# Projet Linux

VANGEEBERGEN Augustin

July 21, 2024


# Table des matières

# 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 distributon 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).

Dans la deuxième itération de ce projet linux, la barre est automatiquement mise plus haut.

Les consignes professeur sont toujours les mêmes, et sont reprises dans le sous-point suivant. Cependant, je souhaite faire tourner un serveur php pour mon homelab (et ainsi faire d'une pierre deux coups). L'option est donc présente en supplément.

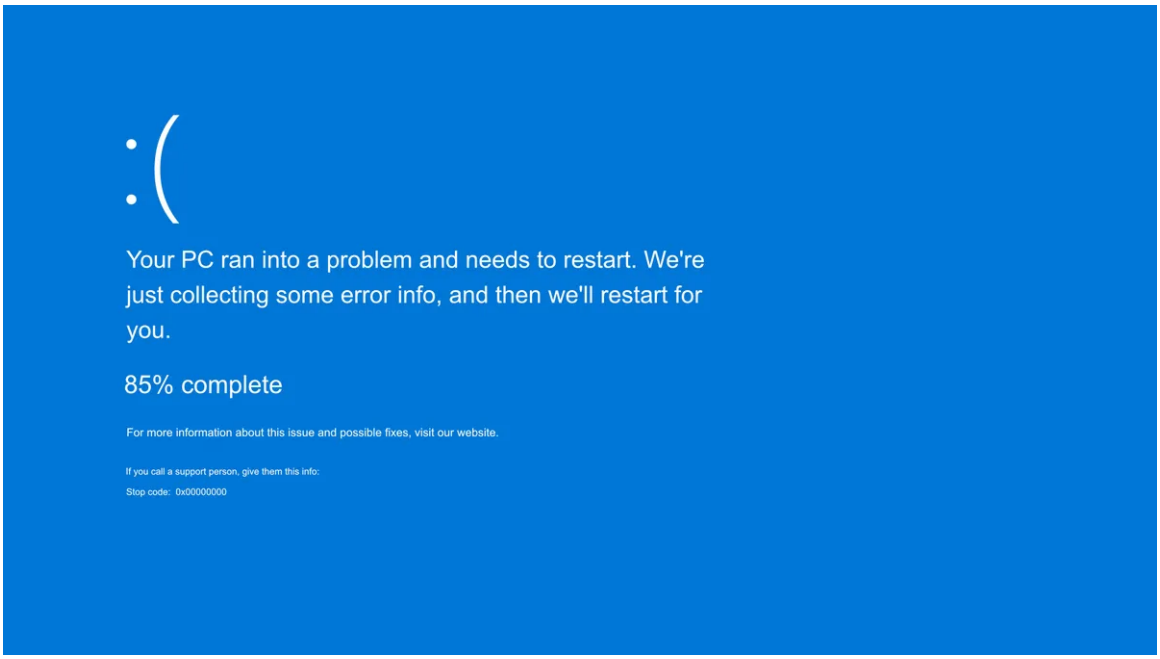
L'OS de test est une machine virtuelle, hébergée sur VirtualBox.

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.

Nous devons 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 polices d'utilisation correctes.

linux meme (19 juillet 2024) :



## 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 maitre 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
- SSH config wizard
- File sharing install wizard
- Web server install wizard
- FTP server install wizard
- MySQL server
- DNS server (+ cache + création de zone + serveur cache)
- Time server
- Sécurisation
- Backup
- Updates
- Partitionnement

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 (principalements 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).

  Perfermances 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 a 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.

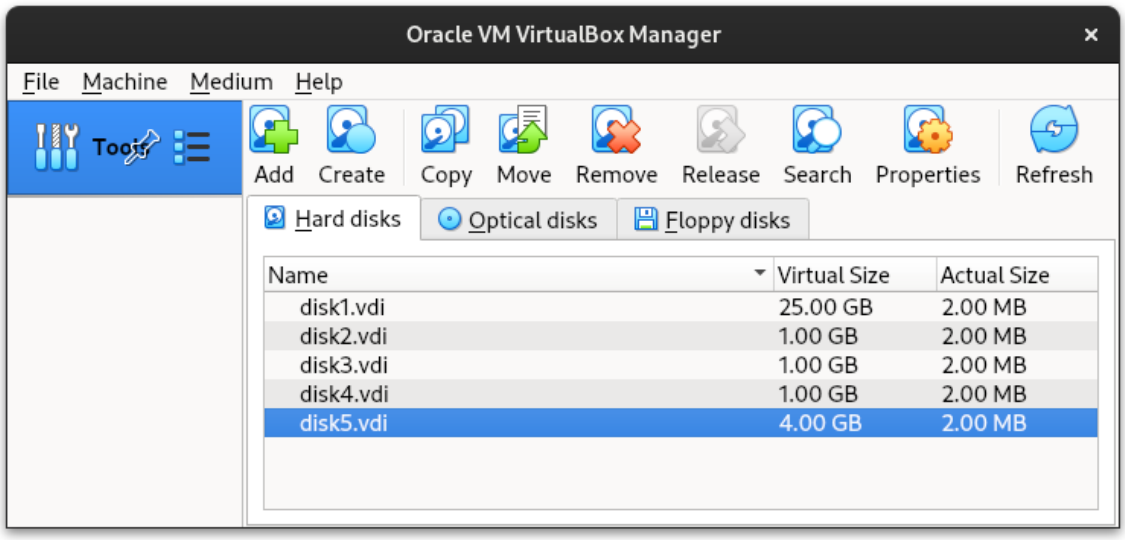
  Si un disque lâche, il suffit de remplacer celui-ci, et il peut être reconstitué à partir des autres diques et de la parité stockée sur ceux-ci.

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 vituels :

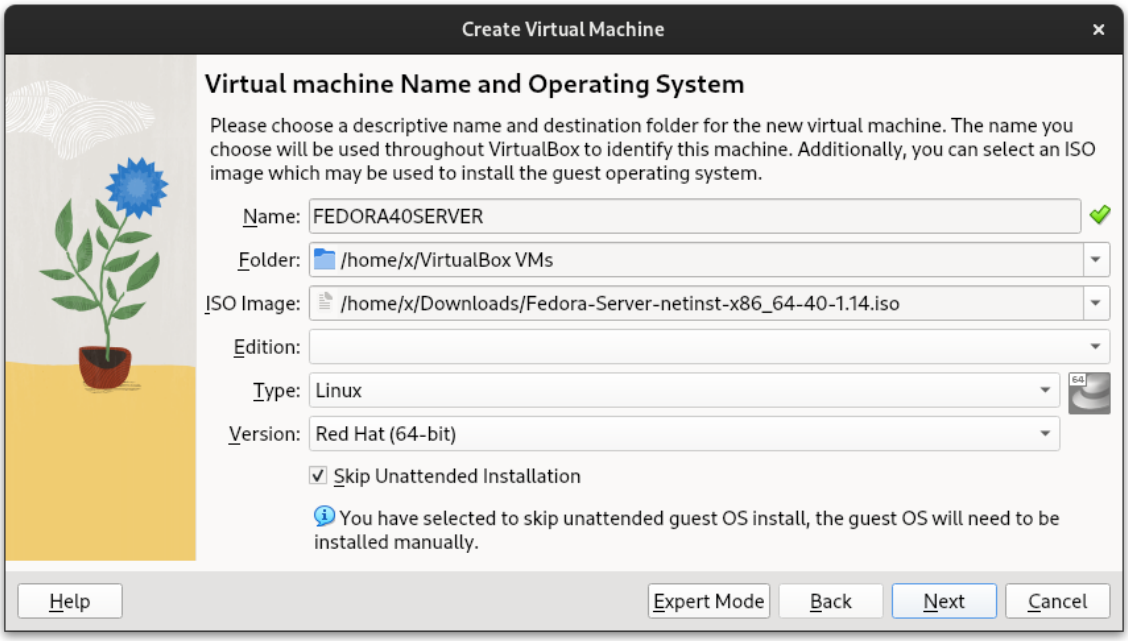
- 1 disque pour l'OS et les fichiers de configuration (disk1)
- 3 disques (c'est à dire le minimum requis pour un RAID 5) pour le stockage (disk2-3-4)
- 1 disque pour la sauvegarde (disk5)

