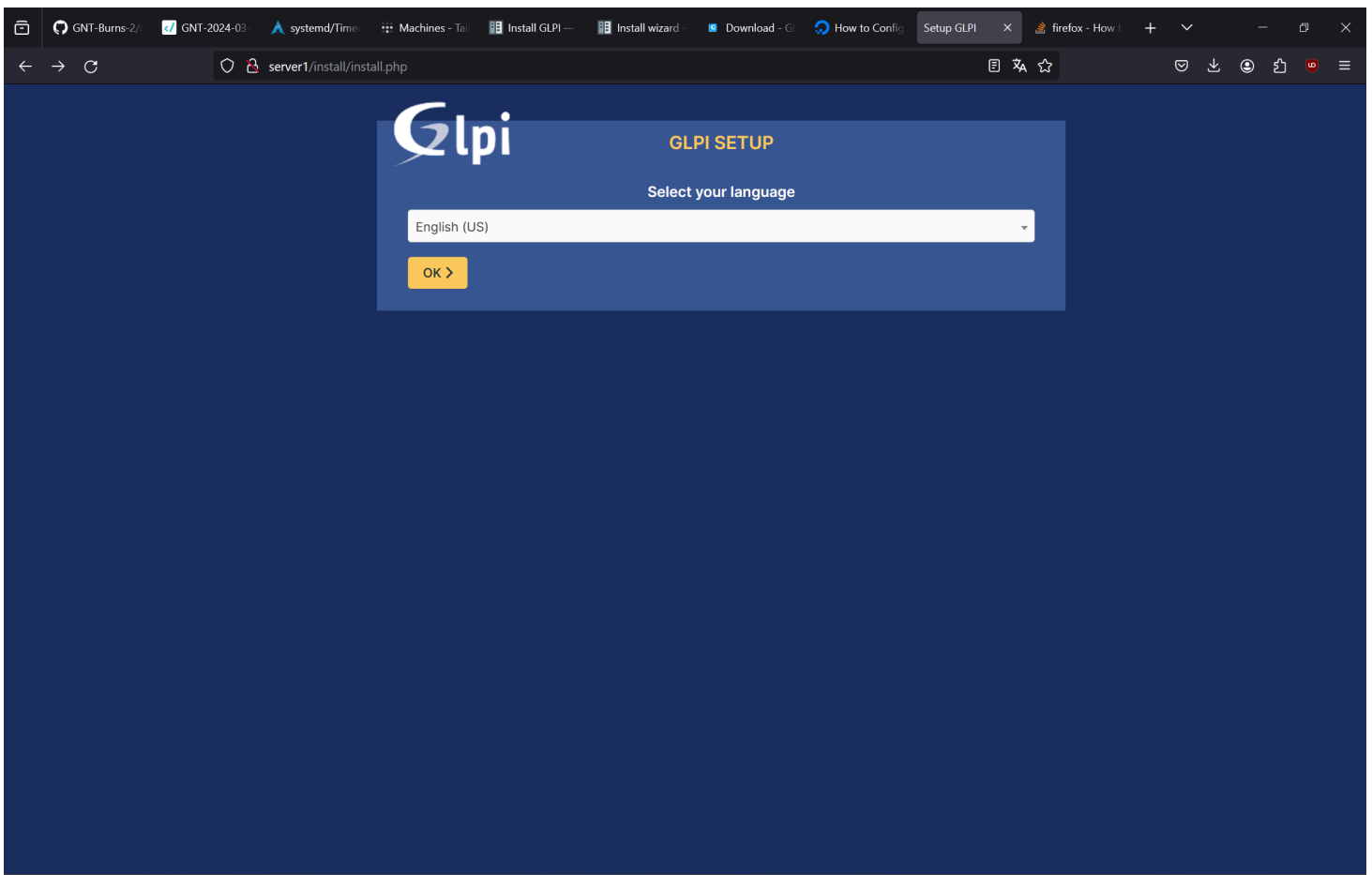
```
chgrp -R www-data config/
```

