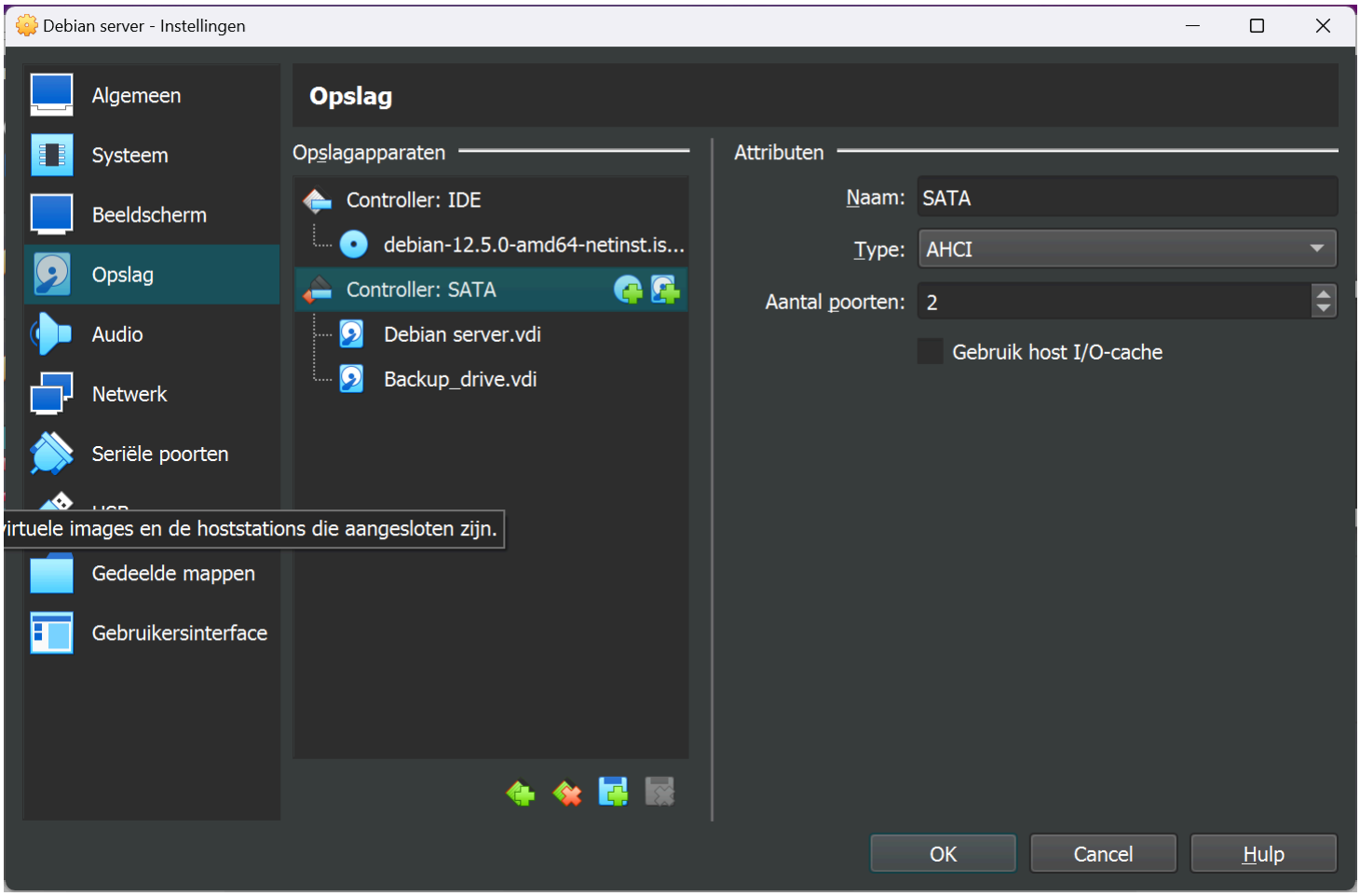
Linux network services Documentation

Server

Virtual Machine Configuration

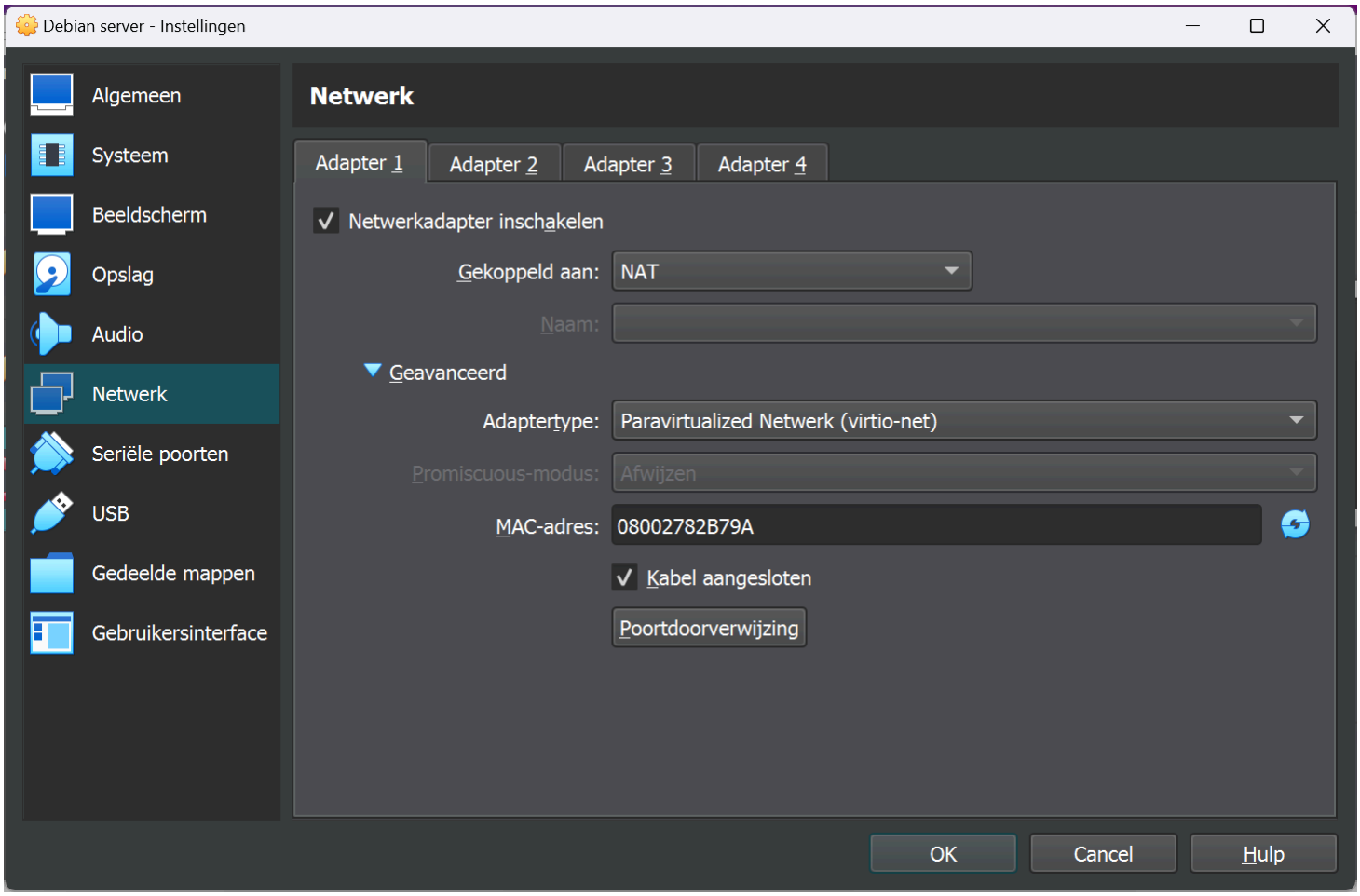
Hard drives

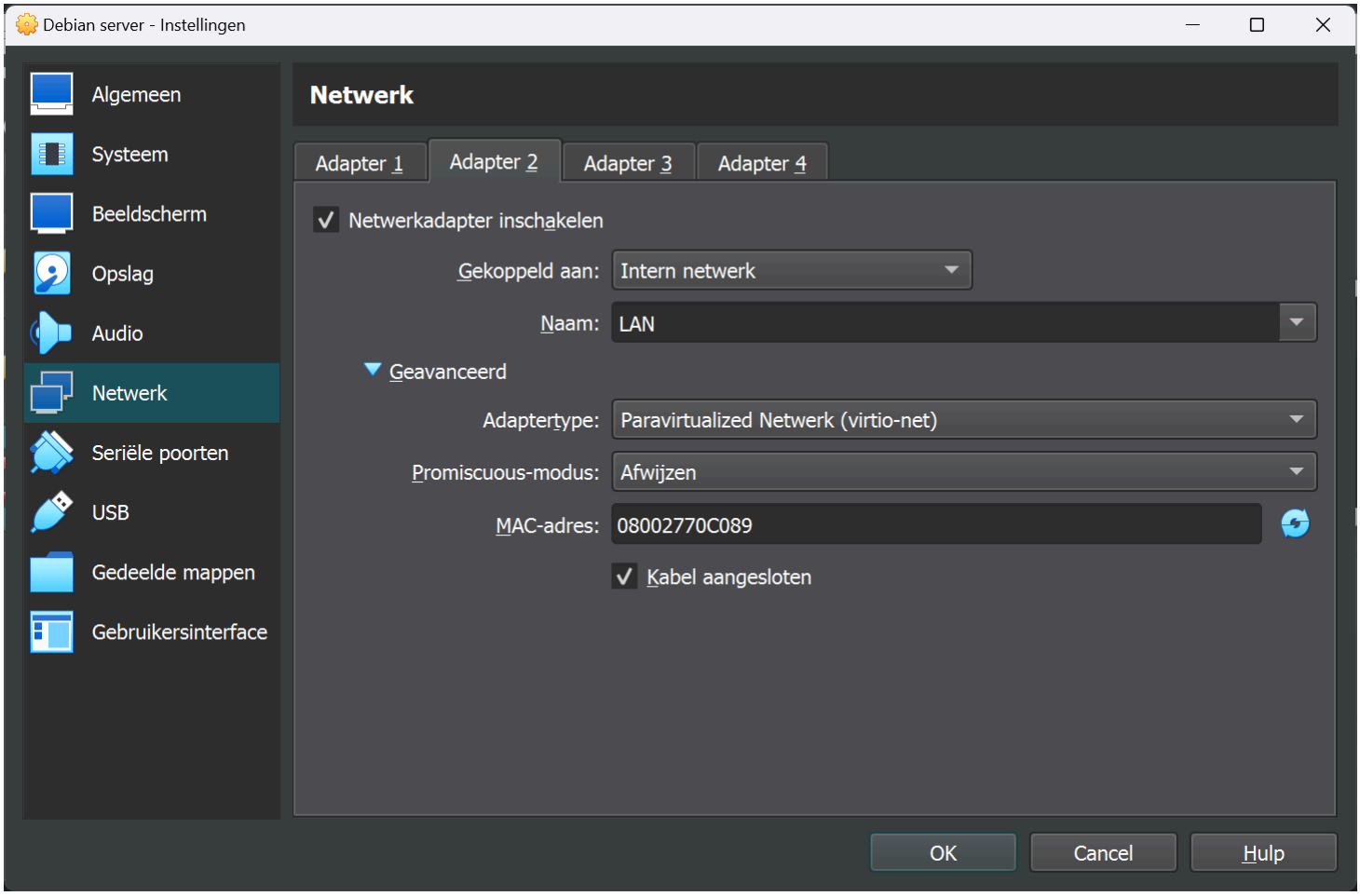
we will use a seperate hard drive for backups



Network Adapters

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


Debian server - Instellingen
Algemeen
Systeem
Beeldscherm
Opslag
Audio
Netwerk
Seriële poorten
USB
Gedeelde mappen
Gebruikersinterface
Netwerk
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Netwerkadapter inschakelen
Gekoppeld aan:
NAT
Naam:
Geavanceerd
Adaptertype:
Paravirtualized Netwerk (virtio-net)
Promiscuous-modus:
Afwijzen
MAC-adres:
08002782B79A
Kabel aangesloten
Poortdoorverwijzing
OK
Cancel
Hulp

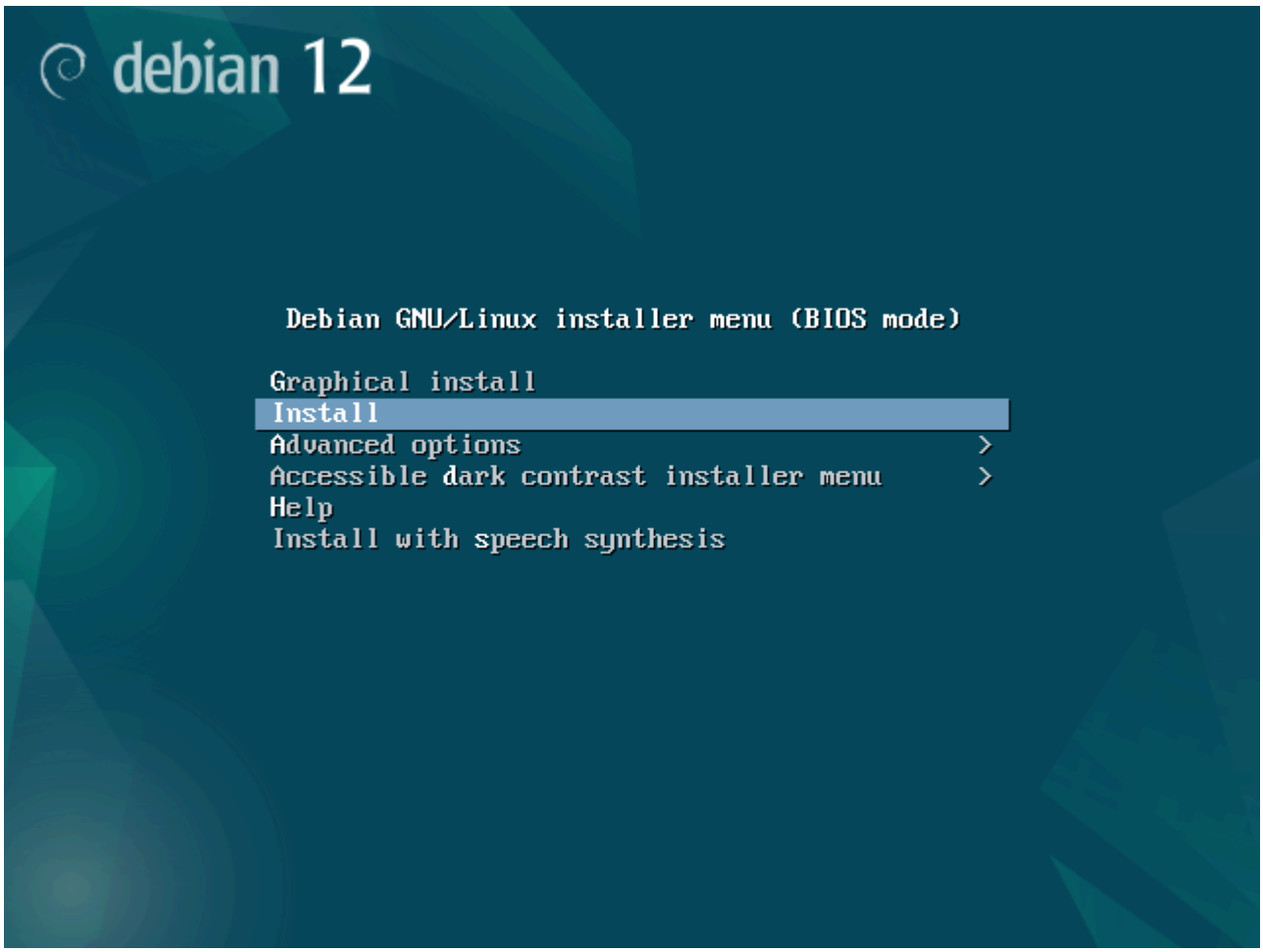

Debian server - Instellingen
Algemeen
Systeem
Beeldscherm
Opslag
Audio
Netwerk
Seriële poorten
USB
Gedeelde mappen
Gebruikersinterface
Netwerk
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Netwerkadapter inschakelen
Gekoppeld aan:
Intern netwerk
Naam:
LAN
Geavanceerd
Adaptertype:
Paravirtualized Netwerk (virtio-net)
Promiscuous-modus:
Afwijzen
MAC-adres:
08002770C089
Kabel aangesloten
OK
Cancel
Hulp

