La Plateforme

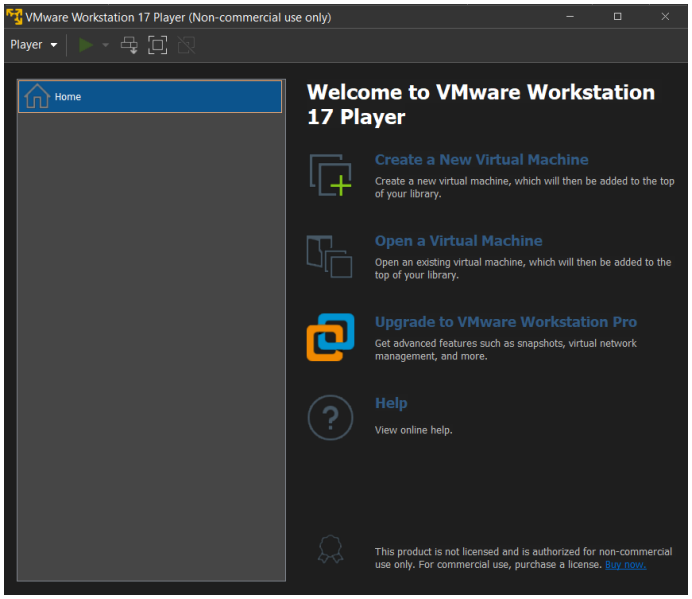
DDWS

Bachelor IT

Rija Rasoanaivo
29/10/2023

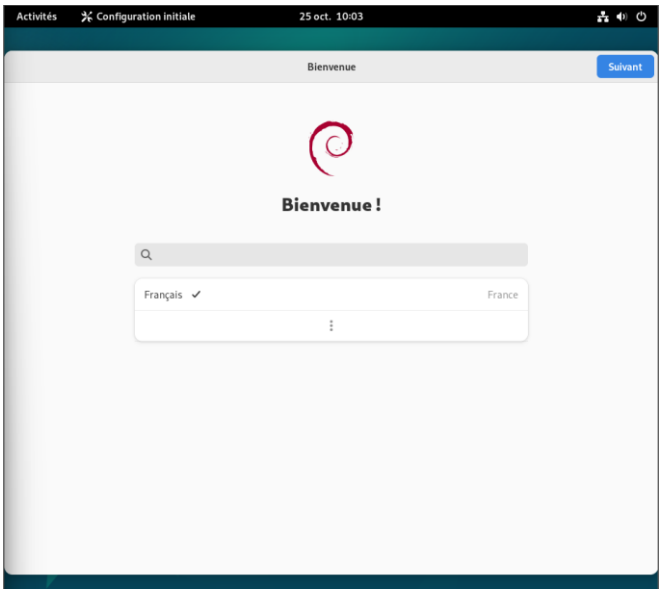
Job 01

Installation de la VM Debian via VMware :



Installation graphique :

Debian installé :



Job 02

Les commandes pour installer Apache2

Mettre à jour le système :

```
apt update && apt upgrade
```

Installer Apache2 :

```
apt install apache2
```

Démarrer Apache2 :

```
sudo systemctl start apache2
```

Activer le démarrage automatique de Apache2 :

```
sudo systemctl enable apache2
```

Trouver l'adresse IP avec la commande :

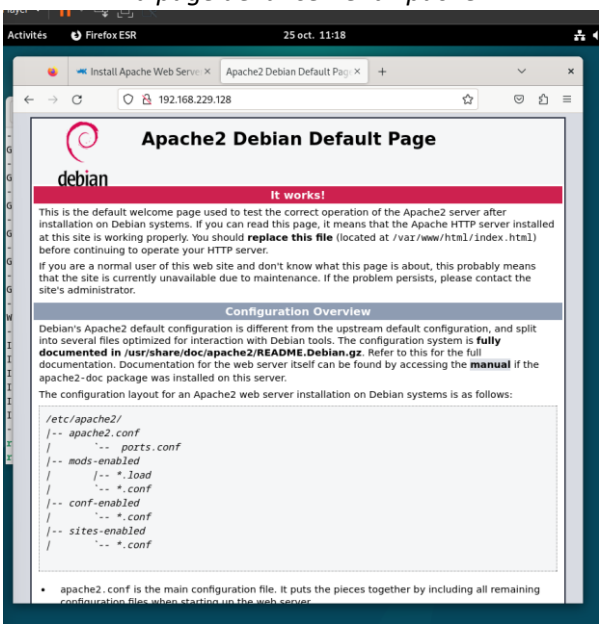
```
nmcli -p device show
```

```
IP4.ADDRESS[1]:                         192.168.229.128/24
IP4.GATEWAY:                            192.168.229.2
IP4.ROUTE[1]:                           dst = 192.168.229.0/24, nh = 0.0.0.0, mt = 100
IP4.ROUTE[2]:                           dst = 0.0.0.0/0, nh = 192.168.229.2, mt = 100
```

Dans la barre d'adresse Chrome de Debian, rentrer l'IP4.ADRESS[1] :

192.168.229.128

Ma page de lancement Apache :



Job 03

Quelques serveurs Web :

