

DDWS

Job 02

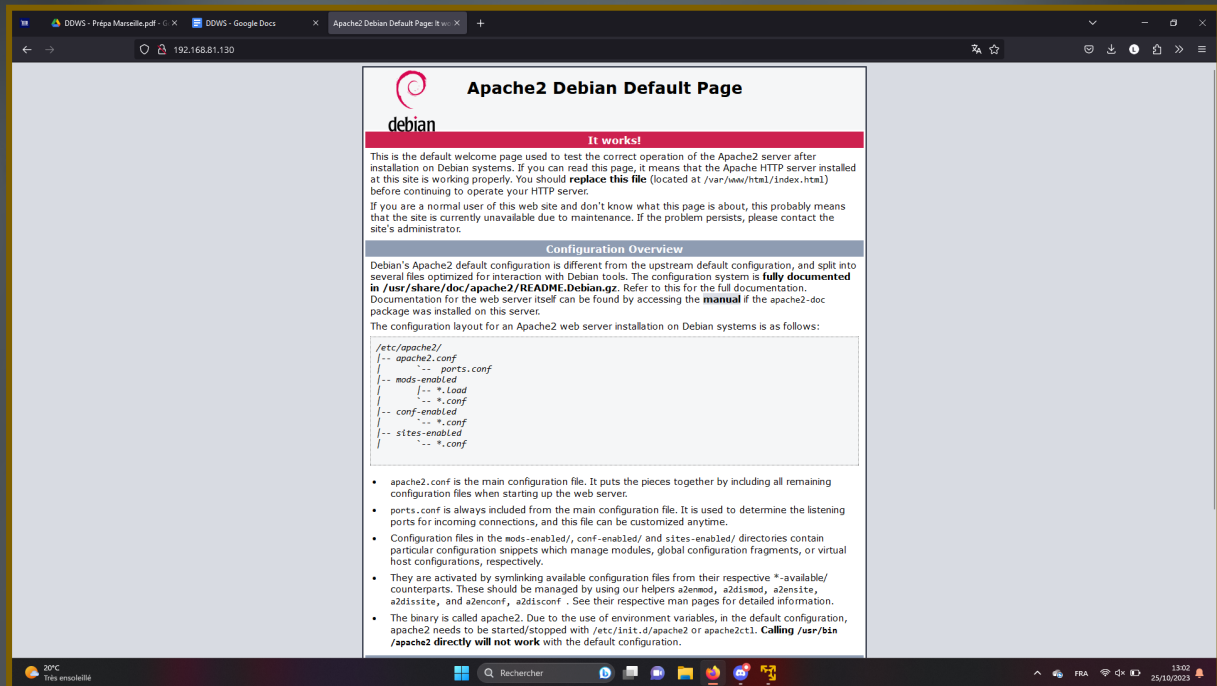
Pour commencer on va installer Apache2 grace a la commande ci-dessous :

```
root@vututu:/home/vututu# apt-get install Apache2
```

On va ensuite récupérer l'ip de la VM grâce à la commande “**ip a**”

```
vututu@vututu: ~  
root@vututu:/home/vututu# 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 noprefixroute  
        valid_lft forever preferred_lft forever  
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 00:0c:29:71:ef:42 brd ff:ff:ff:ff:ff:ff  
    altname enp2s1  
    inet 192.168.81.130/24 brd 192.168.81.255 scope global dynamic noprefixroute ens33  
        valid_lft 1182sec preferred_lft 1182sec  
    inet6 fe80::20c:29ff:fe71:ef42/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
root@vututu:/home/vututu#
```

Pour terminer on se rend sur le navigateur de votre machine et on rentre l'ip de notre VM ce qui nous amène sur cette page.



Job 03

Il existe de nombreux serveurs web disponibles, chacun avec ses propres avantages et inconvénients. Voici une liste de quelques-uns des serveurs web les plus populaires, ainsi que des informations sur chacun d'entre eux :

❖ Apache HTTP Server (httpd) :

➤ Avantages :

- Très populaire et largement utilisé dans le monde entier.
- Une grande communauté de soutien et de nombreuses ressources en ligne.
- Modulaire et extensible grâce à des modules tiers.
- Fonctionne bien sur divers systèmes d'exploitation.

