

Projet Linux

VANGEEBERGEN Augustin

August 19, 2024



Table des matières

1	Introduction	3
1.1	Consignes (pratiques) professeur	4
1.2	Roadmap	5
2	Avant de commencer	6
2.1	Hosting	6
2.2	Partitionnement et RAID	6
2.3	VirtualBox	7
2.4	Réseau	15
2.5	Changer le layout clavier	16
2.6	Snapshots de la machine	16
2.7	Ajout des disques virtuels	16
3	Description du logiciel	18
3.1	Hostname	18
3.2	Configuration RAID	18
3.3	Connection SSH	18
3.4	Partage NFS/SAMBA sans authentification	18
3.5	Services Web	18
3.5.1	Installation initiale	18
3.5.2	Ajout d'utilisateurs	19
3.6	NTP Time Server	19
3.7	Install clamav	19
3.8	Backup	19
3.9	Consult Logs Dashboard	19
3.10	Clonage du repo git	19
3.11	Menu principal	19
3.12	RAID	19
3.13	Partage sans authentification	19
3.14	Connexion par SSH	19
3.15	Setup initial des services	20
3.15.1	IP fixe	20
3.15.2	Gestion DNS interne	20
3.15.3	Gestion du serveur web	20
3.15.4	Gestion de la base de données (serveur SQL)	21
3.15.5	Gestion de la base de données (phpmyadmin)	21
3.15.6	Gestion du mail	21
3.16	Gestion des utilisateurs	21
3.17	Serveur temps	21
3.18	Plan de sauvegarde	21
3.19	Sécurité	21
3.20	Journal de bord	21
4	Conclusion	22

1 Introduction

Dans le cadre de ce projet, l'objectif est de configurer un serveur GNU/Linux. Cet exercice consiste à mettre en application la matière vue en classe, et à se préparer à un environnement réel.

Les objectifs globaux sont donc l'application et la compréhension profonde des mécanismes permettant d'héberger les différents services souhaités, de la gestion des utilisateurs, ainsi que de la sécurité, que ce soit au niveau des attaques ou des sauvegardes.

Nous avons le choix d'utiliser n'importe quelle distribution RedHat-like, par exemple Fedora, ou bien Alma, sur laquelle nous avons travaillé en cours. Le choix se porte sur Fedora, qui a une plus grosse communauté (dont je fais partie pour la partie desktop) et a ma préférence (utiliser alma ne changerait bien sûr quasiment rien, les deux distributions étant très similaires).

Les consignes professeur sont reprises dans le sous-point suivant.

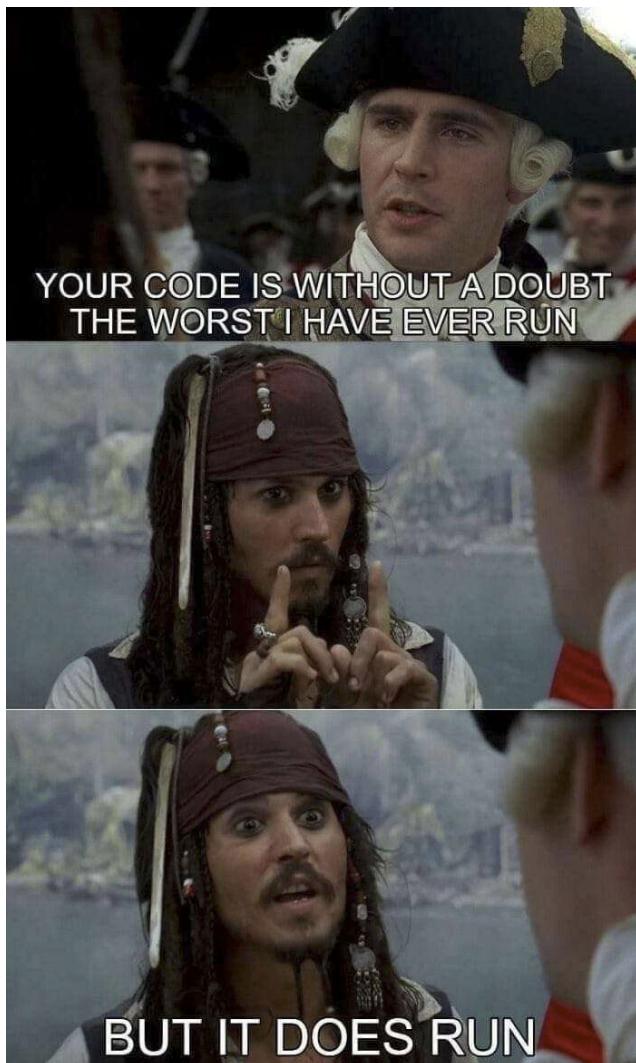
L'OS de test est une machine virtuelle, hébergée sur VirtualBox.

Une machine Windows et une autre machine linux sont également installées comme clients. Le but est aussi de pouvoir gérer en ssh le serveur avec plein d'outils utiles, et de pouvoir installer/désinstaller les services à souhait, diminuant ainsi la surface d'attaque.

Il faut donc gérer des services de partage de fichiers, serveur DNS, serveur Web ainsi que serveur temps.

La dernière étape sera de sécuriser le serveur correctement, notamment en utilisant SELinux, et en définissant les politiques d'utilisation correctes.

La sécurité implique également les sauvegardes.



1.1 Consignes (pratiques) professeur

Les consignes sont les suivantes :

- Chaque groupe devra mettre en place un serveur linux selon les règles de l'art et devra respecter les bonnes méthodologies pour le faire.
- Le serveur devra permettre de partager un dossier sans authentification aussi bien pour l'environnement Linux que Windows à l'aide de NFS et Samba.
- Une connexion SSH judicieusement sécurisée permettra à l'administrateur de configurer le serveur et d'exécuter des scripts sur le serveur.
- Le serveur devra permettre la mise à disposition pour un client : d'un nom de domaine dans notre domaine, d'un serveur web, d'un accès FTP et Samba à son dossier web et d'une base de données différente pour chaque utilisateur. Le tout devra être automatisé à l'aide de scripts de configurations. Bien sûr chaque client aura un dossier web, une base de données et un domaine différent.
- En bonus, chaque utilisateur devra posséder une adresse mail dans notre domaine ainsi qu'une interface web pour consulter ses mails.
- Le serveur de domaine devra également faire cache pour les requêtes, être maître dans sa zone et également posséder une zone inverse.
- Le serveur devra permettre aux ordinateurs de son réseau de pouvoir mettre à jour l'heure de leurs machines.
- Le plan de sauvegarde établi devra être mis en place.
- Une attention particulière sera portée sur la sécurisation du serveur et des services à l'aide des outils disponibles. (FW, antivirus, SELinux, ...)
- Toutes les installations et configurations seront notées dans le journal de bord de votre serveur.

1.2 Roadmap

L'ensemble sera scripté pour coller à l'ensemble des cas d'utilisation. Voici donc la liste prévue de ces scripts (pour installer/désinstaller):

- Menu de sélection OK
- Configuration Raid OK
- Configuration SSH OK
- Configuration partage public OK
- Configuration Web
 - Menu OK
 - DNS OK
 - SSL OK
 - DB OK
 - PHP OK
 - PHGPMYAdmin OK
 - Mail KO
- Time server OK
- Sécurisation OK
- Backup OK
- Logs KO

Il est donc indispensable de se former au BASH, afin de savoir faire un bon TUI, ainsi que des commandes conditionnelles, selon les features qui sont/ne sont pas déjà installées.

Le service SSH est indépendant des autres services. Le DNS, time server également.

Cependant, les Serveurs Web, SQL et FTP doivent fonctionner en symbiose. C'est aussi le cas du NFS et SMB. Ce sera donc une personne qui s'occupera de ces services deux à deux.

2 Avant de commencer

2.1 Hosting

Hyper-V n'ayant pas apporté satisfaction (principalement bugs de corruption de checkpoints), je me suis tourné vers d'autres alternatives :

- Gnome boxes qui offre peu de flexibilité au niveau du réseau
- VMware Workstation qui a cassé lors d'une mise à jour du kernel de la machine hôte (Fedora 39 vers Fedora 40)

La seule solution correcte restante étant donc Oracle VirtualBox.

Virtualbox permet en outre d'associer un ou plusieurs disques virtuels à une machine virtuelle, ce qui est plutôt intéressant au vu du contexte, nous y viendrons dans la sous-section suivante.

2.2 Partitionnement et RAID

Il est assez compliqué de séparer le partitionnement et la gestion des disques en deux sous sections, car ces deux concepts sont intimement liés.

Il faut premièrement assurer la préservation des données, dans n'importe quel scénario.

Il faut également s'assurer que la hiérarchie du stockage a du sens et qu'elle est pratique.

Sur la machine virtuelle, il y aura :

- sur un disque, le système d'exploitation contenant les partitions suivantes :
 - /boot
 - /swap
 - /
 - /home
- sur un autre disque, ou plutôt un array de disques en RAID :
 - /share
 - /web
- et enfin, sur un ou plusieurs disque(s) additionnel(s) :
 - /backup

Petite liste des niveaux de RAID (redundant array of independent disks) les plus courants :

- RAID 0 : volume agrégé par bandes (ou striping).