-Apache (le plus répandu)
-IIS (Microsoft)
-Nginx (NGINX)
-Node.Js
-Web Lighttpd

Serveur	Avantages	Inconvénients
Apache HTTP *Le serveur web Apache est conçu pour gérer des sites web statiques et dynamiques.*	✓ Open-source et gratuit même pour un usage commercial. ✓ Logiciel fiable et stable. ✓ Mise à jour régulière, correctifs de sécurité réguliers. ✓ Flexible grâce à sa structure basée sur des modules. ✓ Facile à configurer, adapté aux débutants. ✓ Plateforme-Cross (fonctionne sur les serveurs Unix et Windows). ✓ Fonctionne avec les sites WordPress. ✓ Grande communauté et support disponible en cas de problème. ✓ Prend en charge plusieurs protocoles de communication tels que HTTP, HTTPS, FTP, etc.	× Problèmes de performances sur les sites web avec un énorme trafic. × Trop d'options de configuration peuvent mener à la vulnérabilité de la sécurité. × Peut être difficile à configurer pour les débutants × Peut nécessiter des ressources matérielles supplémentaires pour gérer des charges élevées de trafic web × Les mises à jour de sécurité peuvent être retardées en raison du processus de développement open source
IIS (Internet Information Server) de Microsoft. *Il est souvent utilisé pour les sites web à faible charge de trafic tels que les sites d'entreprise, les sites d'informations, etc.*	✓ Sécurisé et flexible. ✓ Architecture ouverte qui le rend évolutif et polyvalent. ✓ Intégré au système d'exploitation Windows ✓ Dispose de divers outils de gestion pour déployer et gérer des sites Web. ✓ IIS est le seul serveur Web capable d'héberger des applications ASP.NET sans nécessiter de logiciel supplémentaire. ✓ Prend en charge plusieurs protocoles de communication tels que HTTP, HTTPS, FTP, SMTP, etc.	× Ne fonctionne que sur les systèmes d'exploitation Windows × Peut ne pas être adapté aux sites web à haute performance avec une charge élevée de trafic × Les mises à jour de sécurité peuvent être retardées en raison du processus de développement propriétaire de Microsoft

Nginx *Il est souvent utilisé pour les sites web à haute charge de trafic tels que les sites de médias sociaux, les sites de commerce électronique, les sites de streaming, etc.*	✓ Conçu pour gérer les sites web à haute performance avec une charge élevée de trafic. ✓ Peut être facilement personnalisé avec des modules tiers. ✓ Prend en charge plusieurs protocoles de communication tels que HTTP, HTTPS, SMTP, POP3, etc. ✓ Disponible gratuitement et open source.	× Peut être difficile à configurer pour les débutants. × Peut nécessiter des ressources matérielles supplémentaires pour gérer des charges élevées de trafic web. × Les mises à jour de sécurité peuvent être retardées en raison du processus de développement open source.
Node.Js *Il est souvent utilisé pour les applications web à haute performance telles que les applications de streaming en temps réel, les applications de chat, etc.*	✓ Conçu pour les applications web à haute performance. ✓ Peut être facilement personnalisé avec des modules tiers. ✓ Disponible gratuitement et open source. ✓ Peut être utilisé pour exécuter des applications de backend et de frontend.	× Peut nécessiter des compétences en développement JavaScript pour la configuration et la personnalisation. × Peut ne pas être adapté aux sites web à faible charge de trafic. × Les mises à jour de sécurité peuvent être retardées en raison du processus de développement open source.
Web Lighttpd *Il est souvent utilisé pour les sites web à faible charge de trafic tels que les sites de développement, les blogs personnels, etc.*	✓ Conçu pour être léger et rapide. ✓ Peut gérer des charges de trafic légères à moyennes. ✓ Peut être facilement personnalisé avec des modules tiers. ✓ Disponible gratuitement et open source.	× Peut ne pas être adapté aux sites web à haute performance avec une charge élevée de trafic. × Peut être difficile à configurer pour les débutants. × Les mises à jour de sécurité peuvent être retardées en raison du processus de développement open source.

Job 04

Les étapes pour mettre en place un DNS :

#Installer bind9

```
sudo apt install bind9
```

#Faire une Màj si nécessaire

```
sudo apt update && apt upgrade
```

#Configurer un forwarder en y ajoutant l'adresse IP du serveur, pour cela on va modifier named.conf.options avec la commande.

```
sudo nano /etc/bind/named.conf.options
```

Modifier aussi la partie listen-on-v6 en écrivant « ::1 » :

```
 GNU nano 7.2                        /etc/bind/named.conf.options
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        // forwarders {
                192.168.229.128
                8.8.8.8;
         };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
                                [ Lecture de 25 lignes ]
          //========================================================================>
          // If BIND logs error messages about the root key being expired,
          // you will need to update your keys.  See https://www.isc.org/bind-keys
          //========================================================================>
          dnssec-validation auto;

          listen-on-v6 { ::1; };
};
```

#Héberger notre propre zone en tant que serveur maître, pour cela on va modifier le fichier named.conf.local avec la commande :

```
sudo nano /etc/bind/named.conf.local
```

#Déclarer une zone nommée « dnsproject.prepa.com ». Pour cela écrire dans le fichier :

```
//
// Do any local configuration here
//

        zone "dnsproject.prepa.com" IN {
                type master;
                file "/etc/bind/dnsproject.prepa.com";
        };

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
```

#Créer le fichier « dnsproject.prepa.com » en se basant sur le fichier db.local avec la commande suivant :

```
sudo cp /etc/bind/db.local /etc/bind/dnsproject.prepa.com
```