➤ Inconvénients :

- Peut être gourmand en ressources dans certaines configurations.
- La configuration peut être complexe pour les débutants.

❖ Nginx :

➤ Avantages :

- Conçu pour être léger, rapide et performant.
- Excellente gestion de la charge et de la mise en cache.
- Peut servir de proxy inverse pour équilibrer la charge.

➤ Inconvénients :

- La configuration peut être plus complexe que d'autres serveurs web.
- Moins de modules tiers disponibles que pour Apache.

❖ LiteSpeed :

➤ Avantages :

- Extrêmement rapide et efficace.
- Possède un panneau de contrôle pour une gestion facile.
- Compatible avec la plupart des logiciels serveur Apache.

➤ Inconvénients :

- La version gratuite a des limitations en termes de fonctionnalités.

❖ Caddy :

➤ Avantages :

- Facile à configurer avec un support natif pour HTTPS.
- Possède un générateur de configuration automatique.
- Convivial pour les débutants.

➤ Inconvénients :

- Moins de modules tiers que les serveurs plus établis.
- Des performances légèrement inférieures à Nginx dans certaines situations.

❖ Microsoft Internet Information Services (IIS) :

➤ Avantages :

- Intégré à Windows Server.
- Excellente prise en charge des technologies Microsoft, comme ASP.NET.
- Convivial pour les utilisateurs de Windows.

➤ Inconvénients :

- Principalement limité à la plate-forme Windows.
- Peut nécessiter une licence ou une édition spécifique de Windows.

❖ Cherokee :

➤ Avantages :

- Facile à configurer avec une interface web conviviale.
- Prise en charge de la réécriture d'URL et de la mise en cache.
- Performant pour les sites à fort trafic.

➤ Inconvénients :

- Une base d'utilisateurs moins importante, ce qui signifie moins de ressources en ligne.

Job 04 & Job 06

Tout d'abord on installe bind9 et les utilitaires nécessaires à la configuration d'un serveur DNS avec “**apt-get install bind9 bind9utils dnsutils**”.