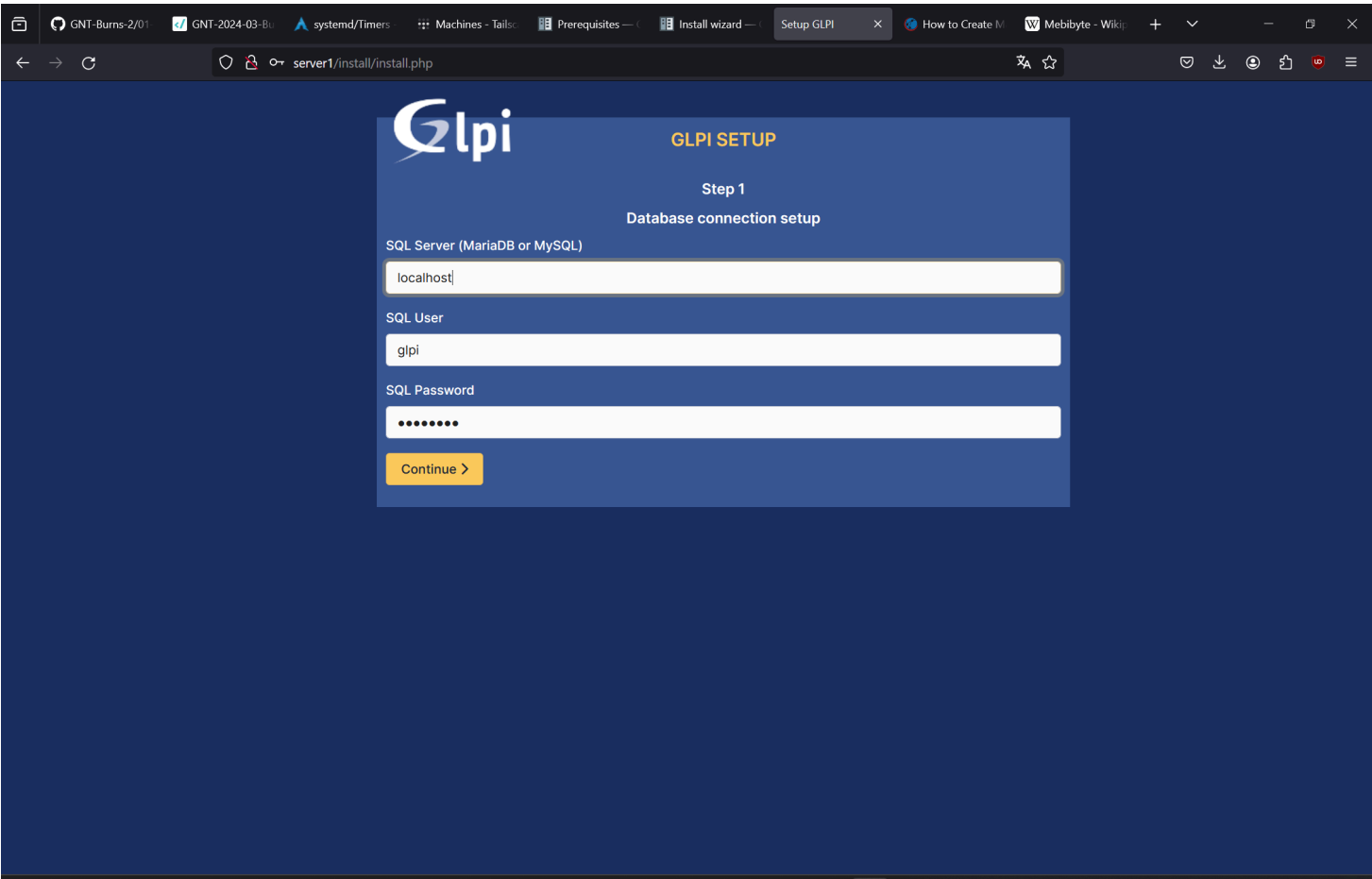
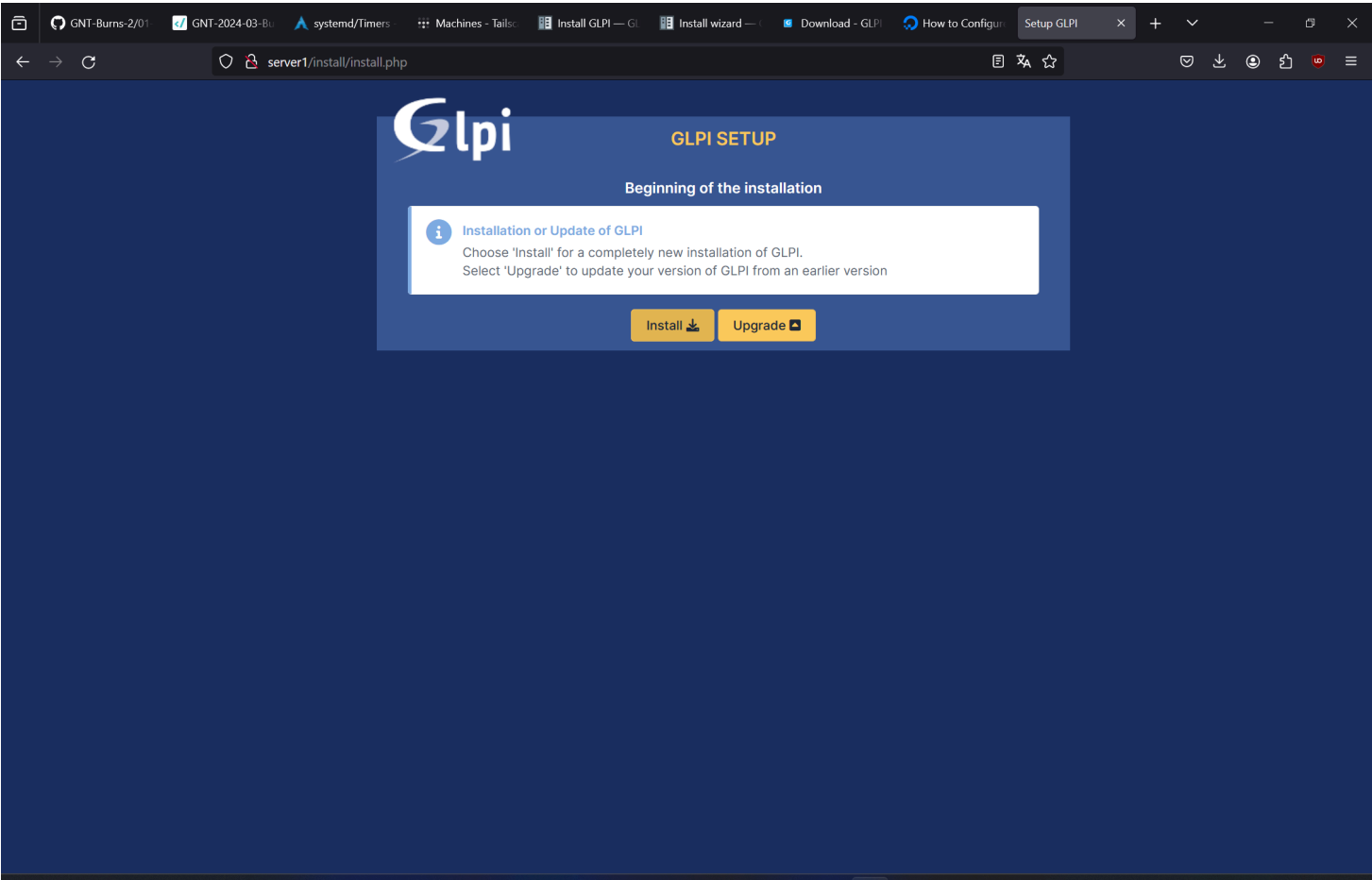
```
chgrp -R www-data files/
```

