

Moonshine - Détails d'installation

1 Debian, Linux

Debian sera le système d'exploitation « Linux » du serveur (le système d'exploitation, aussi appelé Operating System ou OS étant composé de Linux + des logiciels qu'on décidera d'installer autour).

Linux ayant pour rôle de gérer le matériel (pilotes, interactions avec les disques, cartes etc), tandis que les logiciels (bureaux, explorateurs de fichiers, etc) fonctionnent par dessus Linux (et interagissent avec nous).

Debian a la capacité de gérer tout ce qui devrait nous intéresser (administration 100 % réalisable par réseau, mises à jour automatiques, serveur de fichier, compatibilité avec logiciel de sauvegarde, de vidéo surveillance, RAID, VPN, etc...)

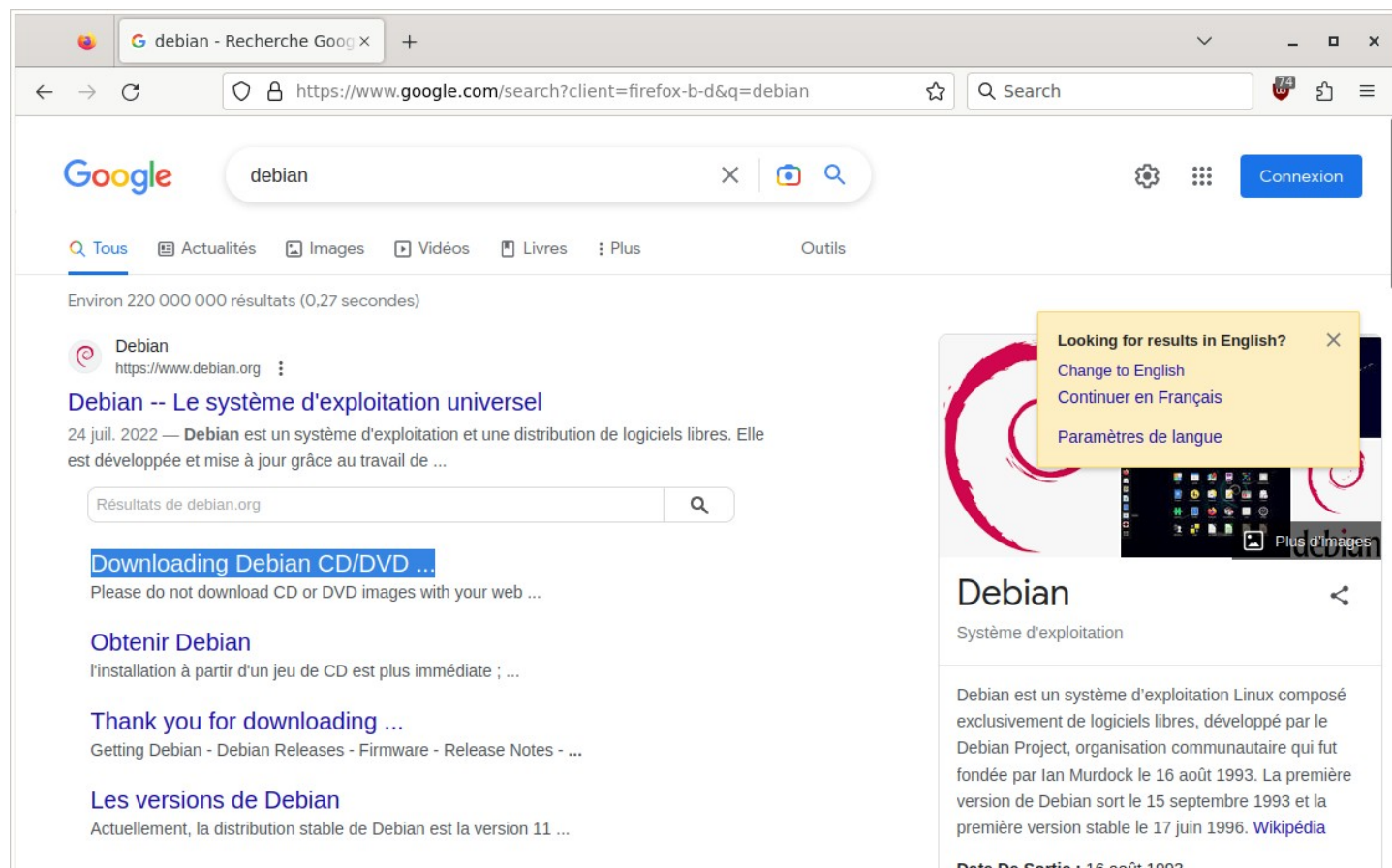
Il existe d'autres systèmes d'exploitation PC basés sur Linux (Ubuntu, Fedora, CentOS, Arch etc). Debian est généralement moins bugué, et souvent utilisé en serveur, le rendant mieux documenté sur Internet pour cet usage. En contre partie il est souvent moins avant-gardiste que les autres.

2 Téléchargement de Debian « Net Installer »

La version « Net installer » de Debian a pour intérêt de n'embarquer aucun superflu, en n'embarquant que le strict minimum pour démarrer le PC, permettant ensuite de n'installer que ce qu'on décide.

En contre partie, il faudra savoir exactement ce dont on a besoin pour composer le système d'exploitation, et le premier démarrage se fera en ligne de commandes.

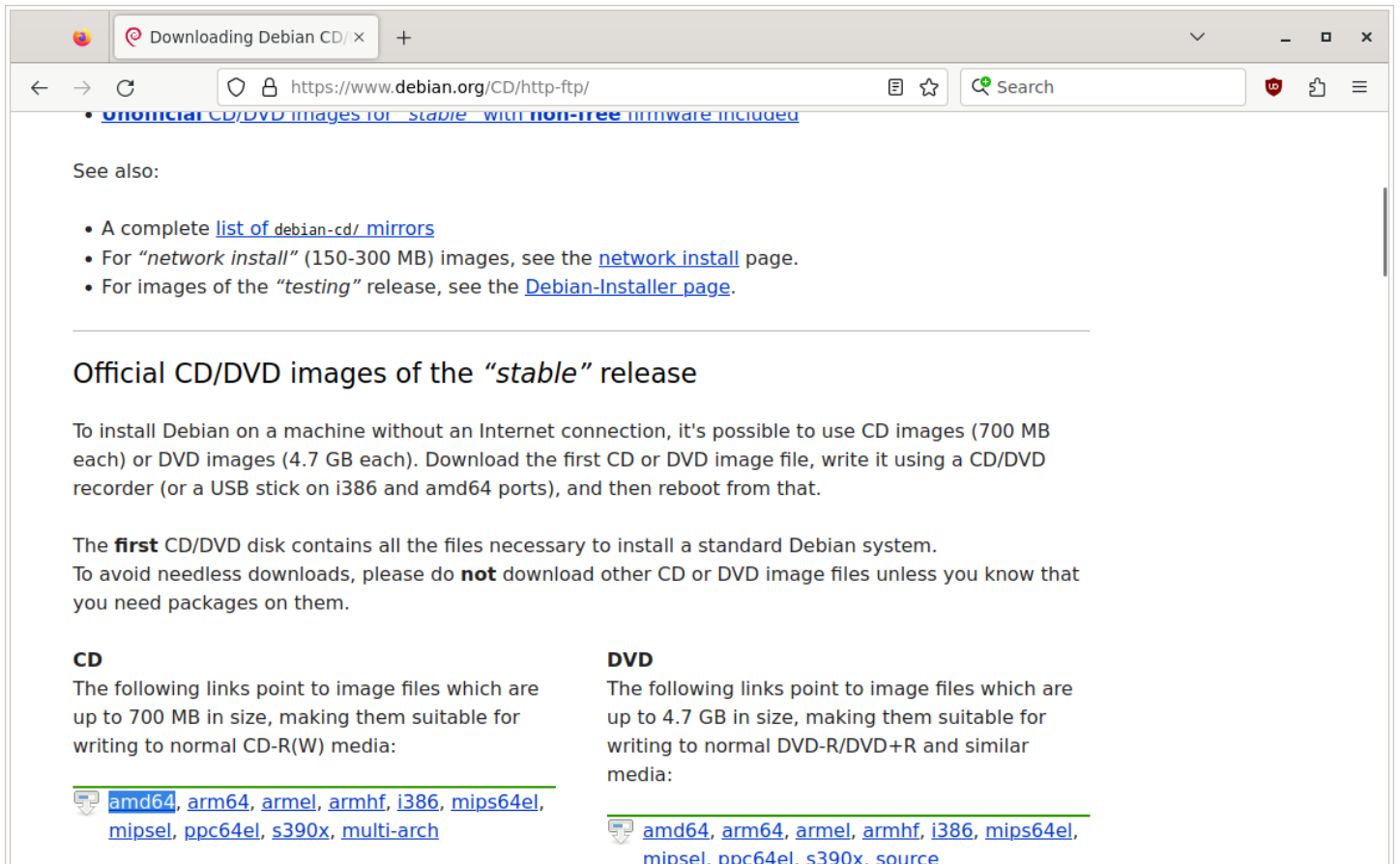
Chercher « Debian » sur Google :



The screenshot shows a Google search for 'debian' on a Firefox browser. The search results page displays the Debian website as the top result. The search bar contains 'debian' and the URL is 'https://www.google.com/search?client=firefox-b-d&q=debian'. The search results show 'Debian -- Le système d'exploitation universel' with a description: '24 juil. 2022 — Debian est un système d'exploitation et une distribution de logiciels libres. Elle est développée et mise à jour grâce au travail de ...'. Below the main result, there are several links: 'Downloading Debian CD/DVD ...', 'Obtenir Debian', 'Thank you for downloading ...', and 'Les versions de Debian'. On the right side, there is a knowledge panel for Debian, which includes a description: 'Debian est un système d'exploitation Linux composé exclusivement de logiciels libres, développé par le Debian Project, organisation communautaire qui fut fondée par Ian Murdock le 16 août 1993. La première version de Debian sort le 15 septembre 1993 et la première version stable le 17 juin 1996. Wikipédia' and the 'Date De Sortie : 16 août 1993'.

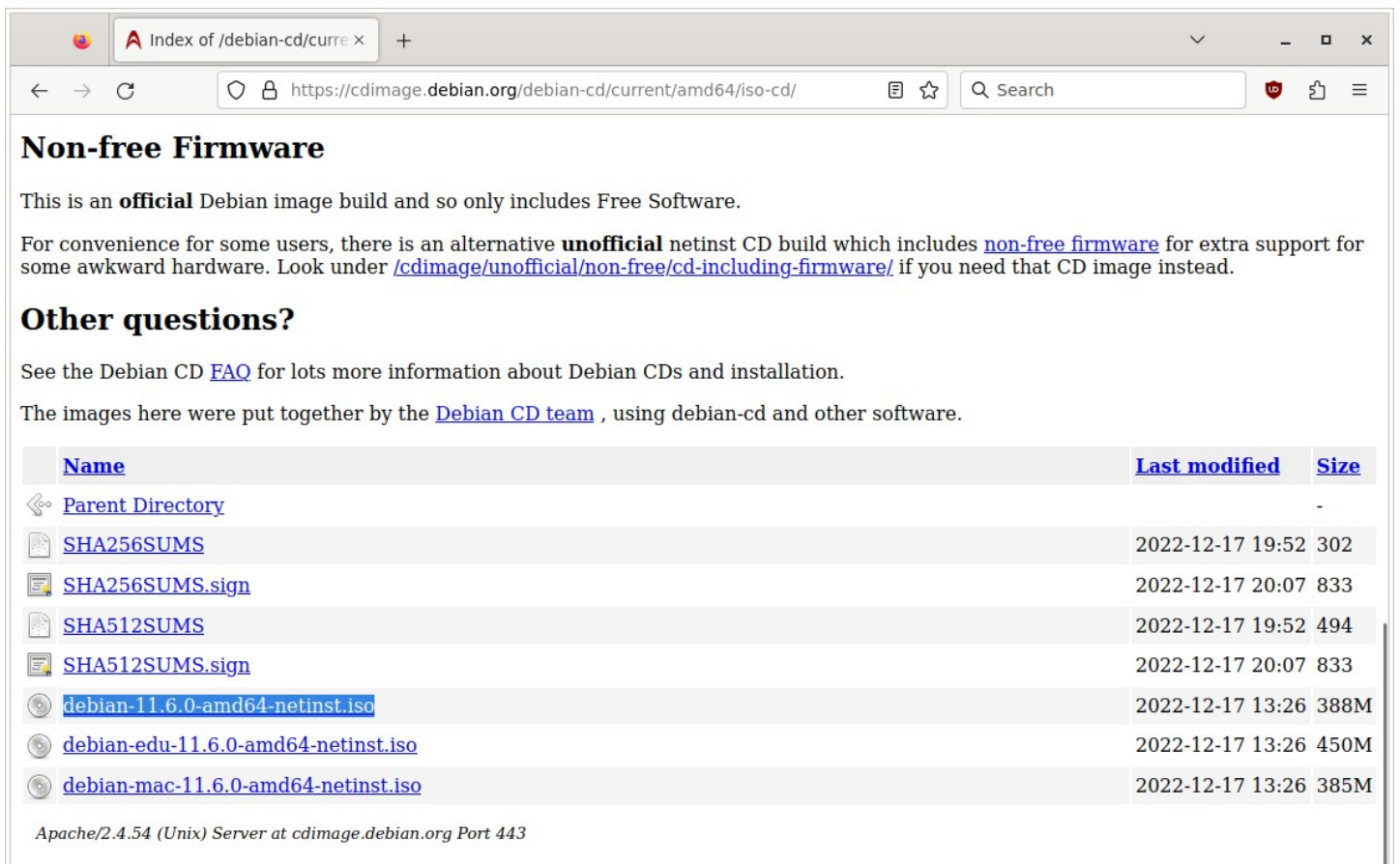
Les CPU Intel et AMD utilisent l'architecture x86_64 (aussi appelée amd64) depuis près de 20 ans (déjà...)

Choisir « **amd64** » dans le coin « **CD** »



The screenshot shows a web browser window with the URL <https://www.debian.org/CD/http-ftp/>. The page content includes a link to "Official CD/DVD images for stable with non-free firmware included", a "See also:" section with links to mirrors, network install, and testing release, and a main section titled "Official CD/DVD images of the 'stable' release". This section explains that CD images are 700 MB and DVD images are 4.7 GB. It notes that the first CD/DVD disk contains all necessary files. Below this, there are two columns: "CD" and "DVD". The "CD" column lists architecture links: [amd64](#), [arm64](#), [armel](#), [armhf](#), [i386](#), [mips64el](#), [mipsel](#), [ppc64el](#), [s390x](#), and [multi-arch](#). The "DVD" column lists architecture links: [amd64](#), [arm64](#), [armel](#), [armhf](#), [i386](#), [mips64el](#), [mipsel](#), [ppc64el](#), [s390x](#), and [source](#).

La version qui nous intéresse n'est ni la «~~edu~~», ni la «~~mac~~», mais la version **normale** :



The screenshot shows a web browser window with the URL <https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/>. The page is titled "Index of /debian-cd/curre x" and contains a section "Non-free Firmware" with a note that the official build only includes Free Software. It also mentions an alternative "unofficial netinst CD build" which includes non-free firmware. Below this is a section "Other questions?" with a link to the FAQ. The main part of the page is a table listing files with columns for Name, Last modified, and Size.

Name	Last modified	Size
Parent Directory		-
SHA256SUMS	2022-12-17 19:52	302
SHA256SUMS.sign	2022-12-17 20:07	833
SHA512SUMS	2022-12-17 19:52	494
SHA512SUMS.sign	2022-12-17 20:07	833
debian-11.6.0-amd64-netinst.iso	2022-12-17 13:26	388M
debian-edu-11.6.0-amd64-netinst.iso	2022-12-17 13:26	450M
debian-mac-11.6.0-amd64-netinst.iso	2022-12-17 13:26	385M

Apache/2.4.54 (Unix) Server at cdimage.debian.org Port 443

3 Support d'installation

Bien que tout ça ait été initialement pensé pour graver des CD / DVD d'installation, et démarrer l'ordinateur à installer via son lecteur CD/DVD, aujourd'hui on utilise plus généralement des clés USB.

Les fichiers « iso » sont initialement faits pour être des images CD prêtes à être gravées, mais les « iso » de Linux sont généralement prêtes à fonctionner sur clé USB également.

Pour préparer une clé USB à partir d'un fichier « iso » d'installation de Linux, télécharger « balena Etcher »

The screenshot shows a Google search for "balena etcher". The search results include a link to the official website, a description of Etcher as a cross-platform tool, and a download link for Windows. On the right, there is a preview of the Etcher software interface.

Google balena etcher Connexion

Tous Vidéos Images Actualités Shopping Plus Outils

Environ 252 000 résultats (0,21 secondes)

balena
<https://www.balena.io/etcher> · Traduire cette page

Etcher - Flash OS images to SD cards & USB drives
A cross-platform tool to flash OS images onto SD cards and USB drives safely and easily. Free and open source for makers around the world.

Clubic
<https://www.clubic.com/telecharger-fiche433933-etc...>

Télécharger Etcher (gratuit)
Etcher est solution simple d'utilisation, rapide et sans erreur pour créer des cartes SD et des clés USB de démarrage. Elle est utile pour « graver » une ...

Système d'exploitation : Windows Dernière mise à jour : 13/01/2023
★★★★★ Note : 3,7 - 101 votes · Gratuit · Windows · Utilitaires/Outils

uptodown.com
<https://etcher.fr.uptodown.com/windows>

balenaEtcher pour Windows

Etcher
Logiciel

Etcher est un logiciel libre, développé avec Electron, de gravure d'images sur différents supports clé USB, Carte SD, pour GNU/Linux, Windows, MacOS. Etcher est simple d'utilisation et assure une gravure efficace grâce à sa fonction de vérification de l'image gravée.

Depuis un ordinateur sous Windows, télécharger la version pour Windows (même pour faire une clé Linux) :

The screenshot shows the balena.io website's download page for Etcher. It features a navigation menu, a hero section with three key features, and a table of download links for various operating systems and architectures.

balena More Products Resources Customers & Partners Pricing Contact Login Sign Up

Open source
Made with JS, HTML, node.js and Electron. Etcher is built on open source tools and is and always will be free and open source to use!

Cross Platform
Works for everyone whether you are on Windows, Linux or Mac with no complicated install instructions.

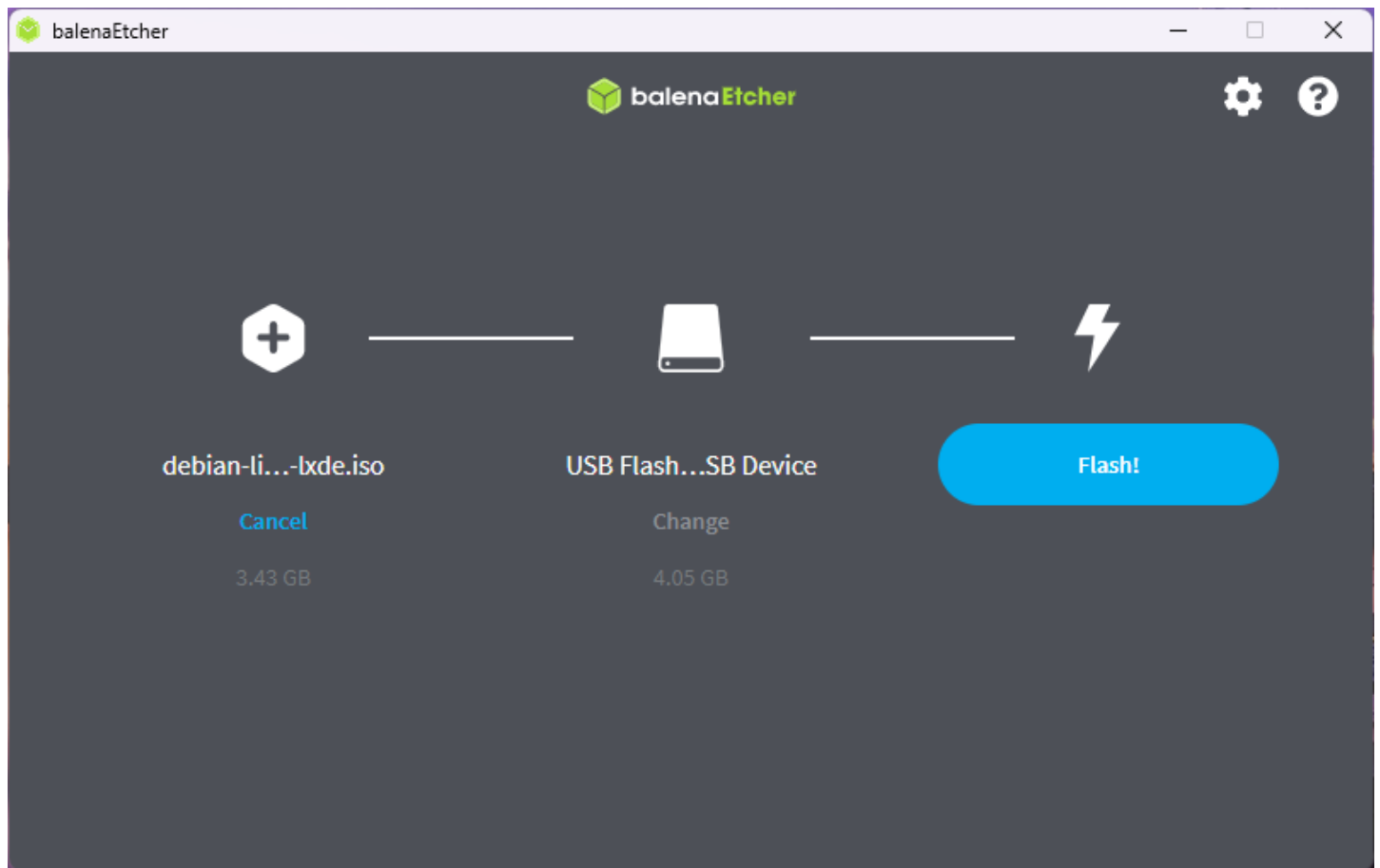
Simultaneous writing
Using balena EtcherPro you can flash up to 16 drives at once. Find out more here.

DOWNLOAD

Download Etcher

ASSET	OS	ARCH	
ETCHER FOR WINDOWS (X86 X64) (INSTALLER)	WINDOWS	X86 X64	Download
ETCHER FOR WINDOWS (X86 X64) (PORTABLE)	WINDOWS	X86 X64	Download
ETCHER FOR WINDOWS (LEGACY 32 BIT) (X86 X64) (PORTABLE)	WINDOWS	X86 X64	Download
ETCHER FOR MACOS	MACOS	X64	Download
ETCHER FOR LINUX X64 (64-BIT) (APPIMAGE)	LINUX	X64	Download

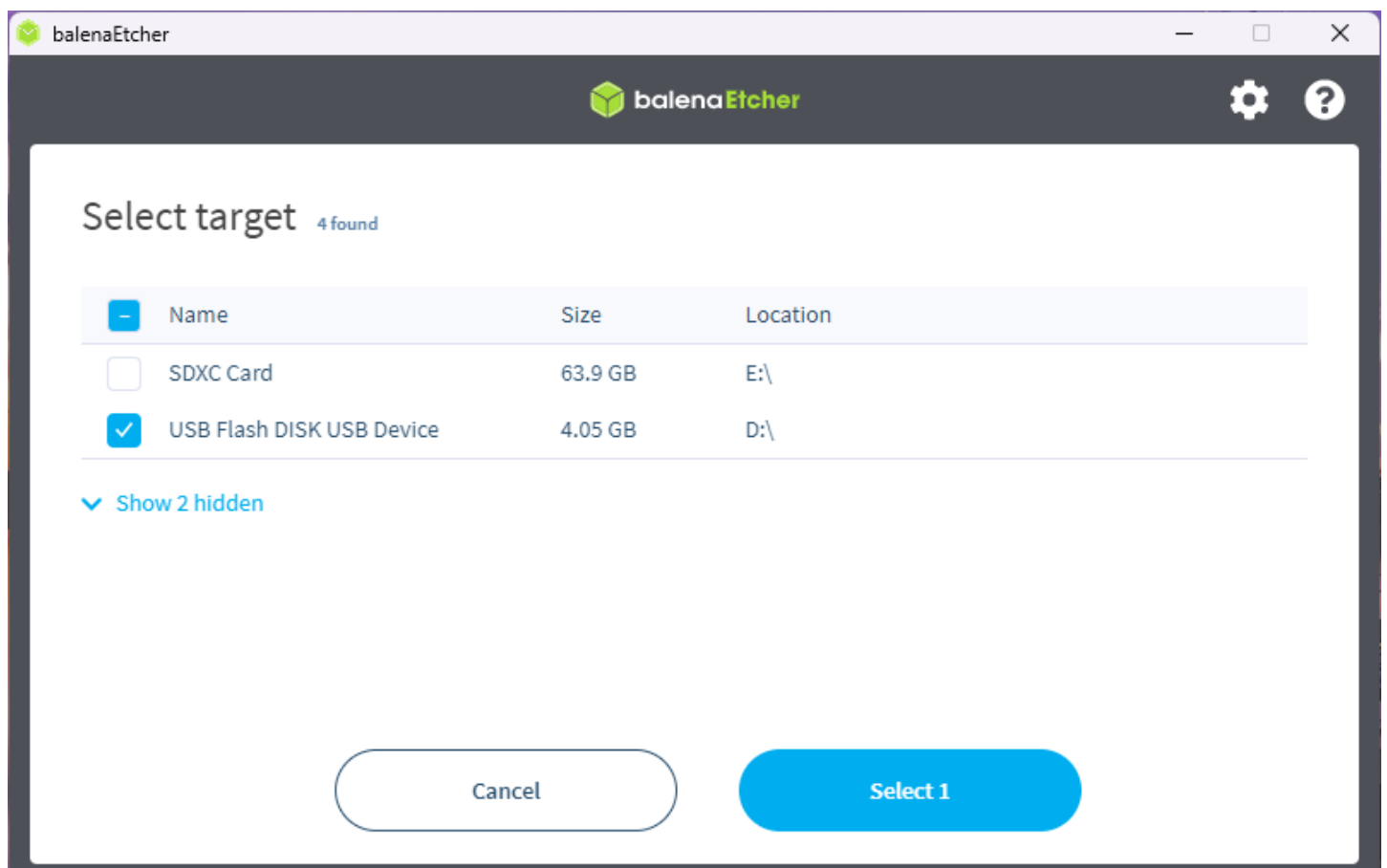
Installer et lancer le logiciel.



Attention, la clé USB qu'on veut transformer en clé d'installation va être effacée !

Pour re-transformer la clé USB en clé normale plus tard, c'est toujours possible, mais rarement intuitif.

Fournir le fichier « iso » téléchargé, et attention à bien sélectionner la clé USB destination qu'on va écraser.



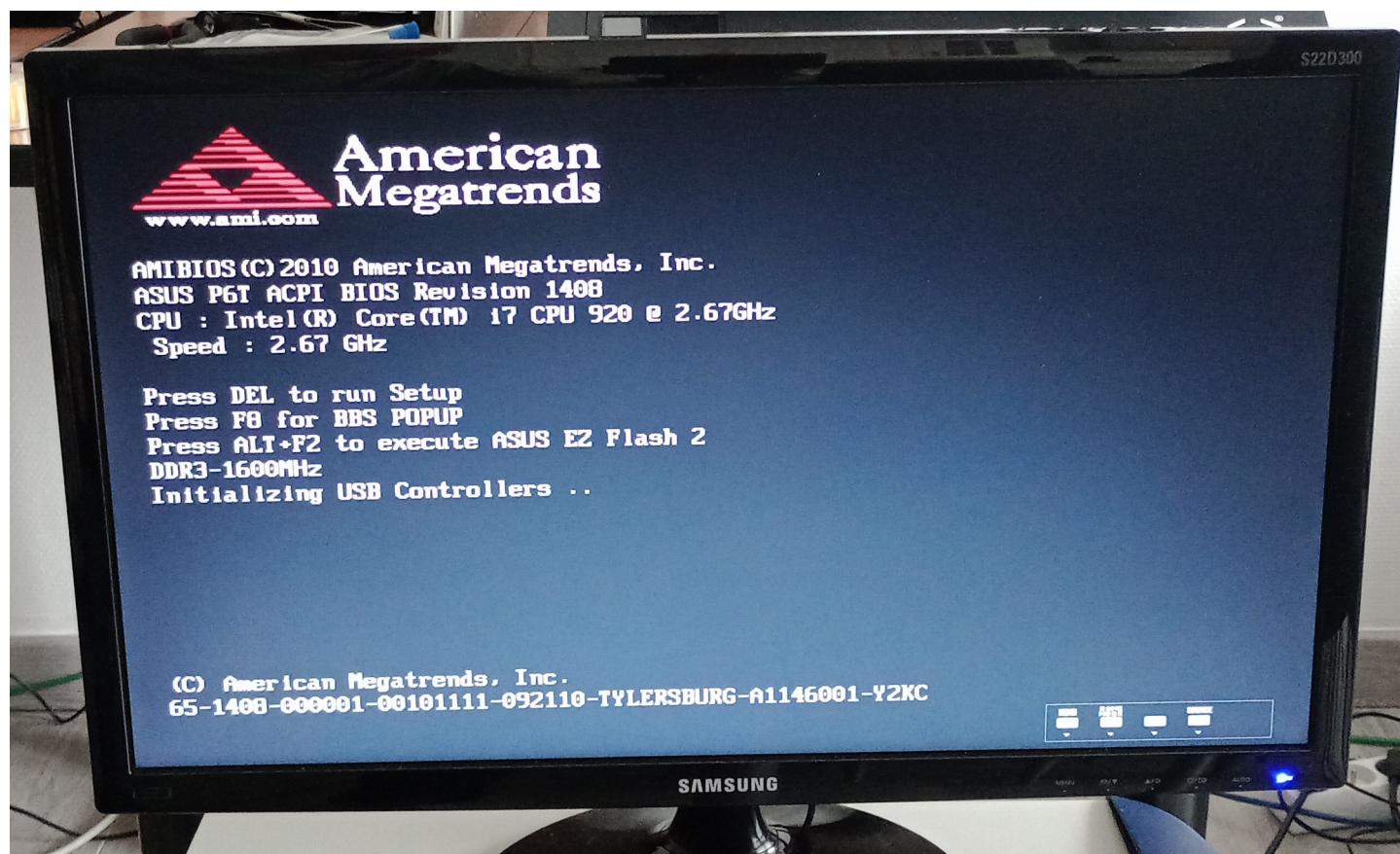
4 Réglage du PC serveur avant installation

Ci-dessous, ce qu'affiche le PC à sa mise sous tension.

Même en l'absence de disques durs et SSD, ce programme sera présent, car embarqué dans la carte mère.

On appelle ça le BIOS (parfois appelé EFI ou UEFI dans ses version modernes).

Les réglages qu'on y fait sont maintenus en mémoire à l'aide de la pile CR2032 (qui maintient aussi l'heure).



Bien noter :

- La touche « **Suppr** » (« **DEL** » en anglais) pour Supprimer (ou Delete en anglais) entre dans le menu de configuration appelé **Setup**, ou « **BIOS Setup** » : on va y faire un tour.
- La touche « **F8** » permet d'ouvrir un « **Popup** » de sélection pour le démarrage (aussi appelé **Boot Menu**). C'est très utile pour démarrer ponctuellement sur une clé USB par exemple, sans devoir modifier la configuration BIOS.

A savoir : tous les ordinateurs n'utilisent pas toujours ces touches pour le Bios Setup ou le Boot Menu.

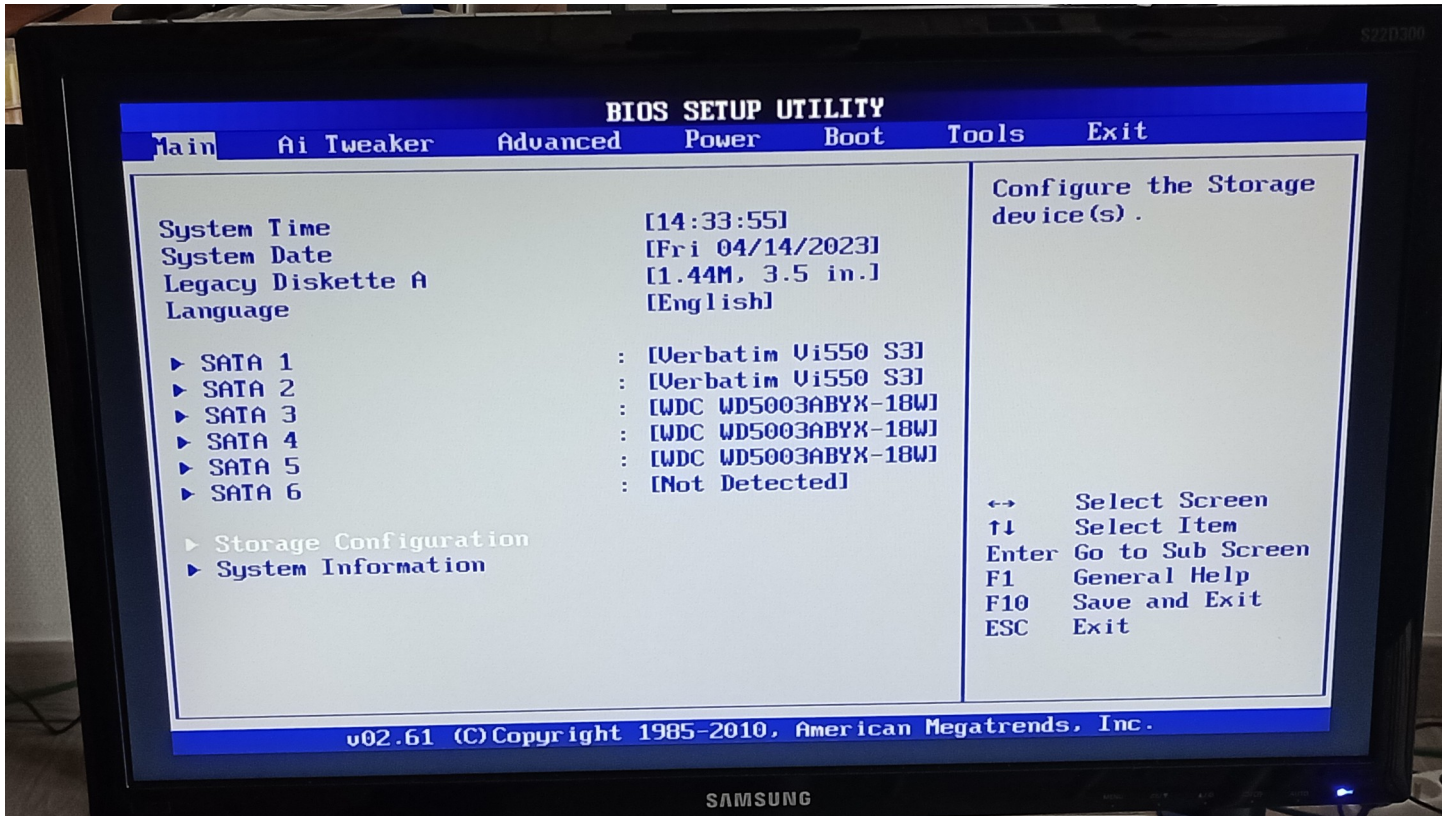
On va configurer le BIOS de façon à ce que ce soit lui qui gère le RAID des 2 SSD sur lequel le système d'exploitation sera installé.

On utilisera un RAID « Miroir » aussi appelé RAID-1.

De cette façon, en cas de souci avec les SSD (impactant le système d'exploitation), ou en cas d'opération sur ce RAID qui serait impossible pendant le fonctionnement du système d'exploitation, les menus du BIOS permettront de gérer ça sans avoir besoin de démarrer Linux. Linux gèrera ensuite le RAID-5 des 3 HDD.

La première chose à faire est d'**appuyer plein de fois sur « Suppr » pour rentrer dans le BIOS Setup**. En effet, le clavier n'étant pas forcément initialisé tout de suite, les premiers appuis ne fonctionnent pas toujours.

4.1 BIOS Setup

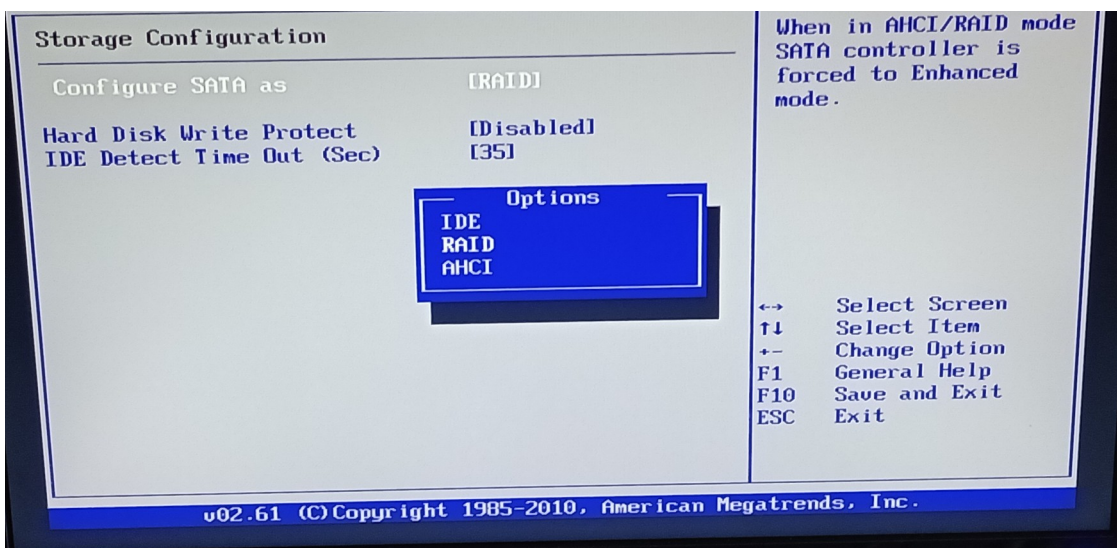


À savoir : rien n'est sauvegardé tant qu'on ne demande pas à enregistrer les changements. Il est donc tout à fait possible de naviguer dans le BIOS Setup dans le simple but de découvrir tout ce qui s'y cache, et ce, sans rien casser.

Pour naviguer dans les différents onglets (Main, Ai Tweaker, Advanced, Power, Boot, Tools et Exit) il faut utiliser les flèches « gauche » et « droite ».

Au sein d'un onglet, c'est les flèches « haut » et « bas » qu'il faut utiliser, et « Entrée » permet d'ouvrir un petit menu pour voir quels sont les réglages / sous menus disponibles. « Échap » pour revenir en arrière.

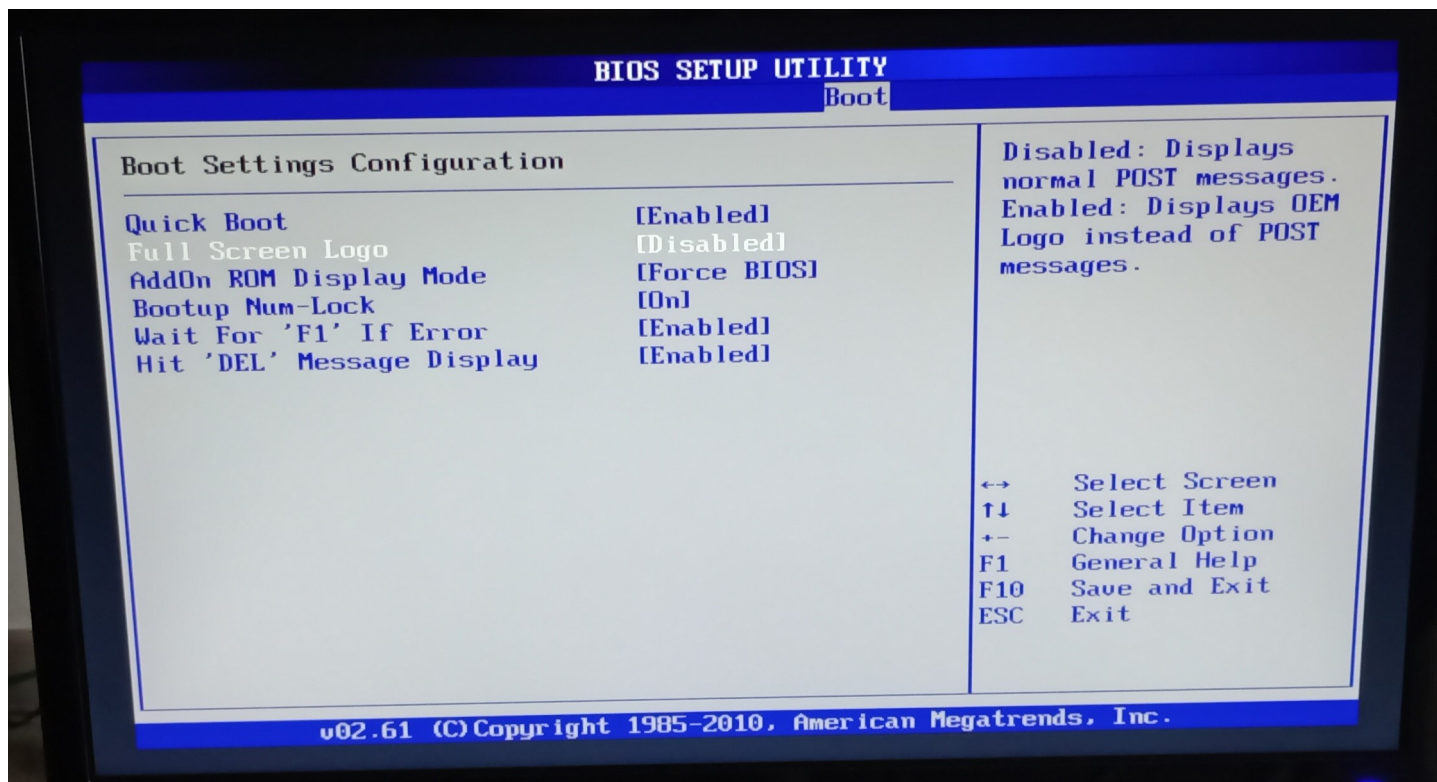
Depuis le premier onglet « **Main** », aller dans « **Storage Configuration** »



En face de « **Configure SATA as** », sélectionner « **RAID** »

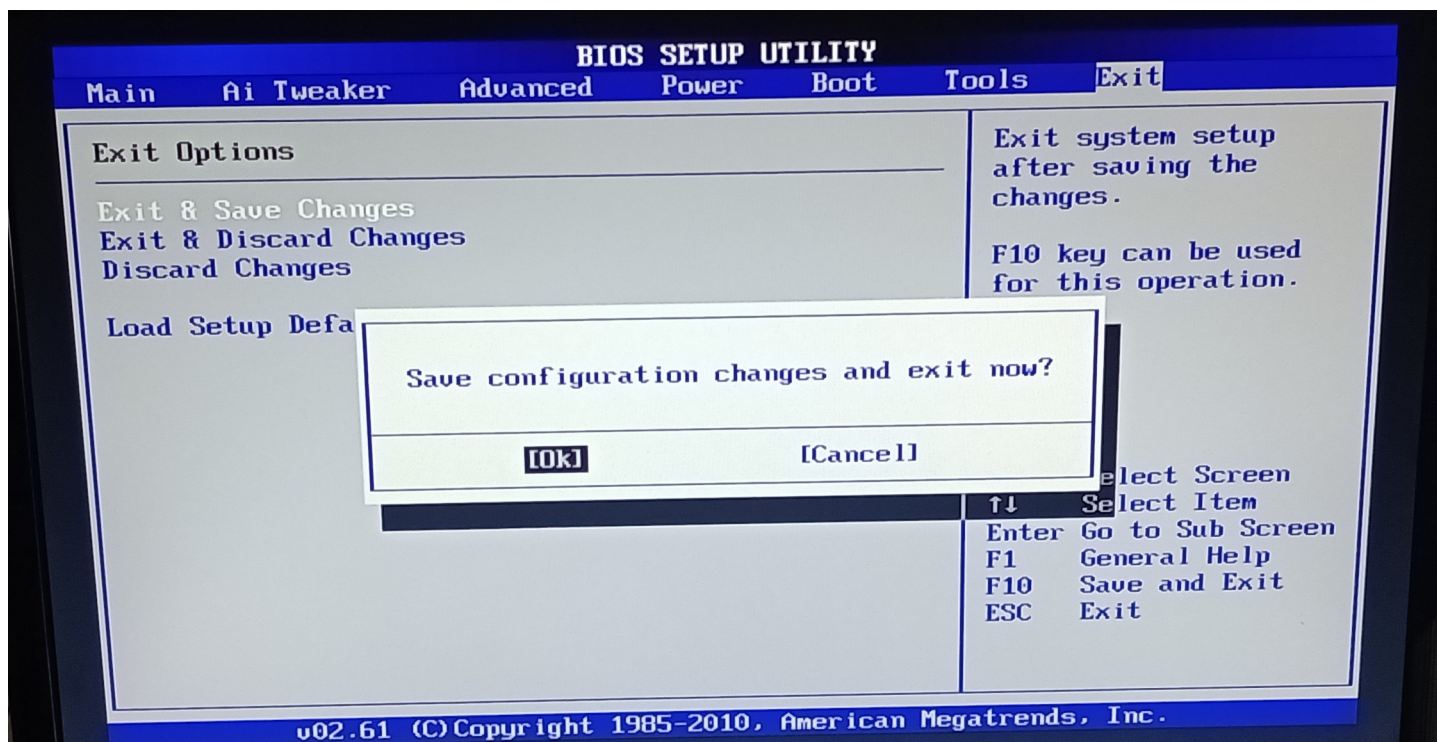
Optionnel :

Dans l'onglet « **Boot** » et dans « **Boot Settings Configuration** », on peut mettre « **Full Screen Logo** » sur « **Disabled** ». En effet le Full Screen Logo n'a aucun intérêt et quand il s'affiche, on ne peut plus voir quelle touche fait quoi (les fameuses touches Suppr, F8 etc qui ne sont pas les mêmes sur tous les PC).



Optionnel : Pour que le ventilateur CPU fasse moins de bruit, activer Q-Fan dans l'onglet « **Power** », « **Hardware Monitor** » puis « **CPU Q-Fan Control** » : mettre « **Enabled** » pour activer la régulation.

