

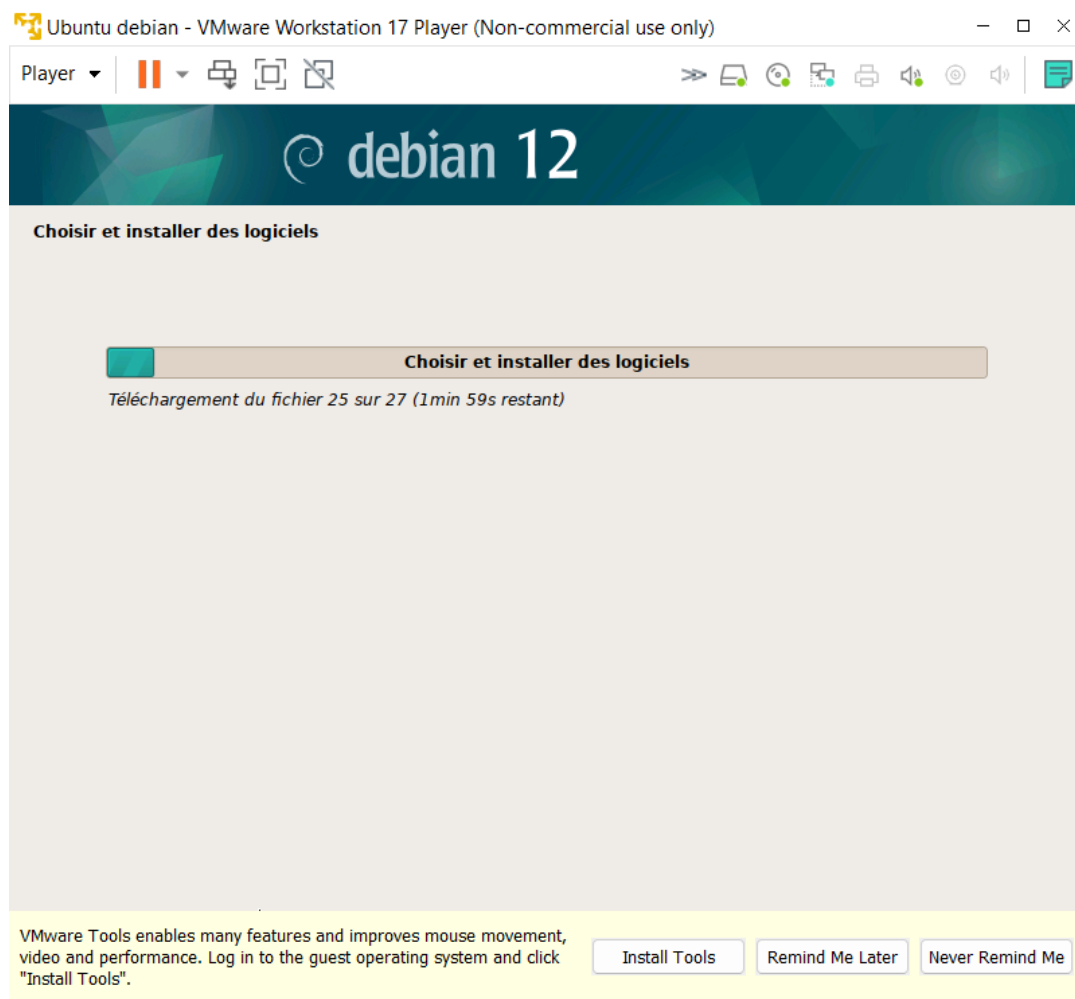


DDWS

Manon RITTLING

Job 01

Pour installer Debian en vm, ouvrir vm ware et crée une nouvelle vm avec le fichier iso de debian.



Job 02

Pour installer un serveur Web Apache2, voici les commandes :

