

# DDWS

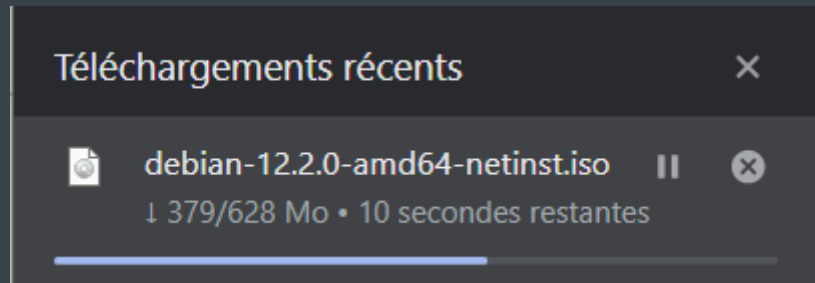
Marion BORNE

## TABLE DES MATIÈRES

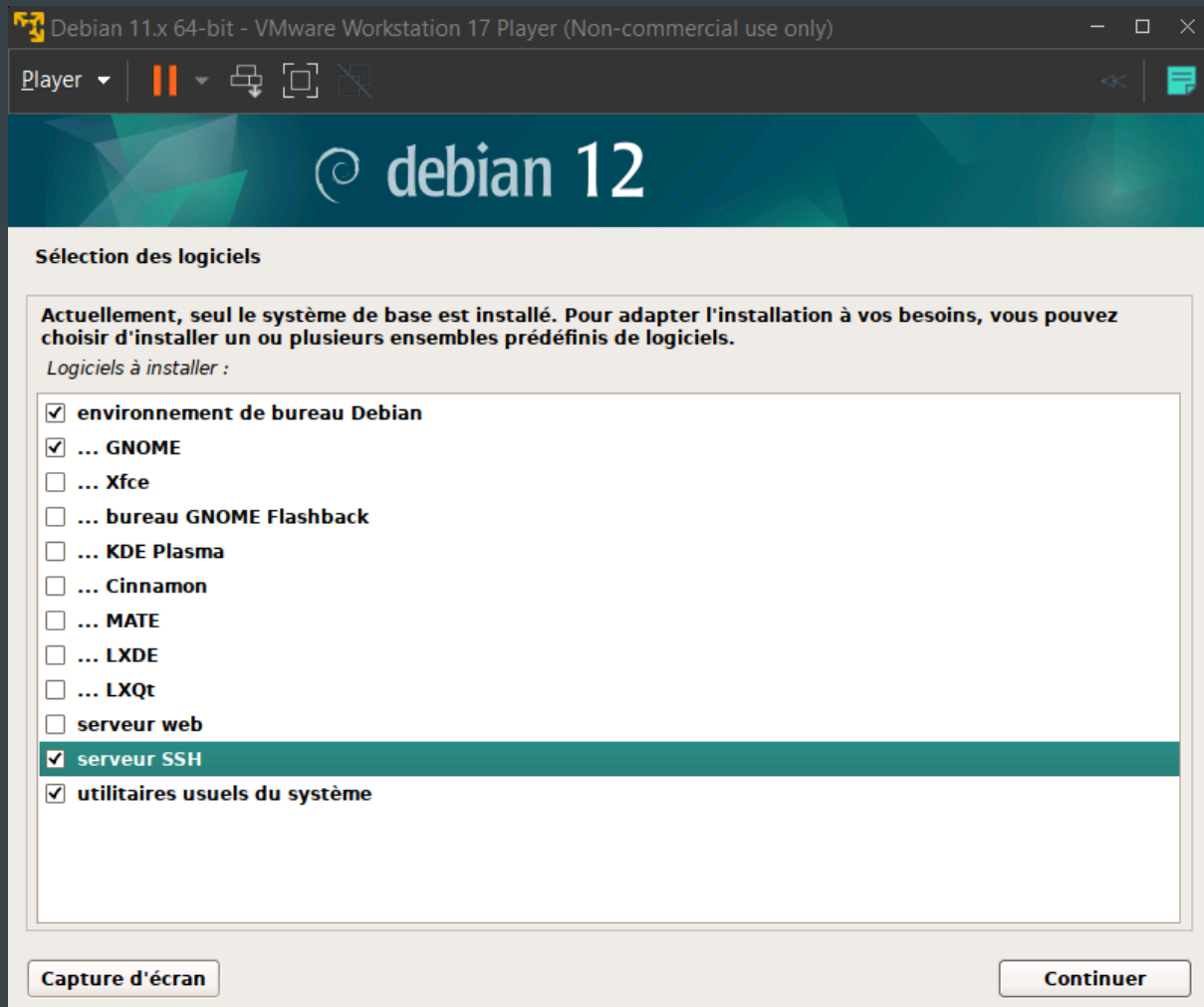
JOB 01 .....	2
JOB 02.....	4
JOB 03 .....	6
JOB 04 .....	8
JOB 05 .....	11
JOB 06 .....	12
JOB 07 .....	13
JOB 08.....	15

# JOB 01 -

Téléchargement de l'ISO de debian en architecture AMD64.



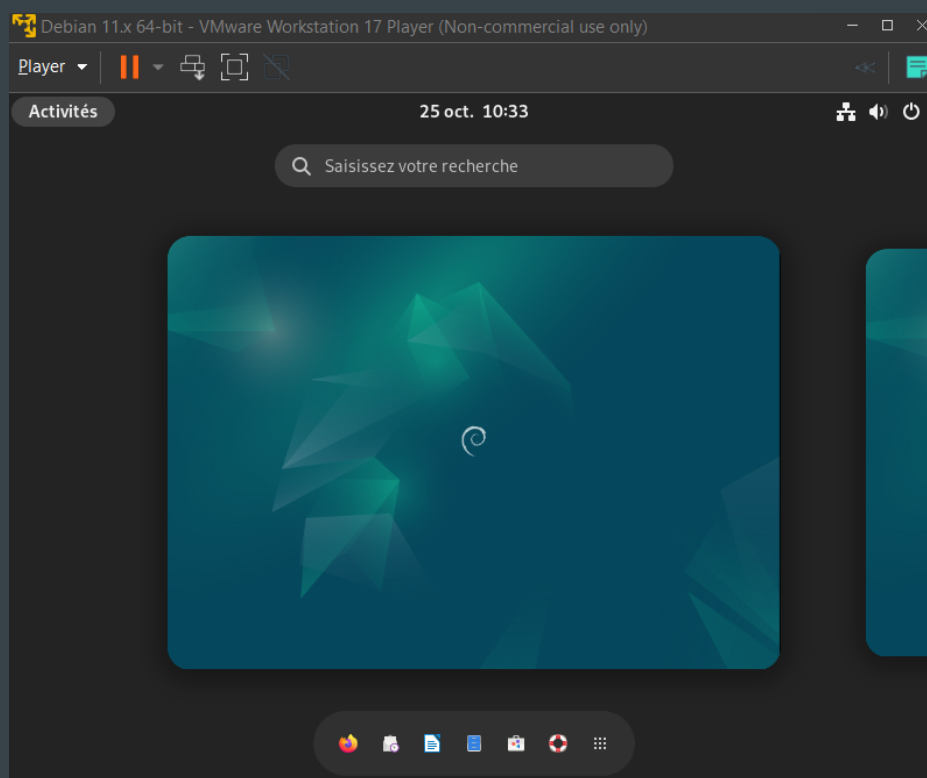
J'ai choisi d'installer directement le serveur SSH via ma configuration de ma VM.