Une fois ces réglages effectués, aller dans le dernier onglet « **Exit** » puis « **Exit & Save Changes** » :

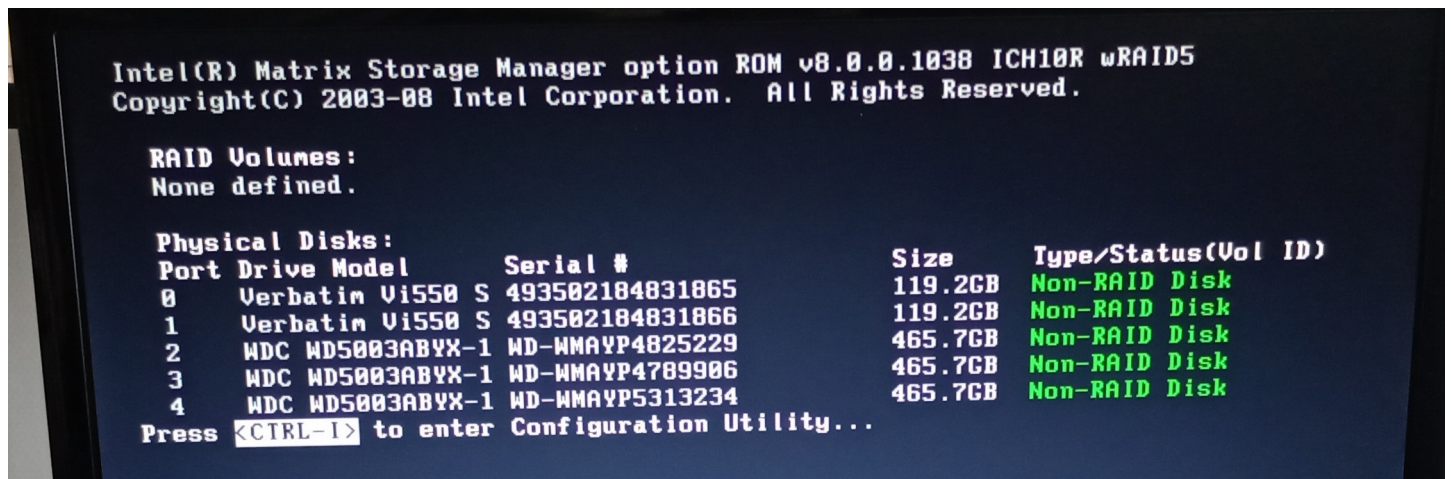


Au prochain démarrage, un écran supplémentaire s'affichera après le BIOS, pour gérer la configuration RAID.

4.2 Configuration RAID (BIOS)

Pour rappel, via le BIOS, on ne va gérer le RAID que des 2 SSD (qui contiendront le système d'exploitation).

Lorsque l'écran ci-dessous s'affiche, appuyer sur **Ctrl + i** pour rentrer dans le menu RAID



Parenthèse : à savoir en cas de changement de carte mère

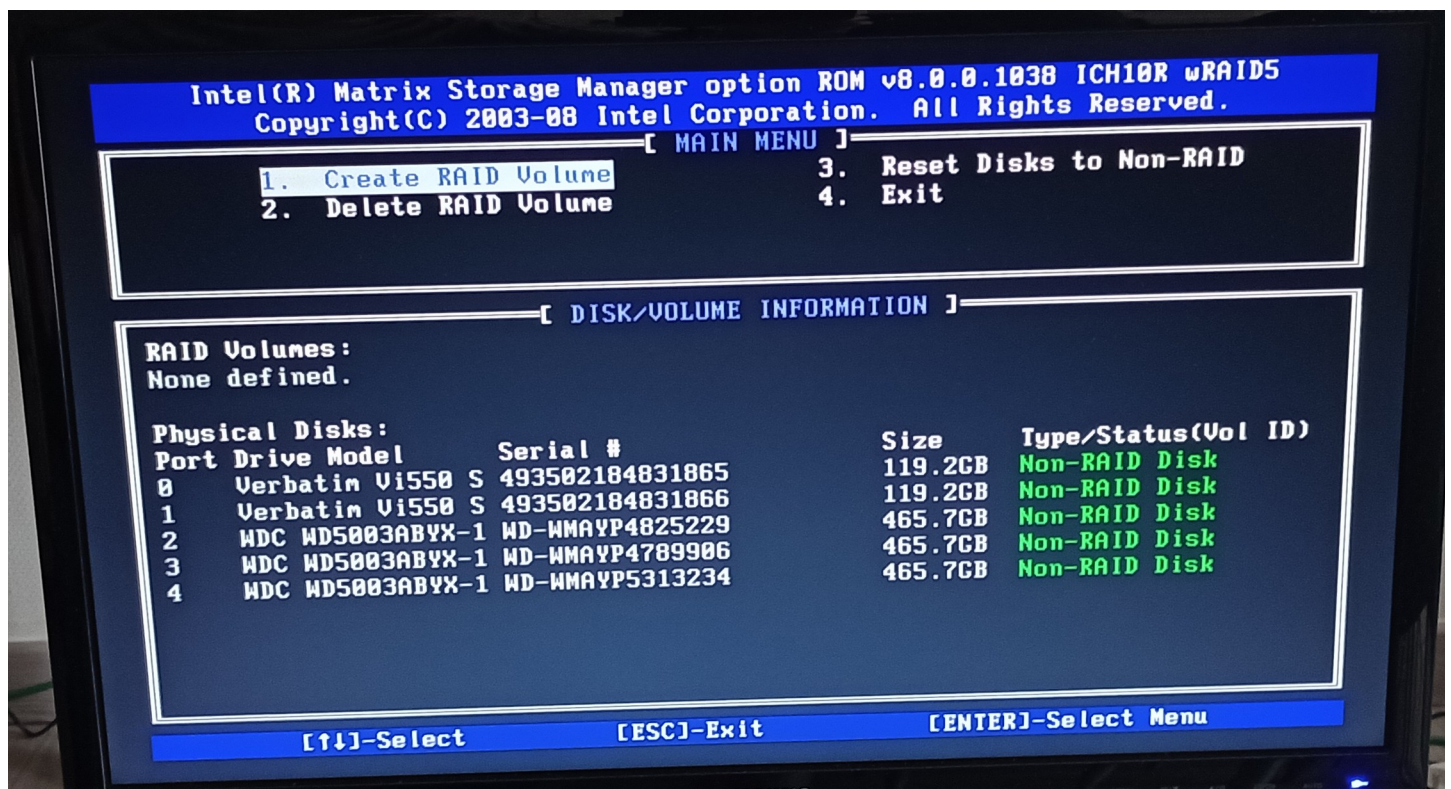
Cette fonctionnalité s'appelle ici « Intel Matrix Storage Manager » (Parfois abrégé **IMSM**).

Elle n'est pas présente sur toutes les cartes mères : en cas de changement de carte mère, en l'absence de cette fonctionnalité, on pourra toutefois démarrer un Linux sur clé USB, et même avec 1 seul SSD sur les deux, rendre possible de récupérer manuellement les données en utilisant la commande suivante :

```
IMSM_NO_PLATFORM=1 mdadm --assemble --scan --readonly --verbose
```

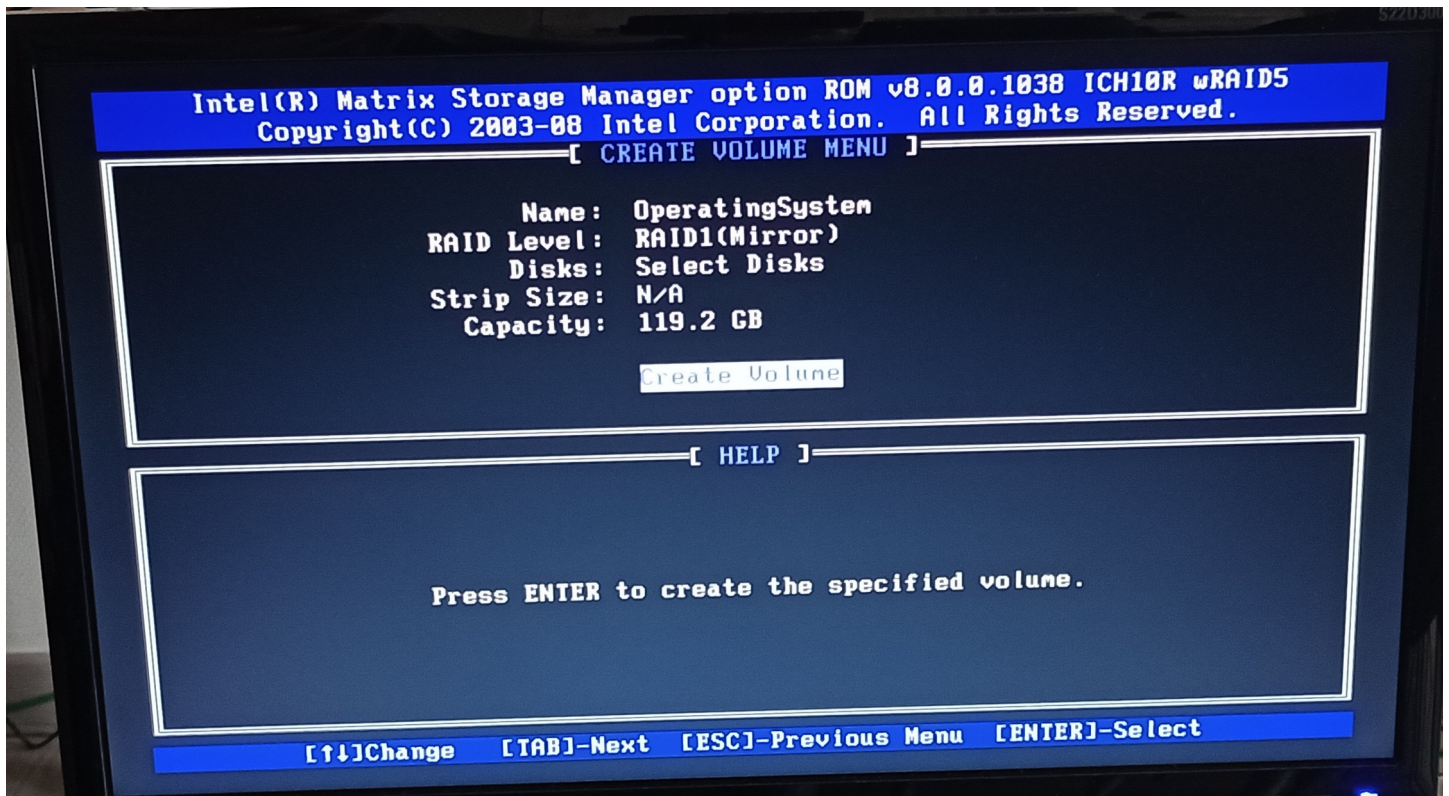
Ensuite on peut utiliser `gnome-disks`, puis un explorateur de fichier pour tout copier.

Un menu s'affiche, avec 4 choix possibles :

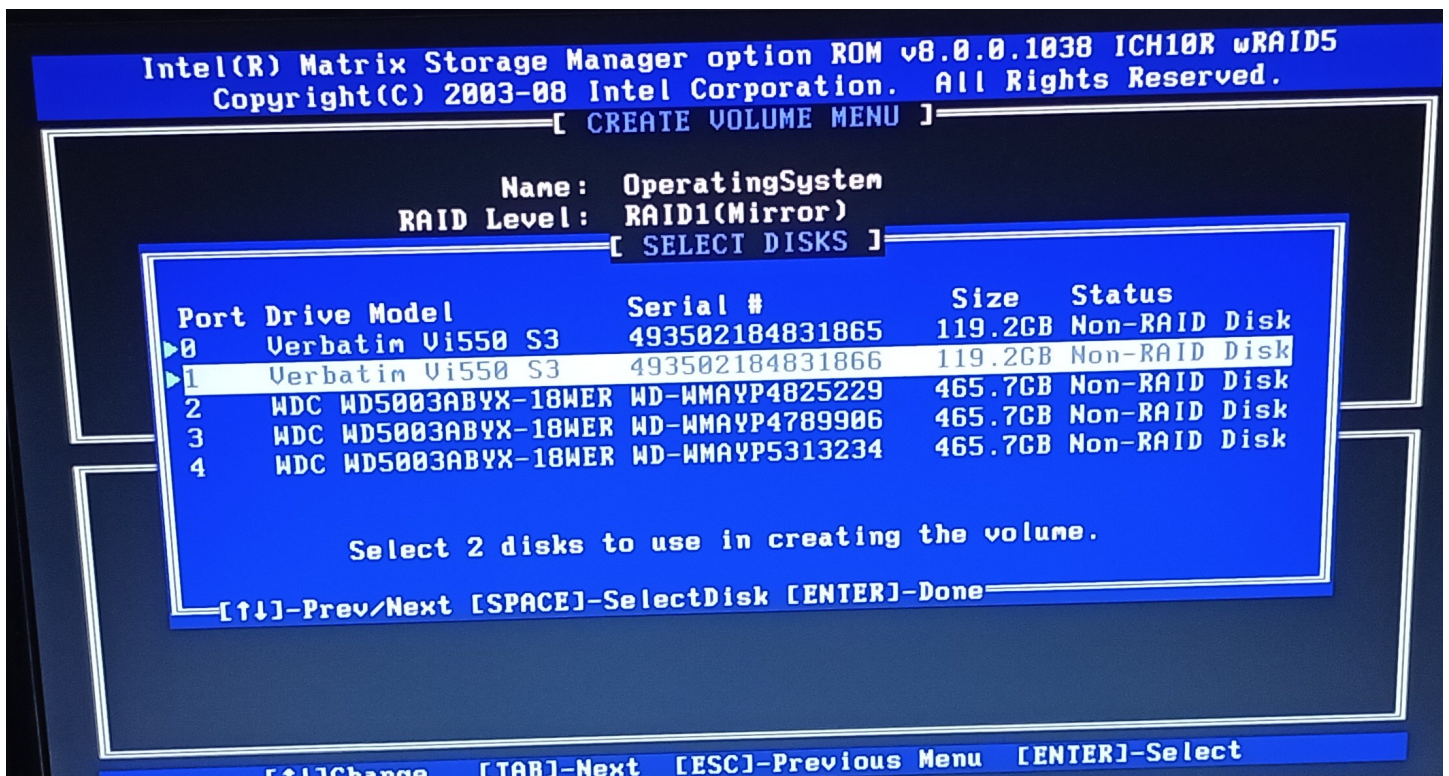


Sélectionner « **1. Create RAID Volume** » (ne le faire que si c'est pas déjà fait, et/ou s'il n'y a encore rien d'important sur les SSD utilisés, car cela va les écraser partiellement, et même écraser totalement l'un deux).

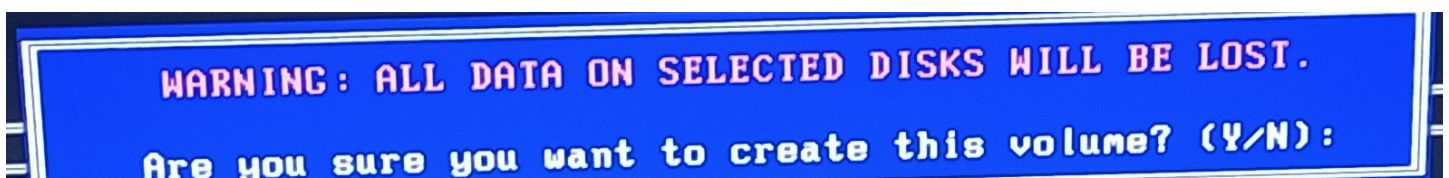
En face de « Name » on pourra mettre « OperatingSystem », pour RAID Level : « RAID1(Mirror) ».



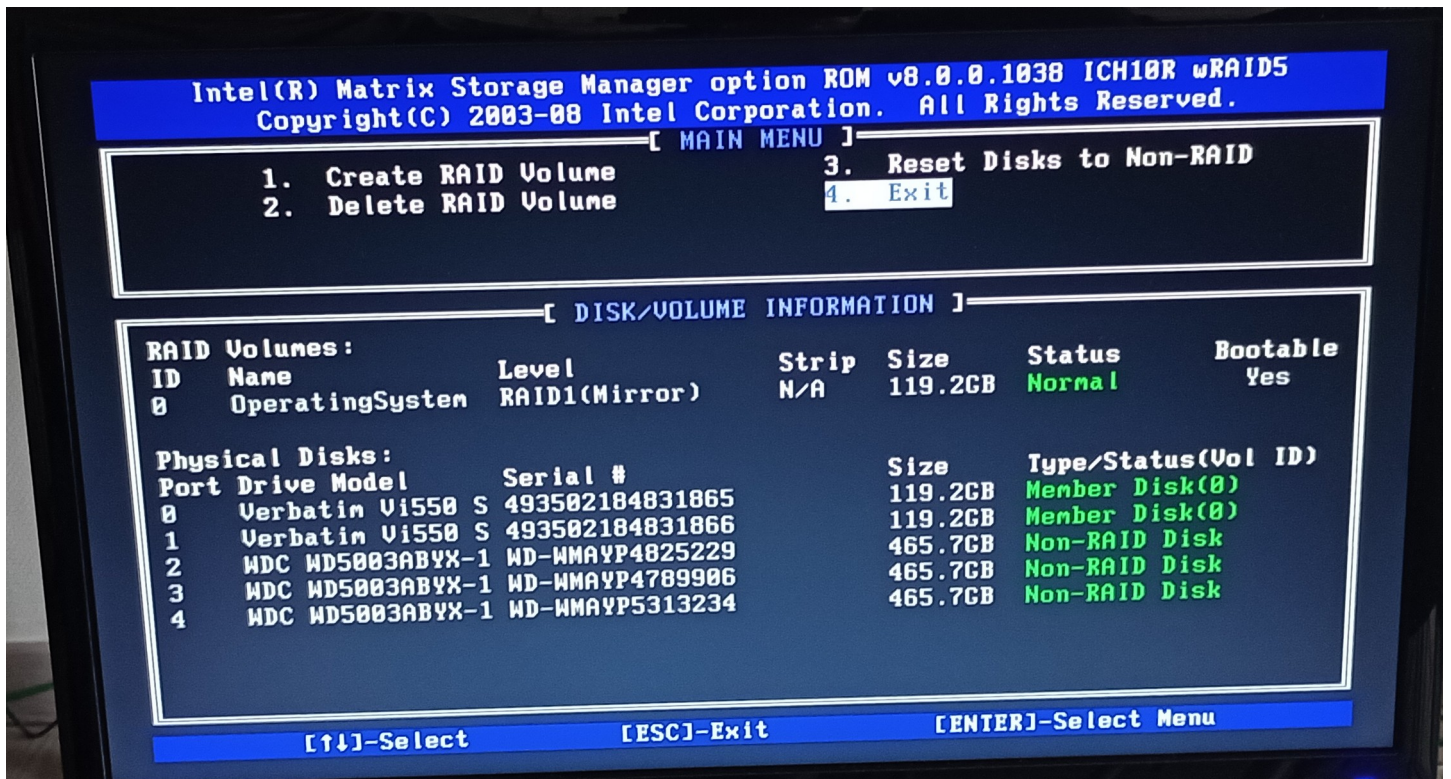
Dans « Select Disks », il faudra sélectionner nos deux SSD :



Puis valider la création.

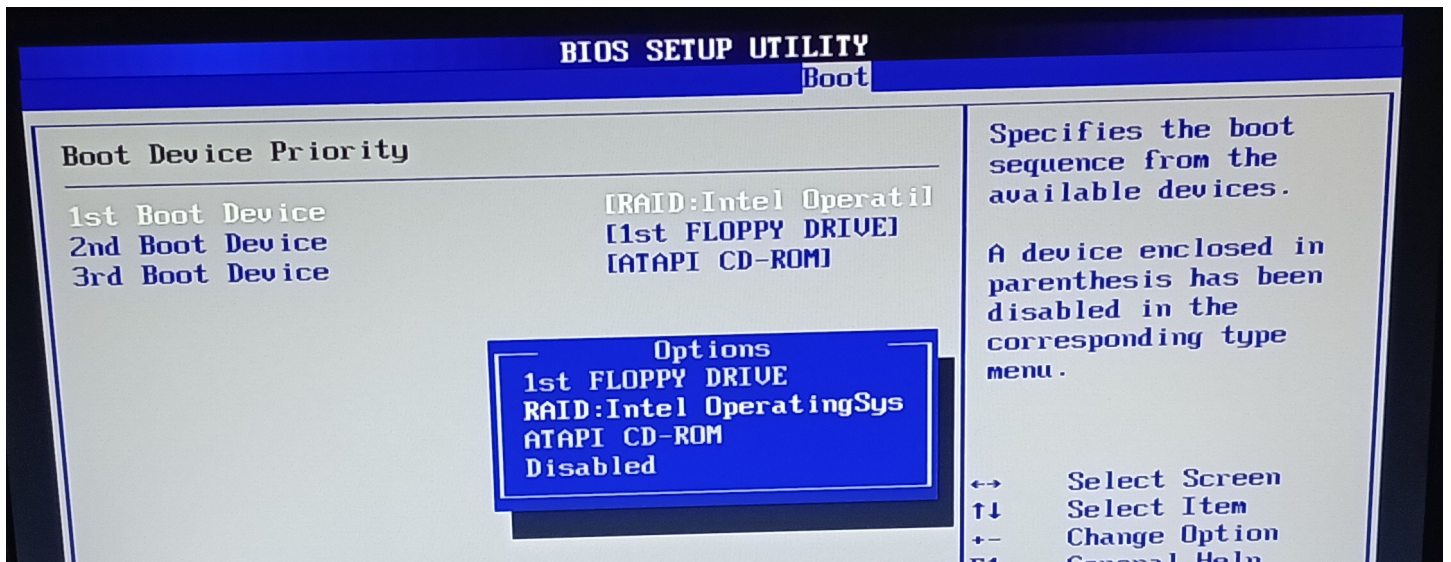


Une fois la création terminée, on peut aller dans « 4. Exit »



Au démarrage suivant, il faudra **retourner dans le BIOS** afin de mettre le « **RAID1 : OperatingSystem** » en périphérique de démarrage par défaut.

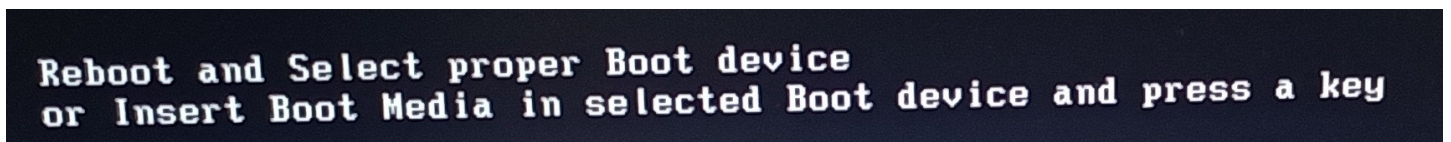
En effet parmi tous les disques, lecteurs de disquettes, CD/DVD possibles, il faut indiquer à l'ordinateur sur lequel d'entre eux il doit chercher à démarrer (il est trop bête pour choisir tout seul).



Onglet « **Boot** », puis « **Boot Device Priority** », choisir notre RAID fraîchement créé.

Ensuite aller dans « **Exit** » puis « **Exit & Save Changes** »

Au démarrage suivant, tout est prêt : il ne manque plus que le système d'exploitation

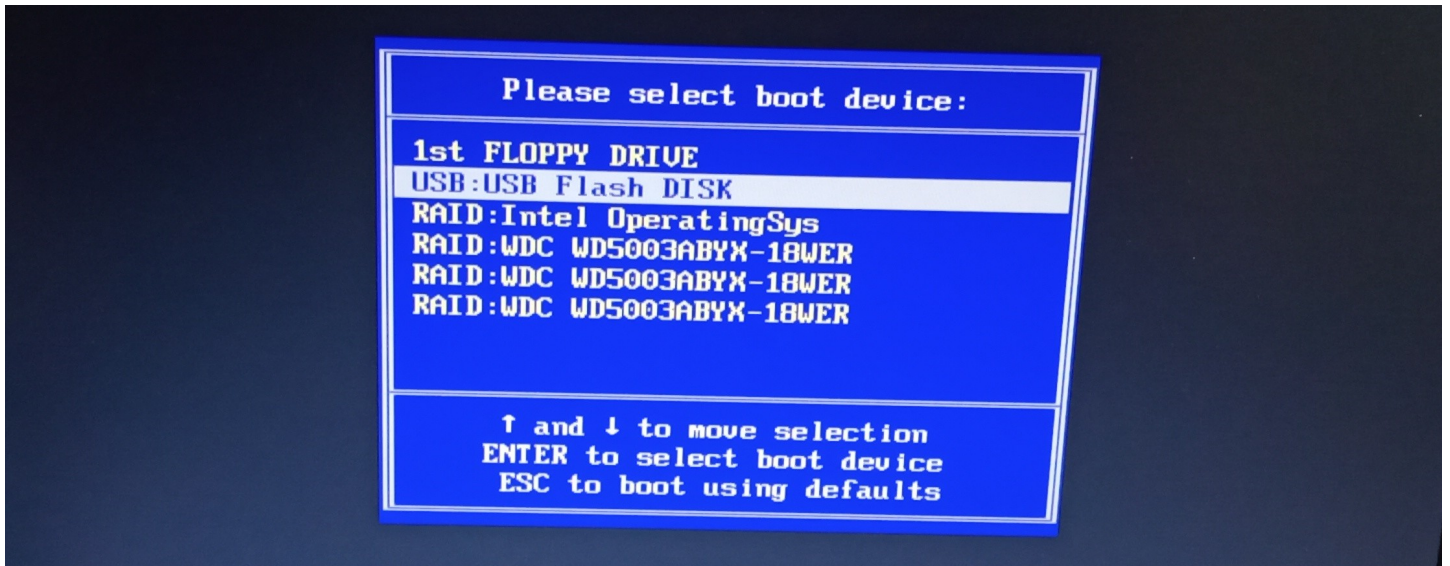


(Ce message date de l'époque où le PC démarrait automatiquement sur disquettes et CD-ROM)

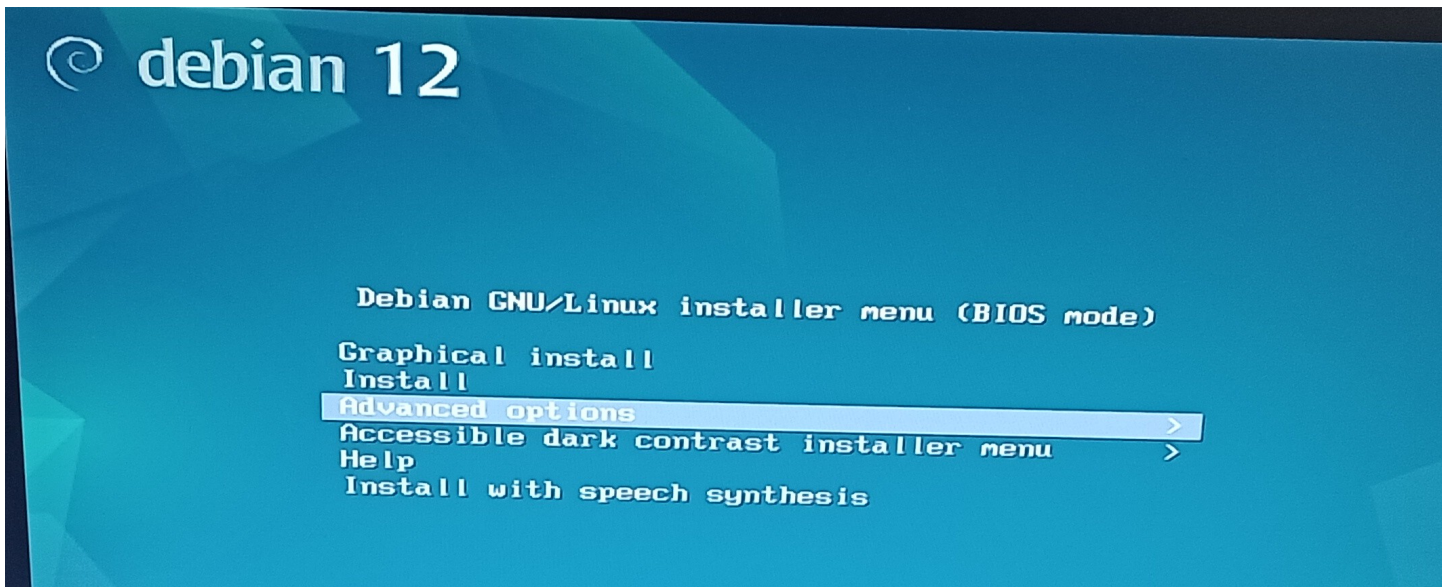
5 Installation de Debian

Brancher la clé USB d'installation au PC puis l'allumer (ou le redémarrer, via Ctrl Alt Suppr par exemple).

Au démarrage, pendant l'écran de BIOS, appuyer sur « **F8** » pour demander l'apparition du « **Boot Menu** »

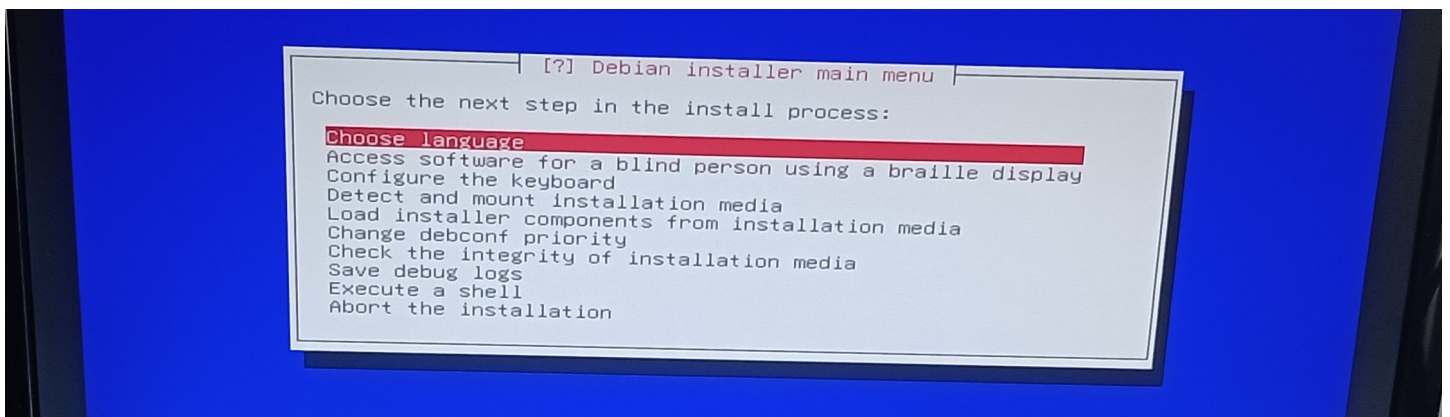


Ici, « **USB Flash DISK** » correspond à la clé USB préparée via balena Etcher quelques minutes plus tôt.



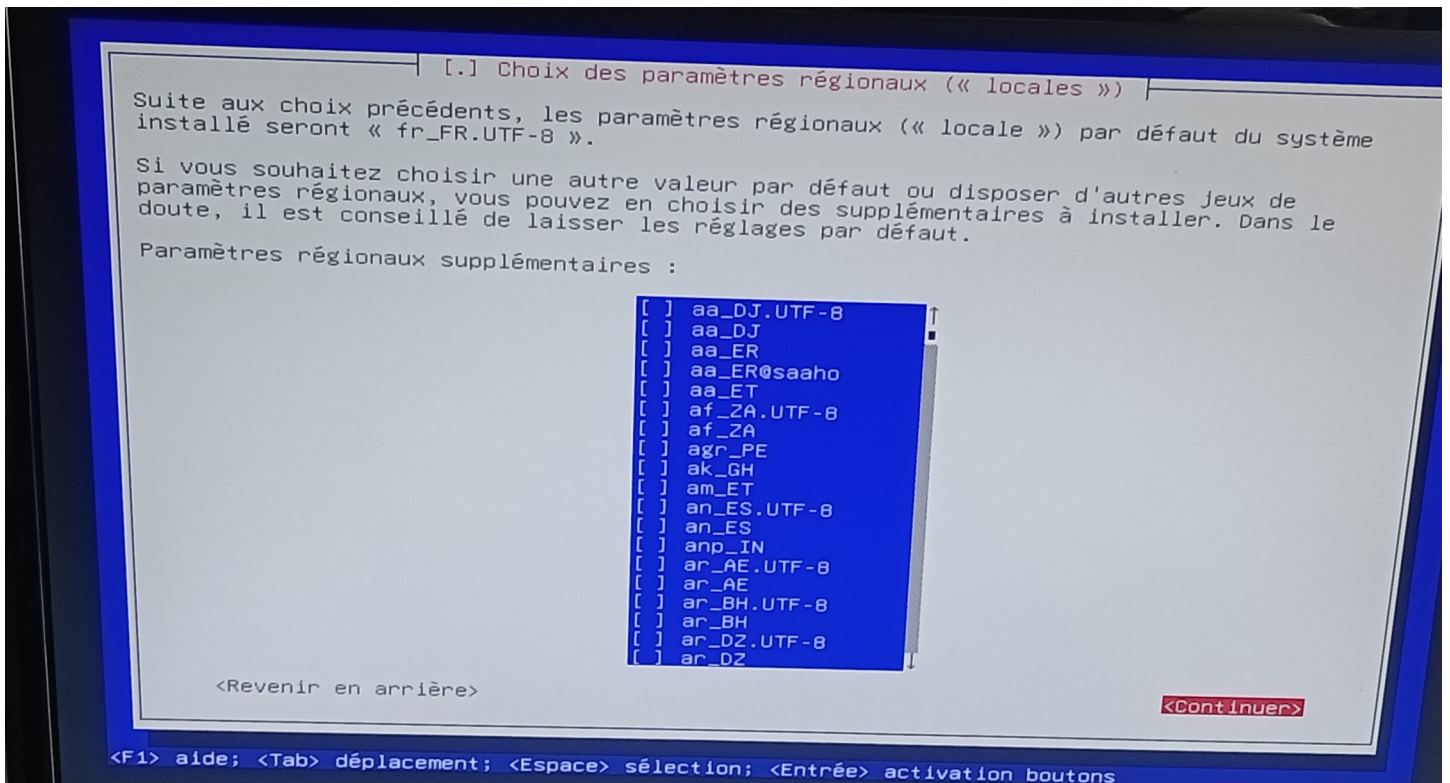
Choisir « **Advanced Options** » puis « **Expert Install** »

L'interface d'installation démarre alors, et ressemble à ça :



Dans « **Choose language** » sélectionner « **Français** », « **France** » puis « **France** ». Respectivement 3 réglages pour les options de langue, de localisation, puis paramètres régionaux (jeu de caractères).

Lorsque l'installateur propose de cocher d'autres cases, pas besoin : aller directement sur « **Continuer** » via la touche « **Tab** » puis « **Entrée** »

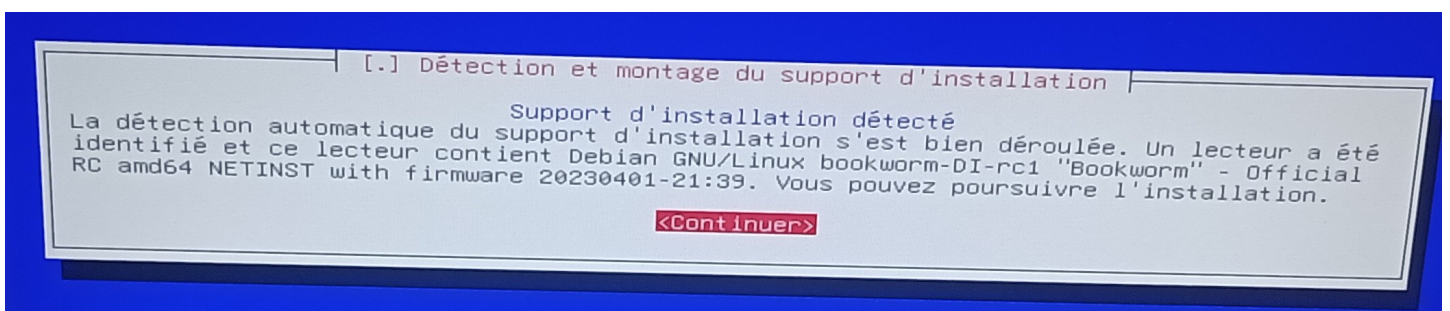


Dans « **Configurer le clavier** », choisir Français (ça passe le clavier en AZERTY)

Puis entrer dans « **Détection et montage du support d'installation** ». Sur des PC normaux, cette étape est transparente et ne pose pas de problème, il devrait trouver sa clé USB.

En cas d'échec, utiliser un autre port USB (arrive parfois sur de vieilles version de Linux avec du matériel trop récent, pas encore entièrement pris en charge par les versions actuelles de Linux – mais c'est rare).

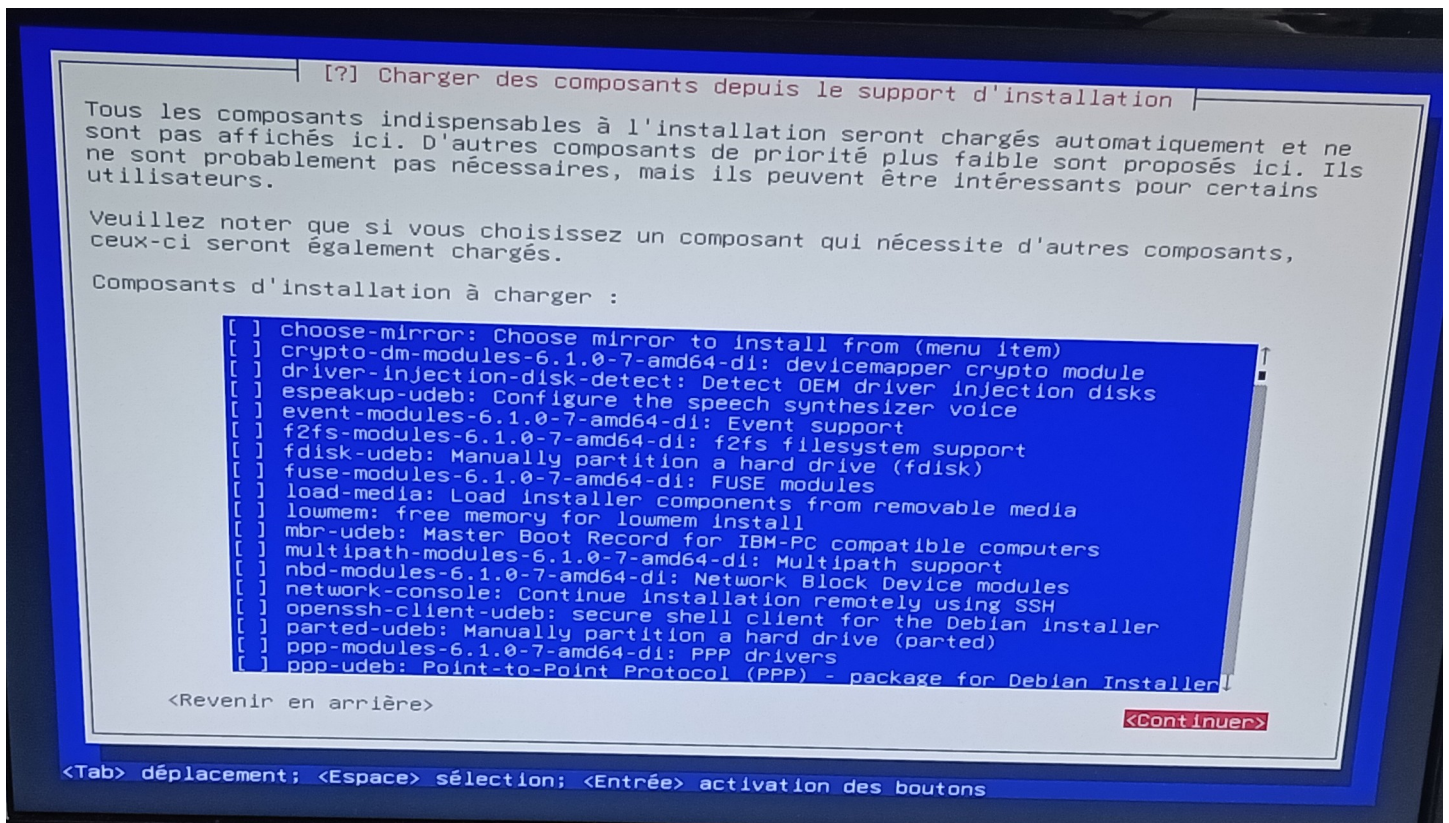
En effet, le BIOS a utilisé la clé USB pour charger la base de cet installateur en mémoire RAM, mais tous les fichiers d'installation sont sur la clé USB et c'est maintenant à l'installateur d'accéder à la clé USB.



Ensuite, sélectionner « **Charger des composants depuis le support d'installation** ».

Cela va charger de morceaux supplémentaire de l'installateur présents dans la clé USB, pour pouvoir continuer l'installation.

Aussi, cela proposera d'ajouter des modules supplémentaires en cas de besoin spécifique, mais sauf cas très spécifique, aucune case n'est à cocher.

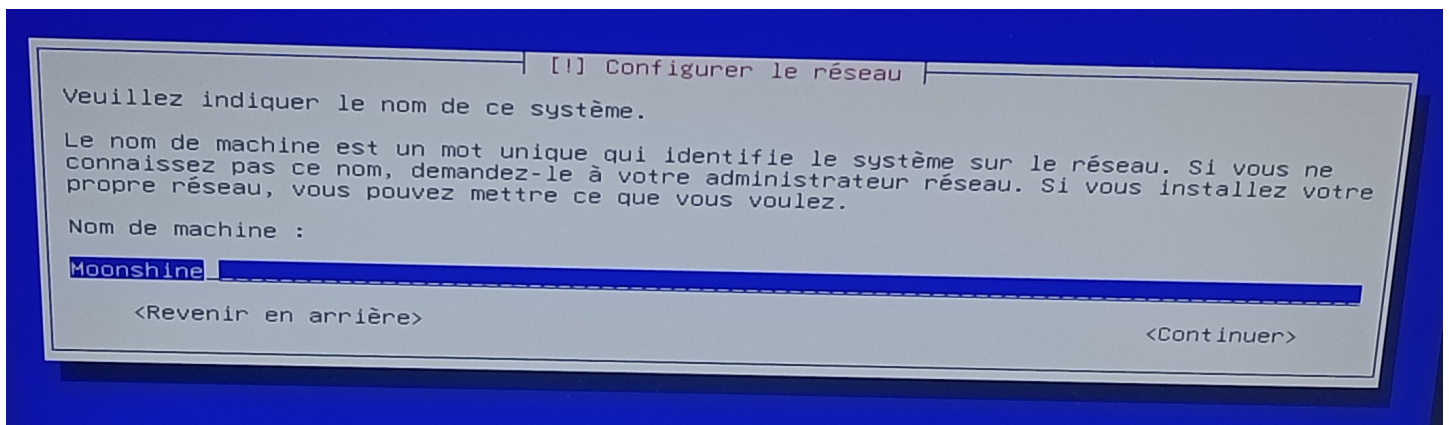


Aller directement sur « **Continuer** ».

Aller ensuite dans « **Détecter le matériel réseau** ».

Puis, dans « **Configurer le réseau** ». A la question « **Faut-il configurer le réseau automatiquement** », si le PC est relié à une box domestique normale, ou sur un routeur « DHCP » standard, répondre « **Oui** ».

Laisser les valeurs par défaut, et configurer le nom qu'aura la machine sur le réseau :



Dans « **Créer les utilisateurs et choisir les mots de passe** », répondre « **Oui** » aux questions liées au « superuser » et au compte utilisateur simple.

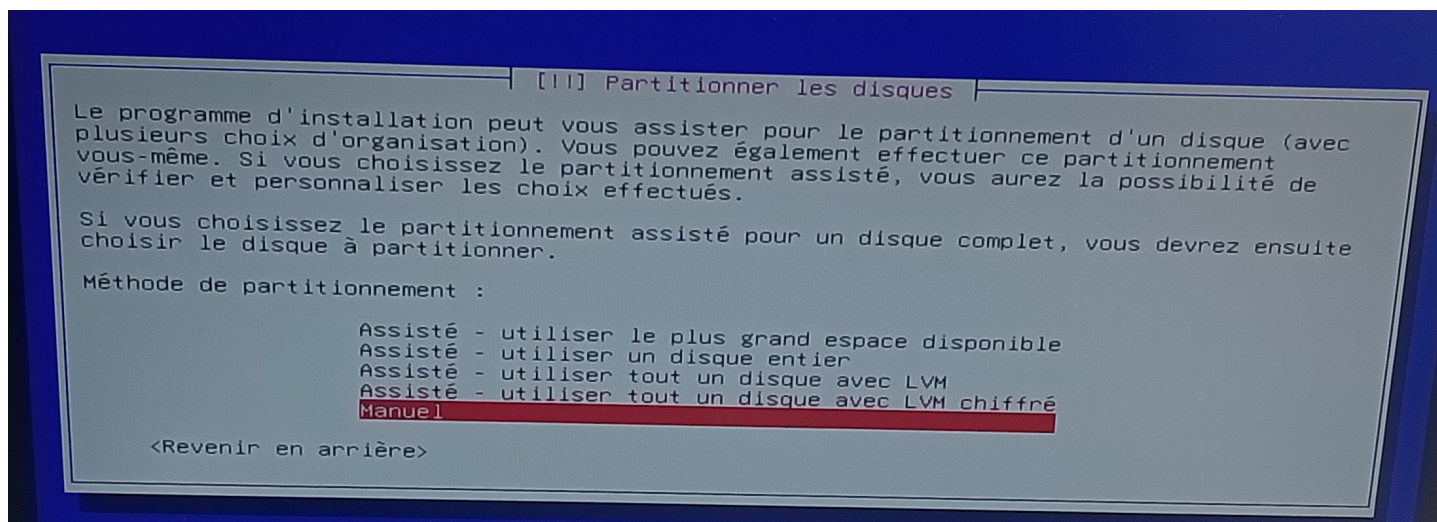
A savoir : Les mots de passes doivent être retenus pour commencer, mais pourront être modifiés après.

Dans « **Configurer l'horloge** » valider les étapes et laisser les choix par défaut. Le serveur quand il s'allumera, utilisera la date et heure BIOS pour démarrer, puis se maintiendra à l'heure par Internet (NTP).