Trouver l'adresse ip

Commande pour voir son adresse IP

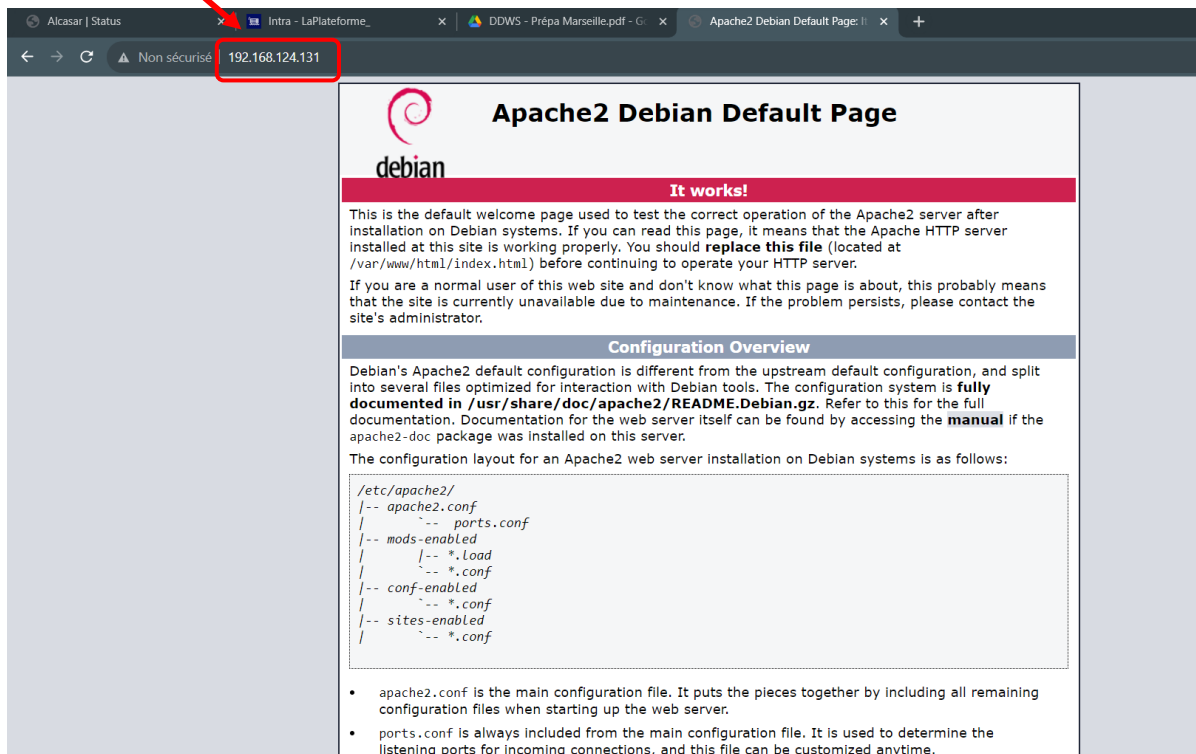
```
manon@debian: /etc/bind$ nmcli -p device show
=====
                Détails de périphérique (ens33)
=====
GENERAL.DEVICE:                ens33
-----
GENERAL.TYPE:                  ethernet
-----
GENERAL.HWADDR:                00:0C:29:3C:C2:B7
-----
GENERAL.MTU:                   1500
-----
GENERAL.STATE:                 100 (connecté)
-----
GENERAL.CONNECTION:            Wired connection 1
-----
GENERAL.CON-PATH:              /org/freedesktop/NetworkManager/ActiveC
-----
WIRED-PROPERTIES.CARRIER:     marche
```

Et faire les commandes surligner en vert pour installer le serveur apache2

```
root@debian:~# apt update && apt upgrade
Atteint :1 http://security.debian.org/debian-security bookworm-security InRelease
Atteint :2 http://deb.debian.org/debian bookworm InRelease
Atteint :3 http://deb.debian.org/debian bookworm-updates InRelease
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Tous les paquets sont à jour.
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Calcul de la mise à jour... Fait
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
root@debian:~# apt install apache2
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
apache2 est déjà la version la plus récente (2.4.57-2).
apache2 passé en « installé manuellement ».
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
```

Vérifions l'accessibilité de notre serveur apache depuis notre navigateur

mettre cette adresse IP dans chrome sur notre Windows et apache 2 s'ouvre



Job 03

Renseignez-vous sur les différents serveurs Web existants et produisez une documentation qui contiendra votre recherche ainsi que les avantages et inconvénients de chacun des serveurs.

SERVEUR	AVANTAGES	INCONVENIENTS
<p>APACHE HTTP</p> <p><i>Il est conçu pour gérer des sites web statiques et dynamiques.</i></p>	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • Problèmes de performances sur les sites web avec un énorme trafic. • Trop d'options de configuration peuvent mener à la vulnérabilité de la sécurité.