## 2.3 VirtualBox

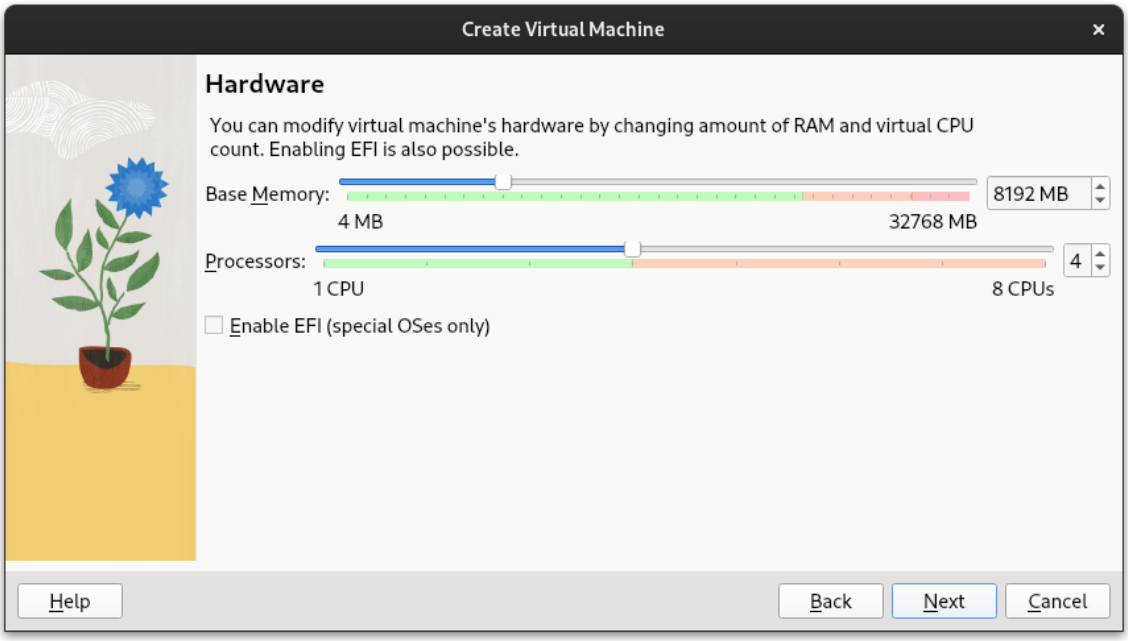
Comme dit précédemment, voici les différents diques virtuels créés et leur taille, dans l'interface de VirtualBox :



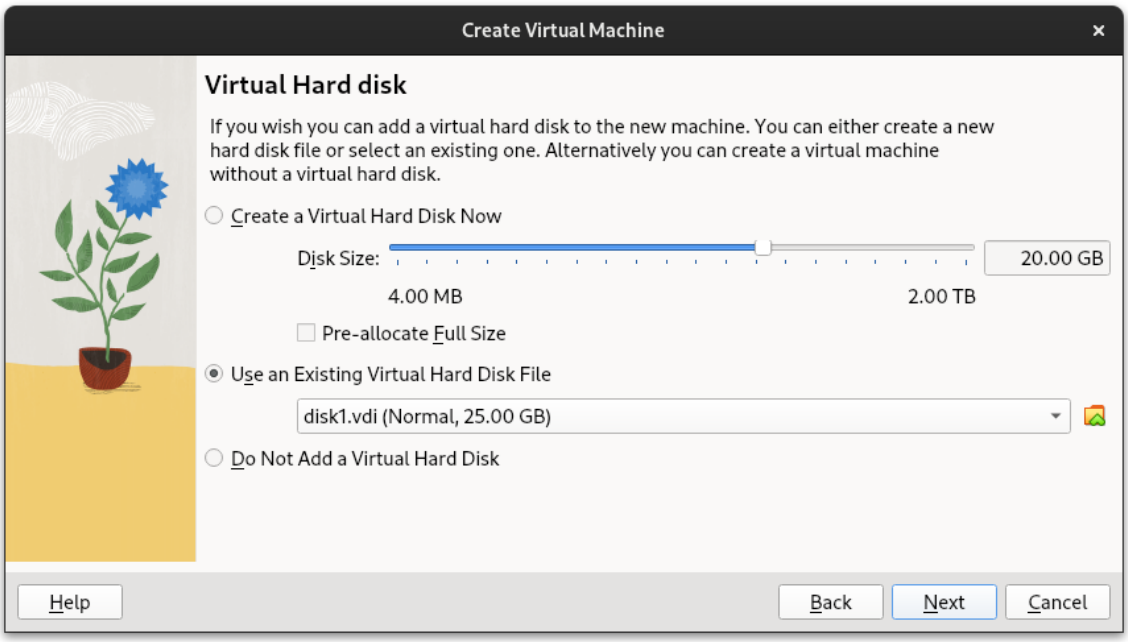

Ensuite, il faut créer la machine virtuelle, en prenant soin de selectionner le bon ISO :



On sélectionne la quantité de ram optimale pour le système :

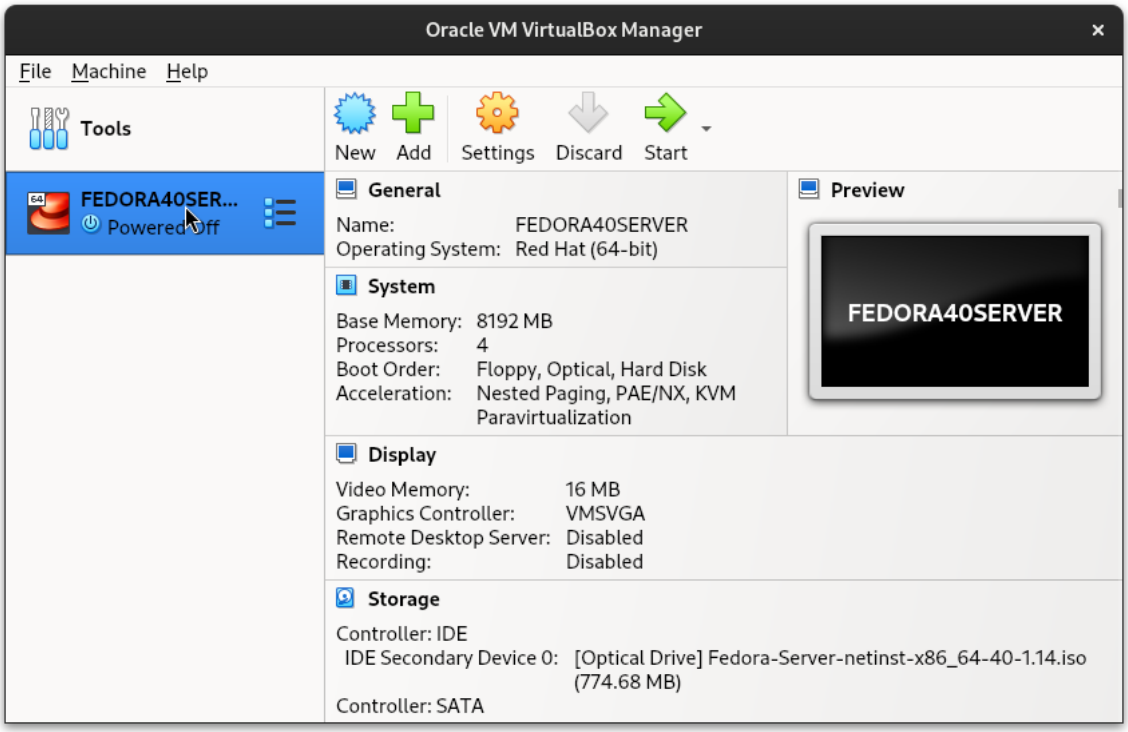



Et on selectionne le disque virtuel créé précedemment :

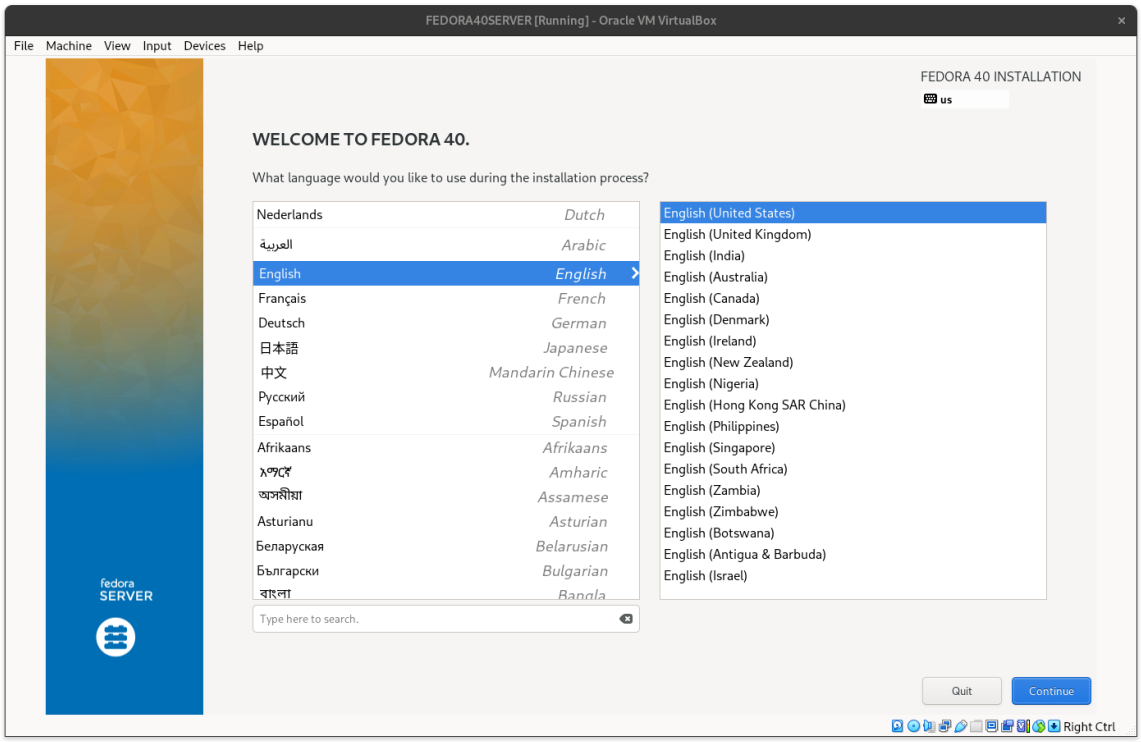



Et cliquer sur Finish ou Terminer.