On peut aussi l'installer via le terminal après avec la commande `sudo apt install openssh-server`

```
marionborne@marionborne: ~  
root@marionborne:/home/marionborne# sudo apt install openssh-server  
Lecture des listes de paquets... Fait  
Construction de l'arbre des dépendances... Fait  
Lecture des informations d'état... Fait  
openssh-server est déjà la version la plus récente (1:9.2p1-2+deb12u1).  
openssh-server passé en « installé manuellement ».  
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.  
root@marionborne:/home/marionborne#
```

Debian est installé avec son interface graphique.



Je dois maintenant démarrer le service SSH en utilisant la commande `sudo service ssh start`

Cela va me permettre des connexions à distance sur ma machine virtuelle.

Pour que le serveur démarre automatiquement à chaque démarrage de ma VM, j'utilise la commande

`sudo systemctl enable.ssh`

```
marionborne@marionborne: ~  
root@marionborne:/home/marionborne# sudo service ssh start  
root@marionborne:/home/marionborne# sudo systemctl enable ssh  
Synchronizing state of ssh.service with SysV service script with /lib/systemd/sy  
stemd-sysv-install.  
Executing: /lib/systemd/systemd-sysv-install enable ssh  
root@marionborne:/home/marionborne#
```

Je vais ensuite sur ma machine hôte (Windows) pour établir la connexion SSH avec ma VM.

J'utilise la commande `ssh marionborne@192.168.1.25` (IP de ma VM)

```
marionborne@marionborne: x + v
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Installez la dernière version de PowerShell pour de nouvelles fonctionnalités et améliorations ! https://aka.ms/powershell

PS C:\Users\mario> ssh marionborne@192.168.1.25
The authenticity of host '192.168.1.25 (192.168.1.25)' can't be established.
ED25519 key fingerprint is SHA256:uoah91aBbgJmFBWVZFciRgBff7PppD4d4LSVn06tTyc.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? Y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.1.25' (ED25519) to the list of known hosts.
marionborne@192.168.1.25's password:
Linux marionborne 6.1.0-13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.55-1 (2023-09-29) 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.
marionborne@marionborne:~$
```

## JOB 02 -

J'utilise la commande `sudo apt install apache2` dans mon terminal Debian pour installer mon serveur web Apache 2.

```
mariondebian@mariondebian: ~
mariondebian@mariondebian:~$ su
Mot de passe :
root@mariondebian:/home/mariondebian# sudo apt install apache2
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  apache2-data apache2-utils
Paquets suggérés :
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
Les NOUVEAUX paquets suivants seront installés :
  apache2 apache2-data apache2-utils
0 mis à jour, 3 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 577 ko dans les archives.
Après cette opération, 1 890 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n]
Réception de :1 http://deb.debian.org/debian bookworm/main amd64 apache2-data all 2.4.57-2 [160 kB]
Réception de :2 http://deb.debian.org/debian bookworm/main amd64 apache2-utils amd64 2.4.57-2 [202 kB]
Réception de :3 http://deb.debian.org/debian bookworm/main amd64 apache2 amd64 2.4.57-2 [215 kB]
577 ko réceptionnés en 0s (4 909 ko/s)
Sélection du paquet apache2-data précédemment désélectionné.
Lecture de la base de données : 149970 fichiers et répertoires déjà installés.)
```

Je démarre le service Apache2 grâce à la commande `sudo systemctl start apache2`

Puis pour que celui-ci se démarre automatiquement à chaque démarrage de ma VM j'utilise la commande

`sudo systemctl enable apache2`

Afin de vérifier que mon service Apache2 est bien actif, je vérifie son statut grâce à la commande

`sudo systemctl status apache2`

On voit que le service est active (running)

```
marionborne@marionborne: ~
root@marionborne:/home/marionborne# sudo systemctl status apache2
• apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enab>
   Active: active (running) since Fri 2023-10-27 09:57:13 CEST; 6min ago
     Docs: https://httpd.apache.org/docs/2.4/
    Main PID: 707 (apache2)
      Tasks: 55 (limit: 6795)
     Memory: 23.6M
        CPU: 145ms
    CGroup: /system.slice/apache2.service
            └─707 /usr/sbin/apache2 -k start
              └─708 /usr/sbin/apache2 -k start
                └─709 /usr/sbin/apache2 -k start

oct. 27 09:57:13 marionborne systemd[1]: Starting apache2.service - The Apache >
oct. 27 09:57:13 marionborne apachectl[696]: AH00558: apache2: Could not reliab>
oct. 27 09:57:13 marionborne systemd[1]: Started apache2.service - The Apache H>
lines 1-16/16 (END)
```