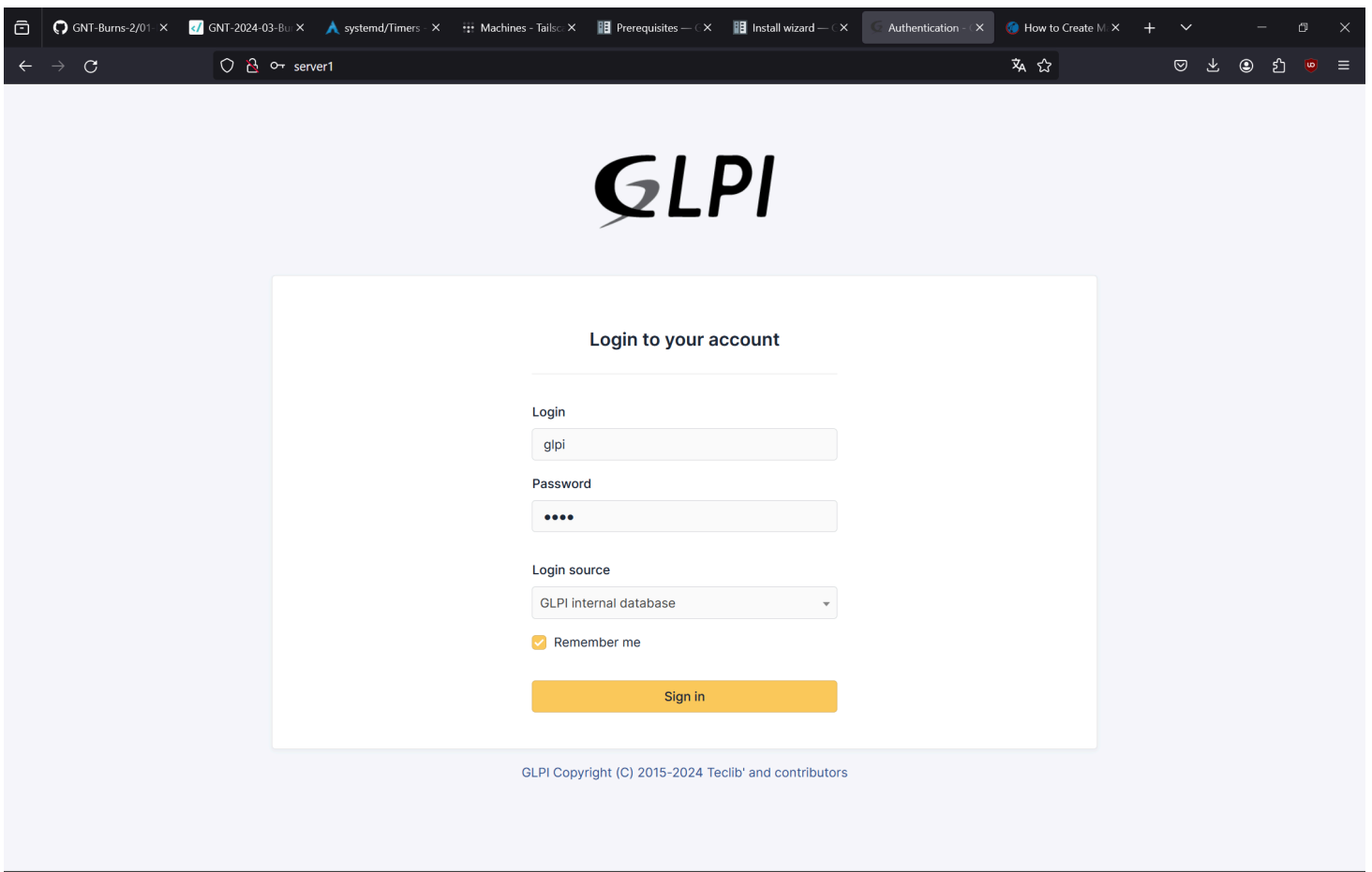
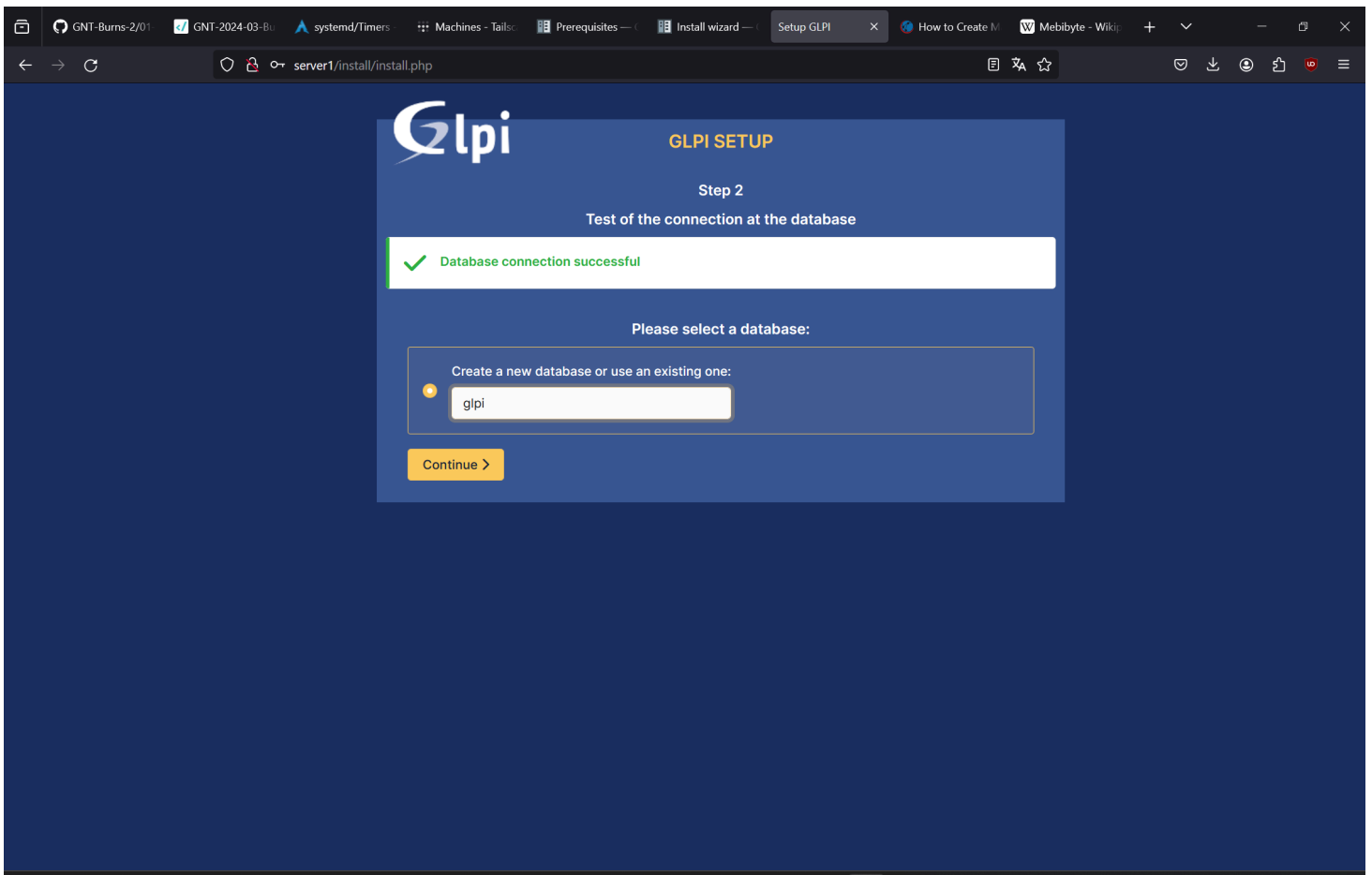
```
chmod -R 770 config/
```

```
chmod -R 770 files/
```

go to <http://10.0.10.100> in a browser







default username: glpi

default password: glpi

# DNS

## Installation

```
apt install bind9
```

## Configuration

- add the following to the file `/etc/bind/named.conf.local`

```
zone "library.be" {  
    type master;  
    file "/etc/bind/db.library.be";  
};
```

- create a file `/etc/bind/db.library.be` and add the following

```
;  
; BIND data file for local loopback interface  
;  
$TTL      604800  
@         IN      SOA      ns1.library.be.  admin.library.be. (  
                                8              ; Serial  
                                604800         ; Refresh  
                                86400          ; Retry  
                                2419200        ; Expire  
                                604800 )       ; Negative Cache  
  
; name servers - NS records  
            IN      NS      ns1.library.be.  
  
; name servers - A records  
ns1.library.be.      IN      A      10.0.10.100  
  
; 10.0.10.0/24 A records  
gpli.library.be.     IN      A      10.0.10.100
```

- restart bind9



```
systemctl restart bind9
```

## Backups

- make the following script in /sbin/settings\_backup and make it executable afterwards

```
#!/bin/bash
mkdir /backups
mount /dev/sdb1 /backups
tar -czPpf /backups/backup-$(date +%F_%H-%M-%S).tar.gz /etc/dhcp/ /etc/bind /etc/nginx /etc/mysql
umount /backups
rmdir /backups
```

- make a systemd service in /etc/systemd/system/backup-settings.service

```
[Unit]
Description=Backup settings for used services

[Service]
Type=oneshot
ExecStart=/bin/bash /sbin/settings_backup.sh
```

- make a systemd timer in /etc/systemd/system/backup-settings.timer

```
[Unit]
Description=Run settings backup weekly

[Timer]
OnCalendar=weekly
Persistent=true

[Install]
WantedBy=timers.target
```