#Editer le fichier « dnsproject.prepa.com » avec :

```
nano /etc/bind/dnsproject.prepa.com
```

#Définir le SOA (Start Of Authority, en remplaçant les éléments du fichier db.local sans oublier de supprimer la ligne «@ IN AAA ::1 »

```
 GNU nano 7.2                          db.local
;
; 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      localhost.
@       IN      A       127.0.0.1
@       IN      AAAA    ::1
```

```
 GNU nano 7.2                          dnsproject.prepa.com
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns.dnsproject.prepa.com root.dnsproject.prepa.com. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns.dnsproject.prepa.com.
ns      IN      A       192.168.229.128
```

Ip de notre serveur

#Editer le fichier hosts avec la commande suivante :

```
sudo nano /etc/hosts
```

#Dans le fichier hosts, ajouter l'adresse IP et le DNS du serveur

```
  GNU nano 7.2                                /etc/hosts
127.0.0.1       localhost
127.0.1.1       debian
192.168.229.128 dnsproject.prepa.com

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

#Réaliser in ping avec le nom de domaine

ping dnsproject.prepa.com

```
rija@debian:/etc/bind$ ping dnsproject.prepa.com
PING dnsproject.prepa.com (192.168.229.128) 56(84) bytes of data.
64 bytes from dnsproject.prepa.com (192.168.229.128): icmp_seq=1 ttl=64 time=1.42 ms
64 bytes from dnsproject.prepa.com (192.168.229.128): icmp_seq=2 ttl=64 time=0.046 ms
64 bytes from dnsproject.prepa.com (192.168.229.128): icmp_seq=3 ttl=64 time=0.025 ms
64 bytes from dnsproject.prepa.com (192.168.229.128): icmp_seq=4 ttl=64 time=0.029 ms
^C
--- dnsproject.prepa.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3038ms
rtt min/avg/max/mdev = 0.025/0.380/1.422/0.601 ms
```

Job 05

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

Pour obtenir un nom de domaine public informatique, suivez ces étapes simples :

- Choisissez un site web pour enregistrer votre nom de domaine, comme GoDaddy ou Namecheap.
- Vérifiez si le nom de domaine que vous souhaitez est disponible en utilisant leur outil de recherche.
- Sélectionnez l'extension de domaine qui convient à votre projet (par exemple, .com, .net, .org).
- Ajoutez le nom de domaine à votre panier et procédez au paiement.
- Configurez les enregistrements DNS pour rediriger le trafic vers votre site Web.
- Assurez-vous de renouveler le domaine chaque année pour le garder.

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

Concernant les spécificités des extensions de domaine, voici quelques points à considérer :

1. Extensions génériques (.com, .org, .net, etc.) : Ce sont les extensions de domaine les plus courantes et peuvent être enregistrées par presque tout le monde. Elles sont adaptées à une utilisation générale.

2. Extensions géographiques (ccTLDs) : Ces extensions sont associées à des pays ou des territoires spécifiques (par exemple, .fr pour la France, .uk pour le Royaume-Uni). Les règles d'enregistrement et les spécificités peuvent varier d'un ccTLD à l'autre. Certaines extensions géographiques ont des restrictions de résidence ou d'entreprise dans le pays correspondant.

3. Extensions de domaine de premier niveau (gTLDs) spécifiques : Il existe également des gTLDs spécifiques qui ont été introduits ces dernières années, tels que .app, .blog, .guru, .io, .dev, etc. Ces gTLDs offrent des options plus spécifiques pour les entreprises et les sites web.

4. Extensions restreintes : Certaines extensions, comme .gov et .edu, sont réservées à des types d'entités spécifiques et nécessitent une vérification de l'éligibilité pour l'enregistrement.

Chaque extension de domaine peut avoir ses propres règles, exigences et politiques, il est donc important de les vérifier auprès du registrar ou de l'organisme qui gère l'extension que vous envisagez d'utiliser.

Job 06

Connectez votre hôte au nom de domaine local de votre serveur, pour que votre page apache soit accessible via ce même nom de domaine.

Dans un premier lieu, vérifier que l'hôte communique avec le serveur en réalisant un PING sur le terminal Windows PowerShell:

ping 192.168.229.128

Ici notre hôte communique bien avec le serveur

