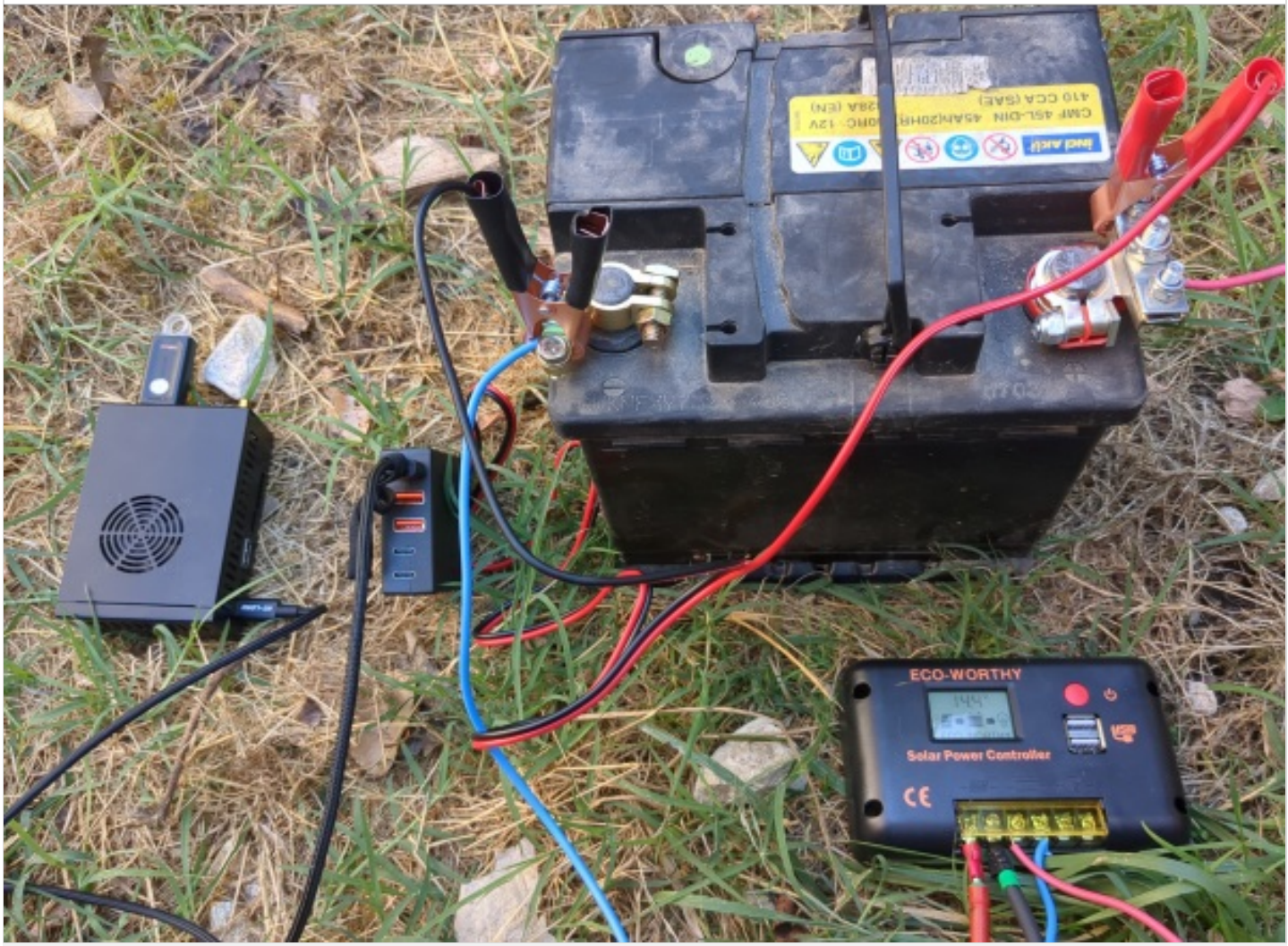
Serveur orangepi-raspberry nextcloud en photovoltaïque autonome

Aurelpere



https://wiki.lowtechlab.org/wiki/Serveur_orangepi-raspberry_nextcloud_en_photovolta%C3%AFque_autonome

Dernière modification le 10/04/2024

Difficulté **Moyen**

Durée **3 heure(s)**

Coût **165 EUR (€)**

Description

Tutoriel pour mettre en place un serveur nextcloud (équivalent drive google mais libre et adapté à l'organisation collective) sur un ordinateur monocarte autonome (alimenté en photovoltaïque avec stockage)

Ce tutoriel n'est pas tout à fait "lowtech" en première approche dans la mesure où il s'agit d'informatique et de photovoltaique.

Cependant, il se veut le plus didactique possible et rejoint la philosophie lowtech de partager les savoirs faires, éviter la tech inaccessible par la rétention d'information, la complexification by design ou la dépendance propriétaire by design.

On donne aussi un outil de dimensionnement photovoltaïque avec quelques explication. A vous de dimensionner pour une informatique lowtech, qui ne fonctionne que sur une plage horaire calé sur les rythmes du soleil, cad qui respecte les temporalités humaines.

Nextcloud (service accessible sur framasoft ici : https://www.frama.space/abc/fr/) est un service assez cool pour s'organiser à plusieurs et permet de partager des fichiers, avoir un annuaire, un chat, de travailler en cooperation sur des fichiers libreoffice voire même de faire des visios. On peut aussi imaginer des infokiosques mobiles sur ce principe.

Le tuto remet en question le marché des vpns, le photovoltaique avec stockage neuf et cher (en réalité le photovoltaique est devenu trop competitif face au pétrole et encore plus face au nucléaire!), et le marché des gafam et leur design de surveillance nocif pour la confiance et le lien social.

Les commandes sont celles pour un systeme debian

Enfin, le tuto est fait avec un modem 4G (et connexion filaire à un orange pi qui n'a pas de carte wifi par défaut), et mis a jour ce 10 avril pour raspberry pi connecté au "partage wifi" de votre téléphone. (voir etap 6 pour wifi en wpa3 et etap 16 pour wifi en wpa2)

Sommaire

Sommaire

Introduction

Tutoriel pour mettre en place un serveur nextcloud (équivalent drive google mais libre et adapté à l'organisation collective) sur un ordinateur monocarte autonome (alimenté en photovoltaïque avec stockage)

Ce tutoriel n'est pas tout à fait "lowtech" en première approche dans la mesure où il s'agit d'informatique et de photovoltaique.

Cependant, il se veut le plus didactique possible et rejoint la philosophie lowtech de partager les savoirs faires, éviter la tech inaccessible par la rétention d'information, la complexification by design ou la dépendance propriétaire by design.

On donne aussi un outil de dimensionnement photovoltaïque avec quelques explication. A vous de dimensionner pour une informatique lowtech, qui ne fonctionne que sur une plage horaire calé sur les rythmes du soleil, cad qui respecte les temporalités humaines.

Nextcloud (service accessible sur framasoft ici : https://www.frama.space/abc/fr/) est un service assez cool pour s'organiser à plusieurs et permet de partager des fichiers, avoir un annuaire, un chat, de travailler en cooperation sur des fichiers libreoffice voire même de faire des visios.
On peut aussi imaginer des infokiosques mobiles sur ce principe.

Le tuto remet en question le marché des vpns, le photovoltaique avec stockage neuf et cher (en réalité le photovoltaique est devenu trop competitif face au pétrole et encore plus face au nucléaire!), et le marché des gafam et leur design de surveillance nocif pour la confiance et le lien social.
Les commandes sont celles pour un systeme debian

Enfin, le tuto est fait avec un modem 4G (et connexion filaire à un orange pi qui n'a pas de carte wifi par défaut), et mis a jour ce 10 avril pour raspberry pi connecté au "partage wifi" de votre téléphone. (voir etap 6 pour wifi en wpa3 et etap 16 pour wifi en wpa2)

Matériaux

Outils

autonomie.ods

- Serveur_orangepi-raspberry_nextcloud_en_photovolta_que_autonome_autonomie_.ods

Étape 1 - Materiel

Les liens vers le materiel photovoltaïque utilisé sont dans le fichier autonomie.ods (lisible avec libreoffice) attaché à ce tutoriel.

- raspberry pi :
42€ sur leboncoin

-Orange pi :
Carte utilisée: Orange pi 5
ordinateur monocarte avec 4,8,16 ou 32 Go de ram
Un processeur à 2,4Ghz ARM Cortex-A55
Cette carte est compatible avec les disques nvme pcie 2.0 ssd 2242 ou 2230 (le pcie étant rétrocompatible cad que les 3.0, 4.0, 5.0 fonctionnent à vitesse réduite sur l'orange pi 5)
Meme principe qu'ici Ordinateur low-tech mais un peu plus puissant et on peut y brancher un disque dur (pratique pour nextcloud qui est fait pour héberger des fichiers) et ca démarre tout seul sur clé usb.
Prix: 143€ neuf sur aliexpress en version 16 Go au 2 août 2023
En occasion leboncoin, on trouve plus facilement des raspberry aux alentours de 100€.
Il est nécessaire d'acheter une petit boitier à 10€ (ou en fabriquer un) en plus pour éviter que la carte soit à nue

-Stockage/disque dur:
Ici on utilise une clé usb Kingston 32Go et une carte nvme samsung de 512Go.
On peut brancher une disque dur de plus grande capacité soit en usb, soit une carte nvme (nvme pcie 2.0 ssd 2242 ou 2230. compatible avec les pcie 3.0 4.0 et superieur mais la vitesse est réduite).
Une carte nvme samsung 2242 de 500Go coute 50€ environ au 2 août 2023.

-clé usb : 10€

-cable rj45: 5€

-Box internet ou modem 4G selon votre connection internet.

-Panneau solaire: Ici on utilise un panneau flexible de 120W acheté 115€ neuf mais on en trouve à 30€ d'occasion sur leboncoin équivalent en puissance.
Note: Pour le besoin théorique. Voir fichier autonomie.ods

-batterie de voiture usée: utiliser sa précédente batterie de voiture plomb acide lorsqu'elle commence à lacher quand il fait trop chaud!

-convertisseur batterie 12/24V-usb 5V: 20€ evitez amazon si vous le pouvez)

- regulateur pwm 30A: 30€ neuf si on ne prend pas de la marque
- DRL (interupteur jour/nuit 13V): 1,5€ neuf
(mot clé "Kit de feux de jour à LED pour voiture, contrôleur marche/arrêt automatique DRL")

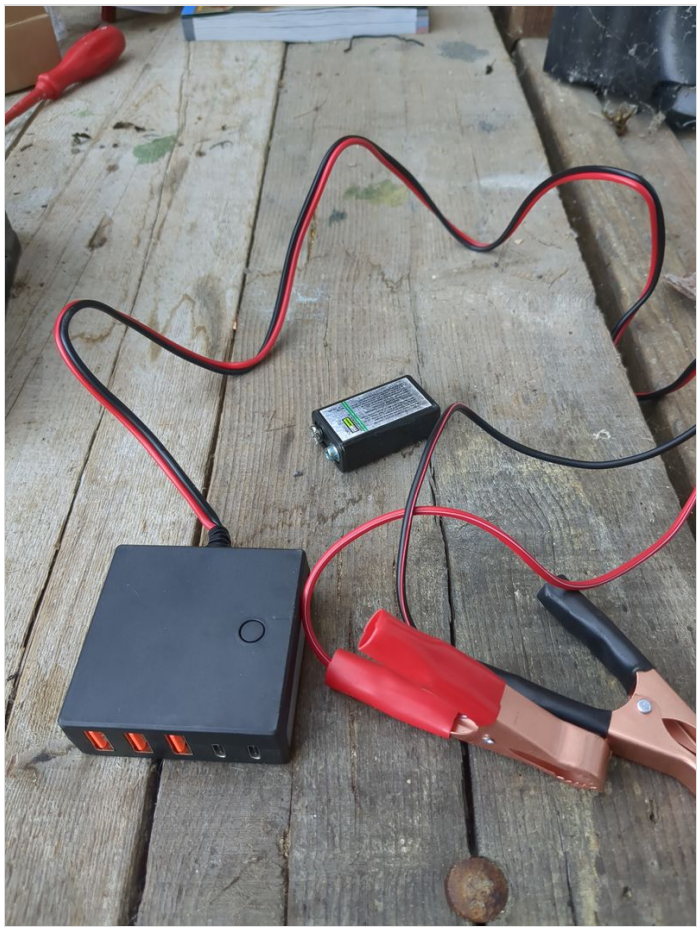
-cable electrique mc4: 20€
Total prix d'occasion orangepi: 256,50€
Total prix neuf orangepi: 431,50€

Total prix d'occasion raspberry: 165€

Voir fichier autonomie.ods

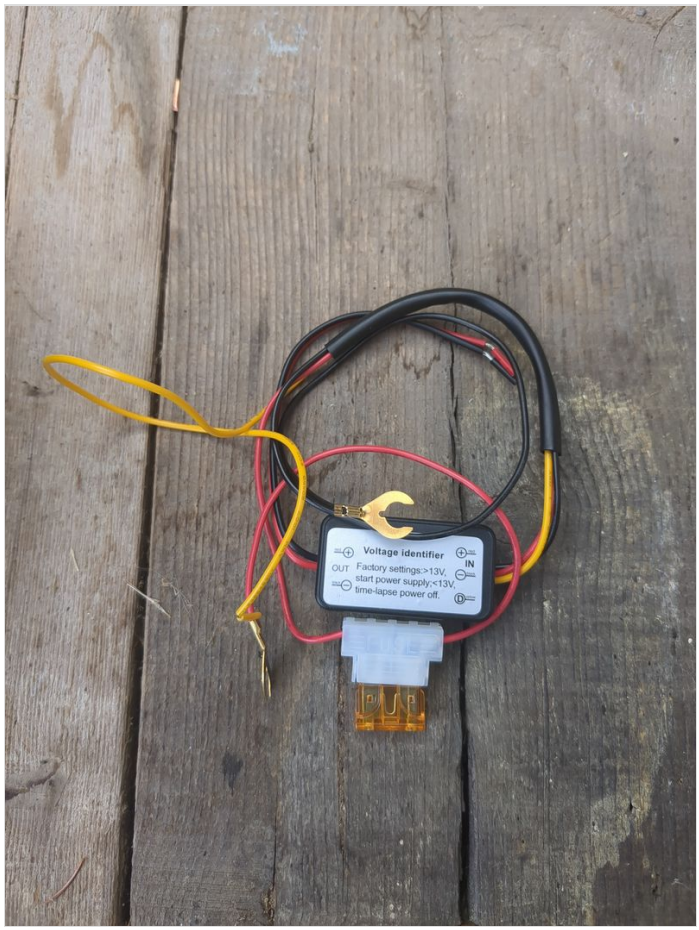
-


Energizer




İNCİ AKÜ
CMF 45L-DIN 45Ah(20HR) 80RC 12V
410 CCA (SAE) 328A (EN)


ECO-WORTHY
12.7V
ECO-WORTHY
Solar Power Controller
USB
CE


Voltage identifier
IN
OUT Factory settings:>13V,
start power supply:<13V,
time-lapse power off.

Étape 2 - Installation de nextcloud 1/4

1.Téléchargement de dietpi et préparation de la clé usb

Pour l'installation, je vous conseille d'utiliser dietpi. L'interet de dietpi est notamment la legereté du systeme pour des ordinateurs monocartes, mais aussi l'installation automatique de logiciels libres par un menu relativement "user friendly". On peut mentionner parmis tous les logiciels installables automatiquement au démarrage du systeme (https://dietpi.com/dietpi-software.html) des applis de domotique, interessante pour économiser de l'énergie en fonction de la meteo, mais aussi les relais "tor" pour contribuer au réseau relativement anonymisant tor, interessant pour les "éco terroristes" que nous sommes.
Il faut aussi mentionner "younohost" (https://yunohost.org/fr) qui est français et qui fait le même boulot que dietpi pour les raspberry et qui est aussi "user friendly" sinon plus. Je n'ai pas encore testé yunohost car j'avais mis de côté le raspberry pi suite à des bugs de souris trop étranges. Mes recherches pour éviter les bugs de souris trop étranges n'ayant pas abouti positivement (purism, odroid, raspberry, orangpi, macbook, windows, voir section sécurité), je ne peux que faire état de ce que j'ai effectivement essayé.

https://dietpi.com/#download
(pour younohost : https://yunohost.org/fr/install/hardware:arm)

Selectionner votre ordinateur monocarte (orange pi dans le cas présent) puis telecharger

Dezipper l'archive obtenue.

Utiliser ensuite balena etcher pour créer une clé usb bootable pour installer dietpi sur votre ordinateur monocarte (orange pi 5 dans le cas présent mais ca fonctionne pareil sur d'autres ordinateurs monocartes).

https://etcher.balena.io/#download-etcher

Double cliquer sur le fichier téléchargé

Selectionner l'image de dietpi téléchargée, selectionner votre clé usb, cliquer sur flash.

Il ne vous reste plus qu'à brancher la clé usb sur le orangepi et il bootera automatiquement sur la clé usb.

Pour un raspberry pi, on utilise une carte sd mais on peut configurer le boot usb également (voir ici : https://makerhelp.fr/booter-un-raspberry-pi-4-sur-un-disque-dur-ou-un-ssd-en-usb/).

2. Installation de nextcloud

Allumer votre orangepi/raspberrypi avec la clé usb branchée.

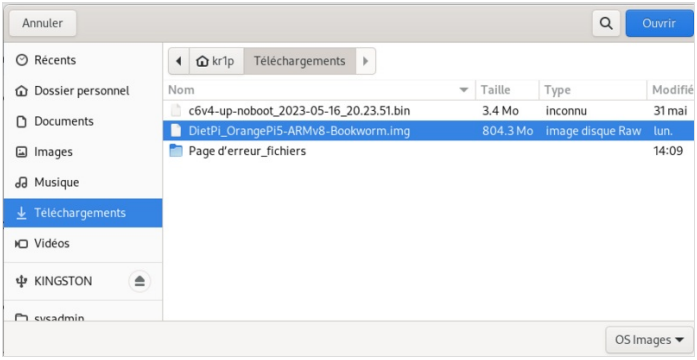
Le login par défaut au démarrage est root et le mot de passe dietpi.