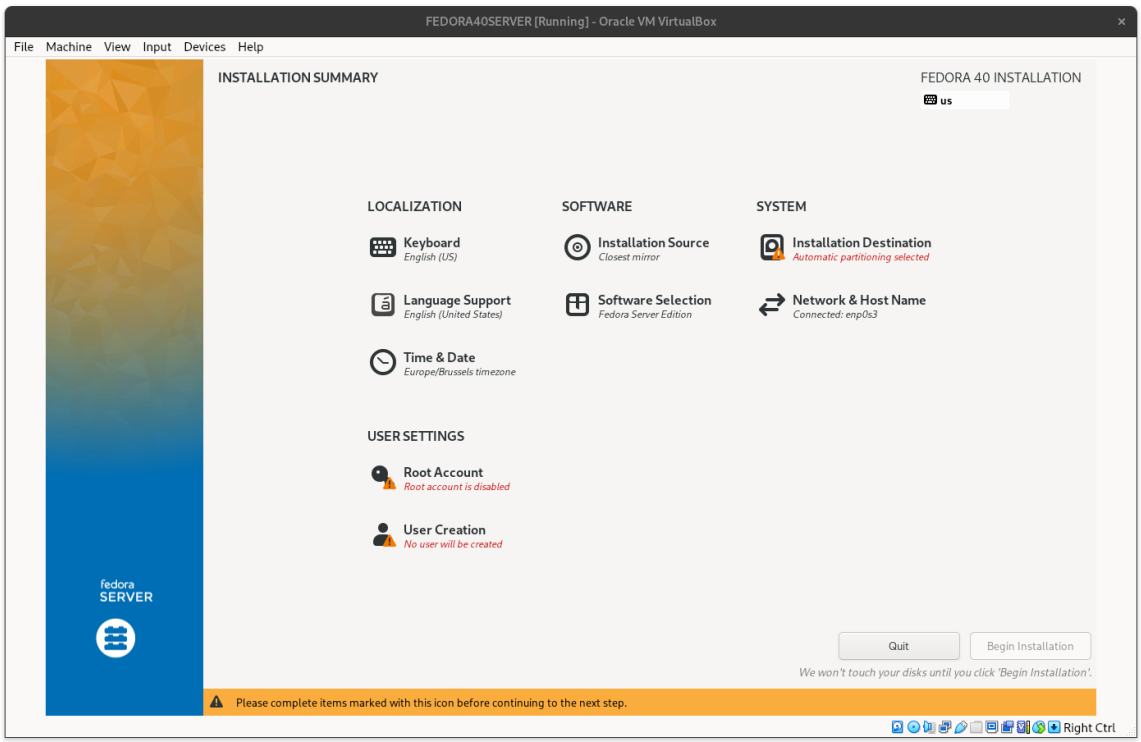
Pour lancer la machine virtuelle, il suffit de double-cliquer sur le nom de la machine, dans le côté gauche :



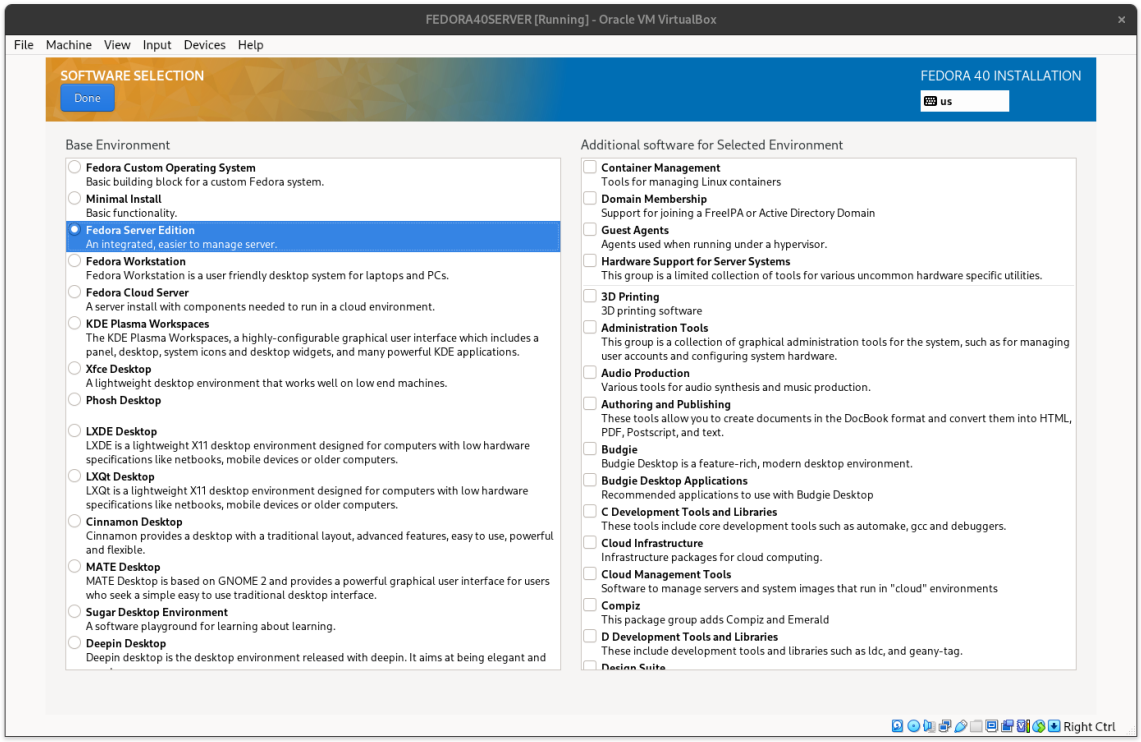

On installe en Anglais, parce que c'est la langue universelle et la seule utilisée en programmation.



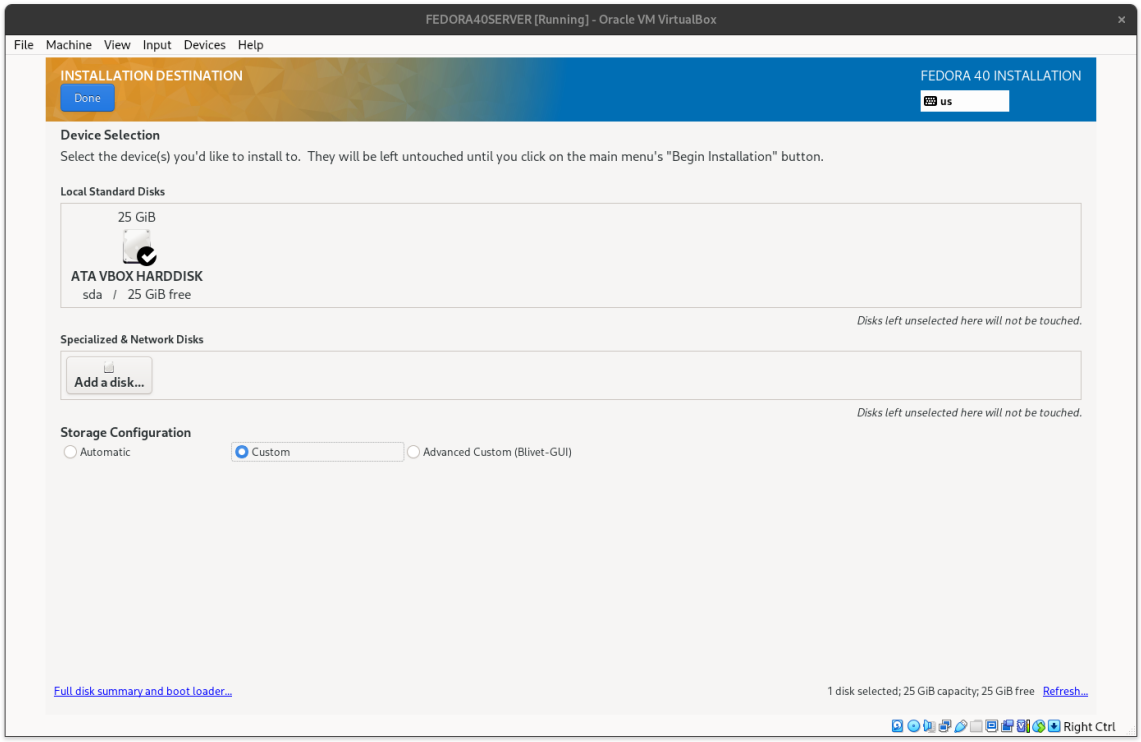
On sélectionne "Continue", et on arrive sur le menu principal d'installation :