```
PS C:\Users\rijar\Desktop> ping 192.168.229.128

Envoi d'une requête 'Ping'  192.168.229.128 avec 32 octets de données :
Réponse de 192.168.229.128 : octets=32 temps=4 ms TTL=64
Réponse de 192.168.229.128 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.229.128 : octets=32 temps<1ms TTL=64
Réponse de 192.168.229.128 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.229.128:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 4ms, Moyenne = 1ms
```

Dans le dossier etc C:\Windows\System32\drivers\etc, modifier le fichier « hosts » afin d'ajouter l'adresse IP et le nom du serveur :

192.168.229.128 dnsproject.prepa.com

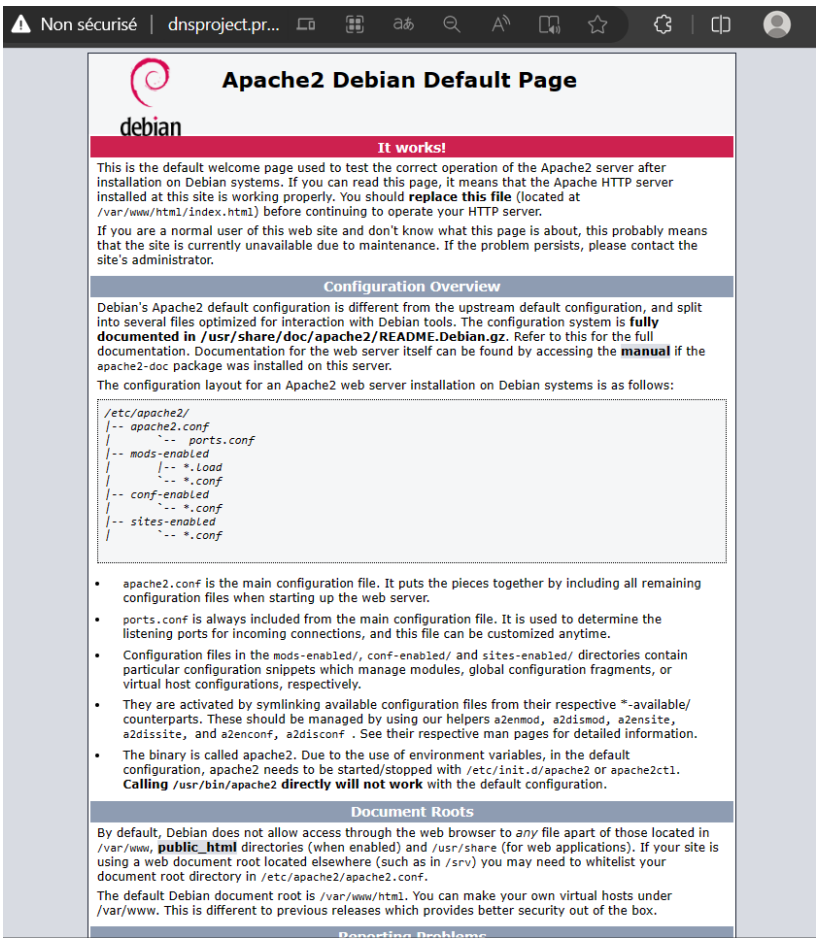
Enregistrer les modifications, puis fermer.

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
       192.168.229.128 dnsproject.prepa.com
```

Rentrer « http://dnsproject.prepa.com/ » dans votre navigateur internet.

Une page Apache2 s'affiche



Job 07

Mettez en place un pare-feu en utilisant ufw sur votre serveur principal de manière que votre hôte puisse accéder à la page apache par défaut, mais qu'il ne puisse plus ping votre serveur.

#Installer ufw

```
sudo apt istall ufw
```

#Faire une Màj si nécessaire

```
sudo apt update && apt upgrade
```

#Activer ufw

```
sudo ufw enable
```

```
#Tester si Debian et le serveur peuvent toujours communiquer
ping 192.168.229.128
```

#Modifier le fichier 'before.rules' situé dans le repertoire ufw

```
cd /etc/ufw/
sudo nano before.rules
```

#Dans la partie '#ok icmp codes for INPUT', passer les lignes de ACCEPT à 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
```

#Recharger ufw

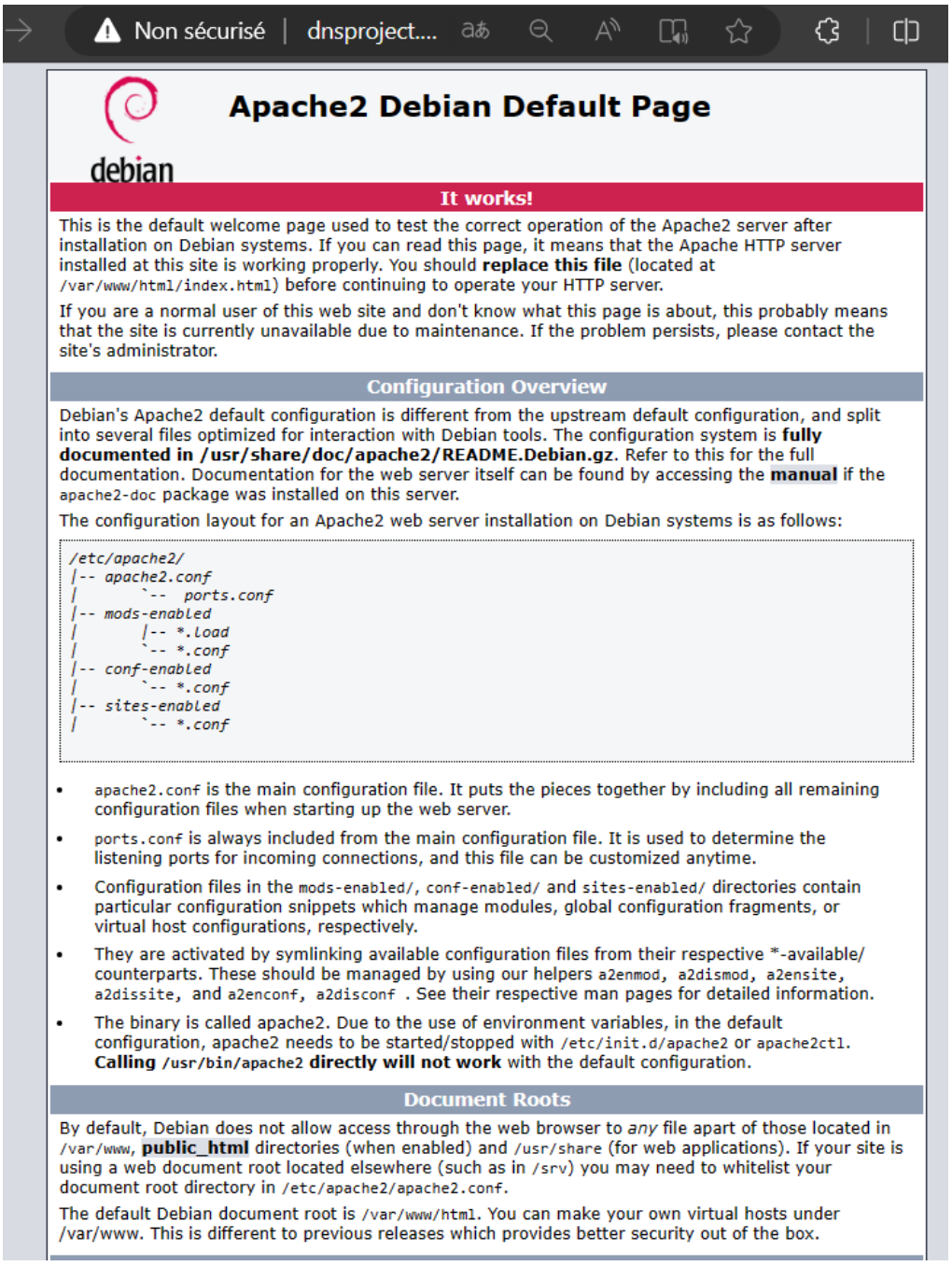
```
sudo ufw reload
```

Je vérifie que l'hôte puisse accéder à la page du serveur mais ne puisse pas réaliser de ping.