Performances en lecture et écriture extrêmement élevées (jusqu'à n fois pour un nombre n de disques en lecture et écriture), mais aucune redondance, et donc non pertinent pour notre serveur.

- RAID 1 : volumes miroirs.

Meilleure redondance des informations (n-1 disques peuvent être retirés). Pire performance niveau vitesse d'écriture (égale à la vitesse d'écriture d'un disque seul) et vitesse de lecture jusqu'à la somme de la vitesse de chaque disque dans l'array (meilleur scénario). Choix rejeté car en pratique on recherche un milieu entre performance et sécurité/redondance.

- RAID 5 : volume agrégé par bandes à parité répartie.

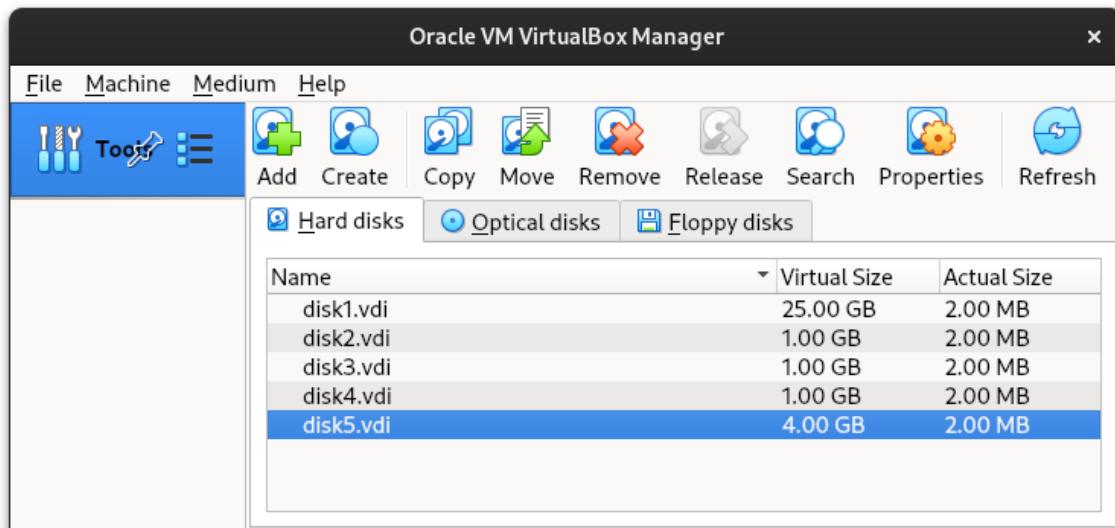
Si un disque lâche, il suffit de remplacer celui-ci, et il peut être reconstruit à partir des autres disques et de la parité stockée sur ceux-ci.

Le choix va se porter sur le RAID 5, qui combine performance et efficacité, en offrant une sécurité sur la casse d'un disque à la fois. On peut donc finir la liste des disques virtuels :

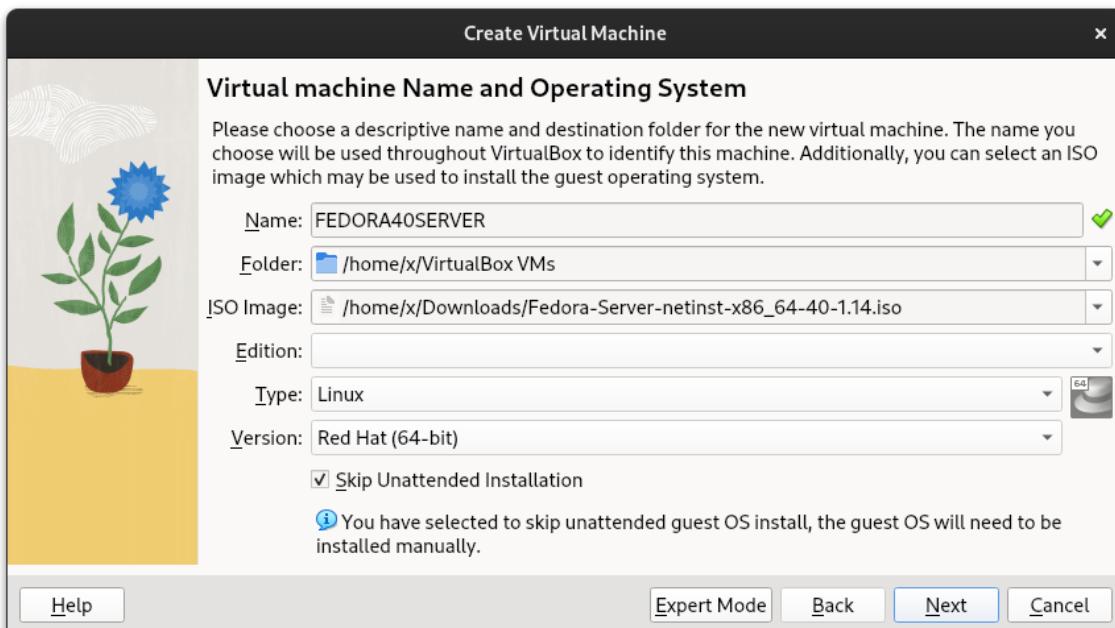
- 1 disque pour l'OS et les fichiers de configuration (disk1)
- 3 disques (c'est à dire le minimum requis pour un RAID 5) pour le stockage (disk2-3-4)
- 1 disque pour la sauvegarde (disk5)

2.3 VirtualBox

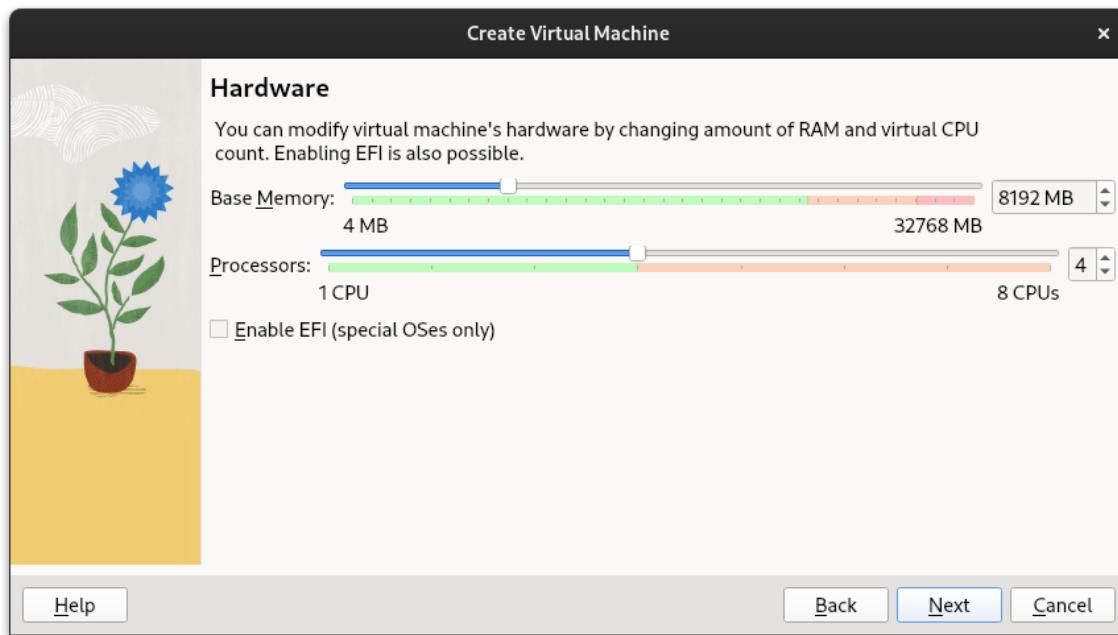
Comme dit précédemment, voici les différents disques virtuels créés et leur taille, dans l'interface de VirtualBox :



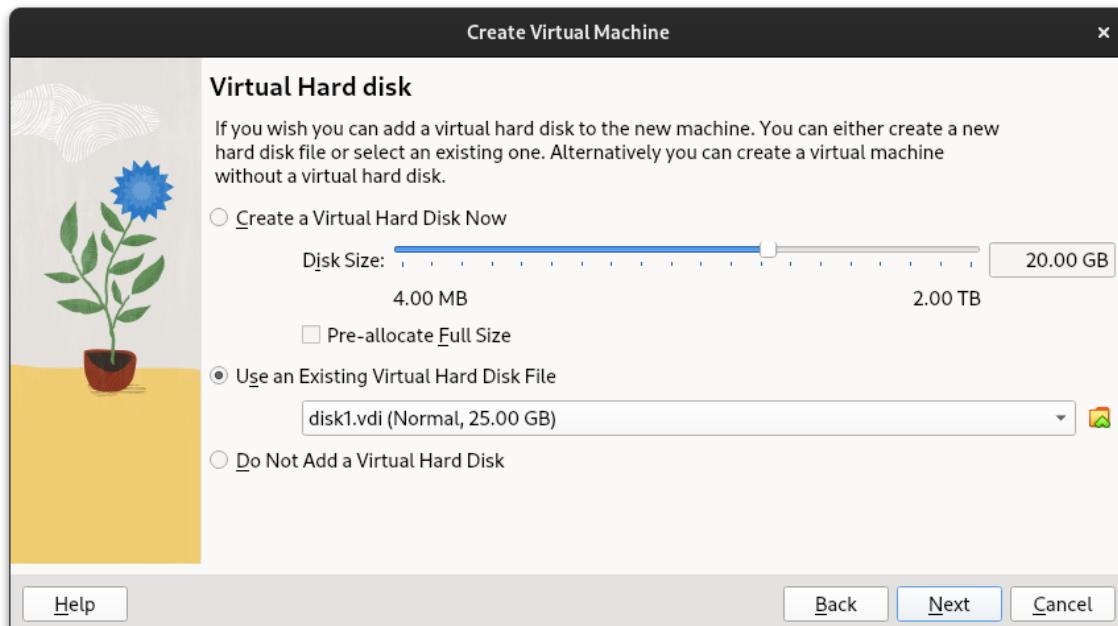
Ensuite, il faut créer la machine virtuelle, en prenant soin de sélectionner le bon ISO :