	<ul style="list-style-type: none"> • Prend en charge plusieurs protocoles de communication tels que HTTP, HTTPS, FTP, etc. 	
<p>IIS (Internet Information Server) de Microsoft</p> <p><i>Il est souvent utilisé pour les sites web à faible charge de trafic tels que les sites d'entreprise, les sites d'informations</i></p>	<ul style="list-style-type: none"> • Sécurisé et flexible • Architecture ouverte qui le rend évolutif et polyvalent • Facile à configurer et a utilisé • Intégré au système d'exploitation Windows • Comprend divers outils pour déployer et gérer des sites web.(ISM gestionnaire de services internet et GUI pour la gestion des paramètres IIS) • Il est le seul serveur Web capable d'héberger des applications ASP.NET sans avoir un logiciel supplémentaire • Prend en charge plusieurs protocoles de communication tels que HTTP, HTTPS, FTP, SMTP, etc. 	<ul style="list-style-type: none"> • 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
<p>NGINX</p> <p><i>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.</i></p>	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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
<p>WEB LIGHTTPD</p> <p><i>Il est souvent utilisé pour les sites web à faible charge de trafic tels que les sites de développement, les blogs personnels, etc.</i></p>	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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
<p>WEB NODE.JS</p> <p><i>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.</i></p>	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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

Job 04

Mettez en place un DNS sur votre serveur Linux qui fera correspondre l'adresse IP de votre serveur au nom de domaine local suivant : "dnsproject.prepa.com". Votre serveur devra donc pouvoir se ping via ce nom de domaine.

Voici les étapes pour mettre en place un DNS sur notre serveur Linux :

1. Installer les paquets bind9 avec la commande : apt install bind9

```
root@debian:~# apt install bind9
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
0 mis à jour, 2 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 900 ko dans les archives.
```

2. On va déclarer la zone en allant dans le fichier **named.conf.local**
Faire la commande suivante :

```
manon@debian: /etc/bind$ sudo nano named.conf.local
```



```
GNU nano 7.2      named.conf.local
//
// 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";

[ Lecture de 12 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
```

Ajouté le texte surligné dans le fichier **named.conf.local**

3. Puis il faut créer le fichier `/etc/bind/dnsproject.prepa.com`. Pour cela on va copier `db.local` qui sert de référence avec la commande suivante :

```
manon@debian:/etc/bind$ sudo cp /etc/bind/db.local /etc/bind/dnsproject.prepa.com
```

4. Editez le fichier `named.conf.options` et modifier en ajoutant l'adresse IP du serveur

```
// forwarders {  
    192.168.124.131;  
    8.8.8.8;  
};
```

Adresse IP du serveur Apache

Adresse IP utilisée par Google pour son service DNS public

```
//=====  
// 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  
//=====
```

5. Modifier de `listen-on-v6` passer `{ any; }` à `{ ::1; }` dans le fichier `named.conf.options`

```
dnssec-validation auto;
```

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

Permet de prendre en compte IPV4 et IPV6

6. Editez et modifier le fichier

```
manon@debian:/etc/bind$ sudo nano /etc/bind/dnsproject.prepa.com
```

Fichier original

```
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
```

Fichier modifié

```
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.  
@ IN A 192.168.229.128  
@ IN AAAA ::1
```

7. Editez le fichier hosts avec la commande suivante et ajouter adresse IP du serveur et son nom domaine

```
manon@debian:/etc/bind$ sudo nano /etc/hosts
```

```
GNU nano 7.2 /etc/hosts
127.0.0.1    localhost
127.0.1.1    debian
192.168.124.131 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
```

Ajouter adresse IP et nom de domaine

[Lecture de 7 lignes]

^G Aide	^O Écrire	^W Chercher	^K Couper	^T Exécuter	^C Emplacement
^X Quitter	^R Lire fich.	^M Remplacer	^U Coller	^J Justifier	^_ Aller ligne

8. Faire un ping avec le nom du domaine

```
manon@debian:/etc/bind$ sudo ping dnsproject.prepa.com
PING dnsproject.prepa.com (192.168.124.131) 56(84) bytes of data.
64 bytes from dnsproject.prepa.com (192.168.124.131): icmp_seq=1 ttl=64 time=0.019 ms
64 bytes from dnsproject.prepa.com (192.168.124.131): icmp_seq=2 ttl=64 time=0.025 ms
64 bytes from dnsproject.prepa.com (192.168.124.131): icmp_seq=3 ttl=64 time=0.027 ms
64 bytes from dnsproject.prepa.com (192.168.124.131): icmp_seq=4 ttl=64 time=0.022 ms
64 bytes from dnsproject.prepa.com (192.168.124.131): icmp_seq=5 ttl=64 time=0.024 ms
^C
--- dnsproject.prepa.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4094ms
rtt min/avg/max/mdev = 0.019/0.023/0.027/0.002 ms
```