```
PS C:\Users\rijar\Desktop> ping 192.168.229.128

Envoi d'une requête 'Ping'  192.168.229.128 avec 32 octets de données :
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.229.128:
    Paquets : envoyés = 1, reçus = 0, perdus = 1 (perte 100%),
Ctrl+C
PS C:\Users\rijar\Desktop>
```

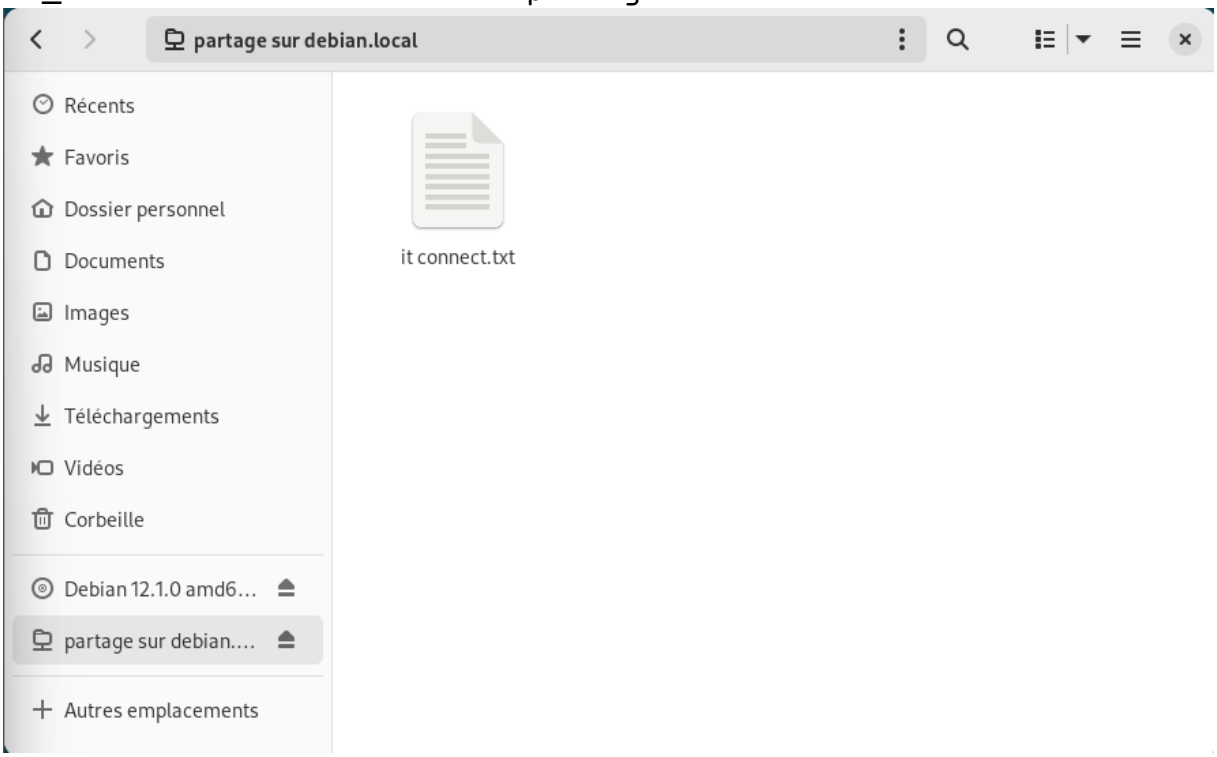


Job 08

Mettez en place sur votre serveur un dossier partagé avec les autres membres de votre réseau (soit la où les autres machines virtuelles). Ils pourront partager des fichiers dans ce dossier, ainsi que récupérer des fichiers depuis ce dossier.

Ce dossier doit être accessible dans votre gestionnaire de fichier en interface graphique.

Pour cet exercice, j'ai au préalables créé un fichier it_connect dans le dossier partage de ma VM