- reload systemd and enable the timer

```
systemctl daemon-reload
systemctl start backup-settings.timer
```

## self signed certificate for nginx

- ```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/nginx-selfsign
```

- create a diffie-helman group

```
sudo openssl dhparam -out /etc/nginx/dhparam.pem 4096
```

- Create a snippet to load the certificate in nginx

```
sudo nano /etc/nginx/snippets/self-signed.conf
```

```
ssl_certificate /etc/ssl/certs/nginx-selfsigned.crt;
ssl_certificate_key /etc/ssl/private/nginx-selfsigned.key;
```

- create a snippet with encryption settings

```
sudo nano /etc/nginx/snippets/ssl-params.conf
```

```
ssl_protocols TLSv1.3;
ssl_prefer_server_ciphers on;
ssl_dhparam /etc/nginx/dhparam.pem;
ssl_ciphers EECDH+AESGCM:EDH+AESGCM;
ssl_ecdh_curve secp384r1;
ssl_session_timeout 10m;
ssl_session_cache shared:SSL:10m;
ssl_session_tickets off;
ssl_stapling on;
ssl_stapling_verify on;
add_header X-Frame-Options DENY;
add_header X-Content-Type-Options nosniff;
add_header X-XSS-Protection "1; mode=block";
```

- change /etc/nginx/sites-enabled/gipi to

```

server {
    listen 443 ssl;
    listen [::]:443 ssl;
    include snippets/self-signed.conf;
    include snippets/ssl-params.conf;

    server_name gp.li.library.be;

    root /var/www/gp.li/public;

    location / {
        try_files $uri /index.php$is_args$args;
    }

    location ~ ^/index\.php$ {
        # the following line needs to be adapted, as it changes depending on OS distributions and
        fastcgi_pass unix:/run/php/php-fpm.sock;

        fastcgi_split_path_info ^(.+\.php)(/.*)$;
        include fastcgi_params;

        fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
    }
}

```

```

server {
    listen 80;
    listen [::]:80;

    server_name gp.li.library.be;

    return 302 https://$server_name$request_uri;
}

```

- restart nginx

```
sudo systemctl restart nginx
```

# Workstation

## Virtual Machine Configuration

### Network Adapters

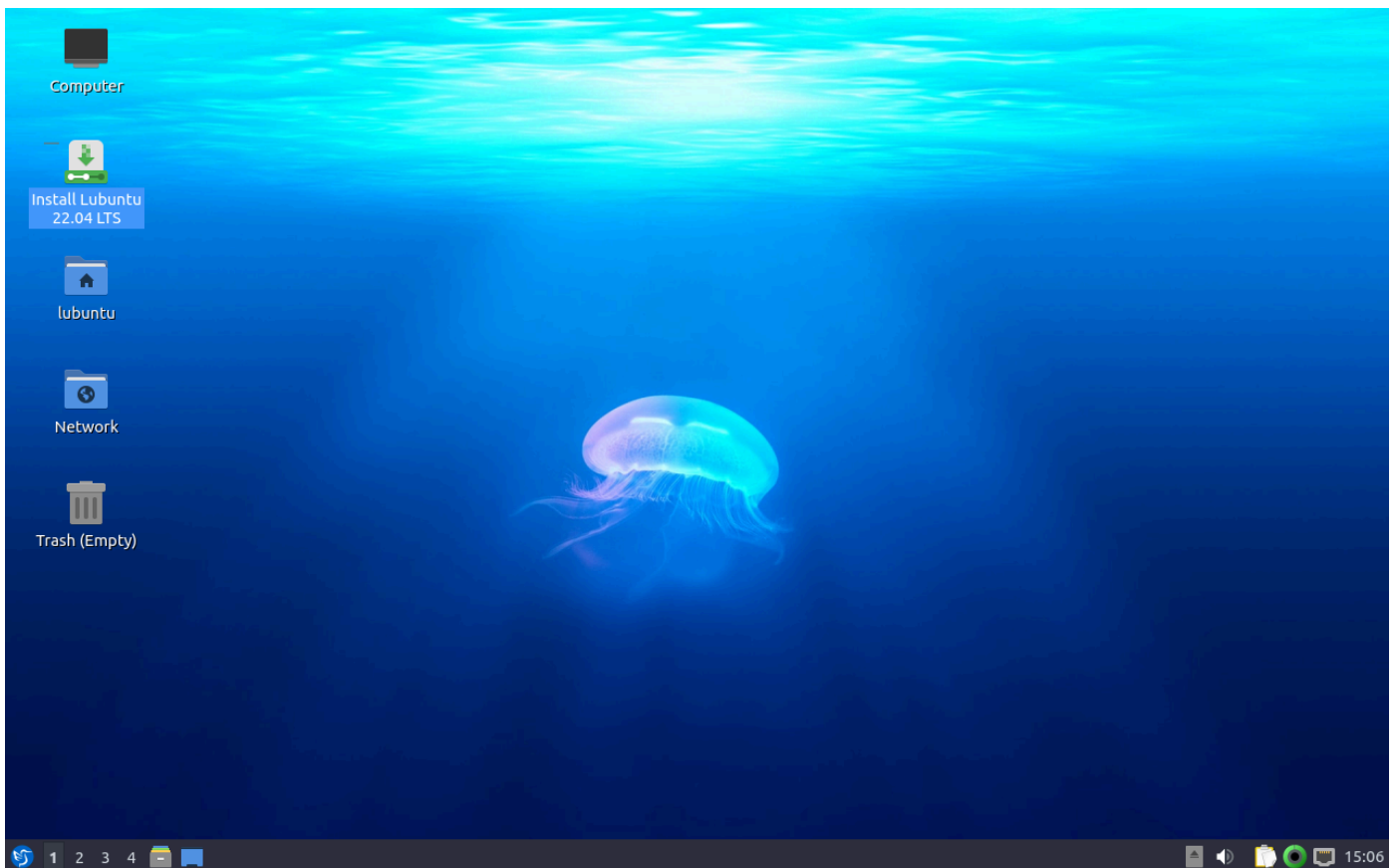
we use one internal network adapter and one NAT network adapter