On sélectionne la quantité de ram optimale pour le système :

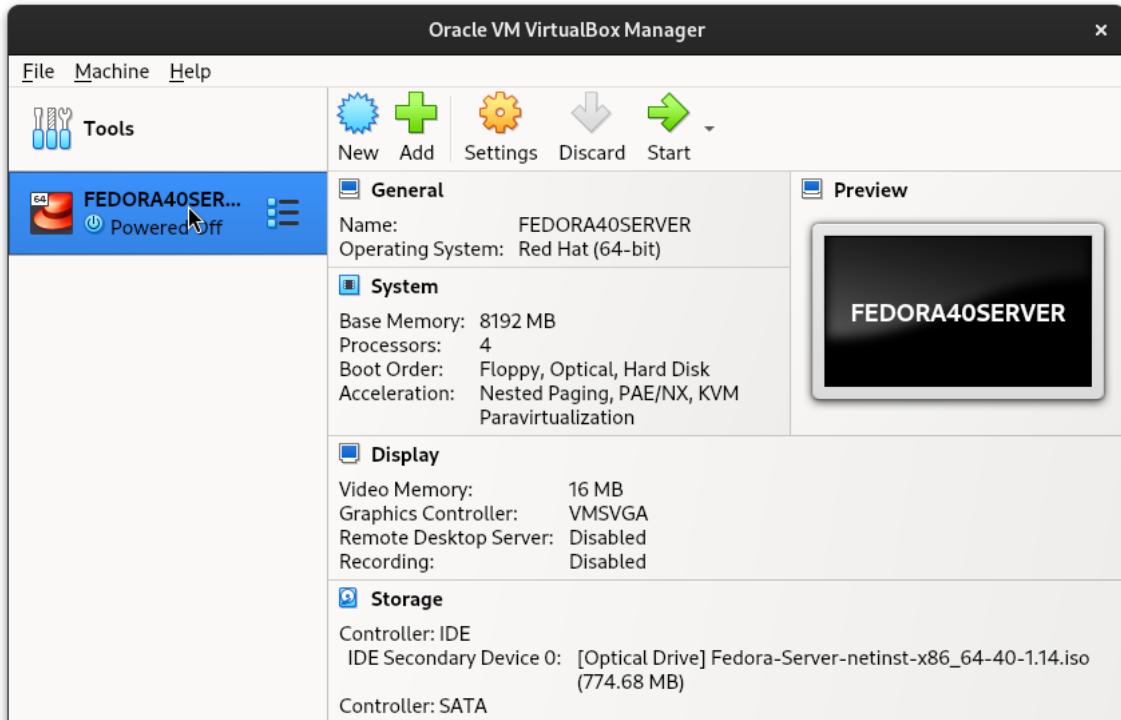


Et on selectionne le disque virtuel créé précédemment :

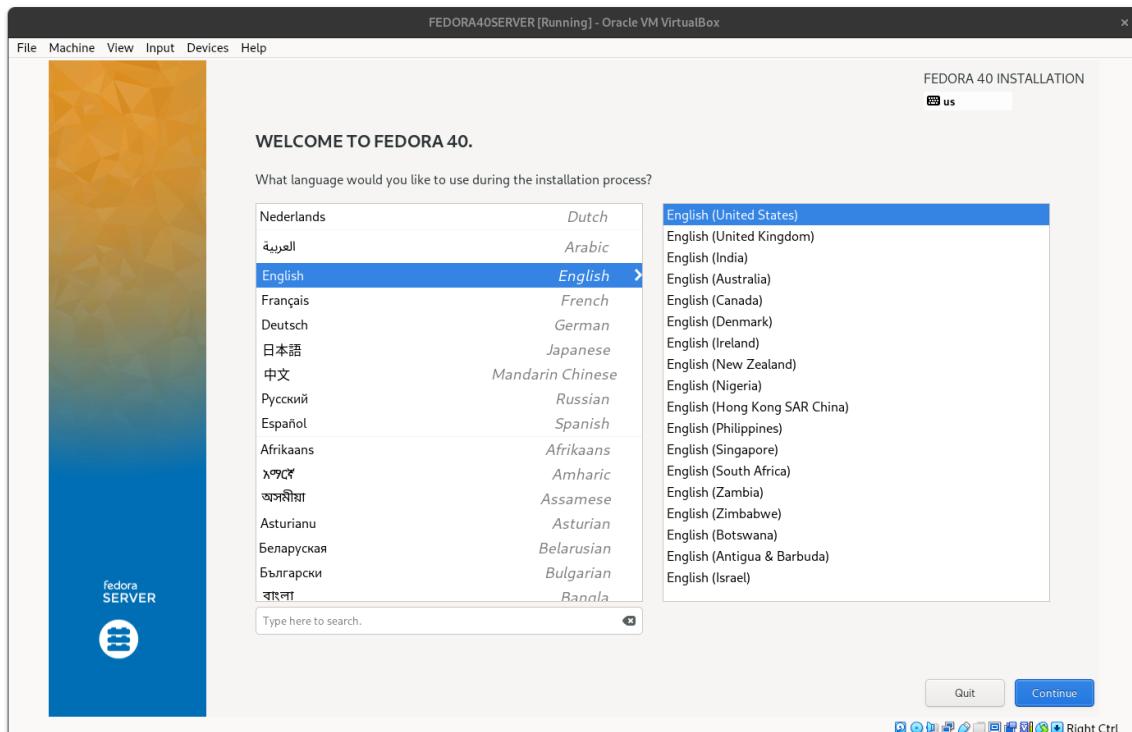


Et cliquer sur Finish ou Terminer.

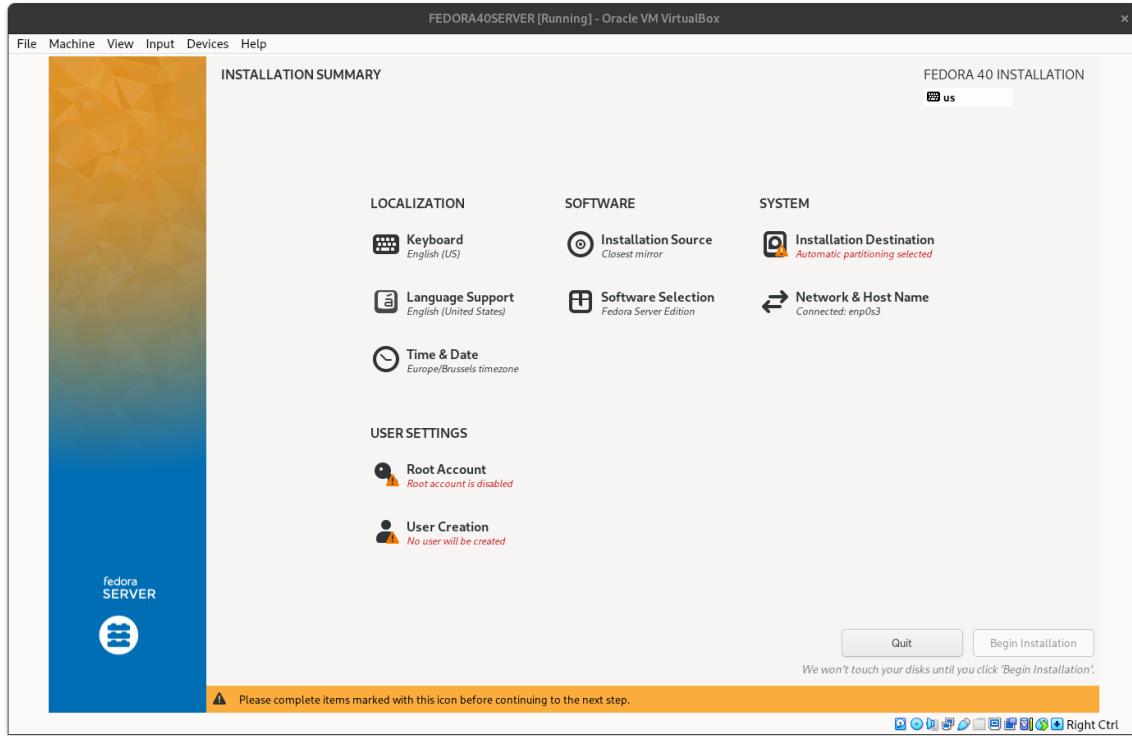
Pour lancer la machine virtuelle, il suffit de double-cliquer sur le nom de la machine, dans le côté gauche :