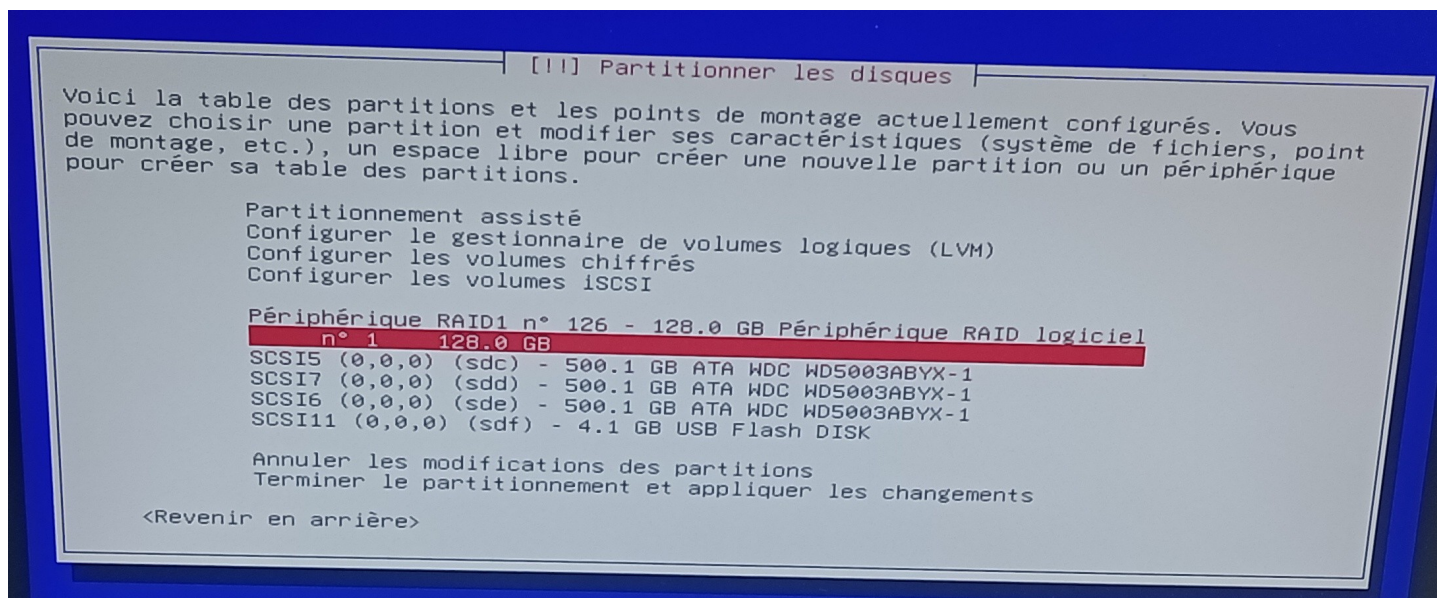
L'heure du BIOS passera (à la fin de l'installation) en temps « **UTC** » pour **Universal Time Clock**. Via cette approche (opposée à celle de Windows), les changements d'heures n'auront plus besoin de modifier l'heure du BIOS, ni de noter où que ce soit si ça a été fait ou non. En fonction de la date, Debian connaîtra automatiquement la différence entre l'heure locale, et l'heure UTC (à laquelle sera réglée le BIOS).

Aller dans « **Détecter les disques** », puis « **Partitionner les disques** ».

Choisir le mode « **Manuel** » car on va décider nous même où est-ce qu'on installe Debian.

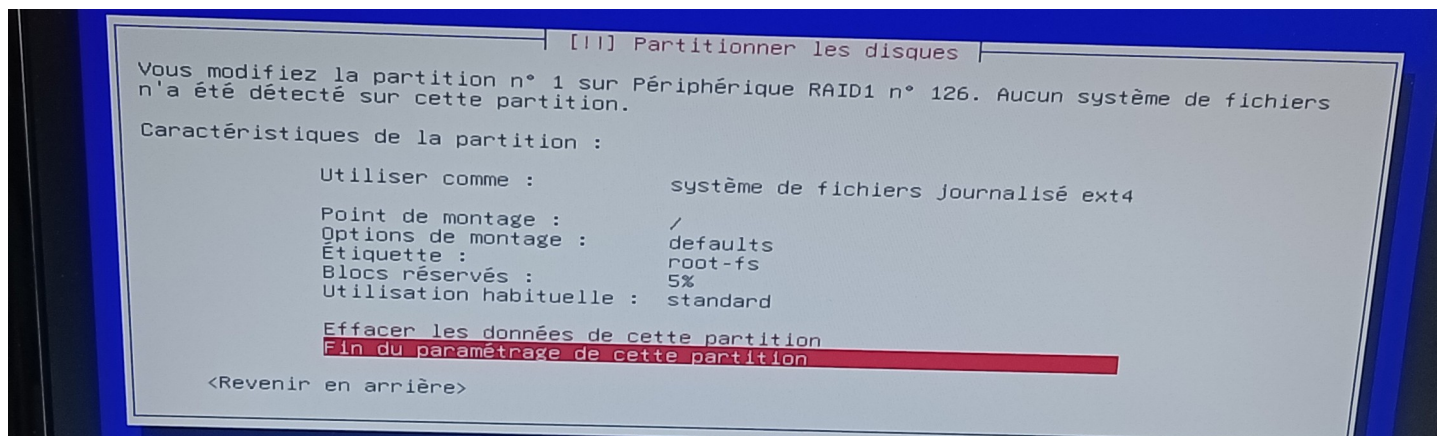


On peut voir ci-dessous que notre « **RAID1** » composé des 2 SSD est bel et bien vu comme 1 seul volume :



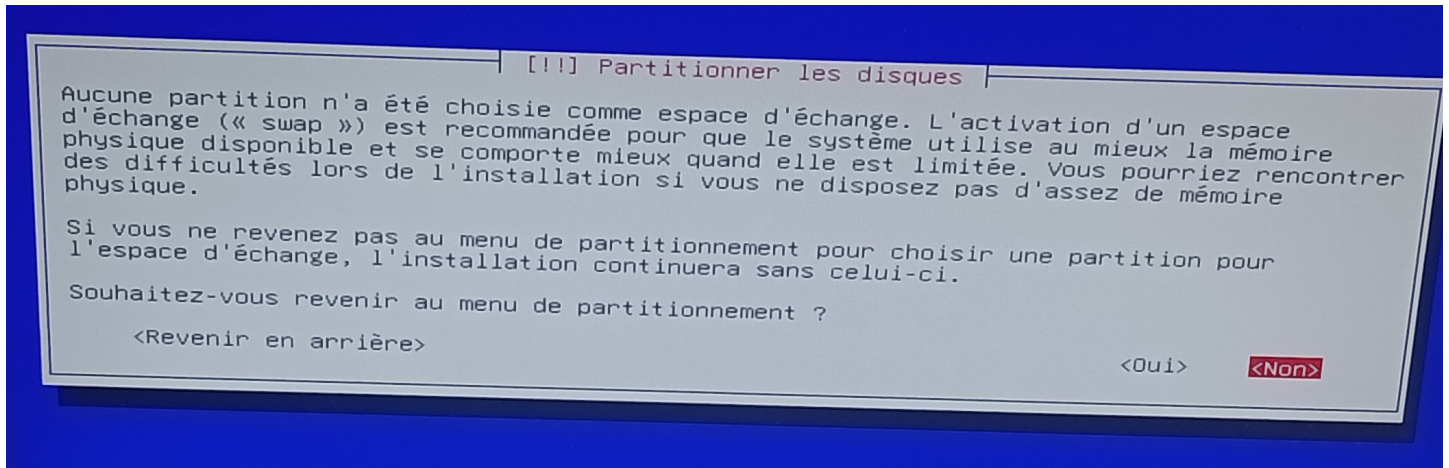
C'est ce volume qu'il va falloir sélectionner. Noter aussi « **RAID1 n° 126** » : on aura besoin de ce numéro plus loin.

Choisir « **ext4** », « **/ - système de fichiers racine** », et le nommer « **root-fs** » (par convention, fs désignant filesystem = système de fichier, ici de type ext4, et « **root-fs** » désignant alors le système de fichier racine sur lequel sera installé Debian).



Aller ensuite dans « **Terminer le partitionnement et appliquer les changements** »

Le message ci-dessous a de grandes chances d'apparaître :

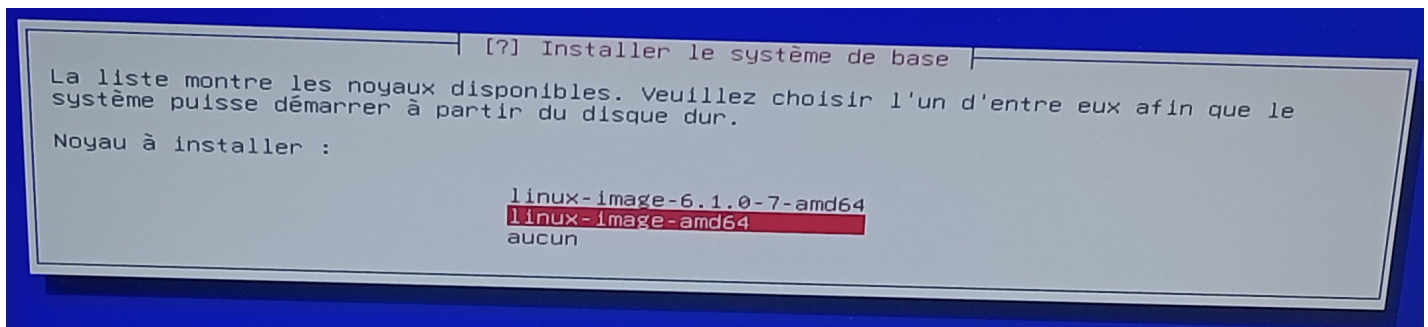


Répondre « **Non** » : Sur des ordinateurs modernes (6GB de RAM pour celui-ci) et étant donné l'utilisation qui sera faite du serveur, ce n'est absolument pas un problème qu'il n'y ait pas de « swap ».

En détails : Si un logiciel devait un jour tenter de manger frénétiquement toute la mémoire RAM disponible, ce ne serait de toute façon pas normal. Inutile donc de mettre en place de quoi aider un tel logiciel à trouver plus de RAM qu'il n'y en a de disponible : Linux se contentera simplement de le laisser planter/se fermer.

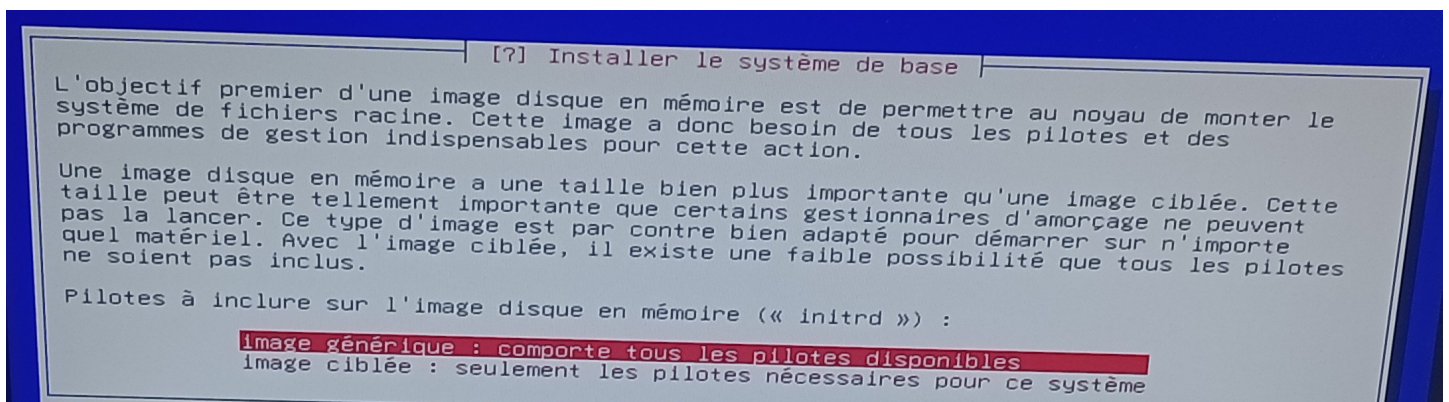
Ensuite au message « **Faut-il appliquer les changements sur les disques** », répondre « **Oui** ».

Entrer ensuite dans « **Installer le système de base** »



Choisir « **linux-image-amd64** » : de cette façon, le système aura le droit de se mettre à jour vers des versions de Linux plus récentes à l'avenir, au lieu de rester coincé sur un numéro de version fixe.

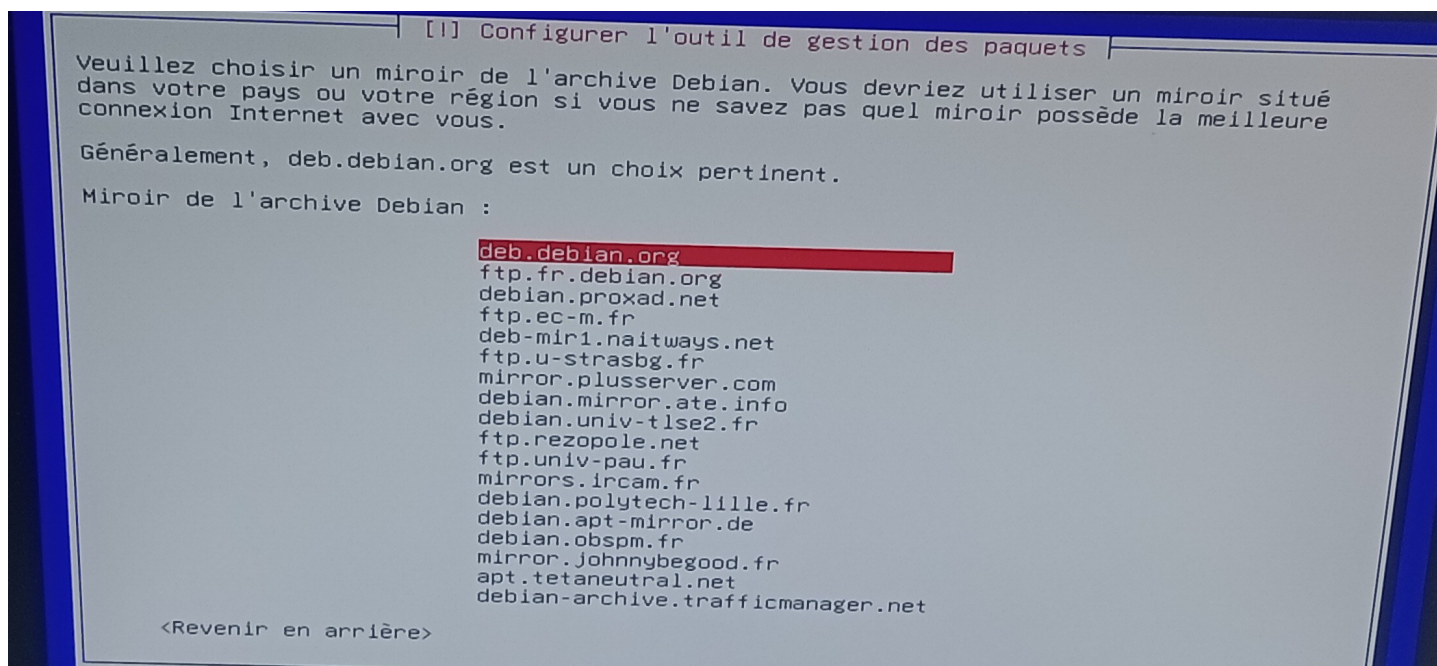
Ensuite, entre l'image générique et l'image ciblée, **préférer l'image générique** : le PC dispose d'assez de mémoire, et en cas de changement de matériel, on diminue les chances de problème au démarrage.



Entrer ensuite dans « **Configurer l'outil de gestion des paquets** ». A la question « **Faut-il utiliser un miroir réseau** » répondre **Oui**

Concernant le protocole, seul « **http** » semble donner une liste de serveurs disponibles. Au choix du pays sélectionner « **France** »

Le choix par défaut « **deb.debian.org** » est généralement le premier à recevoir les mises à jour, et s'il n'était pas toujours très rapide par le passé, il est désormais devenu très performant.

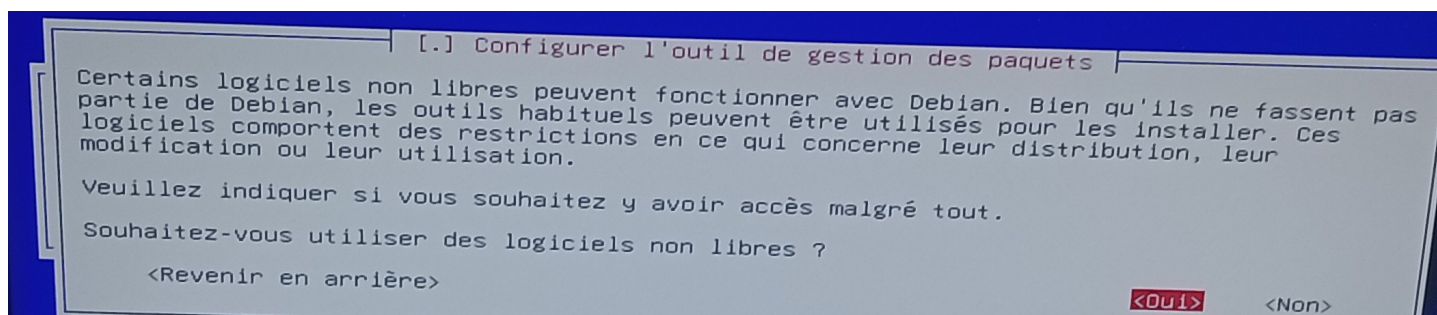


À la question sur de réglage Proxy/Mandataire laisser le champs vide.

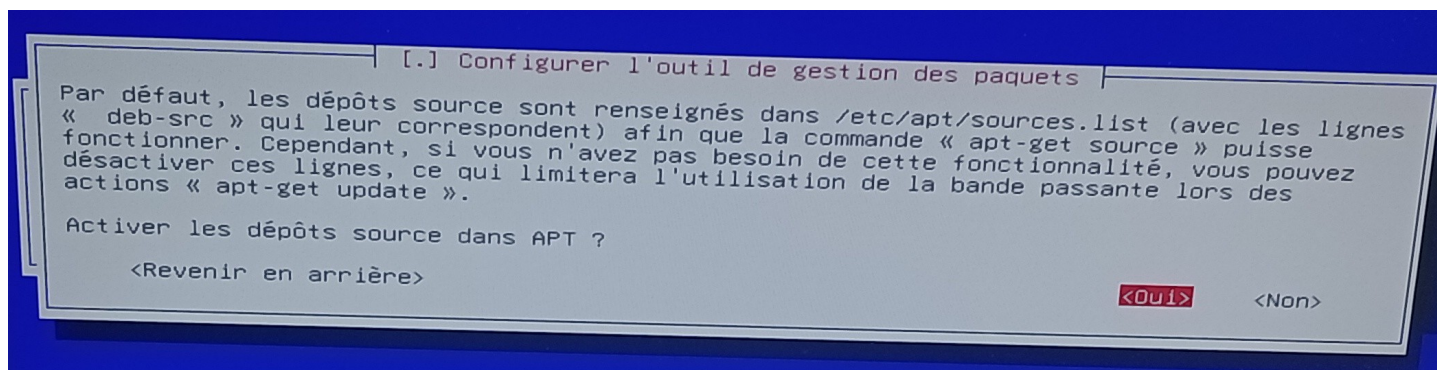
À la question « **Souhaitez-vous utiliser des microprogrammes non libres** » répondre **Oui** : cela n'engage pas à les utiliser mais les rend disponibles en cas de besoin.

En détails : Les ordinateurs étant composés de matériel souvent propriétaire « tous droit réservés » fonctionnant avec des micrologiciels / firmwares « tout droit réservés » eux aussi, quand ils ne sont déjà inclus dans le BIOS, il est généralement illusoire de faire sans.

Concernant « **Souhaitez-vous utiliser des logiciels non libres ?** » répondre « **Oui** », bien qu'assez peu de logiciels soient concernés (notamment Steam pour les jeux vidéos).

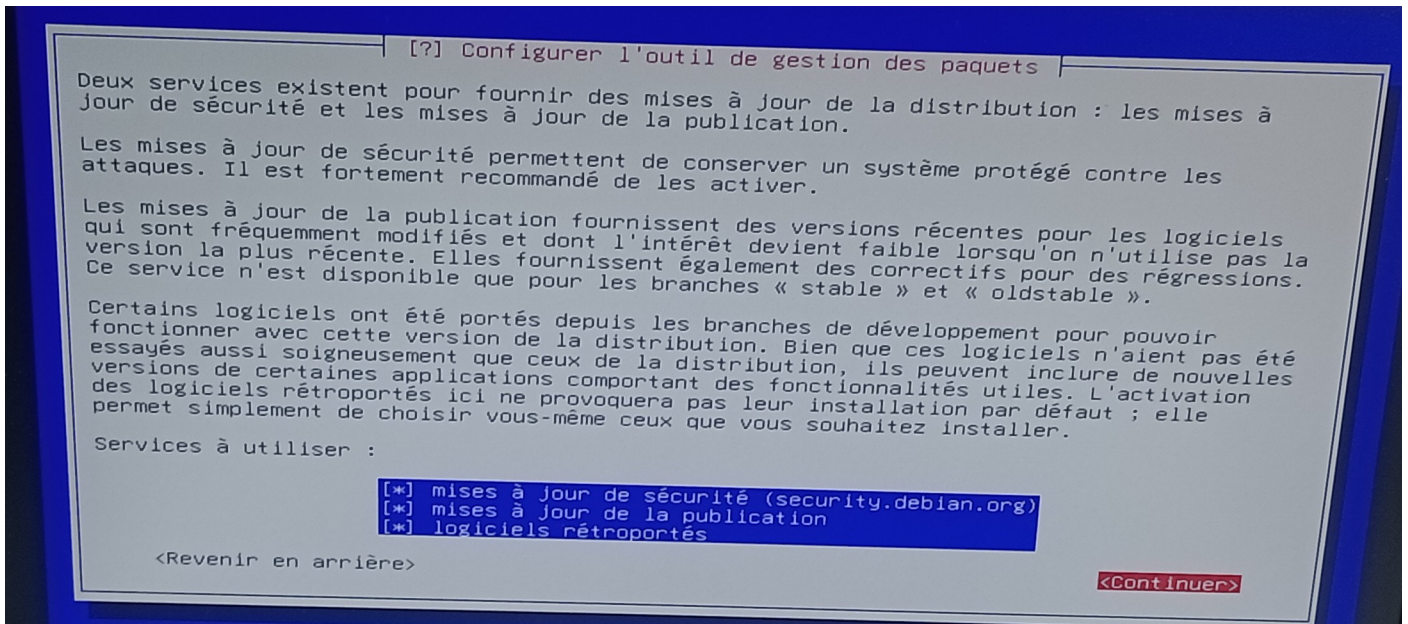


Là encore ça n'oblige en rien leur installation, ça les rend juste disponibles si veut les installer plus tard.

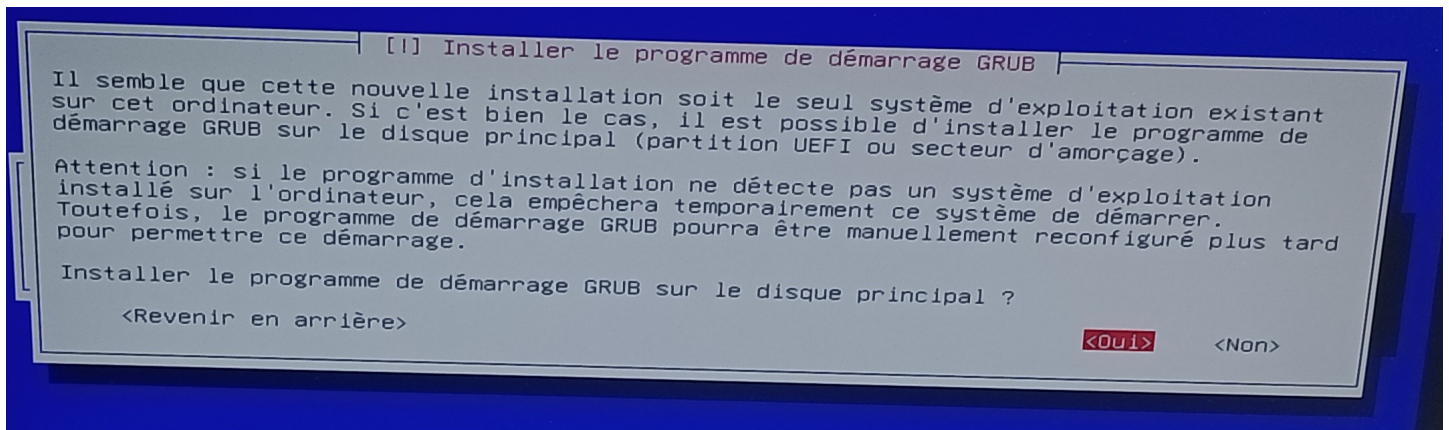


Concernant les dépôts source, nous n'en auront pas besoin ; ceci dit la bande passante n'est plus un problème de nous jours : Oui ou Non, ça aucune importance donc. J'ai laissé sur « **Oui** »...

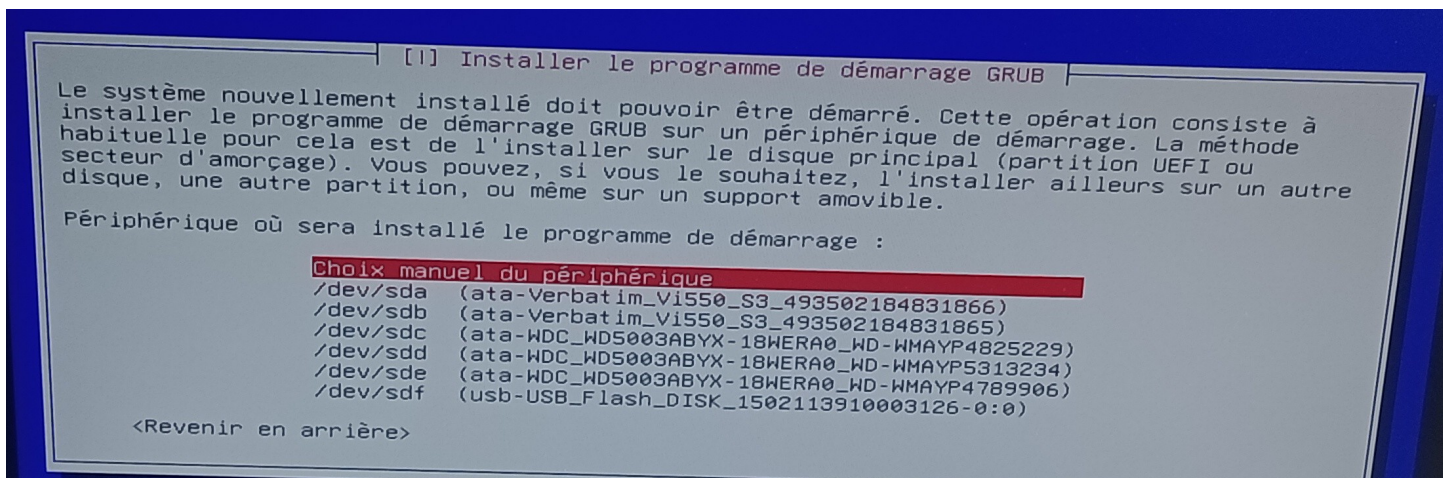
Lorsque le message ci-dessous s'affiche, on peut là aussi tout cocher : ça ne nous engage à rien et ça ne fait que rendre un maximum de choses disponibles.



Passer ensuite directement à « **Installer le programme de démarrage GRUB** »



En effet, aucun autre système d'exploitation. Et on veut que désormais ce soit Debian qui démarre : **Oui**.

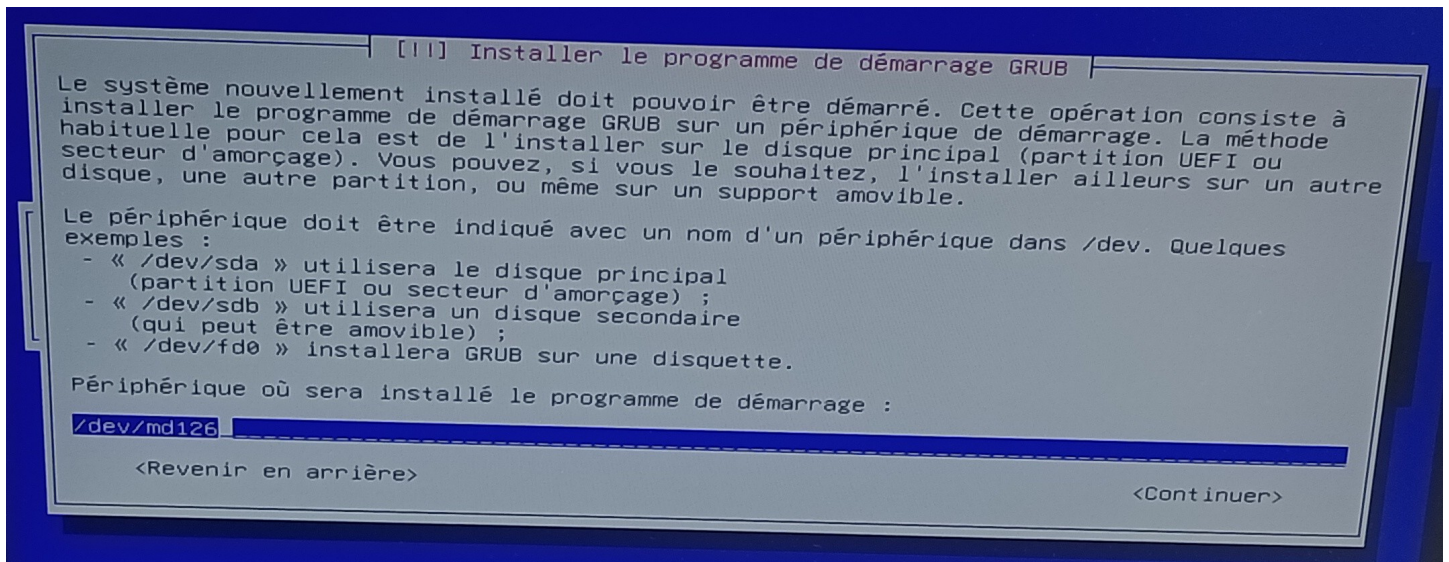


Problème : Ici on voit les deux SSD identifiés individuellement, ainsi que les 3 disques de 500 Go que nous configurons plus tard.

En revanche, **on ne voit pas le volume RAID1** sur lequel on vient d'installer (précédemment désigné comme RAID1 n°126). Les volumes RAID sont généralement identifiés **/dev/md** suivi d'un nombre (ici **126**).

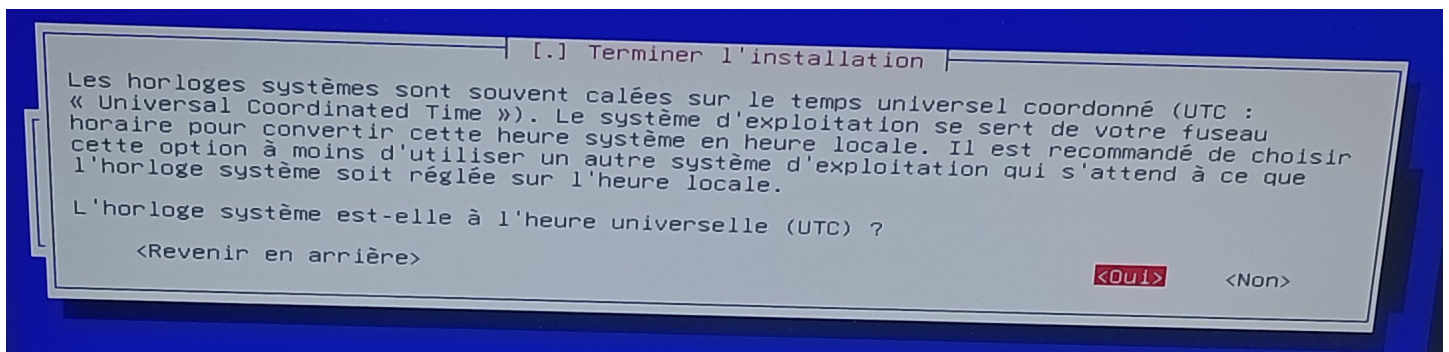
Aller dans « **Choix manuel du périphérique** »

On va entrer manuellement `/dev/md126`



Le fait qu'il ne nous l'ait pas proposé dans la liste est une anomalie. Impossible pour un utilisateur normal de renseigner ça en partant de rien. Il aurait fallu aller dans « **Executer un shell** » et taper `blkid` pour trouver.

Aller ensuite dans « **Terminer l'installation** »



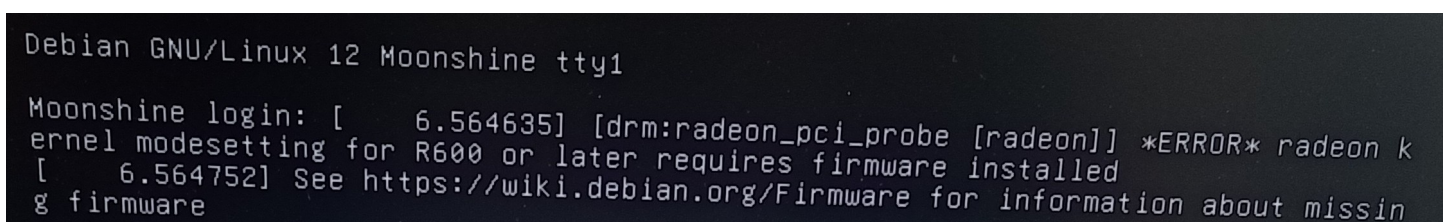
A la question « **L'horloge système est-elle à l'heure universelle (UTC) ?** » il faudrait que l'on puisse répondre « **Pas encore** ». On va répondre « **Oui** » pour qu'à la prochaine mise à jour d'heure par Internet (via protocole NTP, automatique), ça devienne le cas.

Ceci permettra à Linux de maintenir l'horloge interne à l'heure, pour que le PC soit à l'heure à chaque fois qu'il démarre.

Si on répondait « Non » (généralement c'est pour cohabiter avec Windows) Linux ne réglerait jamais l'horloge interne puisque la façon dont l'heure est gérée sous Windows nécessite qu'il soit seul à s'en occuper (notamment du fait des changements d'heures été / hiver).

6 Premier démarrage

L'ordinateur nous accueille avec sa plus belle ligne de commande nous demandant un login en ligne de commandes, aussitôt décoré d'un message d'erreur qui vient d'éructer là où on était sensé écrire. Rien de très grave ceci dit, on va s'en occuper.



Appuyer sur « **Entrée** », puis s'identifier en « **root** »

Une fois identifiés, on va lui demander d'installer « **OpenSSH-Server** » ainsi que les « **firmwares** » dont il est question dans le message d'erreur.

```
Moonshine login: root
Password:
Linux Moonshine 6.1.0-7-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.20-1 (2023-03-19)
) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@Moonshine:~# apt install openssh-server firmware-linux
```

Sur ce PC on peut apercevoir d'autres avertissements liés au firmware de la carte réseau :

```
W: Possible missing firmware /lib/firmware/rtl_nic/rtl8105e-1.fw for module r816
9
W: Possible missing firmware /lib/firmware/rtl_nic/rtl8168e-3.fw for module r816
9
W: Possible missing firmware /lib/firmware/rtl_nic/rtl8168e-2.fw for module r816
9
W: Possible missing firmware /lib/firmware/rtl_nic/rtl8168e-1.fw for module r816
9
W: Possible missing firmware /lib/firmware/rtl_nic/rtl8168d-2.fw for module r816
9
W: Possible missing firmware /lib/firmware/rtl_nic/rtl8168d-1.fw for module r816
9
root@Moonshine:~# apt install firmware-realtek_
```

Du fait qu'il y ait déjà un firmware pour cette dernière inclus dans le BIOS de la carte mère, ce n'est pas bloquant (la carte réseau fonctionne quand même), et on pourra s'en occuper après.

De toute façon, on installera plus tard tous les firmwares qu'il est possible d'installer ensuite, afin de ne plus être embêtés par ces histoires et ces messages. D'autres versions de Linux les installent tous par défaut.

Si on est pressé : Pour s'en occuper tout de suite, on peut entrer « **apt install firmware-realtek** ».

Avant de redémarrer l'ordinateur, taper « **nano /etc/ssh/sshd_config** » puis chercher la ligne « **PermitRootLogin** ».

Modifier la ligne pour avoir ce qui suit, puis appuyer sur **Ctrl** et **X** (suivi de la touche **O** pour sauver).

```
# Authentication:
#LoginGraceTime 2m
PermitRootLogin yes_
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

^G Aide          ^O Écrire
^X Quitter      ^R Lire fich.
^W Chercher     ^N Remplacer
^K Couper      ^U Coller
^T Exécuter    ^J Justifier
^C Emplacement ^_ Aller ligne
```

Redémarrer l'ordinateur en tapant « **Reboot** » : on va désormais pouvoir travailler par le réseau (et utiliser des copier-coller entre autre pour aller plus vite).

7 Première connexion par réseau

7.1 Quelle est l'adresse IP du serveur ?

7.1.1 Première approche : demander au serveur

Pour l'instant, il ne sait parler qu'en lignes de commandes... mais on peut quand même lui demander.

Sur le PC serveur, taper la commande « ip a » : son adresse IP est « 192.168.63.232 » sur cet exemple.

```
utilisateur@Moonshine:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp6s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:24:8c:5a:66:e6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.63.232/24 brd 192.168.63.255 scope global dynamic enp6s0
        valid_lft 214sec preferred_lft 214sec
    inet6 fd02:842a:8223:5500:224:8cff:fe5a:66e6/64 scope global dynamic mngtmpaddr
        valid_lft forever preferred_lft forever
    inet6 2a02:842a:8223:5500:224:8cff:fe5a:66e6/64 scope global dynamic mngtmpaddr
        valid_lft 326sec preferred_lft 325sec
    inet6 fe80::224:8cff:fe5a:66e6/64 scope link
        valid_lft forever preferred_lft forever
```

7.1.2 Autre approche : j'ai demandé à la box

Cette approche est parfois la plus intéressante, car elle permet de s'habituer à prendre la main sur la Box, voir les adresses de tout ce qui y est connecté, voire même de fixer/changer ces dernières.

7.1.2.1 Mais quelle est l'adresse IP de la box ?

The screenshot shows the Windows 'Réseau et Internet' settings window. The 'Ethernet' adapter is selected, and its details are shown in a separate window. The 'État de Ethernet' window shows the connection status and speed.

Détails de connexion réseau :

Propriété	Valeur
Suffixe DNS propre à la ...	lan
Description	Realtek(R) PCI(e) Ethernet Controller
Adresse physique	38-2C-4A-2B-32-81
DHCP activé	Oui
Adresse IPv4	192.168.63.10
Masque de sous-réseau ...	255.255.255.0
Bail obtenu	lundi 17 avril 2023 16:04:41
Bail expirant	lundi 17 avril 2023 20:36:47
Passerelle par défaut IPv4	192.168.63.1
Serveur DHCP IPv4	192.168.63.1
Serveur DNS IPv4	192.168.63.1
Serveur WINS IPv4	
NetBIOS sur TCP/IP act...	Oui
Adresse IPv6	2a02:842a:8223:5500::10
Bail obtenu	lundi 17 avril 2023 16:04:41
Bail expirant	lundi 17 avril 2023 20:34:40

État de Ethernet :

Connexion

Connectivité IPv4 :	Internet
Connectivité IPv6 :	Internet
État du média :	Activé
Durée :	04:27:30
Vitesse :	1,0 Gbits/s

Activité

Envoyés | Reçus

Octets : 7905 774 | 634692 678

Propriétés | Désactiver | Diagnostiquer

Fermer

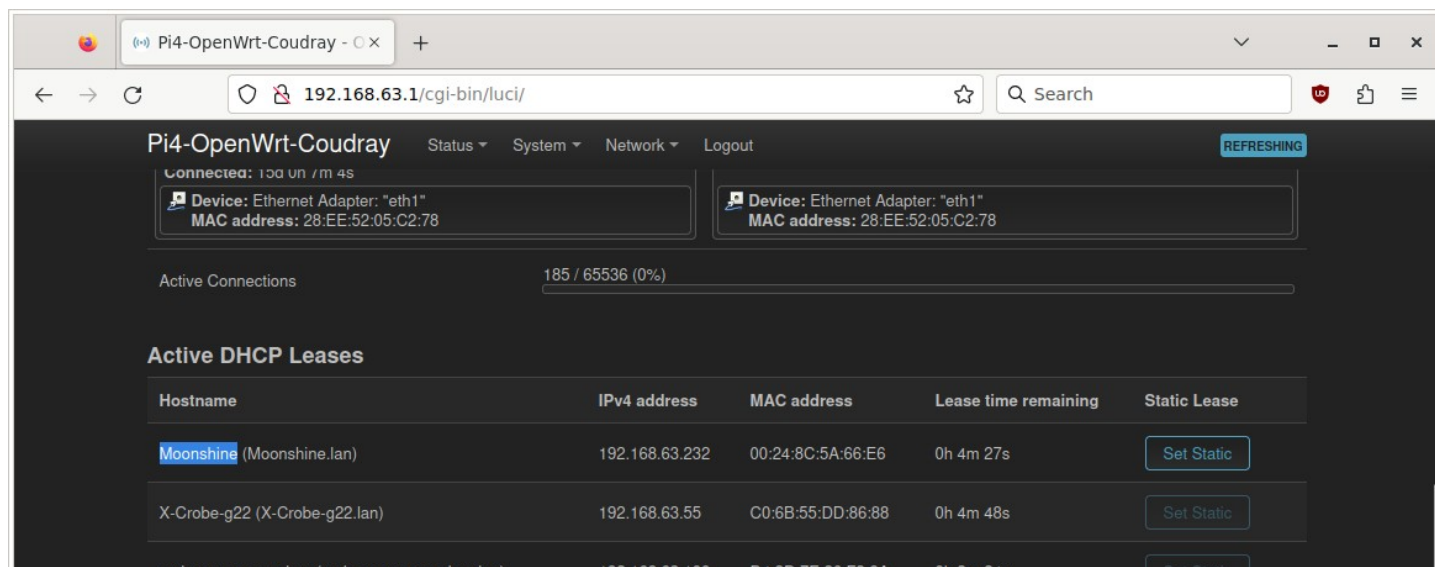
Il est généralement possible depuis un ordinateur connecté (ou même depuis un téléphone Android) d'avoir des informations réseaux parmi lesquelles figurent, en tant que passerelle (voire DNS), l'adresse de la Box.

7.1.2.2 Interroger la box

Dans un navigateur Internet, depuis un PC ou smartphone relié sur le réseau, entrer l'adresse IP de la box.

Il y a généralement un mécanisme d'authentification (différent chez tous les fournisseurs).

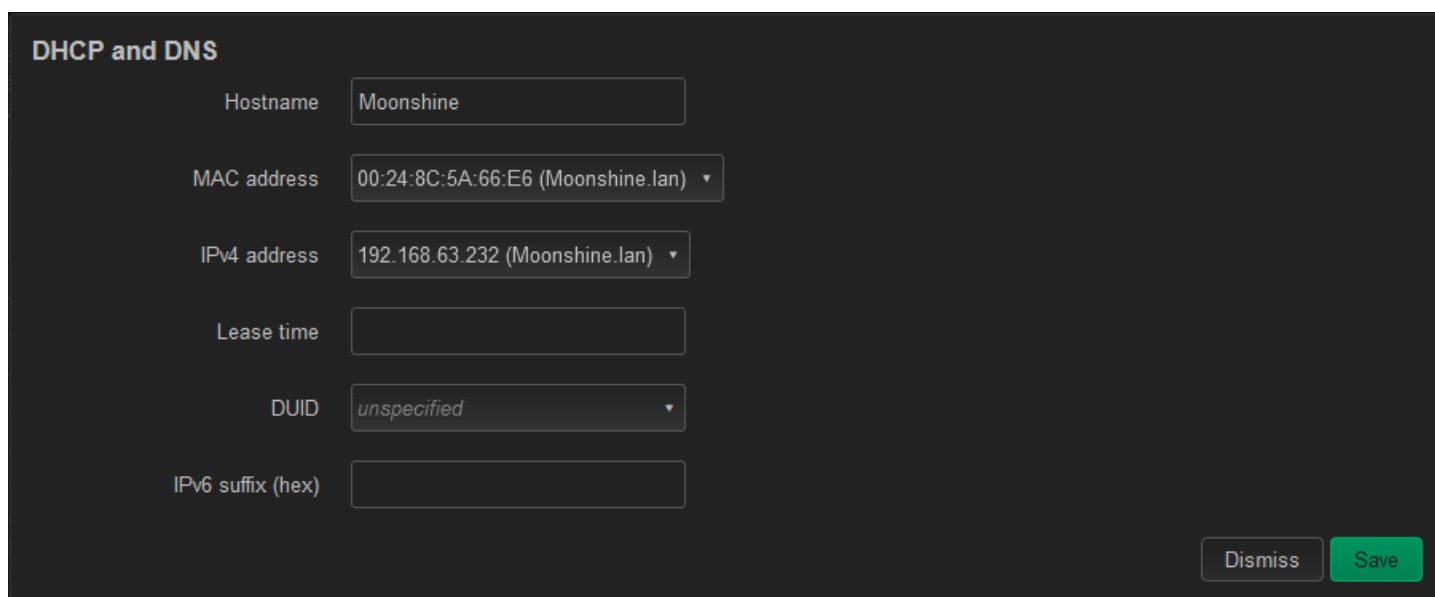
Sur ma box :



On peut voir que « **Moonshine** » est connecté avec l'adresse IP **192.168.63.232** dans cet exemple.

On peut également voir son adresse MAC « **00:24:8C:5A:66:E6** », c'est un peu comme le numéro d'immatriculation de la carte réseau du serveur.

Via les menus avancés, je peux demander à ma Box de lui donner toujours la même adresse IP.