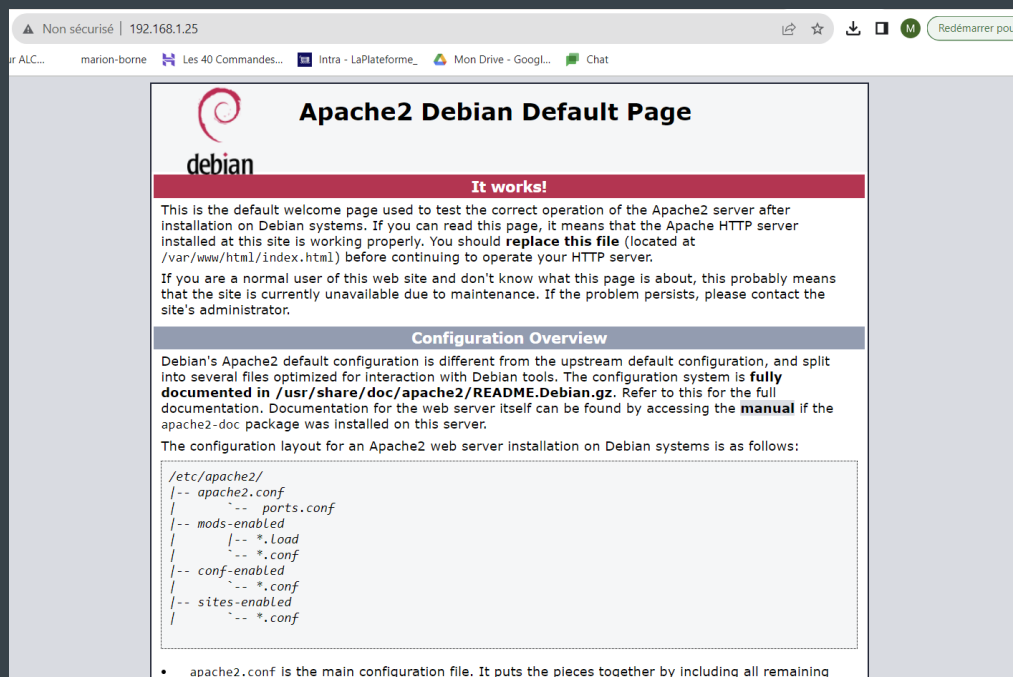
Puis j'ai trouvé l'IP de ma machine virtuelle grâce à la commande `ip a`

OU sinon j'utilise la commande : `mncli -p device show` qui est plus détaillée pour choisir la bonne IP.

Mon adresse ip est la suivante : 192.168.1.25

Je rentre mon IP dans mon navigateur Firefox de ma machine hôte (Windows)

L'installation de Apache2 a bien fonctionné, le serveur SSH aussi.



# JOB 03 -

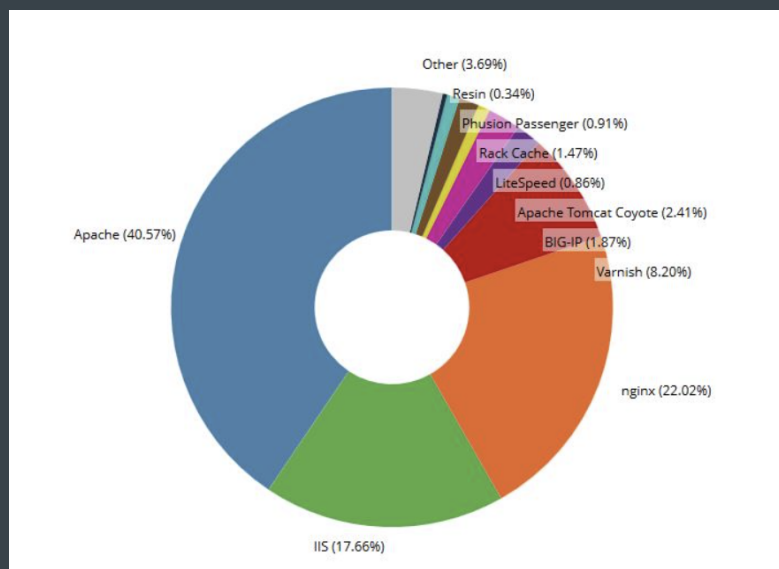
Lorsque vous naviguez sur Internet, le serveur Web est votre interlocuteur permanent.

C'est sur ce serveur qu'est stocké le contenu des sites Web afin d'être mis à la disposition des utilisateurs. La tâche principale d'un serveur Web est de transmettre des données au client, il s'agit des données statiques.

Un serveur Web possède également d'autres fonctionnalités :

- **Mise en cache HTTP** : pour gérer les grandes quantités de données, les serveurs Web peuvent mettre en mémoire tampon les contenus complexes grâce à la mise en cache.
- **Communication** : les messages sont partagés avec le navigateur concerné via des codes d'état ou des pages d'erreur.
  - **Protocole** : toutes les demandes sont enregistrées dans un fichier journal.
  - **Sécurité** : les serveurs Web sont chiffrés via HTTPS.
  - **Gestion des cookies** : les cookies peuvent être gérés par les serveurs Web.
- **Redirections** : les serveurs Web peuvent rediriger vers un autre document grâce à un moteur de réécriture.
- **Restriction d'accès** : le serveur Web permet de contrôler les accès grâce à des demandes d'authentification.

les principaux serveurs web sont les suivants :



Les serveurs Web les plus connus et les plus utilisés sont donc les suivants :

Serveur HTTP

Apache Microsoft IIS

NGINX

## Apache

Le serveur HTTP Apache – communément appelé Apache ou Apache HTTPD – est un logiciel de serveur web gratuit et libre.

Il traite les demandes des clients et sert du contenu web via le protocole de transfert hypertexte (HTTP).

Le serveur web Apache est compatible avec de nombreux systèmes d'exploitation (SE) tels que Microsoft Windows, OpenVMS, et tout système d'exploitation de type Unix comme Linux et macOS.

Apache est particulièrement populaire en raison de la puissance et de la flexibilité.

Grâce aux modules d'Apache, les utilisateurs peuvent facilement ajouter ou supprimer des fonctions, modifiant ainsi leur serveur en fonction de leurs besoins.

## NGINX

NGINX – prononcé comme « Engine X » – est l'un des serveurs les plus fiables en termes d'évolutivité et de vitesse.

Il s'agit également de l'un des serveurs web dont la croissance est la plus rapide du secteur, puisqu'il a atteint la deuxième place en termes de parts de marché.

Tout comme Apache, NGINX est un logiciel libre et gratuit.

NGINX est particulièrement populaire en raison de sa capacité à croître et à augmenter le trafic, tout en étant facile à faire évoluer sur un matériel minimal.

NGINX supporte presque tous les systèmes d'exploitation de type Unix.

Cependant, l'installation de NGINX sur Windows peut entraîner certaines limitations de performance, comme un manque d'évolutivité et des problèmes d'authentification UPD.