OS

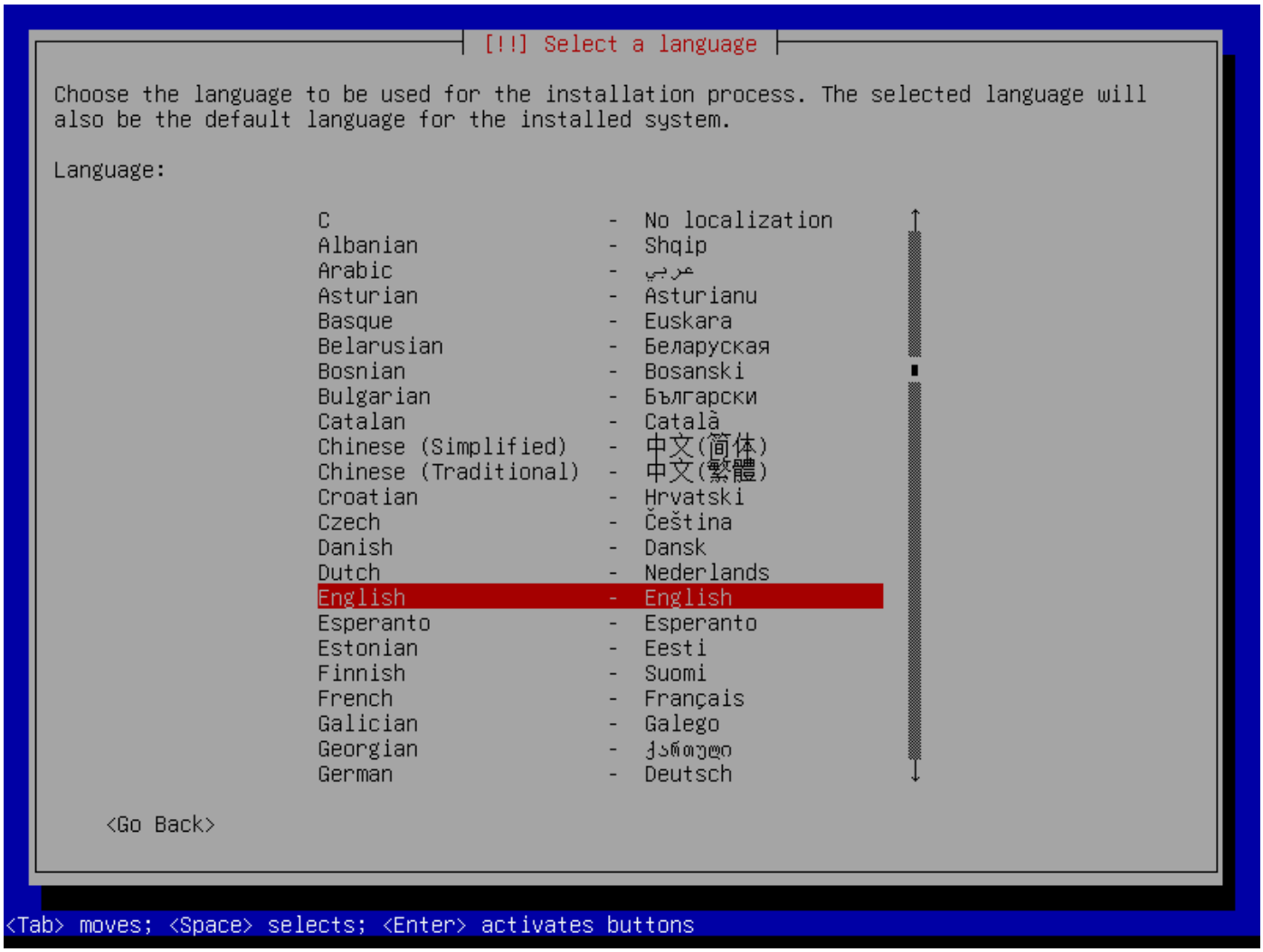
we will use Debian as the server OS as it's a very reliable, trusted linux distribution with minimal system requirements.

Installation steps

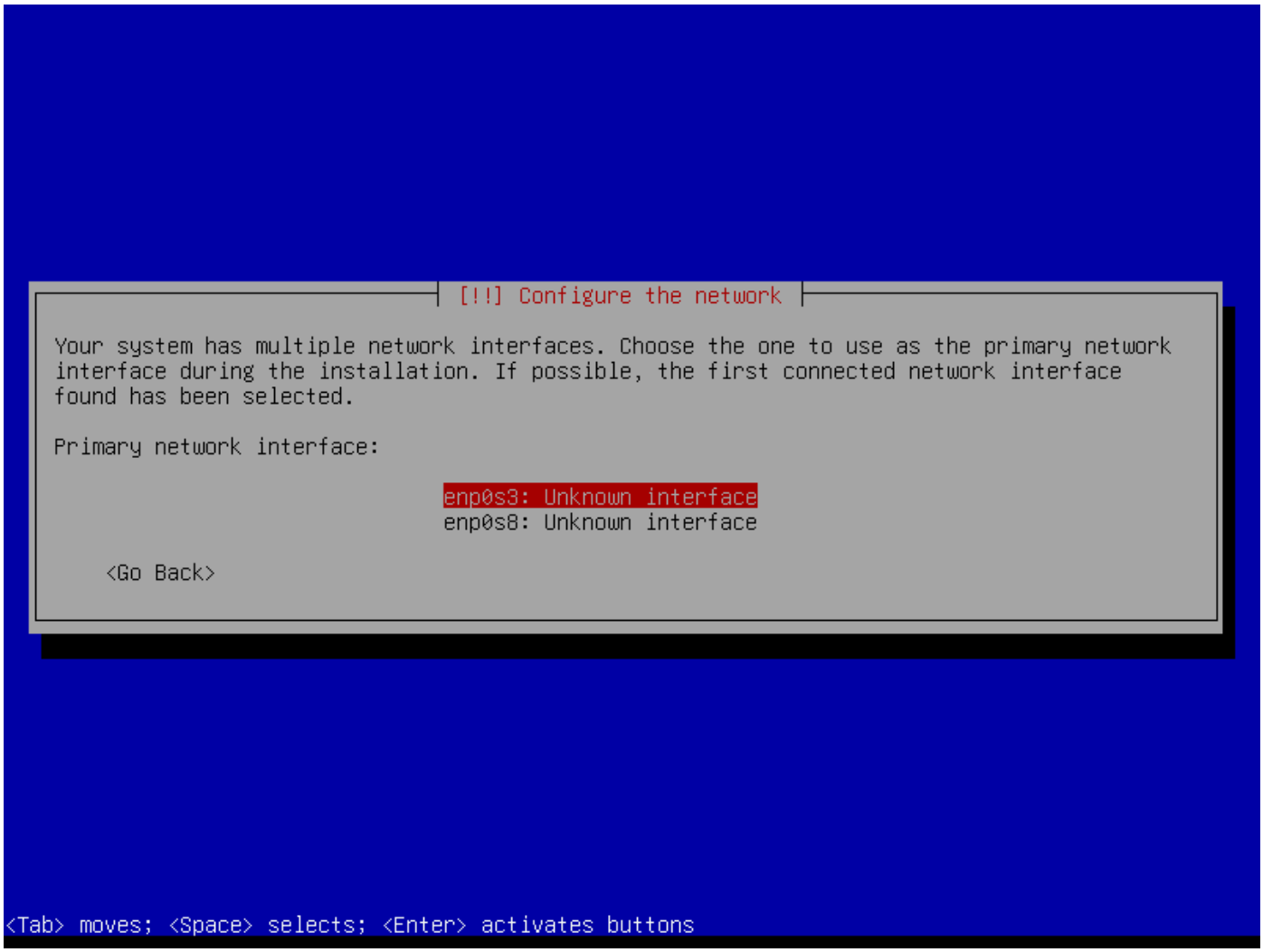
- choose a non graphical install



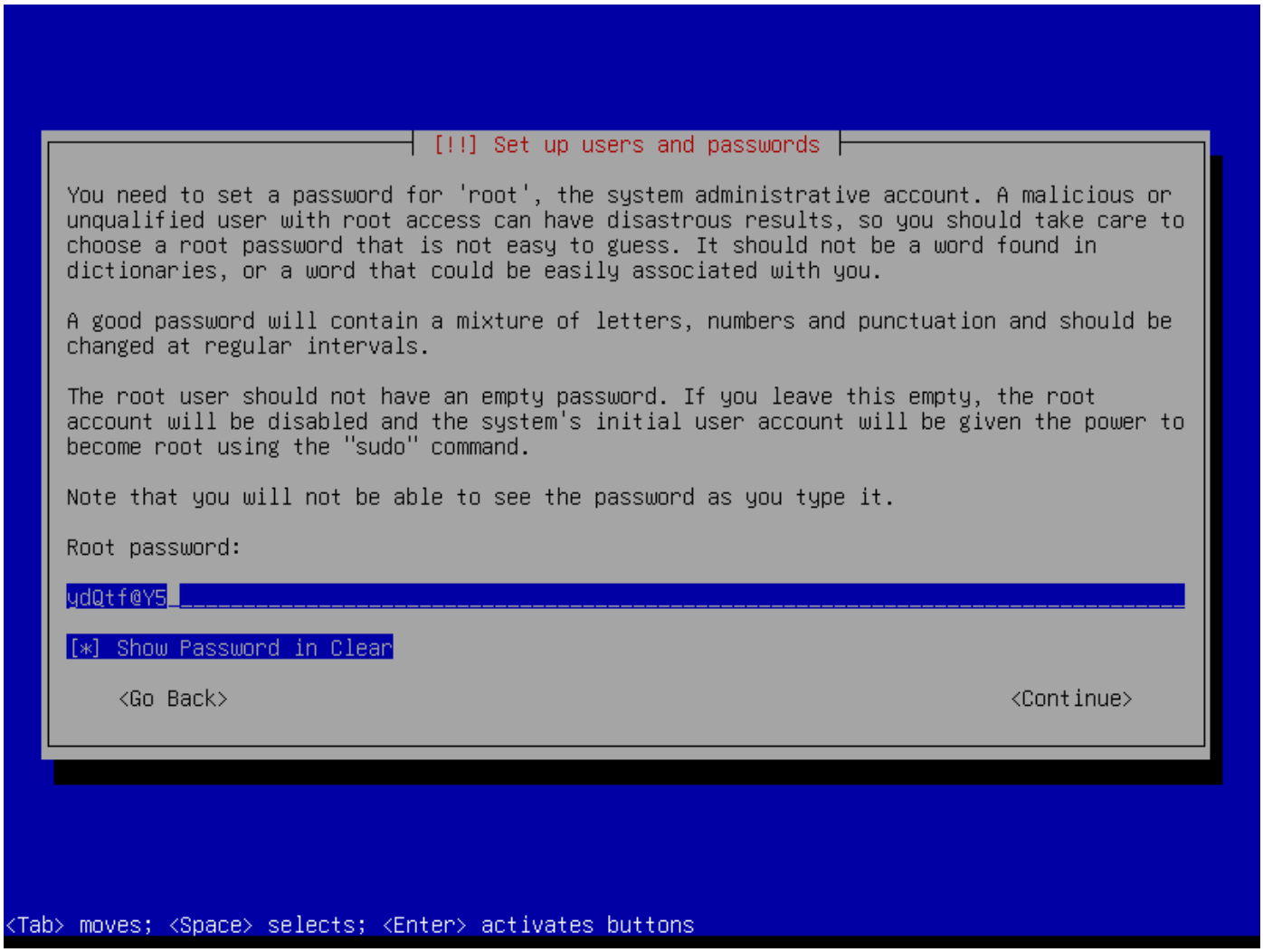
- choose your language, country,locale and keyboard map



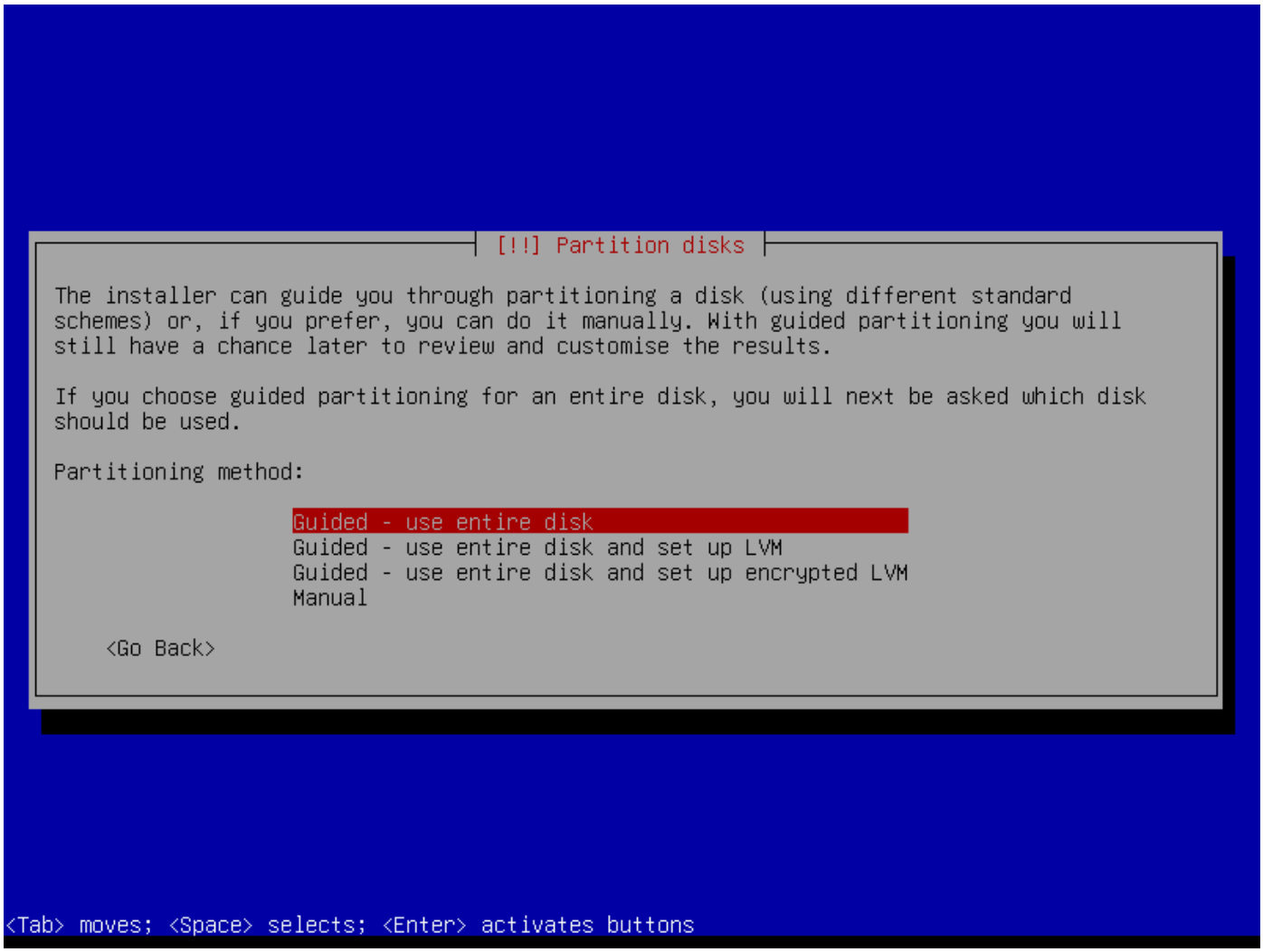
- choose the external network adaptor.