## OS

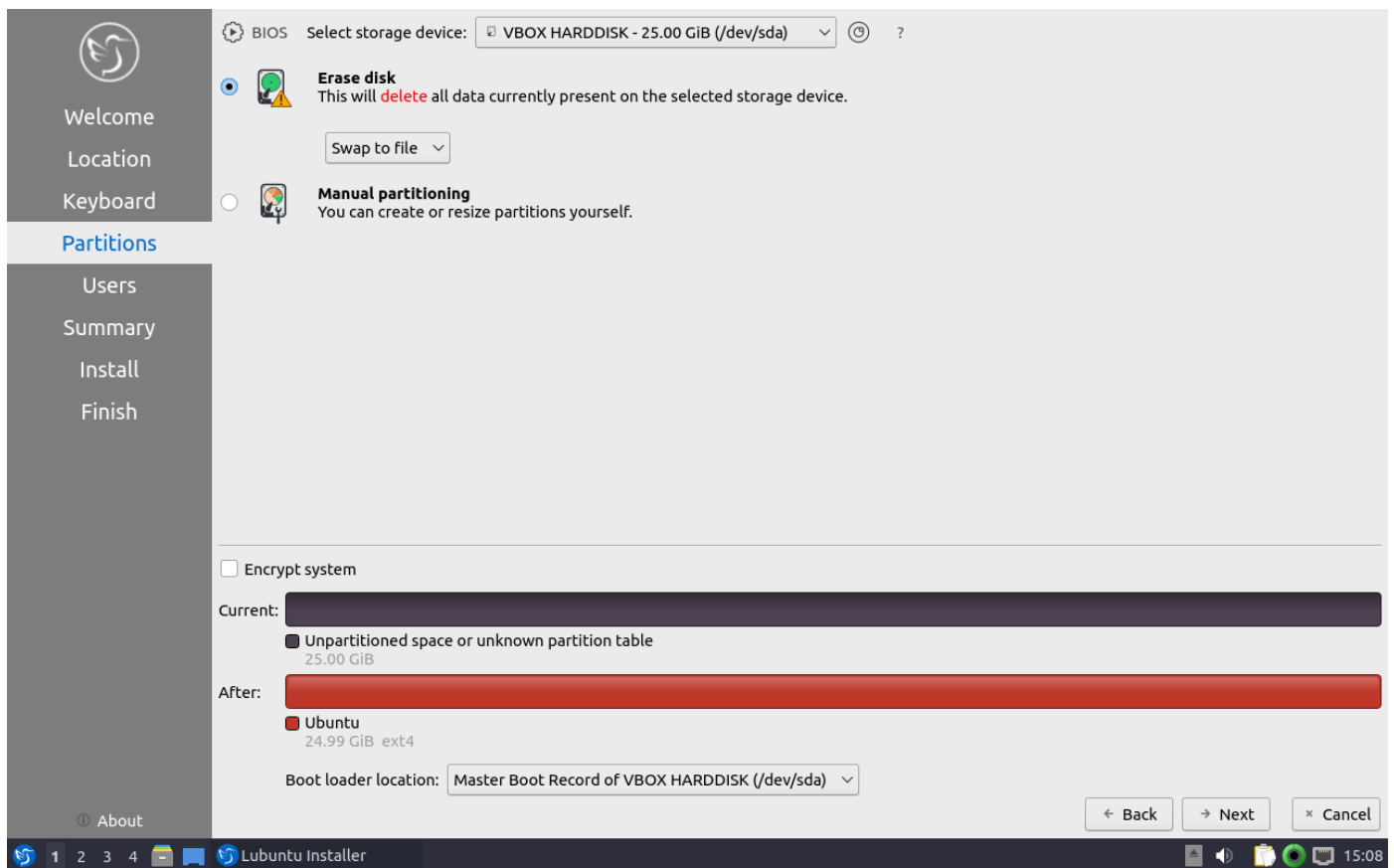
We will use Lubuntu as the workstation os as it offers a solid ubuntu base and a lightweight desktop environment. It will run well on less powerfull hardware

### Installation steps

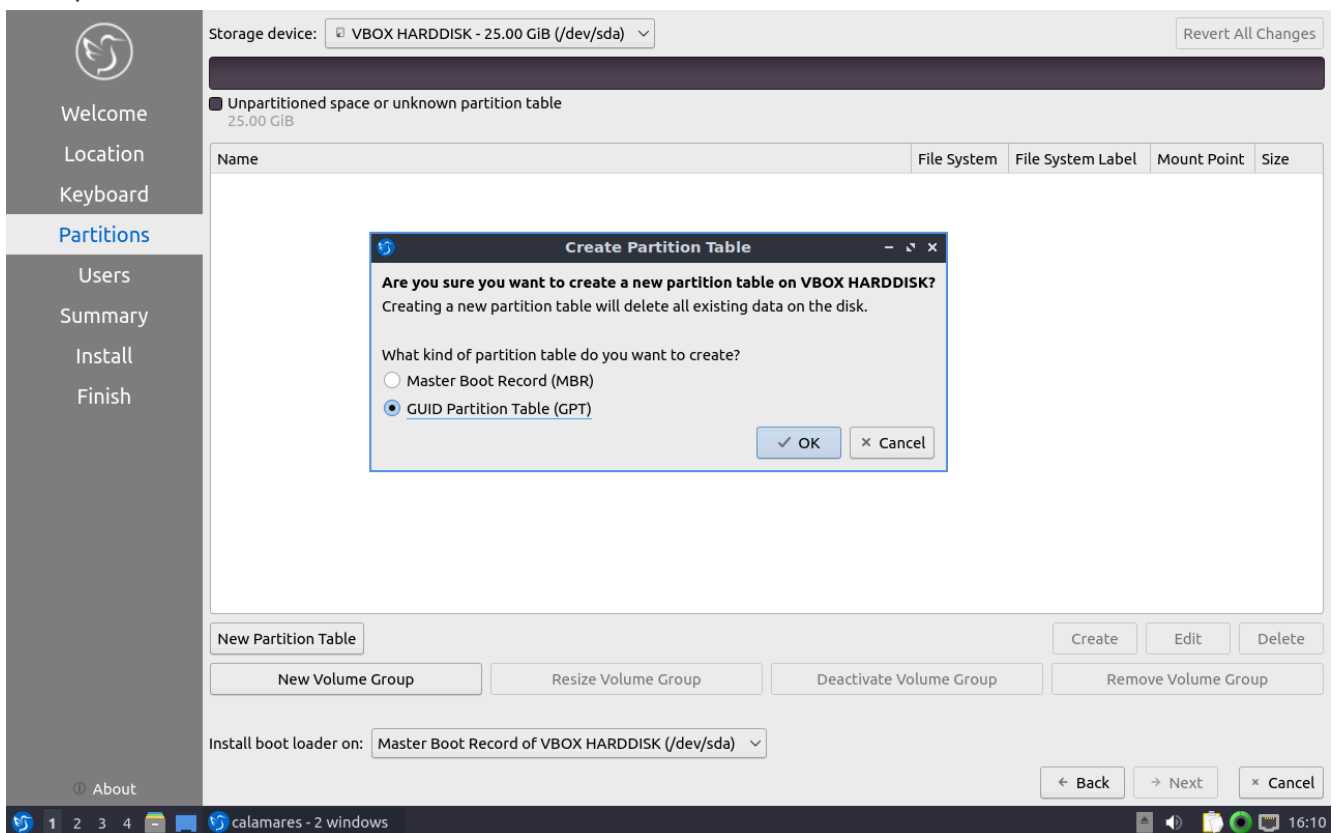
- Download the lubuntu iso from the [lubuntu website](#)
- Start machine with Lubuntu iso inserted.
- click install