## Microsoft IIS

IIS, ou Internet Information Services, est un serveur web créé par Microsoft pour être utilisé avec les systèmes d'exploitation Windows.

IIS est conçu pour être sécurisé et offre plusieurs fonctions de sécurité, telles que l'authentification et l'autorisation, le support HTTPS et la protection contre les attaques malveillantes.

Il est également possible de configurer IIS pour utiliser des technologies de cryptage, telles que TLS et SSL.

SERVEUR WEB	AVANTAGES	INCONVENIENTS
APACHE	Open source et gratuit compatible avec de nombreux systèmes d'exploitation les utilisateurs peuvent facilement ajouter ou supprimer des fonctions	Moins performants que certains autres serveurs La configuration est complexe et fastidieuse (Nous allons le voir par la suite)
NGINX	Open source et gratuit Supporte presque tous les systèmes d'exploitation de type Unix L'un des serveurs les plus fiables en termes d'évolutivité et de vitesse	Configuration complexe comme Apache
IIS (MICROSOFT)	Offre plusieurs fonctions de sécurité Configuration aisée avec Microsoft	Se limite aux systèmes d'exploitation Microsoft

# JOB 04 -

Pour mettre en place mon serveur DNS, j'ai installé les paquets en tapant la commande

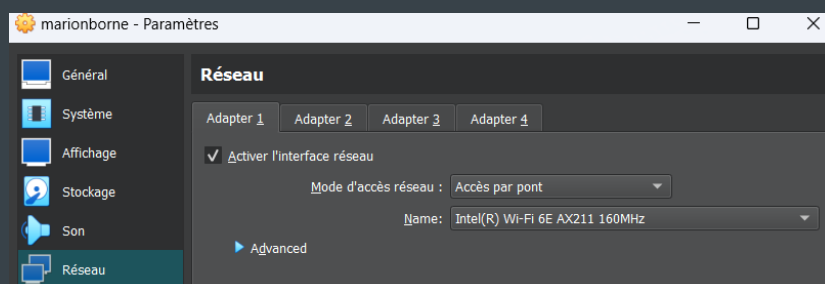
```
apt install bind9 bind9utils dnsutils
```

Bind est le serveur DNS le plus couramment utilisé sur Internet.

```
marionborne@marionborne: ~  
root@marionborne:/home/marionborne# apt install bind9 bind9utils dnsutils  
Lecture des listes de paquets... Fait  
Construction de l'arbre des dépendances... Fait  
Lecture des informations d'état... Fait  
Les paquets supplémentaires suivants seront installés :  
  bind9-utils  
Paquets suggérés :  
  bind-doc resolvconf ufw  
Les NOUVEAUX paquets suivants seront installés :  
  bind9 bind9-utils bind9utils dnsutils  
0 mis à jour, 4 nouvellement installés, 0 à enlever et 0 non mis à jour.  
Il est nécessaire de prendre 1 418 ko dans les archives.  
Après cette opération, 2 565 ko d'espace disque supplémentaires seront utilisés.  
Souhaitez-vous continuer ? [O/n]  
Réception de :1 http://deb.debian.org/debian bookworm/main amd64 bind9-utils amd  
64 1:9.18.19-1~deb12u1 [406 kB]  
Réception de :2 http://deb.debian.org/debian bookworm/main amd64 bind9 amd64 1:9  
.18.19-1~deb12u1 [494 kB]  
Réception de :3 http://deb.debian.org/debian bookworm/main amd64 bind9utils all  
1:9.18.19-1~deb12u1 [259 kB]  
Réception de :4 http://deb.debian.org/debian bookworm/main amd64 dnsutils all 1:  
9.18.19-1~deb12u1 [259 kB]  
1 418 ko réceptionnés en 5s (270 ko/s)  
Sélection du paquet bind9-utils précédemment désélectionné.
```

Puis j'ai configuré dans les réglages de ma VM le réseau en mode "Accès par pont" autrement appelé "Bridged".

Ce mode est le plus utilisé puisqu'il permet de connecter une machine virtuelle directement sur le réseau physique sur lequel est branchée la carte réseau physique de l'hôte.



J'ai ensuite sur ma VM utilisé la commande `hostname -I` pour vérifier mon adresse IP

IP : 192.168.1.25

```
marionborne@marionborne: ~  
marionborne@marionborne:~$ hostname -I  
192.168.1.25 2a01:cb1c:40f:7200:5716:c5d7:be9f:ad35 2a01:cb1c:40f:7200:a00:27ff:  
fe34:77ac  
marionborne@marionborne:~$
```



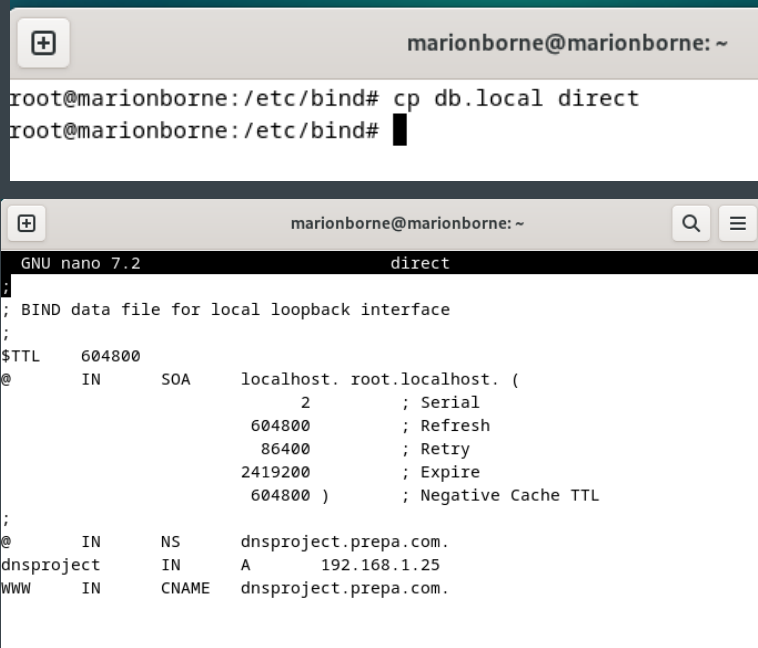
J'ai copié mon répertoire db.local dans mon fichier direct puis je modifie ce dernier grâce à ma commande

`nano direct`

Dans ce fichier direct, je modifie les informations afin de rajouter mon IP et mon nom de domaine.

nous voulons le nom de domaine suivant : `dnsproject.prepa.com`

Cette étape consiste à associer mon adresse IP 192.168.1.25 à mon nom de domaine permettant la bonne résolution entre les deux.