De cette manière, quand le serveur est branché au réseau et qu'il demande une adresse IP en « configuration automatique » (aussi appelé DHCP), la box est sûre de toujours lui donner la même ET de ne donner cette adresse IP à aucun autre équipement.

Généralement le menu permettant de faire ça, s'appelle « **Static Lease** » ou « **Bail statique DHCP** »

7.1.3 Autre approche : Par le nom de la machine sur le réseau

Du fait du nom qu'on a donné à la machine (parfois appelé hostname ou nom d'hôte), lorsque celle-ci est reliée au réseau et demande une adresse IP (protocole DHCP), elle présente également son nom.

La box, qui sert généralement de DNS (traducteur Nom → Adresse IP) prend généralement note de ce nom.

Du fait que la box sert généralement de serveur « DNS » pour les équipements du réseau, lorsqu'au lieu de taper une adresse IP, on tape un nom (www.google.fr, Moonshine...) une requête DNS est faite pour transformer ce nom en adresse IP (et auquel cas c'est la Box qui se charge de cette traduction).

```
Invite de commandes
C:\Users\Utilisateur>ping Moonshine

Envoi d'une requête 'ping' sur Moonshine.lan [192.168.63.232] avec 32 octets de données :
Réponse de 192.168.63.232 : octets=32 temps<1ms TTL=64
Réponse de 192.168.63.232 : octets=32 temps<1ms TTL=64
Réponse de 192.168.63.232 : octets=32 temps<1ms TTL=64
Réponse de 192.168.63.232 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.63.232:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\Utilisateur>ping Moonshine.lan

Envoi d'une requête 'ping' sur Moonshine.lan [192.168.63.232] avec 32 octets de données :
Réponse de 192.168.63.232 : octets=32 temps<1ms TTL=64
Réponse de 192.168.63.232 : octets=32 temps<1ms TTL=64
Réponse de 192.168.63.232 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.63.232 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.63.232:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms

C:\Users\Utilisateur>
```

La box de cet exemple se montre serviable :

Elle reconnaît le nom « **Moonshine** » et nous fournit sa traduction en adresse IP : « **192.168.63.232** »

Pour info : pour www.google.fr par exemple, quand ce n'est pas un nom que la box gère elle-même, elle passe généralement la demande au serveur DNS du fournisseur d'accès Internet. Mais c'est transparent.

```
Invite de commandes
C:\Users\Utilisateur>ping www.sfr.fr

Envoi d'une requête 'ping' sur www.sfr.fr [80.125.163.172] avec 32 octets de données :
Réponse de 80.125.163.172 : octets=32 temps=4 ms TTL=248
Réponse de 80.125.163.172 : octets=32 temps=4 ms TTL=248
Réponse de 80.125.163.172 : octets=32 temps=4 ms TTL=248
Réponse de 80.125.163.172 : octets=32 temps=4 ms TTL=248

Statistiques Ping pour 80.125.163.172:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 4ms, Maximum = 4ms, Moyenne = 4ms

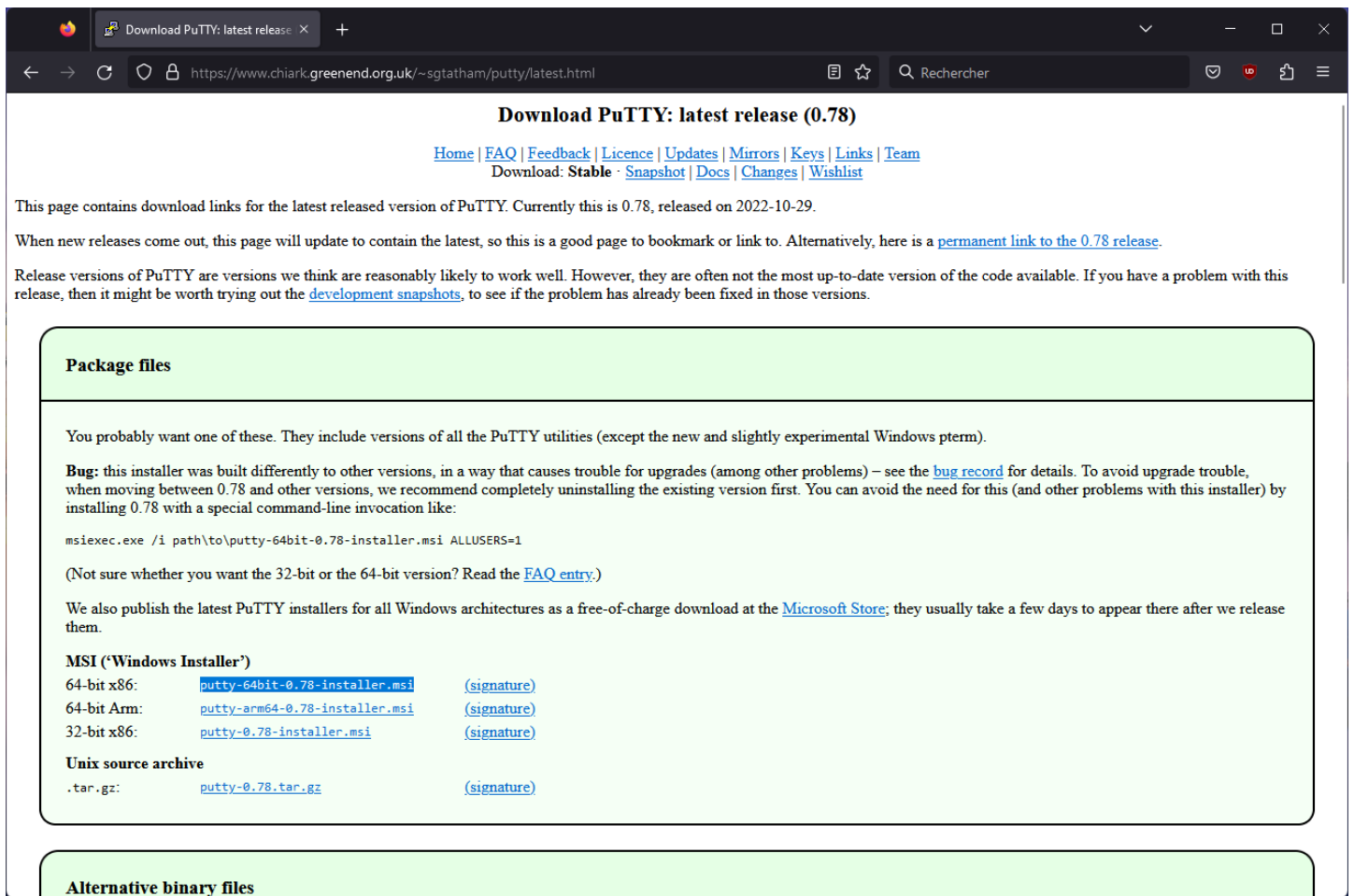
C:\Users\Utilisateur>
```

(Puis c'est hors sujet – c'est juste pour comprendre ce qu'est « DNS »).

7.2 Quels logiciels utiliser pour se connecter au serveur ?

Sous Windows, **PuTTY** (commandes) et **WinSCP** (exploration de fichiers) sont les plus indiqués.

Téléchargement sur leurs sites officiels respectifs :



The screenshot shows the PuTTY website's download page for the latest release (0.78). The page includes navigation links, a brief introduction, and a section for package files. The package files section lists MSI installers for 64-bit x86, 64-bit ARM, and 32-bit x86, along with a Unix source archive. A bug note is also present regarding the installer.

Download PuTTY: latest release (0.78)

[Home](#) | [FAQ](#) | [Feedback](#) | [Licence](#) | [Updates](#) | [Mirrors](#) | [Keys](#) | [Links](#) | [Team](#)
Download: [Stable](#) · [Snapshot](#) | [Docs](#) | [Changes](#) | [Wishlist](#)

This page contains download links for the latest released version of PuTTY. Currently this is 0.78, released on 2022-10-29.

When new releases come out, this page will update to contain the latest, so this is a good page to bookmark or link to. Alternatively, here is a [permanent link to the 0.78 release](#).

Release versions of PuTTY are versions we think are reasonably likely to work well. However, they are often not the most up-to-date version of the code available. If you have a problem with this release, then it might be worth trying out the [development snapshots](#), to see if the problem has already been fixed in those versions.

Package files

You probably want one of these. They include versions of all the PuTTY utilities (except the new and slightly experimental Windows pterm).

Bug: this installer was built differently to other versions, in a way that causes trouble for upgrades (among other problems) – see the [bug record](#) for details. To avoid upgrade trouble, when moving between 0.78 and other versions, we recommend completely uninstalling the existing version first. You can avoid the need for this (and other problems with this installer) by installing 0.78 with a special command-line invocation like:

```
msiexec.exe /i path\to\putty-64bit-0.78-installer.msi ALLUSERS=1
```

(Not sure whether you want the 32-bit or the 64-bit version? Read the [FAQ entry](#).)

We also publish the latest PuTTY installers for all Windows architectures as a free-of-charge download at the [Microsoft Store](#); they usually take a few days to appear there after we release them.

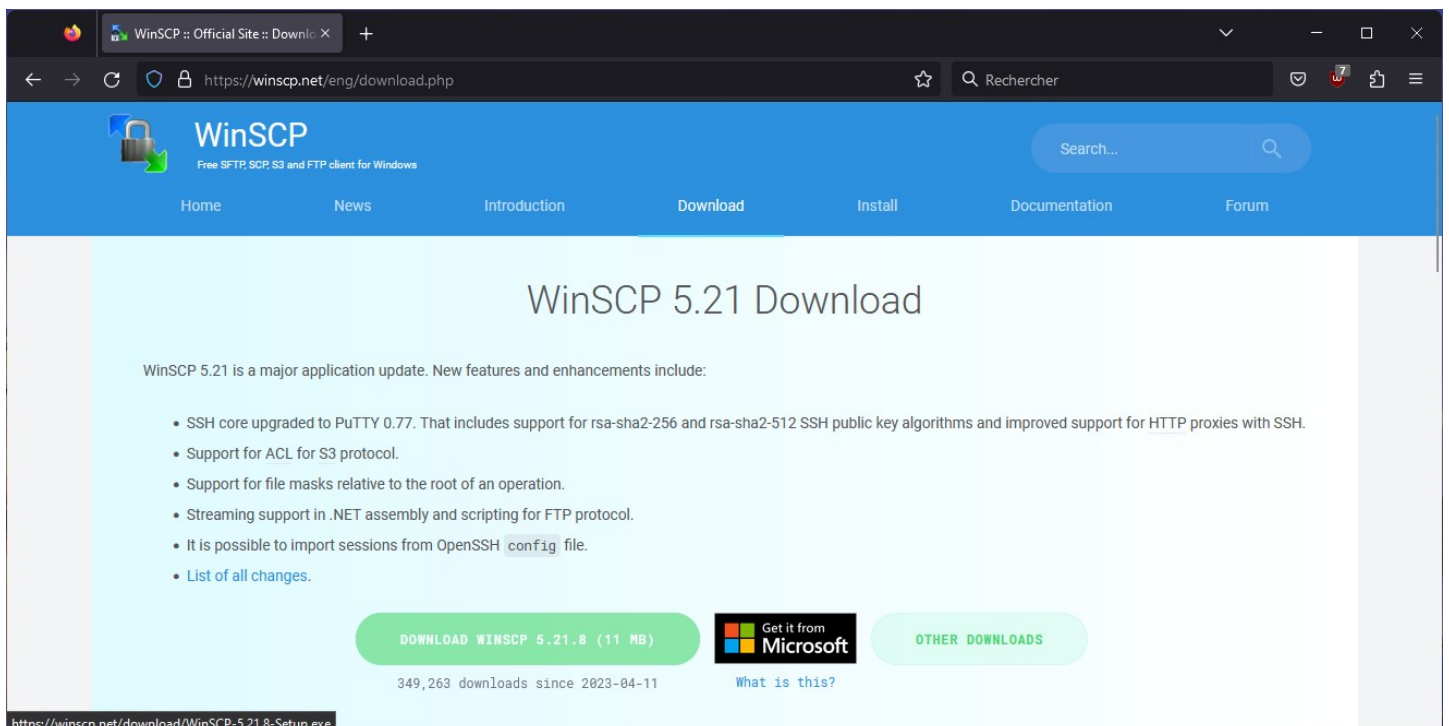
MSI ('Windows Installer')

64-bit x86:	putty-64bit-0.78-installer.msi	(signature)
64-bit Arm:	putty-arm64-0.78-installer.msi	(signature)
32-bit x86:	putty-0.78-installer.msi	(signature)

Unix source archive

.tar.gz:	putty-0.78.tar.gz	(signature)
----------	-----------------------------------	-----------------------------

Alternative binary files



The screenshot shows the WinSCP website's download page for version 5.21.8. The page features a navigation menu, a search bar, and a list of new features and enhancements for the update. A prominent download button is visible, along with a Microsoft logo and a 'What is this?' link.


WinSCP
Free SFTP, SCP, S3 and FTP client for Windows

Home News Introduction Download Install Documentation Forum

WinSCP 5.21 Download

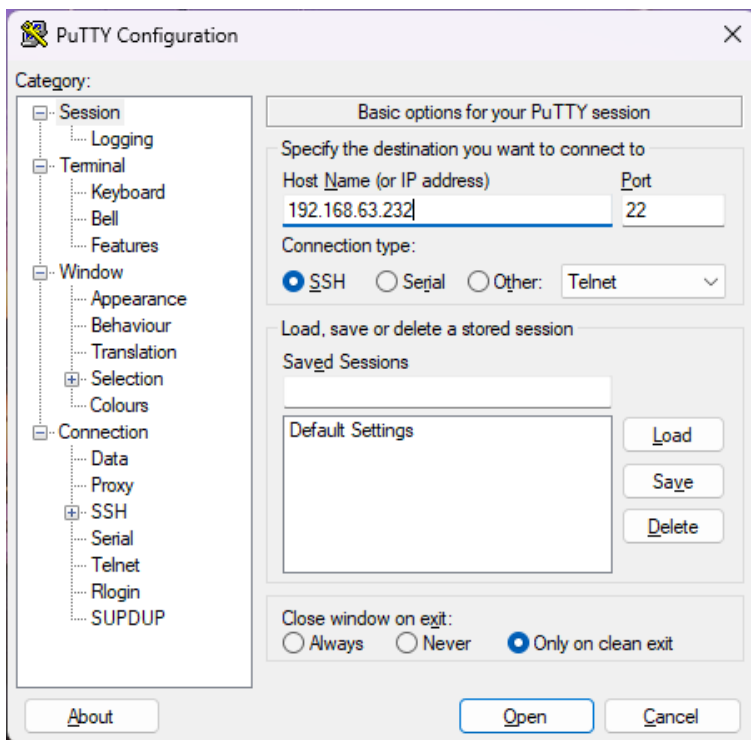
WinSCP 5.21 is a major application update. New features and enhancements include:

- SSH core upgraded to PuTTY 0.77. That includes support for rsa-sha2-256 and rsa-sha2-512 SSH public key algorithms and improved support for HTTP proxies with SSH.
- Support for ACL for S3 protocol.
- Support for file masks relative to the root of an operation.
- Streaming support in .NET assembly and scripting for FTP protocol.
- It is possible to import sessions from OpenSSH `config` file.
- [List of all changes](#).

[DOWNLOAD WINSCP 5.21.8 \(11 MB\)](#)  [OTHER DOWNLOADS](#)

349,263 downloads since 2023-04-11 [What is this?](#)

<https://winscp.net/download/WinSCP-5.21.8-Setup.exe>



Une fois putty installé il est réglé par défaut pour se connecter via « SSH »

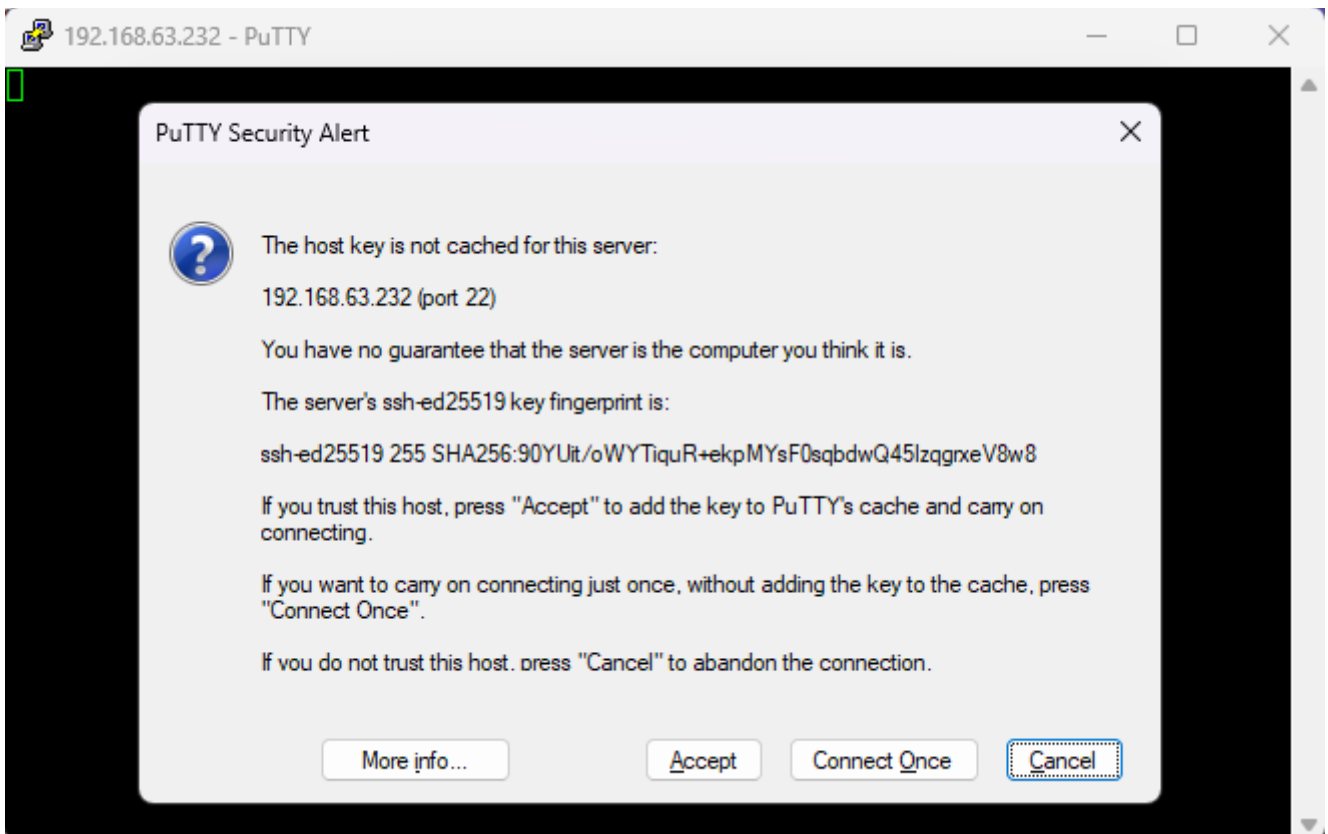
C'est ce qui correspond au mode de connexion qu'on a installé sur le serveur un peu plus tôt (en tapant « apt install openssh-server »)

Bien que putty puisse faire plein de choses un peu techniques on ne l'utilisera ici que pour écrire des commandes sur le serveur.

Attention : Sélectionner du texte à la souris suffit à « Copier » ce dernier

Attention : Un clic droit équivaut à « Coller ».

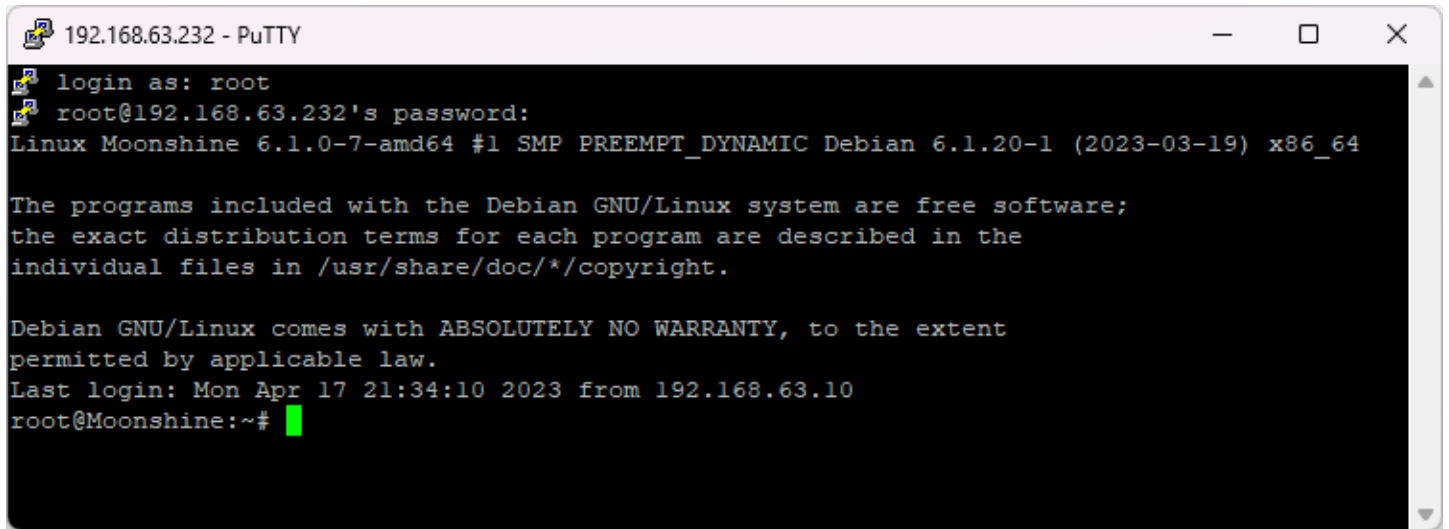
À la première connexion un message de « **Security Alert** » apparaît : il suffit de l'ignorer et de cliquer sur **Accept**. Ceci est dû au fait que ce serveur n'est pas encore reconnu par putty.



En détails : Dès que putty a affaire à un serveur qu'il ne connaît pas encore, il passe en mode psychose, de peur qu'on entre nos identifiants dans un serveur qui n'est pas le notre (et qui voudrait nous voler nos identifiants...)

En bref : c'est juste pas hyper doué pour nous dire que tout va bien.

Une fois authentifié on a accès à la même ligne de commande que quand on se trouve sur le serveur.



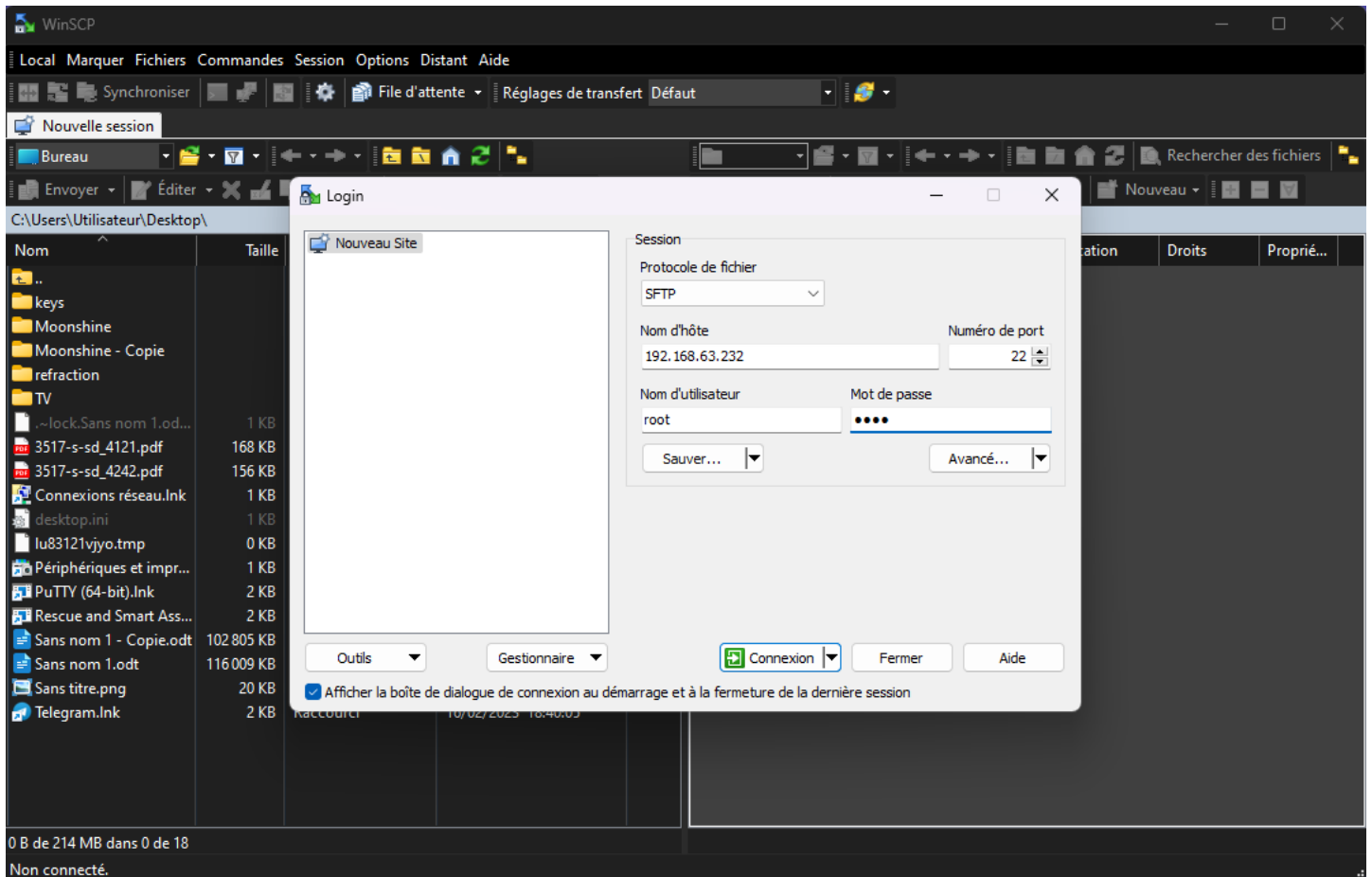
```
192.168.63.232 - PuTTY
login as: root
root@192.168.63.232's password:
Linux Moonshine 6.1.0-7-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.20-1 (2023-03-19) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Apr 17 21:34:10 2023 from 192.168.63.10
root@Moonshine:~#
```

Concernant **WinSCP** même principe d'authentification.

Le protocole « **SFTP** » étant pris en charge par OpenSSH-Server, et fonctionnant sur le port « 22 » lui aussi.



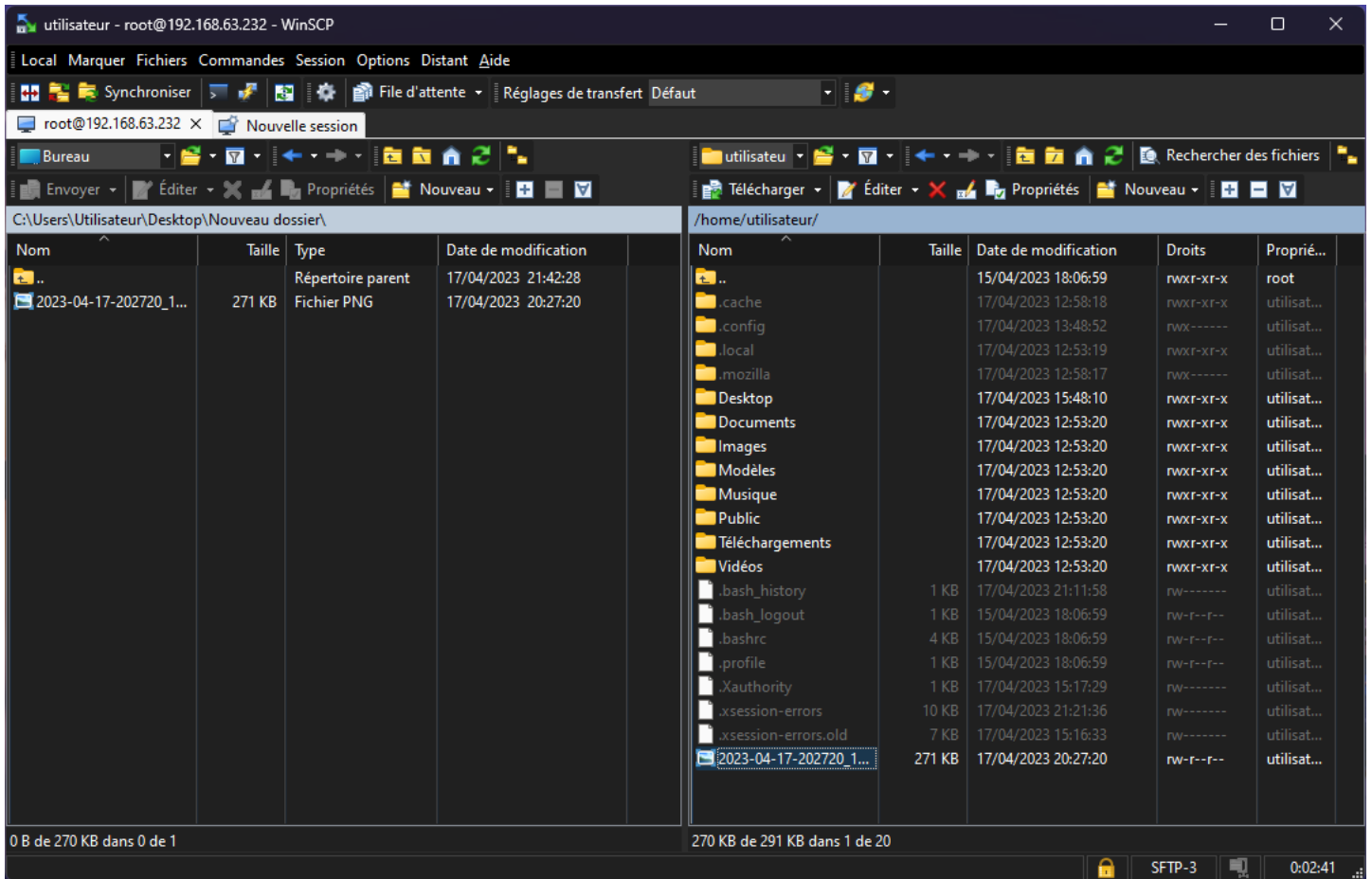
Attention : quand on clique sur « Sauver » **par défaut il n'enregistre pas le mot de passe** et il se permet même de l'effacer (il faudra cocher une case en + pour lui dire d'enregistrer le mot de passe).

Une fois connecté on peut naviguer dans les fichiers du serveur, et même les éditer.

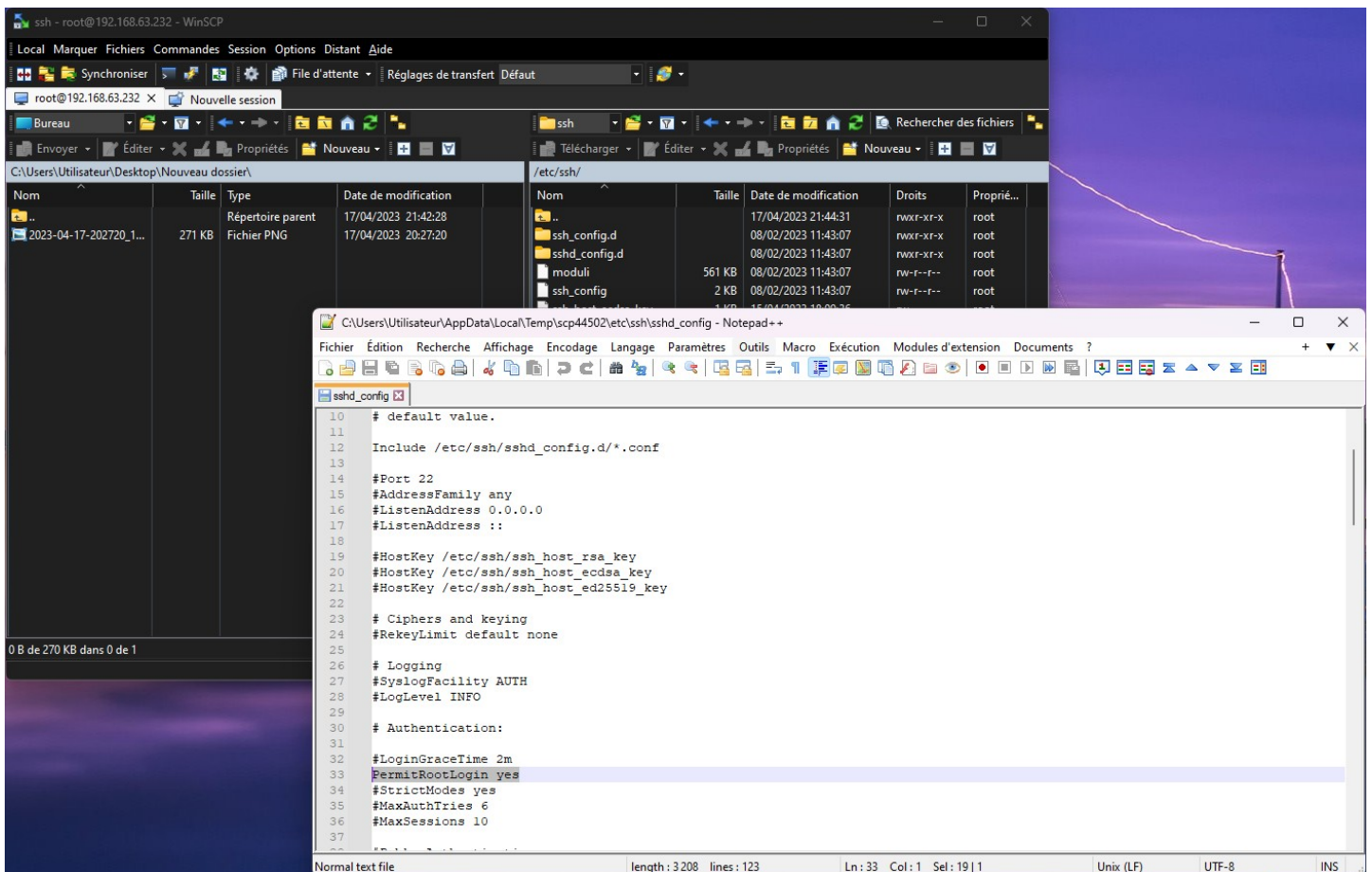
On peut envoyer ou recevoir des fichiers (local vers serveur, serveur vers local).

Remarque : WinSCP ne sait pas ouvrir les photos par exemple : il ne sait ouvrir les fichiers qu'en **édition de texte**. On peut tout de même télécharger les fichiers d'abord, puis les ouvrir séparément en dehors de WinSCP ensuite, par exemple.

Exemple de vue WinSCP :



A gauche, le PC local (sous Windows). Dans un dossier sur le bureau. A droite, le PC distant (sous Linux), dans /home/utilisateur/. On peut utiliser la souris pour glisser un fichier dans un sens ou dans l'autre.



Pour éditer des fichiers texte, c'est bien plus pratique qu'en utilisant la commande « nano » ou pire.

8 Suite de l'installation

8.1 Installation de tous les éléments du système d'exploitation

Comme indiqué plus tôt, la version « Net-Installer » installe tout juste de quoi démarrer le PC, et un nombre très limité d'outils pour pouvoir installer nous même ce dont on a besoin.

Bureau : on va installer une série d'outils graphiques pour faire un véritable bureau (et ne plus être enfermé dans l'invite de commande).

Outils systèmes / commandes : on va également installer un certain nombre d'outils en ligne de commande. Bien qu'ils soient rarement utilisés, et n'aient pas d'interface sympathique depuis le bureau, il peut leur arriver de se montrer utiles (et leur installation n'occupe que très peu de stockage).

Copier-Coller dans putty cette grande commande qui installe ça (ou la recopier à la main sur le serveur) :

```
apt update && apt install dbus firmware-linux firmware-ralink firmware-realtek firmware-iwlwifi dkms systemd-timesyncd acpi net-tools dnsutils whois traceroute nmap ethtool wireless-tools iw lxqt-core scrot lxterminal lightdm numlockx synaptic openssh-server fail2ban baobab brasero gnome-system-monitor gnome-disk-utility gparted wget curl aria2 iperf iperf3 bwm-ng stress-ng memtester memtest86+ zip rar unrar lm-sensors file-roller calculator smartmontools ntfs-3g gedit ghex meld firefox-esr filezilla vlc sysstat ntpdate build-essential gdb valgrind git subversion network-manager-gnome blueman msmtptta s-nail mailutils unattended-upgrades doublecmd-qt usbtopy usbutils cpufrequtils telnet putty tcpdump wireshark ffmpeg vdpauinfo vainfo clinfo vulkan-tools mesa-utils openvpn x11vnc
```

Aux questions sur « Wireshark, MSMTTP et Iperf3 » répondre « **Non** ».

Par défaut, des choses optionnelles et inutiles sont installées avec « **lxqt** », on peut les enlever :

```
apt autoremove --purge zutty featherpad qlipper xarchiver system-config-printer avahi-daemon qterminal gnome-keyring pinentry*
```

8.1.1 Détails sur tous les éléments composant le système

Lire ceci n'est absolument pas indispensable, c'est juste pour information, et pour rendre possible d'apprendre à quoi ils servent, au cas où.

- openssh-server : service réseau pour pouvoir accéder à distance au serveur en protocole SSH (port réseau TCP/IP 22 par défaut). Penser à personnaliser /etc/ssh/sshd_config pour "PermitRootLogin" si on veut explorer le système en root (la commande su/sudo est rarement implémentée dans les explorateurs de fichiers par réseau). Permet entre autre la connexion via Putty et WinSCP.
- openvpn : permet de se connecter à un serveur VPN (ou d'en créer un, moyennant le suivi d'un tutoriel – non couvert dans ce document)
- fail2ban : auto bannissement 10 minutes d'adresse IP en cas de tentatives de connexion SSH erronées. Actif par défaut sur SSH port 22 mais possibilité de l'activer sur d'autres ports et services réseaux.
- dbus : outil/bus de communication entre service logiciels, Debian en a tout le temps besoin.
- systemd-timesyncd : Debian en a besoin pour pouvoir activer le maintien à l'heure de l'horloge BIOS. Requis : régler/considérer l'horloge BIOS en « UTC », commande : `timedatectl set-local-rtc 0`
- acpi : "acpi -bi" permet de connaître les détails de l'état des batteries (sur laptop) incluant charge, usure, durée restante prévisionnelle, etc. Sans doute d'autres applications possibles.

- net-tools : commandes réseaux parfois utiles comme ifconfig, netstat...
- dnsutils whois traceroute nmap ethtool : commandes réseaux comme nslookup entre autres, whois, traceroute, nmap, et gestion des ports Ethernet (EEE, vitesse etc)
- wget : utilitaire simple en ligne de commande pour télécharger un fichier via son adresse http/https/ftp (aucune complexité d'utilisation).
- curl : utilitaire plus poussé pour télécharger via + de protocoles que wget, mais plus tordu à utiliser. Requis par certains scripts et logiciels.
- aria2 : téléchargeur en commande également. Via "aria2c -x 16 -s 16 http://lien", possibilité de télécharger sur 16 connexions simultanées. Aria2c gère aussi le protocole bittorrent.
- iperf / iperf3 : test de bande passante réseau, TCP ou UDP, envoi ou réception, client ou serveur
- stress-ng : stress-test pour charge/conso/chauffe max CPU (utile pour vérifier graisse thermique et capacités ventilations)
- memtester : permet le test RAM de la mémoire disponible depuis Linux
- memtest86+ : permet depuis GRUB de lancer un test de mémoire RAM à la place de lancer Linux
- smartmontools : smartctl -a /dev/sdX pour avoir l'état d'un HDD ou SSD
- bwm-ng : moniteur de bande passante réseaux et disques, fonctionnel en ligne de commandes
- usbtopy : un peu comme "bwm-ng" et "top" mais pour la bande passante des ports USB
- usbutils : commandes "lsusb" et "usb-devices" entre autre
- lm-sensors : commande "sensors" pour voir les températures et parfois + (dépend des cartes mères)
- gvfs-backends gvfs-fuse : accès à sftp://, smb:// etc depuis les explorateurs de fichier graphiques
- ntfs-3g : parfois requis pour pouvoir lire et écrire dans des partitions/disques Windows « NTFS »
- wireless-tools iw : commandes iwconfig, iw phy, iwlist scan, et autres pour avoir toutes les infos WiFi
- cpufrequtils : "cpufreq-info" permet de collecter les infos de fréquence CPU, "cpufreq-set" permet de forcer une fréquence ou un mode (powersave, performance etc).
- firmware-linux firmware-ralink firmware-realtek firmware-iwlwifi : installe tous les fichiers "firmwares" pour insertion dynamique dans les composants de l'ordi (microcodes processeurs, firmware des cartes graphiques, WiFi pour gérer WPA2 voire 3, etc). Nécessaire pour certains drivers
- dkms : en cas d'installation de driver comme NVIDIA propriétaire, nécessaire pour que le driver s'adapte automatiquement aux mises à jour du noyau Linux (plus besoin de réinstaller le driver)
- msmtplib s-nail mailutils : outils d'envoi de mail par ligne de commande (utile pour unattended upgrade ou tout rapport scripté)
- unattended-upgrades : permet les mises à jour automatique via une configuration par défaut ultra tordue dans "/etc/apt/apt.conf.d/50unattended-upgrades", qu'on va grandement simplifier
- sysstat : pour commande "iostat -m" (ou watch -n 1 iostat -m) permettant de suivre l'utilisation disque en temps réel.
- ntpdate : permet de jouer manuellement "ntpdate ntp.u-psud.fr" par exemple si l'heure a merdé ou en cas de doute

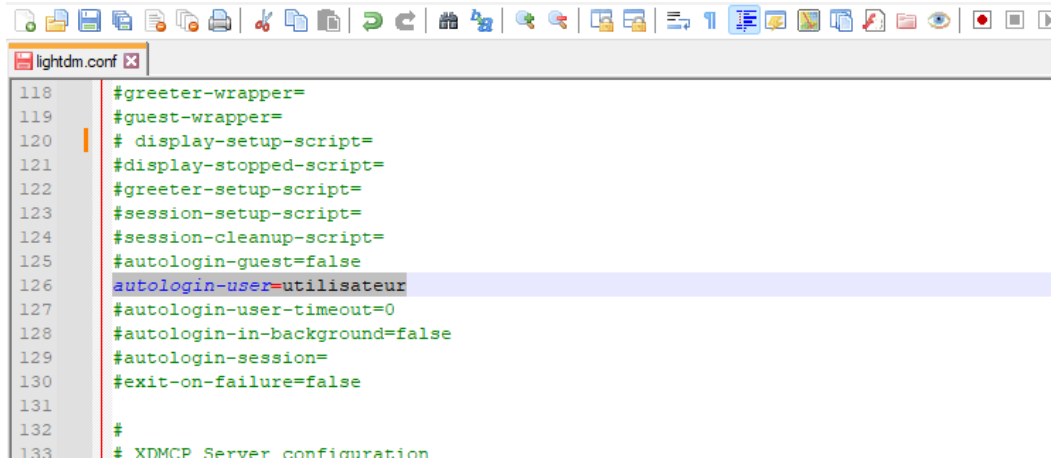
- `ffmpeg` : sous programme utilisé par d'autres, utilisable en ligne de commande. Galère à utiliser à la main soi même, mais peut absolument tout faire en terme d'encodage et décodage vidéo et audio.
- `vdpaudio` `vainfo` : info sur le décodage hardware / GPU. Outil de debug en cas de bug/lenteur sur un décodage vidéo
- `clinfo` `vulkan-tools` `mesa-utils` : infos de compatibilité GPU : OpenCL via "`clinfo`" (calcul par GPU), infos de compatibilité Vulkan (rendu GPU) via "`vulkaninfo`", et OpenGL (rendu GPU) via "`glxinfo`"
- `tcpdump` : capture réseau, `tcpdump` sait fonctionner en l'absence de bureau et tout mettre dans un fichier « pcap ». Wireshark peut ensuite être utilisé pour ouvrir les capture réalisées par `tcpdump`
- `lightdm` : gestionnaire de bureau incluant X.Org, répandu, fiable, fonctionne avec tous les bureaux (KDE, Gnome, LXDE, etc).
- `lxqt-core` : Bureau : ensemble barre des tâches, icônes, explorateur etc, relative simple et propre.
- `numlockx` : allumage automatique de la touche numlock (pavé numérique) au démarrage de X.Org
- `lxterminal` : permet d'ouvrir une invite de commande depuis le bureau
- `baobab` : analyse des occupations d'espace disque, présentées sous une forme hyper pratique
- `brasero` : équivalent Nero Burning ROM, gravure CD/DVD/Blu-ray et création de fichiers ISO.
- `doublecmd-qt` : explorateur à deux fenêtres, pratiques et sait fonctionner en mode « su root »
- `scrot` : gestion Impr-Ecran qui capture aussitôt dans un fichier (dans `/home/utilisateur/`)
- `gnome-system-monitor` : moniteur d'utilisation CPU, RAM, Réseau, et d'applications en cours
- `gnome-disk-utility` : présentation pratique et lisible des disques et de leurs partitions présentes, de l'état physique des disques (SMART), et des points de montage. Relativement incontournable.
- `gparted` : utilitaire graphique plus rustre, mais disposant de fonctionnalités précises pour redimensionner / créer de nouvelles partitions, et de nouvelles tables de partitions (disques vierges)
- `file-roller` : équivalent à 7zip pour linux
- `gcalculator` : calculatrice simple
- `gedit` : éditeur de texte
- `ghex` : éditeur hexadécimal utilisable, pour les rares cas où on en a besoin.
- `meld` : excellent outil de comparaison de dossiers / fichiers, dispo sous Windows également
- `filezilla` : un peu comme WinSCP (mais WinSCP n'existe pas sous Linux)
- `x11vnc`: serveur de bureau à distance, un peu archaïque (vivement la sortie de Stream-Rider).
- `synaptic` : interface graphique pour « apt update » « apt install » permettant de retrouver / supprimer les paquets existants et de faire des recherches (dans les noms de logiciels voire leurs descriptions).
- `build-essential` `gdb` `valgrind` `git` `subversion` `libgl1-mesa-dev` : outils de programmation
- `network-manager-gnome` : service "network-manager" + interface de gestion en tray icon dans le coin
- `blueman` : bluetooth manager, s'active quand un module bluetooth présent sur le PC est fonctionnel
- `wireshark` : peut ouvrir les captures réseaux de `tcpdump`, mais aussi les faire lui même
- `telnet` : outil réseau ancêtre de `putty` et SSH, plus très utilisé de nos jours

8.2 Configuration des éléments installés

8.2.1 LightDM : auto login

On va demander à LightDM (dont le rôle est de lancer le serveur d'affichage à la place de la console, et de charger le bureau LXQT) de faire un login automatique de la session « **utilisateur** ».