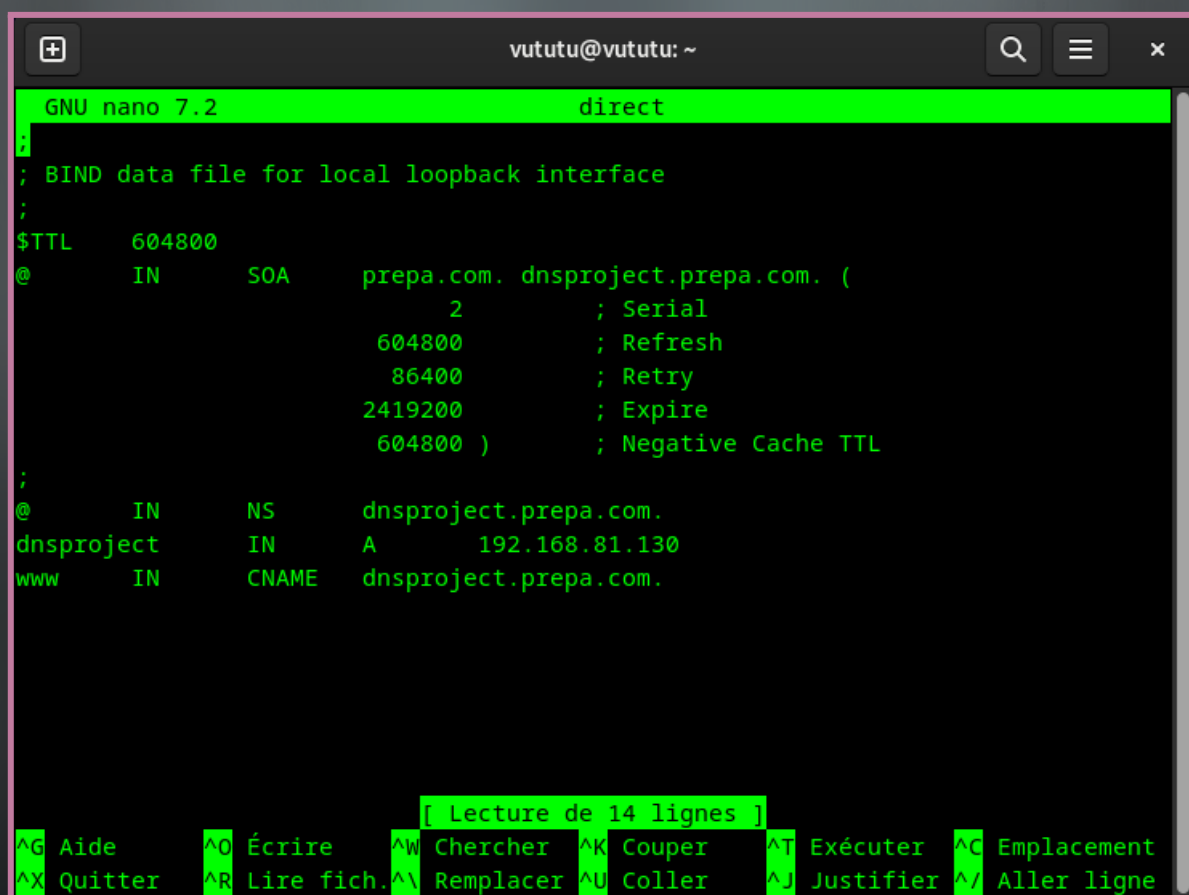
```
vututu@vututu: ~  
vututu@vututu:~$ su  
Mot de passe :  
root@vututu:/home/vututu# apt-get install bind9 bind9utils dnsutils  
Lecture des listes de paquets... Fait  
Construction de l'arbre des dépendances... Fait  
Lecture des informations d'état... Fait  
bind9 est déjà la version la plus récente (1:9.18.19-1~deb12u1).  
bind9utils est déjà la version la plus récente (1:9.18.19-1~deb12u1).  
dnsutils est déjà la version la plus récente (1:9.18.19-1~deb12u1).  
0 mis à jour, 0 nouvellement installés, 0 à enlever et 5 non mis à jour.  
root@vututu:/home/vututu#
```

Je récupère mon ip comme précédemment avec la commande suivante : `"ip a"`

Je me rend par la suite dans le dossier contenant les config de bind a l'aide de la commande : `"cd /etc/bind"`

je me rend ensuite dans les fichiers de configuration afin d'associer l'ip au nom de serveur et nom de domaine. Tout d'abord avec les commandes :

`"cp db.local direct"` puis `"nano direct"`. Il ne reste plus qu'à modifier le fichier comme ceci :



```
vututu@vututu: ~
GNU nano 7.2      direct
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      prepa.com. dnsproject.prepa.com. (
                        2      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       dnsproject.prepa.com.
dnsproject IN      A        192.168.81.130
www       IN      CNAME     dnsproject.prepa.com.

[ Lecture de 14 lignes ]
^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement
^X Quitter   ^R Lire fich.^V Remplacer  ^U Coller    ^J Justifier ^_ Aller ligne
```

On refait la meme manip “**cp direct inverse**” suivi de “**nano inverse**” et on change le fichier précédent :

```
GNU nano 7.2          inverse
;
; BIND data file for local loopback interface
;
$TTL      604800
@        IN      SOA      prepa.com. dnsproject.prepa.com. (
                        2      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@        IN      NS       dnsproject.prepa.com.
dnsproject IN      A       192.168.81.130
213      IN      PTR      dnsproject.prepa.com.

[ Lecture de 14 lignes ]
^G Aide      ^O Écrire   ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement
^X Quitter   ^R Lire fich.^_ Remplacer  ^U Coller    ^J Justifier ^/ Aller ligne
```