Job 05

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

Pour obtenir un nom de domaine public informatique, voici les étapes à suivre :

1. Choisissez un site web pour enregistrer votre nom de domaine.
2. Vérifiez si le nom de domaine est disponible en utilisant leur outil de recherche fourni par le registrar.
3. Sélectionnez l'extension de domaine qui convient à votre projet, exemple, .com, .net, .org.
4. Ajoutez le nom de domaine à votre panier et procédez au paiement sur le site de registrar.
5. Configurez les DNS pour rediriger le trafic vers votre site Web.
6. 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 ?

1. .com : C'est l'une des plus populaires et est généralement utilisée pour des sites Web commerciaux, mais elle est assez polyvalente et peut être utilisée pour divers types de sites.
2. .fr : C'est spécifique à la France. Pour obtenir un nom de domaine .fr, vous devez avoir un lien avec la France, comme une adresse en France.
3. .org : Elle était associée aux organisations à but non lucratif, mais elle est aujourd'hui ouverte à un usage plus général.
4. .net : C'était initialement destinée aux entreprises liées à Internet et aux infrastructures réseau, bien qu'elle soit également utilisée pour d'autres types de sites.
5. .gov : Elle est réservée aux entités gouvernementales des États-Unis. D'autres pays ont des extensions similaires pour leurs organismes gouvernementaux.
6. .io : Elle est couramment utilisée par des entreprises technologiques et des startups, bien qu'elle soit en réalité l'extension de l'île britannique de l'océan Indien.
7. .app : L'extension .app est conçue pour les applications mobiles et les logiciels, et elle peut exiger HTTPS pour des raisons de sécurité.
8. .dev : L'extension .dev est souvent utilisée pour les sites Web de développement, de programmation et de technologies.

Job 06

Pour se connecter avec le nom de domaine local de notre serveur DNS, il suffit de faire les étapes suivantes :

D'abord vérifié dans le terminal de Windows et faire PING avec l'adresse IP du serveur :

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

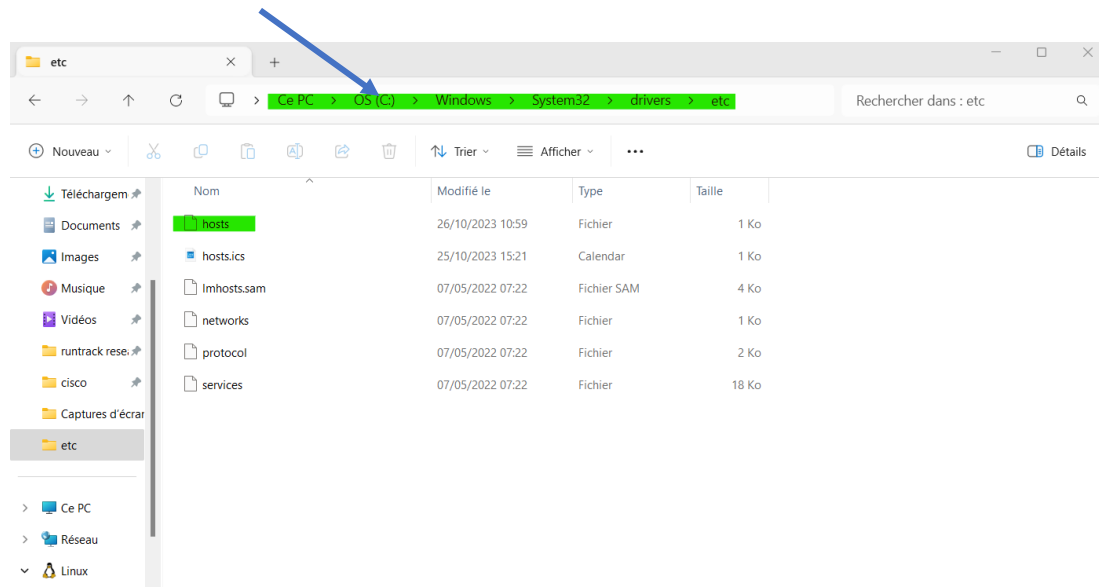
Installez la dernière version de PowerShell pour de nouvelles fonctionnalités et améliorations ! https://aka.ms/PSWindows