Depuis « **nano** » en ligne de commandes, ou via **WinSCP**, éditer le fichier `/etc/lightdm/lightdm.conf`



```
118 #greeter-wrapper=  
119 #guest-wrapper=  
120 # display-setup-script=  
121 #display-stopped-script=  
122 #greeter-setup-script=  
123 #session-setup-script=  
124 #session-cleanup-script=  
125 #autologin-guest=false  
126 autologin-user=utilisateur  
127 #autologin-user-timeout=0  
128 #autologin-in-background=false  
129 #autologin-session=  
130 #exit-on-failure=false  
131  
132 #  
133 # XDMCP Server configuration
```

Au prochain démarrage on n'aura pas besoin de taper le nom d'utilisateur et son mot de passe (en revanche, par le réseau par SSH par exemple, la session « utilisateur » reste bien entendue protégée par mot de passe).

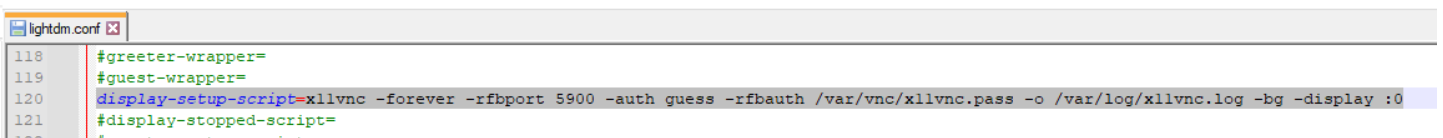
8.2.2 Bureau à distance « X11VNC »

Depuis une ligne de commande / terminal root (par putty par exemple), entrer les commandes suivantes :

```
mkdir -p /var/vnc/  
x11vnc -storepasswd /var/vnc/x11vnc.pass
```

La seconde permet de choisir le mot de passe VNC. Du fait que VNC soit vieux et obsolète, le mot de passe ne peut faire que 8 caractères (les caractères supplémentaires sont silencieusement ignorés).

De façon à ce que X11VNC s'ouvre automatiquement au démarrage, et ce, uniquement quand le serveur d'affichage est prêt (sinon, il plante et se referme), on va ré-utiliser LightDM et son fichier de configuration :



```
118 #greeter-wrapper=  
119 #guest-wrapper=  
120 display-setup-script=x11vnc -forever -rfbport 5900 -auth guess -rfbauth /var/vnc/x11vnc.pass -o /var/log/x11vnc.log -bg -display :0  
121 #display-stopped-script=  
122 -----  
123 -----
```

La commande que LightDM doit exécuter quand il est prêt, est :

```
display-setup-script=x11vnc -forever -rfbport 5900 -auth guess -rfbauth  
/var/vnc/x11vnc.pass -o /var/log/x11vnc.log -bg -display :0
```

8.2.3 Ajustements systèmes

Un réglage par défaut controversé, permet aux logiciels mal développés (mauvaise gestion mémoire) de fonctionner quand même. En contre partie si le système manque de RAM disponible il a tendance à planter.

Les applications mal développées iront se faire mettre, on va garder le système stable :

Depuis un terminal root, entrer les commandes suivantes :

```
echo vm.overcommit_memory=1 > /etc/sysctl.conf  
sysctl -p && update-initramfs -u && reboot
```

Aussi, quand depuis le bureau on ouvre un terminal, on est alors en mode « utilisateur », et certaines opérations d'administration système sont alors impossibles.

La commande « su root » (pour switch user : root) permet de demander à devenir root. Afin que toutes les commandes disponibles pour « root » deviennent alors disponibles après avoir joué « su root », depuis une invite de commande « root » jouer la commande suivante :

```
echo "ALWAYS_SET_PATH yes" > /etc/login.defs
```

Aux prochains usages de « su root », toutes les commandes root seront disponibles (reboot, mdadm etc)

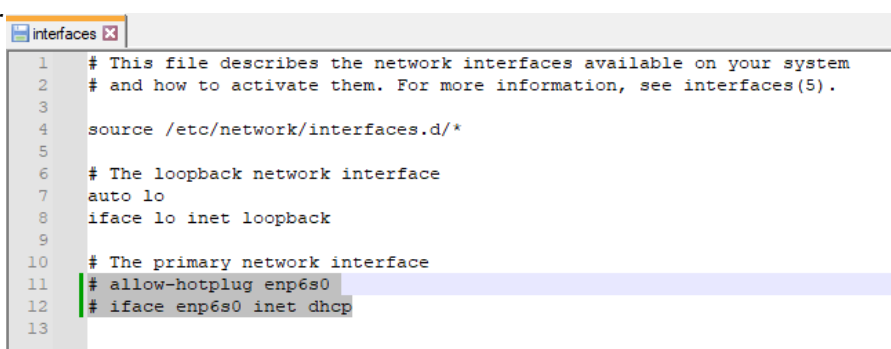
8.2.4 Gestionnaire de réseau

L'installation minimaliste de Debian inclus un gestionnaire de réseau, appelé « ifupdown » qui est réglé via des fichiers dans « /etc/network/ ». Il est réglé pour gérer notre carte réseau. Or, nous n'avons plus besoin de ça après avoir installé « gnome-network-manager », plus intuitif avec son interface graphique.

Pour que le gnome-network-manager soit le seul à gérer la carte réseau, éditer le fichier

« /etc/network/interfaces » et mettre un # devant les lignes suivantes.

Au prochain démarrage, c'est « network-manager-gnome » qui gèrera seul la carte réseau.



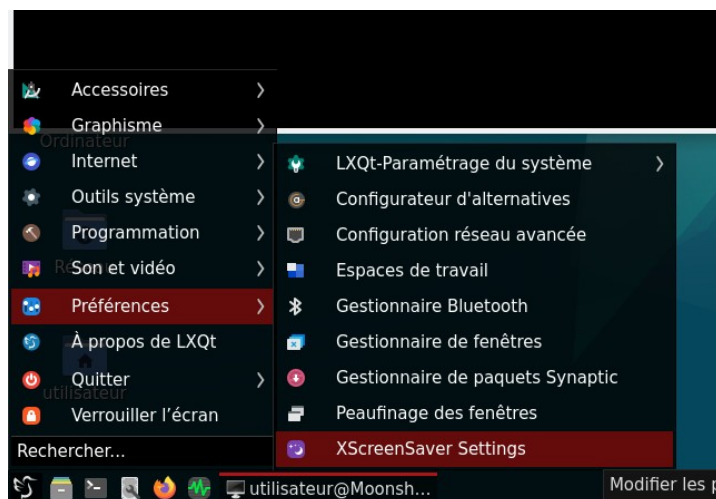
```
1 # This file describes the network interfaces available on your system
2 # and how to activate them. For more information, see interfaces(5).
3
4 source /etc/network/interfaces.d/*
5
6 # The loopback network interface
7 auto lo
8 iface lo inet loopback
9
10 # The primary network interface
11 # allow-hotplug enp6s0
12 # iface enp6s0 inet dhcp
13
```

8.2.5 Personnalisation du bureau

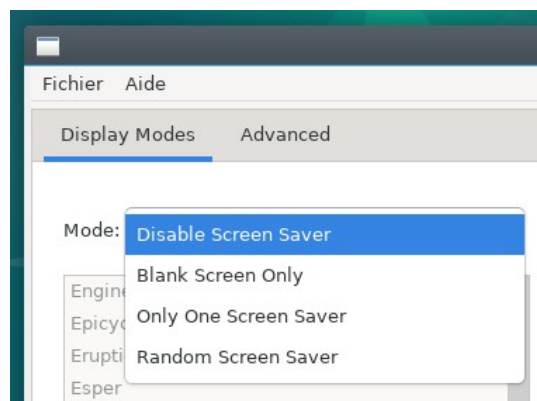
Les configurations qui suivent sont optionnelles, il ne s'agit que de préférences qu'on peut changer quand on le souhaite.

On peut toutefois les regarder en détails, pour mieux connaître le système.

Réglage de l'écran de veille :



Pour personnaliser l'écran de veille, aller dans le menu démarrer, « Préférences », « XScreensaver Settings ».



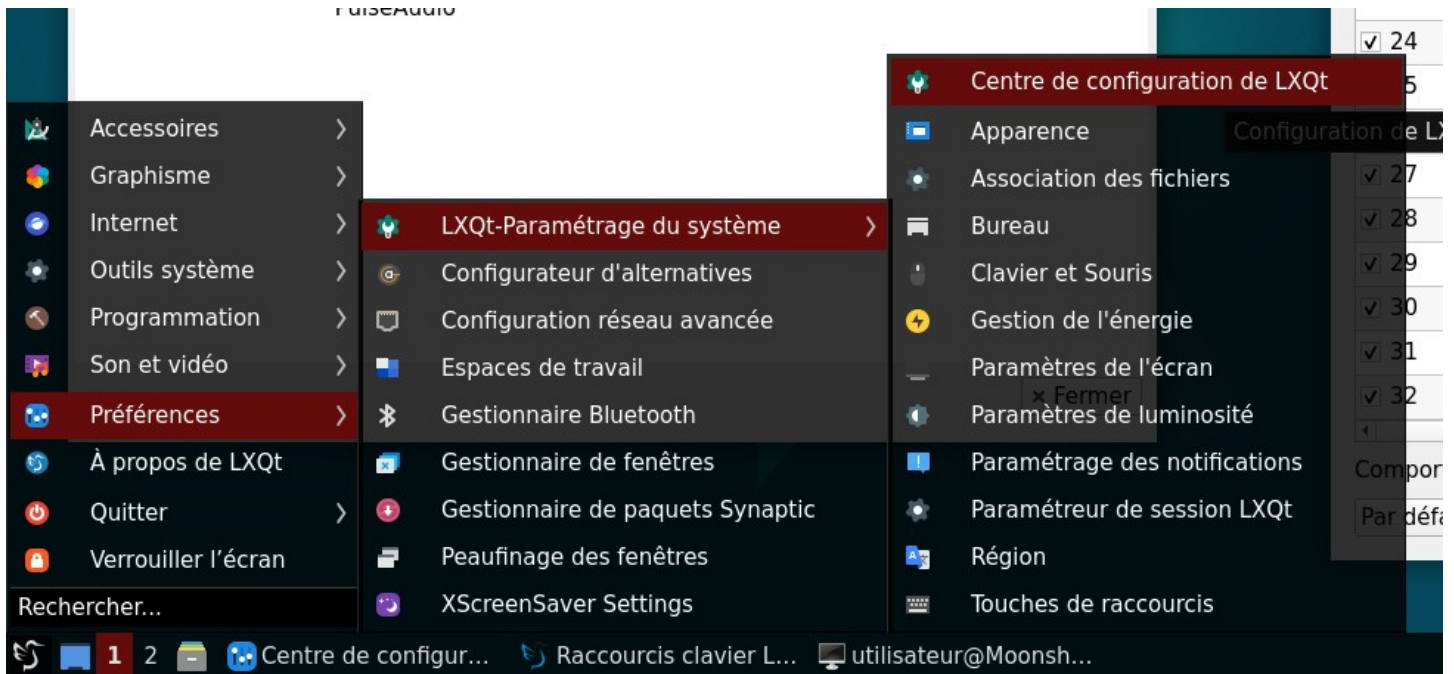
Réglage « multi bureaux » :

Les développeurs / utilisateurs de Linux font souvent une fixette sur le fait d'avoir deux bureaux voire + même pour 1 seul écran, de n'en afficher qu'un seul, en utilisant un raccourci pour passer de l'un à l'autre.

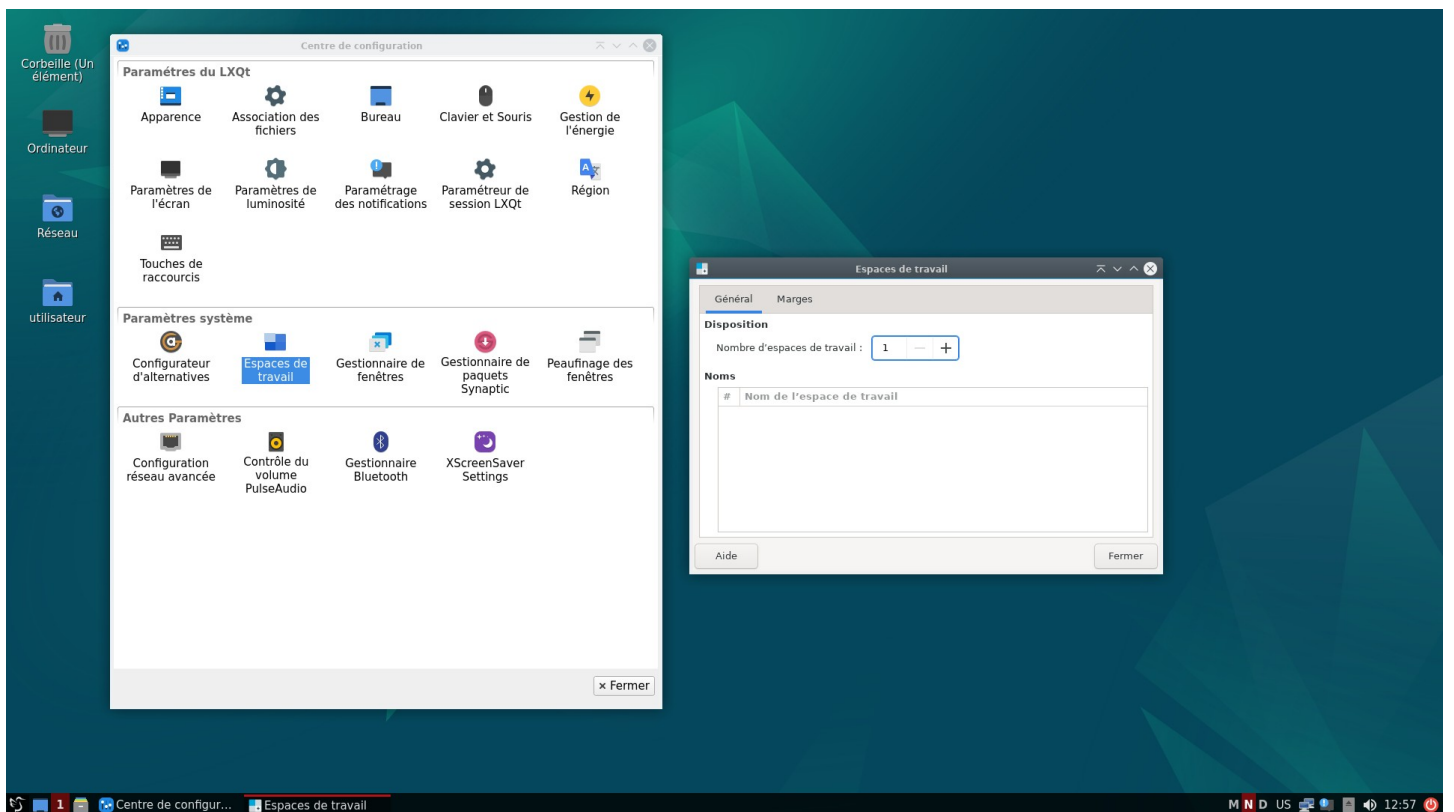
S'il n'est pas prévu d'utiliser cette fonctionnalité, deux choses à faire.

Passage à 1 seul bureau :

Menu démarrer > Préférences → LXQt-Paramétrage du système > Centre de configuration LXQt

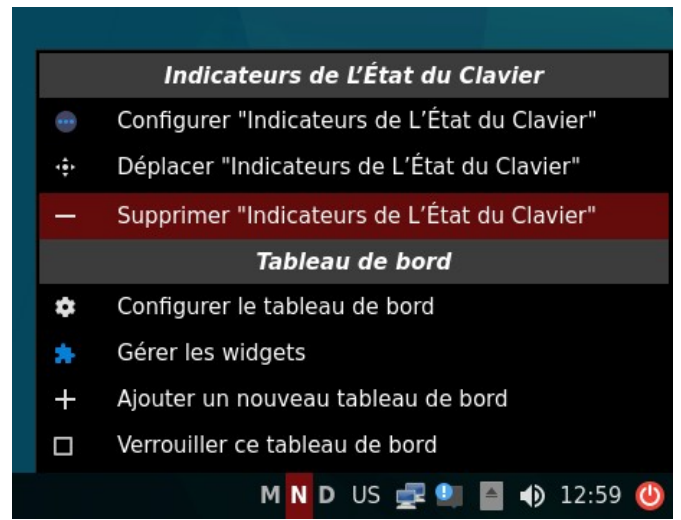
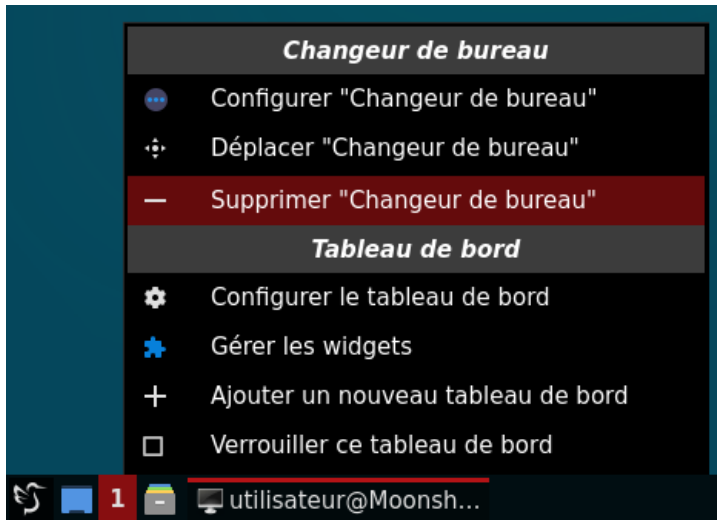


Puis dans « Espaces de travail », mettre le nombre d'espaces de travail à « 1 ».

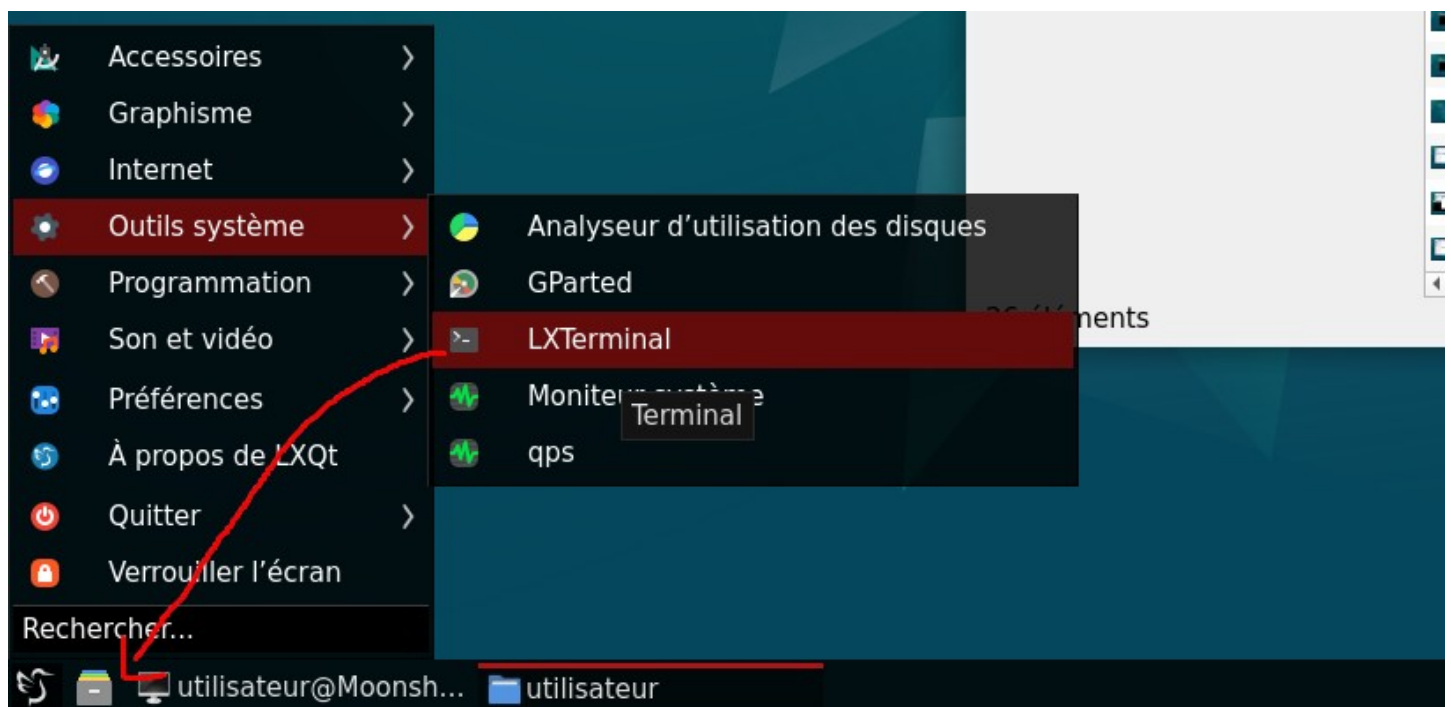
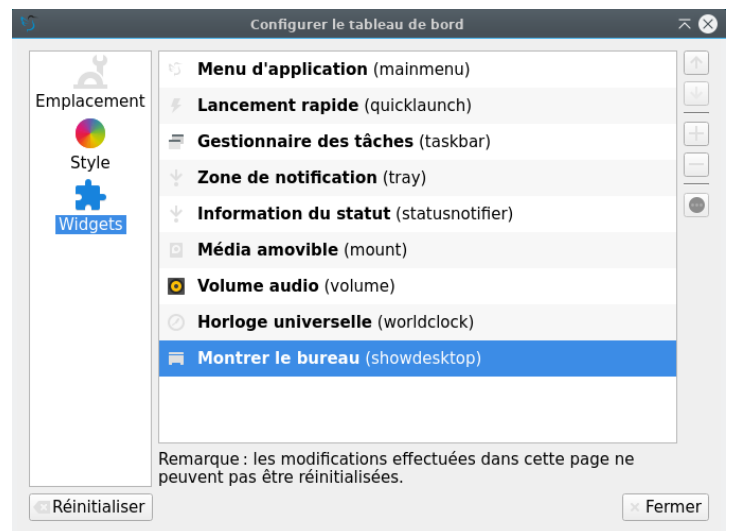
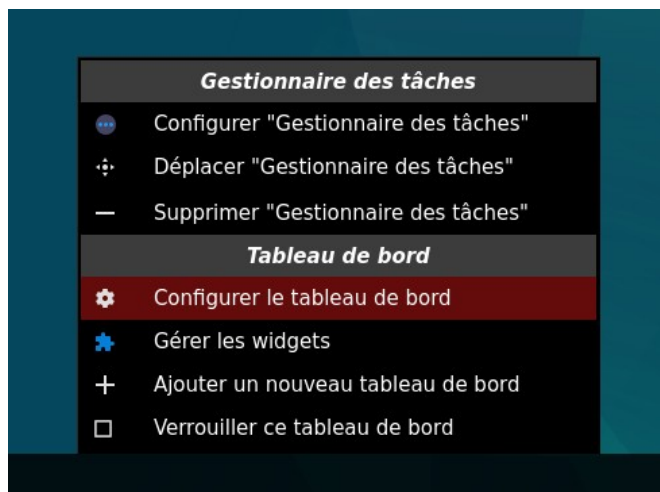


Il reste encore une petite icône en bas à gauche, avec écrit « 1 », permettant de passer du bureau « 1 » à aucun autre, puisqu'il est désormais tout seul.

Il est possible de supprimer cette icône, de même pour les indicateurs claviers « MND US » via clic droit :



Il est également possible de modifier l'ordre des icônes (par exemple le carré bleu pour baisser les applications et accéder au bureau, peut être placé tout à droite, et le bouton power peut être viré)

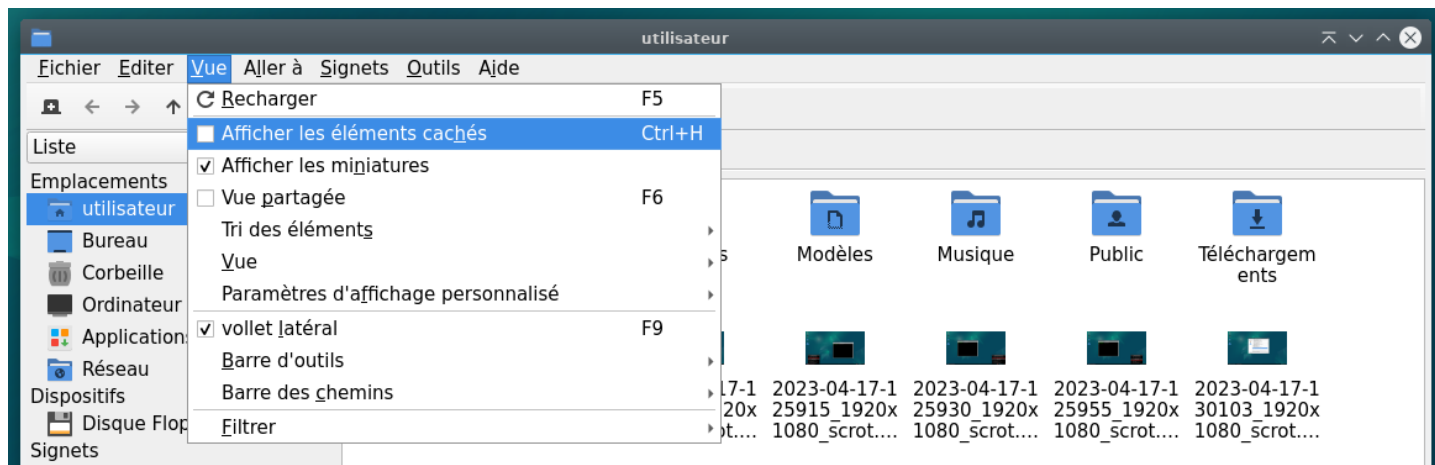


On peut glisser les raccourcis qu'on veut en « Quick launch » à côté du menu démarrer, en les glissant depuis le menu démarrer (ces ajouts s'enregistrent dans /home/utilisateur/.config/lxqt/panel.conf)

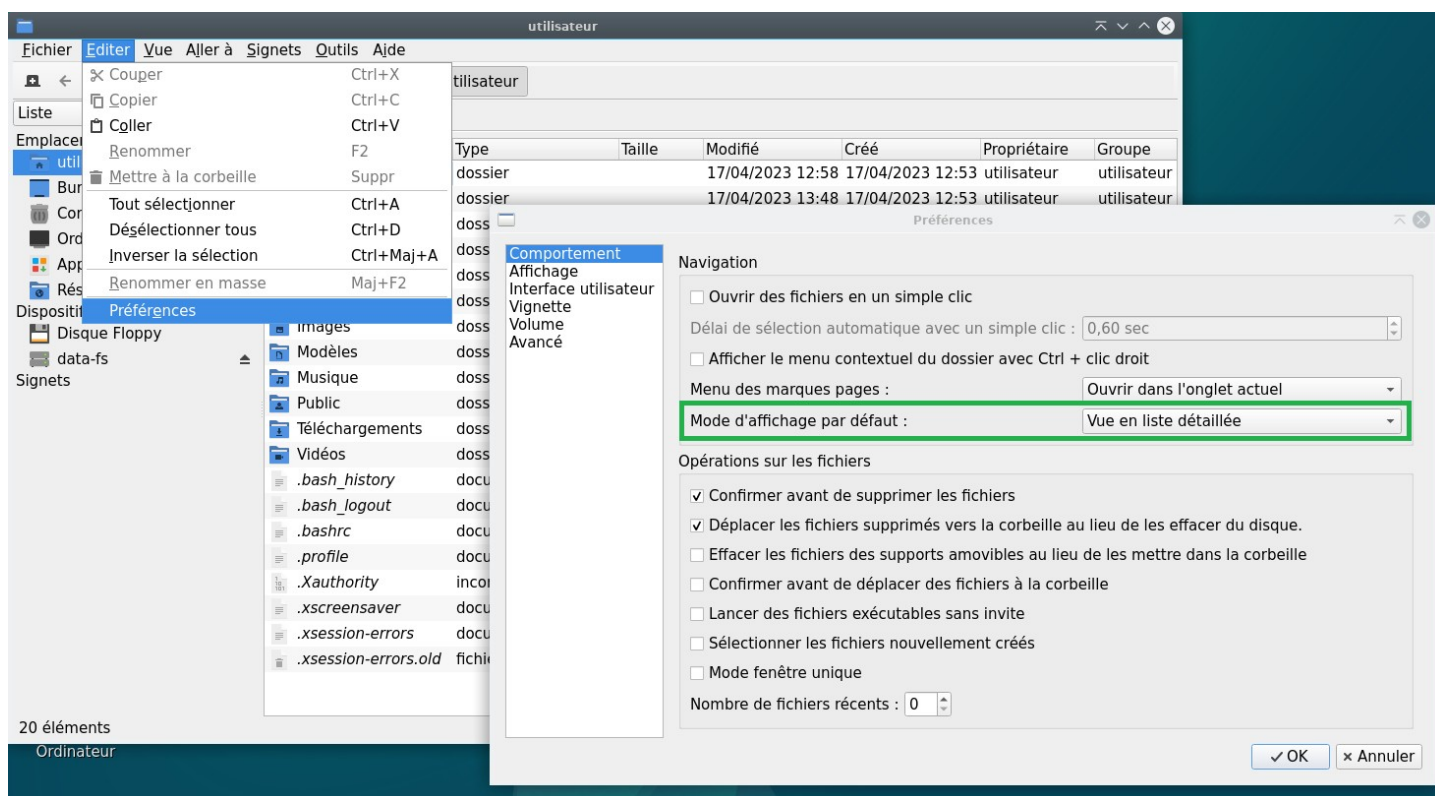
Dans l'explorateur de fichier, il est possible de passer à une vue en « **liste détaillée** » (les noms complets sont affichés, triés dans l'ordre, plus pratique). On peut aussi demander à **voir les fichiers cachés**.

Bon à savoir : Sous Linux les fichiers (et dossiers) cachés sont ceux commençant par un point. Il ne s'agit pas d'un attribut caché comme sous Windows. Depuis un terminal, pour les lister, « **ls -a** ».

Pour voir les fichiers cachés :

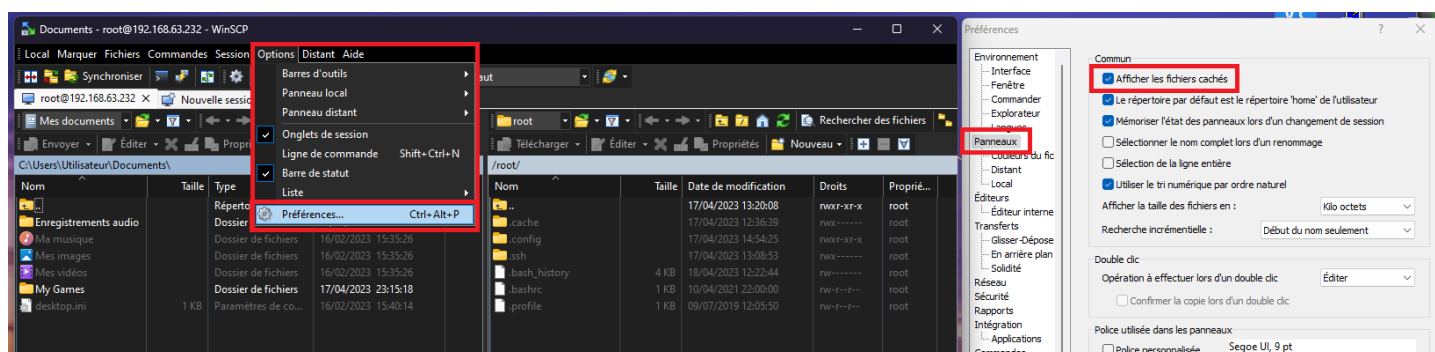


Pour mettre le mode d'affichage par défaut en « **Vue en liste détaillée** » :



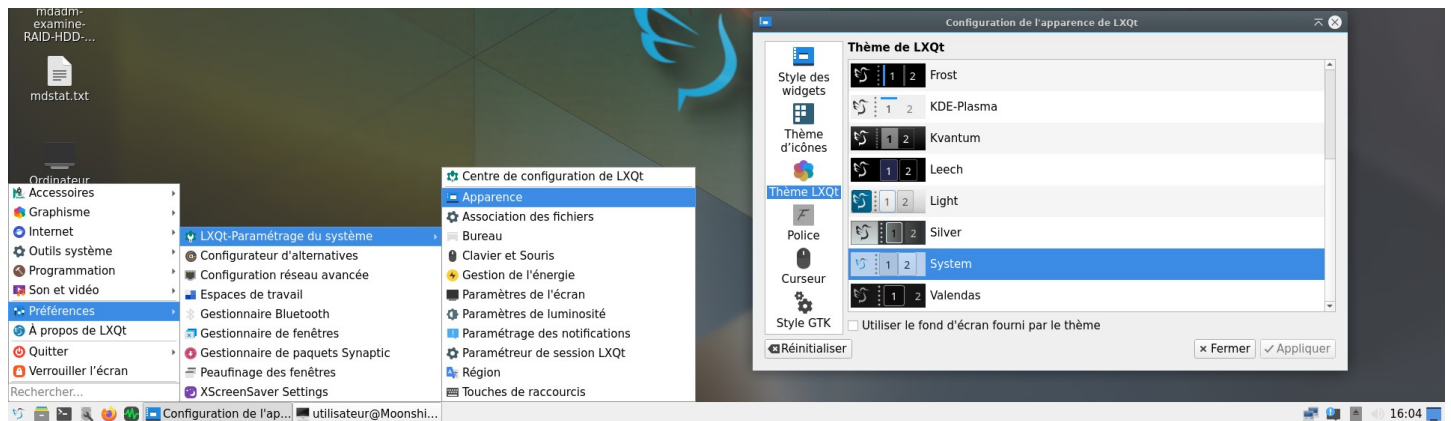
Dans « **Avancé** », sélectionner « **lxterminal** » pour que l'explorateur sache que c'est lui qui est installé.

Petite parenthèse sur **WinSCP** : Par défaut lui non plus ne montre pas les fichiers cachés !

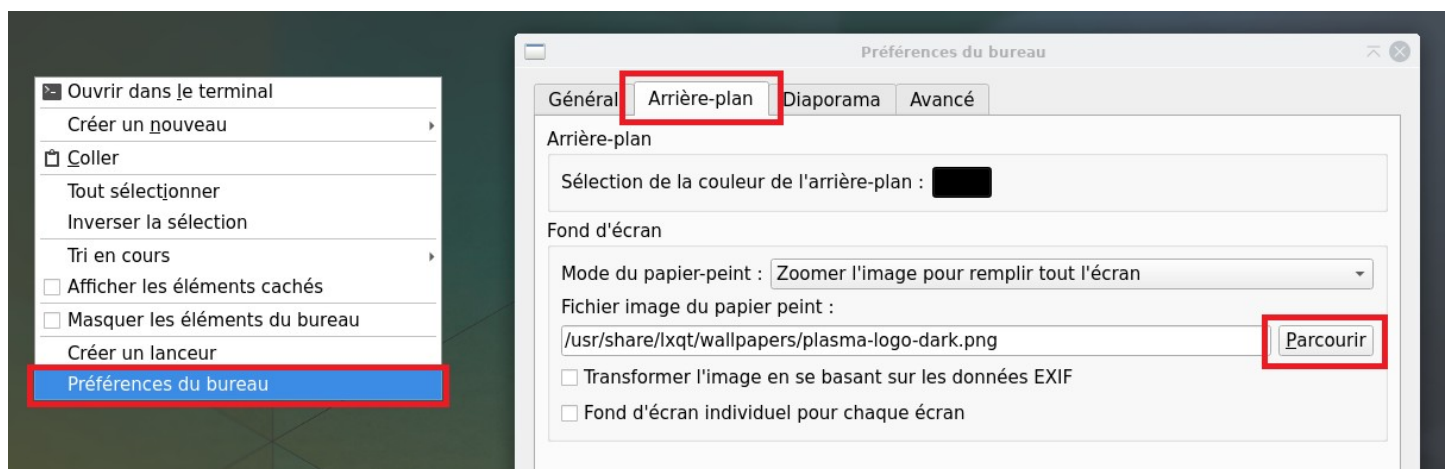


Thèmes et fond d'écran :

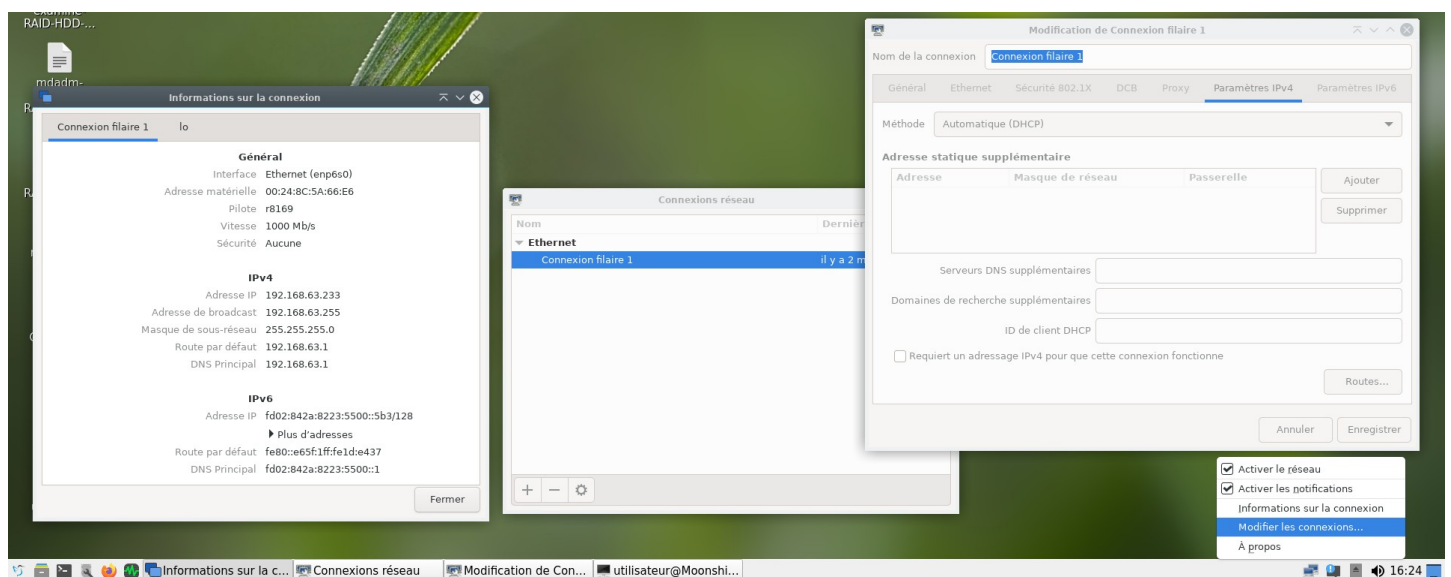
Plusieurs thèmes sont disponibles



Pour le fond d'écran, un « clic-droit » sur le bureau permet d'aller le changer facilement



Petit aperçu de ce que donne le « gnome-network-manager » :



En cas d'insertion de carte WiFi (interne ou USB), ou de branchement de téléphone en partage de connexion USB, ça devrait fonctionner sans problème, la connexion devrait apparaître dans la liste.

Le clic normal (gauche) sur l'icône puis sur une connexion, permet de réinitialiser rapidement celle-ci.

La gestion « IPv6 » est également fonctionnelle (avec réglages possibles concernant DHCPv6, SLAAC...)

9 Création RAID 5 - à parité répartie (sur 3 disques)

L'ordre de création s'effectue en ligne de commandes, mais on va tout de même utiliser quelques outils graphiques pour visualiser ce qu'on fait, et préparer les disques.

Attention : ordre des disques durs

Bien que les SSD et HDD soient branchés dans l'ordre sur la carte mère (tout en haut les SSD en 1 et 2, puis en bas les disques durs HDD en 3 4 et 5, on part d'en haut pour 1 vers en bas pour 5), dans Windows comme dans Linux, l'ordre d'apparition des disques durs n'est pas prévisible.

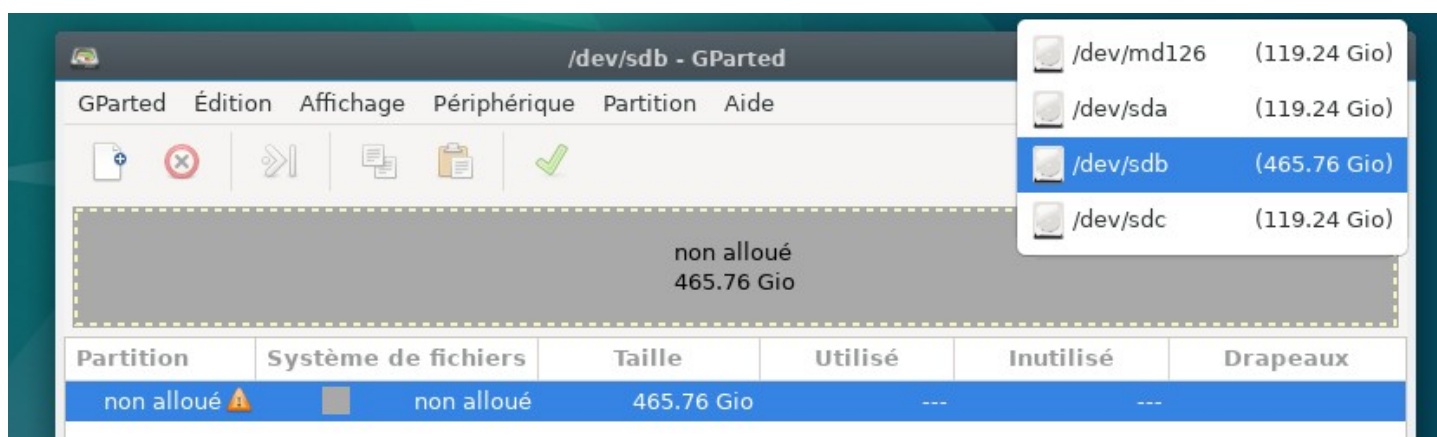
Solution : afin de ne faire aucune erreur, et de pouvoir plus facilement les identifier, il est préférable de les initialiser un par un, en n'en branchant qu'un seul à la fois pour ne pouvoir faire aucune erreur.

Dans chaque disque dur on va créer une partition unique, nommée de façon à ce que son numéro de disque apparaisse de façon évidente pour la suite. On notera aussi leurs numéros de série.

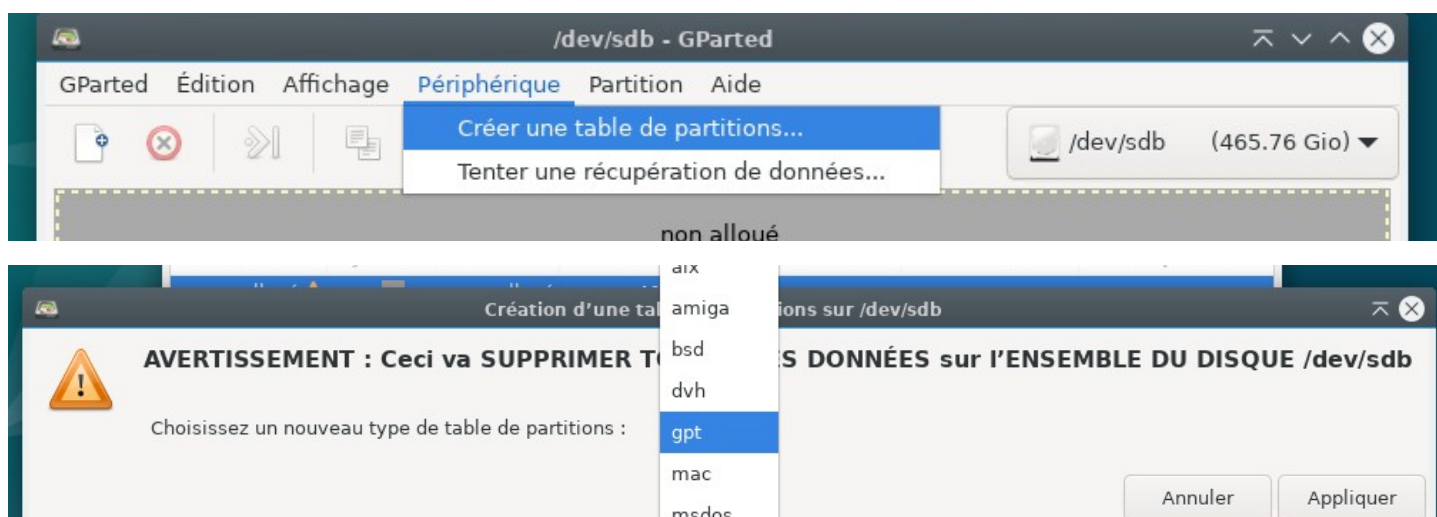
9.1 Initialisation premier disque

Après n'avoir connecté qu'un seul disque sur les 3 (le premier), utiliser « **GParted** » (présent dans le menu démarrer).

Ici, notre 1^{er} disque HDD de 500 Go (500 000 000 000 octets, divisé par 1024 à trois reprise = 465 Gio) apparaît en tant que « /dev/sdb » : attention après redémarrage ça peut changer.



Les disques durs n'étant que des « feuilles blanches » au départ, les partitions sont à définir via un langage bien précis que l'ordinateur peut comprendre. Bien que pendant des années, c'est le langage de partition « MBR / Master Boot Record / MS-DOS » qui prédominait, désormais avec les disques de grande taille et les systèmes modernes, on utilise « GPT » pour « GUID Partition Table »



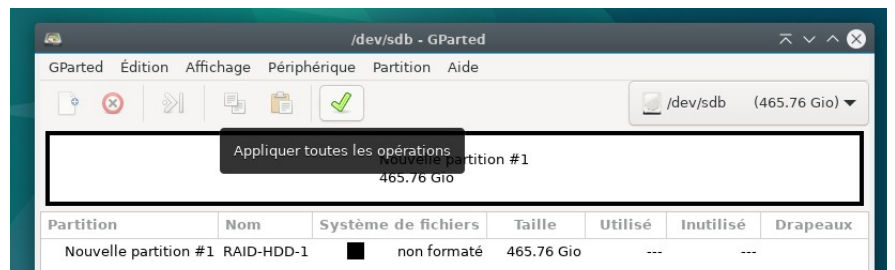
Une fois la table de partition créée, on va créer une partition vierge (non formatée, le sous système RAID s'en chargera lui même).