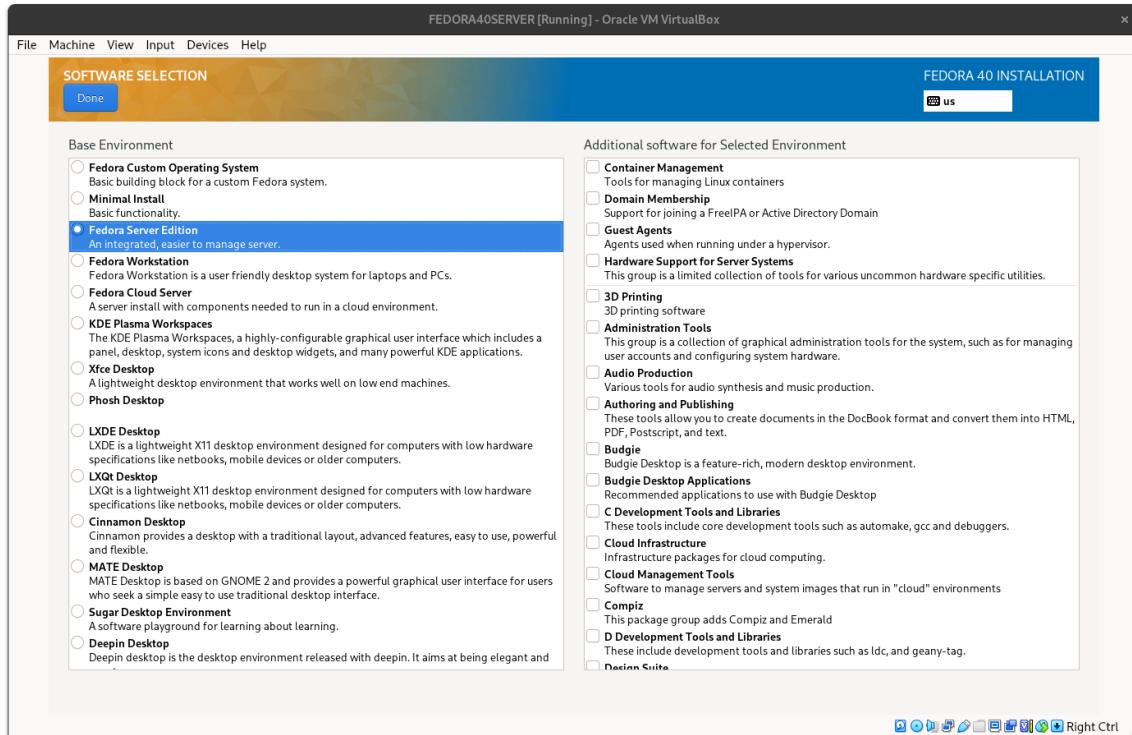
On installe en Anglais, parce que c'est la langue universelle et la seule utilisée en programmation.



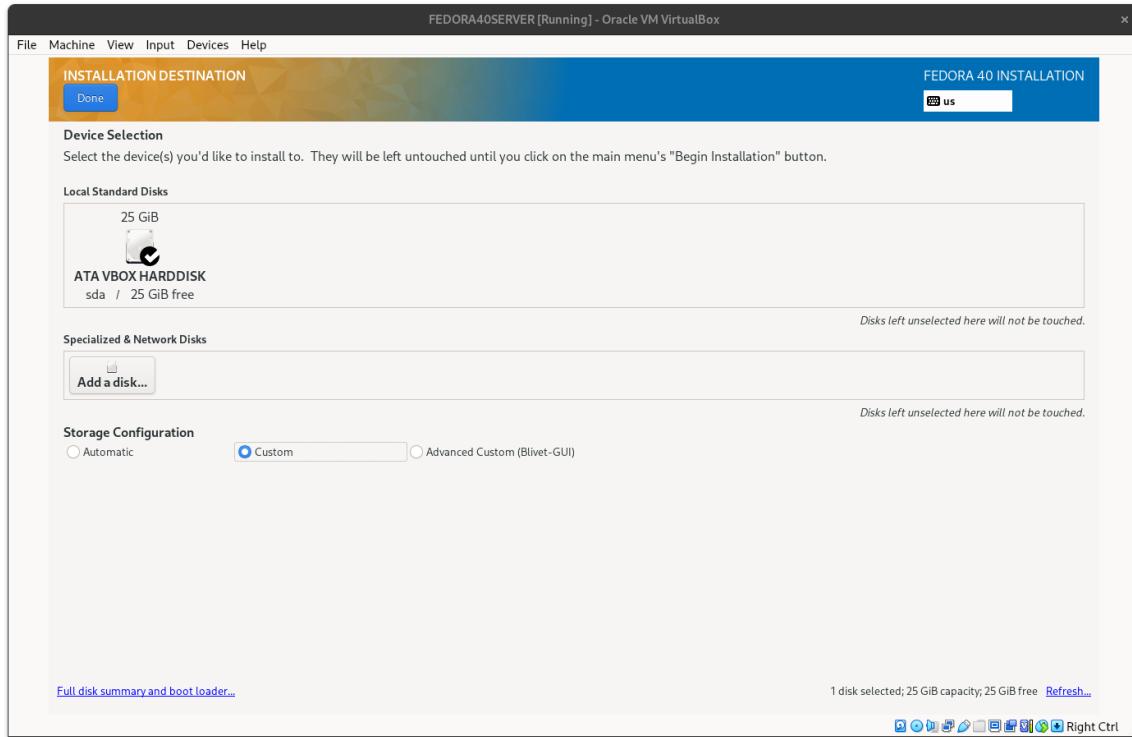
On sélectionne "Continue", et on arrive sur le menu principal d'installation :



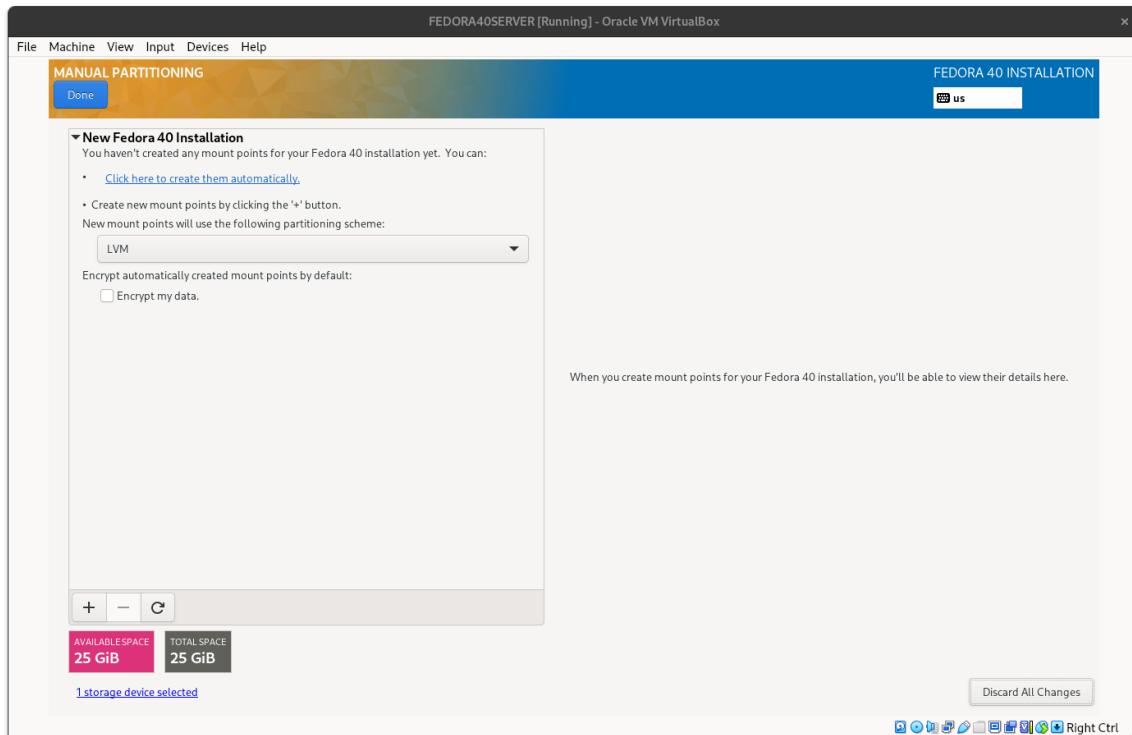
Le clavier est incorrectement configuré, les entrées étant liées à la machine hôte. La date qui dépend également de la machine hôte est correctement configurée. Nous allons aller sélectionner le software dont on a besoin. Dans notre cas, nous pouvons conserver la Server Edition.