```
#Mettre à jour la liste des paquets
apt-get update


#Installer le paquet « samba »
apt-get install -y samba


#Afficher la version actuelle de Samba
sudo smbd -version
rija@debian:~$ sudo smbd --version
[sudo] Mot de passe de rija :
Version 4.17.12-Debian


#activer le démarrage automatique de smbd
sudo systemctl enable smbd
```

#afficher le statut de Samba pour voir s'il est démarré ou arrêté

```
sudo systemctl status smbd
```

```
rija@debian:~$ systemctl status smbd
● smbd.service - Samba SMB Daemon
     Loaded: loaded (/lib/systemd/system/smbd.service; enabled; preset: enabled)
     Active: active (running) since Fri 2023-10-27 09:07:17 CEST; 47min ago
```

##Configurer le partage dans smb.conf
#ouvrir le fichier smb.conf

```
sudo nano /etc/samba/smb.conf
```

#Ajoutez les lignes suivantes pour déclarer notre partage (explication des lignes disponible à la fin du job)

```
[partage]
     comment = Partage de données
     path = /srv/partage
     guest ok = no
     read only = no
     browseable = yes
     valid users = @partage
```

#Sauvegarder le fichier et redémarrer le service smbd

```
sudo systemclt restart smbd
```

##Créer un utilisateur et le groupe « partage »
#Créer l'utilisateur « it_connect »

```
sudo adduser it_connect
```

#Déclarer l'utilisateur et lui créer un mot de passe Samba

```
sudo smbpasswd -a -it-connect
```

#Créer le groupe « partage »

```
sudo groupadd partage
```

#Ajout de l'utilisateur « it_connect » au groupe « partage »

```
sudo gpasswd -a it-connect partage
```

##Préparer le dossier du partage
#Créer le dossier partage

```
sudo mkdir /srv/partage
```

#Attribuer le groupe « partage » comme groupe propriétaire de ce dossier

```
sudo chgrp -R partage /srv/partage/
```

#Ajouter les droits de lecture/écriture à ce groupe sur ce dossier

```
sudo chmod -R g+rw /srv/partage/
```

#Vérifier la configuration des droits

```
ls -l /srv/
```

```
rija@debian:~$ ls -l /srv/
total 4
drwxrwxr-x 2 root partage 4096 26 oct.  22:56 partage
```

##Afin d'éviter de désactiver le Firewall lorsque l'on souhaite accéder au dossier partage, activer le port 139 et le port 145 (explication du port 139 disponible à la fin du job)

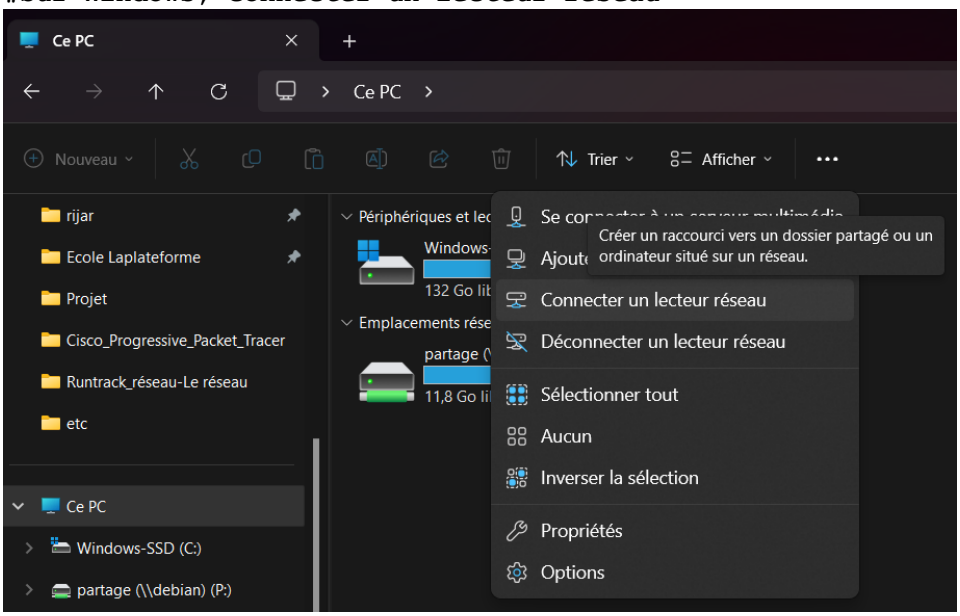
#Activer le port 139