PS C:\Users\rittl> ping 192.168.124.131

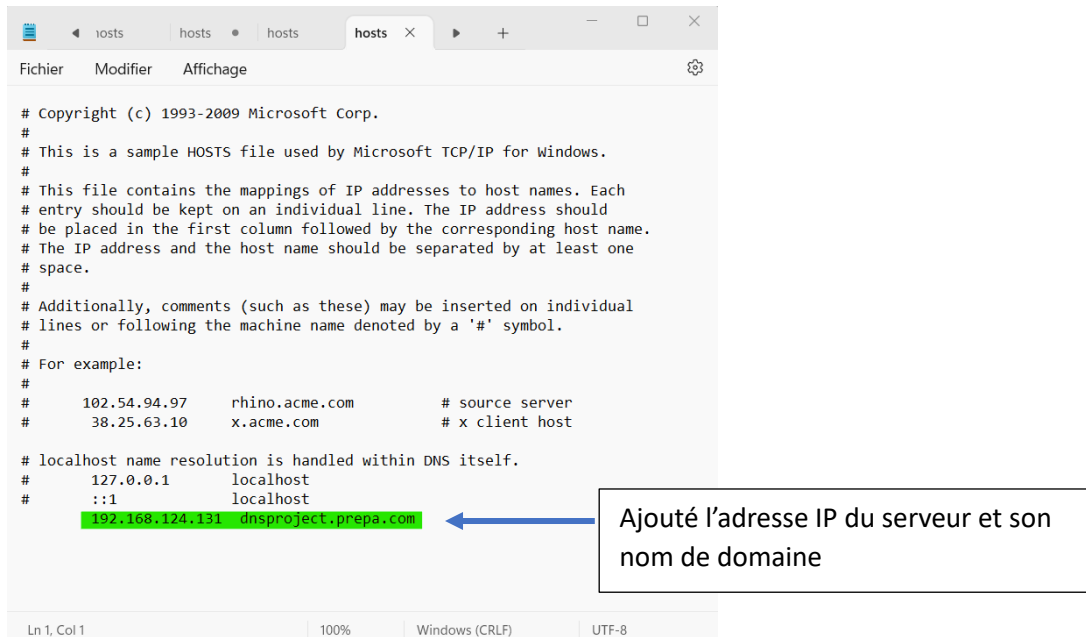
Envoi d'une requête 'Ping' 192.168.124.131 avec 32 octets de données :
Réponse de 192.168.124.131 : octets=32 temps<1ms TTL=64
Réponse de 192.168.124.131 : octets=32 temps<1ms TTL=64
Réponse de 192.168.124.131 : octets=32 temps=2 ms TTL=64

Statistiques Ping pour 192.168.124.131:
    Paquets : envoyés = 3, reçus = 3, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 2ms, Moyenne = 0ms
    Ctrl+C
PS C:\Users\rittl>
```

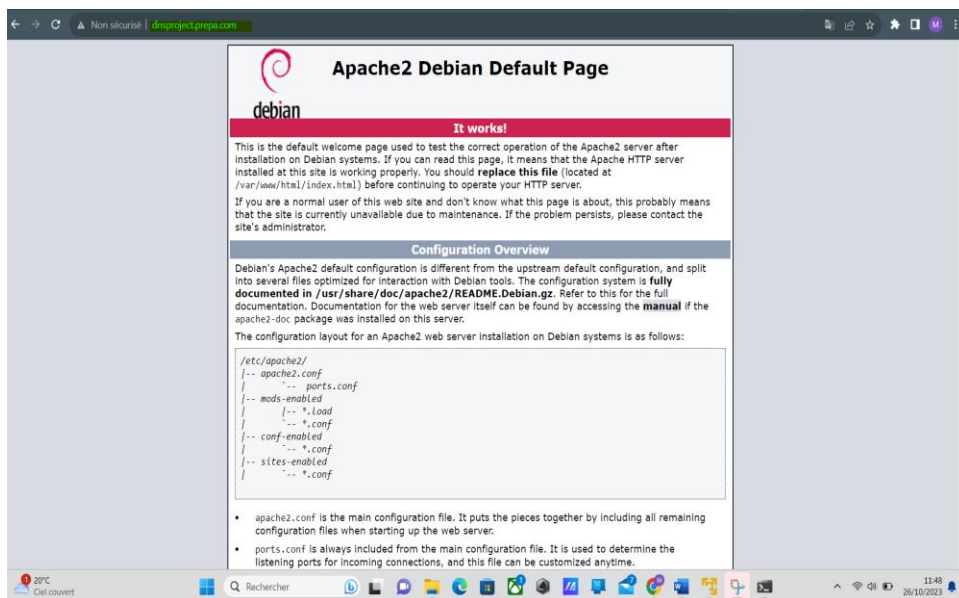
Puis suivre le chemin ci-dessous toujours sur notre windows



Modifié le fichier Hosts



Allé sur chrome et taper le nom de domaine pour ouvrir la page Apache2



Job 07

Pour mettre en place un pare-feu ufw tout d'abord se mettre en root et installer les paquets ufw