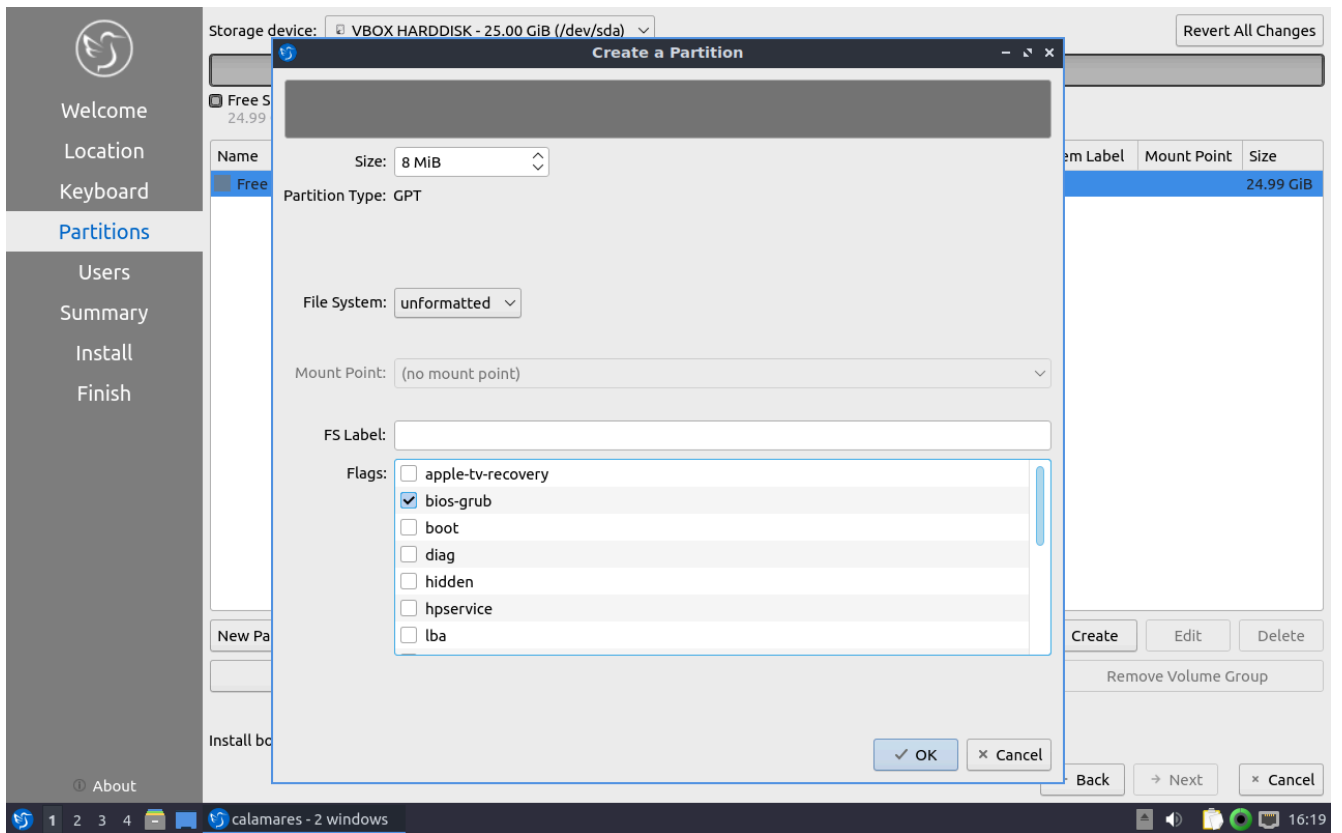
- continue untill partitioning



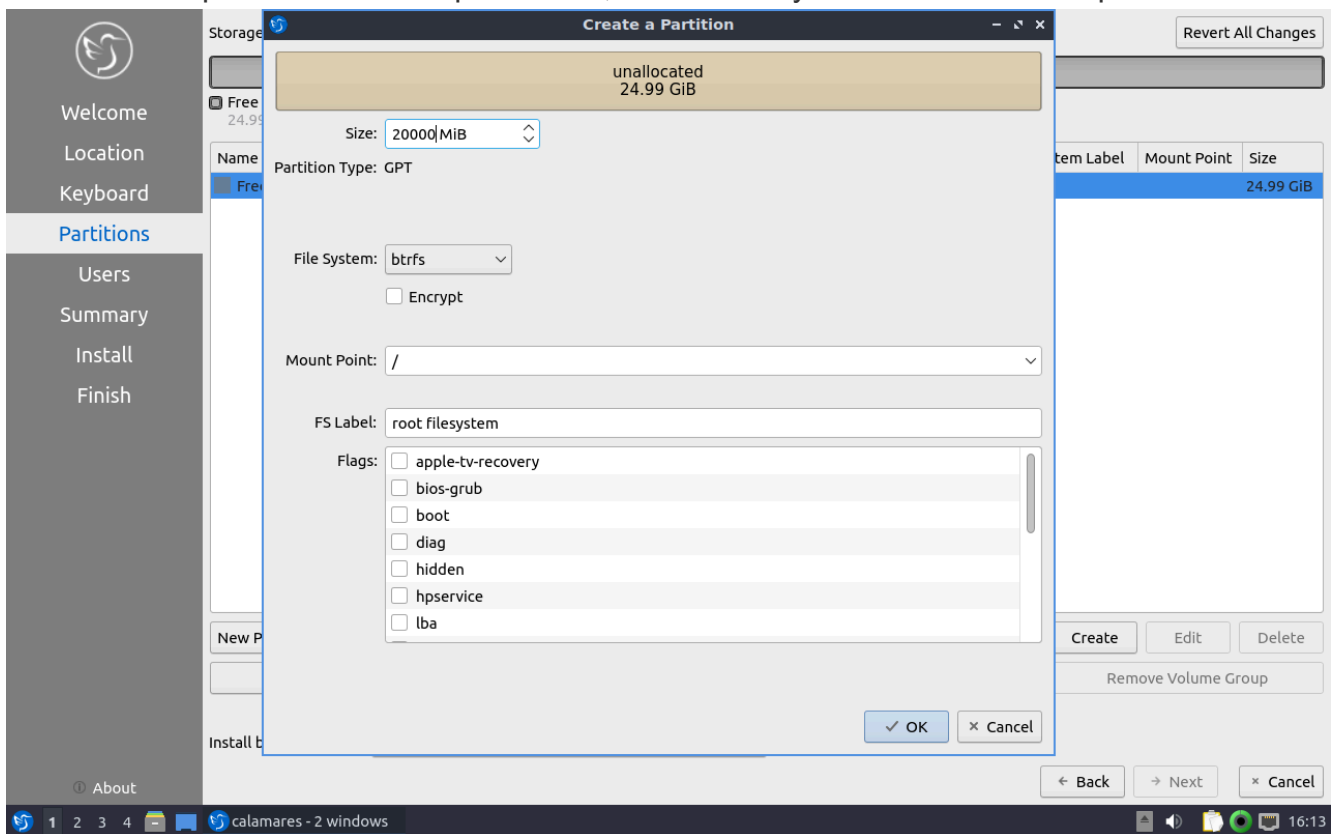
- choose manual partitioning and assign both a / and /home partition
  - new partition table -> GPT