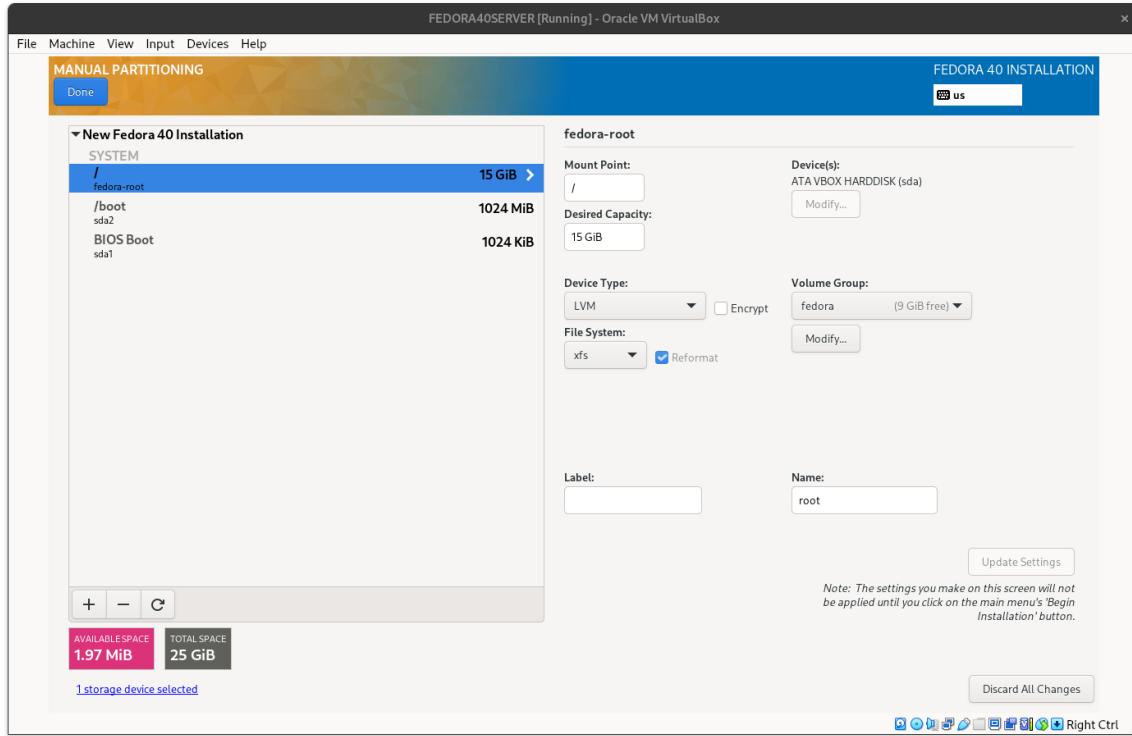
On sélectionne une installation custom :



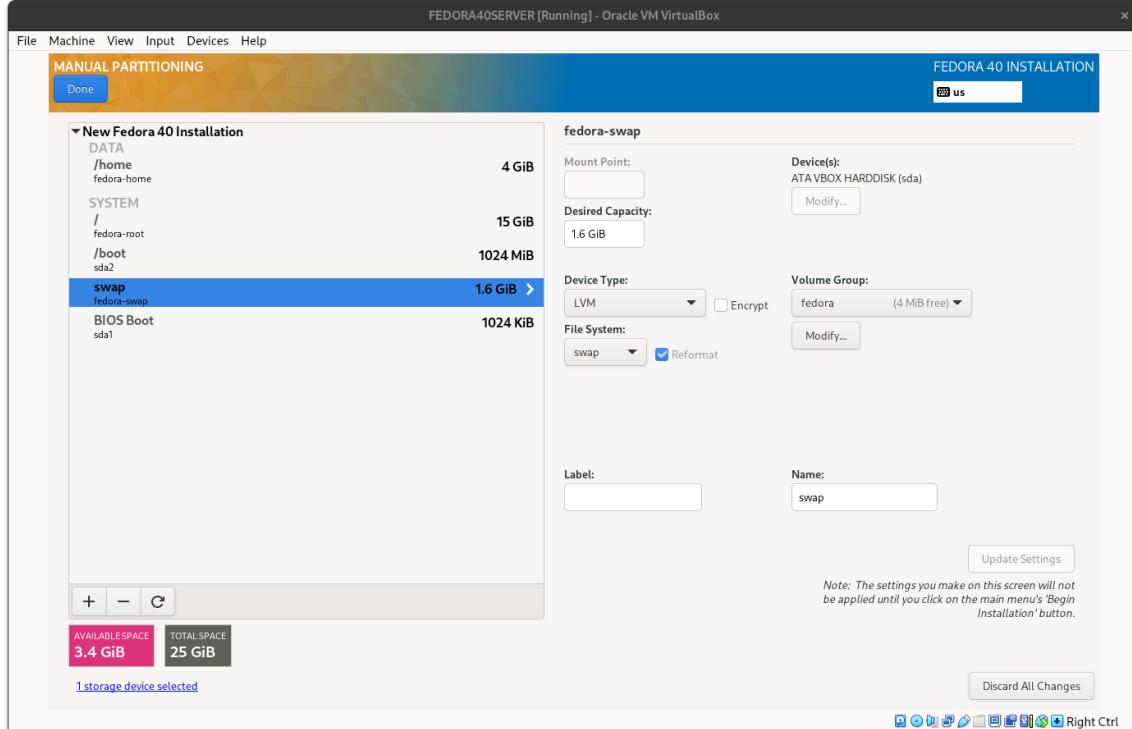
Puis on crée automatiquement les partitions de base.



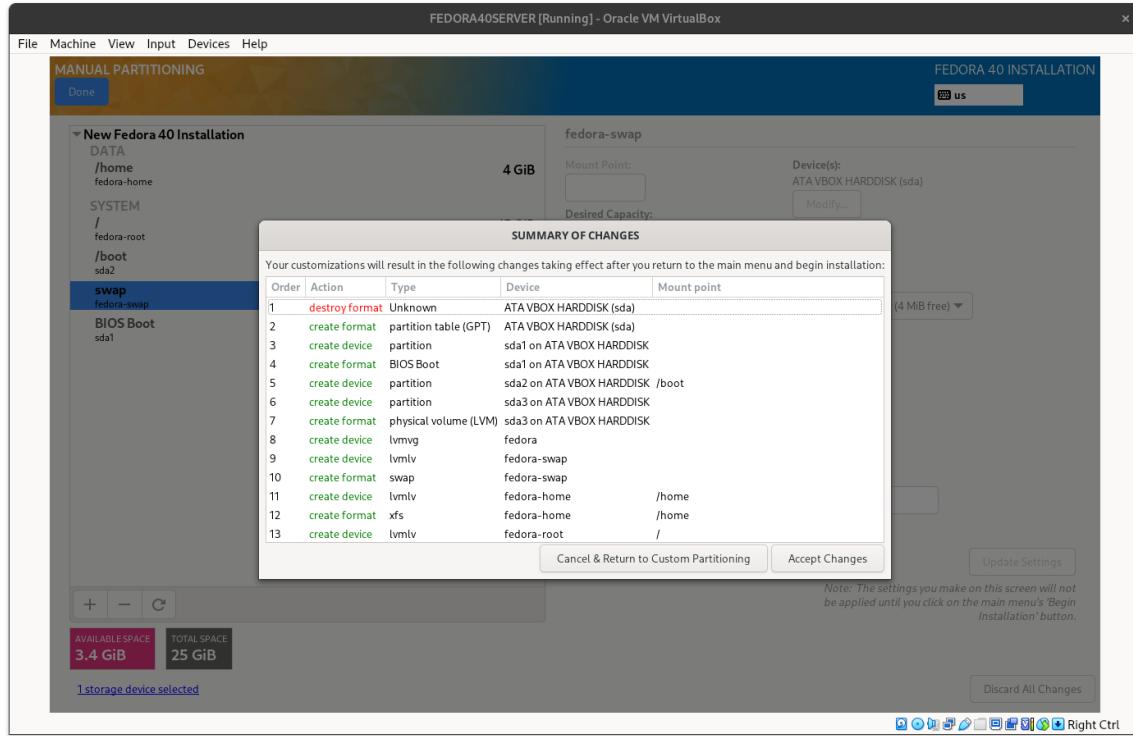
On ne touche pas à la partition automatique :



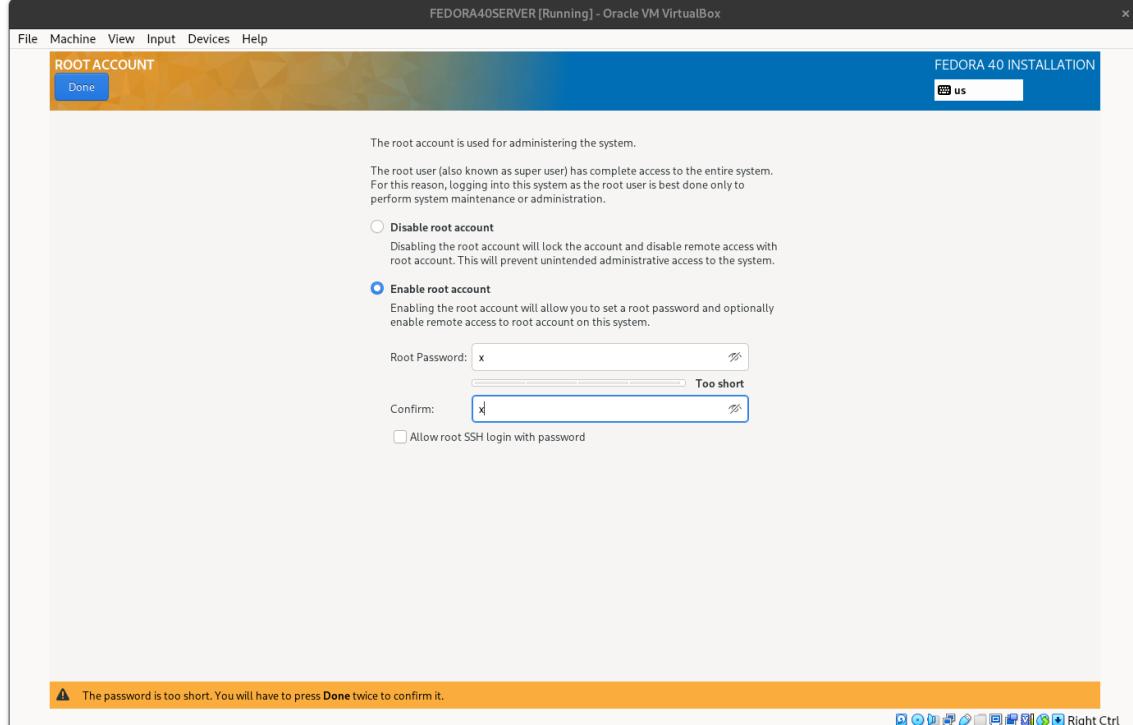
On rajoute les éléments manquants swap (20% de la RAM) et le /home puisqu'on a un utilisateur dont il faut stocker les données) :