On se rend ensuite dans : “**nano named.conf.local**”

Puis dans “**nano /etc/resolv.conf**”

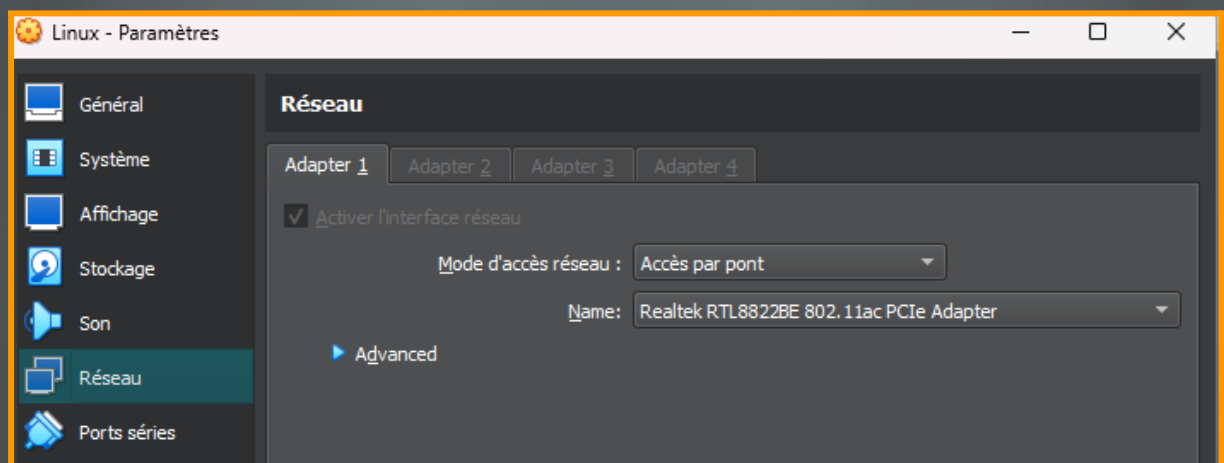
```
GNU nano 7.2          named.conf.local
//
// Do any local configuration here
//

// 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 "8.10.10.in-addr-arpa" IN {
type master;
file"/etc/bind/inverse";
};

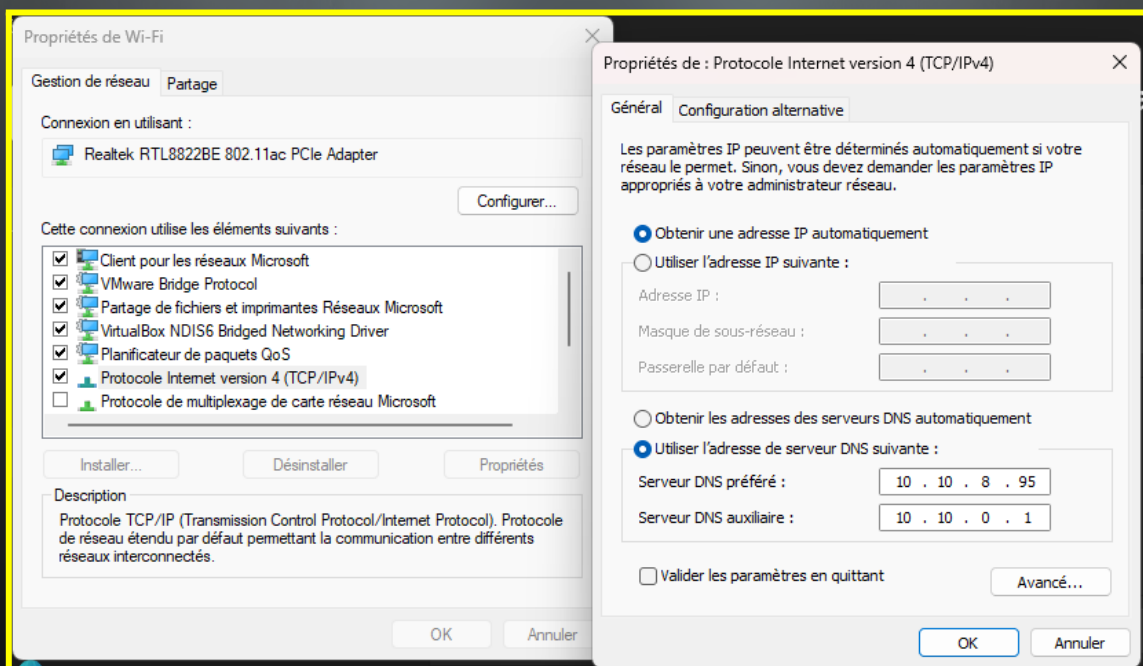
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^_ Replace   ^U Paste     ^J Justify    ^/ Go To Line
```

```
GNU nano 7.2 /etc/resolv.conf *
# Generated by NetworkManager
search prepa.com
nameserver 10.10.8.95
```