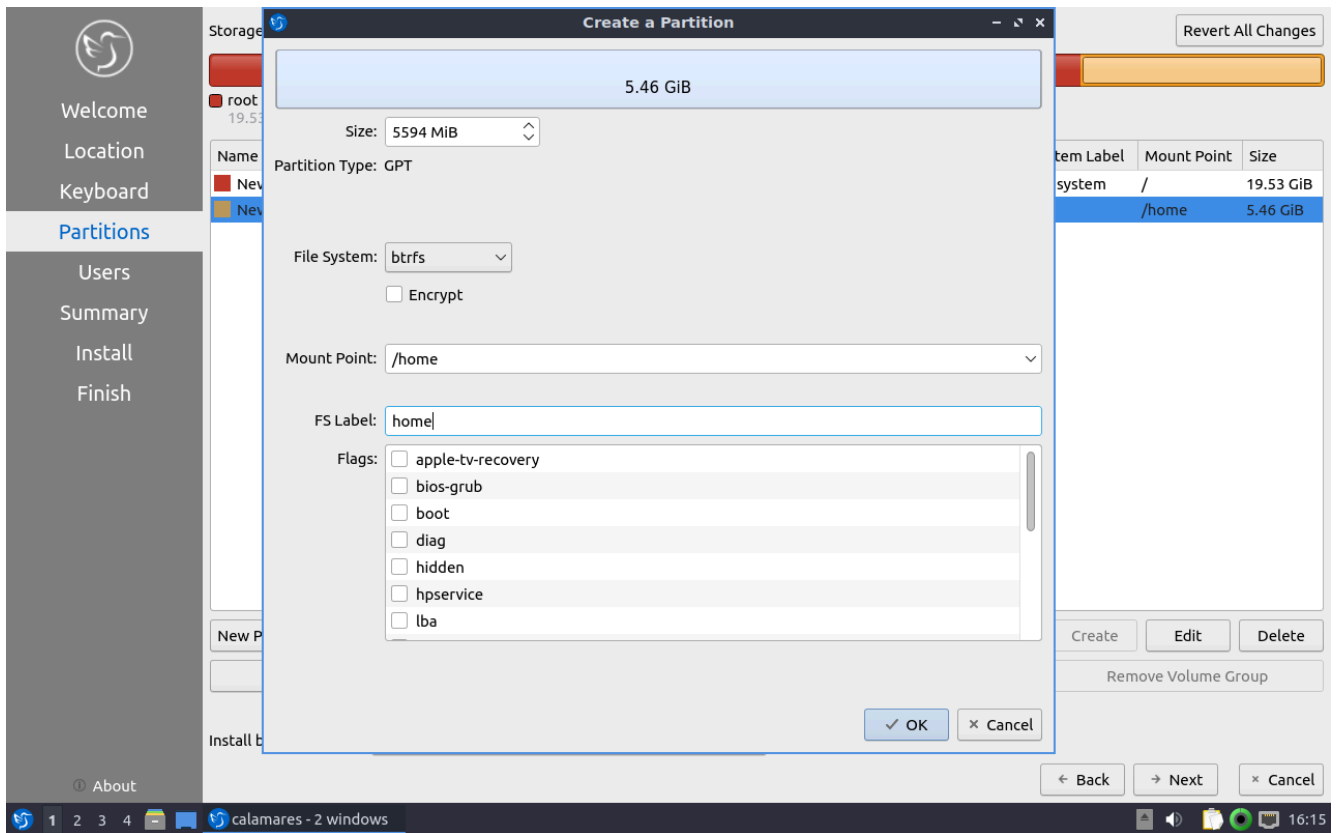
- create a new 8MB unformatted partition and add the bios-grub flag



- click on free space -> create -> pick a size, btrfs as filesystem and / as mountpoint

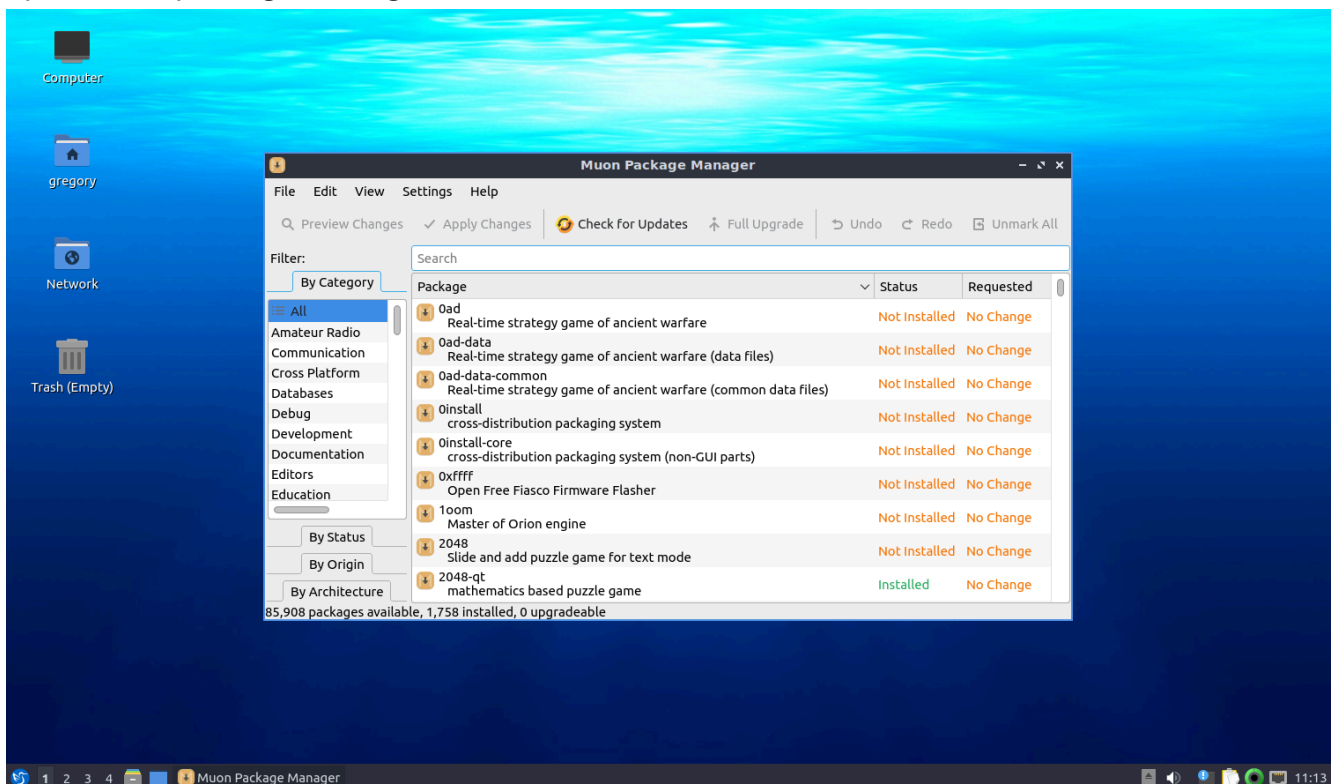


- click on free space -> create -> pick a size, btrfs as filesystem and /home as mountpoint