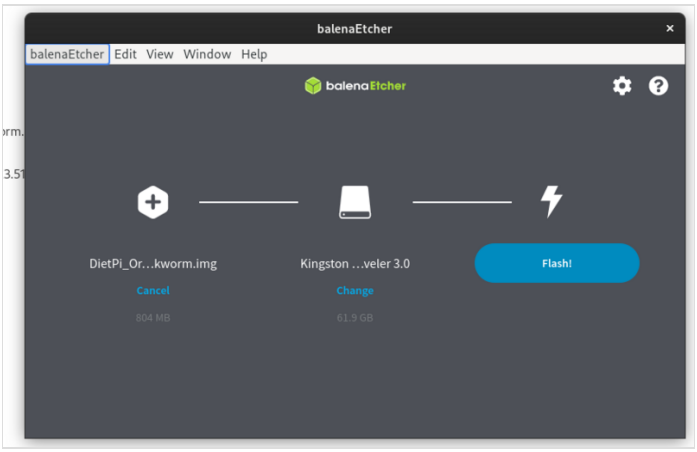
Suivre les menus que vous propose dietpi au premier démarrage pour installer le service nextcloud. C'es très facile, c'est en anglais et tout est automatisé. J'ai mis les images des menus à sélectionner pour l'installation de nextcloud dans cette etape et les étapes 3 à 6.

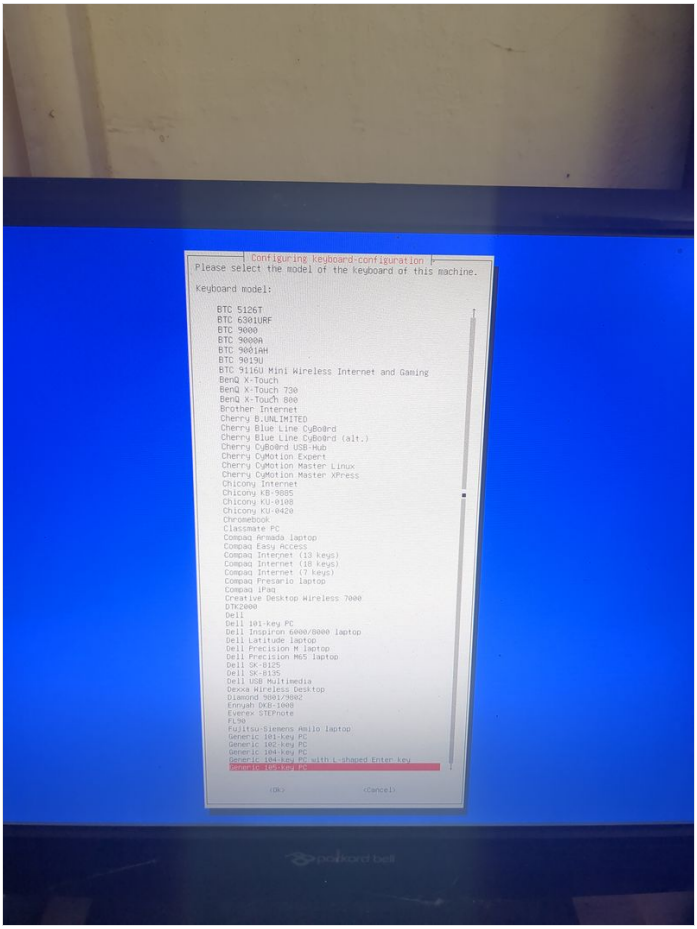
Vous pouvez vous déplacer dans les menus au clavier avec les fleches et la touche tab.

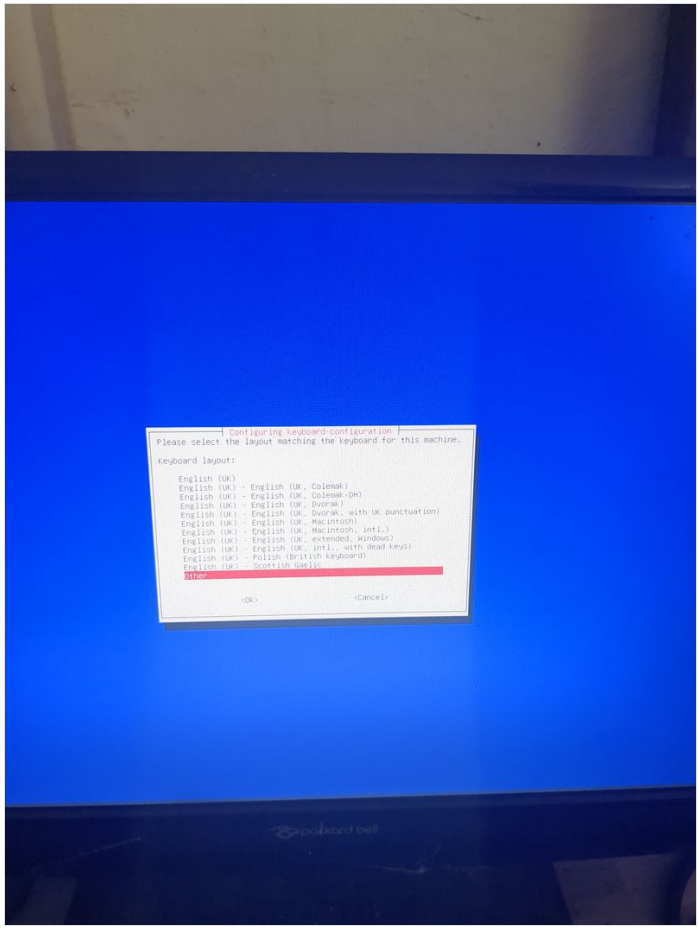
Selectionner avec espace et valider avec entree.

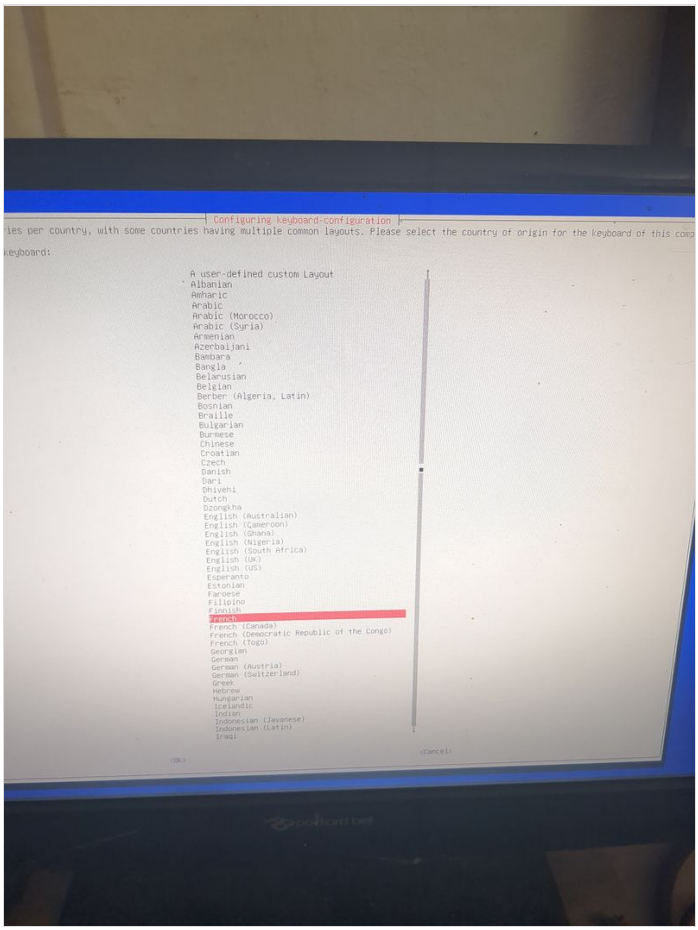
Voir images des étapes 3 à 6 pour le déroulement de l'installation et les entrées à sélectionner.

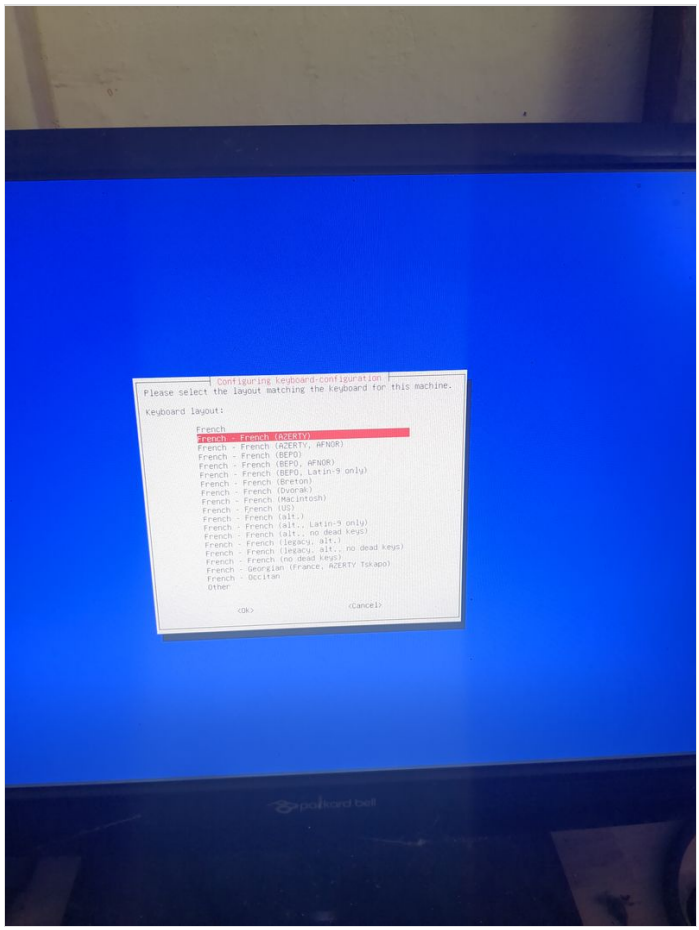



balenaEtcher
balenaEtcher Edit View Window Help
balenaEtcher
DietPi_Or...kworm.img
Cancel
804 MB
Kingston ...veler 3.0
Change
61.9 GB
Flash!


Configuring keyboard-configuration
Please select the model of the keyboard of this machine.
Keyboard model:
BTC 5126T
BTC 6301URF
BTC 9000
BTC 9000A
BTC 9001AH
BTC 9019U
BTC 9116U Mini Wireless Internet and Gaming
BenQ X-Touch
BenQ X-Touch 730
BenQ X-Touch 800
Brother Internet
Cherry B.UNLIMITED
Cherry Blue Line CyBo@rd
Cherry Blue Line CyBo@rd (alt.)
Cherry CyBo@rd USB-Hub
Cherry CyMotion Expert
Cherry CyMotion Master Linux
Cherry CyMotion Master Xpress
Chicony Internet
Chicony KB-9885
Chicony KU-0108
Chicony KU-0420
Chromebook
Classmate PC
Compaq Armada laptop
Compaq Easy Access
Compaq Internet (13 keys)
Compaq Internet (18 keys)
Compaq Internet (7 keys)
Compaq Presario laptop
Compaq iPaq
Creative Desktop Wireless 7000
DTK2000
Dell
Dell 101-key PC
Dell Inspiron 6400/8000 laptop
Dell Latitude laptop
Dell Precision M laptop
Dell Precision M65 laptop
Dell SK-8125
Dell SK-8135
Dell USB Multimedia
Dexxa Wireless Desktop
Diamond 9801/9802
Ennyah DKB-1008
Everex STEPnote
FL90
Fujitsu-Siemens Amilo laptop
Generic 101-key PC
Generic 102-key PC
Generic 104-key PC
Generic 105-key PC with L-shaped Enter key
Generic 105-key PC
<Ok>
<Cancel>

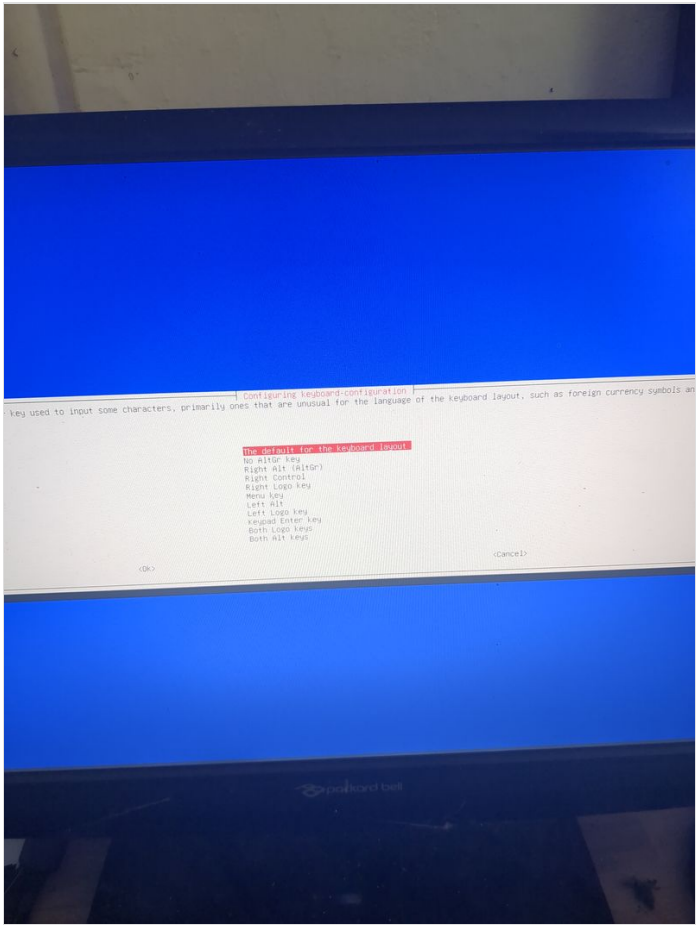

Configuring keyboard-configuration
Please select the layout matching the keyboard for this machine.
Keyboard layout:
English (UK)
English (UK) - English (UK, Colemak)
English (UK) - English (UK, Colemak-DH)
English (UK) - English (UK, Dvorak)
English (UK) - English (UK, Dvorak, with UK punctuation)
English (UK) - English (UK, Macintosh)
English (UK) - English (UK, Macintosh, intl.)
English (UK) - English (UK, extended, Windows)
English (UK) - English (UK, intl., with dead keys)
English (UK) - Polish (British keyboard)
English (UK) - Scottish Gaelic
Other
<Ok>
<Cancel>