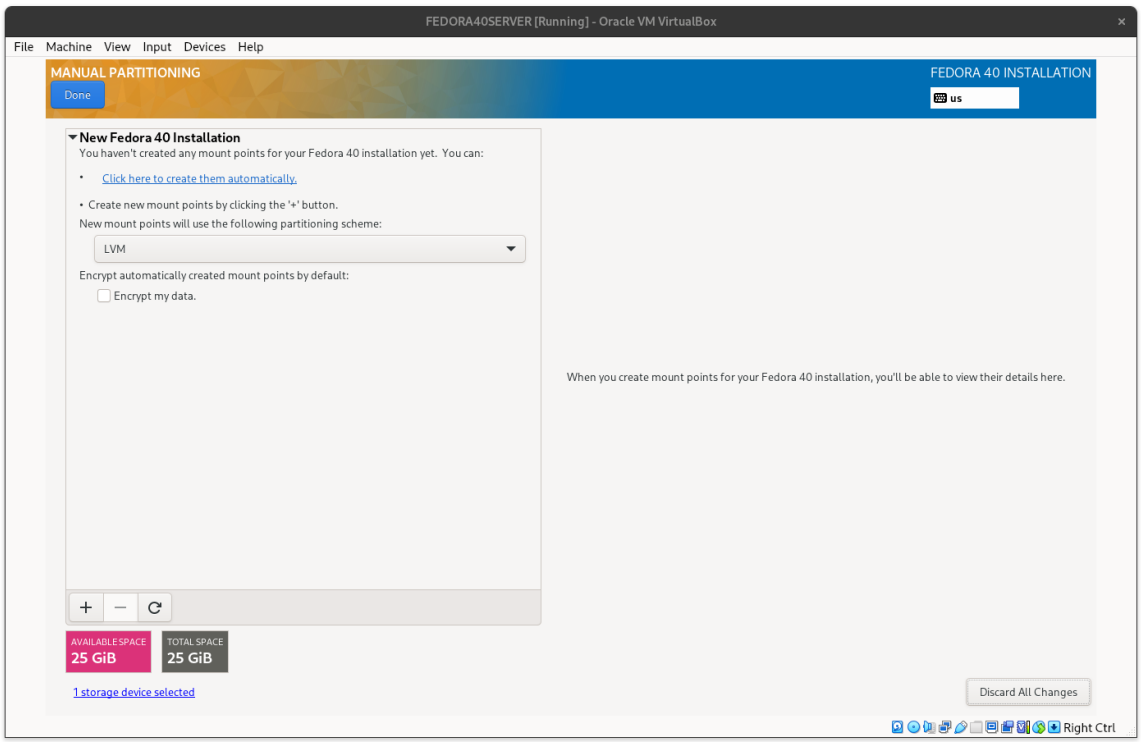

Le clavier est correctement configuré, puisque c'est une machine virtuelle. La langue est également correctement configurée, ainsi que la date qui dépend de ma machine hôte. Nous allons aller sélectionner le software dont on a besoin. Dans notre cas, nous pouvons conserver la Server Edition.



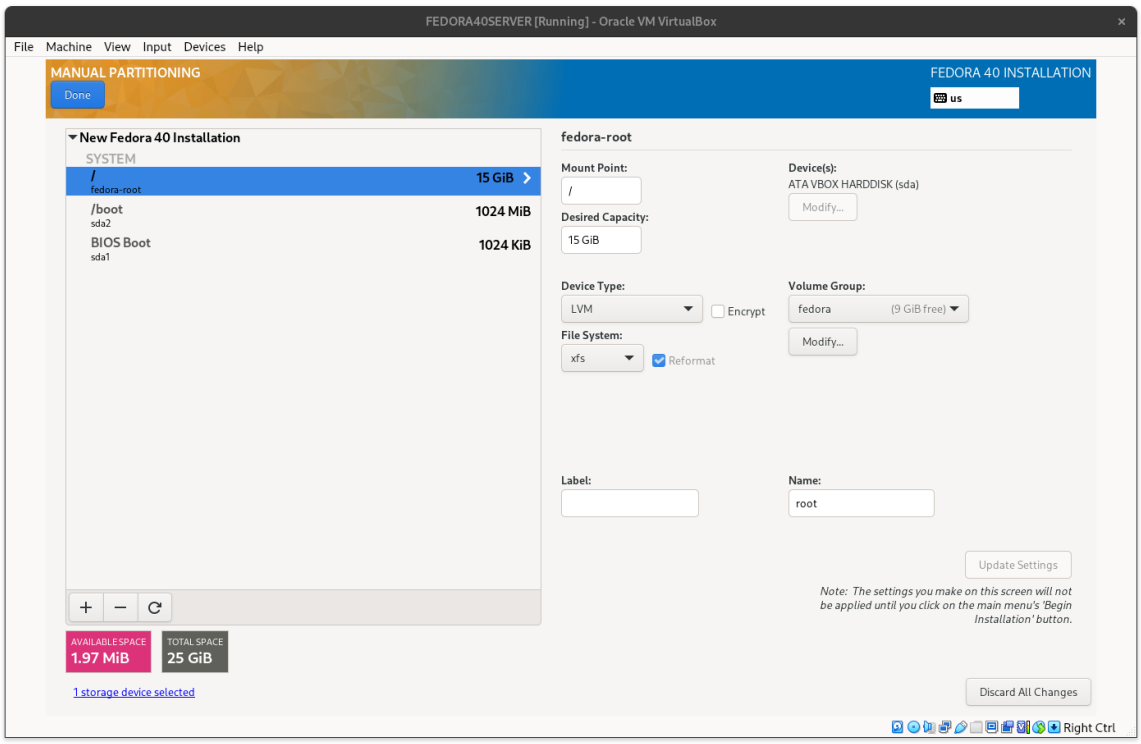
On sélectionne une installation custom :



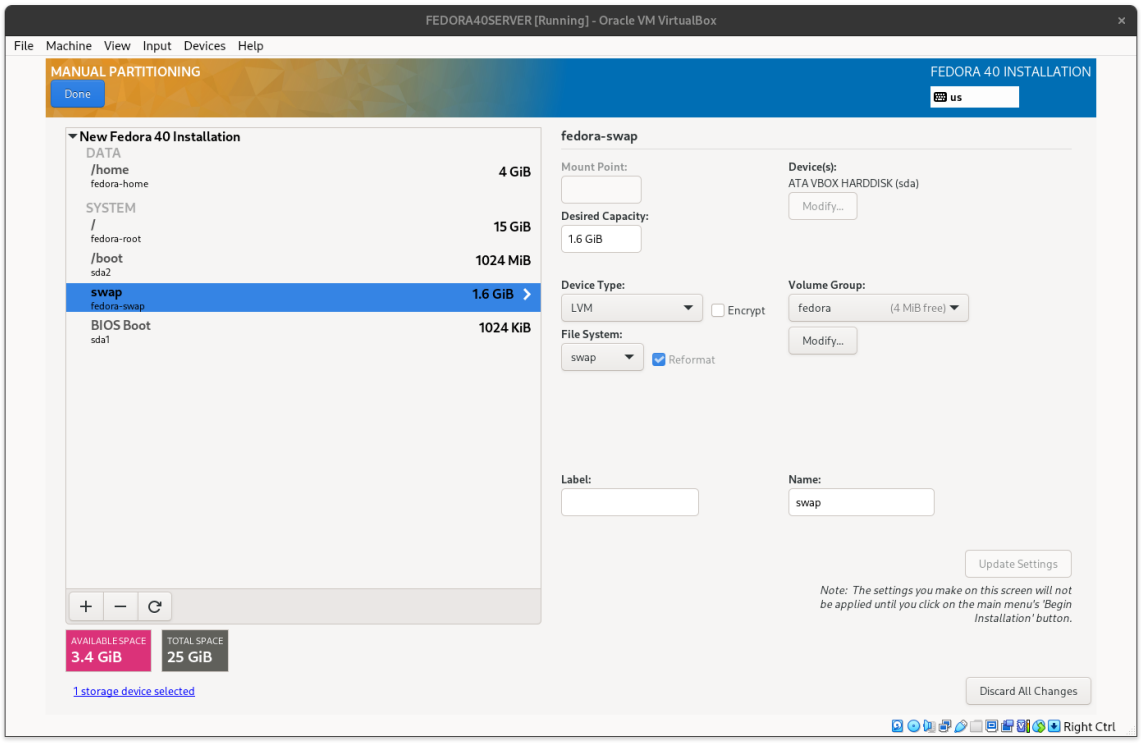

Puis on crée automatiquement les partitions de base.



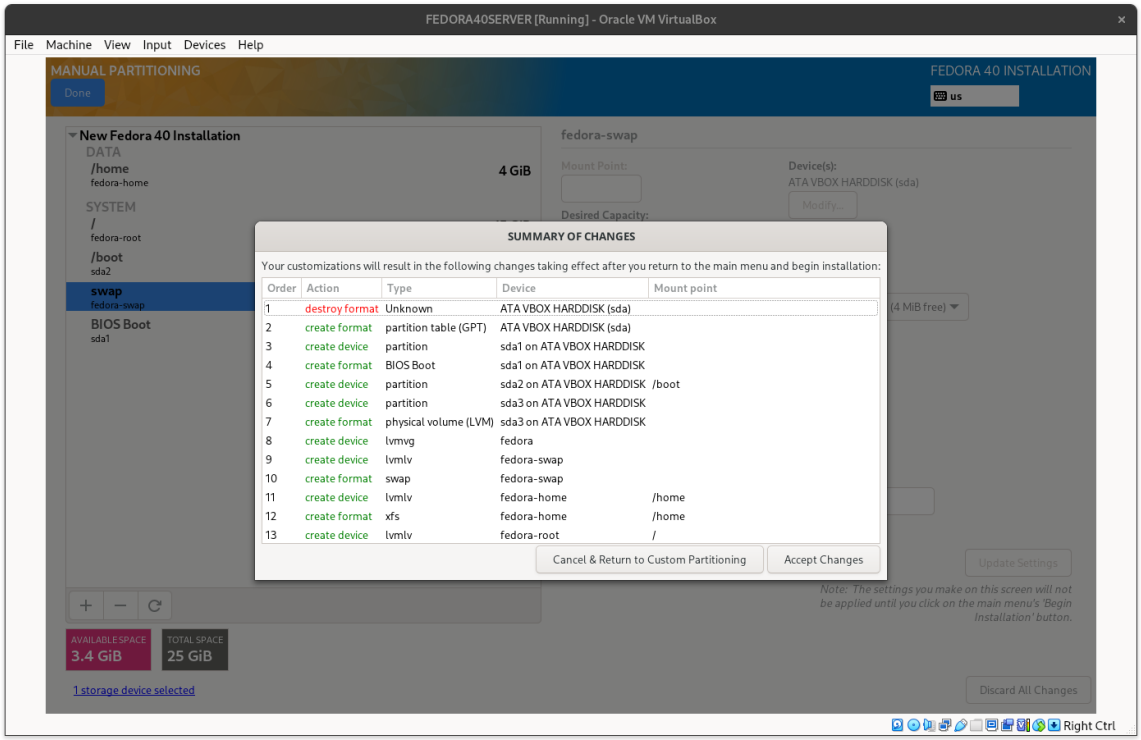
On ne touche pas à la partion automatique :