On peut entrer ici le nom de la partition « **RAID-HDD-1** » et choisir « **non formaté** ».



L'étape suivante consiste à valider en utilisant le petit V en vert.



9.2 Initialisation du second disque

Après avoir connecté le second disque, puis ré-ouvert GParted, trouver ce second disque dans la liste. Le premier contient déjà une partition donc ça devrait être possible de ne pas les confondre.

Certains ordinateurs permettent de connecter un disque dur « SATA » à chaud (sans éteindre le PC). Sur celui-ci ça fonctionne. Attention néanmoins en baladant les fiches d'alimentation (contact accidentel = 🤖)

Suivre les mêmes étapes en appelant sa partition « **RAID-HDD-2** »

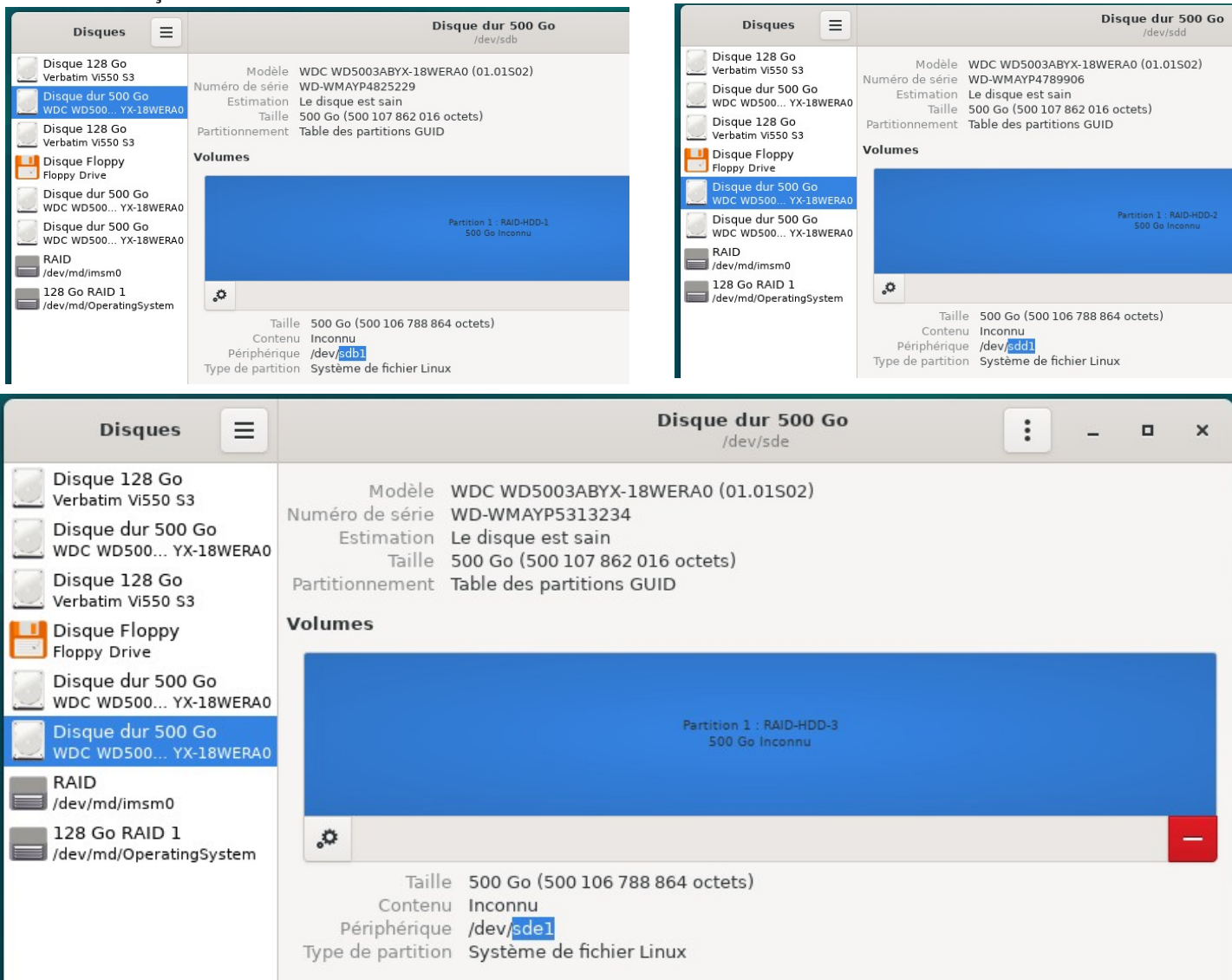
9.3 Initialisation du troisième disque

Tout pareil, nom de la partition : « **RAID-HDD-3** »

9.4 Préparation de la commande de création de RAID 5

Suite à la préparation des trois disques durs, il nous faut, dans l'ordre, l'adresse des partitions qu'on a créé.

L'utilitaire « gnome-disks » (appelé « Disques » dans le menu démarrer) peut nous permettre de bien résumer tout ça.



Les disques sont (dans l'ordre) /dev/sdb /dev/sdd et /dev/sde, contenant chacun 1 partition numérotée 1.

Les partitions qu'on va utiliser sont donc (dans l'ordre) /dev/sdb1 /dev/sdd1 /dev/sde1

La commande de création sera :

```
mdadm --create /dev/md0 --level=5 --name=Data --raid-devices=3 /dev/sdb1 /dev/sdd1 /dev/sde1
```

Le « 0 » de « /dev/md0 » peut être remplacé par un autre nombre (ça n'a pas d'importance) en revanche on a pu voir sur « GParted » que /dev/md126 était déjà pris. Il semble de toute façon que ce numéro n'est pas fixe.

9.5 Exécution

Depuis un terminal root (ou après avoir joué « su root » depuis un terminal utilisateur) entrer les commandes suivantes (remplacer sdb1, sdd1 et sde1 au besoin) :

```
apt install mdadm
```

```
mdadm --create /dev/md0 --level=5 --name=Data --raid-devices=3 /dev/sdb1 /dev/sdd1 /dev/sde1
```

9.6 Mise à l'abri de toutes les informations utiles

Si une maladresse venait à survenir un jour. Par exemple, une commande mdadm jouée par erreur qui effacerait, ou écraserait, ou permuterait la configuration RAID permettant d'accéder aux données du volume RAID, ou si leurs partitions (et leurs noms) étaient effacés ou écrasés par inadvertance :

Il est utile de jouer quelques commandes qui permettront d'avoir toutes les informations requises concernant les détails du volume RAID fraîchement créé, afin de pouvoir retrouver l'accès à tout et réparer les bêtises.

Depuis un terminal root :

```
mdadm --detail /dev/md/Data > /home/utilisateur/Desktop/mdadm-details.txt
cat /proc/mdstat > /home/utilisateur/Desktop/mdstat.txt
mdadm --examine /dev/sdb1 > /home/utilisateur/Desktop/mdadm-examine-RAID-HDD-1.txt
mdadm --examine /dev/sdd1 > /home/utilisateur/Desktop/mdadm-examine-RAID-HDD-2.txt
mdadm --examine /dev/sde1 > /home/utilisateur/Desktop/mdadm-examine-RAID-HDD-3.txt
chown -R utilisateur:utilisateur /home/utilisateur/Desktop/
```

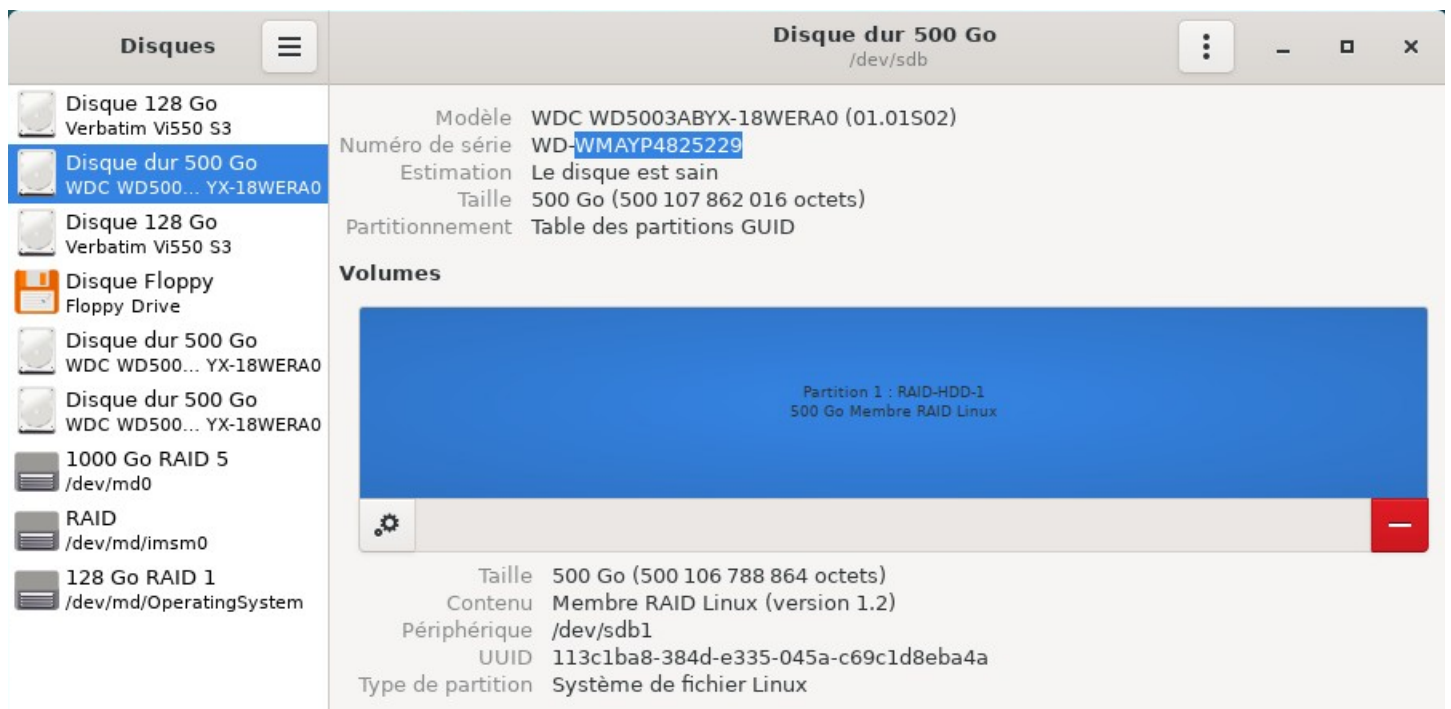
Attention ! Ici /dev/sdb1 est considéré HDD-1 mais après reboot, ce ne sera plus forcément « sdb1 »

Pour info : la dernière commande (chown) permet de donner à « utilisateur » le droit de posséder et modifier les fichiers déposés sur son bureau par « root » (sans ça utilisateur n'arriverait pas à les modifier).

9.7 Ajout de précision dans les informations utiles – pour recovery

Avant de redémarrer l'ordinateur, au risque de voir les adresses /dev/sdXX être permutées dans tous les sens, et de ne plus s'y retrouver :

Il s'agit simplement de remplacer, dans les fichiers, les allusions à /dev/sdXX par le nom des disques, et même leurs numéros de série (idéalement, les deux), en regardant sur « gnome-disks »



The screenshot shows the GNOME Disks application window. The left sidebar lists various storage devices, with the selected 500 Go hard drive highlighted. The main pane displays the following information:

- Disque dur 500 Go** (/dev/sdb)
- Modèle: WDC WD5003ABYX-18WERA0 (01.01S02)
- Numéro de série: WD-WMAYP4825229
- Estimation: Le disque est sain
- Taille: 500 Go (500 107 862 016 octets)
- Partitionnement: Table des partitions GUID
- Volumes**
- Partition 1 : RAID-HDD-1 (500 Go Membre RAID Linux)
- Taille: 500 Go (500 106 788 864 octets)
- Contenu: Membre RAID Linux (version 1.2)
- Périphérique: /dev/sdb1
- UUID: 113c1ba8-384d-e335-045a-c69c1d8eba4a
- Type de partition: Système de fichier Linux

Par exemple on peut voir ci-dessus que le disque « /dev/sdb1 » utilisé en « RAID-HDD-1 » porte le numéro de série « WD-WMAYP4825229 ». C'est important de noter le numéro de série, au cas où les disques seraient mélangés et que leur table de partition (contenant le numéro 1 2 ou 3 dans le nom) serait effacée.

Dans les fichiers indiquant « /dev/sdb1 » au moment de leur création, on pourra donc remplacer cette allusion à l'adresse du disque par son vrai nom + numéro de série.

Voici ce que ça donne avant et après :

```
C:\Users\Utilisateur\AppData\Local\Temp\scp25149\home\utilisateur\Desktop\mdadm-details.txt - Notepad++
Fichier Édition Recherche Affichage Encodage Langage Paramètres Outils Macro Exécution Modules d'extension Documents ?
mdadm-avant.txt
1 /dev/md/Data:
2 Version : 1.2
3 Creation Time : Mon Apr 17 15:13:37 2023
4 Raid Level : raid5
5 Array Size : 976506880 (931.27 GiB 999.94 GB)
6 Used Dev Size : 488253440 (465.63 GiB 499.97 GB)
7 Raid Devices : 3
8 Total Devices : 3
9 Persistence : Superblock is persistent
10
11 Intent Bitmap : Internal
12
13 Update Time : Mon Apr 17 15:45:13 2023
14 State : clean
15 Active Devices : 3
16 Working Devices : 3
17 Failed Devices : 0
18 Spare Devices : 0
19
20 Layout : left-symmetric
21 Chunk Size : 512K
22
23 Consistency Policy : bitmap
24
25 Name : Moonshine:Data (local to host Moonshine)
26 UUID : 49cabf11:47c06513:f0bc08ac:c7f14ccf
27 Events : 3
28
29
30 Number Major Minor RaidDevice State
31 0 8 33 0 active sync /dev/sdb1
32 1 8 65 1 active sync /dev/sdd1
33 2 8 49 2 active sync /dev/sde1
34
mdadm-details.txt
1 /dev/md/Data:
2 Version : 1.2
3 Creation Time : Mon Apr 17 15:13:37 2023
4 Raid Level : raid5
5 Array Size : 976506880 (931.27 GiB 999.94 GB)
6 Used Dev Size : 488253440 (465.63 GiB 499.97 GB)
7 Raid Devices : 3
8 Total Devices : 3
9 Persistence : Superblock is persistent
10
11 Intent Bitmap : Internal
12
13 Update Time : Mon Apr 17 15:45:13 2023
14 State : clean
15 Active Devices : 3
16 Working Devices : 3
17 Failed Devices : 0
18 Spare Devices : 0
19
20 Layout : left-symmetric
21 Chunk Size : 512K
22
23 Consistency Policy : bitmap
24
25 Name : Moonshine:Data (local to host Moonshine)
26 UUID : 49cabf11:47c06513:f0bc08ac:c7f14ccf
27 Events : 3
28
29
30 Number Major Minor RaidDevice State
31 0 8 33 0 active sync WD-WMAYP4825229 - RAID-HDD-1
32 1 8 65 1 active sync WD-WMAYP4789906 - RAID-HDD-2
33 2 8 49 2 active sync WD-WMAYP5313234 - RAID-HDD-3
34
Normal text file length: 1042 lines: 33 Ln: 30 Col: 1 Sel: 249|3 Unix (LF) UTF-8 INS
```

Même principe pour les fichiers « mdadm-examine » de chaque disque :

```
C:\Users\Utilisateur\Desktop\avant.txt - Notepad++
Fichier Édition Recherche Affichage Encodage Langage Paramètres Outils Macro Exécution Modules d'extension Documents ?
avant.txt
1 /dev/sdb1:
2 Magic : a92b4efc
3 Version : 1.2
4 Feature Map : 0x1
5 Array UUID : 49cabf11:47c06513:f0bc08ac:c7f14ccf
6 Name : Moonshine:Data (local to host Moonshine)
7 Creation Time : Mon Apr 17 15:13:37 2023
8 Raid Level : raid5
9 Raid Devices : 3
10
11 Avail Dev Size : 976506880 sectors (465.63 GiB 499.97 GB)
12 Array Size : 976506880 KiB (931.27 GiB 999.94 GB)
13 Data Offset : 264192 sectors
14 Super Offset : 8 sectors
15 Unused Space : before=264112 sectors, after=0 sectors
16 State : clean
17 Device UUID : 66c3f7bc:2e0ae5ca:9fb14c4d:f343f6c6
18
19 Internal Bitmap : 8 sectors from superblock
20 Update Time : Mon Apr 17 15:44:12 2023
21 Bad Block Log : 512 entries available at offset 16 sectors
22 Checksum : 60d2fee8 - correct
23 Events : 3
24
25 Layout : left-symmetric
26 Chunk Size : 512K
27
28 Device Role : Active device 0
29 Array State : AAA ('A' == active, '.' == missing, 'R' == replacing)
30
mdadm-examine-RAID-HDD-1.txt
1 WD-WMAYP4825229 - RAID-HDD-1:
2 Magic : a92b4efc
3 Version : 1.2
4 Feature Map : 0x1
5 Array UUID : 49cabf11:47c06513:f0bc08ac:c7f14ccf
6 Name : Moonshine:Data (local to host Moonshine)
7 Creation Time : Mon Apr 17 15:13:37 2023
8 Raid Level : raid5
9 Raid Devices : 3
10
11 Avail Dev Size : 976506880 sectors (465.63 GiB 499.97 GB)
12 Array Size : 976506880 KiB (931.27 GiB 999.94 GB)
13 Data Offset : 264192 sectors
14 Super Offset : 8 sectors
15 Unused Space : before=264112 sectors, after=0 sectors
16 State : clean
17 Device UUID : 66c3f7bc:2e0ae5ca:9fb14c4d:f343f6c6
18
19 Internal Bitmap : 8 sectors from superblock
20 Update Time : Mon Apr 17 15:44:12 2023
21 Bad Block Log : 512 entries available at offset 16 sectors
22 Checksum : 60d2fee8 - correct
23 Events : 3
24
25 Layout : left-symmetric
26 Chunk Size : 512K
27
28 Device Role : Active device 0
29 Array State : AAA ('A' == active, '.' == missing, 'R' == replacing)
30
Normal text file length: 991 lines: 30 Ln: 1 Col: 1 Sel: 10|1 Windows (CR.LF) UTF-8 INS
```

D'une version à l'autre de Linux, la création de RAID 5 ne structure pas toujours les données de la même façon.

En creusant bien tous les fichiers, on peut se rendre compte que les paramètres utilisés sont les suivants, au cas où il faudrait un jour redéclarer la structure RAID depuis une autre version de Linux :

```
mdadm --create /dev/md0 --level=5 --chunk=512K --metadata=1.2 --layout left-symmetric --data-offset=264 192s --raid-devices=3 RAID-HDD-1 RAID-HDD-2 RAID-HDD-3 --assume-clean --readonly
```

Si l'un des HDD est manquant ou écrasé/corrompu (mais que 2 sur les 3 n'ont pas été altérés), il est possible de remplacer l'adresse de ce disque par « missing », afin de ne récupérer les données que grâce aux 2 autres.

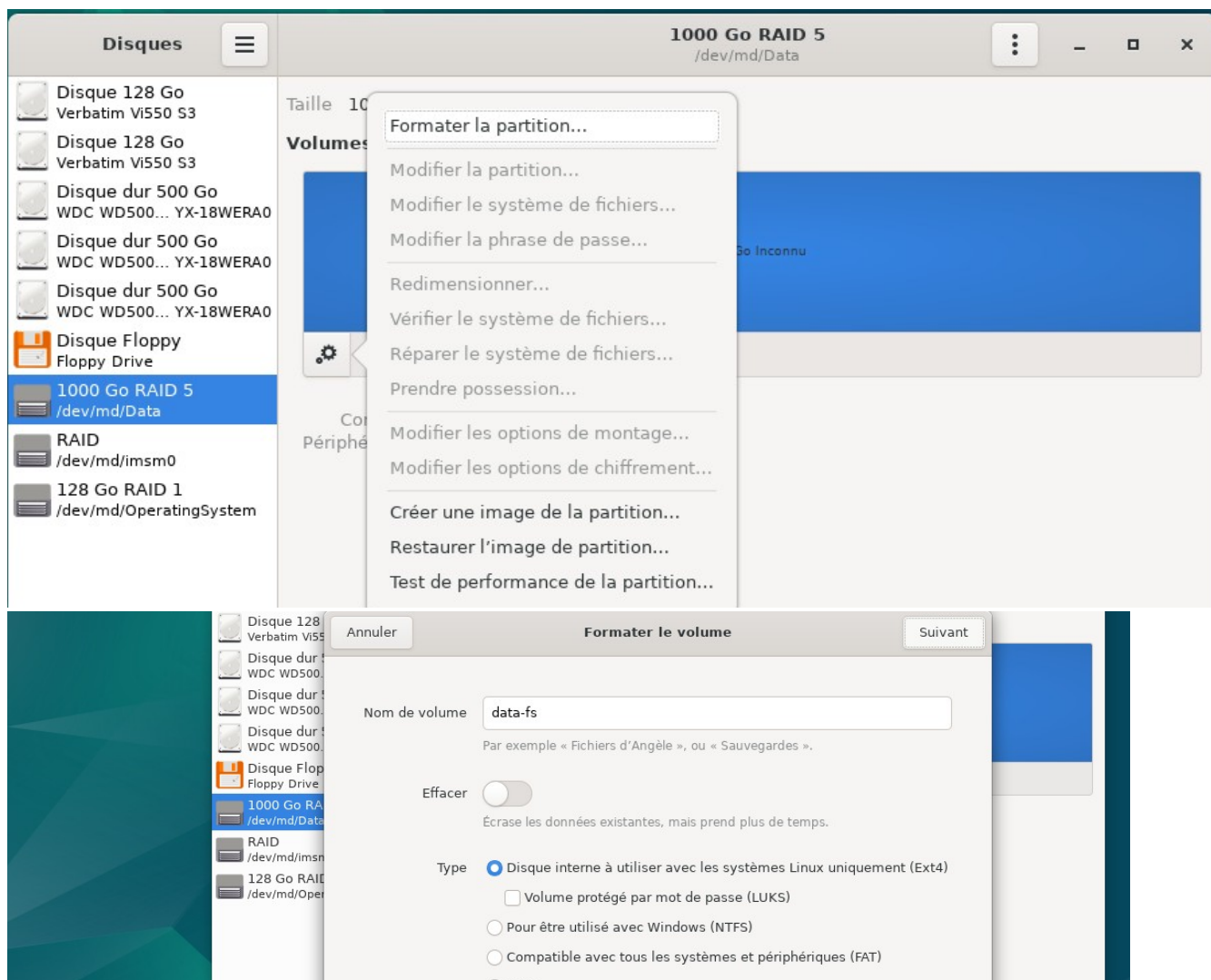
Si l'accès aux données est rétabli avec succès (vérifier le attentivement d'abord), on pourra passer à la suite.

10 Système de fichiers du volume RAID-5

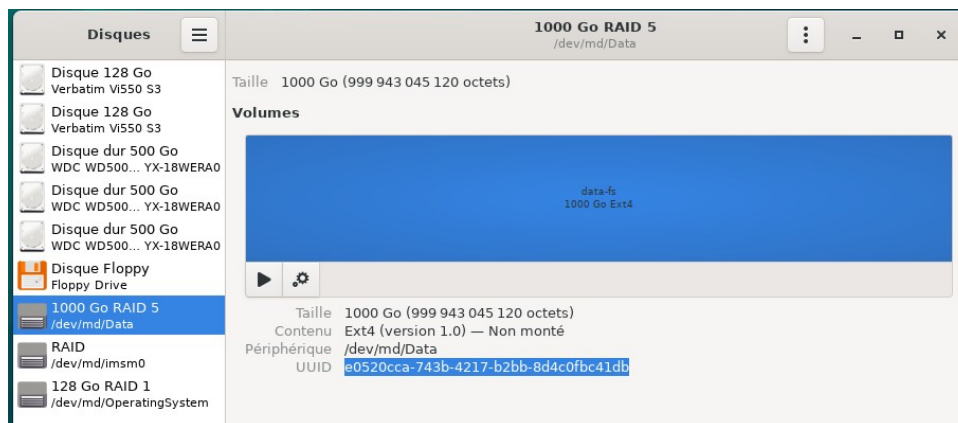
10.1 Formatage ext4 (création d'un « data-fs » vierge)

Le volume RAID, quand il vient d'être créé, n'a pas encore de système de fichiers. Il est, à ce stade, assimilable à une sorte de « gros disque » encore vierge. (**Attention en cas de récupération, le syst. de fichier ext4 doit apparaître, sinon les paramètres RAID sont erronés. Jamais formater s'il s'agit de récupérer un RAID.**)

Utiliser « gnome-disks » pour y créer un système de fichier ext4, qu'on pourra appeler « data-fs » (par analogie à « root-fs » pour le système de fichier ext4 du système d'exploitation, placé sur le RAID1 des SSD).

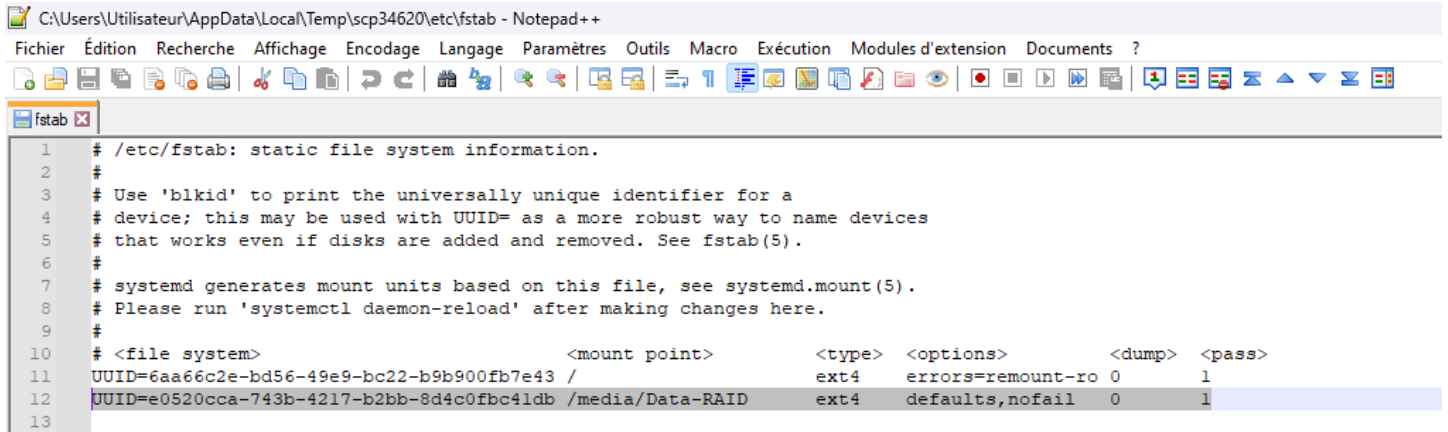


Le système de fichiers « ext4 » nouvellement créé porte un identifiant (UUID) :



Nous aurons besoin de cet identifiant pour ajouter un « point de montage » automatique dans `/etc/fstab`

10.2 Montage automatique du « data-fs » dans /etc/fstab :



```
1 # /etc/fstab: static file system information.
2 #
3 # Use 'blkid' to print the universally unique identifier for a
4 # device; this may be used with UUID= as a more robust way to name devices
5 # that works even if disks are added and removed. See fstab(5).
6 #
7 # systemd generates mount units based on this file, see systemd.mount(5).
8 # Please run 'systemctl daemon-reload' after making changes here.
9 #
10 #<file system>          <mount point>          <type> <options>          <dump> <pass>
11 UUID=6aa66c2e-bd56-49e9-bc22-b9b900fb7e43 /
12 UUID=e0520cca-743b-4217-b2bb-8d4c0fbc41db /media/Data-RAID ext4 defaults,nofail 0 1
13
```

Attention, ne pas redémarrer l'ordinateur tout de suite : après modification de /etc/fstab, aller dans « **gnome-disks** » et jouer le bouton « **play** » sur le système de fichier en question : s'il n'y a aucun problème alors le nouveau système de fichier sera rendu accessible à l'adresse **/media/Data-RAID**. Sinon, un message d'erreur s'affichera, et devra être corrigé (dans le cas contraire ça empêcherait le PC de démarrer).

Détails sur la ligne ajoutée dans /etc/fstab :

```
UUID=e0520cca-743b-4217-b2bb-8d4c0fbc41db /media/Data-RAID ext4 defaults,nofail 0 1
```

UUID=[...] correspond à l'identifiant du système de fichier ext4 « **data-fs** » créé avec « **gnome-disks** ». La commande root « **blkid** » permet également de lister les systèmes de fichiers et les identifiants de ces derniers, ainsi que identifiants et adresse **/dev/xxx** des partitions sur lesquelles ils se trouvent.

/media/Data-RAID correspond à l'adresse dans laquelle on voudrait rendre le système de fichier accessible : le parallèle sous Windows ce serait une lettre de lecteur (Lecteur **D:** par exemple).

« **ext4** » correspond au type de système de fichier : il serait sans doute capable de le trouver tout seul. Mais bon, puisqu'il le demande, on le lui donne.

« **defaults,nofail** » correspond au fonctionnement par défaut de ext4, nofail permet de laisser le système démarrer si jamais le volume RAID n'est pas accessible (indique à Linux qu'il réussirait à démarrer sans).

« **0** » sert à ne pas activer un mécanisme de sauvegarde appelé « **dump** » (que nous n'utilisons pas)

« **1** » sert à préférer vérifier le système de fichier « **ext4** » du volume **avant** de tout démarrer : ça évite généralement que les logiciels (dont Syncthing par exemple) ne démarrent avant le volume RAID.

10.3 Donner les droits d'écriture à « utilisateur »

Par défaut seul root peut créer des dossiers dans un nouveau système de fichier, et définir quels sont les utilisateurs et groupes ayant le droit d'y accéder, et de les modifier.

Jouer cette commande depuis un terminal root pour autoriser « utilisateur » (ou autre) à créer des dossiers avec ses propres règles/permissions :

chmod 777 /media/Data-RAID

De cette manière « root » est toujours propriétaire du système de fichiers, mais il est possible pour des utilisateurs autres que « root » de lire et écrire des fichiers et dossiers dans /media/Data-RAID.

Ces fichiers et dossiers pourront ensuite appartenir à un autre utilisateur que « root » et avoir leurs propres permissions (il ne s'agira pas forcément « 777 » partout heureusement).

11 Remplacement ou ajout de disques du RAID-5 (Data-RAID)

11.1 Retrait d'un disque présent, remplacement par un autre

Si on cherche à retirer du RAID un disque toujours branché, mais qui commence à devenir défaillant par exemple, on peut procéder comme suit :

Identifier la partition à retirer. Si c'est /dev/sdX1 :

```
mdadm --manage /dev/md/Data --fail /dev/sdX1
```

```
mdadm --manage /dev/md/Data --remove /dev/sdX1
```

Le RAID ne tourne alors plus qu'avec 2 disques sur 3.

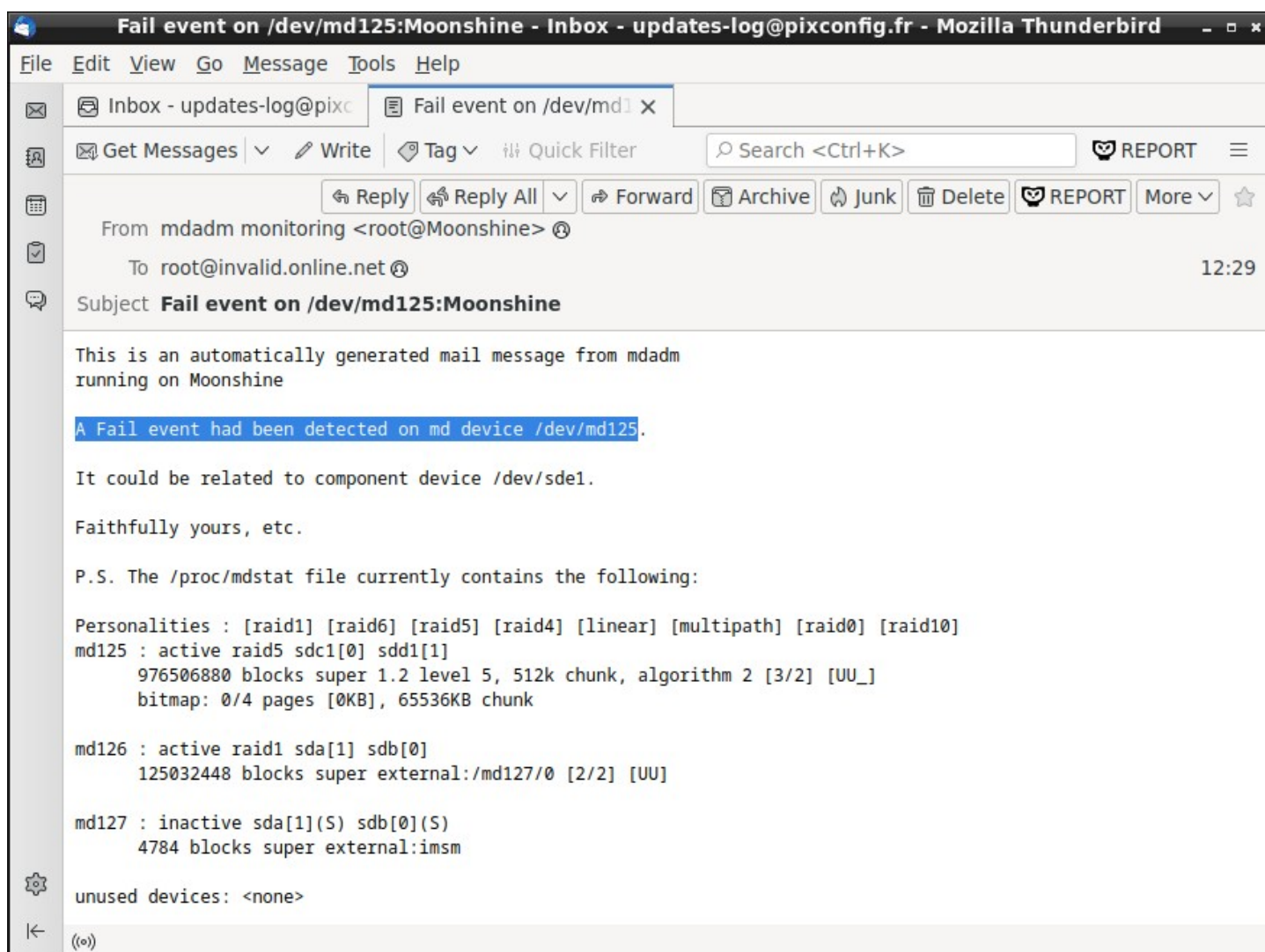
Après avoir préparé via GParted le nouveau disque (table de partition GPT, partition non formatée, nommée correctement pour s'y retrouver). Si le nouveau disque est /dev/sdZ1 :

```
mdadm --manage /dev/md/Data --add /dev/sdZ1
```

La commande « mdadm --detail /dev/md/Data » permettra de consulter l'état d'avancement de la reconstruction RAID.

11.2 Perte d'un disque pendant le fonctionnement – et remplacement

Lorsqu'un disque dur est perdu pendant le fonctionnement de l'ordinateur, après avoir configuré « msmtplib » (plus loin dans ce document), un email est envoyé automatiquement aux adresses destinataires définies :



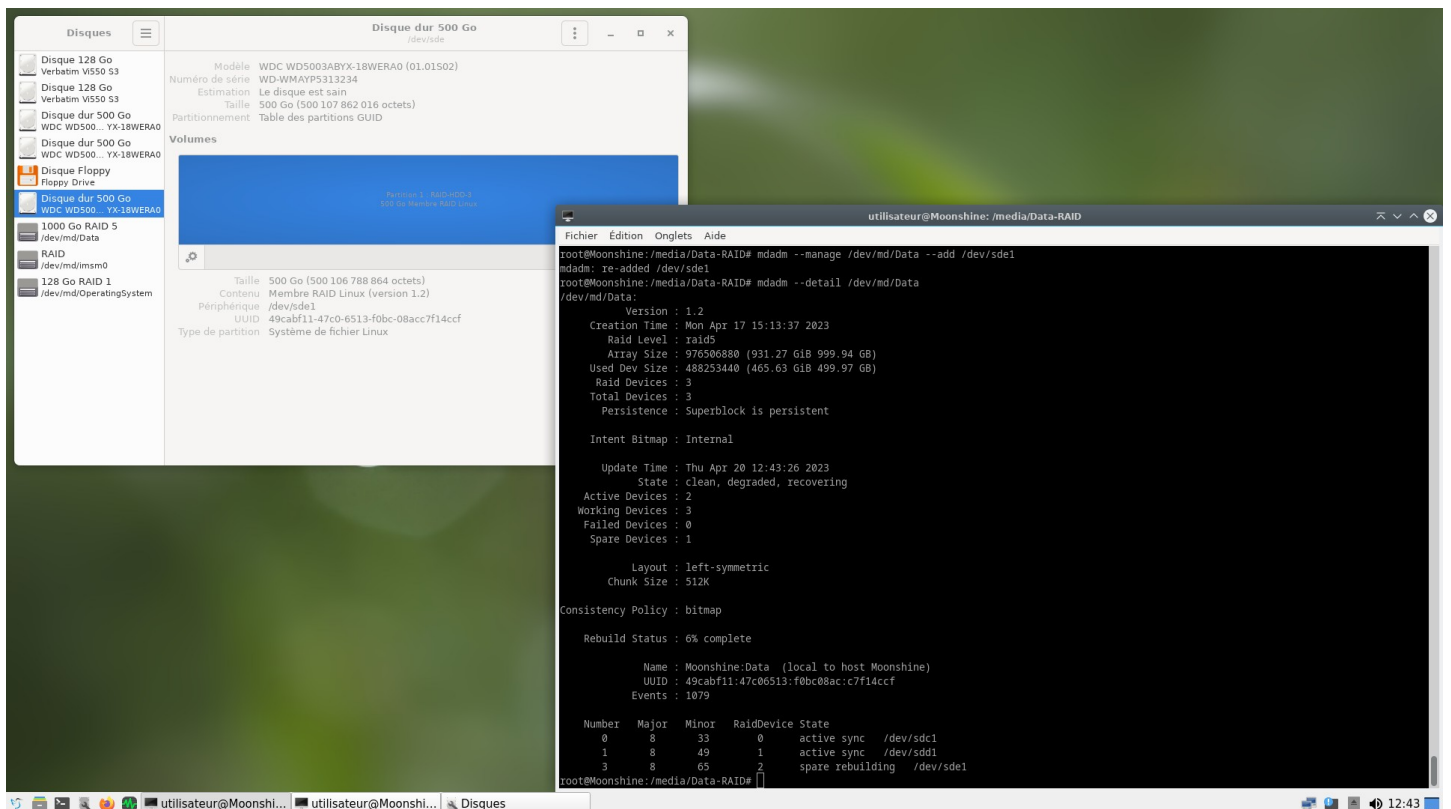
À savoir : dans ce cas, le volume RAID-5 continue de fonctionner sur les disques restants !

De même, la commande « **mdadm --examine /dev/md/Data** » (qu'on peut automatiser pour envoi par email à intervalle régulier) indiquera que l'un des disques est absent (*degraded* au milieu, *removed* en bas)

```
1 /dev/md/Data:
2   Version : 1.2
3   Creation Time : Mon Apr 17 15:13:37 2023
4   Raid Level : raid5
5   Array Size : 976506880 (931.27 GiB 999.94 GB)
6   Used Dev Size : 488253440 (465.63 GiB 499.97 GB)
7   Raid Devices : 3
8   Total Devices : 2
9   Persistence : Superblock is persistent
10
11  Intent Bitmap : Internal
12
13  Update Time : Thu Apr 20 12:41:41 2023
14  State : clean, degraded
15  Active Devices : 2
16  Working Devices : 2
17  Failed Devices : 0
18  Spare Devices : 0
19
20  Layout : left-symmetric
21  Chunk Size : 512K
22
23 Consistency Policy : bitmap
24
25      Name : Moonshine:Data (local to host Moonshine)
26      UUID : 49cabf11:47c06513:f0bc08ac:c7f14ccf
27      Events : 1072
28
29  Number  Major  Minor  RaidDevice State
30     0     8     33     0     active sync  /dev/sdc1
31     1     8     49     1     active sync  /dev/sdd1
32     -     0     0     2     removed
```

Aux dernières lignes on peut voir dans cet **exemple**, que le 3ième disque dans le RAID est absent. Vu qu'on a bien fait les choses, dans le boîtier, c'est le dernier disque en partant du haut (donc tout en bas). En cas de doute, consulter les numéros de série qu'on avait noté, et des HDD restants (sdc1 sdd1) via « *gnome-disks* ».

S'il ne s'agissait que d'un malentendu : (disque débranché en fonctionnement par exemple), après avoir rebranché le disque, il est possible de lui demander de ré-intégrer le RAID-5 :



Commande : **mdadm --manage /dev/md/Data --add /dev/sdZ1** (remplacer sdZ1 par le bon nom après avoir identifié l'adresse de la partition « RAID-HDD-X » à ré-intégrer dans le RAID).

Lorsque un disque est ré-intégré, **mdadm --detail /dev/md/Data** signale une reconstruction des données. De cette façon, tout les changements que le disque a loupé pendant sont absence, sont rattrapés.

Si en revanche, s'agit bien d'un disque dur HS :

Dans cet exemple c'est le disque RAID-HDD-3 qui a disparu, mais ce n'est qu'un exemple.

Première étape :

Après avoir identifié quels sont les disques durs encore fonctionnels, et après avoir identifié le disque HS, éteindre le serveur, retirer le disque dur HS, et en installer un nouveau (de taille identique OU supérieure).

Deuxième étape :

À l'aide de GParted, préparer le nouveau disque de la même façon qu'on avait initialement préparé les disques durs avant de créer le RAID-5 :

- re-crée une table de partition GPT sur le nouveau disque vierge (ne pas se tromper de disque !)
- puis créer une partition non formatée, de taille au moins identique aux autres, nommée correctement
- jouer la commande **mdadm --detail /dev/md*** pour retrouver le RAID-5 s'il n'est plus joignable à l'adresse /dev/md/Data (ça arrive). Dans l'exemple ci-dessous on le retrouve à **/dev/md125** :

```
root@Moonshine:~# mdadm --detail /dev/md*
mdadm: /dev/md does not appear to be an md device
/dev/md125:
  Version : 1.2
  Raid Level : raid5
  Total Devices : 2
  Persistence : Superblock is persistent

  State : inactive
  Working Devices : 2

  Name : Moonshine:Data (local to host Moonshine)
  UUID : 49cabf11:47c06513:f0bc08ac:c7f14ccf
  Events : 1085

  Number Major Minor RaidDevice
  -      8     49      -      /dev/sdd1
  -      8     33      -      /dev/sdc1

/dev/md126:
  Container : /dev/md/ims0, member 0
  Raid Level : raid1
  Array Size : 125032448 (119.24 GiB 128.03 GB)
  Used Dev Size : 125032448 (119.24 GiB 128.03 GB)
```

Troisième étape : récapituler

Dans cet **exemple** : notre RAID-5 est étiqueté **/dev/md125**, toujours composé de **/dev/sdc1** et **/dev/sdd1** (vérifier via gnome-disks leurs numéros de série et noms de partition : tout doit être cohérent, pour vérifier qu'on n'a pas enlevé le mauvais disque !). Dans cet exemple il s'agit des **RAID-HDD-1** et **2**.

On va ajouter à ce RAID-5 un 3ème disque vierge qu'on vient de préparer en remplacement de celui qui était HS. Via gnome-disks vérifier l'adresse et le nom de la partition qu'on vient de préparer. Dans mon cas, l'adresse de la nouvelle partition est **/dev/sde1**, et son nom est **RAID-HDD-3** : récapitulation OK.

Quatrième étape : jouer la commande

Maintenant qu'on est sûrs d'avoir tout récapitulé et que tout est cohérent, voici la commande qu'on entre dans cet exemple :

```
mdadm --manage /dev/md125 --add /dev/sde1
```

Si la commande répond « mdadm: Cannot get array info for /dev/md125 », il faudra **rejouer la commande**, mais après demandé à démarrer le RAID malgré le disque manquant. Dans cet exemple : **mdadm --stop /dev/md125 && mdadm --assemble /dev/md125 /dev/sdc1 /dev/sdd1 --run**

Dans cet exemple, ça répond **/dev/md125 has been started with 2 drives (out of 3)**. Prêt pour l'ajout !

11.3 Perte d'un disque à la mise sous tension

Bien que le remplacement d'un disque se fera finalement de la même façon, initialement, le système se comportera différemment, par rapport à une perte en cours de fonctionnement.

Voici une liste qui récapitule ce qui se passera, dans ces 2 cas de figure distinct.

Cas N°1 : Lorsque le RAID-5 est en cours de fonctionnement pendant la perte d'un disque :

- Linux considère que c'est une panne qui vient de survenir, et marque le RAID comme dégradé.
- Il part du principe qu'il est préférable d'assurer une continuité de service : le RAID-5 reste en cours de fonctionnement, est marqué « degraded » : il se débrouille avec les disques qui lui restent.
- Un mail est envoyé pour prévenir du problème (à condition que « msmtpt » ou autre soit configuré pour pouvoir envoyer des mails et définir des destinataires – voir plus loin dans le document).
- Le RAID ayant pris acte de son nouvel état, il continuera de fonctionner ainsi après redémarrage.

Si le mail n'est pas envoyé, ou pas reçu, la perte d'un disque peut passer inaperçue !

Il est donc utile de créer un système de rapports hebdomadaires par email par exemple. Si les mails cessent de fonctionner pour X raison, on devrait finir par s'en rendre compte avant que des problèmes n'apparaissent (ou avant qu'il y en ait trop).