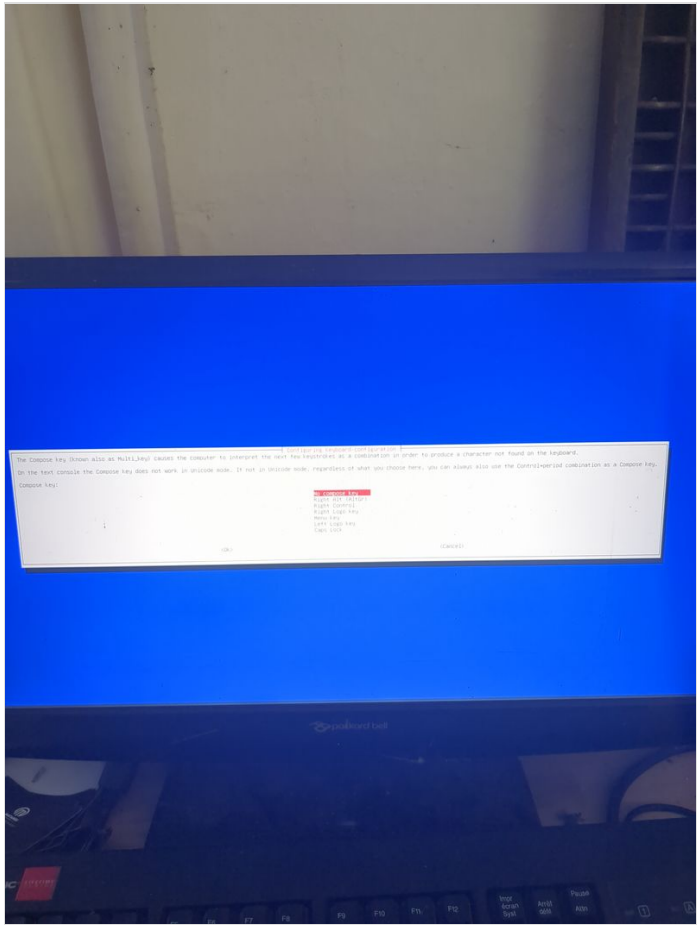


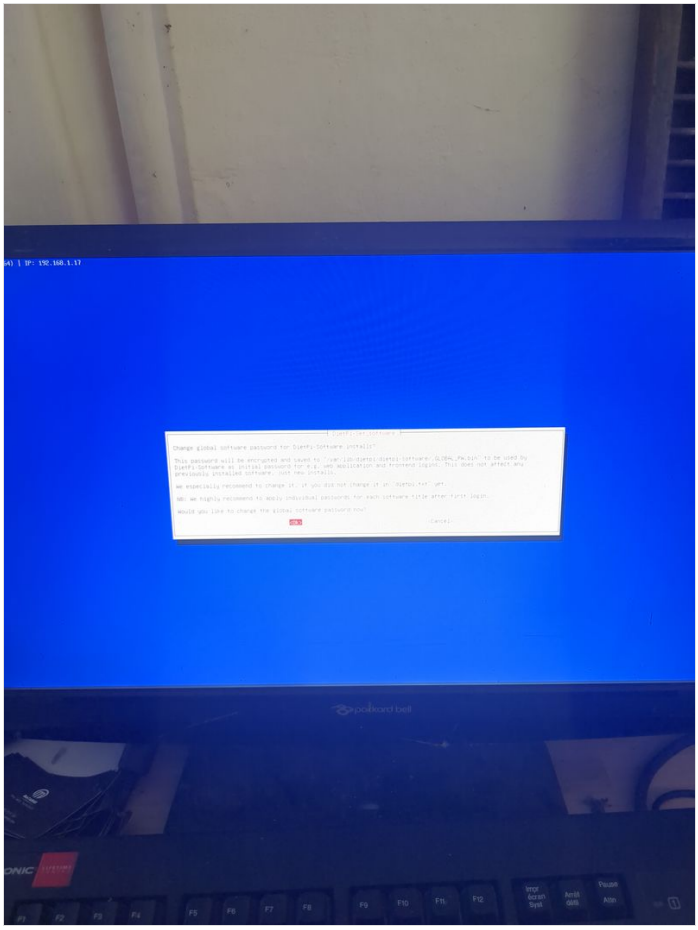


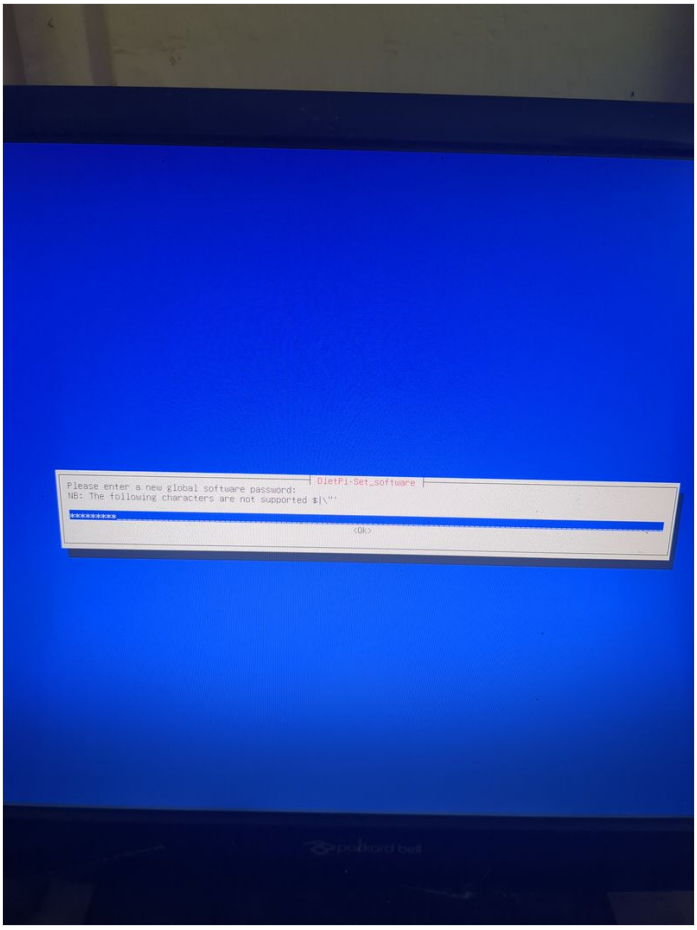
Étape 3 - Installation de nextcloud 2/4

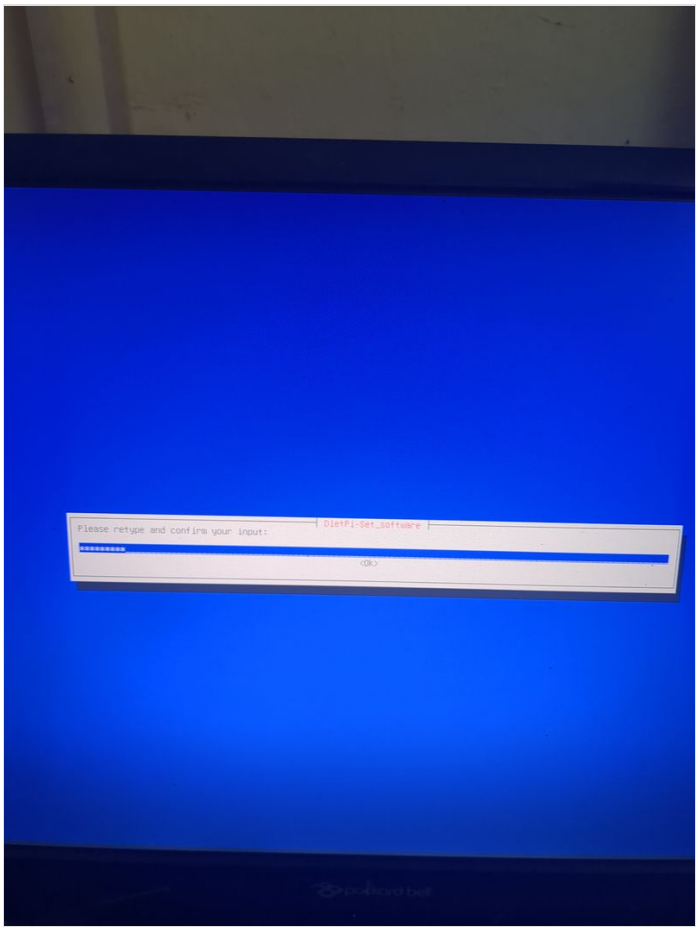
Voir images

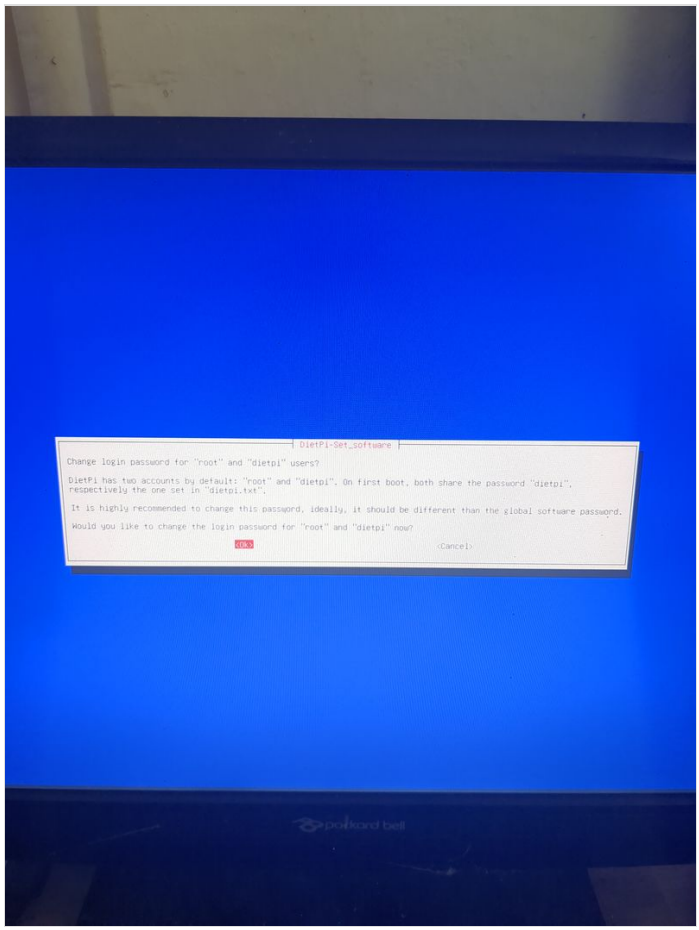

Configuring keyboard-configuration
key used to input some characters, primarily ones that are unusual for the language of the keyboard layout, such as foreign currency symbols an
The default for the keyboard layout
No AltGr key
Right Alt (AltGr)
Right Control
Right Logo key
Menu key
Left Alt
Left Logo key
Keypad Enter key
Both Logo keys
Both Alt keys
<Ok>
<Cancel>


The Compose key (known also as Multi_key) causes the computer to interpret the next few keystrokes as a combination in order to produce a character not found on the keyboard.
On the text console the Compose key does not work in Unicode mode. Regardless of what you choose here, you can always also use the Control+period combination as a Compose key.
Compose key:
No compose key
Right Alt (AltGr)
Right Control
Right Logo key
Menu key
Left Logo key
Caps Lock
<Ok>
<Cancel>


IP: 192.168.1.17

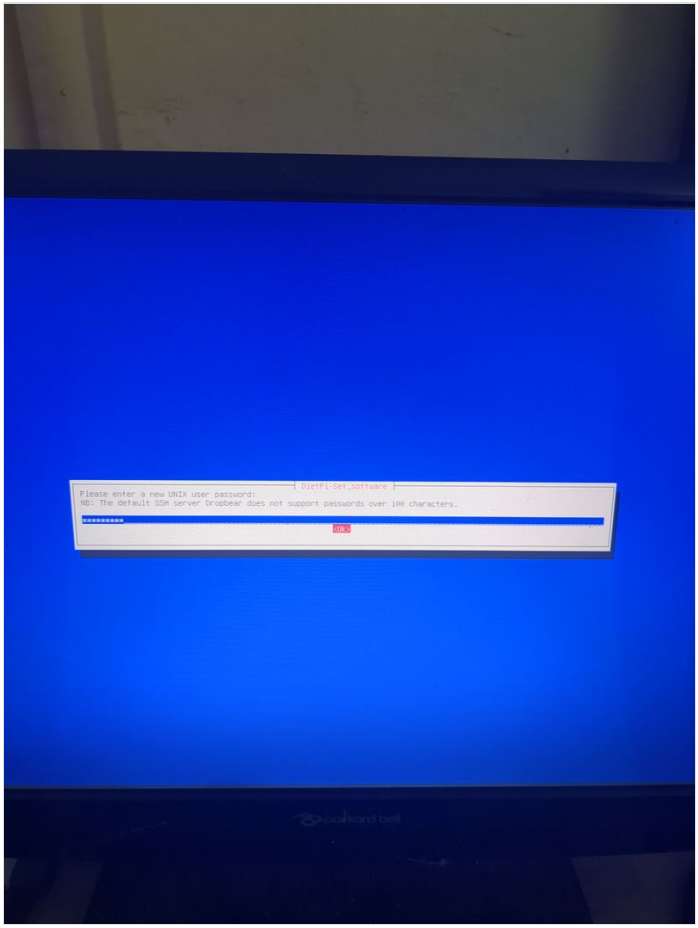

DietPi-Set_software
Please enter a new global software password:
NB: The following characters are not supported $|\'"
<Ok>

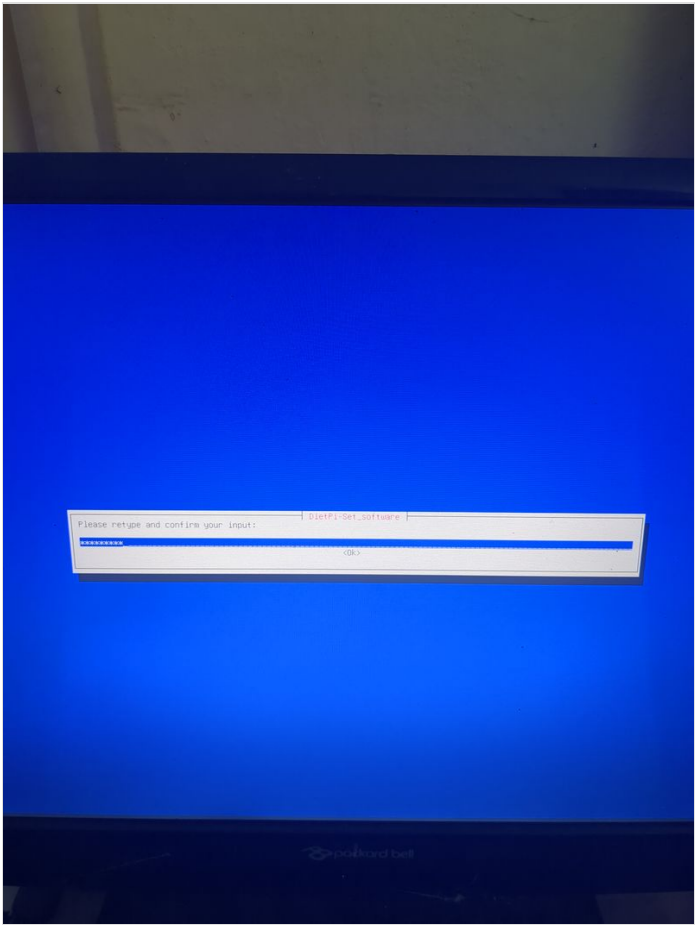


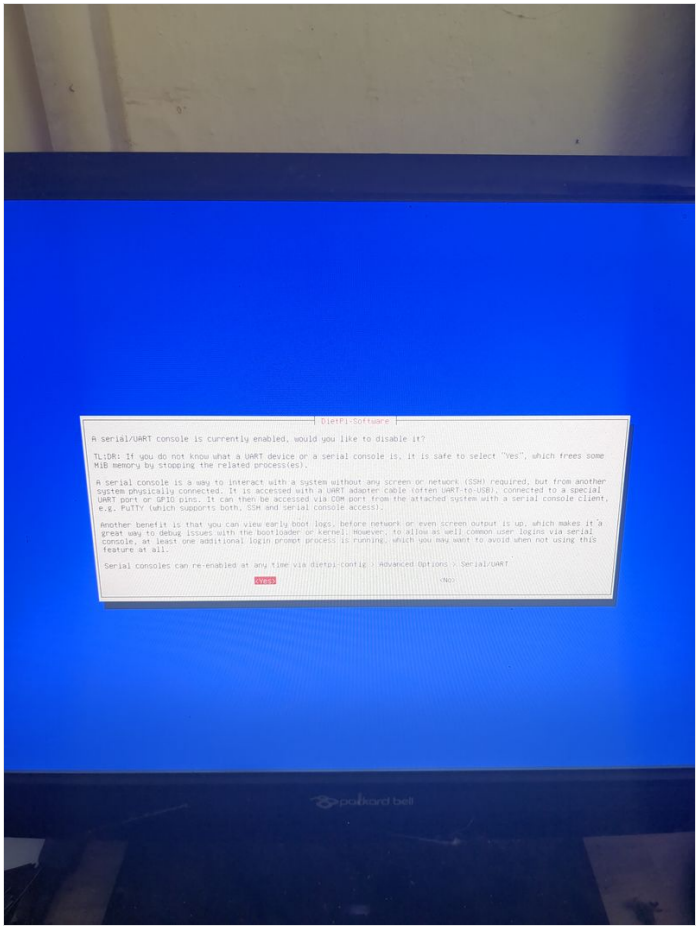


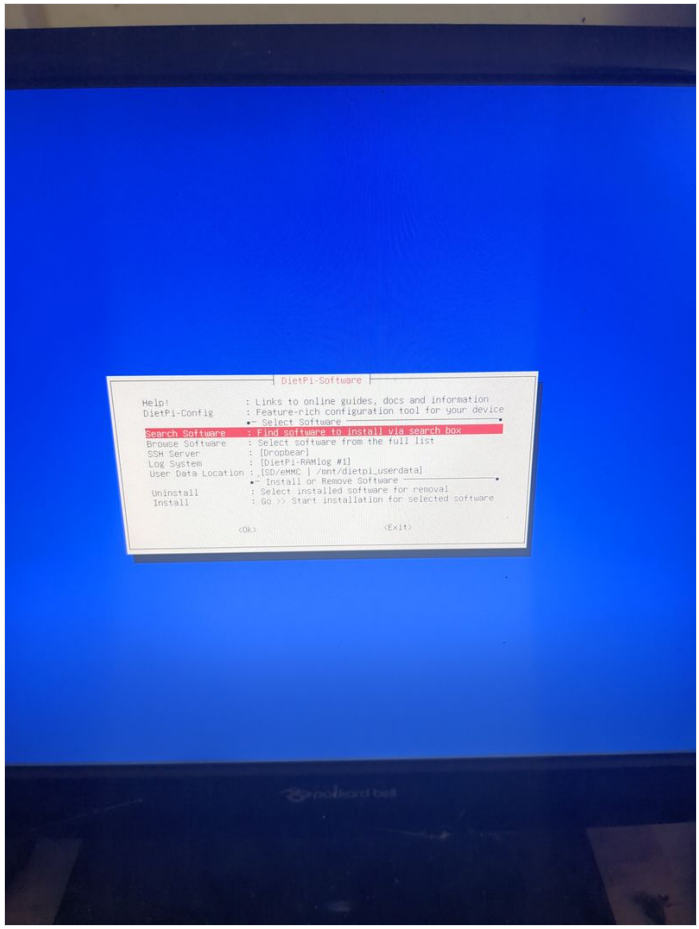
Étape 4 - Installation de nextcloud 3/4

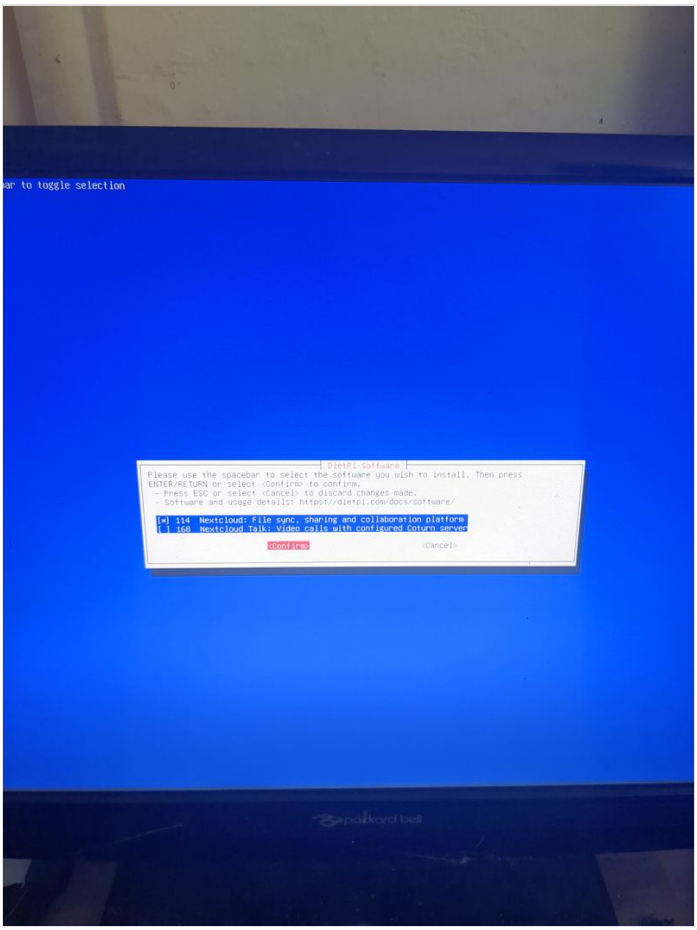
Voir images


DietPi-Set_software
Please enter a new UNIX user password:
NB: The default SSH server Dropbear does not support passwords over 100 characters.
<OK>