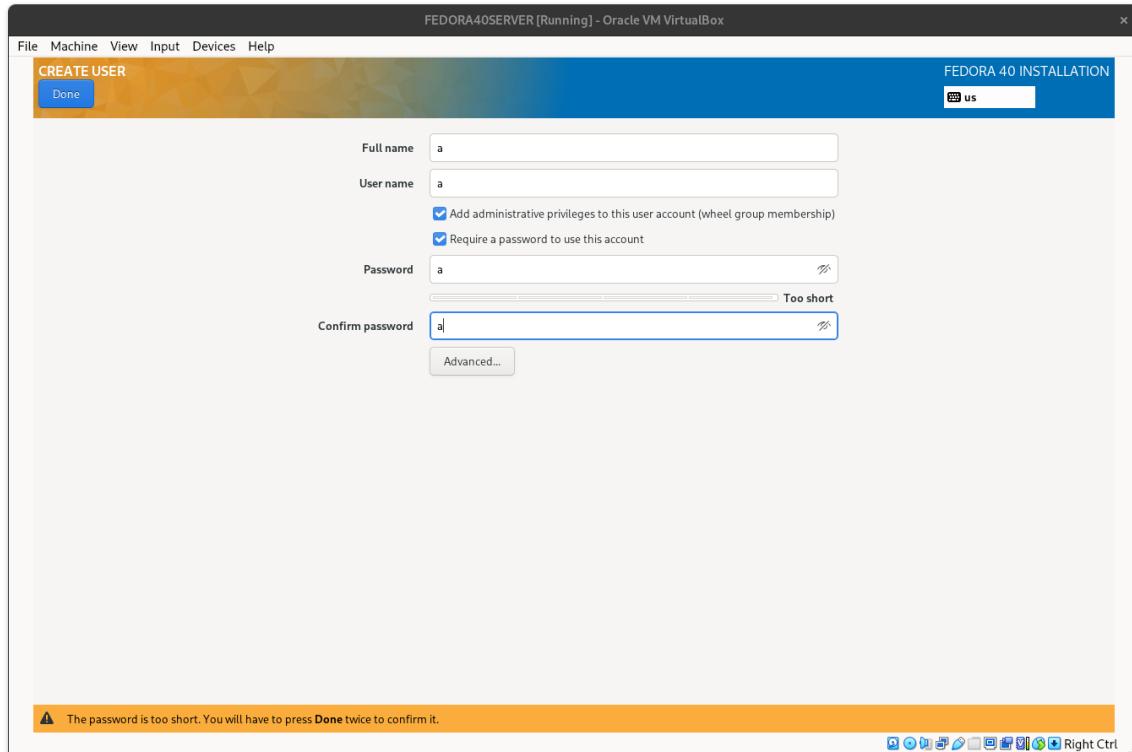
Ensuite on valide les changements :



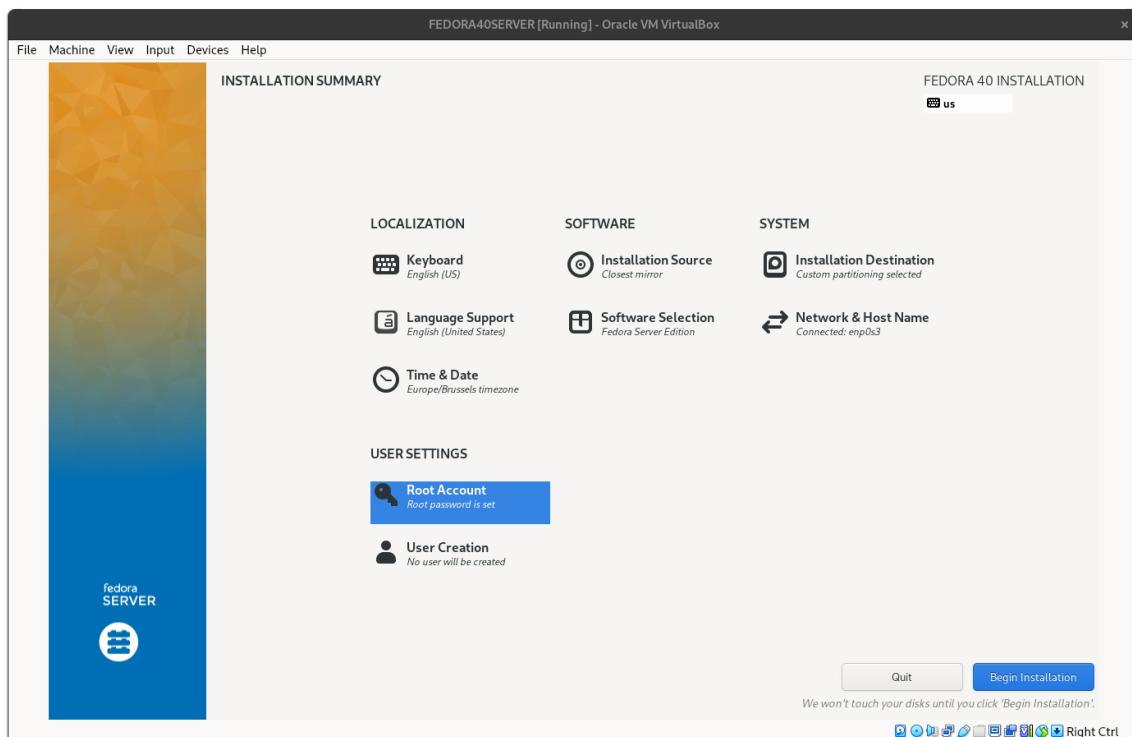
Je choisis personnellement d'avoir un compte root au cas où, mais il n'est pas conseillé en production.



Ensuite, on crée un utilisateur a (admin), avec pour l'exemple, le mot de passe a. Il est non-sécurisé mais facile et rapide à taper.



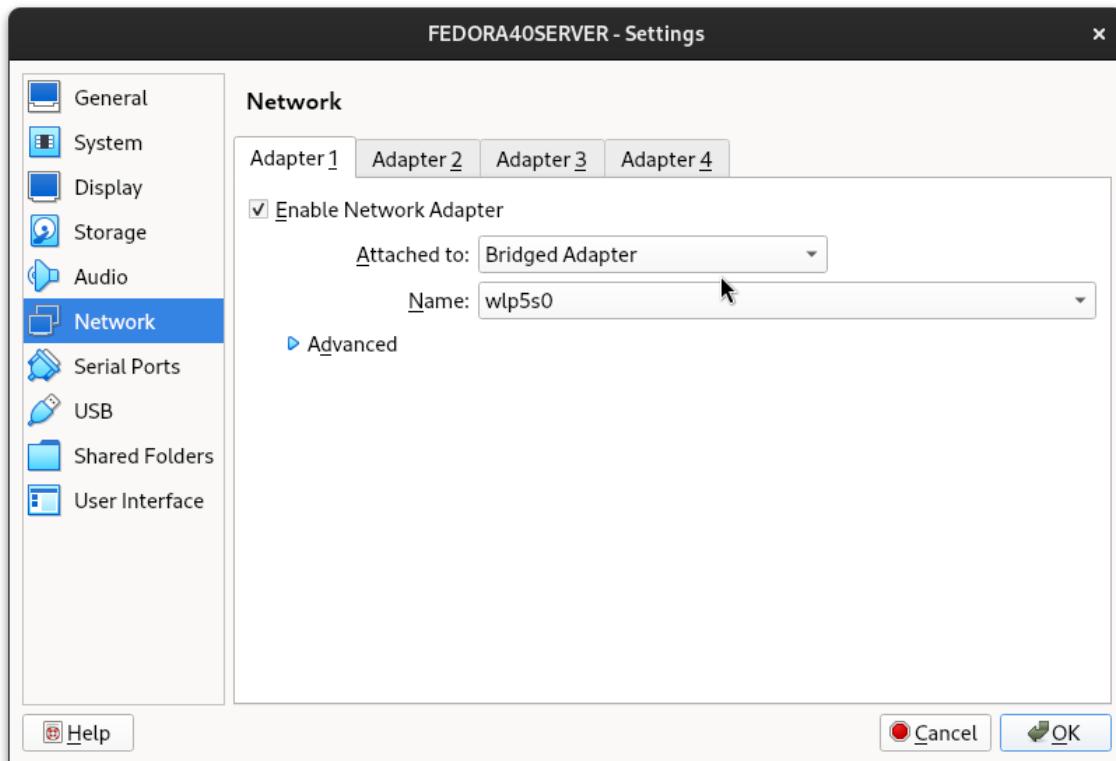
Une fois que tous les paramètres ont été réglés, il suffit de lancer l'installation, puis redémarrer la machine virtuelle (Begin Installation).