```
sudo ufw allow 139
```

#Activer le port 445

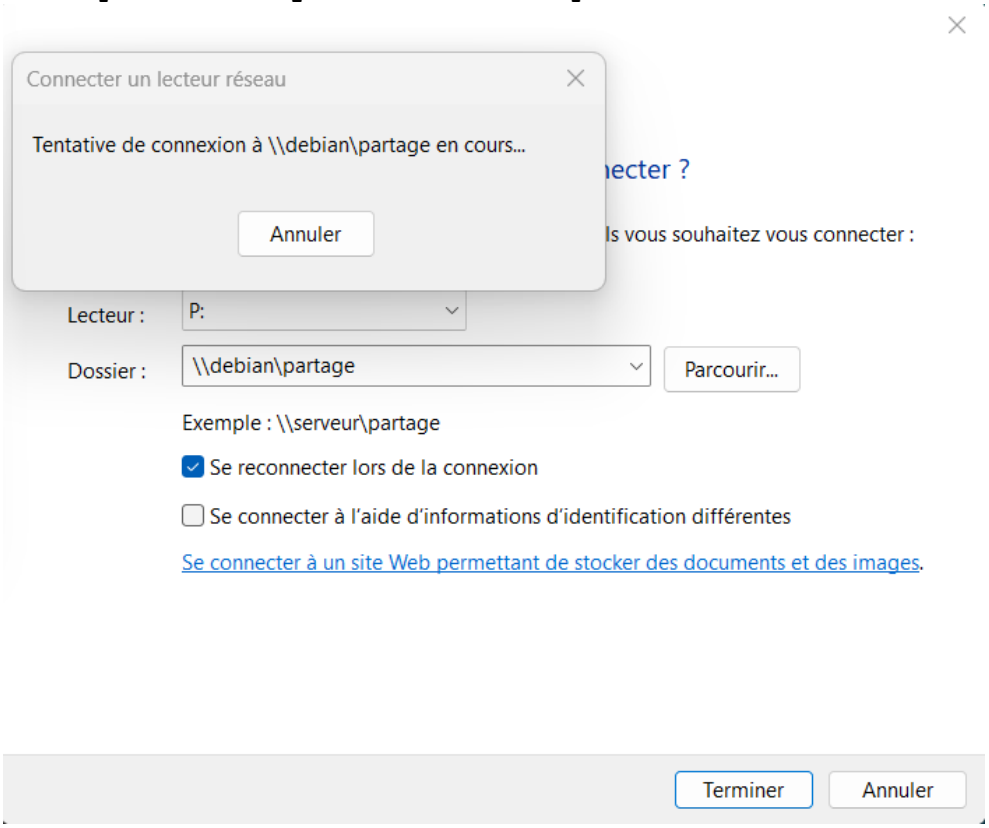
```
sudo ufw allow 445
```

#Sur Windows, connecter un lecteur réseau

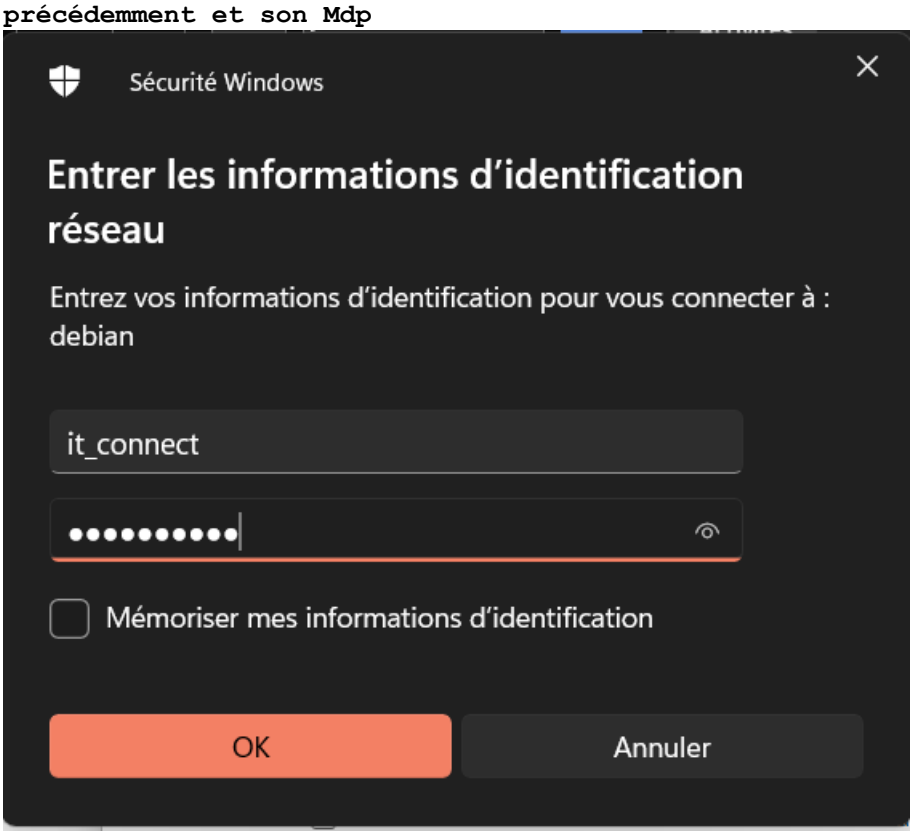


#Dans la partie Lecteur a), selectionner un lecteur. Ici j'ai choisi le lecteur P: (petit rappel pour le « P » de partage), j'aurais pu prendre n'importe lequel.
Dans la partie Dossier b), mettre le nom de la machine et le nom du dossier

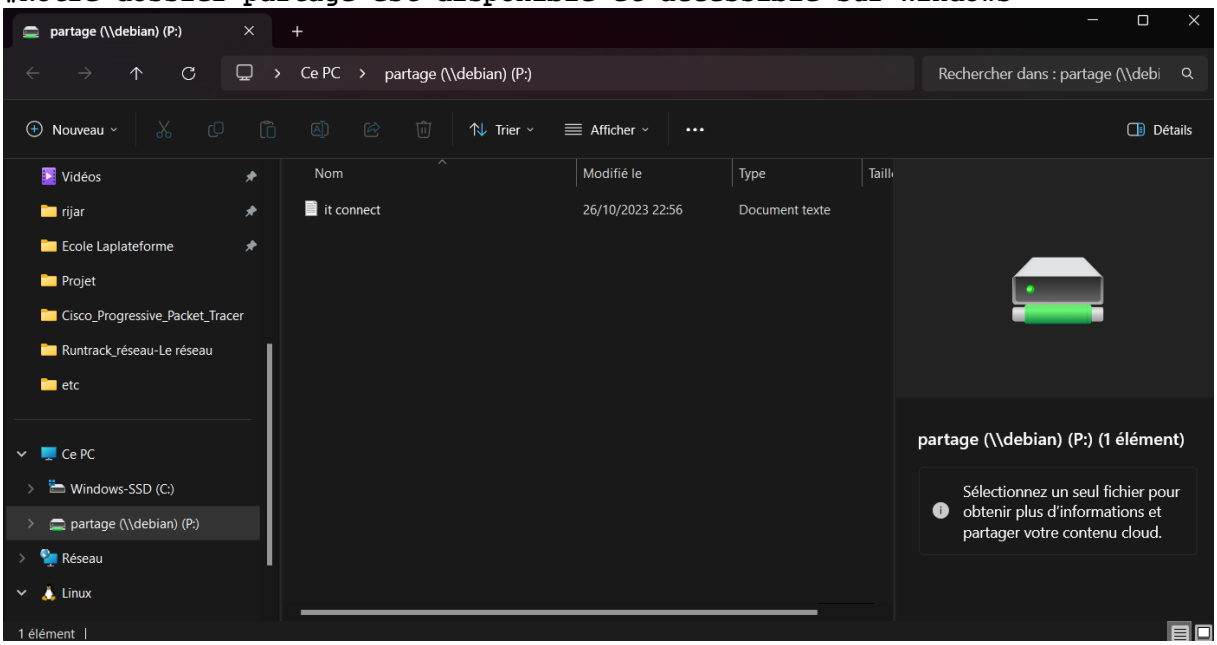
en respectant la syntaxe comme indiqué ci-dessous.



#Une fenêtre va s'ouvrir, rentrer l'identifiant it_connect créer précédemment et son Mdp



#Notre dossier partage est disponible et accessible sur Windows



Les explications :