DietPi-Set_software
Please retype and confirm your input:
<OK>

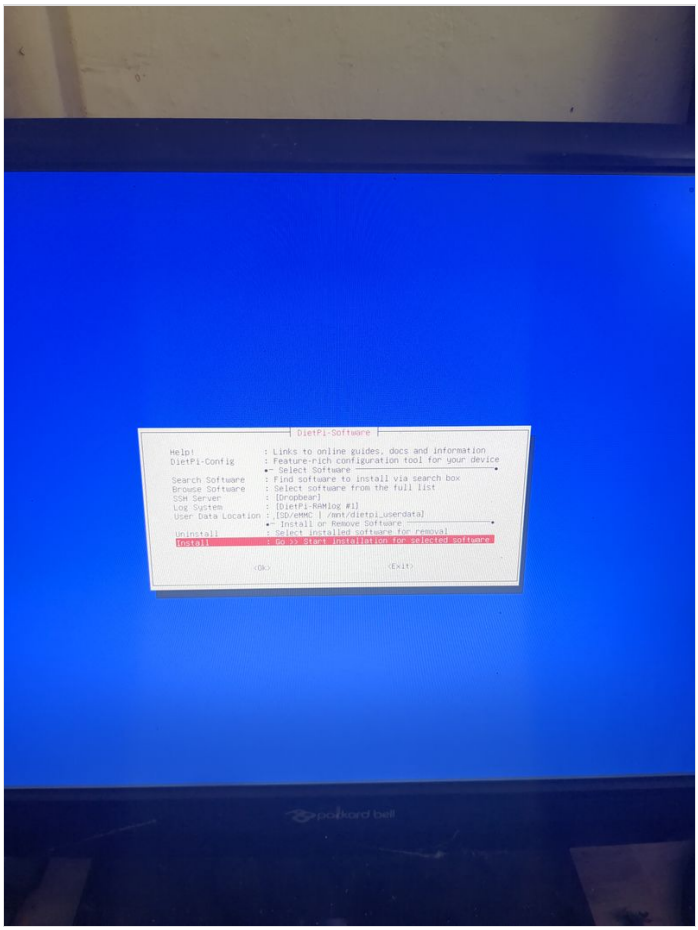

DietPi-Software
A serial/UART console is currently enabled, would you like to disable it?
TL;DR: If you do not know what a UART device or a serial console is, it is safe to select "Yes", which frees some MiB memory by stopping the related process(es).
A serial console is a way to interact with a system without any screen or network (SSH) required, but from another system physically connected. It is accessed with a UART adapter cable (often UART-to-USB), connected to a special UART port or GPIO pins. It can then be accessed via COM port from the attached system with a serial console client, e.g. PuTTY (which supports both, SSH and serial console access).
Another benefit is that you can view early boot logs, before network or even screen output is up, which makes it a great way to debug issues with the bootloader or kernel. However, to allow as well common user logins via serial console, at least one additional login prompt process is running, which you may want to avoid when not using this feature at all.
Serial consoles can re-enabled at any time via dietpi-config >> Advanced Options > Serial/UART
<Yes>
<No>

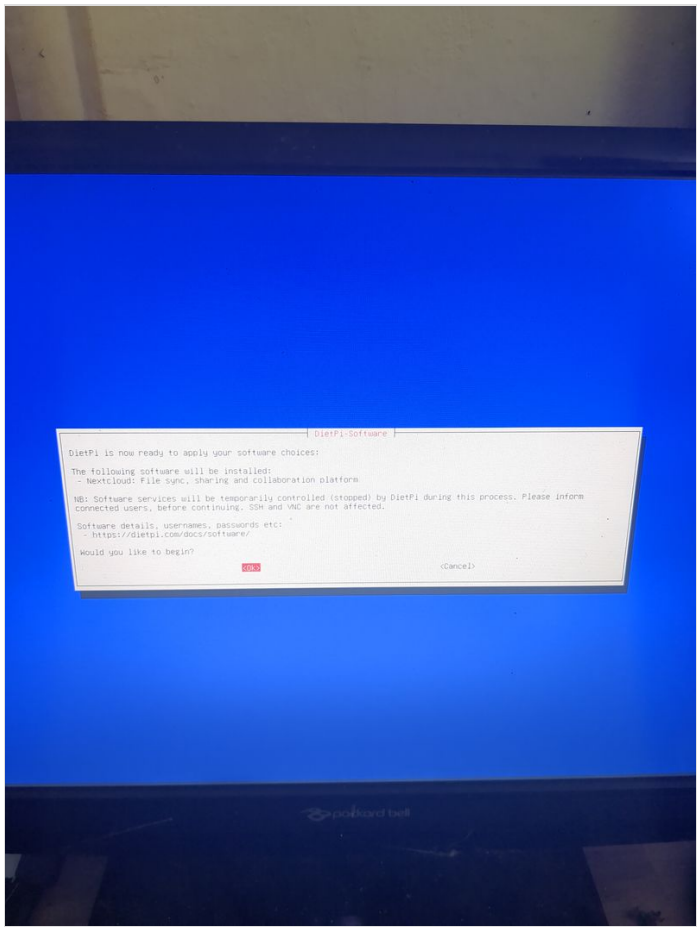

DietPi-Software
Help! : Links to online guides, docs and information
DietPi-Config : Feature-rich configuration tool for your device
Select Software
Search Software : Find software to install via search box
Browse Software : Select software from the full list
SSH Server : [Dropbear]
Log System : [DietPi-RAMlog #1]
User Data Location : [SD/eMMC | /mnt/dietpi_userdata]
Install or Remove Software
Uninstall : Select installed software for removal
Install : Go >> Start installation for selected software
<Ok>
<Exit>

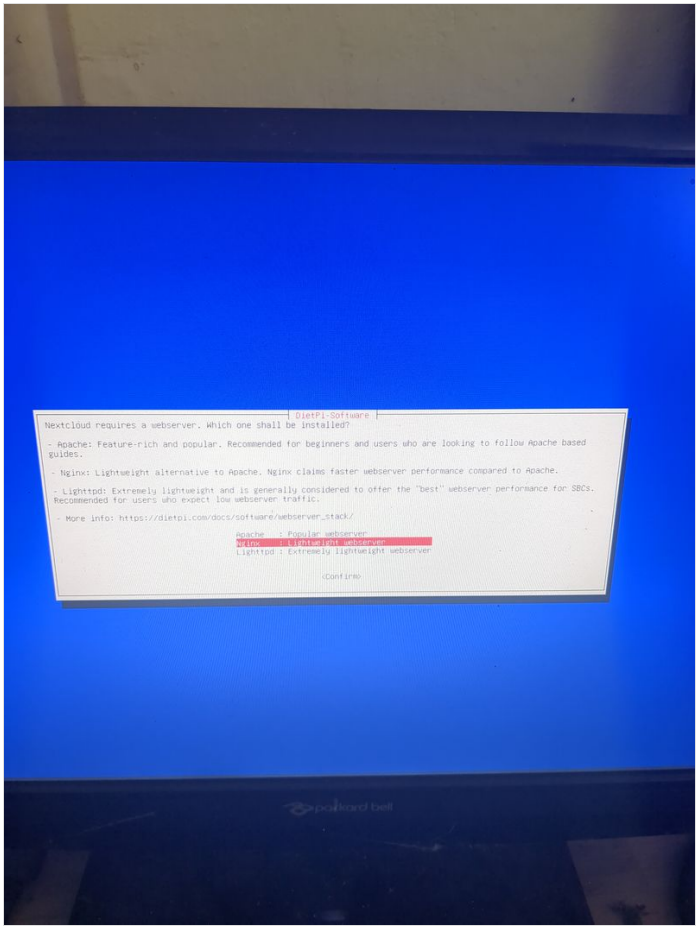


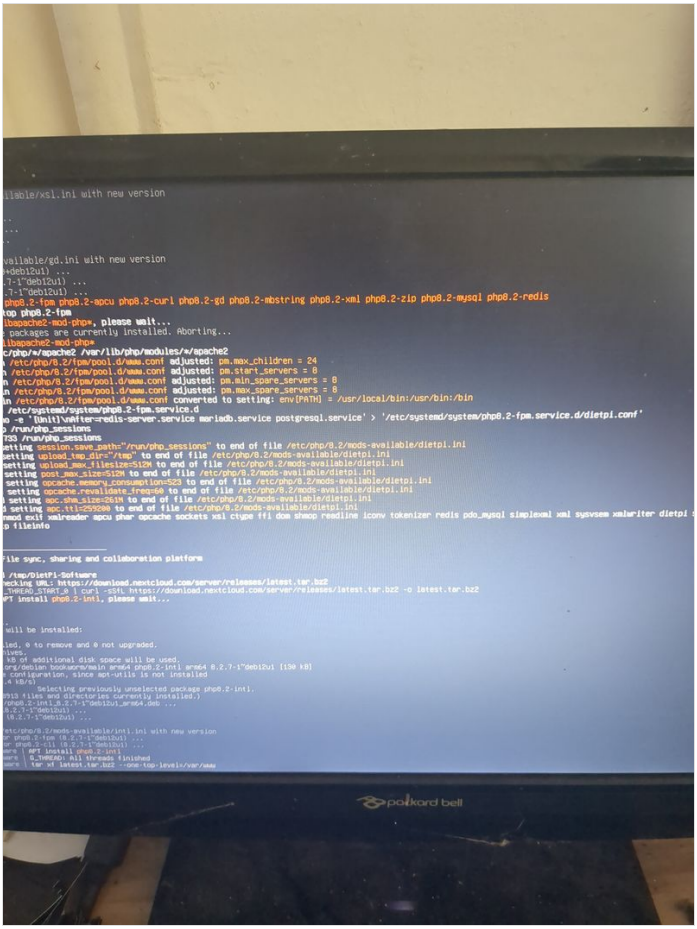
Étape 5 - Installation de nextcloud 4/4

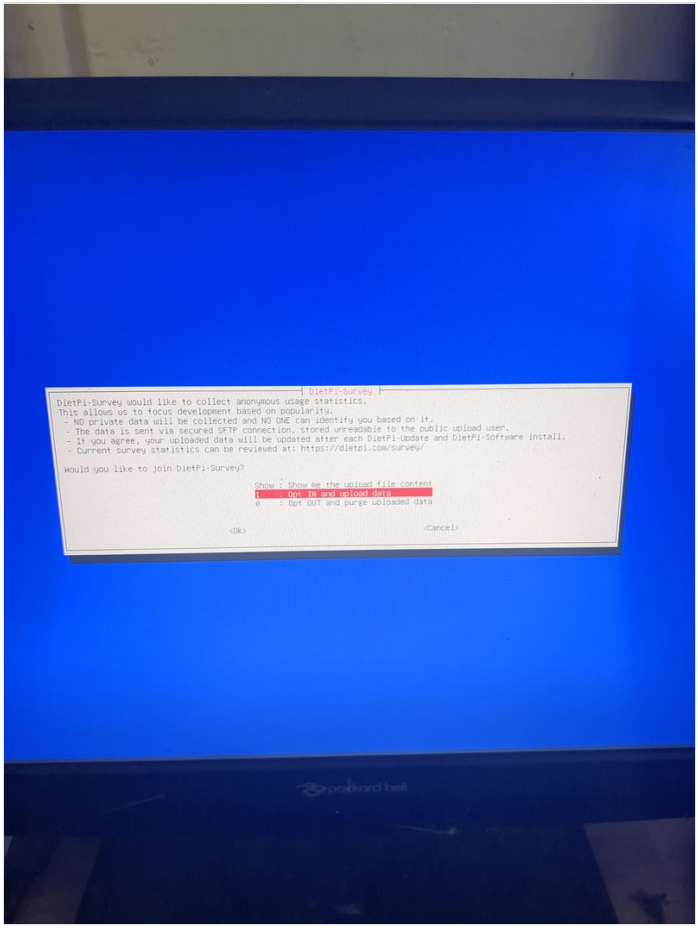
Voir images


DietPi-Software
Help! : Links to online guides, docs and information
DietPi-Config : Feature-rich configuration tool for your device
Select Software
Search Software : Find software to install via search box
Browse Software : Select software from the full list
SSH Server : [Dropbear]
Log System : [DietPi-RAMlog #1]
User Data Location : [SD/eMMC | /mnt/dietpi_userdata]
Install or Remove Software
Uninstall : Select installed software for removal
Install : Go to Start installation for selected software
<Ok>
<Exit>

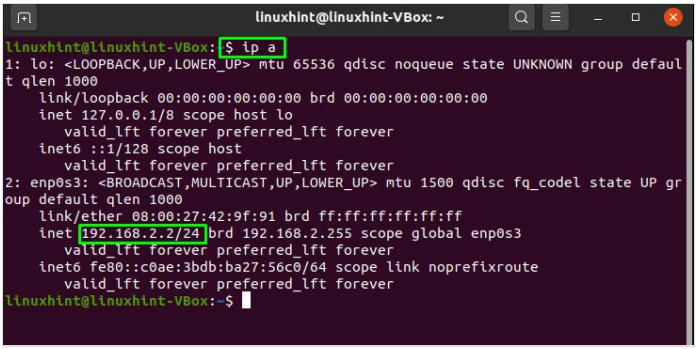

DietPi-Software
DietPi is now ready to apply your software choices:
The following software will be installed:
- Nextcloud: File sync, sharing and collaboration platform
NB: Software services will be temporarily controlled (stopped) by DietPi during this process. Please inform connected users, before continuing. SSH and VNC are not affected.
Software details, usernames, passwords etc:
- https://dietpi.com/docs/software/
Would you like to begin?
<Ok>
<Cancel>


DietPi-Software
Nextcloud requires a webserver. Which one shall be installed?
- Apache: Feature-rich and popular. Recommended for beginners and users who are looking to follow Apache based guides.
- Nginx: Lightweight alternative to Apache. Nginx claims faster webserver performance compared to Apache.
- Lighttpd: Extremely lightweight and is generally considered to offer the "best" webserver performance for SBCs. Recommended for users who expect low webserver traffic.
- More info: https://dietpi.com/docs/software/webserver_stack/
Apache : Popular webserver
Nginx : Lightweight webserver
Lighttpd : Extremely lightweight webserver
<Confirm>
packard bell


liable/xsl.ini with new version
valiable/gd.ini with new version
php8.2-fpm php8.2-apcu php8.2-curl php8.2-gd php8.2-mbstring php8.2-xml php8.2-zip php8.2-mysql php8.2-redis
packages are currently installed. Aborting...
/etc/php/8.2/fpm/pool.d/www.conf adjusted: pm.max_children = 24
/etc/php/8.2/fpm/pool.d/www.conf adjusted: pm.start_servers = 8
/etc/php/8.2/fpm/pool.d/www.conf adjusted: pm.min_spare_servers = 8
/etc/php/8.2/fpm/pool.d/www.conf adjusted: pm.max_spare_servers = 8
/etc/php/8.2/fpm/pool.d/www.conf converted to setting: env[PATH] = /usr/local/bin:/usr/bin:/bin
/etc/systemd/system/php8.2-fpm.service.d
/run/php_sessions
/run/php_sessions
setting session.save_path="/run/php_sessions" to end of file /etc/php/8.2/mods-available/dietpi.ini
setting upload_tmp_dir="/tmp" to end of file /etc/php/8.2/mods-available/dietpi.ini
setting upload_max_filesize=512M to end of file /etc/php/8.2/mods-available/dietpi.ini
setting post_max_size=512M to end of file /etc/php/8.2/mods-available/dietpi.ini
setting opcache.memory_consumption=512 to end of file /etc/php/8.2/mods-available/dietpi.ini
setting opcache.revalidate_freq=60 to end of file /etc/php/8.2/mods-available/dietpi.ini
setting apc.shm_size=256M to end of file /etc/php/8.2/mods-available/dietpi.ini
setting apc.ttl=259200 to end of file /etc/php/8.2/mods-available/dietpi.ini
mod exif xmlreader apcu phar opcache sockets xsl ctype ffi dom shmop readline iconv tokenizer redis pdo_mysql simplexml xml sysvsem xmlwriter dietpi
p fileinfo
File sync, sharing and collaboration platform
/tmp/DietPi-Software
cking URL: https://download.nextcloud.com/server/releases/latest.tar.bz2
_THREAD_START_0 | curl -sSfL https://download.nextcloud.com/server/releases/latest.tar.bz2 -o latest.tar.bz2
PT install php8.2-intl, please wait...
will be installed:
ded, 0 to remove and 0 not upgraded.
tives.
kB of additional disk space will be used.
org/debian bookworm/main arm64 php8.2-intl arm64 8.2.7-1~deb12u1 [130 kB]
configuration, since apt-utils is not installed
.4 kB/s)
Selecting previously unselected package php8.2-intl.
913 files and directories currently installed.)
/php8.2-intl_8.2.7-1~deb12u1_arm64.deb ...
.2.7-1~deb12u1) ...
(8.2.7-1~deb12u1) ...
/etc/php/8.2/mods-available/intl.ini with new version
php8.2-fpm (8.2.7-1~deb12u1) ...
php8.2-intl (8.2.7-1~deb12u1) ...
APT installation of php8.2-intl
1_THREAD_0 | All threads finished
tar xf latest.tar.bz2 --one-top-level=/var/www
packard bell



Étape 6 - configuration du reseau local ethernet ou wifi



Si vous n'avez pas de box et que vous avez un orangepi ou un raspberrypi et que vous voulez vous connecter à un wifi (par exemple le wifi d'un smartphone en partage de connexion)
Dietpi fournit un utilitaire pour configurer automatiquement le wifi qui fonctionne sur raspberry. Chez moi ca ne fonctionne que si le réseau est en wpa2. Si vous voulez activer le WPA3 ou si vous voulez configurer votre wifi à la main, voici les étapes à suivre.