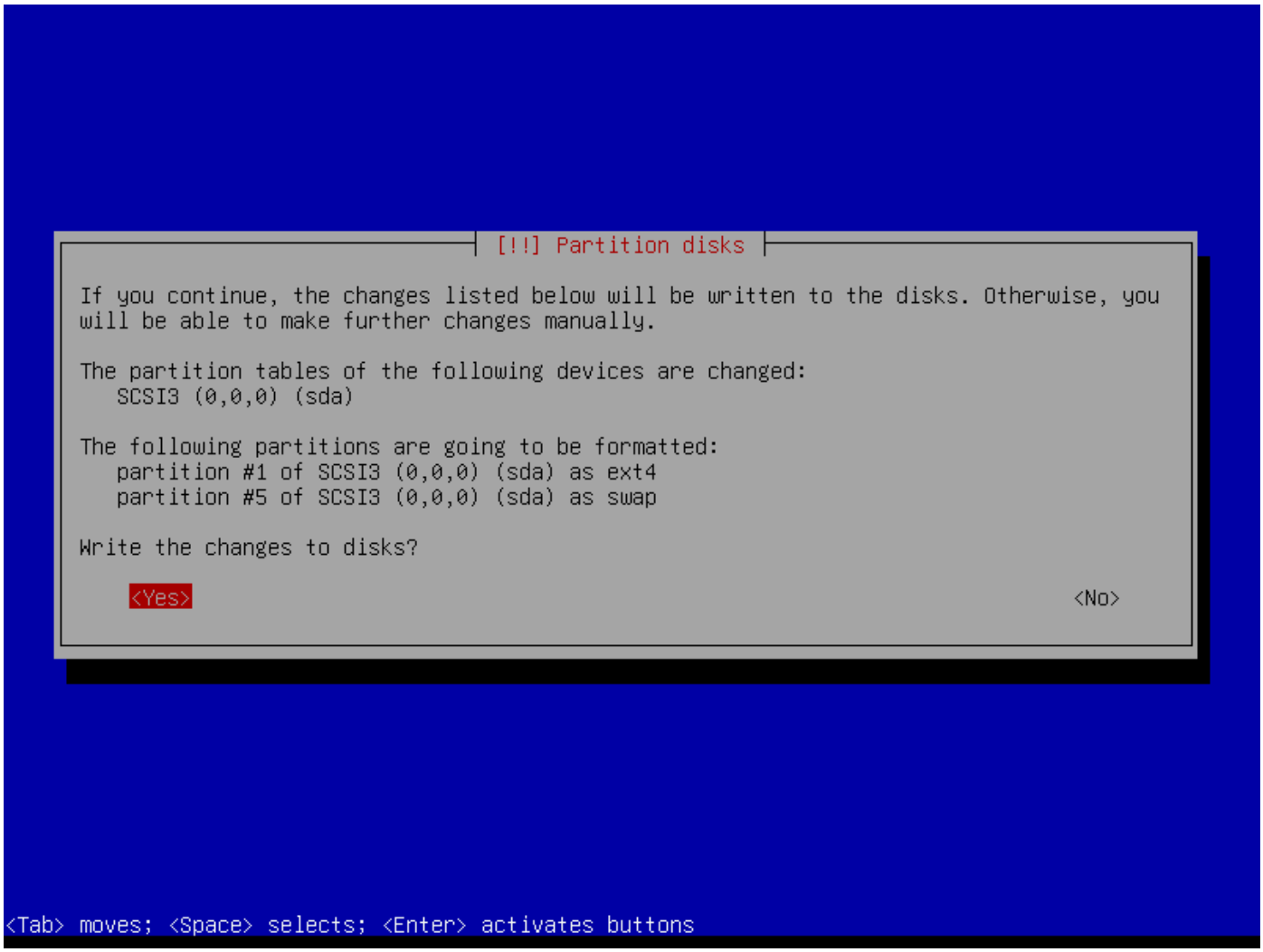
- Enter a hostname and domain name(Server1 and library.be respectively in this case)



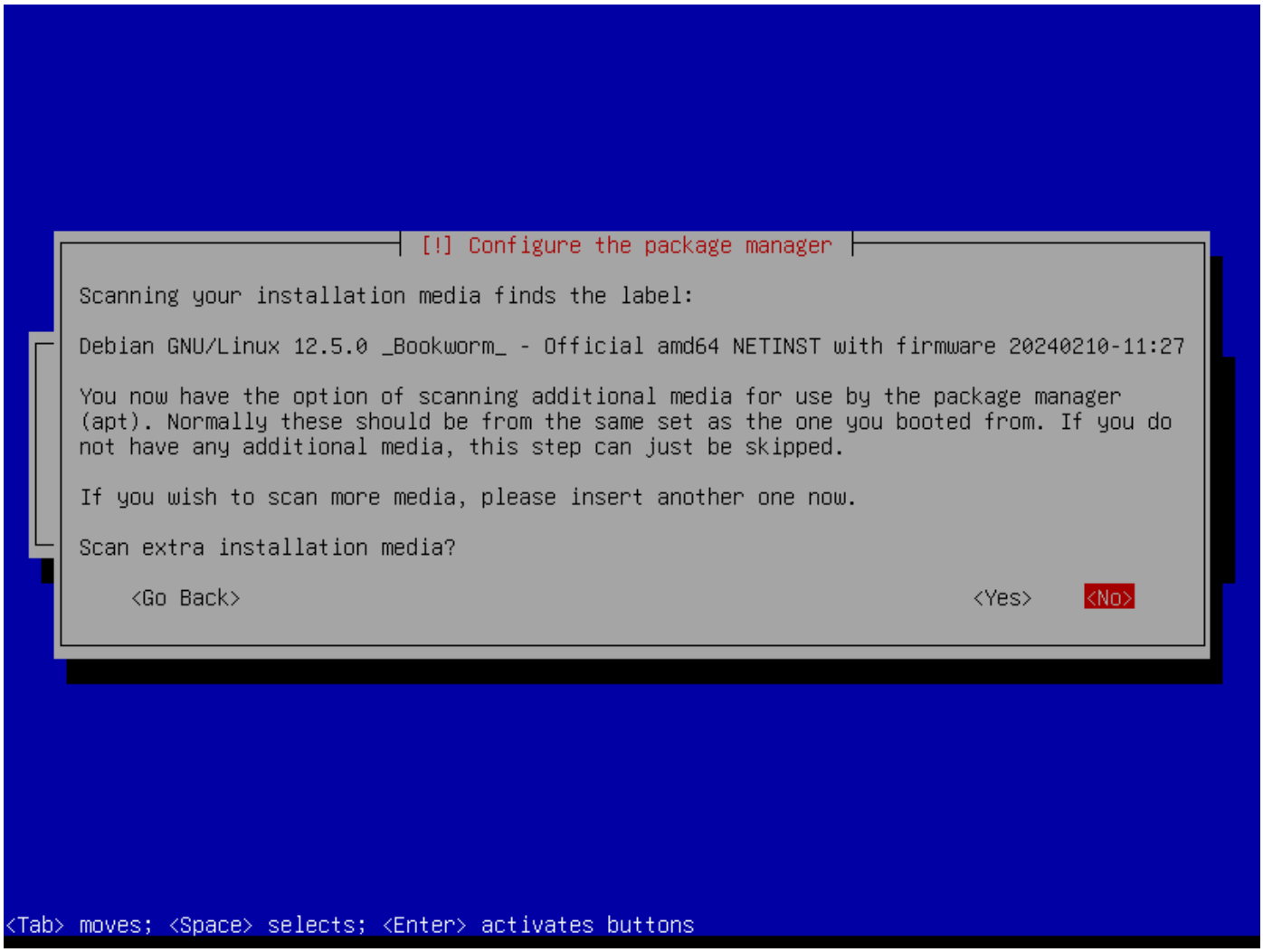
- Choose a root password: ydQtf@Y5
- create a new user by following the prompts
- for partitioning choose guided - use entire disk -> all files in one partition