On va ensuite se rendre dans la configuration de la VM et changer le type de connexion en Bridge (Accès par pont)

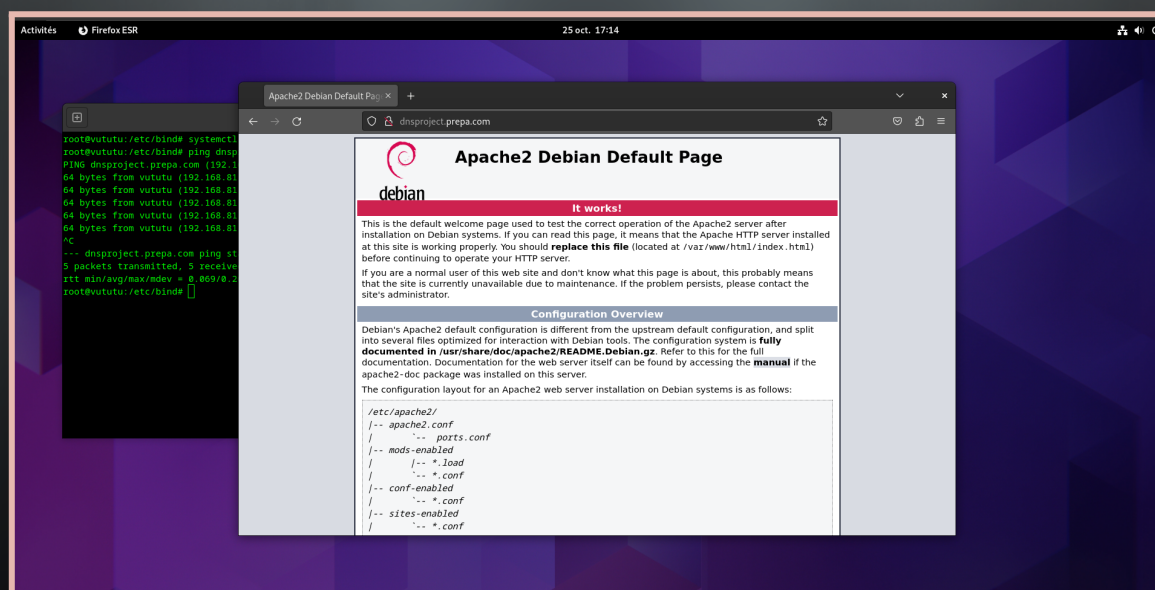


Et sur votre machine hôte vous rendre dans les paramètres réseaux et changer les adresses DNS en mettant l'ip de votre VM utilisé précédemment.