Linux est un peu compliqué pour la gestion des réseaux. Il existe une multitude de programmes permettant de gérer les réseaux (networking, network interfaces, ifup, wpa_supplicant, network_manager, ifconfig, ip...).
Si vous vous y connaissez je vous laisse choisir ce qui vous convient le mieux.
Sinon, on utilisera les programmes installés par défaut dans dietpi pour la gestion des interfaces wifi : wpa_supplicant et dhclient.
Commencer par brancher un adaptateur usb wifi à votre orangepi ou verifier que votre adaptateur wifi sur votre raspberry pi est bien détecté.
Sur un orangepi: verifier que l'adaptateur est bien détecté en tapant

```
lsusb
```

Cette commande va lister les périphériques usb et vous devriez voir votre clé usb wifi dans la liste. Verifier ensuite que les drivers de votre clé ont bien été chargés en tapant:

```
dmesg | grep usb
```

ou pour lire tous les pilotes chargés par linux en tapant

```
dmesg | less
```

Vous pouvez trouver à cette adresse une liste d'adaptateur usb qui fonctionnent nativement sous linux : https://github.com/morrownr/USB-WiFi/blob/main/home/USB_WiFi_Adapters_that_are_supported_with_Linux_in-kernel_drivers.md
Sur un orange pi ou raspberry pi : taper la commande

```
ip a
```

Vous devriez voir votre adaptateur wifi sous le nom d'interface wlan0. On supposera dans la suite du tuto que le nom de l'interface est wlan0. Si ce n'est pas le cas, remplacer wlan0 par le nom de votre interface.
Nou allons vérifier que votre interface est bien déclarée. Ouvrir le fichier /etc/network/interfaces en tapant:

```
nano /etc/network/interfaces
```

Vous devez avoir les lignes suivantes. Si elles n'y sont pas ajouter les.

```
auto wlan0
iface wlan0 inet dhcp
  wpa-conf /etc/wpa_supplicant/wpa_supplicant.conf
```

Nous allons maintenant configurer wpa_supplicant pour activer la connection wifi.
Pour cela, editer le fichier /etc/wpa_supplicant/wpa_supplicant.conf en tapant les commandes suivantes: (remplacer votre.ssid par le nom que vous donnez à votre reseau wifi et votre.password par votre mot de passe)

```
echo "ctrl_interface=/run/wpa_supplicant" | sudo tee /etc/wpa_supplicant/wpa_supplicant.conf
echo "ap_scan=1" | sudo tee -a /etc/wpa_supplicant/wpa_supplicant.conf
echo "update_config=1" | sudo tee -a /etc/wpa_supplicant/wpa_supplicant.conf
echo "network={" | sudo tee -a /etc/wpa_supplicant/wpa_supplicant.conf
echo 'ssid="votre.ssid"' | sudo tee -a /etc/wpa_supplicant/wpa_supplicant.conf
echo "scan_ssid=1" | sudo tee -a /etc/wpa_supplicant/wpa_supplicant.conf
echo "proto=WPA RSN" | sudo tee -a /etc/wpa_supplicant/wpa_supplicant.conf
```

Maintenant, la configuration differe si votre wifi est un wifi WPA2 ou WPA3.
Si cest un wpa2, ajouter:

```
echo "key_mgmt=WPA-PSK | sudo tee -a /etc/wpa_supplicant/wpa_supplicant.conf
echo 'psk="votre.password"' | sudo tee -a /etc/wpa_supplicant/wpa_supplicant.conf
echo "}" | sudo tee -a /etc/wpa_supplicant/wpa_supplicant.conf
```

Si cest un wpa3, ajouter:

```
echo "key_mgmt=SAE | sudo tee -a /etc/wpa_supplicant/wpa_supplicant.conf
echo 'sae_password="votre.password"' | sudo tee -a /etc/wpa_supplicant/wpa_supplicant.conf
echo "ieee80211w=2" | sudo tee -a /etc/wpa_supplicant/wpa_supplicant.conf
echo "}" | sudo tee -a /etc/wpa_supplicant/wpa_supplicant.conf
```

Lancer maintenant wpa_supplicant avec les commandes:

```
export PATH="/usr/sbin:$PATH"
sudo wpa_supplicant -B -i wlan0 -c /etc/wpa_supplicant/wpa_supplicant.conf
```

Lancer ensuite dhclient pour obtenir une ip sur votre reseau:

```
sudo dhclient wlan0
```

Verifier que vous etes connecté:

```
curl google.com
```

Voilà vous êtes connecté.
Si ca ne fonctionne pas bien chez vous, je vous conseille les liens suivants pour débugguer ou comprendre mieux à quoi servent ces commandes: https://wiki.archlinux.org/title/Wpa_supplicant https://doc.ubuntu-fr.org/wifi_ligne_de_commande https://www.linuxbabe.com/command-line/ubuntu-server-16-04-wifi-wpa-supplicant

Pour automatiser la connection au démarrage de l'ordinateur:

```
sudo cp /lib/systemd/system/wpa_supplicant.service /etc/systemd/system/wpa_supplicant.service
sudo nano /etc/systemd/system/wpa_supplicant.service
```

Votre fichier doit ressembler à cela:

```
[Unit]
Description=WPA Supplicant
Before=network.target
After=dbus.service
Wants=network.target
IgnoreOnIsolate=true

[Service]
Type=dbus
BusName=fi.w1.wpa_supplicant1
ExecStart=/sbin/wpa_supplicant -u -s -c /etc/wpa_supplicant/wpa_suppl
icant.conf -i wlan0
Group=netdev
RuntimeDirectory=wpa_supplicant
RuntimeDirectoryMode=0750
Restart=always

[Install]
WantedBy=multi-user.target
```

Lancer ensuite la commande pour automatiser le demarrage du service au boot:

```
sudo systemctl enable wpa_supplicant.service
```

Editer ensuite le service dhclient pour automatiser son demarrage:

```
sudo nano /etc/systemd/system/dhclient.service
```

Ajouter le texte suivant :

```
[Unit]
Description= DHCP Client
Before=network.target

[Service]
Type=forking
ExecStart=/sbin/dhclient wlan0 -v
ExecStop=/sbin/dhclient wlan0 -r
Restart=always

[Install]
WantedBy=multi-user.target
```

puis lancer la commande:

```
sudo systemctl enable dhclient.service
```

Si vous avez une box:
Brancher le orangepi ou le raspberry pi à votre box internet
(avec un cable rj45 pour le orange pi qui n'a pas le wifi par défaut, avec un cable rj45 ou en wifi pour votre raspberry pi)

Pour obtenir l'ip de votre dietpi ou raspberry pi, taper la commande suivante:
ip a
L'adresse ip s'affiche (192.168.2.2 sur l'image jointe)
Verifier que votre serveur est accessible depuis un autre ordinateur connecté à votre box ou routeur connecté au modem 4g ou réseau wifi en tapant dans la barre de votre navigateur (en remplacant adresse_ip par l'adresse trouvée avec la commande ip a)
http://adresse_ip/nextcloud/

Rendre votre réseau local accessible depuis internet:
Si vous n'avez pas de box internet (**reseau wifi de votre telephone ou modem 4g ou box 4g, se reporter aux etapes 7 et 8**)
Si vous avez une box internet:

Pour rendre votre dietpi accessible depuis internet, il faut aller dans la configuration de votre box et
dans la section "NAT" "Port Forwarding" mettre le port 80 et renseigner l'ip trouvée précedemment ainsi que le port 443 et renseigner l'ip trouvée précédemment également.
Je n'ai pas de box donc je n'ai pas pu vous faire de screenshot mais vous trouverez des ressources sur internet pour cela. Par exemple https://pratiquepc.fr/ouvrir-des-ports-sur-une-livebox/

Si vous voulez vous connecter en ssh à votre serveur dietpi depuis un autre ordinateur:

Pour se connecter en ssh sans login avec dropbear au orange pi/raspberry pi
copier votre clé publique ssh dans le fichier authorized_keys placé dans ~/.ssh/authorized_keys
ne pas oublier de faire un chmod 0600 sur ce fichier

Pour le orange pi, qui utilise dropbear:
ajouter la ligne DROPBEAR_EXTRA_ARGS="-s"
au fichier /etc/default/dropbear

Vous pouvez ensuite trouver votre ip publique (celle accessible par tous sur internet) en tapant depuis votre console dietpi
curl ifconfig.me
(si curl n'est pas installé lancer la commande apt update && apt install curl)

Une fois la configuration NAT/Port Forwarding effectué, tester si nextcloud est accessible sur internet en rentrant l'adresse suivante dans la barre de votre navigateur internet:
http://adresse_ip_publique/nextcloud/
(remplacer adresse_ip_publique par l'adresse trouvée précédemment

Attention les navigateurs peuvent être un peu capricieux sans le https, si vous voulez tester en sortant du diagnostic une possible erreur navigateur taper dans un terminal linux :
curl **http://adresse_ip_publique/nextcloud/**

Étape 7 - configuration d'un vpn wireguard pour rendre accessible votre serveur depuis une box 4g ou un modem 4g

[ATTENTION, cette section remet en question le marché des vpns!!]
Cette section n'est utile que pour les connections 4G ou en wifi sur téléphone (4G ou 5G)

La 4g a l'avantage d'être mobile, avec une tres faible consommation du modem autour de 5W, et vous pouvez trouver des modems 4g sans wifi pour limiter la surface d'attaque de votre serveur (exemple netgear lm1200 autour de 150€).

qu'est ce qu'un vpn?
Les VPN sont principalement connus pour les "clients" vpn. C'est à dire que vous l'utilisez sur votre ordinateur pour vous "anonymiser".
Le vpn est en fait un tunnel entre votre ordinateur et un ordinateur distant à partir duquel partent vos requetes vers internet. Tout votre traffic en direction d'internet va passer par ce tunnel.
Internet pense ainsi que vos requetes proviennent de cet ordinateur distant. C'est à dire que votre ip publique devient celle de cet ordinateur distant.
Votre fournisseur d'accès ne voit que le traffic entre votre ordinateur et cet ordinateur distant, ce qui vous "anonymise".

En réalité, vous êtes anonyme vis à vis de votre fournisseur d'acces à internet, mais vous ne faites que déplacer la confiance vers votre fournisseur vpn qui lui peut voir votre traffic.

Le vpn a aussi d'autres utilités comme vous donner accès à des sites qui filtrent l'accès selon la "provenance" de votre adresse ip publique.

Vous pouvez tout à fait créer votre propre serveur vpn, et dans notre cas, ce serveur vpn permettra de rediriger les requetes internet faites sur ce serveur vers votre orange pi/raspberry pi en passant par le tunnel (dans l'autre sens que lorsque vous l'utilisez en tant que client pour accéder à internet).

Et nous allons voir comment.

Créer un serveur sur gandi.net

Créer un compte sur gandi.net, puis créer un serveur dans gandicloud vps. Voir les images jointes pour la création en 3 clics du serveur qui coute 5€/mois.

Pour créer une clé ssh et se logger voir
https://docs.gandi.net/fr/hebergement_web/connexion/cle_ssh.html
https://docs.gandi.net/fr/cloud/operations_courantes/connexion_serveur.html

Une fois loggé sur le serveur,
lancer la commande pour installer wireguard et les dépendances nécessaires

```
sudo apt update && sudo apt install wireguard resolvconf iptables nano -y
```

Lancer la même commande sur votre orange pi/raspberry pi.

lancer ensuite les commandes suivantes sur votre serveur et sur le orange pi/raspberry pi pour creer les cles privés et publiques de wireguard

```
sudo mkdir -p /etc/wireguard


sudo sh -c 'wg genkey | (umask 0077 && tee /etc/wireguard/private_key) | wg pubkey > /etc/wireguard/public_key'
```

Afficher la clé publique sur votre orange pi/raspberry pi en tapant

```
sudo cat /etc/wireguard/public_key
```

Afficher egalement la clé publique sur votre serveur en tapant

```
sudo cat /etc/wireguard/public_key
```

Entrer ensuite les commandes suivantes pour créer un fichier de configuration /etc/wireguard/wg0.conf sur votre serveur:
Taper les lignes suivantes (remplacer cle_publique_du_orange_pi_ou_raspberry_pi par celle affichée précédemment) :

```
echo "[Interface]" | sudo tee /etc/wireguard/wg0.conf


echo "Address=10.10.0.1/24" | sudo tee -a /etc/wireguard/wg0.conf

echo "PrivateKey=$(sudo cat /etc/wireguard/private_key)" | sudo tee -a /etc/wireguard/wg0.conf

echo "ListenPort=12345" | sudo tee -a /etc/wireguard/wg0.conf

echo "[Peer]" | sudo tee -a /etc/wireguard/wg0.conf

echo "PublicKey=cle_publique_du_orange_pi_ou_raspberry_pi" | sudo tee -a /etc/wireguard/wg0.conf

echo "AllowedIPs=10.10.0.2/32" | sudo tee -a /etc/wireguard/wg0.conf
```

Entrer ensuite la commande suivante sur le serveur pour lancer et activer le service vpn

```
sudo systemctl start wg-quick@wg0


sudo systemctl enable wg-quick@wg0
```

taper ensuite

```
curl ifconfig.me
```

pour obtenir l'ip publique de votre serveur

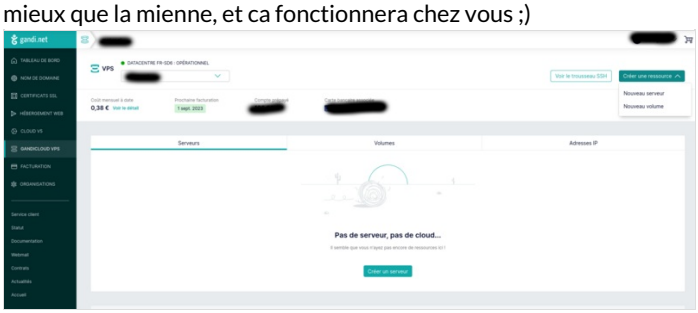
Taper les lignes suivantes (remplacer cle_publique_du_serveur par celle affichée précédemment et ip_publique_du_serveur par celle affichée précédemment) :

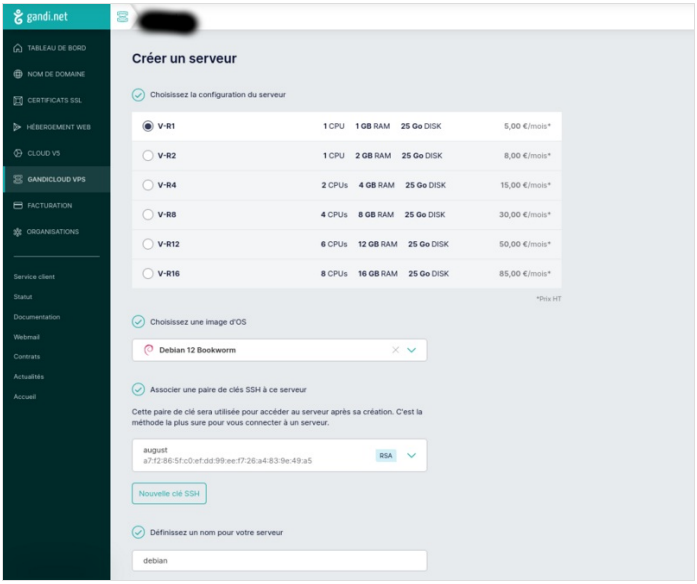
```
echo "[Interface]" | sudo tee /etc/wireguard/wg0.conf


echo "Address=10.10.0.2/24" | sudo tee -a /etc/wireguard/wg0.conf

echo "PrivateKey=$(sudo cat /etc/wireguard/private_key)" | sudo tee -a /etc/wireguard/wg0.conf

echo "[Peer]" | sudo tee -a /etc/wireguard/wg0.conf

echo "PublicKey=cle_publique_du_serveur" | sudo tee -a /etc/wireguard/wg0.conf

echo "AllowedIPs=10.10.0.1/32" | sudo tee -a /etc/wireguard/wg0.conf

echo "Endpoint=ip_publique_du_serveur:12345" | sudo tee -a /etc/wireguard/wg0.conf
```

La ligne AllowedIPS définit les ips de destination (sortantes) qui passeront par le tunnel et seront chiffrées mais aussi les ips entrantes autorisées. Si vous souhaitez configurer votre "client" (orange pi ou raspberry pi) pour utiliser le vpn pour accéder à internet, remplacer AllowedIPs=10.10.0.1/32 par AllowedIPs=0.0.0.0/0 En définissant 0.0.0.0/0 on indique que tout le traffic du orange pi/raspberry pi passera par le tunnel wireguard et toutes les ip entrantes seront autorisées. Il est alors important de bien configurer son firewall sur le serveur!
Pour vérifier que wireguard fonctionne, lancer la commande suivante sur le serveur vpn:

```
ping 10.10.10.2 -c 4
```

Le ping doit fonctionner
Ca ne fonctionne de façon systématique chez moi, mais je suis sur que si vous essayez loin de l'oeil de sauron votre météo numérique ira mieux que la mienne, et ca fonctionnera chez vous ;)





Étape 8 - configuration d'un vpn openvpn pour rendre accessible votre serveur depuis une box 4g ou un modem 4g

Dans le cas où ca ne fonctionnerait pas avec wireguard, vous pouvez utiliser openvpn, (qui est configurable sans ligne de commande à la souris!).

Configuration du serveur proxy gandi.net:
Pour cela suivez les étapes suivantes (https://openvpn.net/vpn-server-resources/installing-openvpn-access-server-on-a-linux-system/):

Update du 27/11/23: il n'y a pas de version bookworm d'openvpn-as disponible pour debian. Pensez à installer debian version bullseye

```
apt update && apt -y install ca-certificates wget net-tools gnupg


wget https://as-repository.openvpn.net/as-repo-public.asc -qO /etc/apt/trusted.gpg.d/as-repository.asc

echo "deb [arch=amd64 signed-by=/etc/apt/trusted.gpg.d/as-repository.asc] http://as-repository.openvpn.net/as/debian bullseye main" | sudo tee /etc/apt/sources.list.d/openvpn-as-repo.list

apt update && apt -y install openvpn-as
```

Si les commandes ci-dessus ne fonctionnent pas, il est possible qu'openvpn ait mis a jour des éléments. Merci alors de se reporter à https://openvpn.net/access-server/, s'inscrire, et suivre les instructions d'installation

Rendez vous ensuite sur la page de configuration du serveur: https://<adresse_ip_du_serveur>
login:openvpn
password: indiqué dans le log de l'installation

screen 1: go to admin panel reentrer vos login/password
screen2: Network settings: Activer UDP seulement et port 1194 puis save settings
screen3: VPN Settings: remplir les champs comme indiqué sur le screenshot puis save settings
screen 4 et 5: User Management/User permission : changer le mot de passe dans local password et entrer l'adresse ip fixe du screeenshot puis save settings. Puis update running server.
Pour vous reconnecter à l'interface de configuration: https://adresse_ip_du_serveur:943
screen 6: User Management/User profile: cliquer sur new profile puis Cliquer sur create profile.