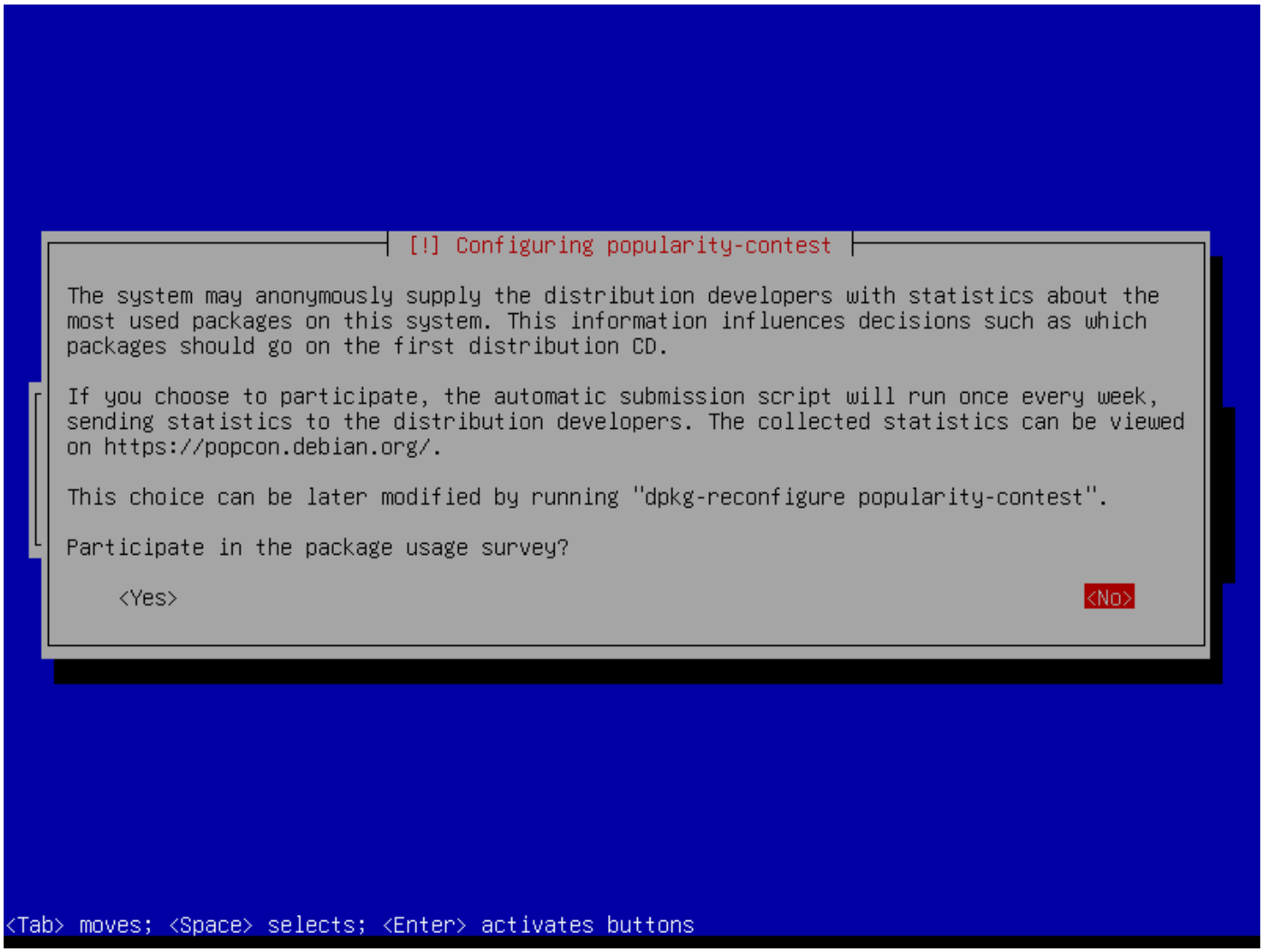
- write changes to disk



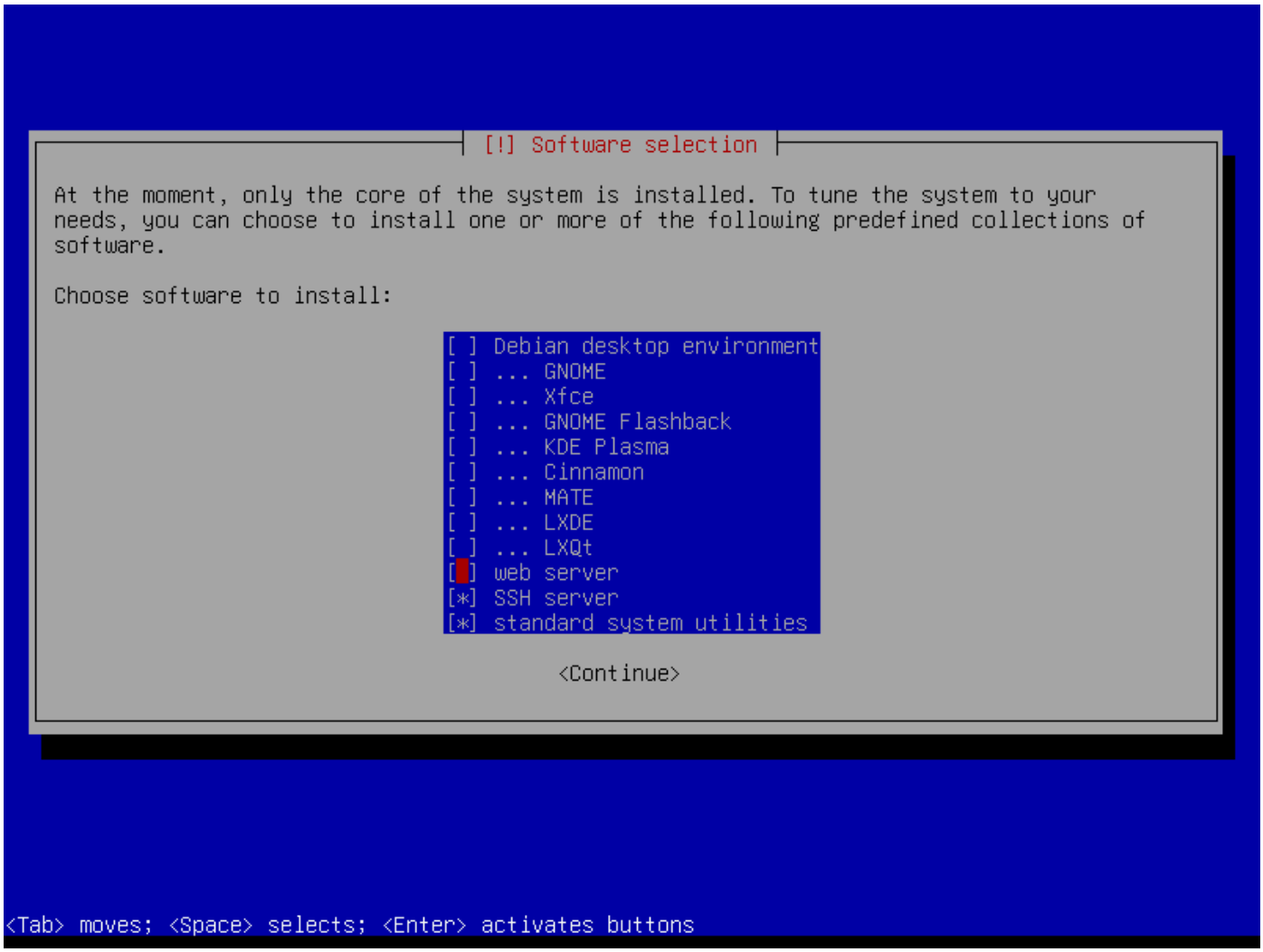
- don't scan extra installation media



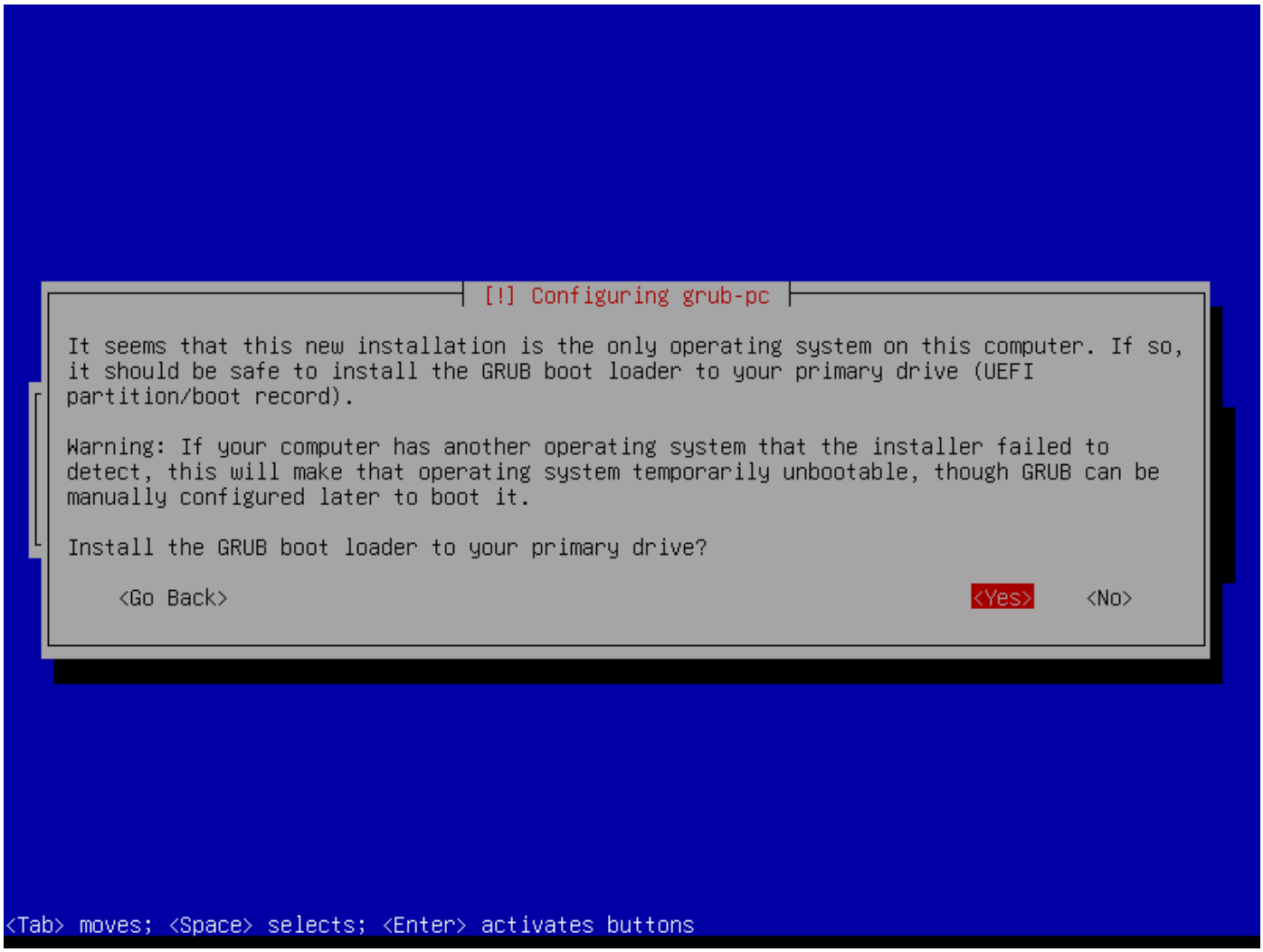
- choose a mirror (any belgian one will work fine)
- don't participate in the package survey

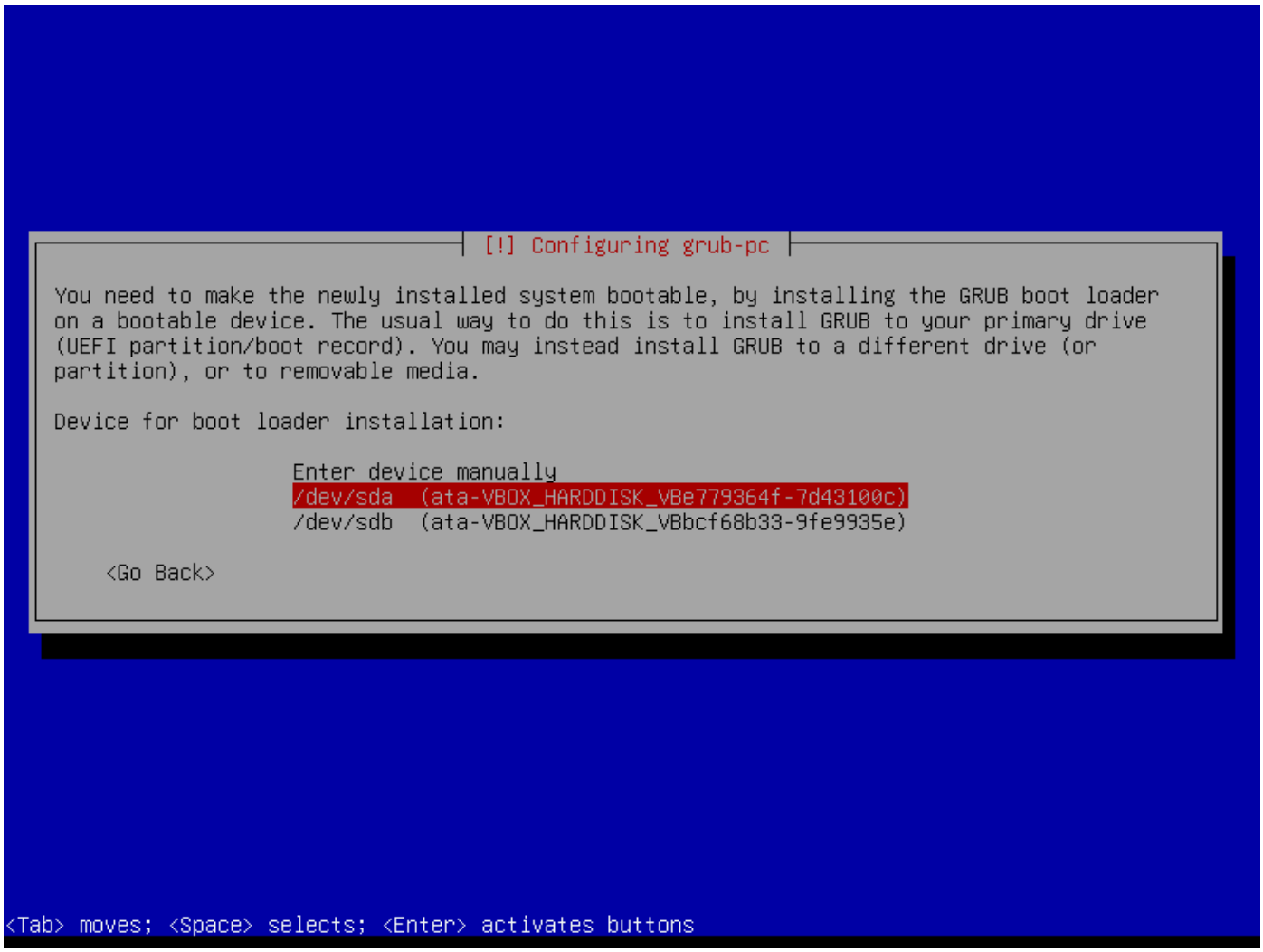


- uncheck the desktop environment, check the ssh server in software selection



- 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



- 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
    ```

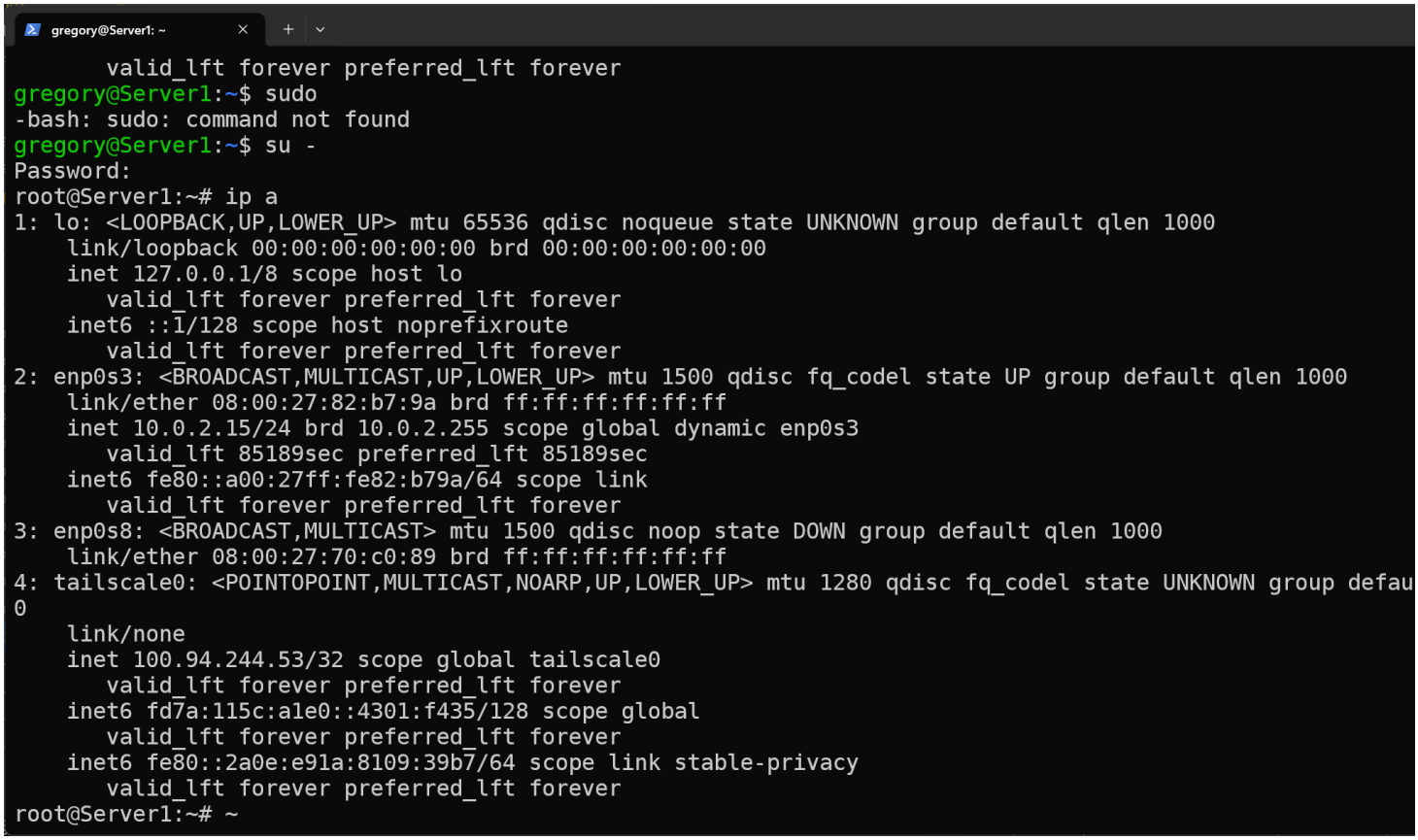
  - add a filesystem to /dev/sdb1

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

Configure the internal network adaptor

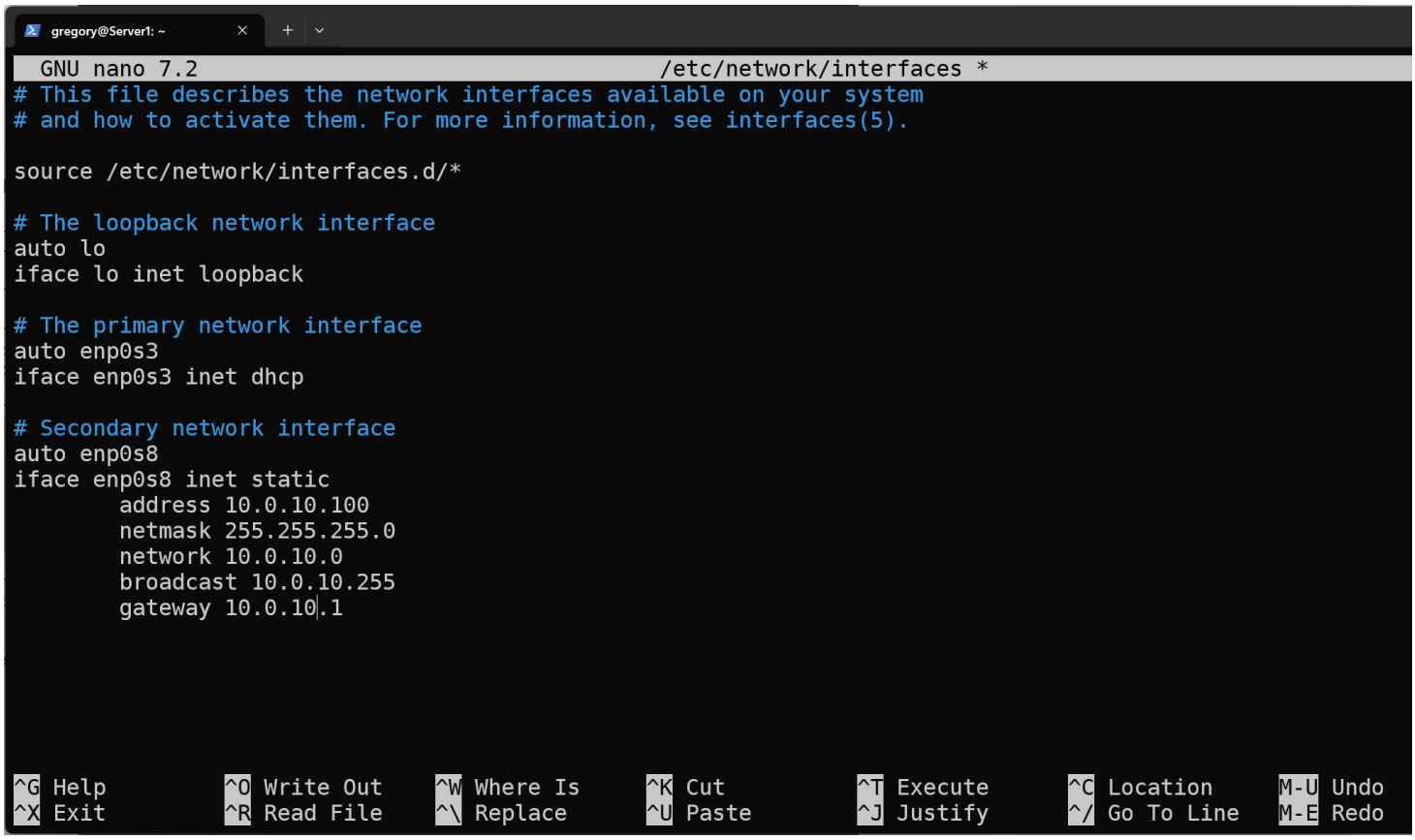
- find your network interface names

```
ip a
```



- 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
```



- 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
```

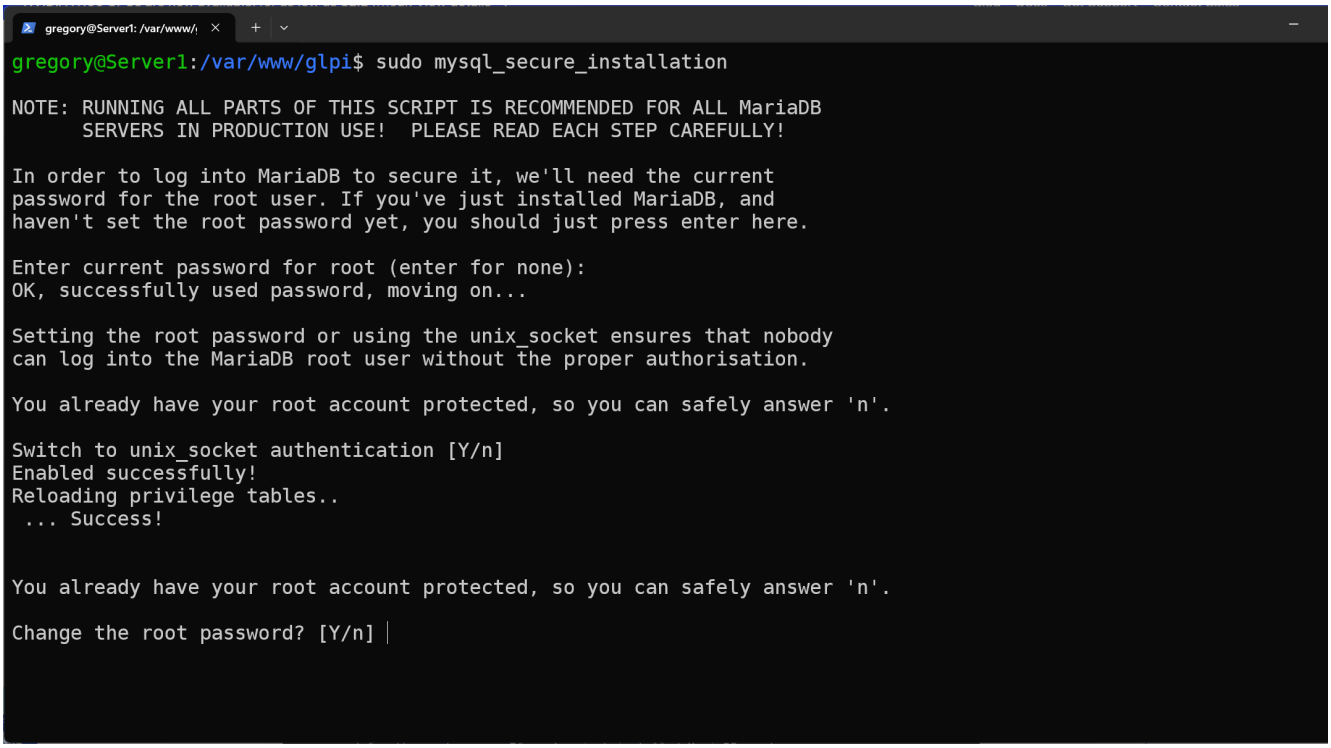
create /etc/nginx/sites-enabled/glpi and add the following

```
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;
    }
}
```