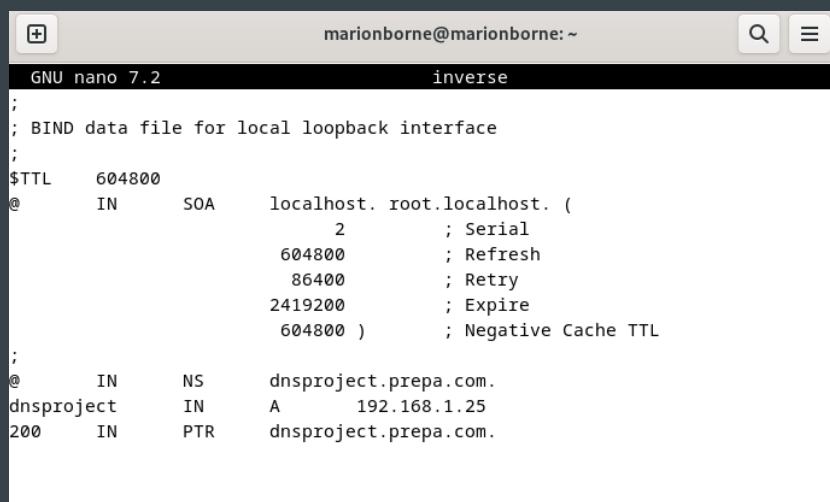


```
marionborne@marionborne: ~  
root@marionborne:/etc/bind# cp db.local direct  
root@marionborne:/etc/bind#  
  
GNU nano 7.2 direct  
;  
; BIND data file for local loopback interface  
;  
$TTL      604800  
@         IN      SOA      localhost. root.localhost. (  
                2          ; Serial  
                604800     ; Refresh  
                86400      ; Retry  
                2419200    ; Expire  
                604800 )   ; Negative Cache TTL  
;  
@         IN      NS       dnsproject.prepa.com.  
dnsproject IN      A        192.168.1.25  
www       IN      CNAME    dnsproject.prepa.com.
```

Après avoir enregistré mes modifications, je copie mon fichier direct dans un fichier nommé inverse

J'ai modifié la dernière ligne "`200 IN PTR dnsproject.prepa.com`"

Cela m'a permis d'associer l'IP 200 à mon domaine pour une résolution inversée.



```
marionborne@marionborne: ~  
GNU nano 7.2 inverse  
;  
; BIND data file for local loopback interface  
;  
$TTL      604800  
@         IN      SOA      localhost. root.localhost. (  
                2          ; Serial  
                604800     ; Refresh  
                86400      ; Retry  
                2419200    ; Expire  
                604800 )   ; Negative Cache TTL  
;  
@         IN      NS       dnsproject.prepa.com.  
dnsproject IN      A        192.168.1.25  
200       IN      PTR      dnsproject.prepa.com.
```

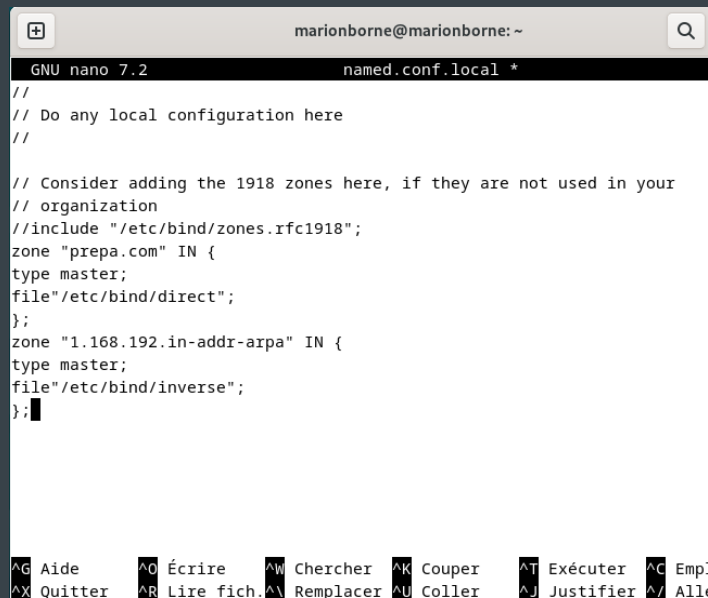
J'ai ensuite configuré mon fichier `named.conf.local` grâce à la commande `nano named.conf.local` afin que le DNS soit configuré et que toutes mes demandes liées à mon domaines soient bien reconnues par celui-ci.

J'ai inclue :

Mon adresse IP

Mon adresse IP à l'envers (ici sur la capture d'écran 1.168.192)

Mon domaine

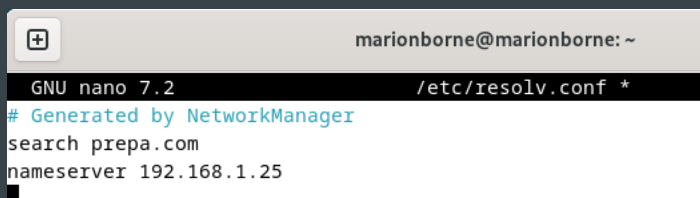


```
marionborne@marionborne: ~
GNU nano 7.2 named.conf.local *
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "prepa.com" IN {
type master;
file "/etc/bind/direct";
};
zone "1.168.192.in-addr-arpa" IN {
type master;
file "/etc/bind/inverse";
};
```

J'effectue la commande `nano /etc/revolv.conf`

Pour configurer les résolutions du DNS en notant mon IP et mon nom de domaine.