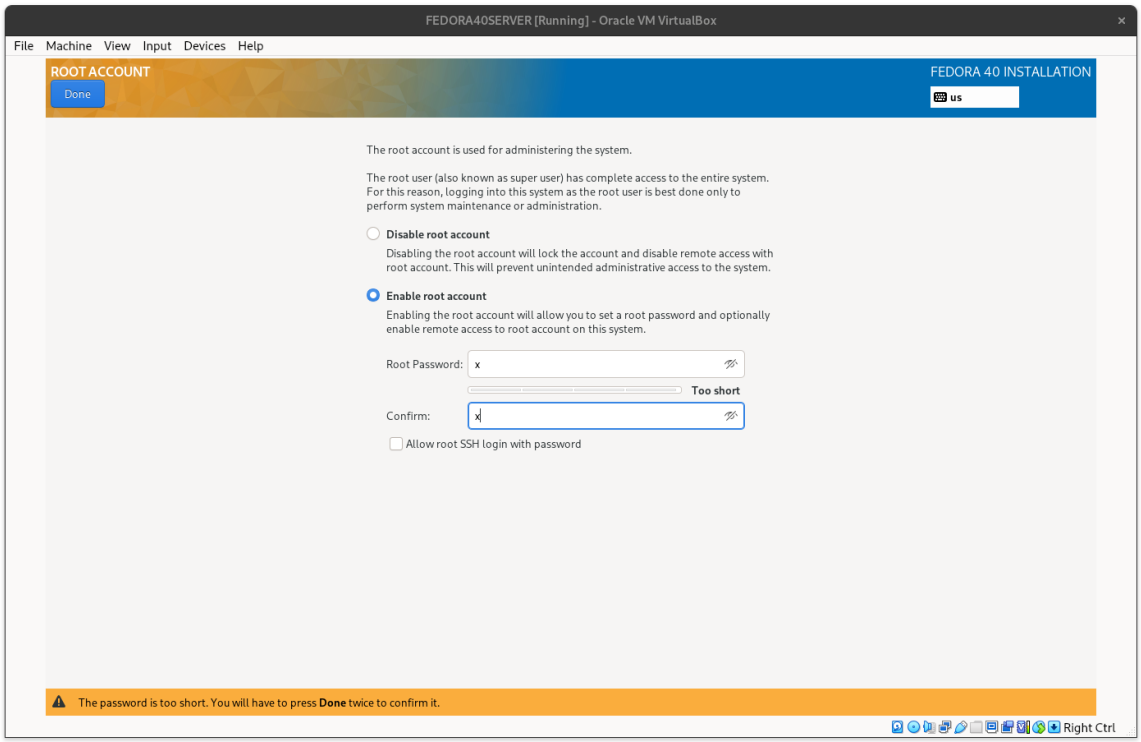

On rajoute les éléments manquants swap (20% de la RAM) et le /home puisqu'on a un utilisateur dont il faut stocker les données) :



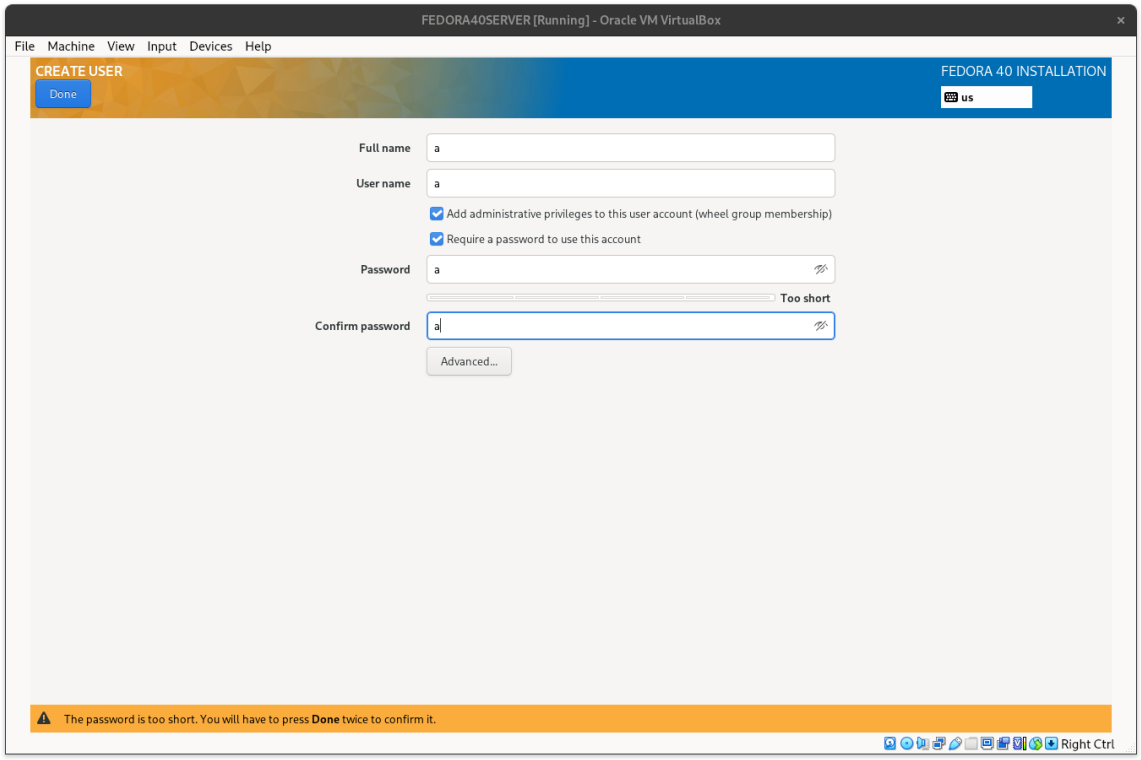
Ensuite on valide les changements :



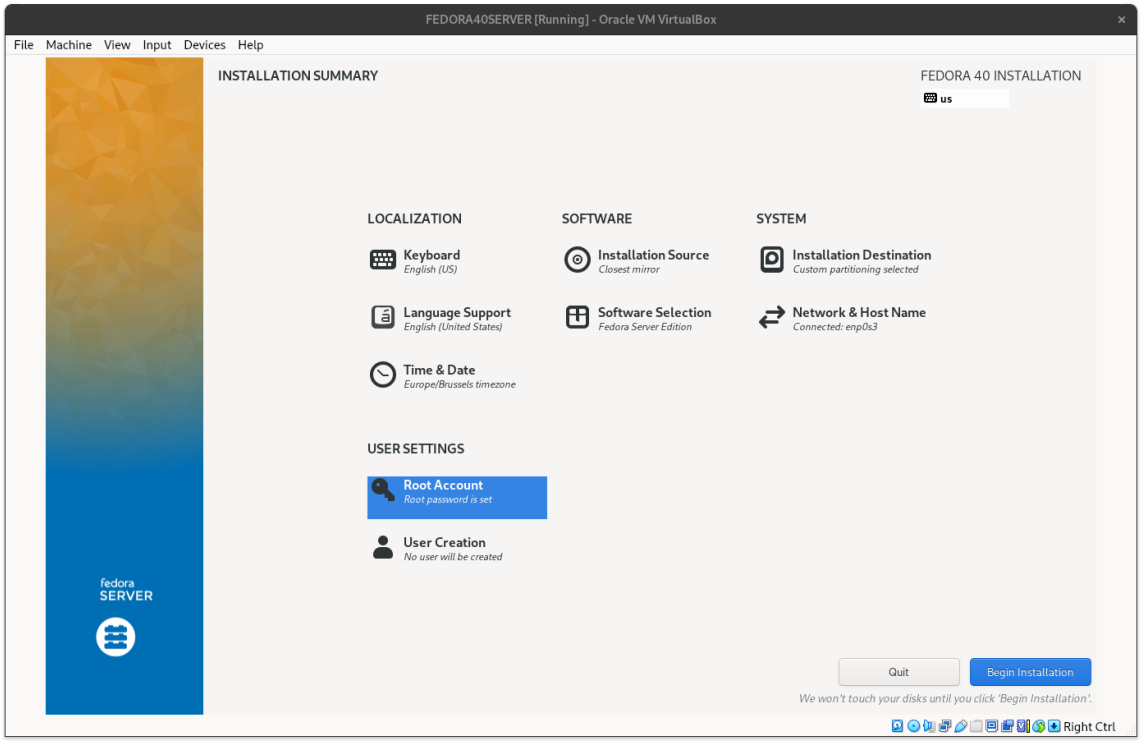

Je choisis personnellement d'avoir un compte root au cas où, mais il n'est pas conseillé en production.