```
root@debian:~# sudo 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] o
Réception de :1 http://deb.debian.org/debian bookworm/main amd64 libip6tc2 amd64 1.8.9-2 [19,4 kB]
Réception de :2 http://deb.debian.org/debian bookworm/main amd64 iptables amd64 1.8.9-2 [360 kB]
Réception de :3 http://deb.debian.org/debian bookworm/main amd64 ufw all 0.36.2-1 [168 kB]
548 ko réceptionnés en 1s (885 ko/s)
Préconfiguration des paquets...
Sélection du paquet libip6tc2:amd64 précédemment désélectionné.
(Lecture de la base de données... 166057 fichiers et répertoires déjà installés.)
```

Commande pour installer UFW

Activé Ufw :

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

Editez le fichier before.rules qui permet de configurer les règles du firewall

```
manon@debian:~$ cd /etc/ufw
manon@debian:/etc/ufw$ sudo nano before.rules
manon@debian:/etc/ufw$ ping 192.168.124.131
PING 192.168.124.131 (192.168.124.131) 56(84) bytes of data.
64 bytes from 192.168.124.131: icmp_seq=1 ttl=64 time=0.054 ms
64 bytes from 192.168.124.131: icmp_seq=2 ttl=64 time=0.072 ms
64 bytes from 192.168.124.131: icmp_seq=3 ttl=64 time=0.073 ms
64 bytes from 192.168.124.131: icmp_seq=4 ttl=64 time=0.075 ms
64 bytes from 192.168.124.131: icmp_seq=5 ttl=64 time=0.069 ms
^C
--- 192.168.124.131 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4075ms
rtt min/avg/max/mdev = 0.054/0.068/0.075/0.007 ms
manon@debian:/etc/ufw$ sudo ufw reload
Firewall reloaded
manon@debian:/etc/ufw$
```

Commande pour éditer le before.rules

Recharge les nouvelles règles pour mettre à jour les modifications

Changer en DROP pour ne pas autoriser les pings entrants

```
# 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
```

```
# 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
```

Faire un ping sur le terminal Windows pour vérifier qui ne marche pas

```
PS C:\Users\rittl> ping 192.168.124.131
```

```
Envoi d'une requête 'Ping' 192.168.124.131 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
```

```
Statistiques Ping pour 192.168.124.131:
```

```
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
PS C:\Users\rittl>
```

Job 08

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

- Installer Samba sur Debian avec cette commande