Renommer le fichier de configuration téléchargé en openvpn.conf Ouvrir le fichier de configuration et trouver la ligne auth-user-pass et la remplacer par la ligne suivante:

```
auth-user-pass auth.txt
```

Configuration du orangepi/raspberrypi

Lancer ensuite sur le orangepi raspberry pi:

```
sudo apt update && sudo apt install openvpn
```

Copier le fichier de configuration télécharger vers /etc/openvpn/client/openvpn.conf sur votre orangepi/raspberry pi

creer un fichier auth.txt dans /etc/openvpn/client/ dans lequel vous copiez les deux lignes suivantes en remplacant password par votre mot de passe:

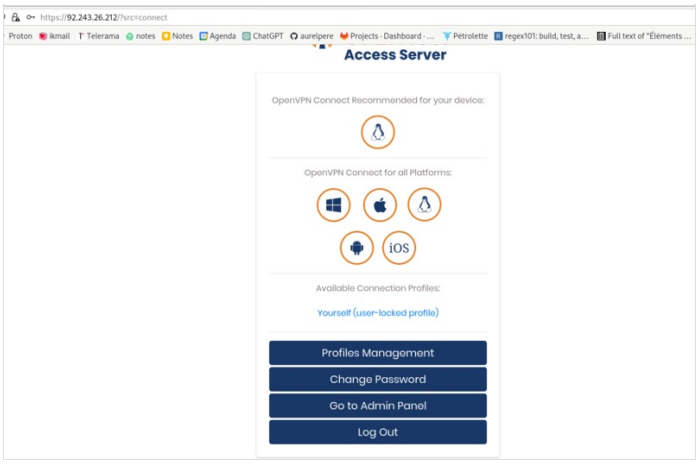
```
openvpn
password
```

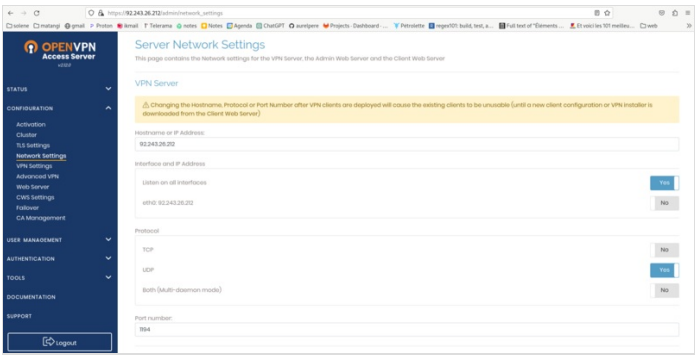
Lancer ensuite le client vpn:

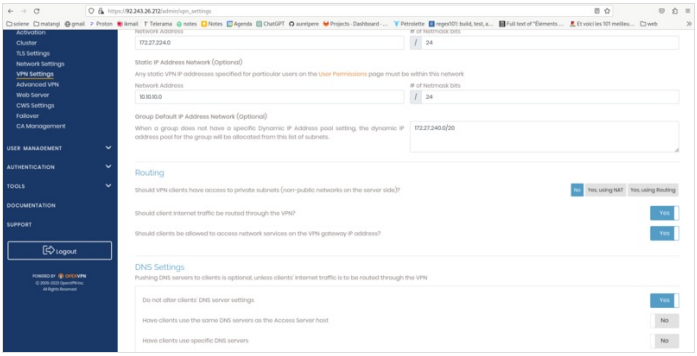
```
sudo systemctl start openvpn-client@openvpn
```

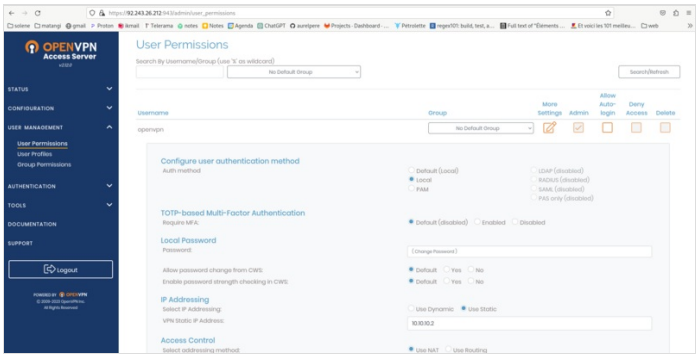
Si vous voulez que le client se connecte automatiquement au lancement de la machine taper

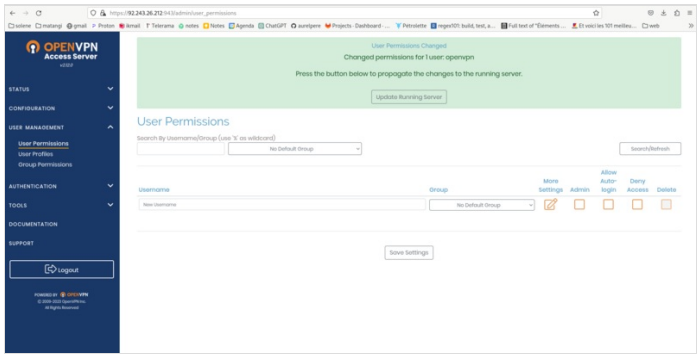
```
sudo systemctl enable openvpn-client@openvpn
```

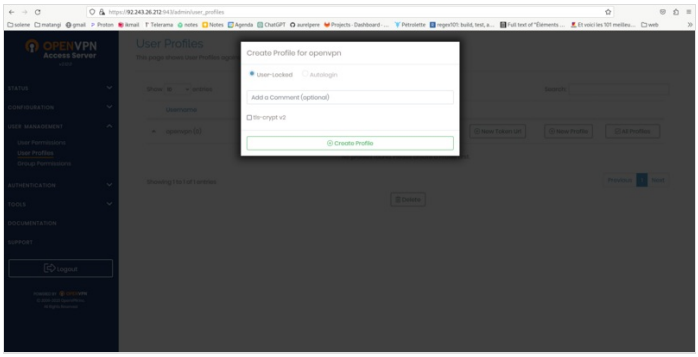












Étape 9 - Rediriger les requetes du serveur vpn vers le orange pi-raspberry pi

Pour rediriger les requetes sur le serveur vers le orange pi / raspberry pi, on met en place un serveur logiciel web nginx:

```
sudo apt install nginx -y
```

On ouvre ensuite le fichier de configuration de ce logiciel serveur web:

```
sudo nano /etc/nginx/sites-enabled/default
```

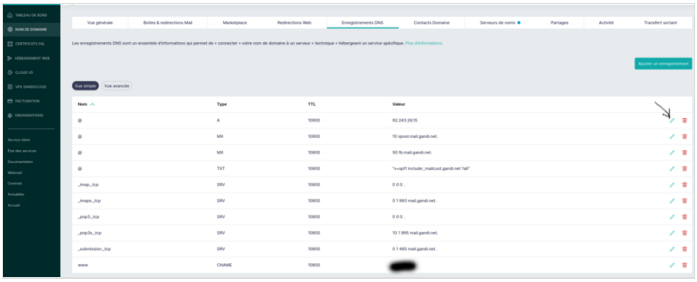
Remplacer le contenu du fichier par ce qui suit:

```
server {
listen 80;
server_name localhost;
server_tokens off;
add_header Permissions-Policy "accelerometer=(),autoplay=(),camera=(),display-capture=(),document-
domain=(),encrypted-media=(),fullscreen=(),geolocation=(),gyroscope=(),magnetometer=(),microphone=
(),midi=(),payment=(),picture-in-picture=(),publickey-credentials-get=(),screen-wake-lock=(),sync-xhr=
(self),usb=(),web-share=(),xr-spatial-tracking=()";
add_header Strict-Transport-Security "max-age=31536000 ; includeSubDomains";
add_header X-Frame-Options "SAMEORIGIN";
add_header X-Content-Type-Options nosniff;
add_header Content-Security-Policy "script-src 'self';";
add_header X-Permitted-Cross-Domain-Policies none;
add_header Referrer-Policy no-referrer;
add_header Clear-Site-Data "cache,cookies,storage";
location / {
proxy_pass http://10.10.0.2;
proxy_set_header Host $host;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-Proto $scheme;
client_max_body_size 20M;
limit_except GET HEAD POST {deny all;}
}

}
```

Nginx va rediriger les requetes faites sur l'ip publique de votre serveur vers le nextcloud de votre orange pi / raspberry pi (ligne proxy_pass http://10.10.0.2;)

Vous pouvez tester si cela fonctionne en vous rendant sur la page:
http://ip_publique_de_votre_serveur_gandi/nextcloud/
(notez bien que c'est en http et pas https)
Attention, de nombreux navigateurs n'acceptent plus tres bien les redirections en http, voir la section https pour configurer le https (il faudra prendre un nom de domaine).

Étape 10 - Nom de domaine et adresse fixe



Le nom de domaine est l'adresse dans votre navigateur : par exemple lowtechlab.org.

Il vous permet de rendre votre serveur accessible plus facilement avec une adresse facilement memorisable. Il ne fait qu'associer le nom de domaine à l'adresse ip de votre serveur vpn ou l'adresse ip de votre box.

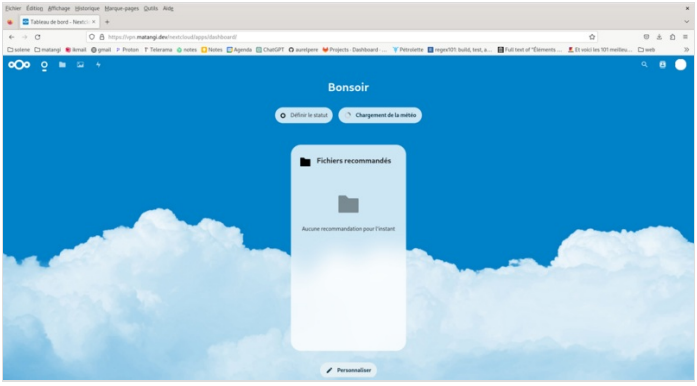
Que vous enregistriez un nom de domaine pour rediriger vers votre adresse ip ou pas (c'est nécessaire pour avoir le https cependant), il faut noter que par défaut, les fournisseurs d'accès vous octroient une adresse ip différente à chaque connexion.

Si vous souhaitez une adresse ip fixe, il faut en faire la demande à votre fournisseur d'accès. Ce n'est malheureusement plus très répandue dans les offres grands publics. Orange propose à la place un "DynDns" qui vous propose une adresse en lettres correspondant à votre adresse ip mais à laquelle vous ne pouvez pas rattacher facilement un nom de domaine. Certains gestionnaires de nom de domaine, comme infomaniak, proposent tout de même d'enregistrer un nom de domaine pour le dyndns qui est acessible assez facilement sans surcout chez les principaux opérateurs.

Si vous avez un accès en 4G, il n'est pas possible d'avoir une adresse ip fixe et votre adresse ip publique correspondra à un "pool". C'est à dire que l'opérateur alloue une adresse ip publique pour plusieurs clients, ne vous permettant pas d'utiliser la technique du NAT/Port Forwarding pour rendre votre dietpi accessible sur internet.
Il faudra alors prendre un nom de domaine pour votre serveur vpn qui redirige les requetes vers votre dietpi.

Voir image jointe pour l'enregistrement d'un nom de domaine: c'est la ligne nom "@" type A qu'il faut renseigner avec l'adresse ip publique de votre box ou de votre serveur vpn.

Étape 11 - Configuration https sur serveur gandi vpn



Si vous avez un serveur vpn

Sur votre serveur gandi, effectuer les opérations suivantes:

Creer un fichier /etc/nginx/conf.d/dietpi.conf et copier les lignes suivante:

```
server {
listen 80;
server_name localhost;
server_tokens off;
add_header Permissions-Policy "accelerometer=
(),autoplay=(),camera=(),display-capture=
(),document-domain=(),encrypted-media=
(),fullscreen=(),geolocation=(),gyroscope=
(),magnetometer=(),microphone=(),midi=
(),payment=(),picture-in-picture=(),publickey-
credentials-get=(),screen-wake-lock=(),sync-xhr=
(self),usb=(),web-share=(),xr-spatial-tracking=()";
add_header Strict-Transport-Security "max-
age=31536000 ; includeSubDomains";
add_header X-Frame-Options "SAMEORIGIN";
add_header X-Content-Type-Options nosniff;
add_header Content-Security-Policy "script-src
'self';";
add_header X-Permitted-Cross-Domain-Policies
none;
add_header Referrer-Policy no-referrer;
#add_header Clear-Site-Data
"cache,cookies,storage";
return 301 https://$host$request_uri;
location / {
return 301 https://$host$request_uri;
}
}
```

lancer ensuite les commandes suivantes:

```
sudo apt install letsencrypt


wget
https://raw.githubusercontent.com/certbot/certbot/master/certbot-nginx/certbot_nginx/_internal/tls_configs/options-ssl-nginx.conf

sudo cp options-ssl-nginx.conf /etc/letsencrypt/options-ssl-nginx.conf

wget
https://raw.githubusercontent.com/certbot/certbot/master/certbot/certbot/ssl-dhparams.pem

sudo cp ssl-dhparams.pem /etc/letsencrypt/ssl-dhparams.pem

sudo rm /etc/nginx/sites-enabled/default

sudo apt remove certbot

sudo apt install python3-certbot-nginx
```

obtenir les certificats (rempalcer __domain__ par votre domaine):

```
sudo certbot certonly --nginx -d __domain__
```

copier ensuite les lignes suivante dans votre fichier /etc/nginx/conf.d/dietpi.conf
en remplacant __domain__ par votre domaine

```
server {
listen 80;
server_name localhost;
server_tokens off;
add_header Permissions-Policy "accelerometer=
(),autoplay=(),camera=(),display-capture=
(),document-domain=(),encrypted-media=
(),fullscreen=(),geolocation=(),gyroscope=
(),magnetometer=(),microphone=(),midi=
(),payment=(),picture-in-picture=(),publickey-
credentials-get=(),screen-wake-lock=(),sync-xhr=
(self),usb=(),web-share=(),xr-spatial-tracking=()";
add_header Strict-Transport-Security "max-
age=31536000 ; includeSubDomains";
add_header X-Frame-Options "SAMEORIGIN";
add_header X-Content-Type-Options nosniff;
add_header Content-Security-Policy "script-src
'self';";
add_header X-Permitted-Cross-Domain-Policies
none;
add_header Referrer-Policy no-referrer;
```

```
#add_header Clear-Site-Data
"cache,cookies,storage";
return 301 https://$host$request_uri;
location / {
return 301 https://$host$request_uri;
}
}
server {
listen 443 ssl http2;
server_name localhost;
server_tokens off;
ssl_certificate
/etc/letsencrypt/live/__domain__/fullchain.pem;
ssl_certificate_key
/etc/letsencrypt/live/__domain__/privkey.pem;
include /etc/letsencrypt/options-ssl-nginx.conf;
ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem;
add_header Permissions-Policy "accelerometer=
(),autoplay=(),camera=(),display-capture=
(),document-domain=(),encrypted-media=
(),fullscreen=(),geolocation=(),gyroscope=
(),magnetometer=(),microphone=(),midi=
(),payment=(),picture-in-picture=(),publickey-
credentials-get=(),screen-wake-lock=(),sync-xhr=
(self),usb=(),web-share=(),xr-spatial-tracking=()";
add_header Strict-Transport-Security "max-
age=31536000 ; includeSubDomains";
add_header X-Frame-Options "SAMEORIGIN";
add_header X-Content-Type-Options nosniff;
add_header Content-Security-Policy "script-src
'self';";
add_header X-Permitted-Cross-Domain-Policies
none;
add_header Referrer-Policy no-referrer;
#add_header Clear-Site-Data
"cache,cookies,storage";
location / {
proxy_pass http://10.10.10.2;
proxy_set_header Host $host;
proxy_set_header X-Forwarded-For
$proxy_add_x_forwarded_for;
proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-Proto $scheme;
client_max_body_size 20M;
limit_except GET HEAD POST {deny all;}
}
}
```

redémarrer nginx

```
sudo systemctl restart nginx
```

Une fois ces étapes réalisées, votre serveur est accessible en ligne
en https en tapant dans votre navigateur
https://votre_domaine/nextcloud/
Vous pouvez alors configurer nextcloud en ligne par le compte
administrateur login par défaut sur dietpi: admin mot de passe par
défaut sur dietpi: mot de passe entrée à l'installation de dietpi

Étape 12 - Configuration https sur dietpi si vous etes branché en box

Je n'ai pas de box, je vous updaterai quand ce sera le cas et prooftesté! :)

Étape 13 - Rendre votre serveur nomade et autonome énergétiquement en photovoltaique

Que ce soit pour des raisons écologiques, ou pour d'autres raisons, il est intéressant d'avoir un serveur autonome énergétiquement,
qui ne dépendra pas des aléas du réseau électrique.
NB: pour une version légèrement modifié du dimensionnement photovoltaïque (production moyenne/par intervalle calée sur modèle jrc en décembre au lieu du nombre d'heure d'ensoleillement minimum), voir mon autre tuto ici:
Dimensionner une installation photovoltaïque autonome
videos:
bases debutant(panneaux, regulateur, onduleur, conso/prod): https://www.youtube.com/watch?v=8Ft4XQj9lQ4
montage simple kit myshop solaires pour 230V: https://www.youtube.com/watch?v=SvmPEhPq_S8
kit prêts à acheter (si vous avez des subventions et des collègues qui coopèrent bien):
https://allo.solar/kit-solaire-1650w-230v-autoconsommation-aps.html?gclid=EAIaIQobChMIkY_fxvu-gAMVyLfVCh014gadEAYYASABEgJd8_D_BwE
solution de stockage intermédiaire intégrée (cher et pas tres lowtech):
Station énergie portable extensible 230V BLUETTI AC200MAX
EcoFlow River 2 pro
kits semi lowtech (celui utilisé dans ce guide):
panneaux photovoltaïque 120W et batterie de voiture plomb acide.
kit vraiment lowtech:
fabriquer sa batterie lithium à partir de déchets: voir barnabé chaillot
https://www.youtube.com/watch?v=_hwj7Ds50lU
rappel de base: branchement en série (+ sur - et + sur -) on ajoute le voltage et on garde le meme amperage, branchement en paralelle (+ sur +, - sur -) on ajoute l'amperage et on garde le meme voltage
idem pour les batteries: à mettre en paralelle pour garder la meme tension (voltage)

La première problématique du photovoltaïque lowtech autonome est le dimensionnement de l'installation (Se reporter à mon autre tuto Dimensionner une installation photovoltaïque autonome)

Pour cela on trouve pas mal d'informations sur internet.
Vous pouvez utiliser la feuille libreoffice en piece jointe en haut de ce tutoriel pour du dimensionnement "bricolé".
Le dimensionnement - le besoin journalier:
Le orange pi consomme environ 20W
Un disque usb supplémentaire consomme environ 5W
Un modem 4G consomme environ 5W
Soit un besoin constant de 35W en prenant 16% de marge d'erreur.
Le besoin journalier pour un serveur qui tourne 24h/24: 35W*24h=840Wh
Le besoin journalier pour un serveur qui tourne en journéee seulement:
en été: 35W*14h=490Wh
en hiver: 35W*8h=280Wh
Notez qu'il s'agit là d'un besoin moyen et si vous souhaitez dimensionner
pour des usages divers, il est recommander de procéder de façon plus précise
en calculant les besoins temps réels.
Le dimensionnement du stockage par le temps d'autonomie :
Estimer les pertes à 20% et augmenter le besoin en consquénce:
besoin 24h/24=840/0,80=1050Wh
Estimer le temps d'autonomie voulue:
exemple 24h
On va alors dimensionner le stockage pour tenir 24h.