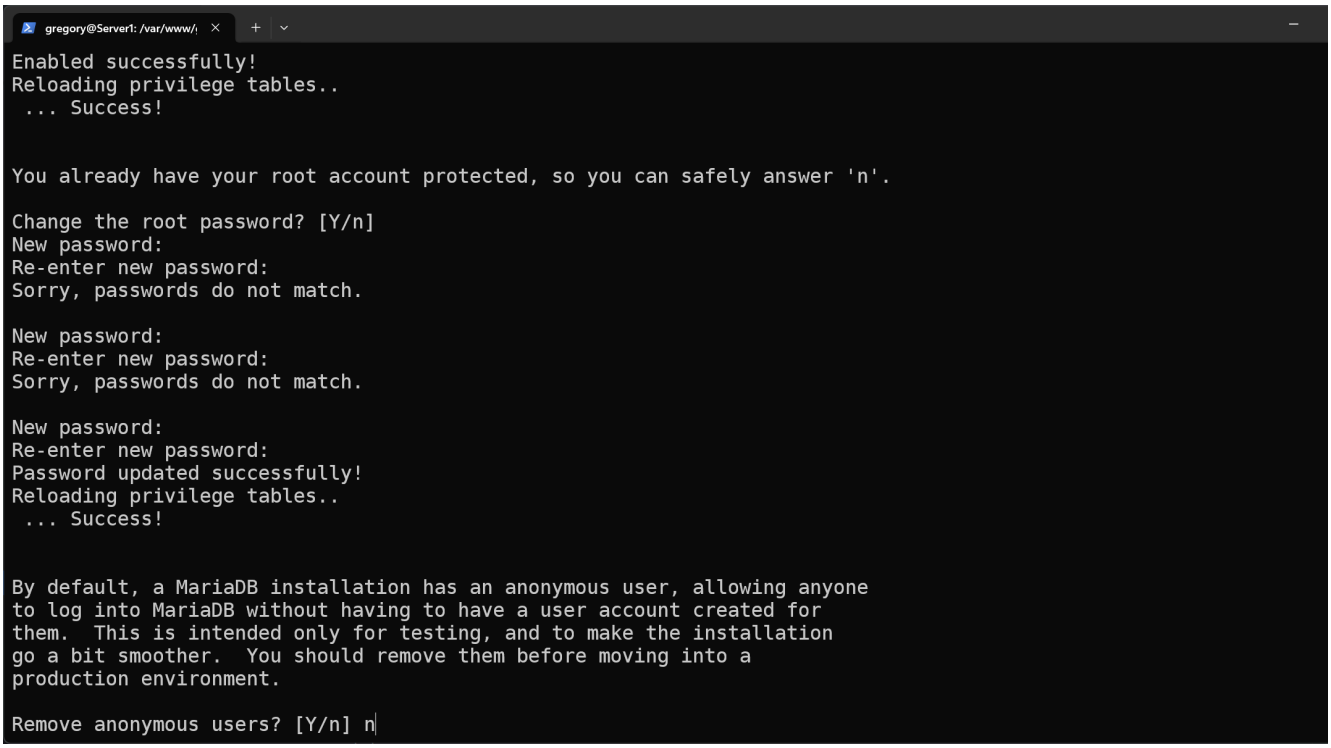
- install mariadb

```
apt install mariadb-server
mysql_secure_installation
```

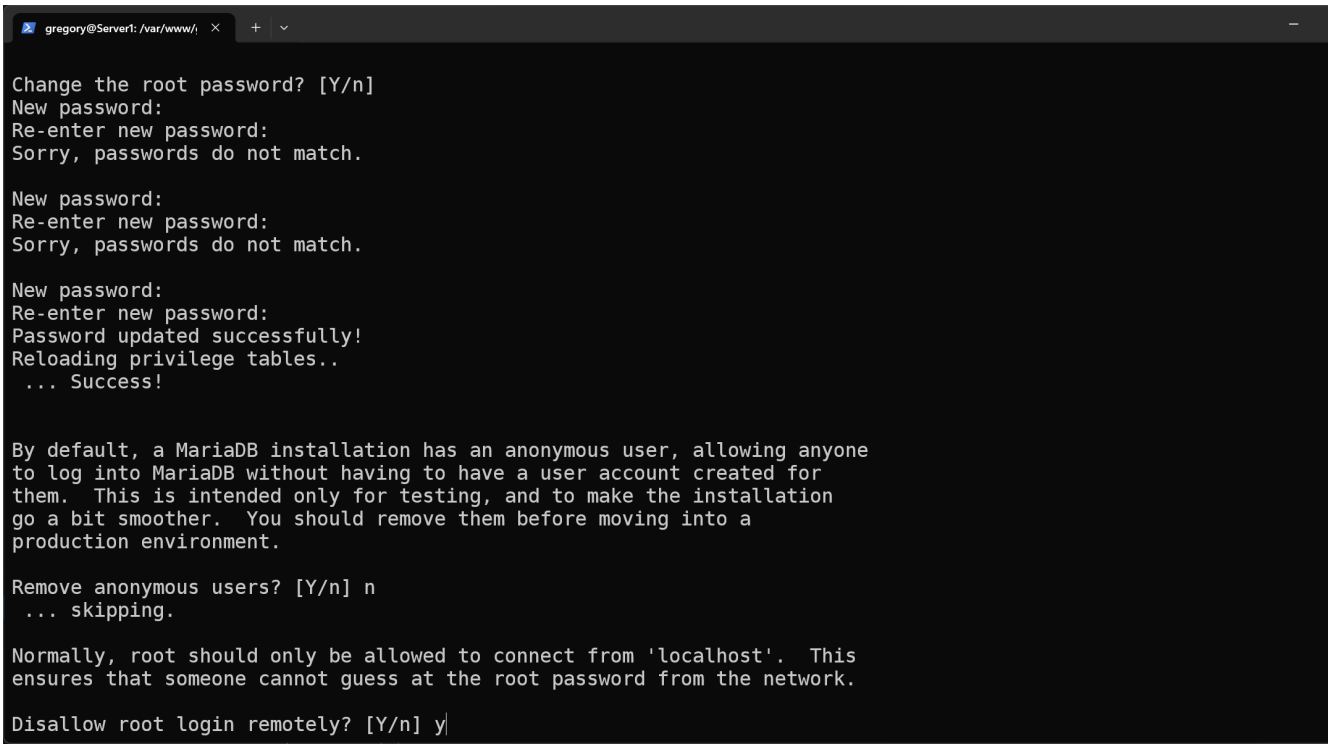
- configure root user
    - set root password for mariadb to b4#9etCY



- disallow anonymous users



- disallow root remote login



- 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

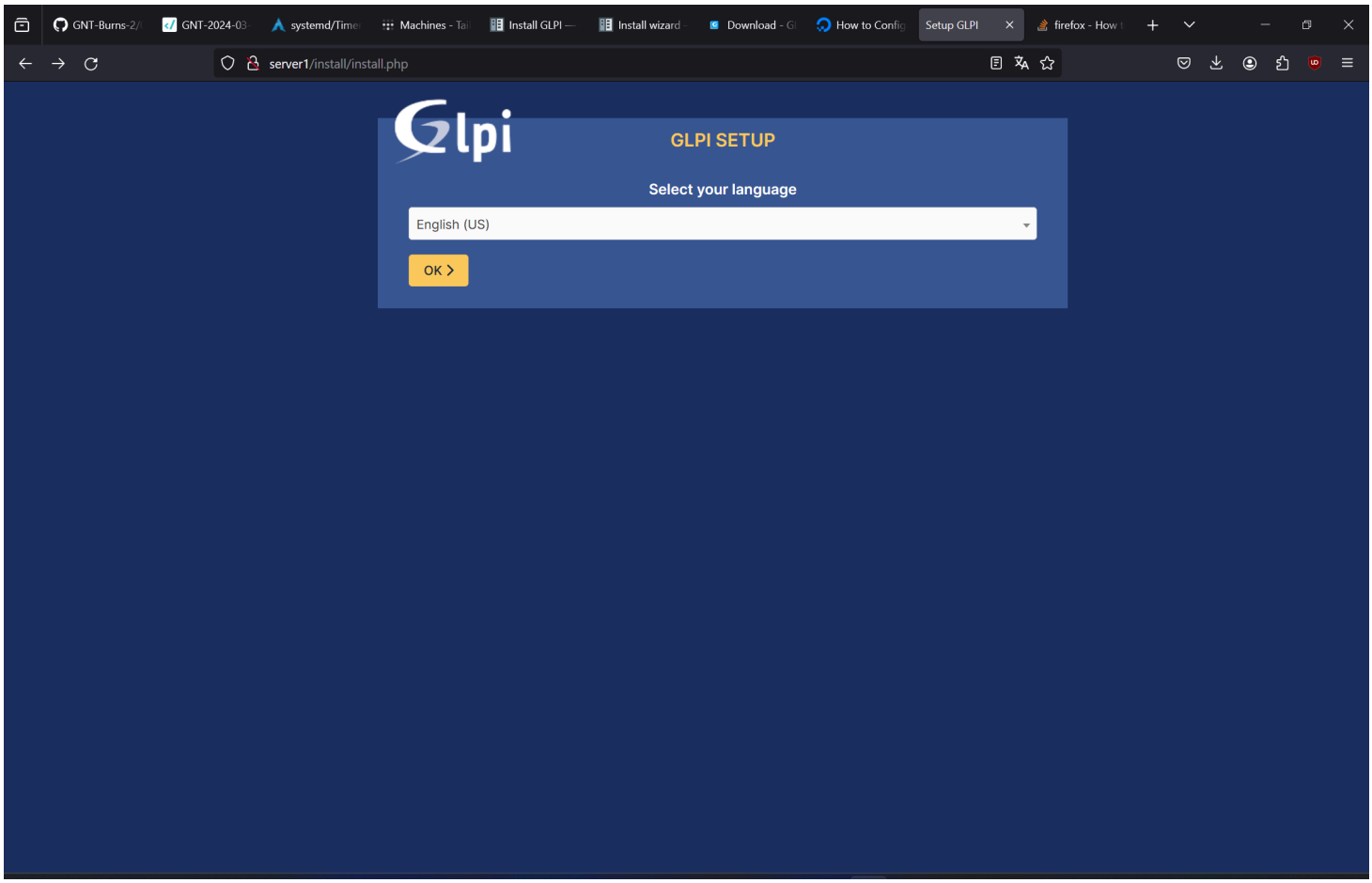
- restart php-fpm

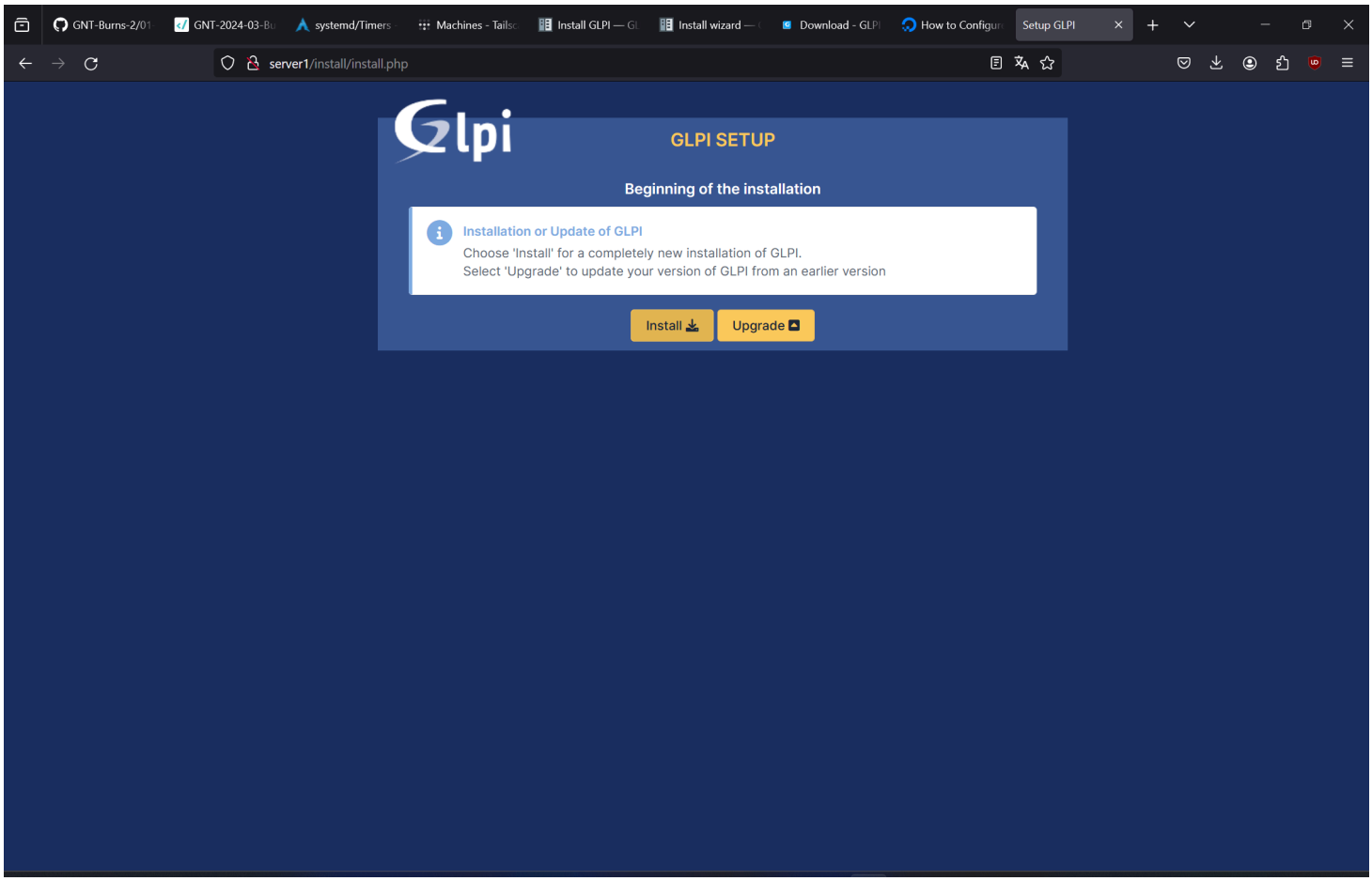
  ```
  systemctl restart php8.2-fpm.service
  ```