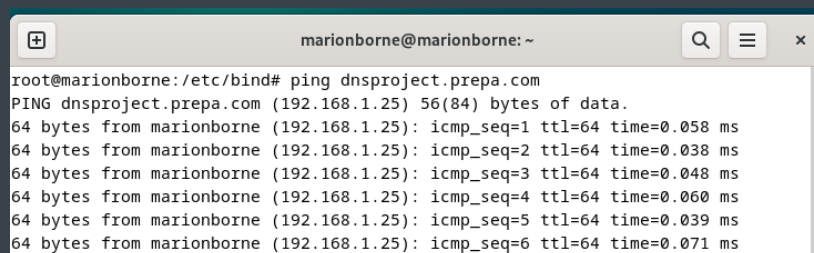
Cela m'assure que lorsque je taperai mon nom de domaine dans mon navigateur, celui-ci sera bien correctement pris en compte.



```
marionborne@marionborne: ~
GNU nano 7.2 /etc/resolv.conf *
# Generated by NetworkManager
search prepa.com
nameserver 192.168.1.25
```

Je redémarre le service Bing9 avec la commande `systemctl restart bing9`

Puis j'effectue un ping de mon via mon nom de domaine afin de vérifier que ma configuration DNS fonctionne.



```
root@marionborne:/etc/bind# ping dnsproject.prepa.com
PING dnsproject.prepa.com (192.168.1.25) 56(84) bytes of data.
64 bytes from marionborne (192.168.1.25): icmp_seq=1 ttl=64 time=0.058 ms
64 bytes from marionborne (192.168.1.25): icmp_seq=2 ttl=64 time=0.038 ms
64 bytes from marionborne (192.168.1.25): icmp_seq=3 ttl=64 time=0.048 ms
64 bytes from marionborne (192.168.1.25): icmp_seq=4 ttl=64 time=0.060 ms
64 bytes from marionborne (192.168.1.25): icmp_seq=5 ttl=64 time=0.039 ms
64 bytes from marionborne (192.168.1.25): icmp_seq=6 ttl=64 time=0.071 ms
```

Tout est ok.

# JOB 05 -

## Comment obtient-on un nom de domaine public ?

Choisir le nom de domaine et son extension

Vérifier la disponibilité du nom de domaine

Trouver un registrar (bureau d'enregistrement) et/ou un hébergeur web.

Enregistrer le nom de domaine

Sélectionner l'extension appropriée (fr, com, be, io ...)

Une fois enregistré, le nom de domaine est directement repris dans la base de données WHOIS. Le WHOIS est un moteur de recherches permettant de voir la disponibilité des noms de domaine et de fournir des informations techniques et administratives sur le titulaire d'un nom de domaine.

Ne pas oublier le nom de domaine régulièrement pour qu'il reste actif

## Quelles sont les spécificités que l'on peut avoir sur certaines extensions de nom de domaine ?

Les extensions de domaine sont les lettres qui suivent le point final d'une URL.

Il existe trois types d'extensions de domaines : les TLD génériques, les TLD sponsorisés et les TLD avec code pays.

La catégorie des TLD génériques comprend les extensions que nous connaissons et aimons tous, comme : .com / .org / .net

sTLD : Les TLD sponsorisés sont des extensions utilisées par une entité spécifique. Cela peut être une entreprise, une branche du gouvernement ou un autre type de groupe. : / .gov (gouvernement américain) / .mil (armée américaine)

ccTLD : Les TLD de code pays représentent un pays spécifique, comme .jp pour le Japon. Chaque extension de domaine de code de pays a ses propres règles. Certaines sont réservées aux organisations du pays, tandis que d'autres sont accessibles à tous.

Protocole	Sous-domaine (domaine de troisième niveau)	Nom de domaine (domaine de deuxième niveau)	Extension de domaine (domaine de premier niveau)	Description
https://	www	exemple	org	Adresse avec un domaine de premier niveau générique (gTLD) pour les organisations à but non lucratif (.org)
https://	www	exemple	fr	Adresse avec le domaine de premier niveau national (ccTLD) de la France (.fr)
https://	www	exemple	blog	Adresse avec un domaine de premier niveau générique récent (.blog)
https://	exemple	co	uk	Adresse avec un domaine de deuxième niveau national (.co), le nom de domaine réel (exemple) devient le domaine de troisième niveau, un sous-domaine supplémentaire deviendrait le domaine de quatrième niveau
https://	en	exemple	org	Adresse avec sous-domaine (.en) pour la page d'un site Web en langue anglaise

# JOB 06-

Je mets à jour mon serveur DNS dans les réglages de ma machine hôte (Windows) en mettant l'IP de ma VM.