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.



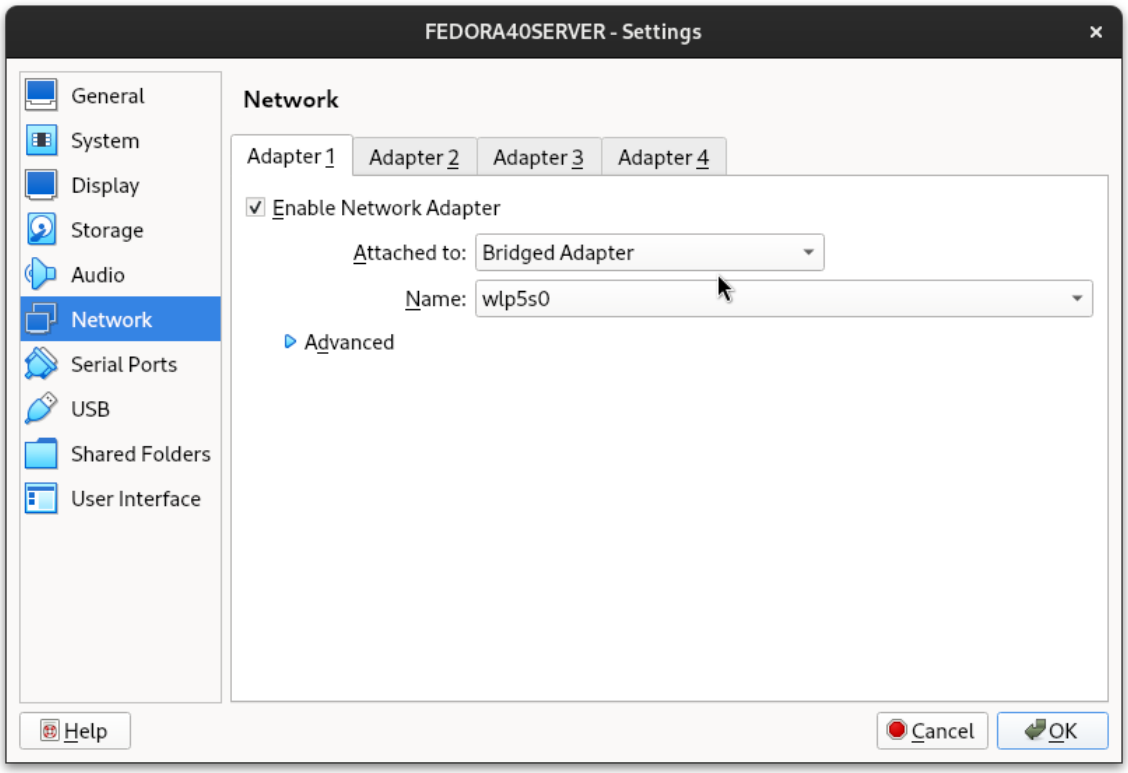

Une fois que tous les paramètres ont été réglés, il suffit de lancer l'installation, puis redémarrer la machine virtuelle (Begin Installation).



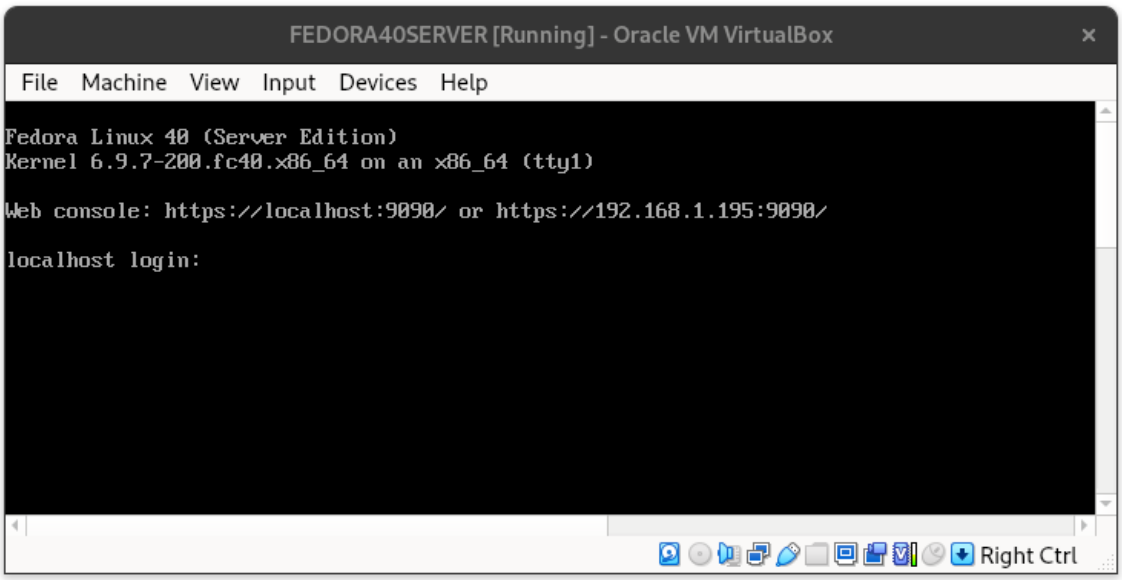
## 2.4 Réseau

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.)

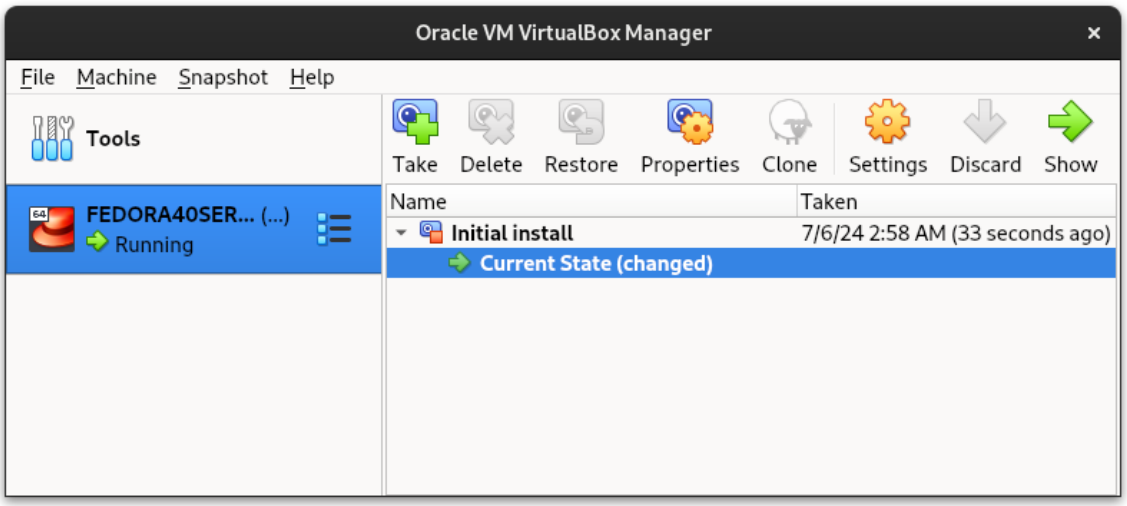


## 2.5 Changer le layout clavier

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

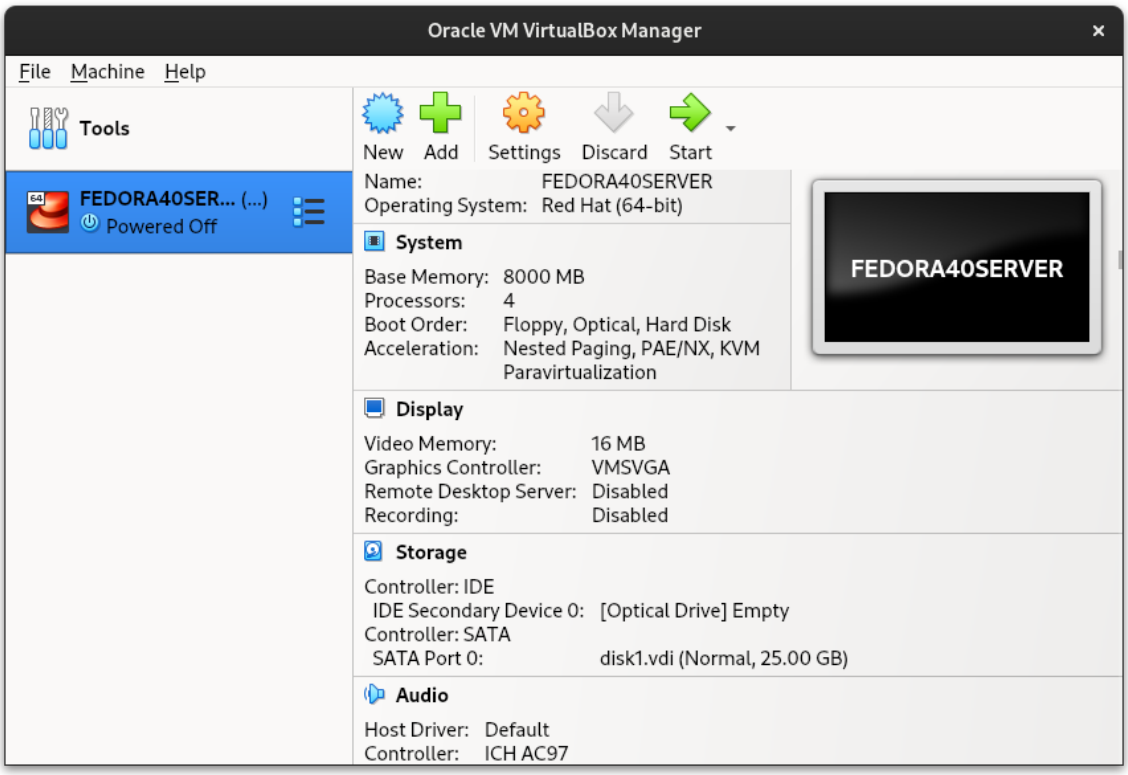
## 2.6 Snapshots de la machine

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.