Cas N° 2 : Lorsqu'un disque n'apparaît pas au redémarrage

- Linux ne peut pas savoir si le disque va arriver ni sous combien de temps (le temps qu'il soit détecté). En effet on peut insérer les disques « RAID » à chaud sur certains serveurs. Donc s'il en manque un, il va continuer de l'attendre, pour éviter de « dégrader » inutilement le RAID.
- Le volume RAID n'est pas mis en fonctionnement, tant que tous les disques ne sont pas présents.
- Le volume RAID n'est pas marqué « dégradé ». Aucune alerte de « RAID dégradé » n'est envoyée !

Dans les faits, ce cas de figure a moins de chances de passer inaperçu.

En effet, le point de montage associé, par exemple « /media/Data-RAID » est alors absent, et tous les logiciels qui l'utilisent habituellement, mettront des erreurs. Dès qu'il y aura des fichiers à envoyer, Syncthing par exemple, sur les autres postes, indiquera rapidement que Moonshine n'est pas à jour.

Dans les 2 cas : Il reste de toute façon toujours utile de créer un système de rapports hebdomadaires par email par exemple. Même si on ne s'aperçoit pas d'une perte de disque, l'un des mails ressemblera à ça :

```
From root@pix-server-boutigny.lan @
To Me <updates-log@pixconfig.fr> @
Subject Pix-Server-Boutigny SDH SMART Status

smartctl 7.2 2020-12-30 r5155 [x86_64-linux-5.10.0-21-amd64] (local build)
Copyright (C) 2002-20, Bruce Allen, Christian Franke, www.smartmontools.org

Smartctl open device: /dev/sdh failed: No such device
```

Même quand les disques fonctionnent encore : Dans les mails « SMART Status », le champs « Reallocated_Sector_Ct » entre autre permettra de suivre l'état de santé des disques, de regarder l'évolution de l'état des disques au fil des semaines par exemple, en cas de doute. Si par exemple, Reallocated Sector Count (nombre de secteurs défectueux déplacés) augmente voire passe la barre de « 100 », remplacer.

11.4 Passage à 4 disques au lieu de 3

Après avoir préparé le nouveau disque via GParted (table de partition GPT, partition non formatée, nommée correctement pour s'y retrouver). Si le nouveau disque est /dev/sdZ1 :

```
mdadm --add /dev/md/Data /dev/sdZ1
mdadm --grow /dev/md/Data --raid-devices=4
```

La première commande place le disque en « spare » (disque de rechange, non utilisé sauf s'il en manquait justement un), tandis que la seconde lui demande de commencer à s'en servir pour agrandir le RAID.

Cela doit démarrer une phase de déplacement des données (elles ne seront plus agencées pareil) au terme de laquelle la capacité du volume RAID sera incrémentée.

Pour agrandir le système de fichier ext4 « data-fs » :

Une fois que le volume RAID a fini sa reconstruction (consulter mdadm --detail /dev/md/Data pour connaître son état d'avancement), il sera présenté avec une nouvelle taille (1500 Go au lieu de 1000 Go par exemple).

Or, dans l'explorateur de fichier, l'ancienne taille (1000 Go par exemple) apparaîtra toujours à l'écran.

Ceci indiquera que le volume RAID sur lequel est placé le système de fichier « data-fs » a bien augmenté, mais que la taille du système de fichier « data-fs » qu'on a mis dessus, n'a pas augmenté pour autant !

Solution : A l'aide de gnome-disks il faudra donc stopper /media/Data-RAID, puis utiliser la fonction « resize » de GParted, pour redimensionner le système de fichier qui se trouve sur le volume RAID.

Si jamais on n'arrive pas à mettre en « Stop » /media/Data-RAID :

Cela indique probablement que des logiciels travaillent dessus. Notamment Syncthing (s'il est installé), qu'on peut stopper en jouant la commande suivante :

```
systemctl stop syncthing@utilisateur
```

Un autre format de commande existe pour obtenir le même effet :

```
service syncthing@utilisateur stop
```

Si jamais d'autres services ont été ajoutés et ont été réglés pour travailler dans le volume RAID, les fermer également. Par exemple, pour Motion qu'on va voir plus loin dans ce document :

```
service motion stop
```

Si ça ne marche toujours pas, et que cette chasse à (on ne sait même pas ce qui bloque) devient gonflante :

Une autre approche consiste à modifier temporairement /etc/fstab (mettre un # au tout début la ligne qui définit le montage automatique de /media/Data-RAID) puis de redémarrer le PC.

De cette manière, on n'aura plus à galérer à le mettre sur « Stop » puisqu'il y sera déjà après le redémarrage.

12 Remplacement d'un SSD du RAID-1 (OperatingSystem, BIOS)

12.1 Symptômes en cas de perte d'un SSD

Lorsqu'un SSD du RAID-1 est perdu, l'ordinateur continue de fonctionner de façon transparente.

Si Linux est en cours de fonctionnement lorsque de la disparition d'un SSD sur les deux, un mail est envoyé.

```
Inbox - updates-log@pixc | Fail event on /dev/md: X
Get Messages | Write | Tag | Quick Filter
From mdadm monitoring <root@Moonshine>
To root@invalid.online.net
Subject Fail event on /dev/md126: Moonshine

This is an automatically generated mail message from mdadm
running on Moonshine

A Fail event had been detected on md device /dev/md126.
It could be related to component device /dev/sdb.

Faithfully yours, etc.

P.S. The /proc/mdstat file currently contains the following:

Personalities : [raid1] [linear] [multipath] [raid0] [raid6] [raid5] [raid4] [raid10]
md125 : active raid5 sda1[3] sdd1[0] sde1[1]
          976506880 blocks super 1.2 level 5, 512k chunk, algorithm 2 [3/3] [UUU]
          bitmap: 0/4 pages [0KB], 65536KB chunk

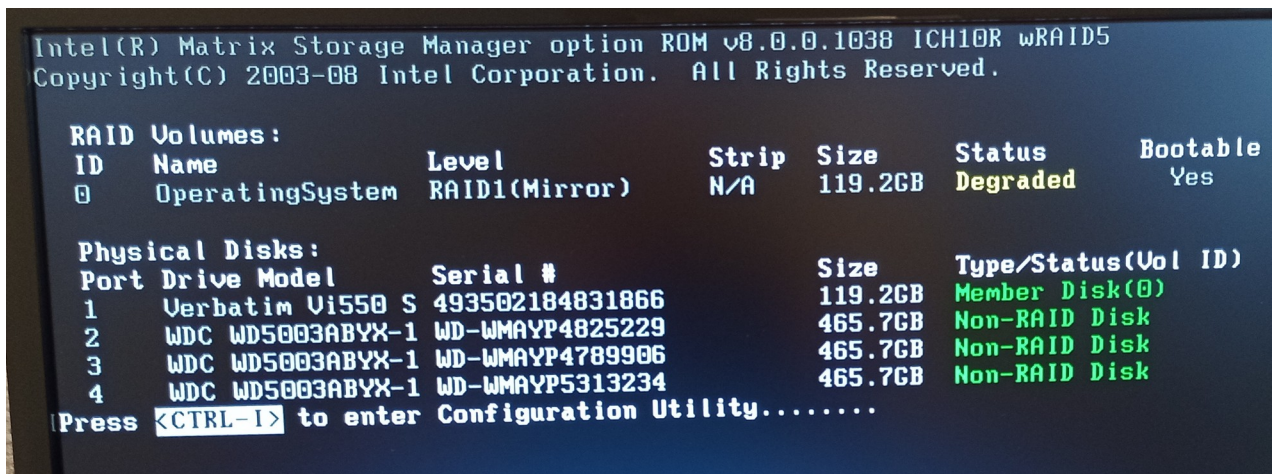
md126 : active raid1 sdc[0]
          125032448 blocks super external:/md127/0 [2/1] [_U]

md127 : inactive sdc[1](5)
          2392 blocks super external:inms

unused devices: <none>
```

Si en revanche c'est au redémarrage que l'un des SSD n'apparaît plus, aucun mail n'est envoyé sur le coup : il faudra compter sur le système de rapport hebdomadaire qu'on a mis en place pour s'en rendre compte.

Au démarrage ça affiche ça :



A part concernant la mention « Degraded » en jaune, et qu'un seul SSD « Verbatim Vi550 » apparaisse dans la liste, là aussi ça peut passer inaperçu (surtout que le serveur redémarre généralement tout seul après ses mises à jour, et que son écran pourrait bien rester éteint quasiment tout le temps).

12.2 En cas de retour du SSD

S'il s'agissait d'une fausse alerte (SSD débranché accidentellement par ex.), dès qu'il sera rebranché (à chaud PC allumé, ou bien au redémarrage), il sera dans les 2 cas automatiquement reconnu, automatiquement ré-intégré, et re-synchronisé avec l'autre, pour recevoir tout ce qu'il a loupé pendant son absence.

Mais si le SSD qui a disparu de la liste est bien HS, il faudra en mettre un neuf.

Auquel cas, le nouveau SSD (vierge) ne sera pas ré-intégré automatiquement : il faudra le faire manuellement en suivant les instructions suivantes.

12.3 Intégration d'un nouveau SSD en remplacement

Après avoir installé un SSD de capacité identique ou supérieure, il faudra presser « Ctrl » et « i » lorsque l'écran ci-dessous s'affichera :

```
Intel(R) Matrix Storage Manager option ROM v8.0.0.1038 ICH10R wRAID5
Copyright(C) 2003-08 Intel Corporation. All Rights Reserved.

RAID Volumes :
ID   Name                Level           Strip   Size   Status   Bootable
0   OperatingSystem    RAID1(Mirror)  N/A    119.2GB Degraded Yes

Physical Disks :
Port Drive Model      Serial #        Size   Type/Status(Vol ID)
0   Verbatim Vi550 S   493502184831865 119.2GB Non-RAID Disk
1   Verbatim Vi550 S   493502184831866 119.2GB Member Disk(0)
2   WDC WD5003ABYX-1  WD-WMAYP4825229 465.7GB Non-RAID Disk
3   WDC WD5003ABYX-1  WD-WMAYP4789906 465.7GB Non-RAID Disk
4   WDC WD5003ABYX-1  WD-WMAYP5313234 465.7GB Non-RAID Disk

Press <CTRL-I> to enter Configuration Utility....
```

On peut y apercevoir ici que sur le port « 0 », un nouveau SSD vierge, qualifié de « Non-RAID Disk » est disponible (en réalité c'est le même qu'au début de ce document, je l'ai juste effacé depuis un autre ordi).

Après avoir pressé Ctrl et i, l'écran suivant apparaît :

```
Intel(R) Matrix Storage Manager option ROM v8.0.0.1038 ICH10R wRAID5
Copyright(C) 2003-08 Intel Corporation. All Rights Reserved.

[ MAIN MENU ]
[ DEGRADED VOLUME DETECTED ]
"Degraded" volume and disk available for rebuilding detected. Selecting
a disk initiates a rebuild. Rebuild completes in the operating system.

Select the port of the destination disk for rebuilding (ESC to exit):
Port Drive Model      Serial #        Size
0   Verbatim Vi550 S3   493502184831865 119.2GB
2   WDC WD5003ABYX-18WER WD-WMAYP4825229 465.7GB
3   WDC WD5003ABYX-18WER WD-WMAYP4789906 465.7GB
4   WDC WD5003ABYX-18WER WD-WMAYP5313234 465.7GB

[↑↓]-Previous/Next [ENTER]-Select [ESC]-Exit

RAID ID 0
Ph Po 0
0   Verbatim Vi550 S   493502184831865 119.2GB Non-RAID Disk
1   Verbatim Vi550 S   493502184831866 119.2GB Member Disk(0)
2   WDC WD5003ABYX-1  WD-WMAYP4825229 465.7GB Non-RAID Disk
3   WDC WD5003ABYX-1  WD-WMAYP4789906 465.7GB Non-RAID Disk
4   WDC WD5003ABYX-1  WD-WMAYP5313234 465.7GB Non-RAID Disk

[↑↓]-Select [ESC]-Exit [ENTER]-Select Menu
```

Il nous propose de remplacer le disque/SSD qu'il a perdu avec l'un de ceux de la liste qu'il nous présente.

Attention à bien sélectionner le bon (ici, le Port 0 Verbatim Vi550 S3 au N° série finissant par 65 est le bon).

Une fois que c'est fait, le « Status » passe à « Rebuild ». On peut alors aller sur « 4. Exit » et redémarrer.

Remarque : Voici pourquoi il a été judicieux de demander au BIOS de gérer ce RAID-1 contenant le système d'exploitation. En effet, dans le cas contraire (RAID géré par Linux) en cas de perte d'un SSD survenant à l'allumage ou au redémarrage, Linux aurait attendu indéfiniment l'arrivée de son SSD et n'aurait jamais pu démarrer, et il aurait fallu apporter un moyen de démarrer Linux par clé USB pour gérer/réparer le RAID.

13 Mises à jour automatiques + système d'envoi mail

13.1 Installation des logiciels requis

La première chose à faire est d'avoir installé les applications suivantes, via « apt install », si ça n'a pas déjà été fait (sinon pas de souci, il se contentera de dire que c'est déjà installé) :

```
apt install msmtplib s-nail mailutils unattended-upgrades
```

13.2 Création des fichiers de configuration

Le fichier de configuration de unattended-upgrades doit être grandement simplifié, en le remplaçant par ce qui suit, afin d'avoir la même portée que « apt update && apt upgrade -y »

/etc/apt/apt.conf.d/50unattended-upgrades :

```
Unattended-Upgrade::Origins-Pattern {
    "o=*";
};
Unattended-Upgrade::Package-Blacklist {
};
Unattended-Upgrade::Mail "updates-log@pixconfig.fr";
Unattended-Upgrade::Remove-Unused-Dependencies "true";
Unattended-Upgrade::Automatic-Reboot "true";
```

Y définir la (ou les) adresse(s) email destination des rapports de mise à jour.

Pour définir plusieurs adresses mail il est possible d'écrire :

```
Unattended-Upgrade::Mail "exemple1@mail.fr,exemple2@mail.fr";
```

Pour l'envoi des emails, il faut créer le fichier **/etc/msmtplib** :

```
# Initially based on https://wiki.archlinux.org/index.php/msmtplib
# See https://marlam.de/msmtplib/msmtplib.html for all options and changes since then

# Set default values for all accounts
defaults
auth                on
tls                 on
tls_starttls       on
tls_trust_file      /etc/ssl/certs/ca-certificates.crt
logfile             ~/.msmtplib.log
from                updates-log@pixconfig.fr
allow_from_override off
domain              %H
# Starting from Debian 12 msmtplib version, %H is replaced by computer hostname for
# the ELHO/HELO smtp command (default "localhost" causes troubles)

# Pixconfig
account             pixconfig
host                smtp.online.net
port                587
user                updates-log@pixconfig.fr
password            MotDePasse

# Set a default account
account default : pixconfig

aliases             /etc/msmtplib-aliases # Only starting from Debian 12
```

Attention, dans cet exemple il faut remplacer MotDePasse par quelque chose de valable, ou configurer son propre compte SMTP à l'aide d'un fournisseur et d'une adresse mail, comme dans Outlook ou Thunderbird.

Ensuite (ne marche qu'à partir de Debian 12), il faut créer le fichier `/etc/msmtpc-aliases` :

```
# Send any local name ("root" or anything else) to
default: updates-log@pixconfig.fr
```

Ce fichier a pour but de transmettre les messages systèmes vers la ou les adresses qui y figurent. Certaines erreurs systèmes, y compris les pertes de disque RAID par exemple, sont envoyées automatiquement à « root ». Le but c'est que « root » soit alors remplacé par des adresses email qui existent.

Pour faire en sorte qu'il y en ait plusieurs :

```
# Send any local name ("root" or anything else) to
default: exemple1@mail.fr, exemple2@mail.fr
```

Pour tester l'envoi d'un message par email :

```
echo "Contenu de test mail" | mail -s "Sujet de test mail" "exemple@adresse.fr"
```

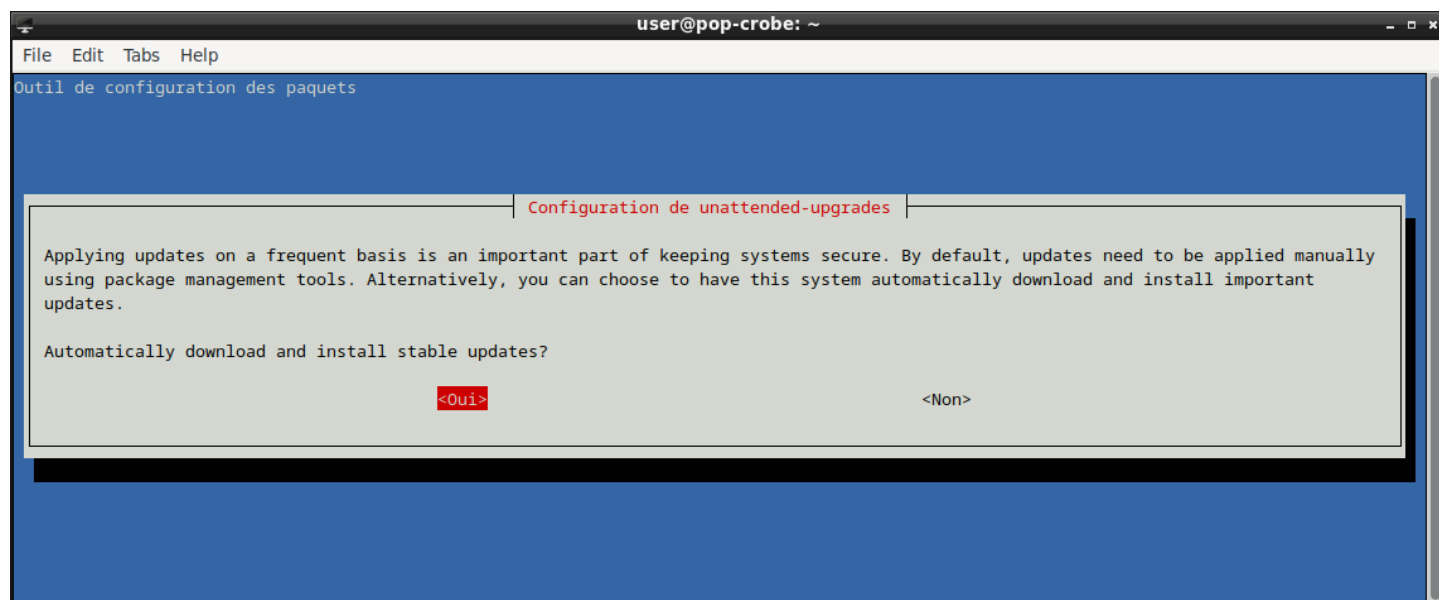
```
echo "Contenu de test mail" | mail -s "Sujet de test mail" "root"
```

Là aussi il est possible d'écrire deux adresses : "exemple1@mail.fr, exemple2@mail.fr"

Activation des mises à jour automatiques :

Jouer la commande suivante (en terminal root) pour activer les mises à jour automatiques :

`dpkg-reconfigure -plow unattended-upgrades`



Répondre « **Oui** ».

Pour tester sans attendre : Si des mises à jour sont disponibles, il est possible de tester tout de suite en jouant la commande « unattended-upgrade » depuis un terminal root.

Sinon, c'est généralement vers ~6h30 tous les jours (\pm 30 minutes) que les mises à jour se font.

14 Rapport hebdomadaire mail - état des disques durs

Après avoir configuré le système d'envoi de messages, il est possible de créer un script qui sera exécuté à intervalle régulier, qui nous enverra un rapport détaillé par email sur l'état de chaque disque.

14.1 Création et test du script

Placer le fichier suivant à l'adresse `/usr/local/sbin/smart-report-mail.sh` :

```
#!/bin/sh
smartctl -a /dev/sda | mail -s "_SERVER_NAME_SDA SMART Status" "updates-log@pixconfig.fr"
smartctl -a /dev/sdb | mail -s "_SERVER_NAME_SDB SMART Status" "updates-log@pixconfig.fr"
smartctl -a /dev/sdc | mail -s "_SERVER_NAME_SDC SMART Status" "updates-log@pixconfig.fr"
smartctl -a /dev/sdd | mail -s "_SERVER_NAME_SDD SMART Status" "updates-log@pixconfig.fr"
smartctl -a /dev/sde | mail -s "_SERVER_NAME_SDE SMART Status" "updates-log@pixconfig.fr"
mdadm --detail /dev/md* | mail -s "_SERVER_NAME_ MDADM Status" "updates-log@pixconfig.fr"
```

Remarque 1 : Remplacer « `_SERVER_NAME_` » par le nom de la machine, ici « Moonshine ».

Remarque 2 : Remplacer par les adresses email qu'on souhaite, "exemple1@mail.fr, exemple2@mail.fr"

Rendre ce fichier exécutable en jouant la commande suivante :

```
chmod 755 /usr/local/sbin/smart-report-mail.sh
```

Pour info : 755 correspond à « `rwX r-X r-X` » ce qui veut dire que tout le monde peut exécuter ce fichier, mais que seul « root » peut le modifier. Sécurité importante car root va exécuter tout ce qui se trouve dedans.

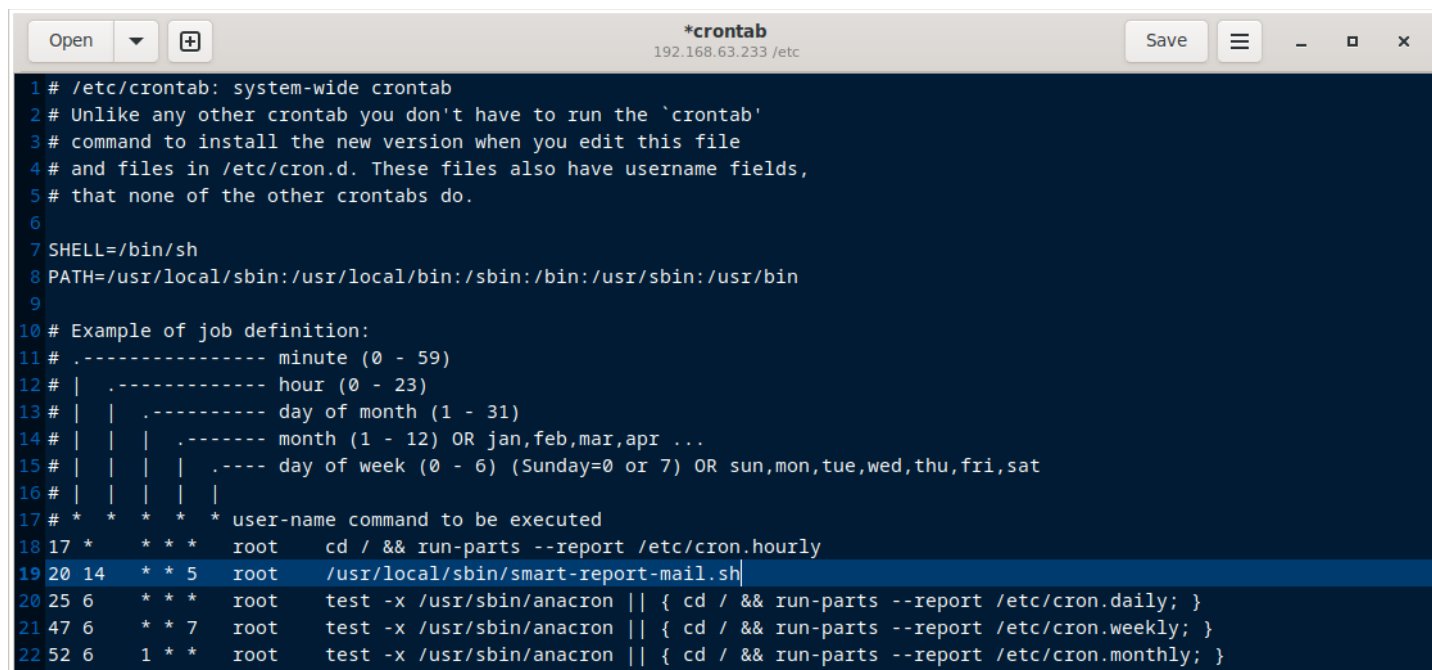
Puis tenter de l'exécuter en tapant son adresse complète depuis un terminal. Vérifier les emails arrivent bien à destination.

14.2 Exécution automatique

Sous Linux, un mécanisme appelé « cron » est chargé de faire les exécutions automatiques à intervalle fixe.

Pour lui confier la mission d'exécuter chaque semaine notre script défini ci-dessus, on peut procéder ainsi :

Éditer le fichier « `/etc/crontab` » afin d'ajouter la ligne suivante :



```
Open 192.168.63.233 /etc Save [Menu] - [Close] X
1 # /etc/crontab: system-wide crontab
2 # Unlike any other crontab you don't have to run the `crontab'
3 # command to install the new version when you edit this file
4 # and files in /etc/cron.d. These files also have username fields,
5 # that none of the other crontabs do.
6
7 SHELL=/bin/sh
8 PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
9
10 # Example of job definition:
11 # .----- minute (0 - 59)
12 # | .----- hour (0 - 23)
13 # | | .----- day of month (1 - 31)
14 # | | | .----- month (1 - 12) OR jan,feb,mar,apr ...
15 # | | | | .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
16 # | | | | |
17 # * * * * * user-name command to be executed
18 17 * * * * root cd / && run-parts --report /etc/cron.hourly
19 20 14 * * 5 root /usr/local/sbin/smart-report-mail.sh
20 25 6 * * * root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.daily; }
21 47 6 * * 7 root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.weekly; }
22 52 6 1 * * root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.monthly; }
```

Désormais tous les 5ème jours de la semaine, à 14h20, le script sera lancé par l'utilisateur « root ».

15 Syncthing

15.1 Installation

Bien qu'une version de Syncthing soit disponible dans les commandes « apt » de Debian, ce sera généralement un version ancienne et rapidement obsolète qui ne sera qu'excessivement rarement maintenue à jour (seulement en cas de faille de sécurité ou de perte totale de compatibilité, et encore... !)

Il est donc préférable d'utiliser une version de Syncthing qui se maintiendra correctement à jour, comme c'est le cas sous Windows.

Le site officiel de Syncthing propose un moyen d'autoriser « apt » à se fournir directement chez Syncthing.

Commencer par jouer la commande suivante, à l'aide de putty par exemple :

```
apt install curl && curl -s -o /usr/share/keyrings/syncthing-archive-keyring.gpg https://syncthing.net/release-key.gpg
```

Ensuite, à l'aide de WinSCP par exemple, éditer **/etc/apt/sources.list**, pour y ajouter :

```
deb [signed-by=/usr/share/keyrings/syncthing-archive-keyring.gpg] https://apt.syncthing.net/ syncthing stable
```

Ensuite, après avoir joué « apt update », la version qu'on installera via « apt install » sera la bonne.

```
apt update && apt install syncthing
```

15.2 Démarrage automatique

Une fois syncthing installé, qu'il s'agisse de Windows comme de Linux, il n'y a pas de démarrage automatique tant qu'on ne s'en charge pas soi même (ou qu'on n'installe pas quelque chose d'autre pour s'en charger, comme Synctrayzor sous Windows).

Commencer par créer le fichier **/etc/systemd/system/syncthing@.service** :

```
[Unit]
Description=Syncthing - Open Source Continuous File Synchronization for %I
Documentation=man:syncthing(1)
After=network.target
Wants=syncthing-inotify@.service

[Service]
User=%i
ExecStart=/usr/bin/syncthing -no-browser -no-restart -logflags=0
Restart=on-failure
SuccessExitStatus=3 4
RestartForceExitStatus=3 4
UMask=0002

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

Ensuite, jouer les deux commandes suivantes :

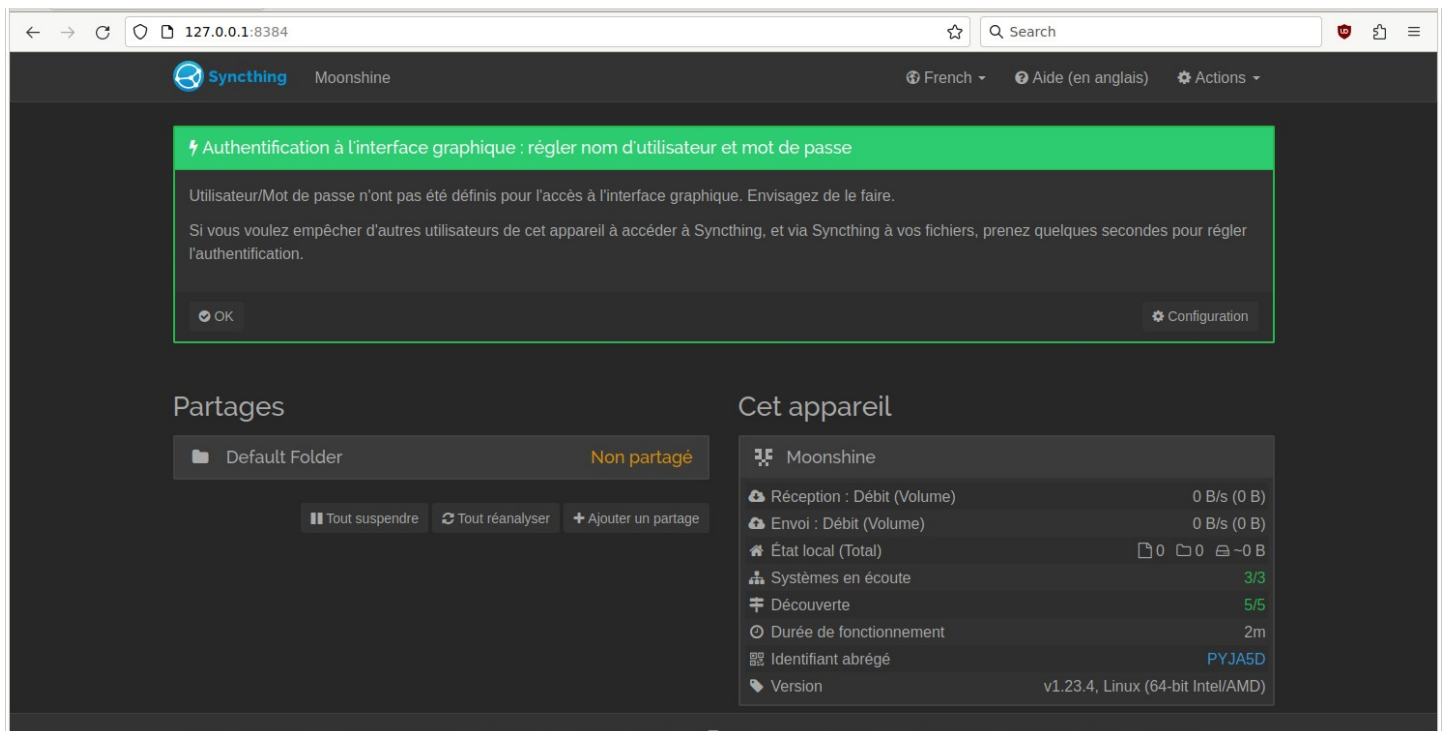
```
systemctl enable syncthing@utilisateur
systemctl start syncthing@utilisateur
```

Désormais, Syncthing devrait être en marche, en tant que « utilisateur ». Ses fichiers de configuration seront alors dans « /home/utilisateur/.config/syncthing/ », et depuis le serveur, via un navigateur, on peut entrer l'adresse <http://127.0.0.1:8384> pour accéder à son interface (ajouter des dossiers, d'autres ordinateurs...)

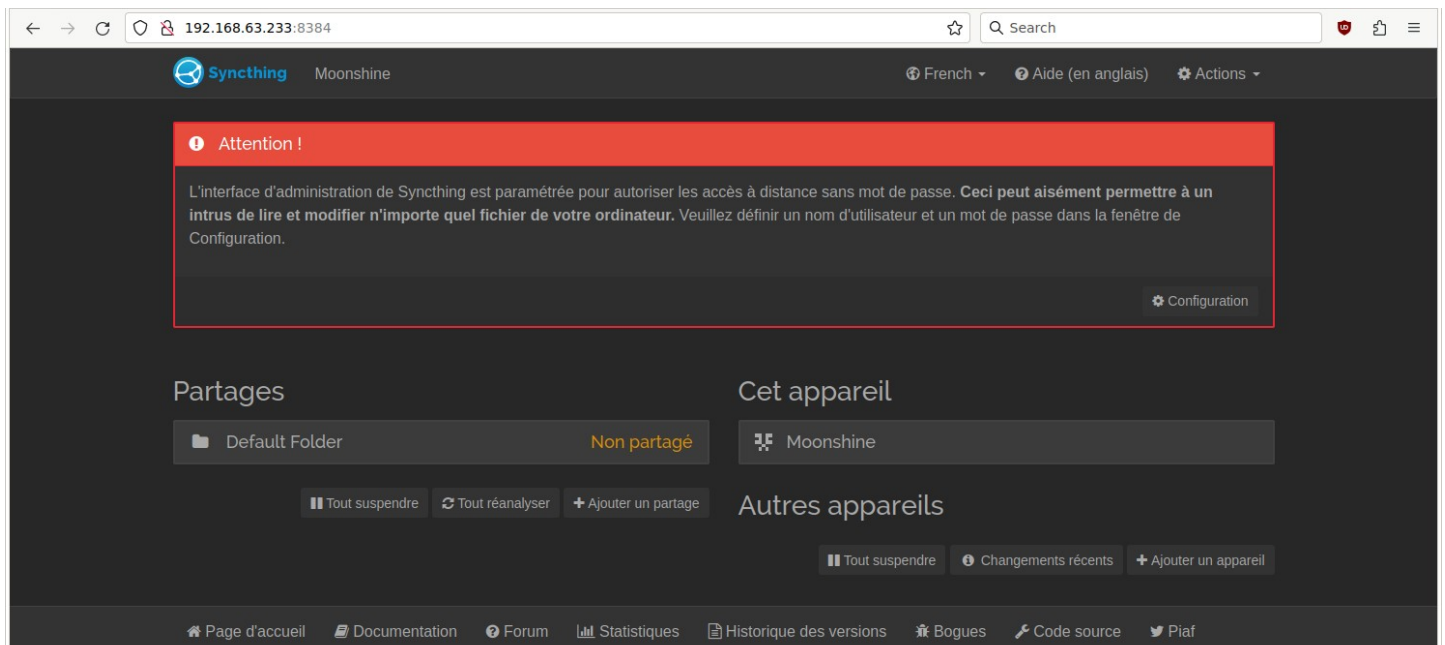
15.3 Configuration de Syncthing : accès à l'interface

Une fois Syncthing installé et lancé, voici ce qu'on obtient en entrant <http://127.0.0.1:8384> dans le navigateur depuis le serveur. Il est possible ensuite, d'ouvrir l'accès à cette interface depuis d'autres PC du réseau.

L'avertissement concernant l'absence de nom d'utilisateur et mot de passe, n'est justifié qu'en cas d'ouverture de l'accès à cette page depuis d'autres PC du réseau, ce qui n'est pas le cas par défaut.



En revanche, il est possible d'ouvrir l'accès à cette interface depuis les autres PC du réseau (voire + en fonction du réglage de box Internet). Auquel cas, fixer un nom d'utilisateur + mot de passe devient essentiel !



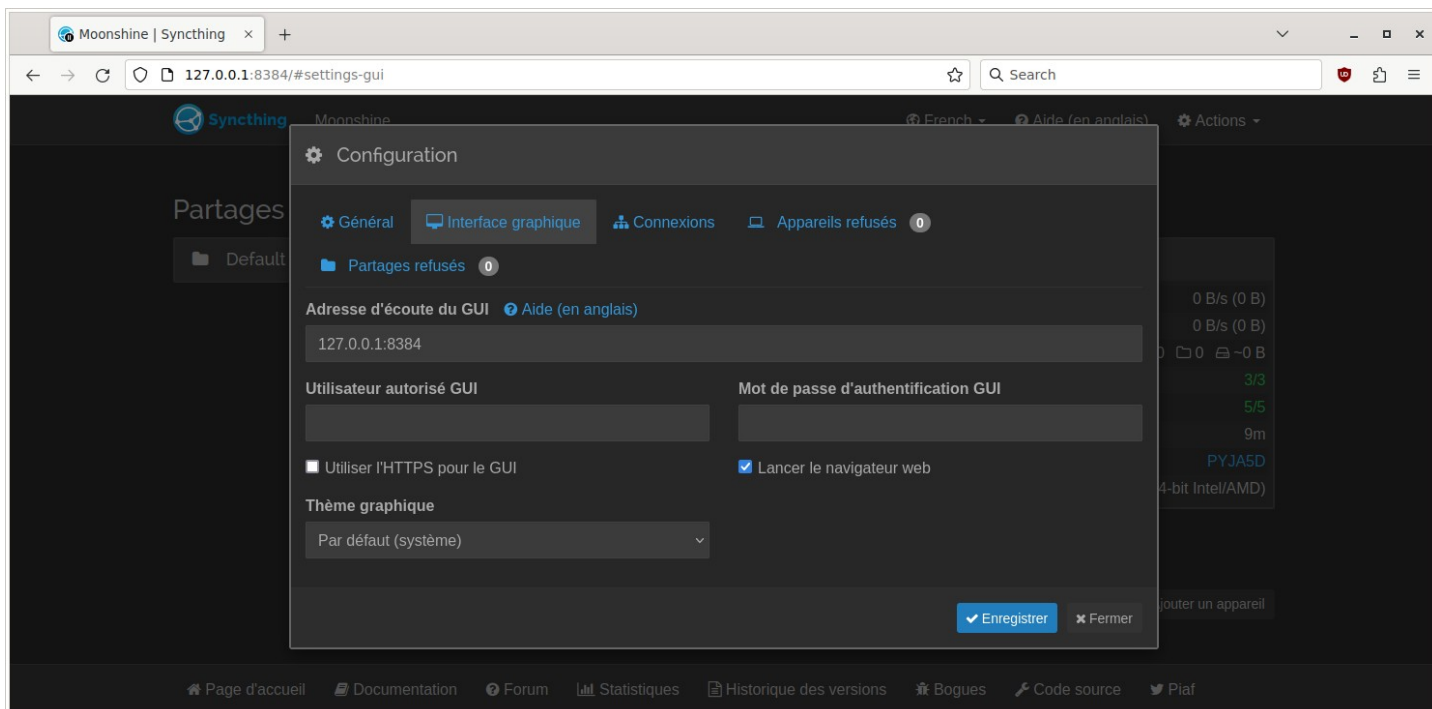
Même sur un réseau domestique, du fait de tous les smartphones, et autres (nombreux) objets connectés criblés de failles et de logiciels obscurs en provenance de partout sur terre, laisser un serveur en accès libre sans authentification est dangereux. Quiconque se connecterait au WiFi aurait également accès à tout.

Pire, en cas de mauvaise configuration box (genre configuration par défaut d'une Freebox V6), le serveur est déjà joignable à distance sur Internet sans même qu'on ne soit mis au courant !

Bref, si on rend l'interface joignable depuis le réseau : authentification **OBLIGATOIRE**. Voyons donc comment **fixer un identifiant + mot de passe**.

Aller dans Actions (en haut à droite, la roue dentée) puis Configuration :

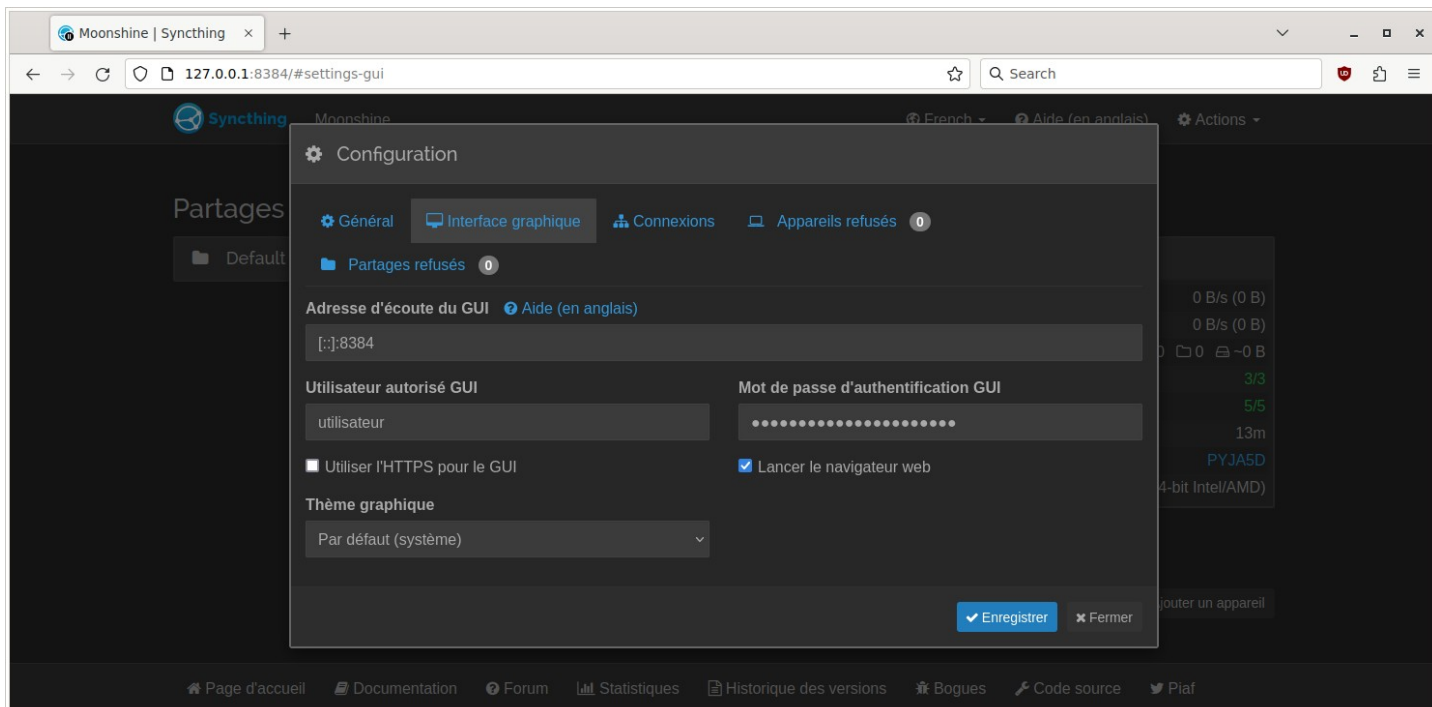
Dans l'onglet « Interface graphique » on trouve ceci :



L'adresse d'écoute « 127.0.0.1:8384 » correspond à un accès depuis le serveur uniquement. S'utilise en étant physiquement devant le PC, ou via VNC, en utilisant son navigateur, voire en « tunnel SSH » avec Putty une fois qu'on est déjà connectés et authentifiés via SSH. Ça ne crée donc aucune porte supplémentaire.

Pour étendre cet accès : remplacer **127.0.0.1:8384** par **[::]:8384**

Fixer également « **Utilisateur autorisé GUI** » et « **Mot de passe d'authentification GUI** »

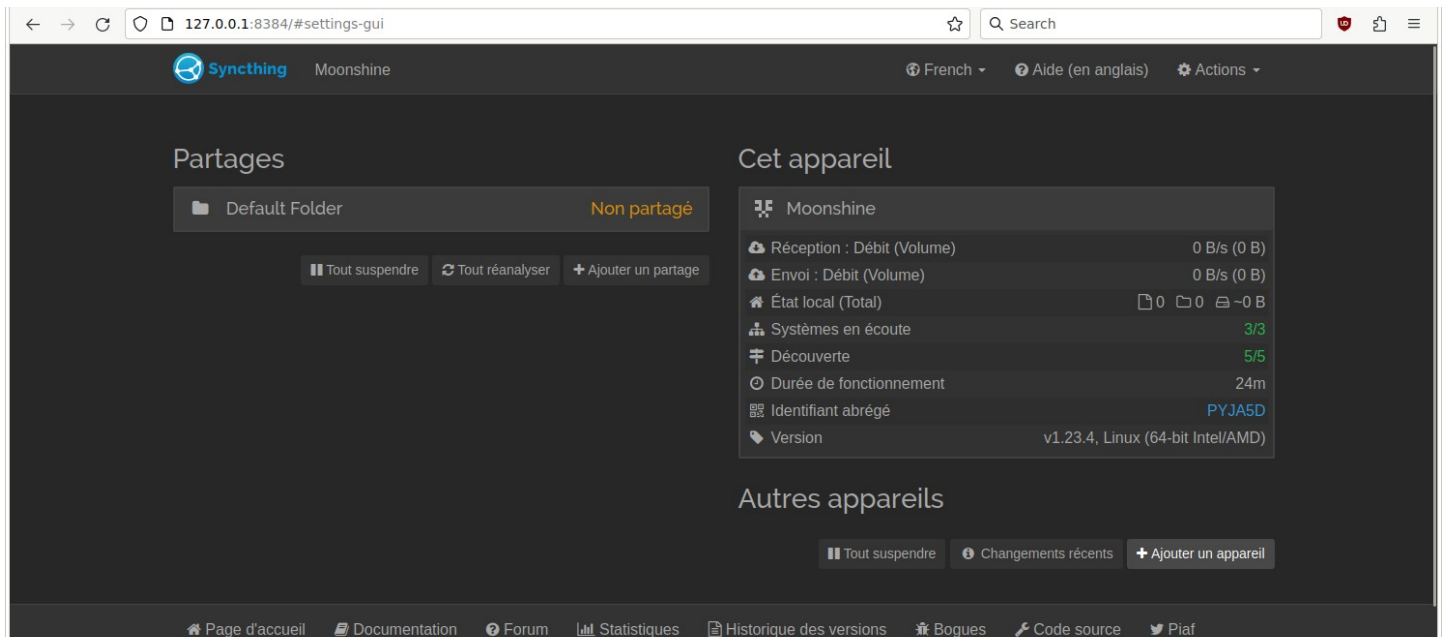


Choix de l'identifiant et du mot de passe :

Du fait que Syncthing tourne en tant que « **utilisateur** » (et qu'il a donc la possibilité de lire et d'écrire tous les fichiers que « utilisateur » peut lire et écrire), il n'est probablement pas utile de définir un couple « identifiant + mot de passe » qui ne soit pas le même que celui de la session utilisateur.

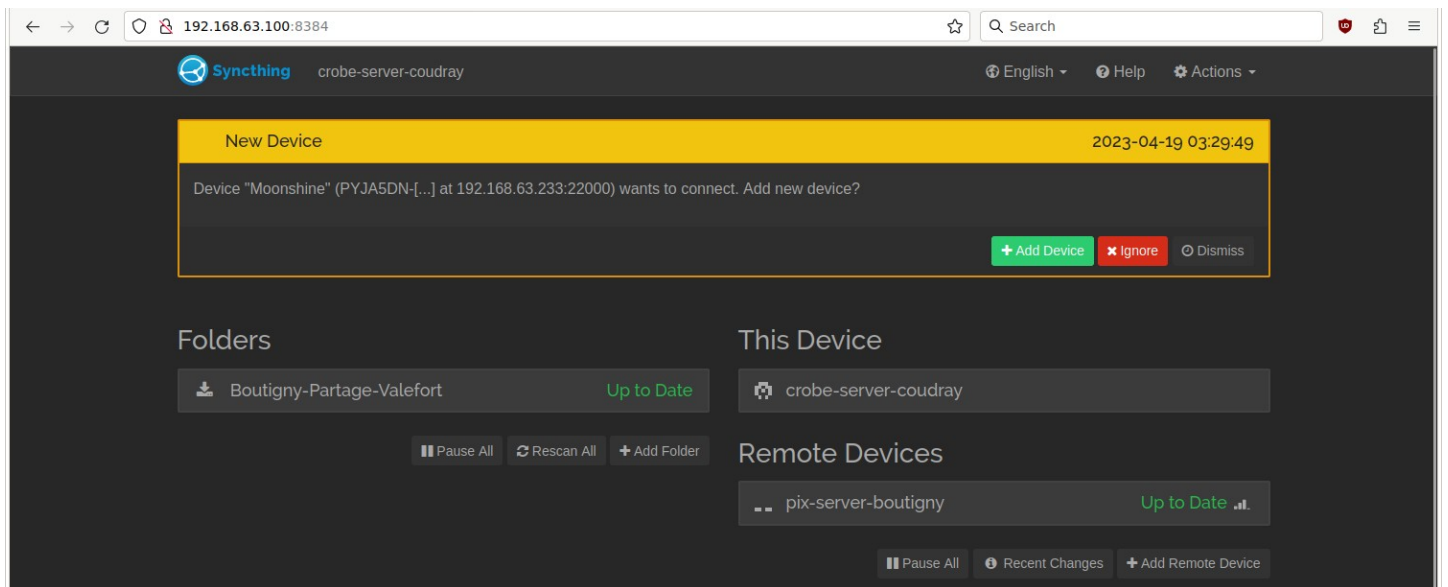
15.4 Configuration Syncthing : lien avec d'autres PC

Toujours via la même interface, cliquer sur « **Ajouter un appareil** » en bas à droite.

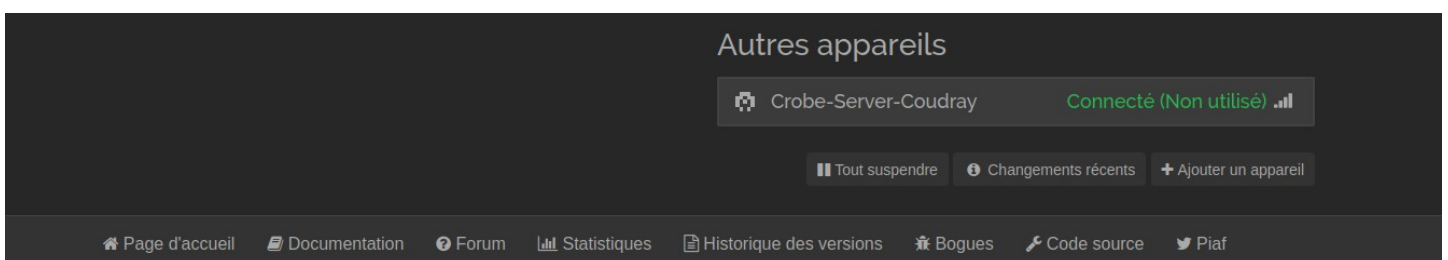


Il nous demande le code de la machine qu'on veut ajouter. On le récupère, sur l'autre machine, en cliquant sur « Action » puis « Afficher mon ID »

Cet identifiant ne suffit pas : L'autre machine nous demande si on est bien d'accord pour l'ajouter (il faut que les deux se disent « oui » avant de pouvoir s'échanger des dossiers).



Une fois les consentements échangés les deux PC sont désormais unis par le protocole TCP/IP.

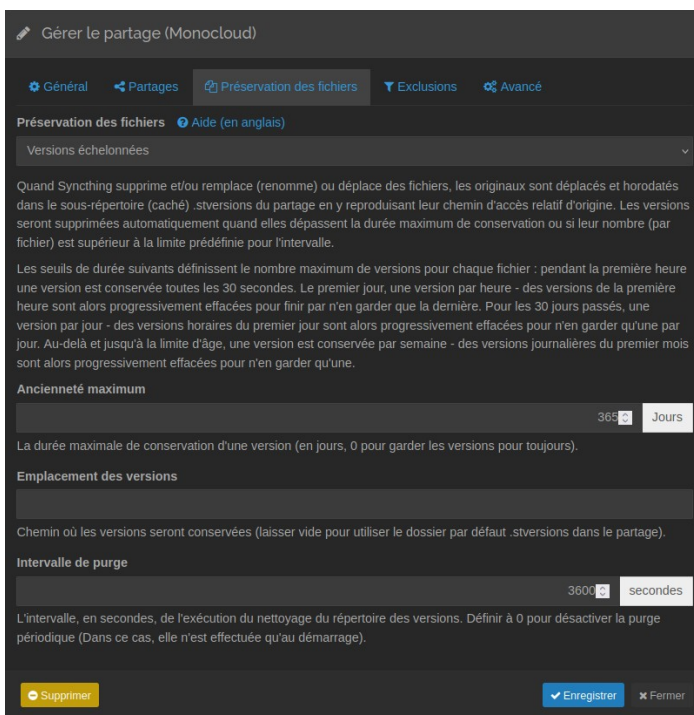
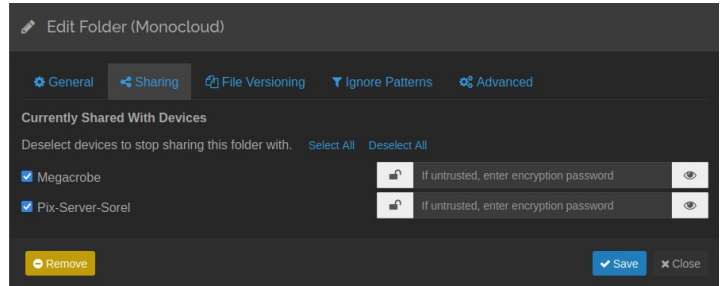
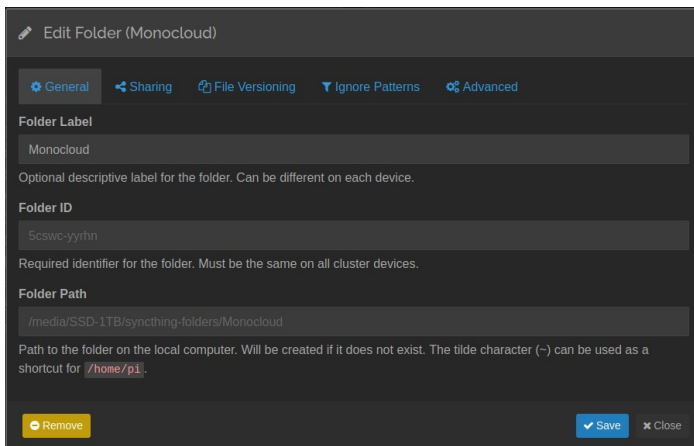


Il devient alors possible, de part et d'autre, de partager / créer / recevoir des dossiers.

Il est également possible de faire en sorte qu'un ordinateur soit le seul à décider du contenu d'un dossier (envoi uniquement : si appareil distant modifie un fichier, cette modification ne sera pas téléchargée localement, elle sera ignorée). Voyons ça plus en détails.

15.5 Configuration Syncthing : Partage de dossiers

En cliquant sur « **Ajouter un partage** » ou en **modifiant** les options de partage d'un dossier existant, plusieurs choses peuvent être réglées.



On peut définir, pour chaque dossier, avec quelle(s) machine(s) on veut partager ce dossier. Si un dossier local est réglé en « **Envoi & Réception** » : toutes les autres machines auront le droit d'y faire des modifications (tous les PC auront le même contenu, dès qu'un fichier change à un endroit, les autres reçoivent le fichier).

Pour info : c'est grisé, mais le changement d'adresse d'un dossier est possible. Pendant que Syncthing est éteint, et en éditant le fichier « config.xml » dans « /home/utilisateur/.config/syncthing/ ». Mais l'idéal c'est donc de créer et/ou placer les dossiers aux bons endroits du premier coup.

Mode « **Réception seulement** » : idéal côté serveur de sauvegarde.

Si Syncthing, sur une machine donnée, est réglé en « Réception seulement », il n'est pas prévu que les fichiers sur son disque dur, soient édités localement (la modification doit venir des autres appareils).

Si cela arrivait (par mégarde par exemple, en éditant localement les fichiers soi même depuis un explorateur), dans ce cas Syncthing affichera un avertissement sur son interface, comme quoi il n'est pas réglé pour transmettre cette modification locale vers aucun appareil. Il proposera d'annuler / écraser la modification locale (en re-téléchargeant la version présente sur les autres appareils, par le réseau).

Mode « **Envoi (lecture seule)** » : idéal côté PC de tous les jours.

Dans ce cas, Syncthing enverra les fichiers présents sur le disque, vers d'autres ordinateurs. Mais il ne créera ou ne modifiera pas ces fichiers lui-même : il se contentera de les lire, et de les envoyer.

Dans ce cas : même si d'autres appareils sont réglés autrement qu'en « Réception seulement » sur le même dossier, et tentent d'envoyer une modification de fichier : Syncthing de ce côté « lecture seule » refusera de recevoir cette modification.

Bien comprendre : il est toujours possible de modifier les fichiers localement, mais dans ce mode ce n'est pas Syncthing qui le fera (lui, il se contentera d'envoyer les fichiers présents mais n'en sera pas le créateur).

15.6 Préservation des fichiers

Lorsque c'est actif, en « Versions échelonnées », lors de toute modification en provenance d'un autre appareil, Syncthing prendra d'abord le temps de déplacer la version locale précédente du fichier avant de recevoir la nouvelle.

Très utile en cas d'écrasement accidentel de fichier, ou de suppression accidentelle.

Sur les machines distantes, la version précédente du fichier est alors conservée dans un sous-dossier « .stversions », pendant la durée souhaitée (Syncthing fait un tri régulier dans .stversions).

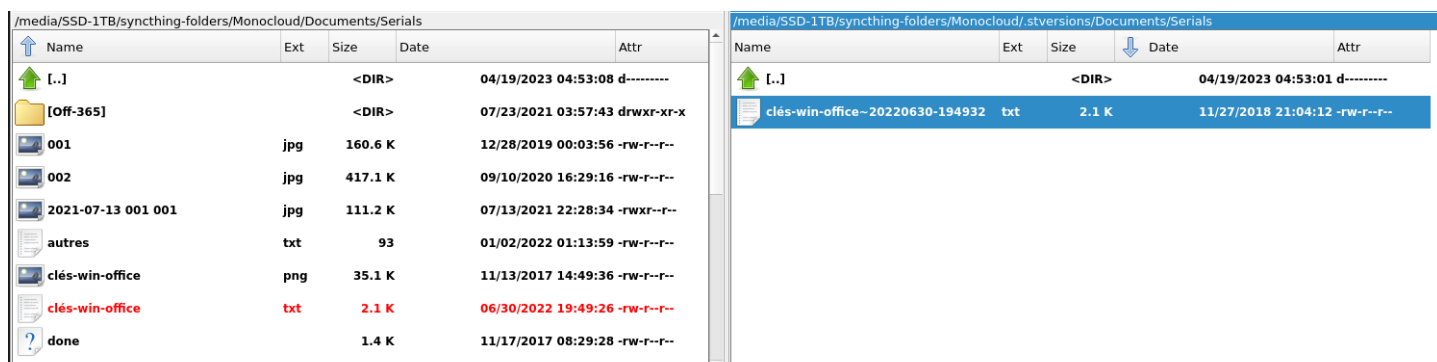
Ça fonctionne en cas de modification d'un fichier, comme en cas de suppression.

Attention : il n'y a pas de préservation locale sur les modifications locales !

En effet, si un logiciel (par exemple, Microsoft Word) décide d'écraser localement un fichier sur le disque dur, au moment où Syncthing s'en rend compte, localement la version précédente du fichier n'existe plus (c'est trop tard il est déjà écrasé).

C'est sur les autres machines que la version précédente va rester : quand un appareil Syncthing est prévenu qu'une nouvelle version d'un fichier arrive, ou qu'un fichier a été supprimé, lui il possède encore à ce stade une copie du fichier non modifié. Il peut donc prendre le temps de placer une sauvegarde de sa version locale du fichier dans son dossier « .stversions » avant de recevoir et d'appliquer le changement.

Exemple de fichier préservé :



Le fichier « clés-win-office.txt » a été modifié le 30 juin 2022 à 19h49 (voir à gauche) depuis Sorel-Moussel.

Par conséquent, dans mon appareil au Coudray, dans `.stversions/Documents/Serials/` j'ai bien un fichier « clés-win-office~20 220 630-194 932.txt » : le nom du fichier est modifié pour contenir la date à laquelle il a été placé dans `.stversions`.

Au 30 juin 2023 cette ancienne version aura été là depuis 365 jours et sera supprimée de `.stversions`.

16 Motion – Gestion de caméras de surveillance

16.1 Installation

Pour installer motion, commencer par entrer en tant que root la commande suivante :