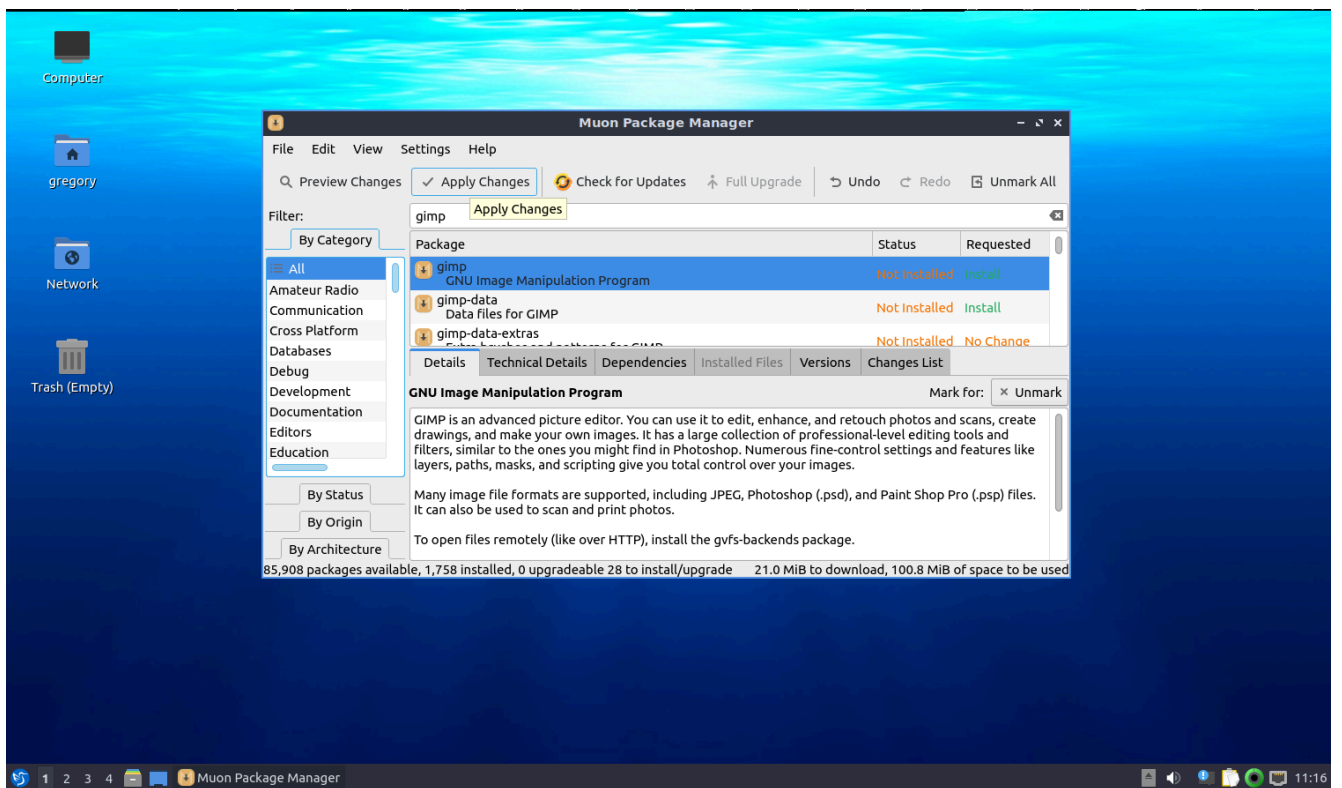
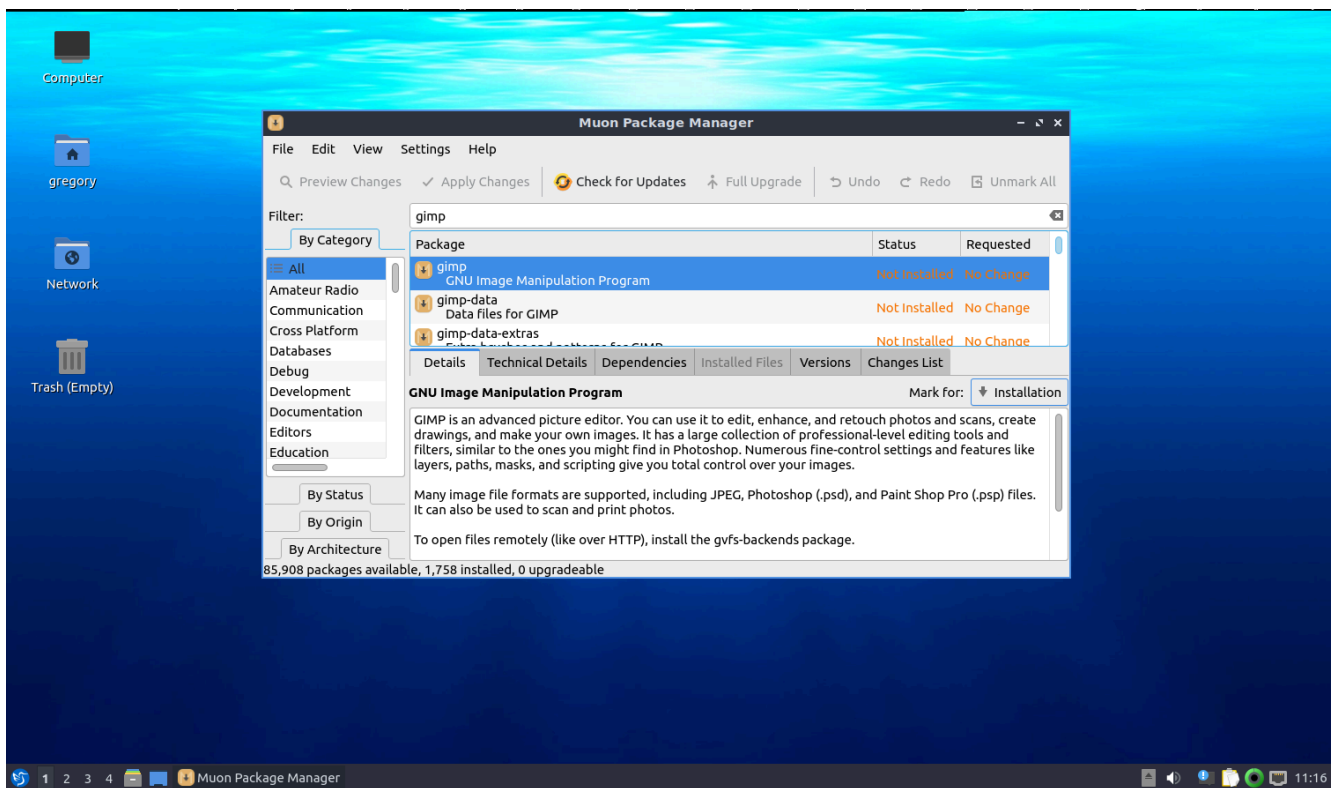
## post installation

- install extra software
  - open muon package manager from start menu



- select gimp and click mark for installation, then apply changes





libreoffice and firefox are already preinstalled

- remote help
  - on workstation install the tigervnc server
  - set password to %\*H7ex&f

```
sudo apt install tigervnc-scraping-server
vncpasswd
sudo ufw allow 5900/tcp
touch ~/.vnc/tigervnc.conf
echo "$localhost=\"no\" " > ~/.vnc/tigervnc.conf
```

- make the vnc server run on login  
make .config/autostart/x0vncserver.desktop and add the following

```
[Desktop Entry]
Exec=x0vncserver -passwordfile ~/.vnc/passwd -display :0
Name=x0vncserver
Type=Application
Version=1.0
```