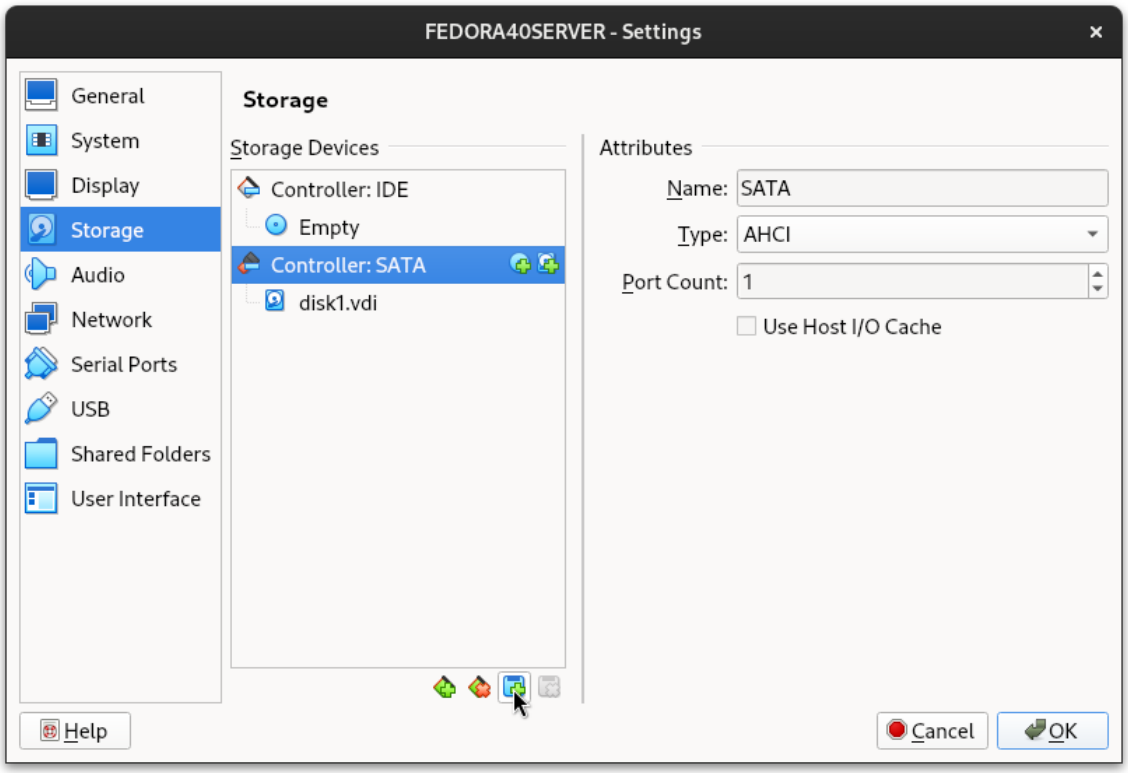



## 2.7 Ajout des disques virtuels

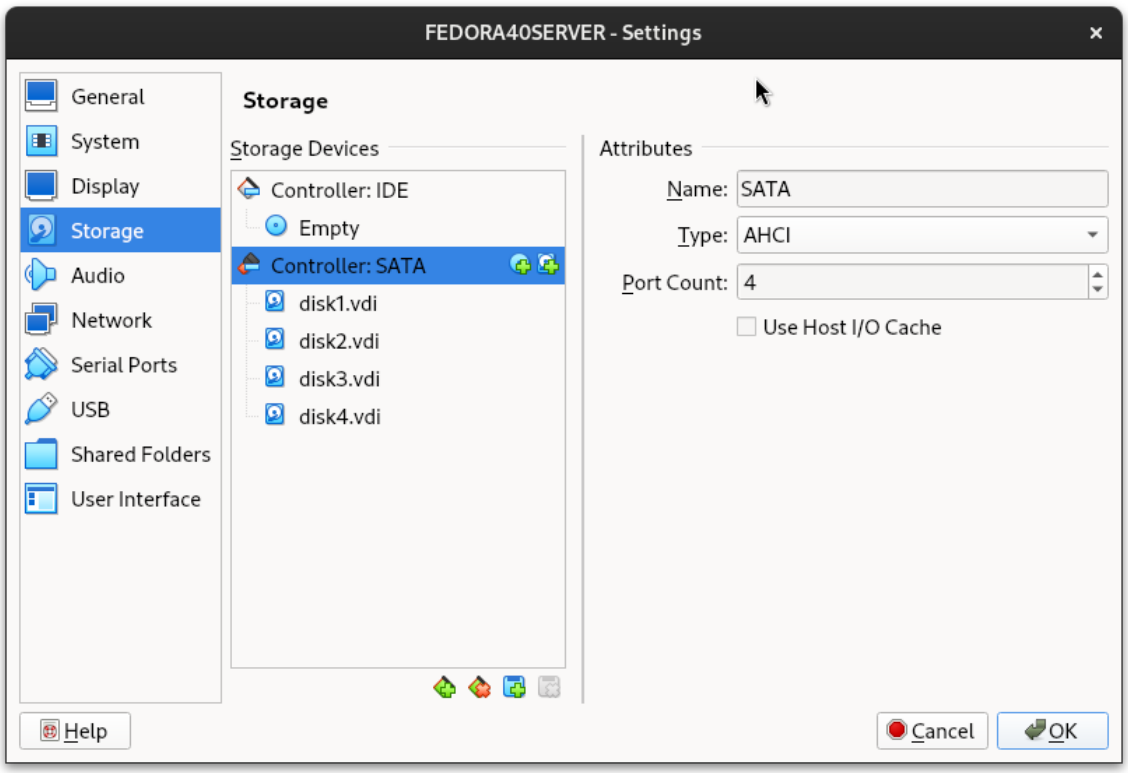
Dans les details de la machine, on selectionne "Storage" :



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 RAID

!! A finir

Les volumes dans lesquels viennent se mettre les partages et fichiers web sont `/mnt/raid5_share` et `/mnt/raid5_web`.

## 3.4 Partage sans authentification

Le partage sans authentification, donc avec accès libre en écriture et lecture, doit être accessible depuis Linuw et Windows. NFS sera donc utilisé pour linux et Samba pour Windows.

Le script offre la possibilité de créer un dossier dans le chemin préétabli, ou de choisir le chemin.

Il offre aussi la possibilité de créer séparément un partage NFS et un partage SMB.

Il gère également les autorisations pour que SELinux autororise l'accès.

!! Ajouter limites de poids du dossier

# 4 Autopsie par rapport au cahier des charges

# 5 Code

## 5.1 Menu TUI

### 5.1.1 Introduction

Nous avons besoin d'un menu qui reprenne la somme de tout notre travail. Le menu principal en TUI est un simple menu permettant de choisir le script concernant une manipulation spécifique d'un ou plusieurs services destiné(s) au serveur. Tout cela en une seule ligne de commande.

### 5.1.2 Explications

Le contenu du menu est connu à l'avance, nous pouvons donc imprimer chaque ligne de sélection de choix à l'écran. Une boucle maintient le menu à l'écran et regarde si une option est entrée. Si elle est valide, elle fait un chmod +x sur le script concerné,et le lance.

L'utilisation du script est assez explicite, il suffit de lire la liste des options et sélectionner le caractère correspondant. Etant assez simple, le menu est également robuste et ne requiert pas de précautions d'usage particulières.

## 5.2 NTP

### 5.2.1 Introduction

Pour le NTP, on utilise chrony. C'est un logiciel de synchronisation de l'heure pour les systèmes unix, et sert à synchroniser notre serveur et les machines qui y sont connectées disposent tous de la même heure système.

### 5.2.2 Explications

La première partie du script install chrony si il n'est pas déjà installé, et par défaut, la timezone est réglée sur Bruxelles. La deuxième partie permet de choisir une timezone correcte. La troisième permet d'afficher les infos.