Pour finir on redémarre alors le service bind9 pour appliquer les changements, puis on ping le serveur avec le nom de domaine ainsi apache sera bien accessible via le nom de domaine avec “**systemctl restart bind9**” et “**ping dnsproject.prepa.com**”

```
vututu@vututu: ~  
root@vututu:/etc/bind# systemctl restart bind9  
root@vututu:/etc/bind# ping dnsproject.prepa.com  
PING dnsproject.prepa.com (192.168.81.130) 56(84) bytes of data:  
64 bytes from vututu (192.168.81.130): icmp_seq=1 ttl=64 time=0.615 ms  
64 bytes from vututu (192.168.81.130): icmp_seq=2 ttl=64 time=0.129 ms  
64 bytes from vututu (192.168.81.130): icmp_seq=3 ttl=64 time=0.069 ms  
64 bytes from vututu (192.168.81.130): icmp_seq=4 ttl=64 time=0.128 ms  
64 bytes from vututu (192.168.81.130): icmp_seq=5 ttl=64 time=0.069 ms  
^C  
--- dnsproject.prepa.com ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4009ms  
rtt min/avg/max/mdev = 0.069/0.202/0.615/0.208 ms  
root@vututu:/etc/bind#
```



Job 05

→ Faites des recherches sur comment obtient-on un nom de domaine public ?

1. Choisissez un nom de domaine pertinent et vérifiez sa disponibilité.
2. Sélectionnez un registrar de noms de domaine, comme GoDaddy ou Namecheap.
3. Enregistrez le nom de domaine en fournissant des informations et en payant les frais d'enregistrement.
4. Configurez les enregistrements DNS pour diriger le nom de domaine vers votre site.
5. Renouvelez le nom de domaine chaque année pour le maintenir actif.

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

Certaines extensions de noms de domaine ont des spécificités particulières. Par exemple :

- .gov est réservé aux entités gouvernementales.
- .edu est réservé aux établissements d'enseignement.
- .museum est destiné aux musées.
- .io est populaire pour les startups et la technologie.
- .tv est associé à l'industrie de la télévision et du divertissement.
- .mil : Réservé aux entités militaires des États-Unis, telles que l'armée, la marine, etc.

Il existe de nombreuses autres extensions de noms de domaine, et certaines d'entre elles peuvent avoir des restrictions ou des spécificités particulières. Avant de choisir une extension de domaine, assurez-vous de comprendre les règles et les exigences associées à celle-ci, car elles varient d'une extension à l'autre.

Job 07

Tout d'abord il faut installer ufw, on utilise donc “**apt-get install ufw**”

On utilise ensuite ces commandes :

- **ufw enable**
- **ufw allow 80/tcp**
- **ufw default deny incoming**
- **ufw default deny outgoing**

```
root@Linux:/etc/bind# ufw enable
Firewall is active and enabled on system startup
root@Linux:/etc/bind# ufw allow 80/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)
root@Linux:/etc/bind# ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
root@Linux:/etc/bind# ufw default deny outgoing
Default outgoing policy changed to 'deny'
(be sure to update your rules accordingly)
root@Linux:/etc/bind#
```

Qui s'en suit la commande “**nano /etc/ufw/before.rules**” et modifier ses lignes :

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

↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

```
# 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
```

Une fois ceci réalisé on check si tout est bon a l'aide de “**ufw status verbose**” et si tout est bon on redémarre ufw avec “**ufw reload**”.

```
root@Linux:/etc/bind# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), deny (outgoing), disabled (routed)
New profiles: skip

To Action From
--
80/tcp ALLOW IN Anywhere
80/tcp (v6) ALLOW IN Anywhere (v6)

root@Linux:/etc/bind# ufw reload
Firewall reloaded
root@Linux:/etc/bind# █
```

Job 08

Tout d'abord pour mettre en place le système de fichier partager il faut installer samba avec : “**sudo apt-get install samba**”

Il faut ensuite se rendre dans le fichier de configuration de samba à l'aide de la commande : “**sudo nano /etc/samba/smb.conf**” et rajouter :