```
[partage]
    comment = Partage de données
    path = /srv/partage
    guest ok = no
    read only = no
    browseable = yes
    valid users = @partage
```

- **[partage]** : sert à spécifier le nom du partage entre "[]", c'est le nom qui devra être utilisé pour accéder au partage
- **comment** : description du partage
- **path** : chemin vers le dossier à partager, sur le serveur
- **guest ok** : accès invité au partage (par défaut "*no*"). Si vous décidez d'activer cette option, vous devez configurer l'option "*guest account*" qui par défaut prend la valeur "*nobody*".
- **read only** : partage accessible uniquement en lecture seule (*yes* ou *no*)
- **browseable** : le partage doit-il être visible ou masqué si on liste les partages du serveur avec un hôte distant (découverte réseau). La valeur "*yes*" permet de le rendre visible.
- **valid users** : spécifier les utilisateurs ou les groupes qui ont les droits d'accès au partage (*les droits sur le système de fichiers doivent être cohérents vis-à-vis de cette autorisation*). On précise un utilisateur avec son identifiant et un groupe avec son identifiant précédé du caractère "@". Pour indiquer plusieurs valeurs, séparez-les par une virgule.

Qu'est-ce que le port 139 ?

Le port 139 est un port TCP qui fonctionne lorsque vous accédez à un fichier partagé ou à un e imprimante partagée sur votre réseau local via votre voisinage réseau.
Si le port 139 est exploité par un attaquant sur Internet, il peut devenir une grave faille de sé curité. Si un pirate établit une connexion avec le port 139 de l'hôte cible, il est possible de pa rcourir toutes les informations partagées sur tous les postes de travail du segment de réseau spécifié, et même de modifier et de supprimer les dossiers partagés sur l'hôte cible. Si l'attaq uant connaît également l'adresse IP et le compte de connexion de l'hôte cible, les informatio ns partagées cachées sur l'hôte cible peuvent être facilement visualisées.

Qu'est-ce que le port 445

Le port 445 est également un port TCP qui fonctionne exactement comme le port 139 sur un système Windows 2000 Server ou Windows Server 2003. Plus précisément, il fournit égale ment des services de partage de fichiers ou d'imprimantes sur le réseau local. Cependant, ce port fonctionne sur la base du protocole CIFS (protocole de système de fichiers Internet com mun), tandis que le port 139 fournit des services de partage basés sur le protocole SMB (suit e de protocoles de serveur). De même, un attaquant peut obtenir diverses informations part agées dans un réseau local spécifié en établissant une connexion de demande avec le port 44 5.
Pour désactiver le partage de fichiers, désactivez les ports 139 et 445.