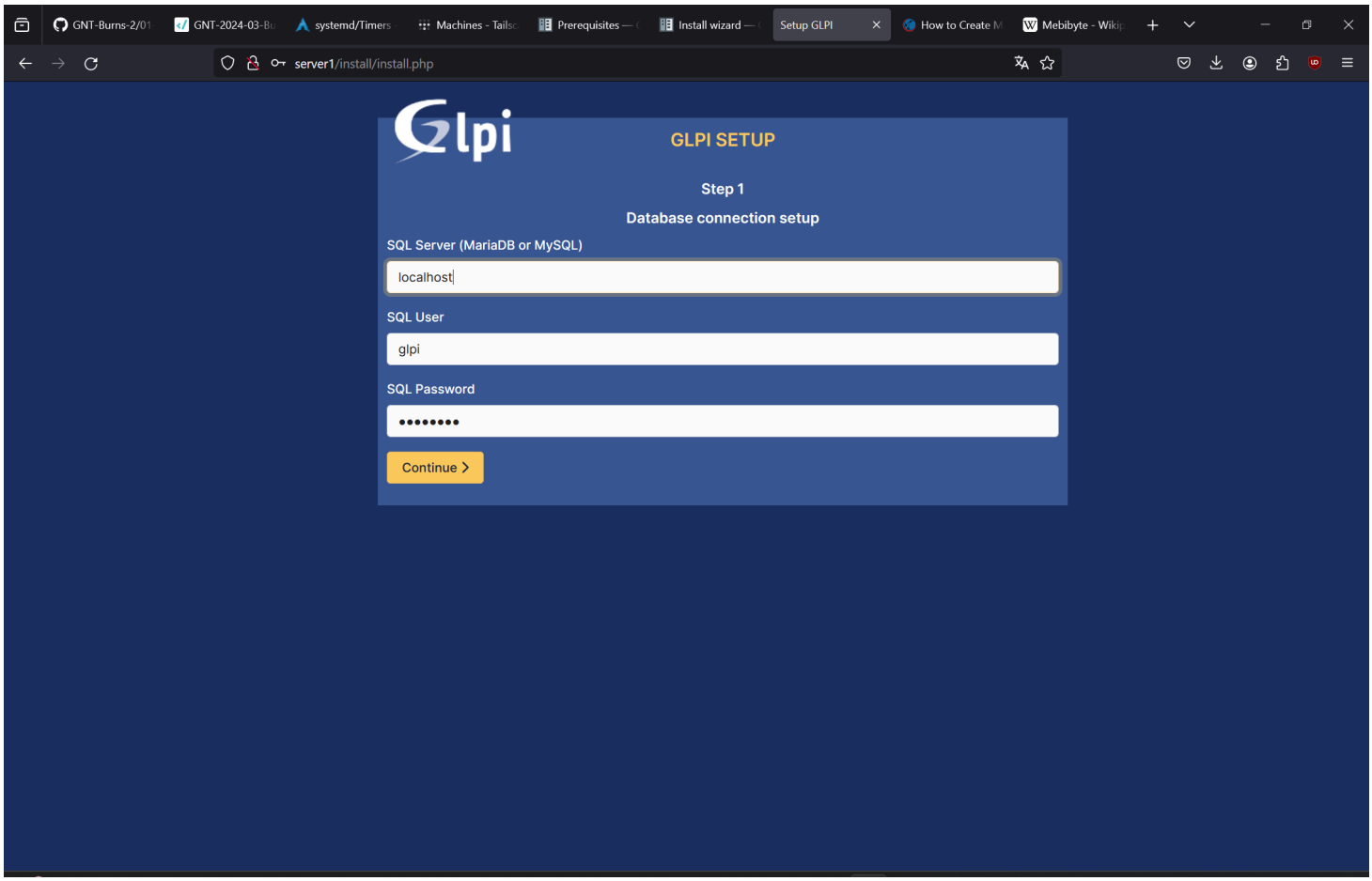
- install glpi

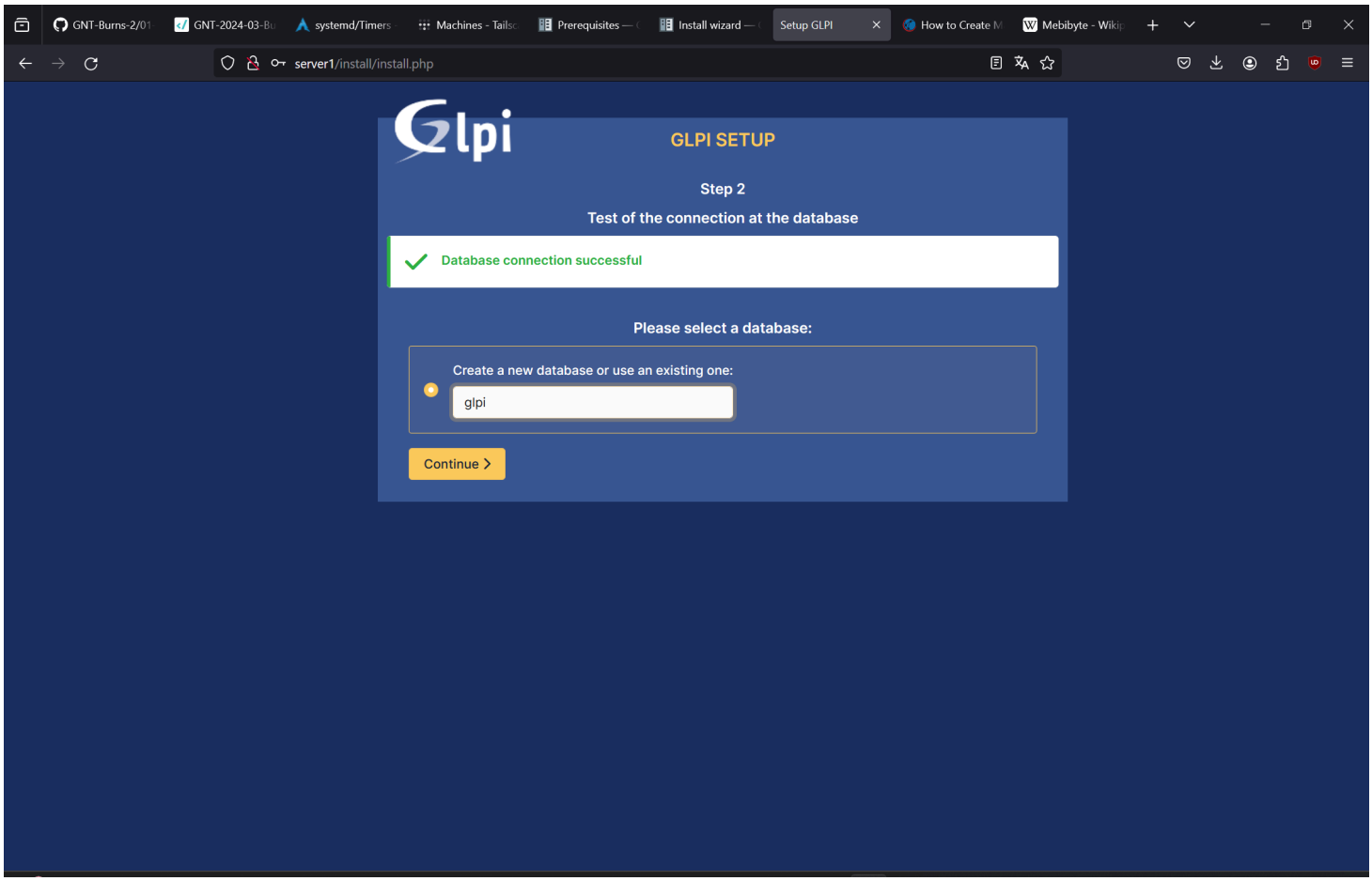
```
wget https://github.com/glpi-project/glpi/releases/download/10.0.14/glpi-10.0.14.tgz
tar -xf glpi-10.0.14.tgz --directory=/var/www/
rm glpi-10.0.14.tgz
cd /var/www/glpi
chgrp -R www-data config/
chgrp -R www-data files/
chmod -R 770 config/
chmod -R 770 files/
```

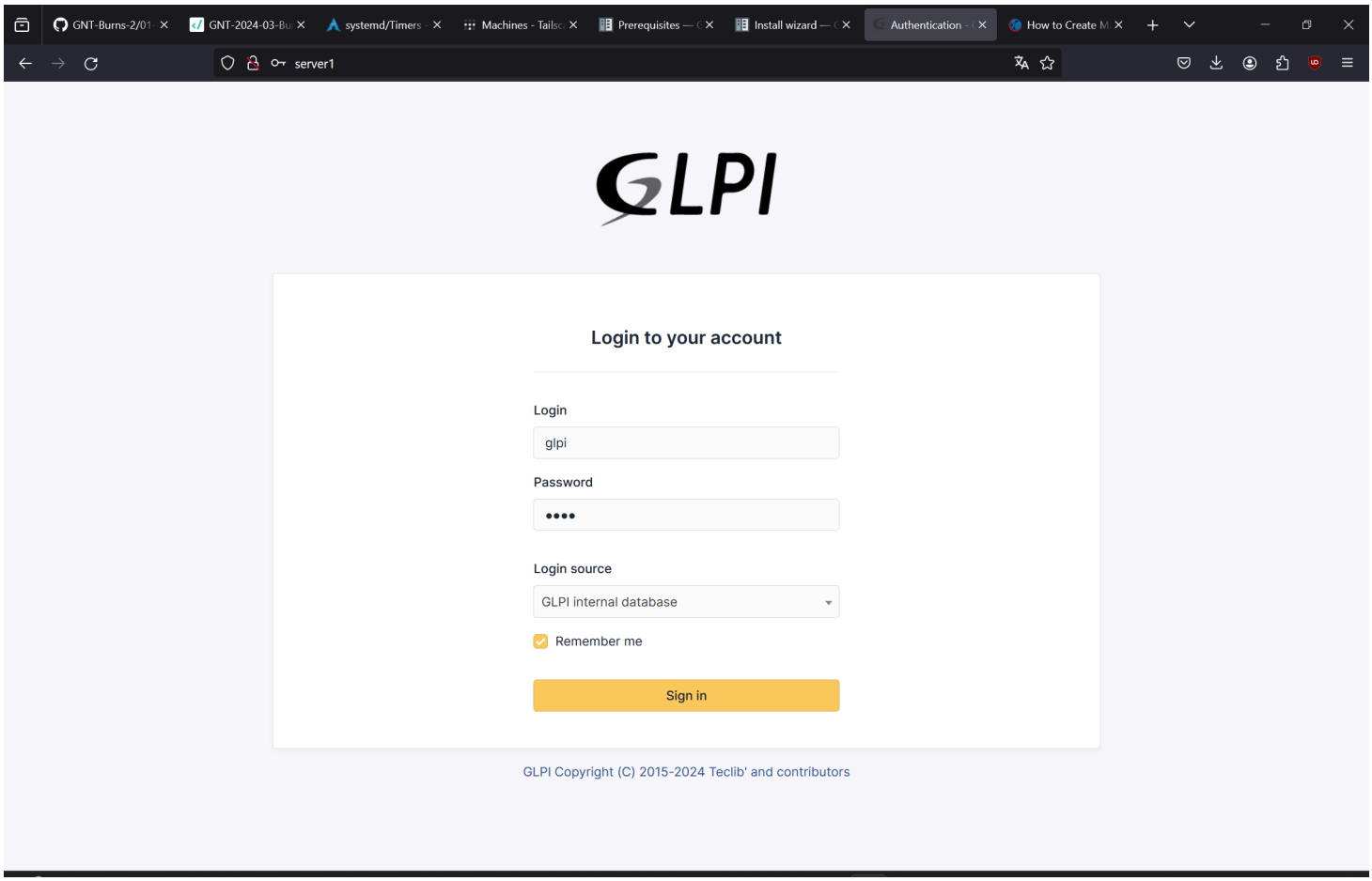
go to http://10.0.10.100 in a browser




server1/install/install.php
GLPI SETUP
Beginning of the installation
Installation or Update of GLPI
Choose 'Install' for a completely new installation of GLPI.
Select 'Upgrade' to update your version of GLPI from an earlier version
Install
Upgrade


server1/install/install.php
GLPI SETUP
Step 1
Database connection setup
SQL Server (MariaDB or MySQL)
localhost
SQL User
glpi
SQL Password
Continue


server1/install/install.php
GLPI SETUP
Step 2
Test of the connection at the database
Database connection successful
Please select a database:
Create a new database or use an existing one:
glpi
Continue


server1
Login to your account
Login
glpi
Password
Login source
GLPI internal database
Remember me
Sign in
GLPI Copyright (C) 2015-2024 Teclib' and contributors

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/mysq
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

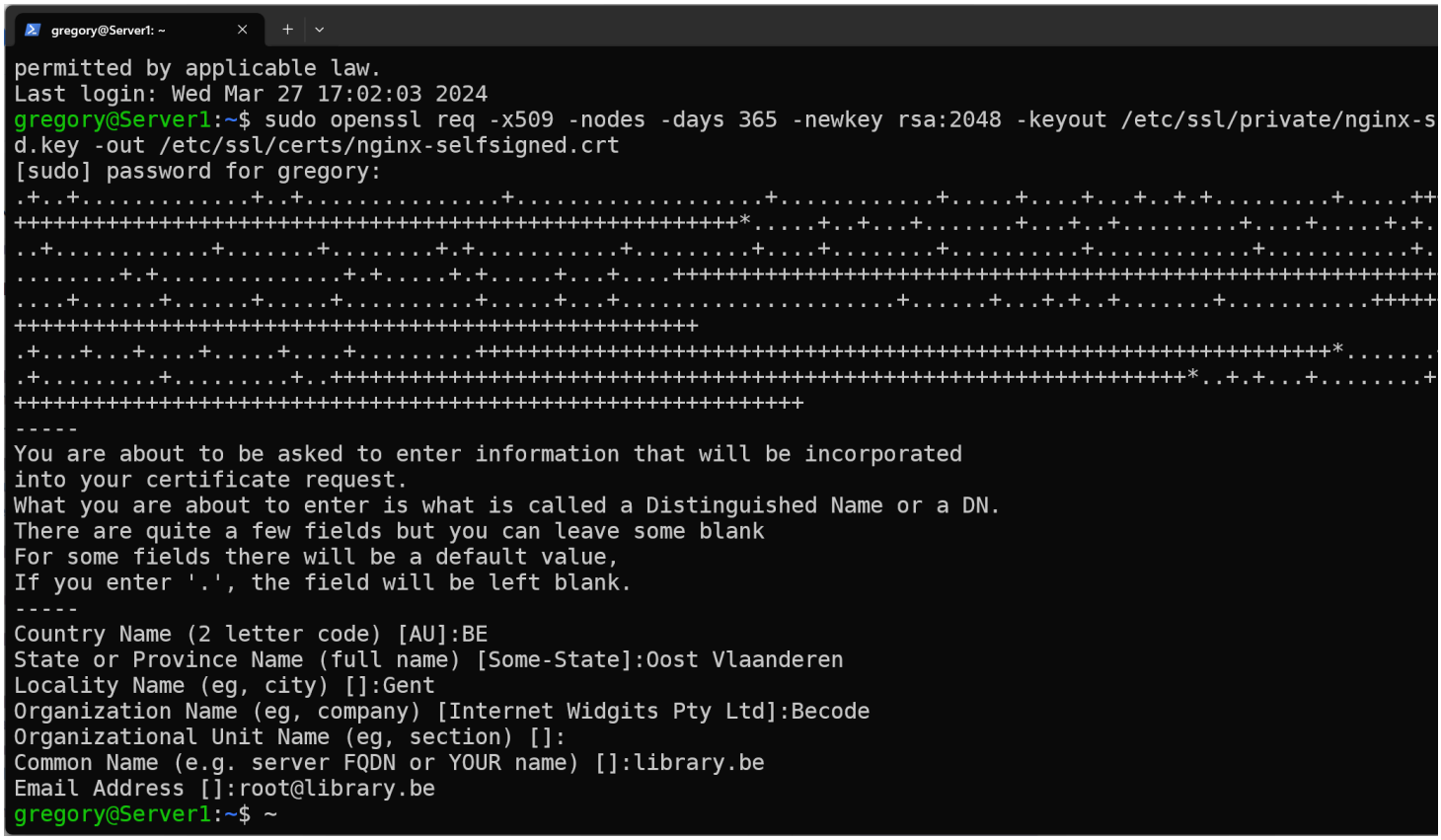
```
systemctl daemon-reload
systemctl start backup-settings.timer
```

extras

self signed certificate for nginx

- create the certificate on the server

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



- 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/glpi to

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

    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;
    }
}

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

    server_name gpli.library.be;