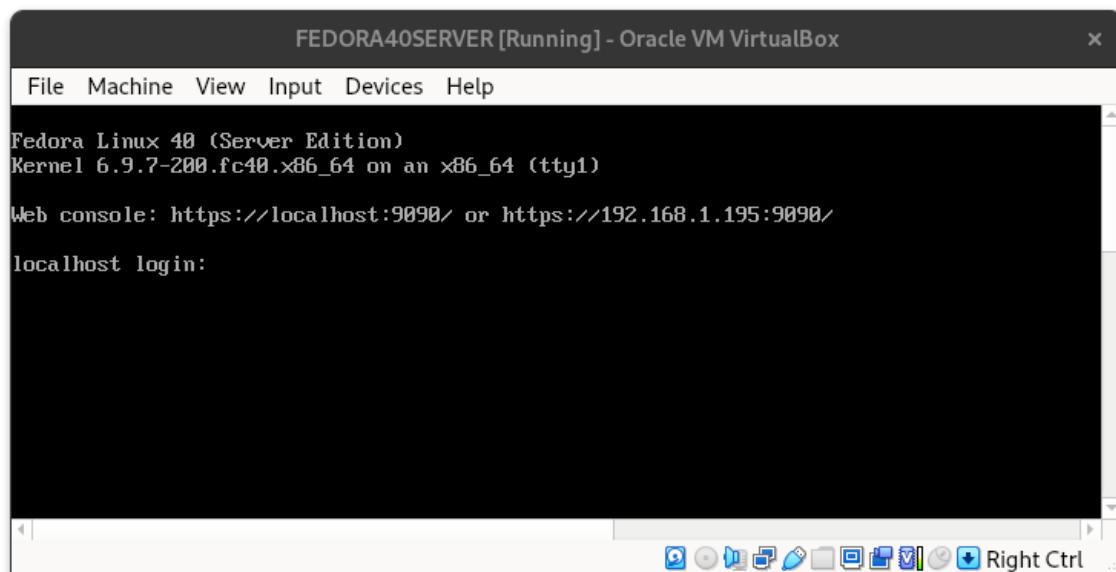
2.4 Réseau

Par défaut, le réseau virtuel sur lequel se trouve la machine est le NAT. Il est donc inaccessible depuis l'extérieur.

Il faut donc aller dans "Devices" → "Network" → "Network Settings", et changer le "Attached To" en "Bridged".



Lorsqu'on lance la machine, on peut voir que son adresse n'est pas 10.10.etc mais bien 192.168.etc, et que l'on est bien en bridge mode. (De plus, ma machine hôte n'a pas la même adresse.)

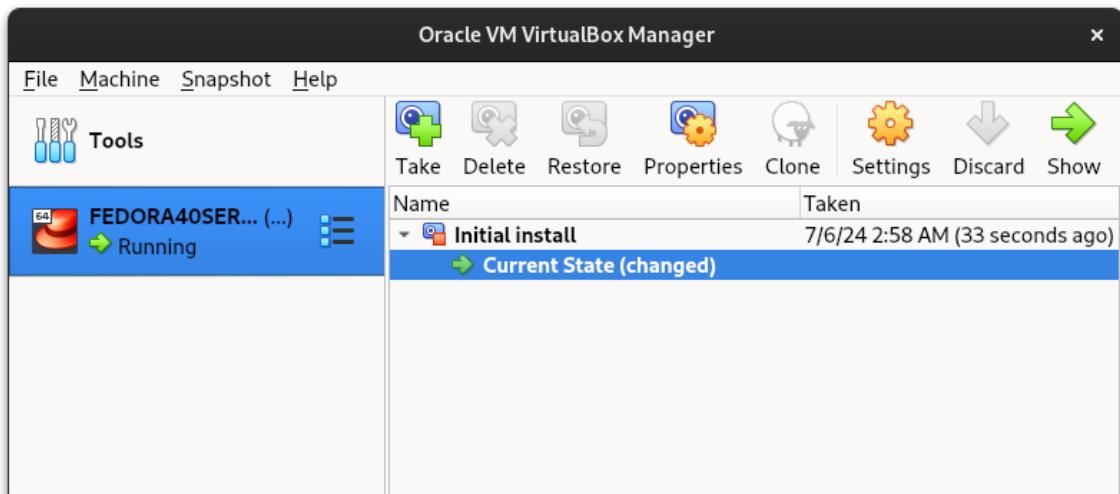


2.5 Changer le layout clavier

On utilise "localectl list-keymaps" pour avoir la liste des layouts disponibles.
Pour sélectionner un layout, par exemple, le "fr" : "localectl set-keymap fr"

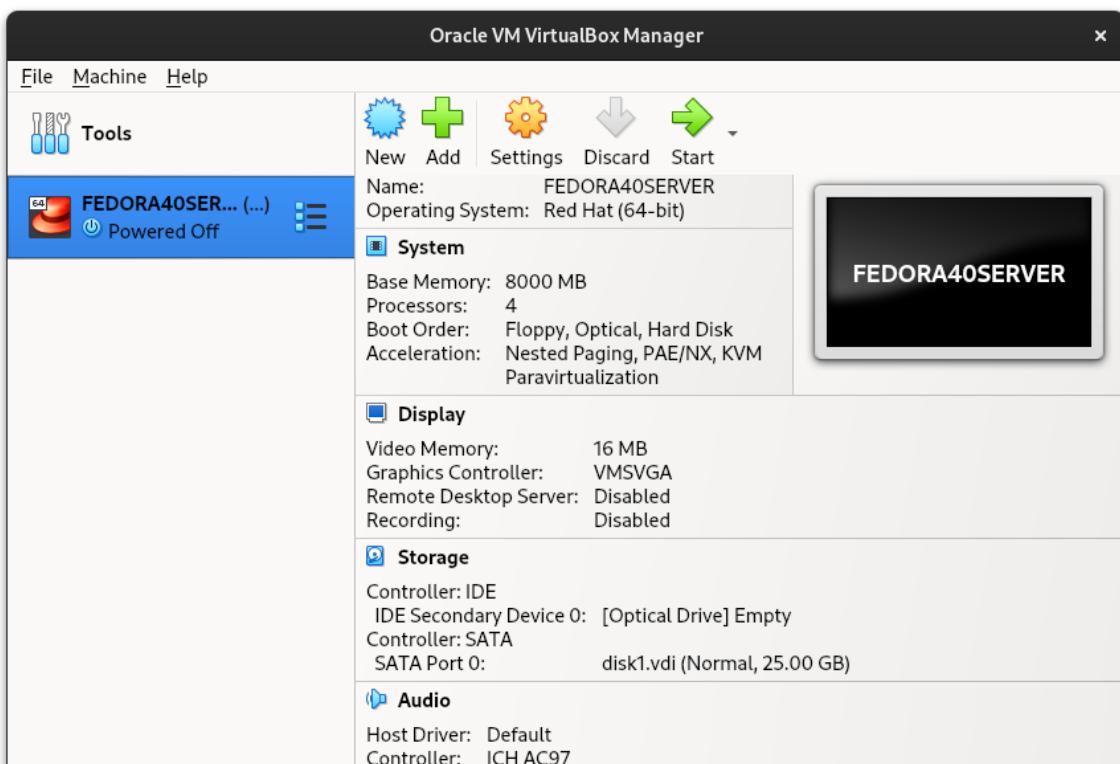
2.6 Snapshots de la machine

Pour faire une sauvegarde de l'état de la machine, il suffit de sélectionner la machine, puis de cliquer sur "Take" pour créer un snapshot.