Je choisis le mode Manuel et non Automatique

Modifier les paramètres DNS du réseau

Manuel

IPv4

☒ Activé

DNS préféré

192.168.1.1

DNS sur HTTPS

Désactivé

Autre DNS

192.168.1.25

DNS sur HTTPS

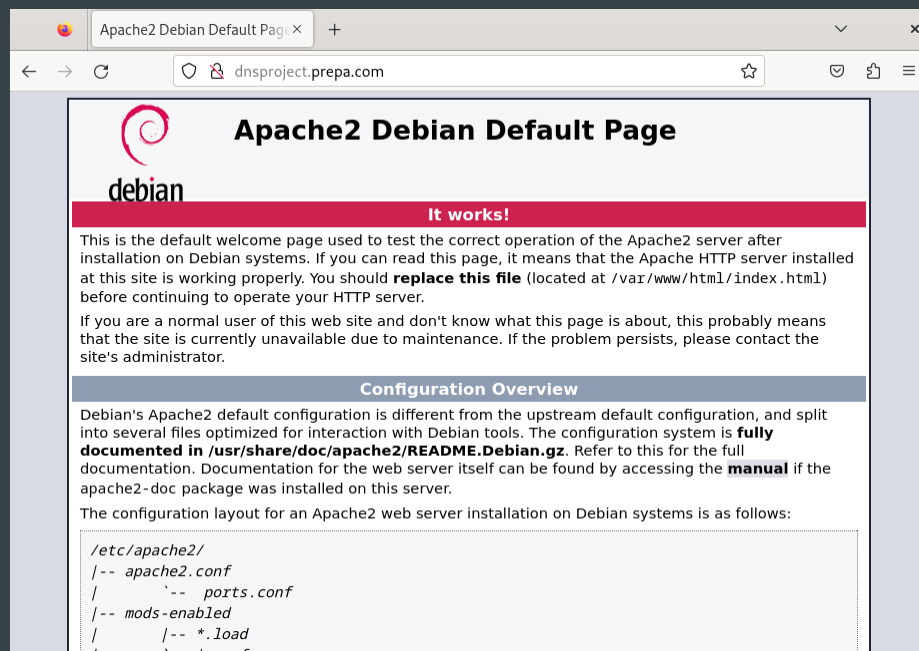
Désactivé

IPv6

☐ Désactivé

Enregistrer Annuler

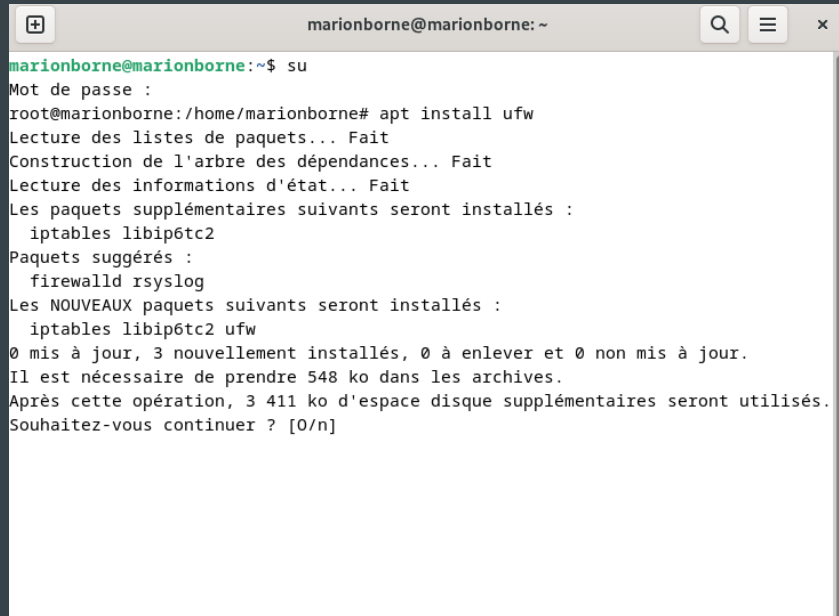
Je peux maintenant avoir accès à cette page ci-dessous



# JOB 07 -

J'installe les paquets UFW grâce à la commande `apt install ufw`

UFW est un outil de configuration de pare-feu qui est inclus dans Ubuntu par défaut.



```
marionborne@marionborne:~$ su
Mot de passe :
root@marionborne:/home/marionborne# apt install ufw
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  iptables libip6tc2
Paquets suggérés :
  firewalld rsyslog
Les NOUVEAUX paquets suivants seront installés :
  iptables libip6tc2 ufw
0 mis à jour, 3 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 548 ko dans les archives.
Après cette opération, 3 411 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n]
```

Les premières règles à définir sont vos politiques par défaut.

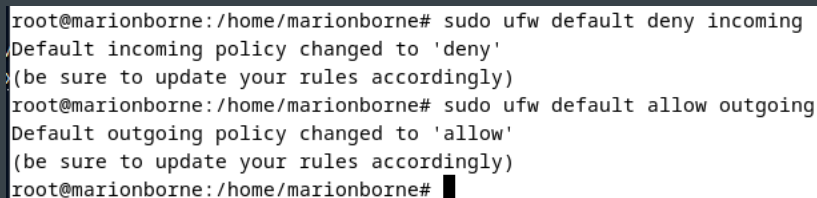
Ces règles contrôlent la manière de traiter le trafic qui ne correspond pas explicitement à d'autres règles. Par défaut, UFW est configuré pour refuser toutes les connexions entrantes et autoriser toutes les connexions sortantes. Cela signifie que toute personne essayant d'atteindre votre serveur ne pourra pas se connecter, tandis que toute application à l'intérieur du serveur pourra atteindre le monde extérieur.

Remettons vos règles UFW à leur valeur par défaut afin que nous puissions être sûrs que vous pourrez suivre ce tutoriel.

Pour définir les valeurs par défaut utilisées par UFW, utilisez ces commandes :

`sudo ufw default deny incoming`

`sudo ufw default allow outgoing`



```
root@marionborne:/home/marionborne# sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
root@marionborne:/home/marionborne# sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
root@marionborne:/home/marionborne#
```

Ces commandes définissent les valeurs par défaut pour refuser les connexions entrantes et autoriser les connexions sortantes.

Ces paramètres par défaut du pare-feu peuvent suffire pour un ordinateur personnel, mais les serveurs doivent généralement répondre aux demandes entrantes d'utilisateurs extérieurs.

Si nous activons notre pare-feu UFW maintenant, il refuserait toutes les connexions entrantes.

Cela signifie que nous devons créer des règles qui autorisent explicitement les connexions entrantes légitimes – connexions SSH ou HTTP, par exemple – si nous voulons que notre serveur réponde à ce type de demandes. Si vous utilisez un serveur cloud, vous voudrez probablement autoriser les connexions SSH entrantes afin de pouvoir vous connecter à votre serveur et le gérer.

Pour configurer votre serveur afin d'autoriser les connexions SSH entrantes, vous pouvez utiliser cette commande :

`sudo ufw allow ssh`

```
marionborne@marionborne: ~  
root@marionborne:/home/marionborne# sudo ufw allow ssh  
Rules updated  
Rules updated (v6)  
root@marionborne:/home/marionborne#
```

Nous devons autoriser toutes les autres connexions auxquelles notre serveur a besoin de répondre.

Les connexions que nous devons autoriser dépendent de nos besoins spécifiques.

HTTP sur le port 80, qui est ce qu'utilisent les serveurs web non cryptés, en utilisant

`sudo ufw allow http` ou `sudo ufw allow 80`

HTTPS sur le port 443, qui est ce qu'utilisent les serveurs web cryptés, en utilisant

`sudo ufw allow https` ou `sudo ufw allow 443`

Il existe plusieurs autres moyens d'autoriser d'autres connexions, outre la spécification d'un port ou d'un service connu.

```
marionborne@marionborne: ~  
root@marionborne:/etc/bind# sudo ufw allow http  
Rules updated  
Rules updated (v6)  
root@marionborne:/etc/bind# sudo ufw allow https  
Rules updated  
Rules updated (v6)  
root@marionborne:/etc/bind#
```

Nous autorisons le trafic sur les ports 139 et 445 en utilisant les commandes

`ufw allow 139/tcp` et `ufw allow 445/tcp`

Ces ports sont associés au protocole SMB (Server Message Block) et sont utilisés pour le partage de fichiers et d'imprimantes.

```
marionborne@marionborne: ~  
root@marionborne:/etc/bind# sudo ufw allow 139/tcp  
Rules updated  
Rules updated (v6)  
root@marionborne:/etc/bind# sudo ufw allow 445/tcp  
Rules updated  
Rules updated (v6)  
root@marionborne:/etc/bind#
```