```
apt install motion
```

Attention l'installation de motion est foireuse depuis Debian 11 (toujours le cas sous Debian 12). Elle crée le dossier `/var/lib/motion/` mais n'autorise pas motion à écrire dedans... or c'est là qu'il va chercher à écrire les vidéos. Aussi, le dossier `/var/log/motion/` n'est pas créé (or c'est là qu'il va nous dire s'il fonctionne normalement, et dans le cas contraire, pourquoi – donc là il ne peut pas marcher, et ne peut pas nous le dire).

Pour corriger tout ça, depuis un terminal root :

```
chown -R motion:adm /var/lib/motion
mkdir /var/log/motion
chown -R motion:adm /var/log/motion
service motion restart
```

Normalement après ça, c'est rattrapé.

Comprendre : À ce stade, il devient sans doute clair que ceux qui nous disent que « Windows c'est plein de bugs », et qu'ils utilisent Linux parce qu'il y en a moins, sont dans le déni ! Linux a des avantages certains, mais l'absence de bugs est très loin d'en faire partie.

Bon à savoir : via WinSCP il est également possible de créer et modifier (sans lignes de commandes) des dossiers, et leurs permissions, via clic droit sur un élément, en naviguant sur le serveur.

16.2 Configuration (principe) :

Il faut éditer le fichier `/etc/motion/motion.conf` pour y placer l'adresse des caméras qu'on veut utiliser, ainsi que les réglages d'enregistrement.

Une fois la modification effectuée, jouer la commande « **service motion restart** » pour redémarrer motion. Une fois motion redémarré, aller voir dans `/var/log/motion/` s'il indique des erreurs, puis dans `/var/lib/motion/` si les images ou vidéo apparaissent bien (ou dans tout autre dossier choisi)

IMPORTANT : quel que soit le dossier choisi (`/var/lib/motion/` ou autre), s'assurer que les permissions du dossier permettront à l'utilisateur « motion » d'écrire dedans ! CF les commandes un peu plus haut après l'installation.

16.3 Exemple de configuration : Caméra RTSP à Sorel, Pi 4

C'est une configuration relativement rudimentaire, que j'ai rendu accessible depuis le réseau local mais pas depuis Internet (la configuration de ma Box est faite en sorte qu'elle n'autorise pas l'accès depuis Internet)

Voici les champs que j'ai modifiés dans `/etc/motion/motion.conf`:

- `; videodevice /dev/video0`
- `netcam_url rtsp://192.168.28.230:554/11`
- `width 1280`
- `height 720`
- `; text_left CAMERA1`

- `# Always save pictures and movies even if there was no motion.`
- `emulate_motion on`

- `movie_output off`
- `movie_max_time 1800`

- `stream_localhost off`
- #####
CUSTOM ADDITIONS

`stream_maxrate 4`
`use_extpipe on`
`extpipe ffmpeg -loglevel error -y -f rawvideo -pix_fmt yuv420p -video_size %wx%h -framerate %fps -i pipe:0 -c:v h264_v4l2m2m -profile:v 100 -b:v 800000 -f mpegts %f.ts`

Tous ces réglages permettent de traiter 16 images par seconde d'une caméra 1280x720, et de passer le travail d'encodage non pas à motion lui même, mais à « ffmpeg » (utilisant l'encodeur hardware du Pi 4).

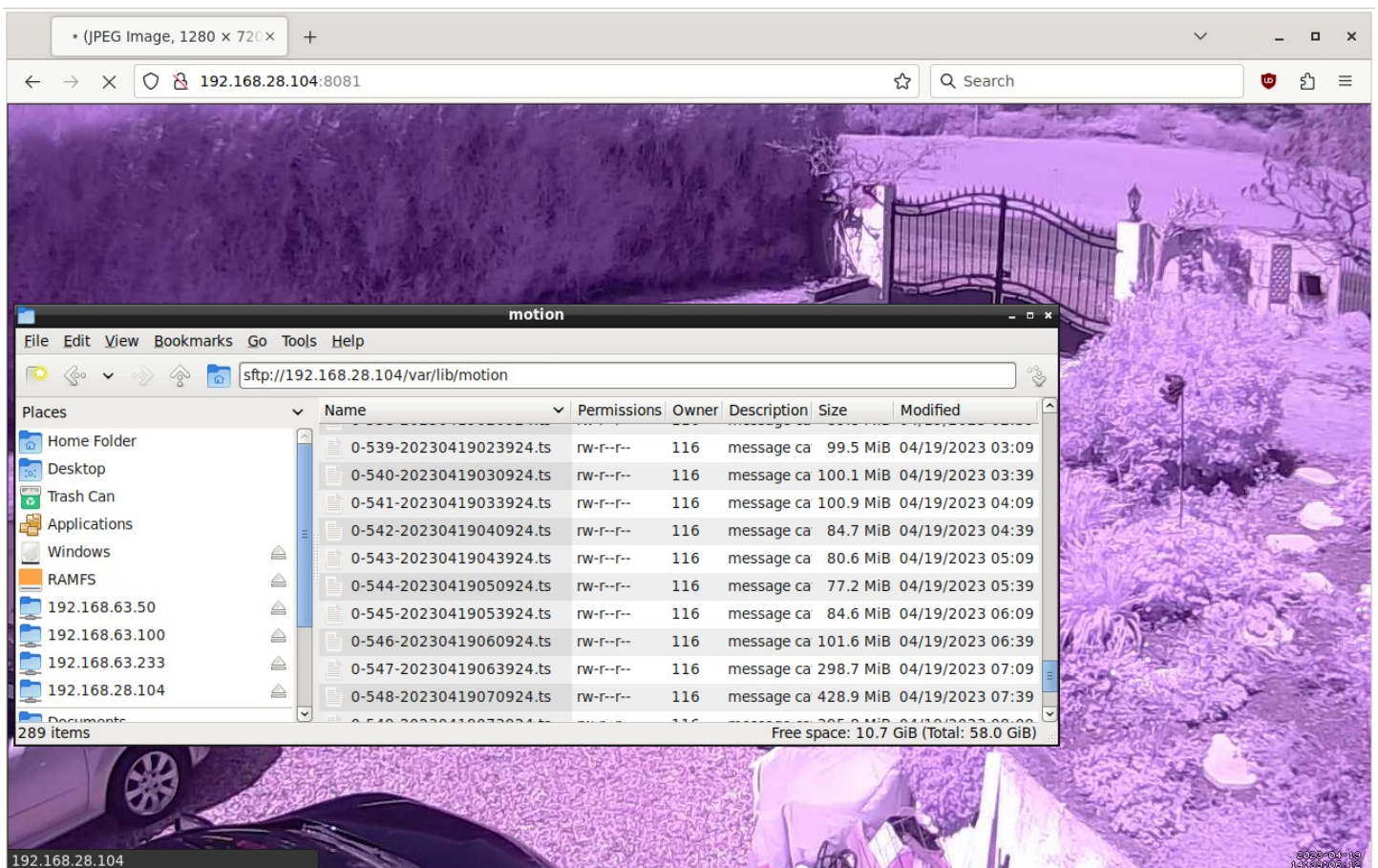
On ouvre également le port « 8081 » de motion aux autres équipements du réseau pour voir 4 images par seconde depuis un navigateur Web (stream_localhost à « on » activerait une restriction à 127.0.0.1)

Motion enregistrera en continu plutôt de de chercher à savoir si quelque chose bouge. Les fichiers dureront 1800 secondes soit 30 minutes chacun. Tout est dit normalement.

L'accès au port 8081 ne permet que de visualiser l'image caméra, mais ne permet pas de modifier quoi que ce soit. C'est donc safe (en cas de piratage, les gens verront simplement notre allée, rien de compromettant).

Résultat :

Voici une petite capture d'écran qui montre un peu tout en une fois :



On peut se connecter à l'image de la caméra en tapant l'adresse du Pi4 sur lequel tourne motion, dans ce cas <http://192.168.28.104:8081> et on peut via SSH, aller récupérer les fichiers vidéos dans `/var/lib/motion/`

16.4 Exemple de configuration : 3 Caméras RTSP avec mots de passe

Configuration très poussée et détaillée pour accès sécurisé (identifiants + <https>) depuis Internet, pour empêcher quiconque d'accéder aux images caméras sans en avoir le droit, ainsi qu'au port de contrôle (8080).

Voici les champs qu'on a modifié dans `/etc/motion/motion.conf`

```
• target_dir /media/Data-RAID/Cameras/
• ; videodevice /dev/video0
• framerate 25
• # text_left CAMERA1
• # Threshold for number of changed pixels that triggers motion.
  # 1% de 1920x1080 = 20 000
  # valeur par défaut : 1500
  threshold 20000
• # Gap in seconds of no motion detected that triggers the end of an event.
  event_gap 0
• # 125 images à 25 FPS = 5 secondes
  post_capture 125
• movie_output off
• movie_max_time 600
• webcontrol_ipv6 on
  webcontrol_auth_method 2
  stream_auth_method 2
webcontrol_authentication UTILISATEUR:MOTDEPASSE
stream_authentication UTILISATEUR:MOTDEPASSE
  webcontrol_tls on
  stream_tls on
  webcontrol_cert /etc/letsencrypt/live/exemple/fullchain.pem
  webcontrol_key /etc/letsencrypt/live/exemple/privkey.pem
  webcontrol_lock_attempts 5
  webcontrol_lock_minutes 10
• webcontrol_localhost off
• webcontrol_parms 1
• ; stream_port 8081
• ; stream_localhost on
• camera /etc/motion/1-salon.conf
• camera /etc/motion/2-exterieur.conf
• camera /etc/motion/3-bureau.conf
• #####
  # CUSTOM ADDITIONS
  #####
  stream_maxrate 4
  use_extpipe on
  extpipe ffmpeg -y -f rawvideo -pix_fmt yuv420p -video_size %wx%h -framerate %fps -i
  pipe:0 -c:v libx265 -preset ultrafast -f mpegts %f.ts
```

Cette configuration demande à `/etc/motion/motion.conf` de ne pas gérer de caméra, puisque c'est dans `/etc/motion/1-salon.conf`, `2-exterieur.conf` et `3-bureau.conf` qu'on va s'en charger, avec des paramètres différents pour chaque caméra.

L'enregistrement n'est pas fait en continu mais au lieu d'enregistrer 60 secondes de + à chaque fin de détection, on lui demande d'enregistrer 125 images (soit 5 secondes à 25 images/seconde) de plus.

Le seuil de détection (en nombre de pixels qui changent) peut-être modifié dans le cas où la sensibilité de détection est insuffisante ou trop élevée.

On va même jusqu'à activer la gestion IPv6 et le « <https> » grâce à la présence d'un serveur HTTPS et de ses certificats « lets encrypt ». On fait en sorte d'automatiquement bloquer l'accès pendant 10 minutes dans le cas où ont lieu 5 tentatives d'authentification erronées.

On protège l'accès par navigateur Web avec identifiant + mot de passe (il y aura un port séparé pour chaque caméra). Chacun de ces ports sera protégé par `stream_authentication`.

En écrivant « webcontrol_localhost off » on fait en sorte que le port 8080 soit lui aussi joignable en dehors de « localhost », donc depuis le réseau voire depuis Internet. Protégé par `webcontrol_authentication`.

Fichier de configuration de caméra individuel : `/etc/motion/1-salon.conf`

Voici les lignes ajoutées ou modifiées :

- `camera_name Salon`
- `netcam_url rtsp://AdresseIP-Camera-1:554/s0`
- `netcam_userpass USERCAMERA1:PASSCAMERA1`
- `movie_filename Salon/Salon-%Y-%m-%d_%Hh%Mm%Ss`
- `width 1920`
- `height 1080`
- `# The port number for the live stream.`
`stream_port 8081`
- `stream_localhost off`
- `emulate_motion off`

Ici on indique que le port 8081 servira à accéder à l'image de cette caméra, et par dessus le « target_dir » défini dans « motion.conf », les enregistrements seront placés dans le sous dossier « Salon » (attention, créer ce sous dossier soi même ! Et donner à « motion » le droit d'écrire dedans).

Enfin, `emulate_motion` étant à off, les enregistrements n'auront lieu qu'en cas de détection de mouvement.

Fichier de configuration de caméra individuel : `/etc/motion/2-exterieur.conf`

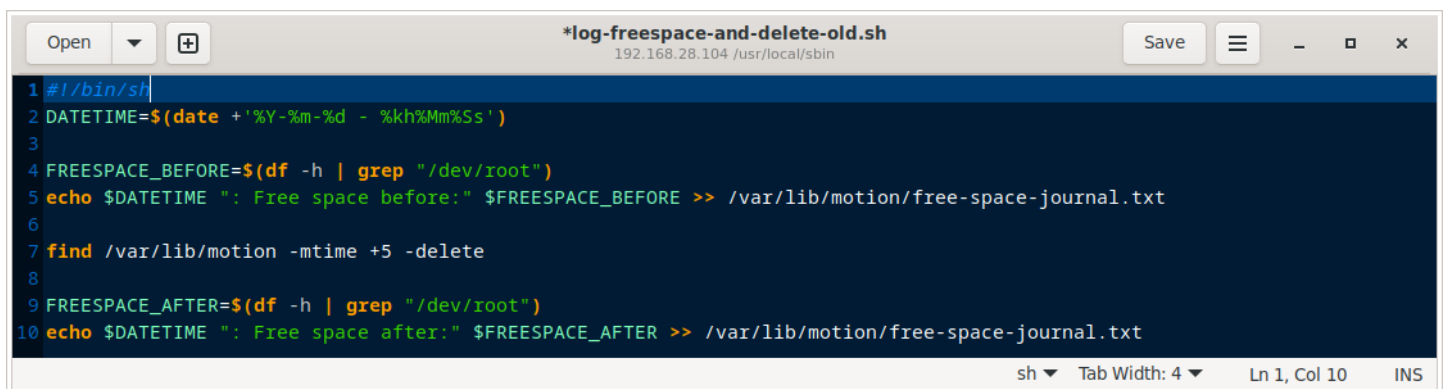
- `camera_name Exterieur`
- `netcam_url rtsp://AdresseIP-Camera-2:554/s0`
- `netcam_userpass USERCAMERA2:PASSCAMERA2`
- `width 1920`
- `height 1080`
- `movie_filename Exterieur/Exterieur-%Y-%m-%d_%Hh%Mm%Ss`
- `# The port number for the live stream.`
`stream_port 8082`
- `stream_localhost off`
- `# Always save pictures and movies even if there was no motion.`
`emulate_motion on`

Principe semblable, ici néanmoins on demande à motion d'enregistrer en continu (`emulate_motion on`), et le stream port (pour visualiser l'image depuis un navigateur) est 8082.

Même principe pour la caméra 3.

16.5 Nettoyage régulier

De façon à ce que les images ne s'empilent pas éternellement, une commande peut-être exécutée tous les jours. Ou même un script, exemple : `/usr/local/sbin/log-freespace-and-delete-old.sh` :



```
*log-freespace-and-delete-old.sh
192.168.28.104 /usr/local/sbin

1 #!/bin/sh
2 DATETIME=$(date +%Y-%m-%d - %kh%Mm%Ss')
3
4 FREESPACE_BEFORE=$(df -h | grep "/dev/root")
5 echo $DATETIME ": Free space before:" $FREESPACE_BEFORE >> /var/lib/motion/free-space-journal.txt
6
7 find /var/lib/motion -mtime +5 -delete
8
9 FREESPACE_AFTER=$(df -h | grep "/dev/root")
10 echo $DATETIME ": Free space after:" $FREESPACE_AFTER >> /var/lib/motion/free-space-journal.txt
```

La commande « find » est suffisante, le reste n'est qu'un petit montage perso optionnel pour faire un suivi d'utilisation d'espace disque.

Contenu pour copier coller :

```
#!/bin/sh
DATETIME=$(date +%Y-%m-%d - %kh%Mm%Ss')

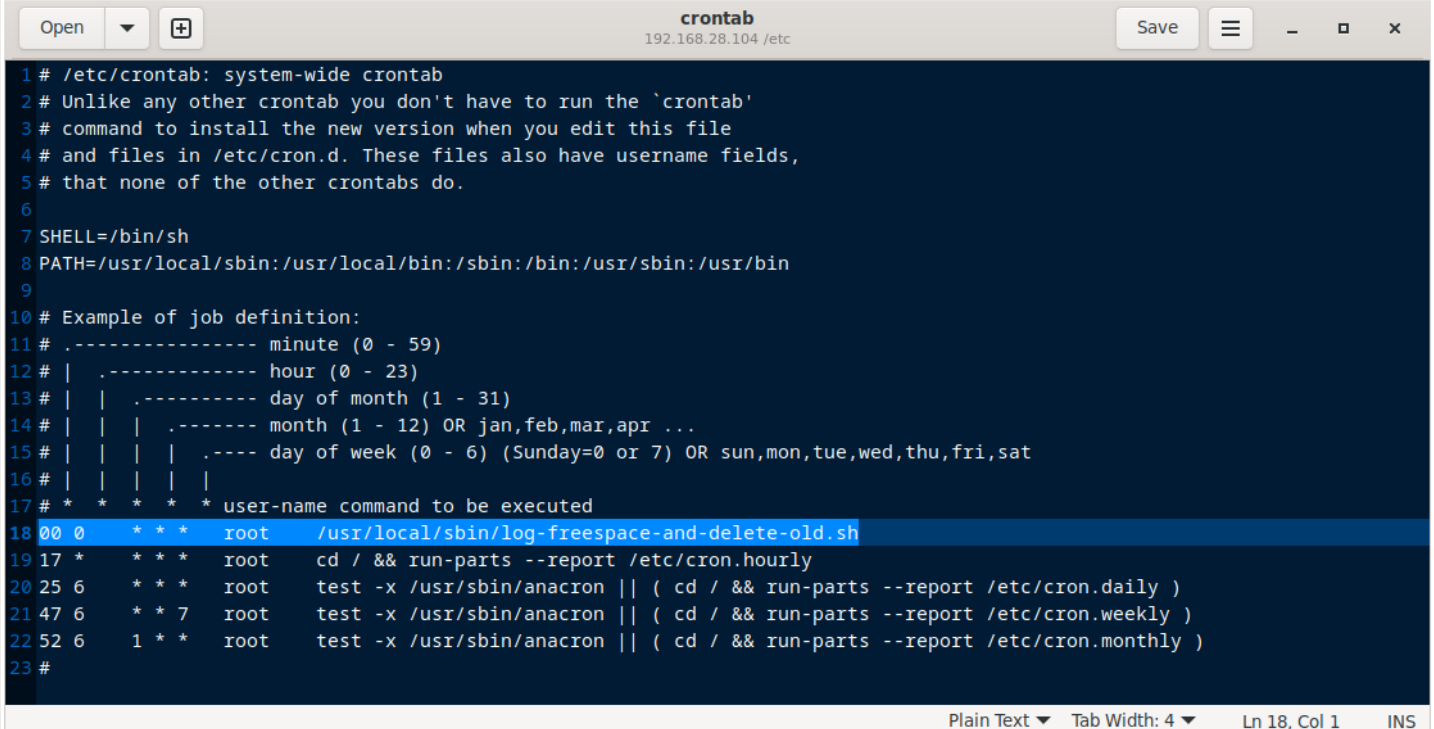
FREESPACE_BEFORE=$(df -h | grep "/dev/root")
echo $DATETIME ": Free space before:" $FREESPACE_BEFORE >> /var/lib/motion/free-space-journal.txt

find /var/lib/motion -mtime +5 -delete

FREESPACE_AFTER=$(df -h | grep "/dev/root")
echo $DATETIME ": Free space after:" $FREESPACE_AFTER >> /var/lib/motion/free-space-journal.txt
```

On peut évidemment adapter ce script en cas de besoin. **Attention, penser à le rendre exécutable !**
On pourra ensuite demander à `/etc/crontab` de nous exécuter ce script tous les jours à minuit via la ligne suivante :

```
00 0 * * * root /usr/local/sbin/log-freespace-and-delete-old.sh
```



```
1 # /etc/crontab: system-wide crontab
2 # Unlike any other crontab you don't have to run the `crontab'
3 # command to install the new version when you edit this file
4 # and files in /etc/cron.d. These files also have username fields,
5 # that none of the other crontabs do.
6
7 SHELL=/bin/sh
8 PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
9
10 # Example of job definition:
11 # .----- minute (0 - 59)
12 # | .----- hour (0 - 23)
13 # | | .----- day of month (1 - 31)
14 # | | | .----- month (1 - 12) OR jan,feb,mar,apr ...
15 # | | | | .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
16 # | | | | |
17 # * * * * * user-name command to be executed
18 00 0 * * * root /usr/local/sbin/log-freespace-and-delete-old.sh
19 17 * * * * root cd / && run-parts --report /etc/cron.hourly
20 25 6 * * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
21 47 6 * * 7 root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
22 52 6 1 * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
23 #
```

En procédant ainsi, lorsqu'il y a dans le script « `-mtime +5` » on conserve entre 6 jours de vidéo (juste après l'effacement) et 7 jours (juste avant l'effacement). Le fichier « `free-space-journal.txt` » me permet de savoir, sur un Raspberry Pi, s'il n'y a pas des jours où le disque était plein (ou limite de l'être) avant l'exécution du script. Puis de voir combien de place était rendue disponible juste après son exécution.

17 Mots de passe

Pour que la machine reste sécurisée en étant sur un réseau local, voire pour qu'elle reste sécurisée en étant (même partiellement) joignable depuis Internet, les mots de passe ne doivent pas être faibles (du genre nom commun + 2 chiffres c'est insuffisant). Même une série de 8 lettres et chiffres mélangées sont aujourd'hui crackables facilement.

Selon la CNIL :

« *Un bon mot de passe peut contenir, par exemple, au moins 12 caractères et 4 types différents : des minuscules, des majuscules, des chiffres et des caractères spéciaux* »

Aussi, ils ne doivent pas être utilisés sur des sites Internet (quand les sites se font pirater, les mots de passe utilisateurs, même complexes, finissent parfois dans des base de données pour les pirates, pour des logiciels automatiques). Un super mot de passe divulgué sur Internet devient une super porte ouverte !

17.1 Changer les mots de passe

Depuis un terminal root :

```
passwd root
passwd utilisateur

x11vnc -storepasswd /var/vnc/x11vnc.pass
```

Pour **Syncthing**, se rendre sur son interface via navigateur, et dans Action > Configuration.

Pour **motion**, les mots de passe d'accès aux caméras sont dans /etc/motion/motion.conf, ainsi que les mots de passe d'accès à l'aperçu HTTP.

17.2 Mots de passe systèmes Linux perdu ?

Sous Linux, si les mots de passe sont perdus, il faut démarrer le système depuis une clé USB par exemple (démarrage d'un système « Live », volatile : ses fichiers sont chargés ou modifiés en mémoire et tout disparaîtra après reboot).

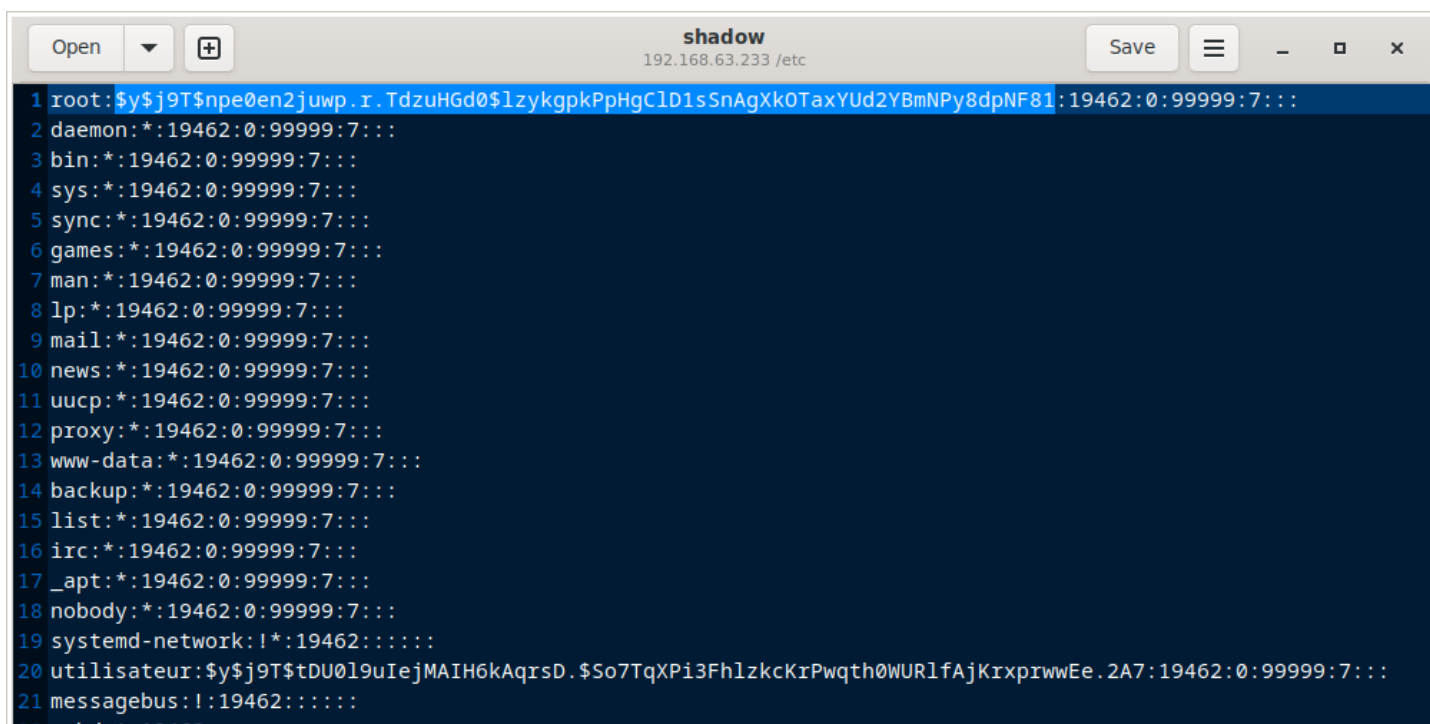
Il faut alors utiliser ce système pour :

- monter le « root-fs » quelque part via gnome-disks (exemple : /media/user/root-fs/)
- aller y écraser les « hash » dans le fichier « /media/user/root-fs/etc/shadow »

Commandes utiles à connaître depuis un système live :

- sudo -i (pour devenir root)
- setxkbmap fr (pour passer le clavier en azerty – important si on veut fixer des mots de passes !)

Ci-dessous, voici ce qu'est un « hash » (il y en a un pour « root » et un autre pour « utilisateur ») :



```
shadow
192.168.63.233 /etc

1 root:$y$j9T$npe0en2juwp.r.TdzuHGd0$lzykgpkPpHgC1D1sSnAgXkOTaxYUd2YBmNPY8dpNF81:19462:0:99999:7:::
2 daemon:*:19462:0:99999:7:::
3 bin:*:19462:0:99999:7:::
4 sys:*:19462:0:99999:7:::
5 sync:*:19462:0:99999:7:::
6 games:*:19462:0:99999:7:::
7 man:*:19462:0:99999:7:::
8 lp:*:19462:0:99999:7:::
9 mail:*:19462:0:99999:7:::
10 news:*:19462:0:99999:7:::
11 uucp:*:19462:0:99999:7:::
12 proxy:*:19462:0:99999:7:::
13 www-data:*:19462:0:99999:7:::
14 backup:*:19462:0:99999:7:::
15 list:*:19462:0:99999:7:::
16 irc:*:19462:0:99999:7:::
17 _apt:*:19462:0:99999:7:::
18 nobody:*:19462:0:99999:7:::
19 systemd-networkd:*:19462:0:99999:7:::
20 utilisateur:$y$j9T$tDU0l9uIejMAIH6kAqrsD.$So7TqXPi3FhlzkcKrPwqth0WURlfaJkRxprrwEe.2A7:19462:0:99999:7:::
21 messagebus:*:19462:0:99999:7:::
22 systemd-logd:*:19462:0:99999:7:::
```

Le principe d'un hash, c'est qu'à moins de brute-forcer pour finir par tomber sur un mot de passe qui correspond, lire le hash ne doit pas permettre de savoir à quel mot de passe valide il correspond.

Il ne doit permettre que de valider si un mot de passe entré est valable ou non (c'est un vérificateur de mot de passe, en gros).

Les hashes montrés ici correspondent à des mots de passe faibles, respectivement root (pour la session root) et... utilisateur pour la session utilisateur (c'est très bien pour faire des essais hors ligne, mais pas au-delà !)

Créer ses propres hashes de remplacement :

On peut créer ses propres « hash » de remplacement, en fixant tout simplement via « passwd » un mot de passe connu sur un autre système, puis en regardant dans son fichier /etc/shadow. Il est possible qu'il existe des commandes pour faire encore plus simple (mais je n'en connais pas – les curieux pourront chercher ça).

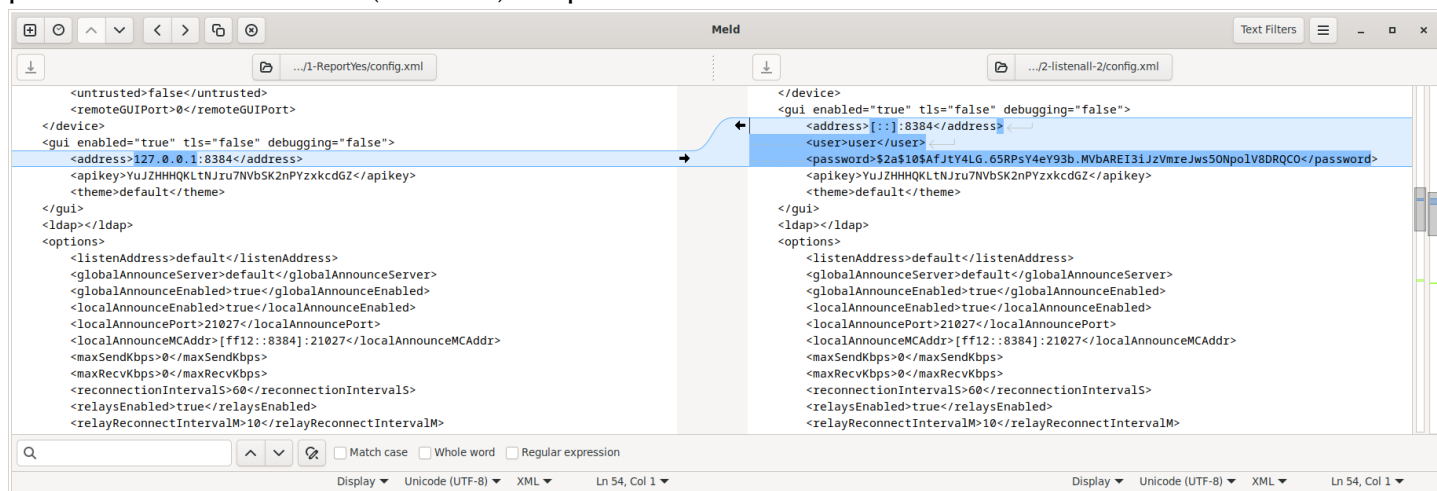
Bon à savoir : Pour trouver un autre système, pas besoin d'aller très loin : juste en tapant les commandes « passwd » depuis un système live USB volatile : ça les mettra dans le fichier volatile « /etc/shadow », dans lequel on peut venir lire ensuite pour piquer les « hashes » que ça a généré. Puis les appliquer dans le fichier /etc/shadow du système cible.

17.3 Mot de passe de l'interface Syncthing perdu ?

L'ajout d'un nom d'utilisateur + mot de passe dans l'interface Syncthing se traduit par l'ajout de deux lignes dans /home/utilisateur/.config/syncthing/config.xml :

- Un champs xml <user>...</user>
- Un champs xml <password>...</password>

C'est également ici que le champs « address » passe de 127.0.0.1:8384 à [::]:8384 quand on demande de ne plus limiter l'accès en local (localhost) uniquement.



Éteindre Syncthing (via « systemctl stop syncthing@utilisateur »), puis éditer le fichier config.xml. La suppression de ces deux lignes devrait suffire à retrouver l'accès à l'interface.

Une fois la modification effectuée, pour redémarrer syncthing, taper la commande « reboot » pour tout relancer, sinon « systemctl start syncthing@utilisateur ».

17.4 Mot de passe pour les caméras « Motion » perdu ?

Normalement, ils sont tout simplement écrits en clair dans le (ou les) fichier(s) du dossier /etc/motion/

Si toutefois on parle de remettre à zéro le mot de passe d'une caméra, qu'on ne parviendrait plus à retrouver, se référer à la notice du fabricant. Il peut arriver que ce soit tout con (appuyer sur un bouton caché pendant la mise sous tension, par exemple). Il peut aussi arriver que ce soit compliqué, ça dépend de ce que le fabricant a voulu faire.