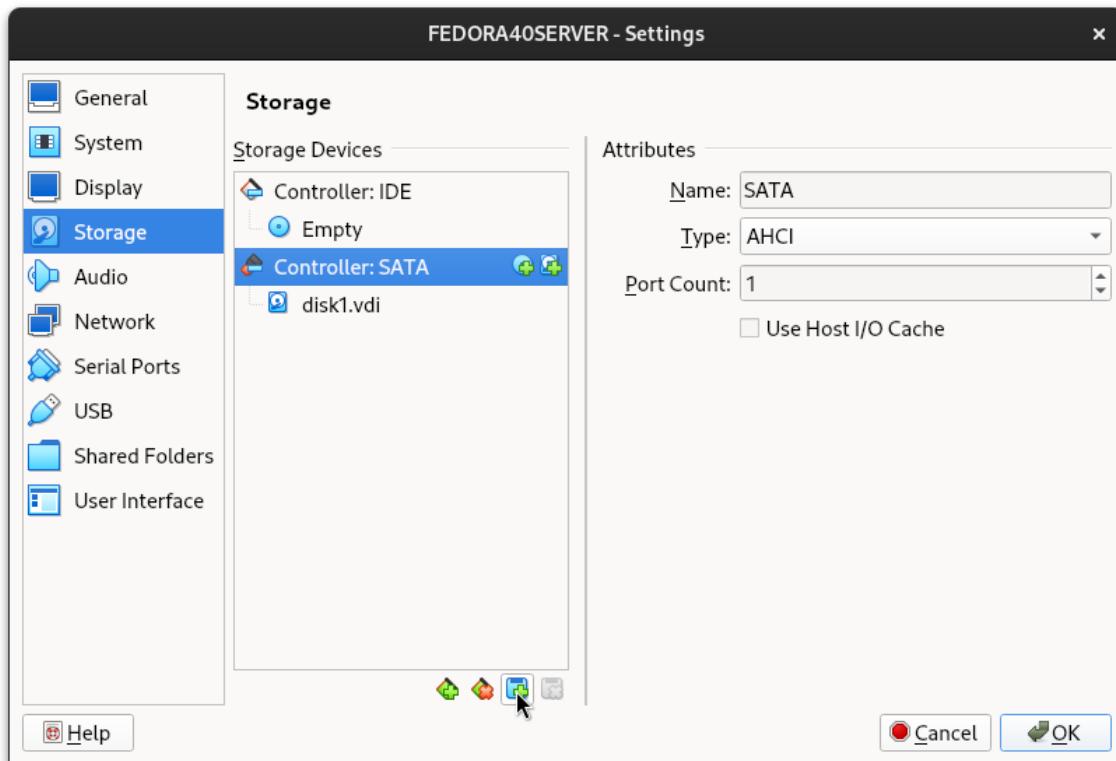


2.7 Ajout des disques virtuels

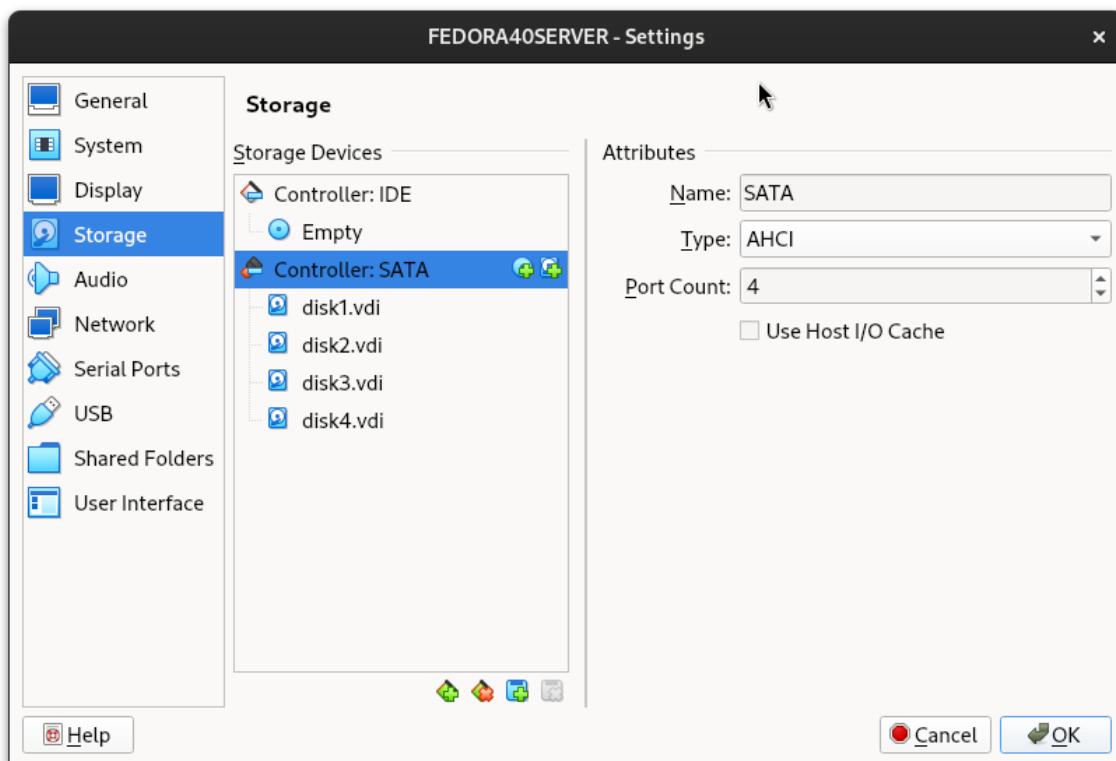
Dans les détails de la machine, on sélectionne "Storage" :



On va choisir "Add Attachment", "Hard Disk", puis sélectionner un à un les disques pré-créés.



And voilà ! (Je laisse le disque de backup en attente pour pouvoir identifier facilement les disques à mettre en RAID. Il suffit de répéter cette étape pour le disque de backup)



3 Description du logiciel

3.1 Clonage du repo git

```
git clone https://github.com/trifoil/School-LINUX-PROJECT.git
```

3.2 Menu principal

Pour lancer le script, il suffit de se rendre dans le directory School-LINUX-PROJEC, et d'exécuter le script intitulé "install.sh" en sudo.

3.3 Hostname

Cette partie du script sollicite une entrée clavier de l'utilisateur en lui proposant :

- de choisir un nouveau nom d'hôte
- d'afficher le nom d'hôte actuel

C'est un script relativement simple et totalement indépendant du reste

3.4 Configuration RAID

Comme ce n'était pas demandé, cette partie se limite à une petite démonstration. Elle pourrait être améliorée afin de démonter, remonter, effacer le stockage du serveur.

Actuellement ce script monte les trois premiers disques non-montés qui sont branchés sur la machine.

Le type de RAID utilisé est un RAID5.

Les partitions sont montées sur `/mnt/raid5_share` et `/mnt/raid5_web`

3.5 Connection SSH

Cette partie installe le service sshd et le configure pour qu'il fonctionne avec une clé privée/publique.

Puisque j'utilise Fedora Cockpit, je ne passe pas par le ssh mais le service est disponible.

3.6 Partage NFS/SAMBA sans authentification

Un partage peut être créé dans le directory `/mnt/raid5_share` Ce partage est sans authentification.

Comment l'utiliser?

Pour le partage samba, on y accède simplement par l'explorateur de fichiers, par exemple si l'adresse est 192.168.1.102, on aura: `smb://192.168.1.102`

Pour le partage NFS, il suffit de monter le volume sur la machine cliente :

```
mkdir /mnt/nfs
sudo mount -t nfs 192.168.1.102:/mnt/raid5_share /mnt/nfs
sudo umount /mnt/nfs
```

Une limite douce de 500Mo est ajoutée, ainsi qu'une limite dure de 600Mo (pour l'utilisateur nobody).

3.7 Services Web

Les services web sont une collection d'un tas de services différents listés ci-après.

Deux options sont disponibles, installation initiale et ajout d'utilisateur.

3.7.1 Installation initiale

Au niveau de l'installation générale, on retrouve déjà la plupart des services.

- DNS

Le script sauvegarde le fichier de configuration initial, puis le modifie selon les paramètres prédefinis, le nom de domaine et adresse IP fournis par l'administrateur.

Ensuite deux zones sont créées dans le DNS :

- Forward
- Reverse

Et puis quelques autres choses sont configurées comme par exemple l'IPv4 seulement, ou encore le hostname.

- httpd

La page web de base est une simple page qui redirige vers l'adresse de la base de données.

- ssl

Un certificat auto-signé ssl est configuré lors du setup.

3.7.2 Ajout d'utilisateurs

- Dossier utilisateur web

Le dossier est partagé par Samba et FTP.

Pour le partage samba, on y accède simplement par l'explorateur de fichiers, par exemple si le username est joe, on aura: `smb://192.168.1.102/joe/`

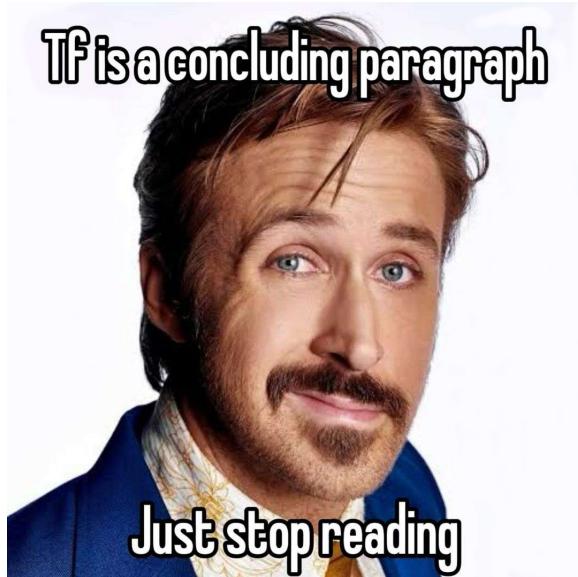
3.8 Serveur temps

3.9 Clamav et Fail2ban

3.10 Backup

3.11 Logs d'installation

4 Conclusion



References

- [1] Author, A. (Year). Title of the article. *Journal Name*, Volume(Issue), Pages.
- [2] Raid sous Oracle VirtualBox <https://youtu.be/ZHVmGfteHCg>
- [3] Configuration de Fedora Server 40 <https://www.server-world.info>

Remerciements

Remerciements à Pauline M. pour ses encouragements et son aide à la concentration :)