- [Nom du partage]
- path = /emplacement/du/répertoire
- **guest ok** = yes – indique que le partage est accessible au public.
- **browseable** = **yes** fera apparaître le partage comme disponible pour tous les utilisateurs. Définissez **browseable** = no pour obliger les utilisateurs à taper manuellement le nom du partage pour y accéder
- **read only** = **yes** – pour empêcher les utilisateurs d'apporter des modifications au répertoire à distance via la lecture seule
- **writable** = **yes** – pour autoriser l'écriture sur le partage


```
GNU nano 7.2 /etc/samba/smb.conf *
# Windows clients look for this share name as a source of downloadable
# printer drivers
[print$]
    comment = Printer Drivers
    path = /var/lib/samba/printers
    browseable = no
    read only = yes
    guest ok = yes
# 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

[Share]
path = /home/vututu/share
guest ok = no
writable = yes
█
```

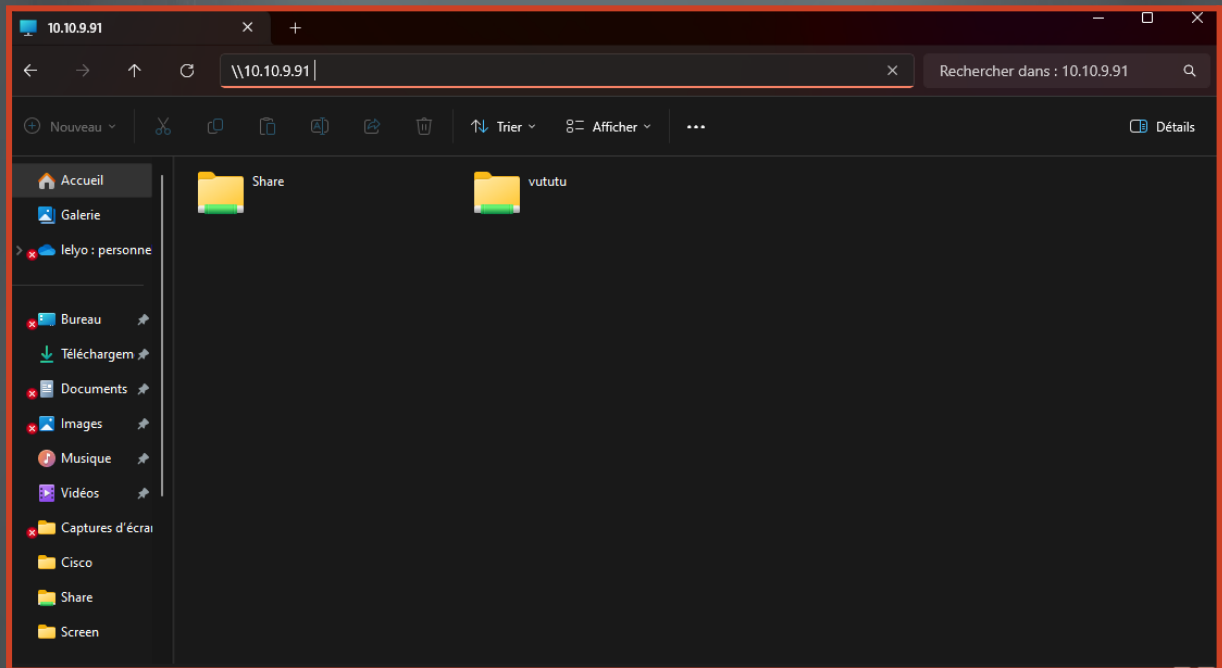
Il faut ensuite s'ajouter au groupe d'utilisateurs de samba avec la commande : “**sudo adduser (votre nom d'utilisateur) sambashare**”

On va ensuite définir un mot de passe pour l'utilisateur samba avec : “**sudo smbpasswd -a vututu**”

Et pour terminer on redémarre le service avec : “**sudo service smbd restart**”

```
vututu@Linux:~$ sudo adduser vututu sambashare
adduser: The user `vututu' is already a member of `sambashare'.
vututu@Linux:~$ sudo smbpasswd -a vututu
New SMB password:
Retype new SMB password:
vututu@Linux:~$ sudo service smbd restart
vututu@Linux:~$ █
```


On va ensuite se rendre dans la machine hôte et rentrer l'ip de la VM pour trouver le serveur de partage de fichier.



et on peut voir qu'il y a le même fichier sur la VM et la machine hôte.