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

- restart nginx

```
sudo systemctl restart nginx
```

Workstation

Virtual Machine Configuration

Network Adapters

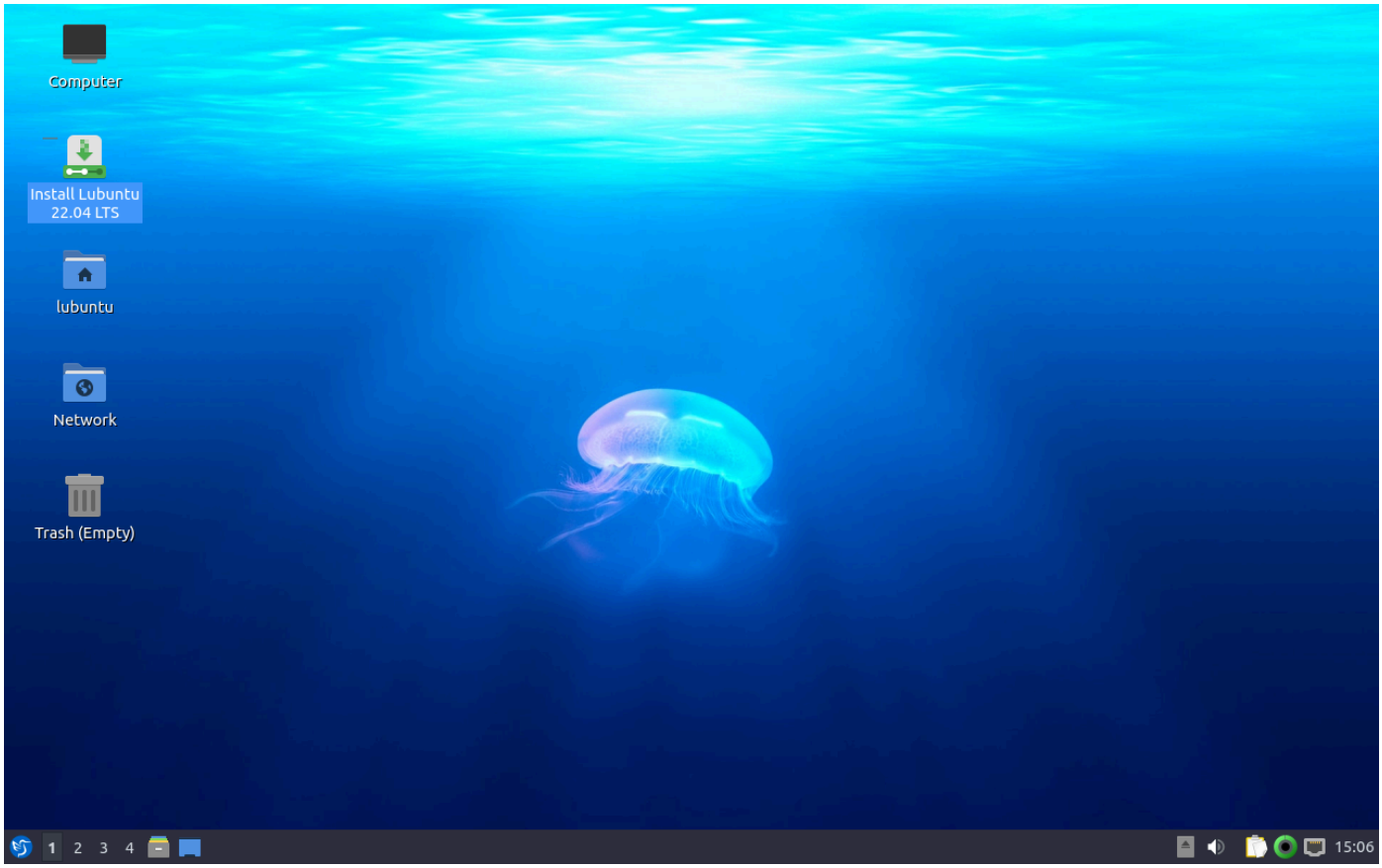
we use one internal network adapter and one NAT network adapter

OS

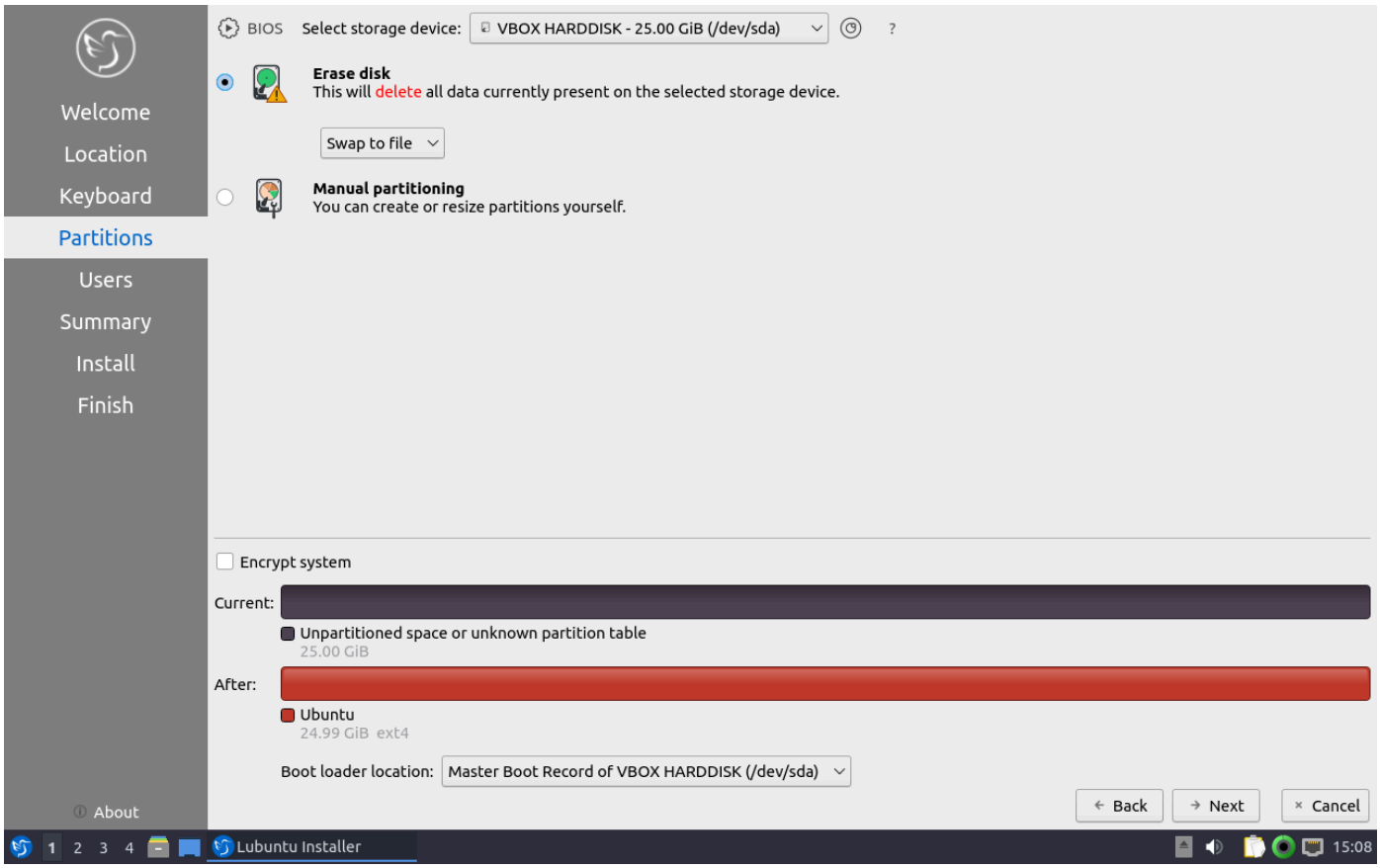
We will use Lubuntu as the workstation os as it offers a solid ubuntu base and a lightweight desktop environment. It will run well on less powerfull hardware

Installation steps

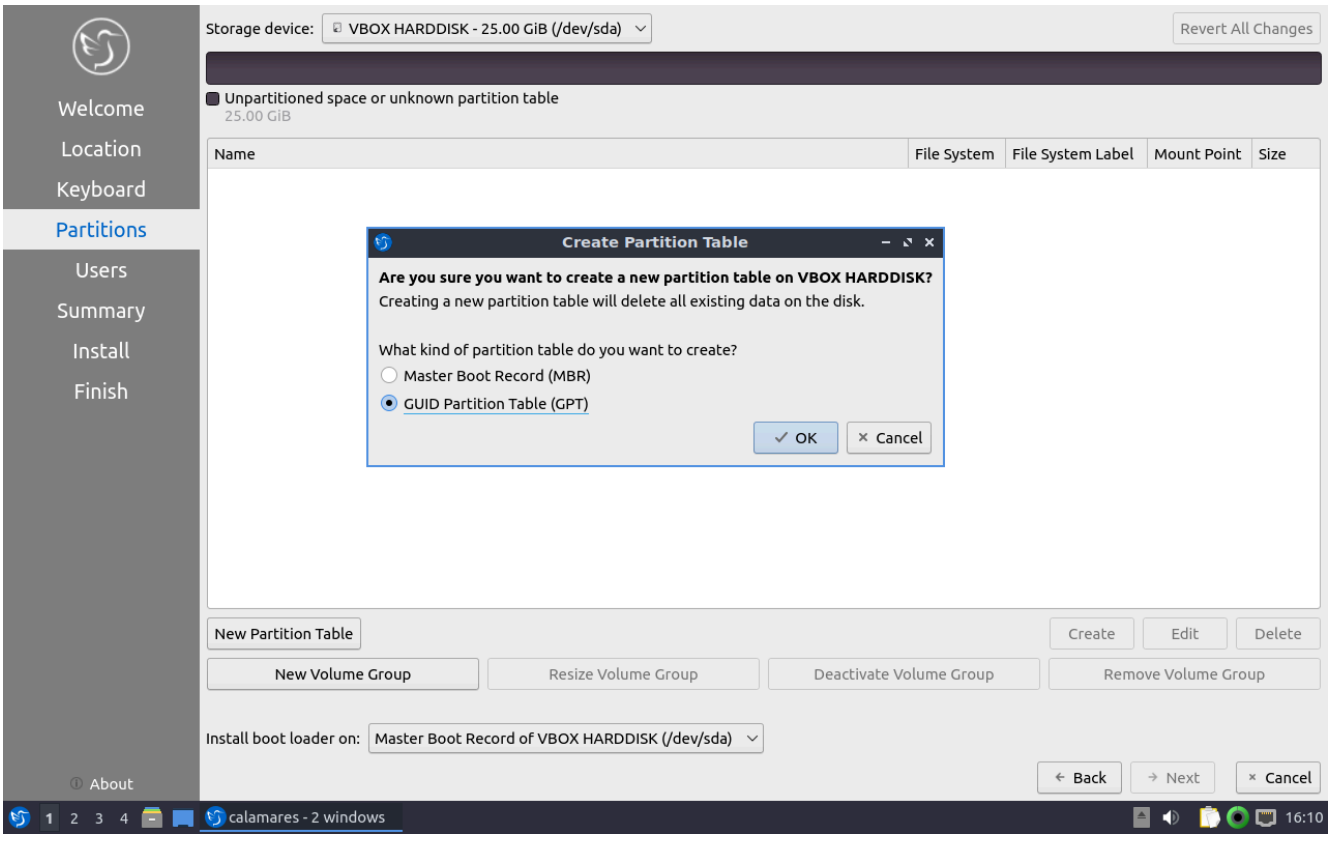
- Download the lubuntu iso from the lubuntu website
- Start machine with Lubuntu iso inserted.
- click install



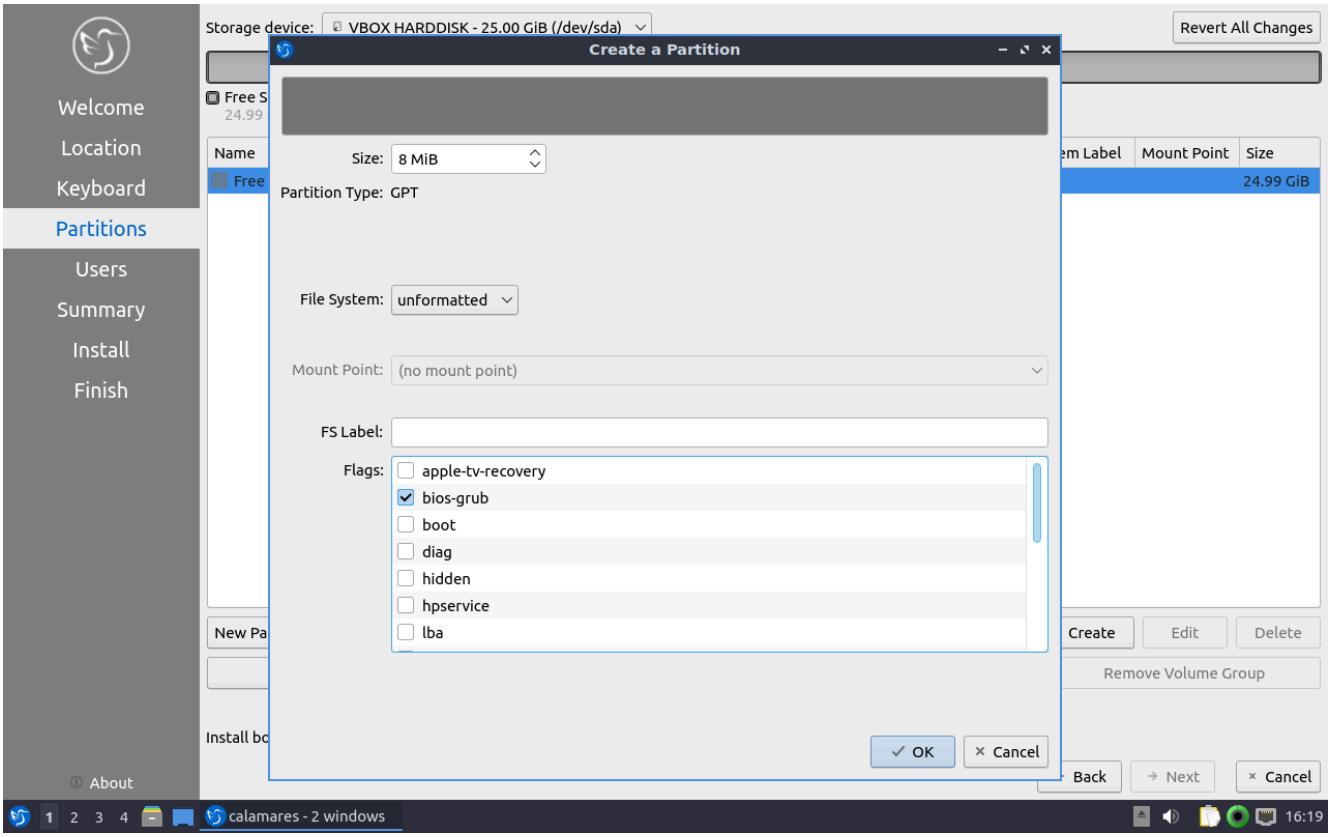
- continue untill partitioning



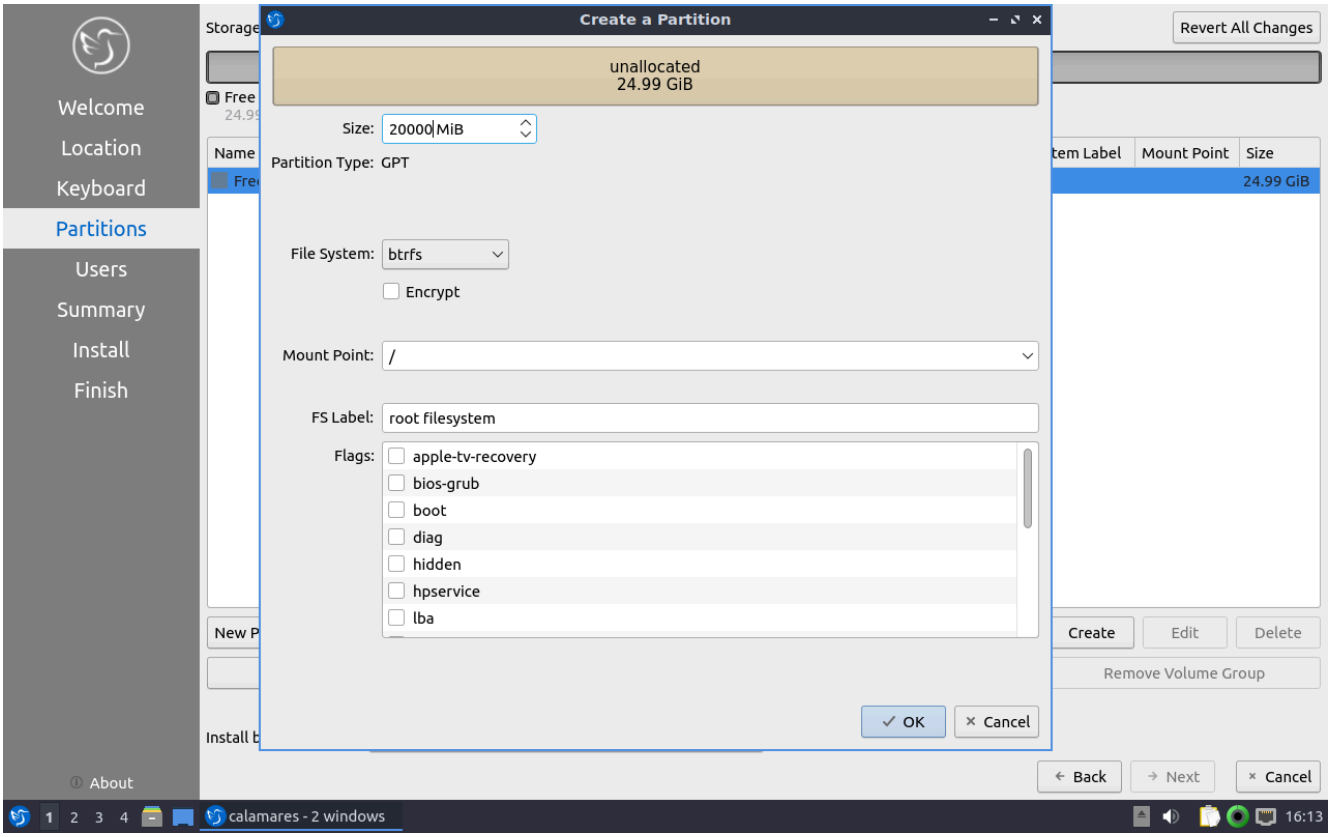
- choose manual partitioning and assign both a / and /home partition
  - new partition table -> GPT