Afin de sécuriser un maximum mon serveur en réduisant le risque d'attaques basées sur les paquets ICMP, je dois modifier mon fichier `/etc/ufw/ before.rules`

commande `nano before.rules`

Je remplace les ACCEPT par DROP dans la section ICMP codes for INPUT

```
marionborne@marionborne: ~
GNU nano 7.2 before.rules *
-A ufw-before-input -i lo -j ACCEPT
-A ufw-before-output -o lo -j ACCEPT

# quickly process packets for which we already have a connection
-A ufw-before-input -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A ufw-before-output -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A ufw-before-forward -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT

# drop INVALID packets (logs these in loglevel medium and higher)
-A ufw-before-input -m conntrack --ctstate INVALID -j ufw-logging-deny
-A ufw-before-input -m conntrack --ctstate INVALID -j DROP

# ok icmp codes for INPUT
-A ufw-before-input -p icmp --icmp-type destination-unreachable -j DROP
-A ufw-before-input -p icmp --icmp-type time-exceeded -j DROP
-A ufw-before-input -p icmp --icmp-type parameter-problem -j DROP
-A ufw-before-input -p icmp --icmp-type echo-request -j DROP
```

J'active mon pare-feu UFW en utilisant la commande

`sudo ufw enable`

```
marionborne@marionborne: ~
root@marionborne:/home/marionborne# sudo ufw enable
Firewall is active and enabled on system startup
root@marionborne:/home/marionborne#
```

## JOB 08 -

Pour mettre en place sur notre serveur un dossier partagé avec les autres membres de notre réseau.

J'installe le paquet Samba grâce à la commande `apt install samba`

Le logiciel Samba est un outil permettant de partager des dossiers et des imprimantes (d'où l'autorisation de trafic sur les ports 139 et 445 dans le job 07) à travers un réseau local.

Il permet de partager et d'accéder aux ressources d'autres ordinateurs fonctionnant avec des systèmes d'exploitation Microsoft® Windows® et Apple® Mac OS® X, ainsi que des systèmes GNU/Linux, \*BSD et Solaris dans lesquels une implémentation de Samba est installée.

Pour partager de manière simple des ressources entre plusieurs ordinateurs, l'utilisation de Samba est conseillée.

```
marionborne@marionborne: ~  
root@marionborne: /home/marionborne# apt install samba  
Lecture des listes de paquets... Fait  
Construction de l'arbre des dépendances... Fait  
Lecture des informations d'état... Fait  
Les paquets supplémentaires suivants seront installés :  
  attr ibverbs-providers libcephfs2 libfmt9 libgfs2 libgfs2-utils libgfs2xdr0  
  libglusterfs0 libibverbs1 librados2 librdmacm1 liburing2 python3-anyio  
  python3-click python3-colorama python3-dnspython python3-gpg python3-h11  
  python3-h2 python3-hpack python3-httpcore python3-httpx python3-hyperframe  
  python3-ldb python3-markdown python3-markdown-it python3-mdurl  
  python3-pygments python3-requests-toolbelt python3-rfc3986 python3-rich  
  python3-samba python3-sniffio python3-talloc python3-tdb python3-yaml  
  samba-ad-provision samba-common samba-common-bin samba-dsdb-modules  
  samba-vfs-modules tdb-tools  
Paquets suggérés :  
  python3-trio python3-aioquic python-markdown-doc python-pygments-doc  
  ttf-bitstream-vera ctdb ldb-tools ntp | chrony winbind heimdal-clients  
Les NOUVEAUX paquets suivants seront installés :  
  attr ibverbs-providers libcephfs2 libfmt9 libgfs2 libgfs2-utils libgfs2xdr0  
  libglusterfs0 libibverbs1 librados2 librdmacm1 liburing2 python3-anyio  
  python3-click python3-colorama python3-dnspython python3-gpg python3-h11  
  python3-h2 python3-hpack python3-httpcore python3-httpx python3-hyperframe  
  python3-ldb python3-markdown python3-markdown-it python3-mdurl  
  python3-pygments python3-requests-toolbelt python3-rfc3986 python3-rich
```

Pour configurer samba, je créer un dossier “Partage” qui servira de dossier commun entre ma VM et ma machine hôte  
(Windows)

commande : `sudo mkdir /home/Partage`

Puis j'ai édité mon fichier smb.conf qui se trouve dans /etc/samba pour que mon dossier “Partage” soit accessibles à  
d'autres machine (par exemple ma machine hôte)

commande : `nano /etc/samba/smb.conf`

J'ai ajouté dans mon fichier les lignes entourées dans la capture ci dessous

```
GNU nano 7.2 /etc/samba/smb.conf *  
comment = Printer Drivers  
path = /var/lib/samba/printers  
browseable = yes  
read only = yes  
guest ok = no  
# Uncomment to allow remote administration of Windows print drivers.  
# You may need to replace 'lpadmin' with the name of the group your  
# admin users are members of.  
# Please note that you also need to set appropriate Unix permissions  
# to the drivers directory for these users to have write rights in it  
; write list = root, @lpadmin  
  
[Partage]  
comment = Partage  
path = /home/Partage  
valid users = @users  
force group = users  
create mask = 0660  
directory mask = 0771  
writable = yes  
  
^G Aide ^O Écrire ^W Chercher ^K Couper ^T Exécuter ^C Emplacement  
^X Quitter ^R Lire fichier ^M Remplacer ^U Coller ^J Justifier ^_ Aller ligne
```



Je définie un utilisateur sur Samba pour pouvoir accéder au fichier "Partage"

commande : `smbpasswd -a marionborne` (nom d'utilisateur)

```
marionborne@marionborne: ~  
root@marionborne:/home# smbpasswd -a  
New SMB password:  
Retype new SMB password:  
Added user root.  
root@marionborne:/home#
```

Je termine en donnant les droits à mon utilisateur pour accéder et gérer les fichier dans le dossier "Partage"

commande : `chmod -R /home/Partage`

```
marionborne@marionborne: ~  
root@marionborne:/home# chmod -R 777 /home/Partage  
root@marionborne:/home#
```

Je redémarre le service samba avec la commande `service smb restart`

Cela permet à toutes nos dernières configurations d'être prises en compte

L'utilisateur de la VM et de la machine hôte pourrons tous deux accéder au dossier "Partage".