## 5.3 DNS

### 5.3.1 Introduction

Un Domain Name Server (DNS) est un système de nommage hiérarchique et décentralisé pour ordinateurs, services et autres ressources connectées à internet ou à un réseau privé. Sa fonction est de traduire un nom de domaine facilement appréhendable en une adresse IP que les machines utilisent pour s'identifier sur un réseau.

- A Record : Mappe un nom de domaine à une adresse IPv4
- CNAME : Mappe un nom de domaine à un autre nom de domaine
- NS : Définit le serveur DNS autoritatif sur le domaine
- Pointer : Mappe une adresse IP à un nom de domaine
- MX :
- TXT :
- AAAA Record :

Un DNS cache quant à lui est un serveur DNS qui stocke les réponses DNS pour une certaine période de temps, à savoir la valeur Time To Live (TTL) des enregistrements DNS. Les requêtes DNS passent donc par ce serveur, et en cas d'absence de l'information dans sa base de données, celui-ci fera office de serveur DNS récursif.

### 5.3.2 Explications

1. Configuration du DNS
2. Configuration du DNC cache

## 5.4 Partage SAMBA

### 5.4.1 Introduction

Le service SMB a été configuré à l'aide de cet article.

### 5.4.2 Explications

Premièrement le script va installer le package "samba", si ce n'est pas déjà fait. Il va ensuite donner le choix à l'utilisateur pour gérer son partage samba.

(afin de voir quels sont les utilisateurs existants, ainsi que les groupes et directories associés au(x) partage(s).) A noter que les utilisateurs samba ont par défaut besoin d'être associés à un utilisateur UNIX, même si les deux bases de données sont bien distinctes. Il va nous falloir un menu pour pouvoir éditer :

- Les utilisateurs :
  - ✓ Lister
    - ✓ utilisateurs UNIX
    - ✓ utilisateurs samba
  - ✓ Ajouter
    - ✓ utilisateur UNIX
    - ✓ utilisateur samba
  - – Retirer
    - ∗ utilisateur UNIX
    - ✓ utilisateur samba
    - ✓ tous les utilisateurs samba (à part root)
  - – Désactiver utilisateur samba
  - – Activer utilisateur samba
  - – Changer le mot de passe

## 5.5 Partage NFS

### 5.5.1 Introduction

### 5.5.2 Explications

Concu pour partager des fichiers entre OS de type Unix,

Montage d'un FS samba sous Unix : `mount -t smbfs -o` (voir annexes du cours de linux P78)

## 5.6 Serveur Web

### 5.6.1 Introduction

Le déploiement d'un serveur web sous alma (ou fedora) est décrit dans cet article.

### 5.6.2 Explications

Deux subdirectories sont utiles pour la configuration :

- `/etc/httpd/conf.d`

  Pour stocker la configuration des différents sites web

- `/etc/httpd/conf.modules.d`

  Pour les modules chargés dynamiquement

Historiquement, les données du site web sont par défaut stockées dans :

- `/var/www/`

Cependant, pour plusieurs sites, il existe deux méthodes.

- utiliser le directory `/var/www/` et stocker les sites dans des subdirectories (facile pour SELinux, peu orthodoxe car modifie la configuration de base)
- utiliser le directory /srv et stocker les sites dans des subdirectories avec dans ceux-ci :
  - htdocs
  - webapps
  - mail
  - ...

Nous utiliserons donc :

- `/srv/<DOMAINNAME>/` pour stocker les données relatives au domaine
- `/srv/<DOMAINMANE>/htdocs/` pour les pages html statiques

!! A compléter pour le setup des LVM !!

Il faut ensuite installer le package httpd. Le manuel en ligne conseille d'installer les packages pour la gestion ssl et pour le monitoring de domaine.

Il suffit ensuite de démarrer le service httpd et de l'enable avec systemctl.

La page d'accueil par défaut ressemble à ceci sur AlmaLinux :

Le menu de selection contient donc :

- Install web server
- Show httpd status
- Create web dir for user
- Remove web directory of user
- Display web directories

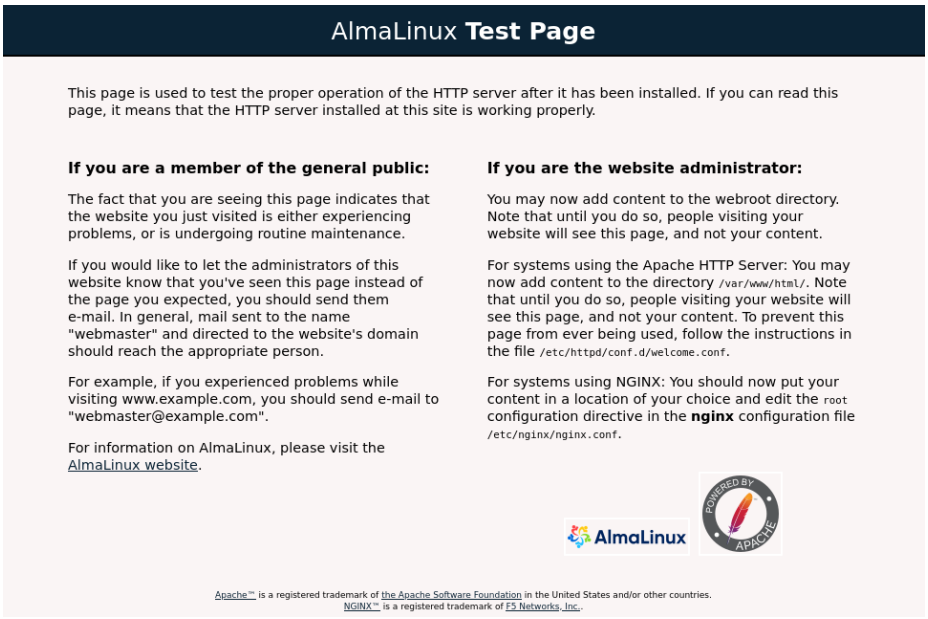



Figure 1: Page web par défaut sur Alma

## 5.7 Serveur SQL

### 5.7.1 Introduction

### 5.7.2 Explications

## 5.8 Serveur FTP

### 5.8.1 Introduction

Le service FTP a été configuré à l'aide de cet article de référence.

Chaque utilisateur spécifié doit être en mesure d'utiliser le service FTP pour accéder à :

- son dossier root
- son dossier web

### 5.8.2 Explications

Le service choisi est vsftpd (Very Secure FTP Daemon). Il est le plus répandu au sein des distributions RedHat-like, peu gourmand, stable et sécurisé (d'où son nom).

L'installation est similaire celle du serveur web. Par conséquent, il faudra en premier installer le service, le démarrer et puis ensuite le configurer.

Le fichier de configuration de vsftpd est :

`/etc/vsftpd/vsftpd.conf`

Dans ce fichier de configuration, on va choisir ces options :

- On écoute sur le port 21/tcp
- On est en standalone

  Le mode standalone indique que le serveur est autonome, et que le service tourne en permanence.
- On refuse les utilisateurs anonymes
- On accepte les utilisateurs système et les utilisateurs virtuels
- Les utilisateurs virtuels sont mappés sur l'utilisateur système "ftp"

- Les utilisateurs n'ont aucun droit d'écriture par défaut
- Ils sont chrootés dans:

  /var/ftp/

- Le dossier pour les configurations d'utilisateurs virtuels :

  /etc/vsftpd/vsftpd_user_conf/

- La liste des utilisateurs refusés (pour lesquels on ne demandera même pas le mot de passe) sera contenue dans :

  /etc/vsftpd/user_list

Le menu présente diverses options :

- Install and enable ftp server
- Start ftp server
- Stop ftp server
- Enable ftp server
- Disable ftp server
- Show ftp server status
- Directory attribution for users :
  - enable srv for all users
  - enable home for all users
  - disable srv for all users
  - disable home for all users
  - enable srv for the specified user
  - enable home for the specified user

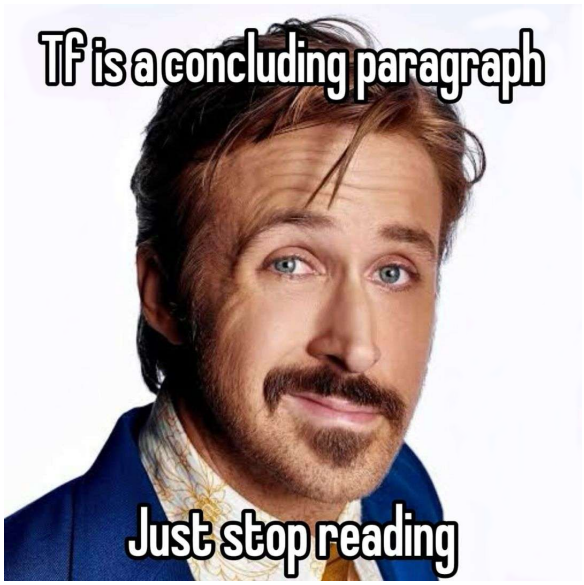
## 5.9 Backup

Le menu Backup doit comporter deux options :

- Backup
- Restore

### 5.10 Partitionnement

# 6 Conclusion




## References

[1] Author, A. (Year). Title of the article. *Journal Name*, Volume(Issue), Pages.

[2] Raid sous Oracle VirtualBox https://youtu.be/ZHVmGfteHCg

## Remerciements

Remerciements à Pauline M. pour ses encouragement et à la concentration :)