Pour des batteries en 12V: 1050Wh/12V=87,5Ah
Etant donné qu'on veut limiter la décharge des batteries à 50%, on prendra donc
87,5Ah/0,5=175Ah
Soit 2100 Wh en 12V
Selon les caractéristiques des panneaux (voir feuille de calcul), on peut estimer la recharge de la batterie lorsque l'ensoleillement est minimal (en décembre).

Le dimensionnement par la méthode du nombre de jours voulues pour recharger entierement les batteries:
Si on veut pouvoir recharger les batteries en un jour en hiver, il faut considérer la puissance produite par vos panneaux au jour d'hiver avec le moins d'ensoleillement.
Si on prend 3,5h pour le minimum, le nombre de panneaux nécessaire de puissance x Watt sera:
C_batterie:Capacité batterie en Wh
Dans notre exemple 2100Wh
T_hiver:temps de recharge journalier minimal en hiver (en h)
Dans notre exemple 3,5h
B_hiver:besoin journalier hors temps ensoleillement en hiver (en Wh)
Dans notre exemple (24h-3,5h)*35W=897Wh
n_voulus:nombre de jour voulus pour recharger entierement la batterie
Dans notre exemple 1
I:amperage sortie d'un panneau photovoltaique
Dans notre exemple 7A
U:tension sortie d'un panneau photovoltaique
Dans notre exemple 12V
Nb_panneaux=C_batterie+B_hiver*n_nvoulus/T_hiver*I*U*n_voulus
Dans l'exemple:
Nb_panneaux=(2100+897*1)/(3,5*12*7*1)
Il faudra donc 10 panneaux de 84W de 7A 12V

Noter que la valeur cardinale ici est à la ligne 42 du fichier joint, il s'agit
de l'ensoleillement journalier minimal en décembre à production nominale. Des valeurs de référence peuvent être trouvées sur https://re.jrc.ec.europa.eu/api/v5_2/seriescalc?lat=44.203142&lon=0.616363&loss=14&angle=45&aspect=0&startyear=2005&endyear=2005&pvcalculation=1&peakpower=1&pvtechchoice=crystSi&browser=0&outputformat=csv

Mais rien ne vaut une mesure empirique pour vérifier tout ca.
Le graphique en illustration provient du monitoring de deux installations à 400km de distance d'une entreprise qui installe et suit du photovoltaïque depuis 2018. J'attend de mesurer tout ça avec un voltmetre fiable sur plusieurs panneaux achetés d'occasions pour updater ce tuto en décembre! :)
Tout commentaire et "retour d'experience" est bienvenu à ce sujet en bas de cette page!

Le dimensionnement par la méthode essais et erreurs
La feuille de calcul propose aux lignes 41 et 42 d'ajuster le nombre de panneaux et le temps d'ensoleillement moyen en décembre et donne le besoin journalier hors temps ensoleillement hiver en Wh et la recharge batterie journaliere maximale en hiver (en Ah et Wh). En faisant des essais sur les deux paramètres, on peut obtenir le nombre de panneaux minimum pour que la(les) batterie(s) se recharge(nt) positivement en hiver.
La problématique principale du photovoltaïque lowtech autonome est le stockage de l'énergie.

Vous pouvez lire les caractéristiques des panneaux qu'on vous a donné ou trouvés sur leboncoin à pas cher:
-puissance crete: elles s'aditionnent pour obtenir la puissance nécessaire trouvée lors de la phase de dimensionnement.
-tension : 12V,24V ou 48V. voir regles série/paralelle pour leur additions
-intensité: variable selon les modèles mais souvent inferieure à 10A. voir regles série/paralelle pour leur additions
Pour recharger des batteries, en principe, si vous connectez votre panneaux en direct sur une batterie, il suffit que la tension à la sortie de vos panneaux soit la même que celles de vos batterie, et ca devrait charger.

Il y a un composants importants à retenir pour charger correctement vos batteries:
le regulateur ou controleur de charge
il en existe de trois sortes: les tor (tout ou rien) les mppt (Maximum power point tracking) et les pwm (Pulse Width Modulation)
Ils sont composés d'un adaptateur DC/DC (courant continu vers courant continu) et d'un coupe circuit. Le mppt comprend également un adaptateur d'impédence (il a une résistance pour adapter l'amperage injecté dans la batterie). Les mppt accepte des puissances nominales plus élevées, cad des tensions et intensité plus élevées.

Le régulateur ou controleur de charge permet principalement de couper le circuit quand la batterie est rechargée en surveillant la tension et l'intensité de charge. Il coupe le circuit si leurs valeurs dépassent les intervalles de référence (pour cela le regulateur arrete la charge temporairement et mesure la tension aux bornes des batteries).
Le mppt a un "algorithme" électronique intégré qui va chercher le point de puissance optimal grace a son adaptateur d'impedance.
Si vous connectez plusieurs panneaux et plusieurs batteries, il est recommandé d'avoir un regulateur pour couper la charge correctement lorsque la batterie est chargée.
Les tensions de charge de référence sont 12V,24V et 48V.
Cependant, les prix des modèles augmentent avec la puissance nominales (qui va dépendre de l'amperage) qu'ils acceptent.

Pour limiter l'intensité du courant de la production photovoltaïque, il est plus judicieux d'utiliser des panneaux de plus forte puissance qui sont généralement à des tensions plus élevées
(rappel P=U*I,
rappel E=P*t se conserve dans un systeme fermé).
note: si le systeme de stockage par batterie ou l'appareil connecté à vos panneaux n'absorbe pas toute la puissance produite, et si le régulateur de charge ne coupe pas le circuit, le reste sera dégagé en chaleur.

L'amperage va aussi dependre de la capacité de stockage de vos batteries, dimensionnées pour couvrir vos besoins pendant une periode définie au dimensionnement.

Le courant de charge est calculé en divisant par 4 ou 5 la capacité nominale de la batterie exprimée en Ah qui devrait alors se recharger en 4 ou 5h. Cependant une batterie se rechargera aussi avec un courant de charge de la capacité nominale de la batterie divisée par 20 mais plus lentement (en 20h).
Dimensionnez et/ou agencez vos panneaux en conséquence.
Des montages de panneaux serie+paralelle peuvent permettrent d'ajuster tension et amperage.

Il y a enfin un dernier point sur lequel être attentif: le déclenchement de la recharge de la batterie par le regulateur/controleur de charge (qui déclenche quand la tension de la batterie diminue en dessous d'un certain seuil).
En effet, si la puissance soutirée à la batterie est trop faible, il est possible que le temps nécessaire à la décharger avec votre consommation journalière pour déclencher la recharge dans le régulateur dépasse le temps d'ensoleillement journalier. La batterie ne se recharge alors pas du tout pendant la journée.
Dans ce cas, votre batterie ne se rechargera qu'un jour sur deux ou sur trois (selon le seuil de déclenchement de la recharge du regulateur).
C'est un paramètre à prendre en compte dans le dimensionnement (non inclus dans la feuille de calcul).

Le régulateur a 3 phases:

1.bulk: le regulateur laisse passer le courant

2.floating: le regulateur alterne interupteur fermée et ouvert à une fréquence donnée pour maintenir la batterie chargée
En outre il faut prendre des précautions car la charge des batteries présente certains risques.

3.absorption (pour les mppt): la tension de charge augmente un peu pour créer une difference de potentiel suffisante pour continuer à charger la batterie presque pleine.

En théorie le courant de charge diminue lorsque la batterie est presque rechargée (courant de queue etc.)

La charge de batteries en paralelle ou en série sur des batteries usagées qui n'ont pas les mêmes tensions ou intensité présente en théorie des risques. En effet vous lirez un peu partout que la résistance des fils pour relier ces batteries
créee des différences de potentiels entre les batteries qui produisent des décharges d'une batterie envers une autre etc.
créant des risques d'explosion, de degazage pour les batteries plomb etc.

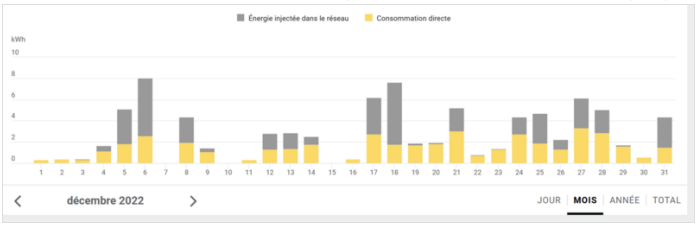
Il faut bien se rapeller que les batteries sont des assemblages de composants unitaires de faible tension mis en séries et en paralelle pour obtenir un générateur de l'intensité et la tension voulue et qu'à priori faire de même avec des batterie entiere ne présente pas vraiment de risques..

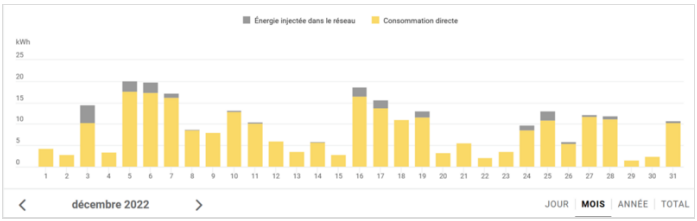
On parle souvent de "battery management system" (bms) "intégré" pour les batteries lithium ion.

En réalité le régulateur de charge est déjà un "bms". En théorie, le bms intégré s'assure que les tensions et les intensités de chaque unité composant la batterie est la même et la rééquilibre au besoin.

On peut bien sûr s'interroger si tout ceci n'est pas une façon de rendre le stockage de l'énergie plus cher avec des composants BMS artificiellement chers et si ce n'est pas une façon d'éviter de réutiliser des unités de batteries usagées.
Il est par exemple étonnant qu'il n'existe pas de BMS pour rééquilibrer automatiquement des batteries plomb acide, ce qui rendrait utilisable toutes les batteries mises au rebut de l'industrie automobile pour stocker l'énergie photovoltaïque sans risque!

Dans tous les cas, si vous réutilisez des batteries au plomb, utilisez un régulateur pour éviter de continuer à charger vos batteries rechargées (risques de production d'hydrogene) -ou si vous n'en utilisez pas dimensionnez avec beaucoup de soin-, évitez les décharges profondes, et maintenez les batteries à une temperature constante autant que possible.





Étape 14 - Montage et test

On dimensionne sur un dixieme de la puissance de panneaux et un quart de la capacité de batterie de ce que la théorie nous a indiqué pour être autonome 24h/24h et en capacité de recharger en un seul jour en hiver, soit un panneau de 120W et une vieille batterie de voiture de 45Ah en 12V.

C'est raccord avec une approche lowtech de ne faire tourner le serveur que lorsqu'il fait jour, pour une informatique qui respecte la temporalité humaine.
Pour être bien en hiver (à hypothèse 3,5h d'ensoleillement moyen), il faudrait une batterie de plus de 58Ah, mais pour raisons budgétaire, on fait pour l'instant avec ce qu'on a! :).

Le regulateur utilisé n'accepte pas les panneaux 40V donc on n'a pas utilisé le panneau photovoltaïque d'occasion de 180W à 20€ trouvé sur leboncoin, mais je ne manquerai pas d'updater ce tuto avec des raccordement de panneaux et de batteries dès que j'aurai le materiel et avec les valeurs de production hivernale si j'y arrive!

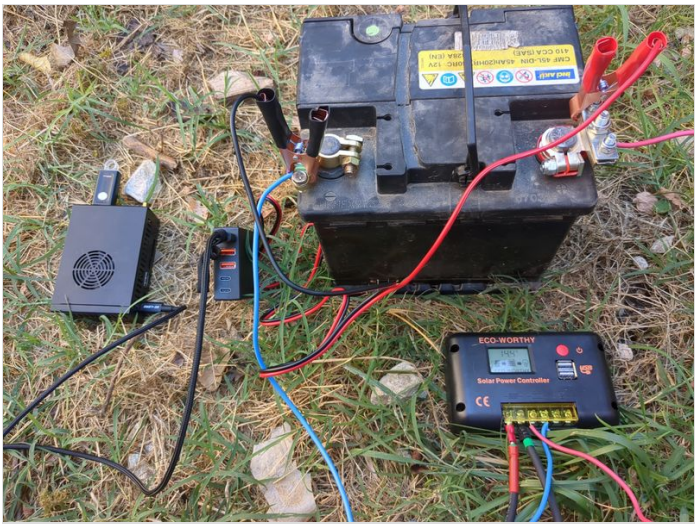
Etapes de montage:

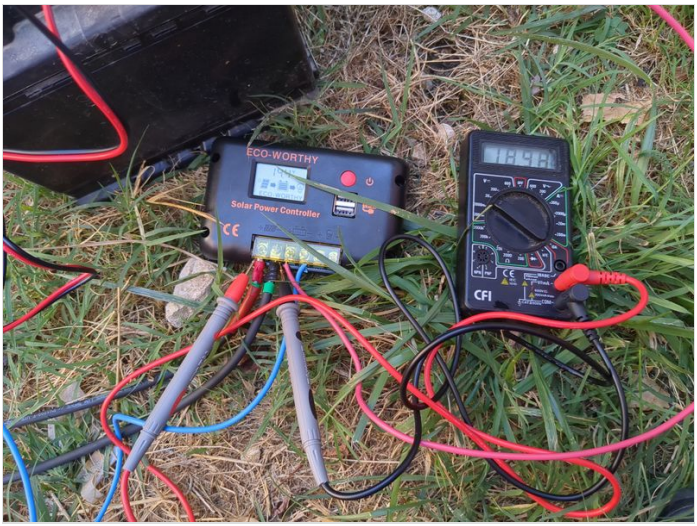
1. Raccorder un cable electrique de la borne + de la batterie à la borne + du regulateur pwm (sortie batterie). Raccorder un cable electrique de la borne - de la batterie à la borne - du regulateur pwm (sortie batterie)
2. Raccorder les panneaux aux cables mc4. Brancher le côté dénudé du cable + au + du régulateur pwm (entree panneaux). Brancher le côté dénudé du cable - au - du régulateur pwm (entree panneaux).
3. Brancher les pinces du convertisseur 12V batterie/5V USB avec le + sur le + et le - sur le -
4. Brancher le cable rj45 de votre box ou modem 4g au orange pi ou raspberry pi
5. Brancher le cable usb du orange pi ou raspberry pi au convertisseur 12V batterie/5V USB
6. Pour automatiser le fonctionnement quand il fait jour et éteindre quand il fait nuit, on utiliser un module DRL (Daytime Running Light) de voiture. Le module est un interupteur qui laisse passer le courant quand la tension est supérieure à 13V (quand le panneau solaire charge la batterie). L'interrupteur est à brancher borne + du IN sur le + de la batterie, borne - du IN sur le - de la batterie, borne + du out sur la pince rouge et borne - du out sur la pince rouge (entre la batterie et le convertisseur 12V batterie/5V USB).