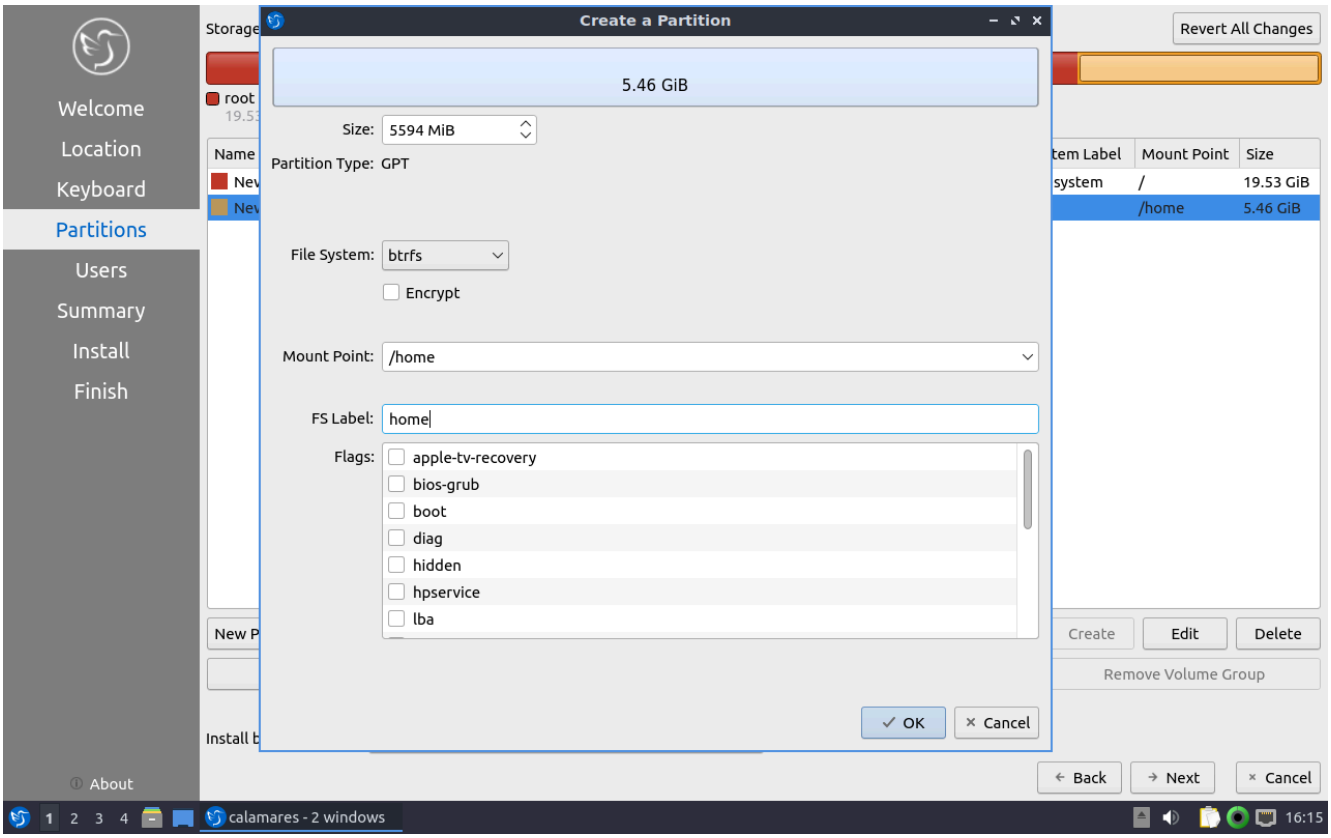
  - create a new 8MB unformatted partition and add the bios-grub flag



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

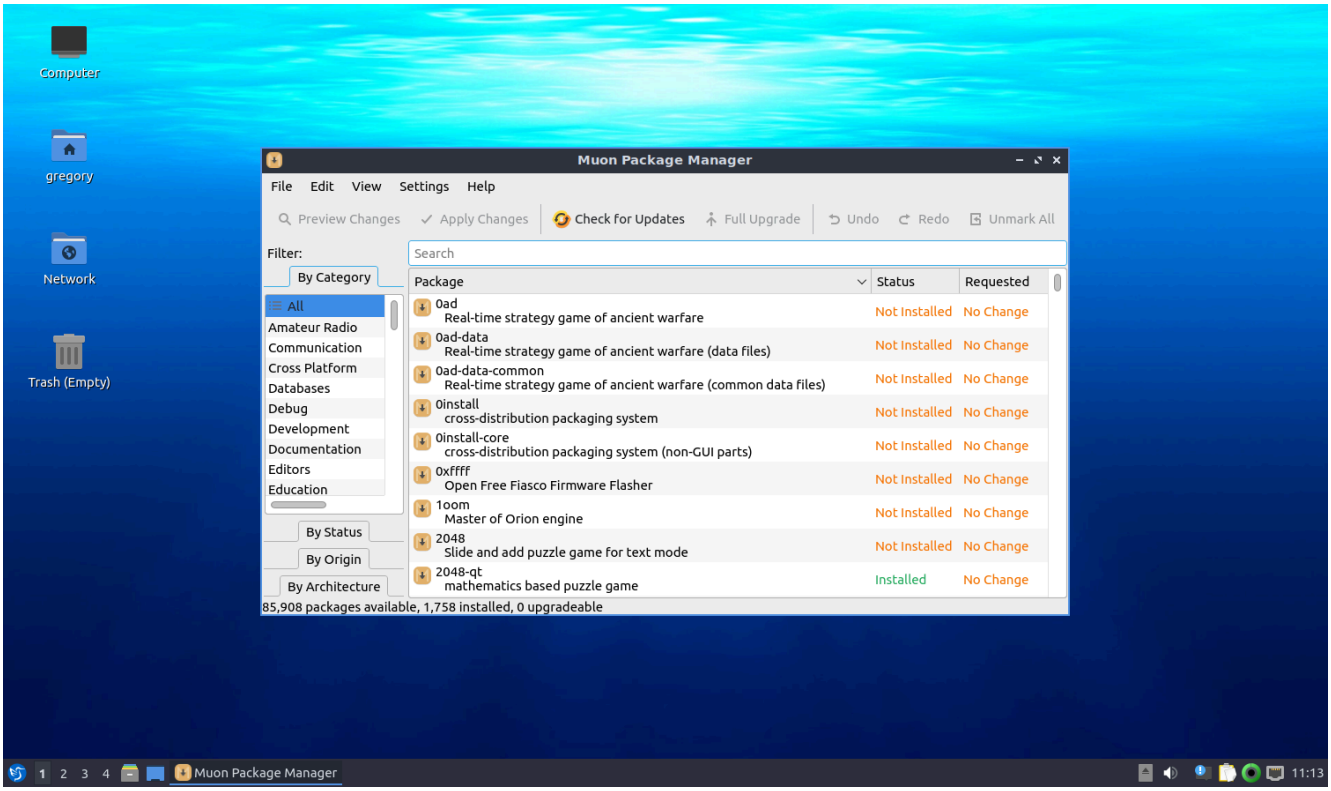


- click on free space -> create -> pick a size, btrfs as filesystem and /home as mountpoint

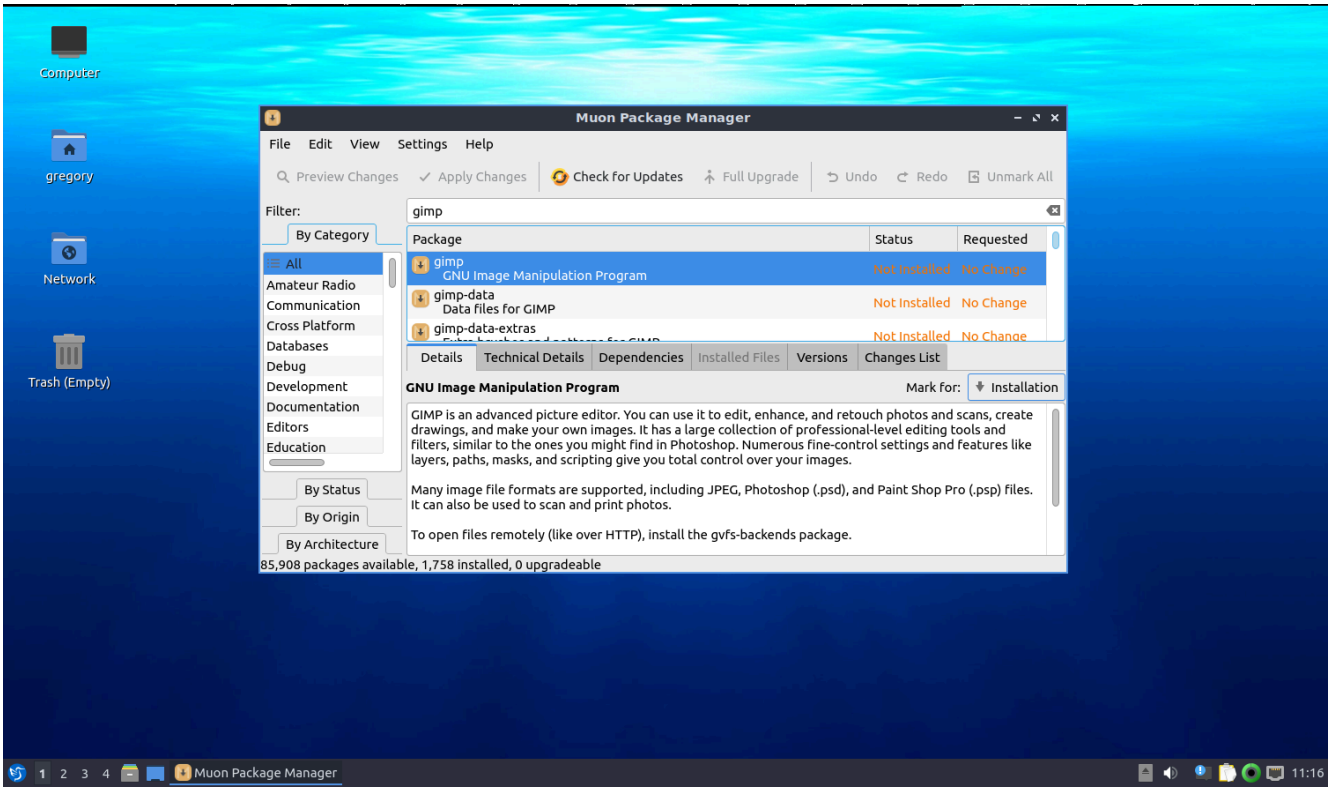


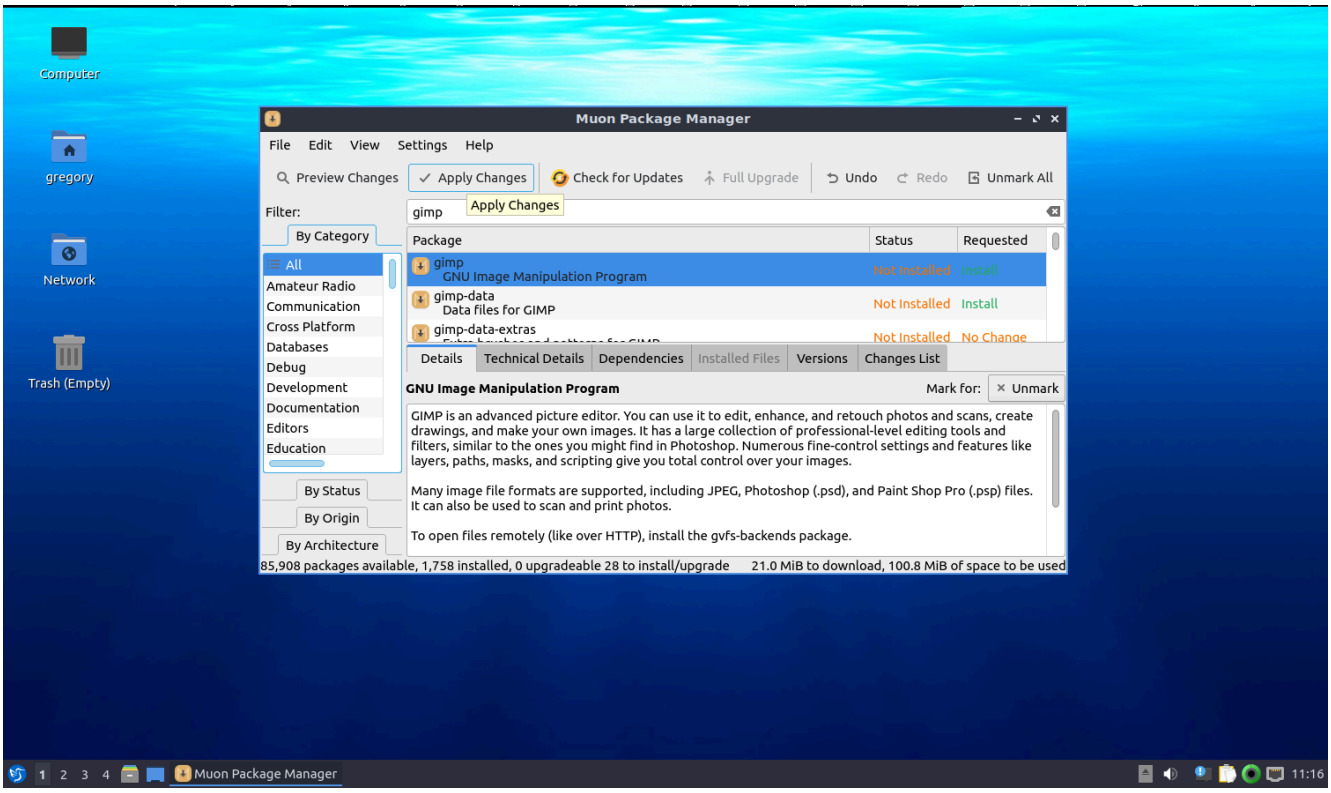
post installation

- 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
```