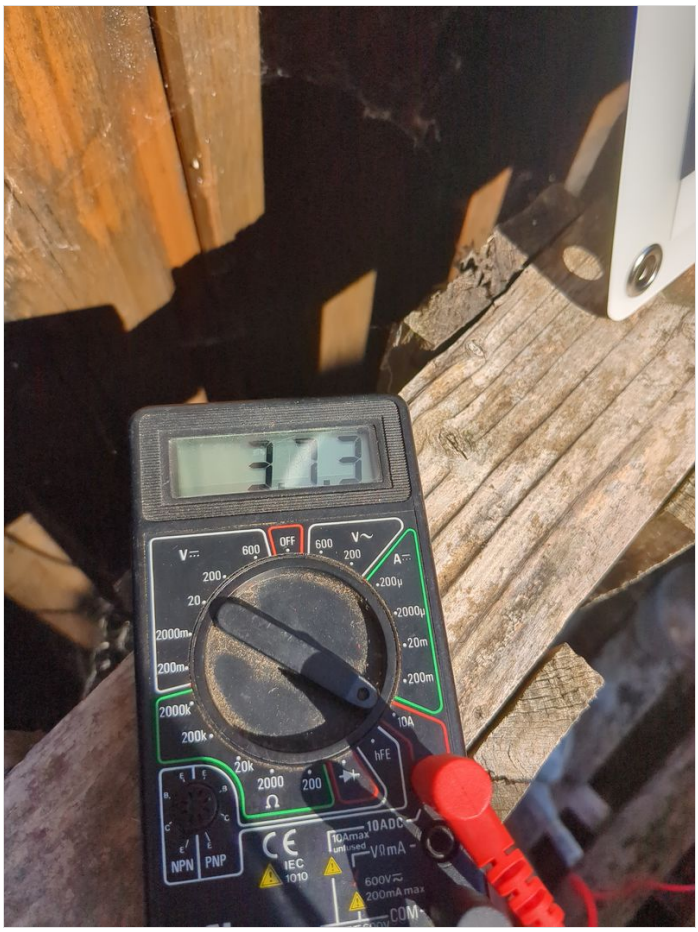
Attendre quelques minutes que ca boot. Et voilà , votre serveur nextcloud est accessible en ligne ! :)

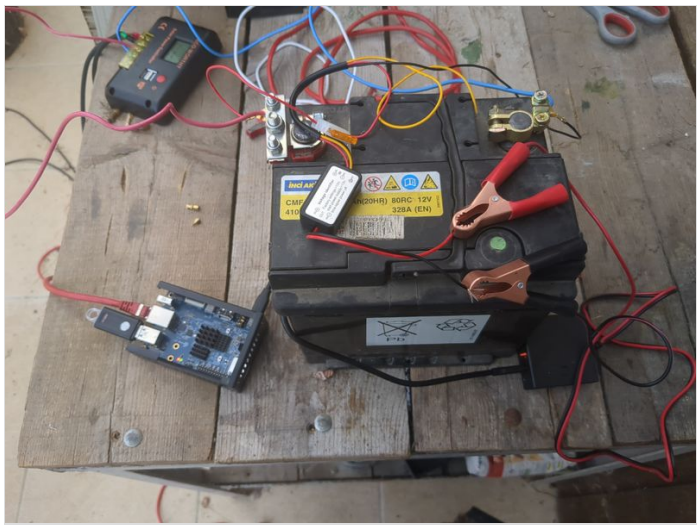
Notez que si vous voulez alimenter quelque chose en courant alternatif 220V, la seule chose qu'il manque au montage est un convertisseur DC/AC (courant continu alternatif) qu'on trouve facilement en magasin de camping car ou sur leboncoin.


ECO-WORTHY®
Product: Solar Module
Model: ECOM-130
Rated Max Power(*STC): 130W
Solar Cell: Monocrystalline
Max Power Voltage(Vmp): 21.10V
Open Circuit Voltage(Voc): 24.50V
Max Power Current(Imp): 6.16A
Short Circuit Current(Isc): 6.50A
Weight: 4.40 lbs(2.0 kg)
Size: 37.8 x 27.1 x0.1 in(960 x 690 x 2.5mm)
All technical data at STC:
AM=1.5
Irradiance=1000w/m²
Tc=25℃
ISO 9001
CE


ECO-WORTHY
Solar Power Controller


ECO-WORTHY
Solar Power Controller





Étape 15 - Securisation du serveur

Au niveau sécurité, les failles connues des cpus peuvent être trouvées sous linux en faisant:

```
grep -r . /sys/devices/system/cpu/vulnerabilities
```

Cette commande sur le orange pi (cpu CortexA55) avec dietpi installé donne:

```
/sys/devices/system/cpu/vulnerabilities/spectre_v2:Mitigation: Unprivileged eBPF enabled
/sys/devices/system/cpu/vulnerabilities/itlb_multihit:Not affected
/sys/devices/system/cpu/vulnerabilities/mmio_stale_data:Not affected
/sys/devices/system/cpu/vulnerabilities/mds:Not affected
/sys/devices/system/cpu/vulnerabilities/l1tf:Not affected
/sys/devices/system/cpu/vulnerabilities/spec_store_bypass:Mitigation: Speculative Store Bypass disabled via prctl
/sys/devices/system/cpu/vulnerabilities/tsx_async_abort:Not affected
/sys/devices/system/cpu/vulnerabilities/spectre_v1:Mitigation: __user pointer sanitization
/sys/devices/system/cpu/vulnerabilities/retbleed:Not affected
/sys/devices/system/cpu/vulnerabilities/srbds:Not affected
/sys/devices/system/cpu/vulnerabilities/meltdown:Not affected
```

Ayant testé un orange pi un raspberry pi et un odroid, le probleme reste le même.

basiques:

on peut passer sa vie à augmenter la sécurité d'un systeme informatique...
trouver le bon compromis et évaluer les risques ou appats en termes financiers.
Le hack est toujours possible, et vu le nombre de failles 0day non encore publié, quel que soit le systeme d'exploitation, la question est moins d'avoir un système infaillible, que de savoir de qui on cherche à se protéger quand on cherche à "sécuriser" ou réduire sa surface d'attaque.

Je pense que la philosophie libre reste supérieure en termes de sécurité car auditable et réparable plus vite par la "commu", mais il faut bien avouer que les reglages par défaut ne sont pas tip top car linux a été pensé pour être stable au départ (rappelez vous des écrans bleux windows il y a 30 ans), et pas "sécurisé".
Ayant subi des hacks que je considère très avancés et pas à la portée du premier venu(et ce quel que soit le système d'exploitation, quelle que soit la machine, et quel que soit le niveau de sécurisation -hors compilation de kernel-), j'ai cherché à sécuriser mes dispositifs numériques et j'en arrive aujourd'hui à penser que la "souveraineté" numérique n'existe pas ou plus, les failles créent un marché de la sécurité, ca fait travailler des gens... Voir l'article intéressant de w0nderfall au sujet de la sécurité sous linux: https://wonderfall.space/linux-securite/

Cependant quelques éléments car c'est un sujet sur lequel on trouve peu d'informations didactiques rassemblées.
-**principe de limiter surface d'attaque** : principe général, la sécurisation ne fait que diminuer la surface d'attaque potentielle

-**acces physique sécurisé et config logicielle liée:**
- acces physique: à vous de voir
-mot de passe grub

Lancer dans un terminal:

```
grub-mkpasswd-pbkdf2
```

Copier le texte qui commence par grub.pbkdf2.sha512.10000.xy
où xy est une longue suite de lettres et de chiffres
Ajouter les lignes suivantes à un fichier /etc/grub.d/42_pw
en remplacant user par votre nom d'utilisateur linux et pw par le
texte précemment copié

```
cat << EOF
set superusers=user
password_pbkdf2 pw
EOF
```

lancer ensuite la commande

```
update-grub
```

-bons mots de passes en general
pour changer le mot de passer de l'utilisateur courant taper

```
passwd
```

pour changer le mot de passe de l'utilisateur root taper

```
sudo passwd root
```

-éventuellement vérification d'intégrité du boot (voir ordinateurs de purism par exemple)

-chiffrer (crypter) ses supports de stockage:
https://doc.ubuntu-fr.org/tutoriel/chiffrer_ses_donnees
https://www.dwarmstrong.org/remote-unlock-dropbear/

sécurité d'un serveur:
-apt update automatisé : https://www.linuxtricks.fr/wiki/debian-activer-les-mises-a-jour-automatique-avec-unattended-upgrades

-ssh renforcé :

lignes à inclure dans votre configuration ssh (/etc/ssh/sshd_config):

```
Port 22 #changer sur un autre port si vous le souhaitez
Protocol 2
PermitRootLogin no
StrictModes yes
PermitEmptyPasswords no
X11Forwarding no
Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr
MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-512,hmac-sha2-256,umac-128@openssh.com
KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256
AllowTcpForwarding no
MaxSessions 1
UsePAM yes
AllowUsers user #remplacer par les utilisateurs autorisées
AllowGroups group #remplacer par les groupes autorisés
PasswordAuthentication no
AuthorizedKeysFile .ssh/authorized_keys
```

-firewall logiciel:
ufw: https://doc.ubuntu-fr.org/ufw
ou fichier de configuration iptables:
https://gitlab.com/aurelpere/bp028-hardening/-/blob/main/rhel_iptables_ipv4/files/server_firewall.sh
-backup: regle du 321 : 3 copies, 2 supports de stockages differents, 1 copie sur un autre lieux que les autres. borgbackup reste un standard pour sa fiabilité dans la communauté du libre (je confirme apres avoir testé plusieurs trucs) et offre un cloud pas cher pour stocker des sauvegardes "remote" qui finance le developpement de son logiciel libre.

fail2ban: https://doc.ubuntu-fr.org/fail2ban
fail2ban pour nextcloud: https://tuxicoman.jesuislibre.net/2015/01/fail2ban-pour-owncloud-7-sur-debian-jessie.html

-desactiver ipv6 (ou configurer le firewall aussi pour ipv6)
3 méthodes pour désactiver ipv6:
1.dans grub
2.avec sysctl
ajouter les lignes suivantes à /etc/systcl.conf

```
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.all.router_solicitations = 0
net.ipv6.conf.default.router_solicitations = 0
net.ipv6.conf.all.accept_ra_rtr_pref = 0
net.ipv6.conf.default.accept_ra_rtr_pref = 0
net.ipv6.conf.all.accept_ra_pinfo = 0
net.ipv6.conf.default.accept_ra_pinfo = 0
net.ipv6.conf.all.accept_ra_defrtr = 0
net.ipv6.conf.default.accept_ra_defrtr = 0
net.ipv6.conf.all.autoconf = 0
net.ipv6.conf.default.autoconf = 0
net.ipv6.conf.all.accept_redirects = 0
net.ipv6.conf.default.accept_redirects = 0
net.ipv6.conf.all.accept_source_route = 0
net.ipv6.conf.default.accept_source_route = 0
net.ipv6.conf.all.max_addresses = 1
net.ipv6.conf.default.max_addresses = 1
```

3.avec le network manager nmcli
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/configuring_and_managing_networking/using-networkmanager-to-disable-ipv6-for-a-specific-connection_configuring-and-managing-networking

-sécuriser le serveur en cas de multi utilisateur ou autres utilisateurs ayant obtenu un accès:

listes de fichiers à sécuriser (permissions etc.): https://linuxfr.org/forums/linux-general/posts/liste-des-fichiers-linux-a-securiser-owner-group-permissions-setuid-setgid-sticky-bit

guides de durcissement anssi : https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-un-systeme-gnulinux/

Pour aller plus loin en termes de sécurité:

firewall physique libre: pcengines/ logiciel libre OPNSense

fail2ban avec listes géographiques: https://thecustomizewindows.com/2016/11/fail2ban-geoip-action-script-block-ssh-country/

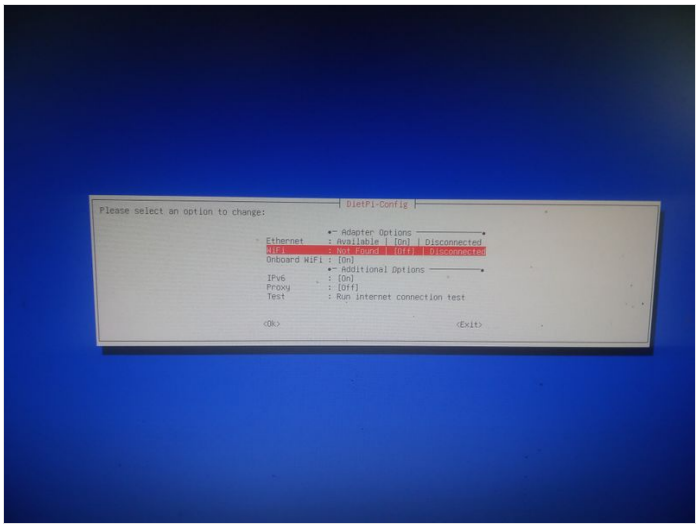
Créer un sas de connection à votre service en ligne (MySafeip): https://linuxfr.org/news/mysafeip-un-tiers-de-confiance-pour-votre-pare-feu
sécuriser les services systemd linux: https://github.com/juju4/ansible-harden-systemd

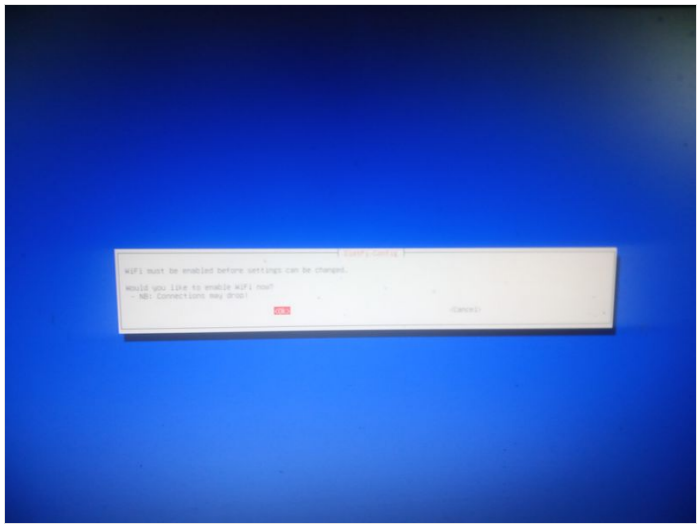
compiler un kernel :
https://doc.ubuntu-fr.org/tutoriel/comment_compiler_un_kernel_de_kernel.org
https://github.com/robertdebock/ansible-role-kernel

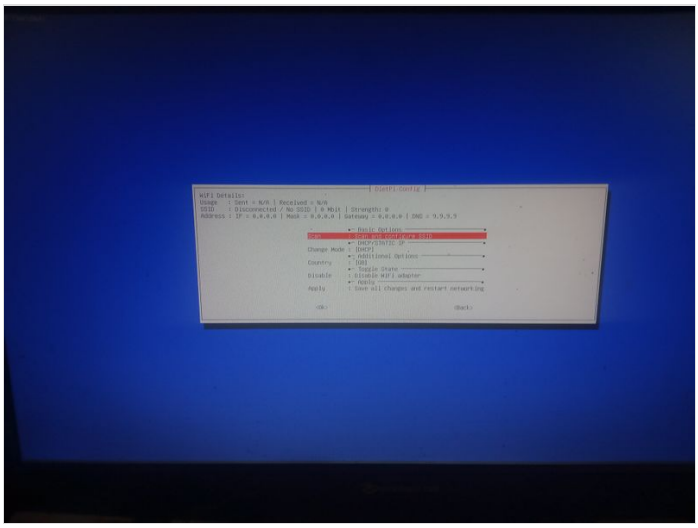
Étape 16 - Activer le wifi lors de l'installation (par exemple avec un raspberry)

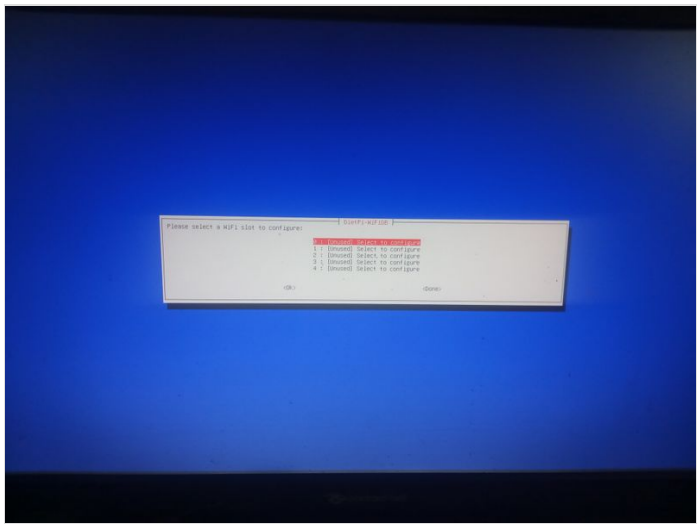
wpa2:
Lorsque vous démarrez pour la premiere fois votre raspberry avec dietpi sur la clé usb ou la carte sd, le programme d'installation va vous afficher un menu suite à une erreur ("Checking ipv4 network connectivity") [...] ping: connect: Network is unreachabel")

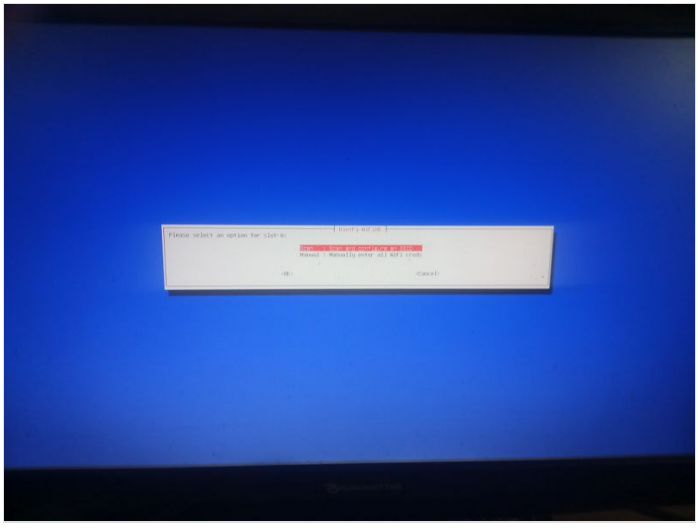
Aller alors dans "network-settings" puis suivez les menus indiqués dans les images jointes
wpa3: voir etape 6

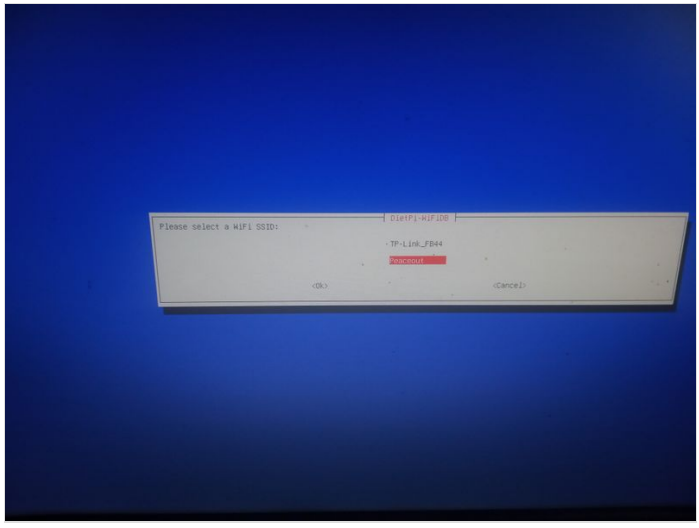












Notes et références

Pas de remerciements, c'est galère et on m'a pas aidé ;)
Le tuto et son contenu ne sont pas issus d'expertise ou de formation spécifique mais de bidouillages et d'informations glanées ça et là donc soyez indulgents ;)
Tout retour d'experience est bienvenu dans les commentaires