```
manon@debian:~$ sudo apt install samba
```

- Vérifier si le service est bien activé

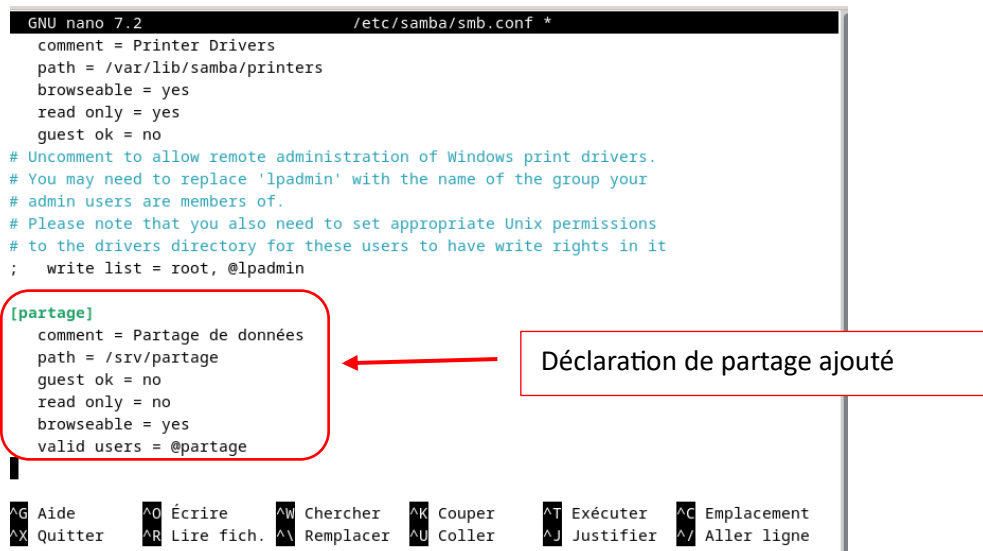
```
manon@debian:~$ sudo systemctl status smbd
● smbd.service - Samba SMB Daemon
   Loaded: loaded (/lib/systemd/system/smbd.service; enabled; preset: enabled)
   Active: active (running) since Thu 2023-10-26 14:49:39 CEST; 7min ago
```

- Et activé le démarrage automatique de samba avec cette commande

```
manon@debian:~$ sudo systemctl enable smbd
Synchronizing state of smbd.service with SysV service script with /lib/systemd/systemd-
sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable smbd
```

- Configurer le partage dans smb.conf

Pour se faire aller dans le fichier smb.conf et ajouter les lignes pour déclarer le partage



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

← Déclaration de partage ajouté

^G Aide ^O Écrire ^W Chercher ^K Couper ^T Exécuter ^C Emplacement
^X Quitter ^R Lire fich. ^M Remplacer ^U Coller ^J Justifier ^_ Aller ligne

Explication :

- **[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.

- Sauvegarder les modifications du fichier smb.conf

```
manon@debian:~$ sudo systemctl restart smb
```

- Ajouter un utilisateur

```
manon@debian:~$ sudo adduser sambatest
Ajout de l'utilisateur « sambatest » ...
Ajout du nouveau groupe « sambatest » (1001) ...
Ajout du nouvel utilisateur « sambatest » (1001) avec le groupe « sambatest » (1001) ..
.
Création du répertoire personnel « /home/sambatest » ...
Copie des fichiers depuis « /etc/skel » ...
Nouveau mot de passe :
Retapez le nouveau mot de passe :
Les mots de passe ne correspondent pas.
Mot de passe : Erreur de manipulation du jeton d'authentification
passwd : mot de passe inchangé
Essayer à nouveau ? [o/N]o
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
Modifier les informations associées à un utilisateur pour sambatest
Entrer la nouvelle valeur, ou appuyer sur ENTER pour la valeur par défaut
NOM []:
Numéro de chambre []:
Téléphone professionnel []:
Téléphone personnel []:
```

- Autoriser l'utilisateur dans Samba et lui attribuer un mot de passe

```
manon@debian:~$ sudo smbpasswd -a sambatest
New SMB password:
Retype new SMB password:
Added user sambatest.
```

- Maintenant nous allons créer le groupe « partage » et ajouter l'utilisateur au groupe partage

```
manon@debian:~$ sudo groupadd partage
manon@debian:~$ sudo gpasswd -a sambatest partage
Ajout de l'utilisateur sambatest au groupe partage
```

```
sambatest:x:1001:
partage:x:1002:sambatest
```

- Pour préparer le dossier partage, il suffit de créer un dossier sur le serveur, attribuer le groupe "partage" comme groupe propriétaire de ce dossier, puis ajouter les droits d'écriture et lecture au groupe puis vérifier

```
manon@debian:~$ sudo mkdir /srv/partage
manon@debian:~$ sudo chgrp -R partage /srv/partage/
manon@debian:~$ sudo chmod -R g+rw partage /srv/partage/
chmod: impossible d'accéder à 'partage': Aucun fichier ou dossier de ce type
manon@debian:~$ sudo chmod -R g+rw /srv/partage/
manon@debian:~$ ls -l /srv/
total 4
drwxrwxr-x 2 root partage 4096 26 oct. 15:55 partage
manon@debian:~$
```

- Faire le partage entre ma VM Debian et mon Windows.

Il faut ajouter à notre firewall le port 139 et 445 qui permet le partage des fichiers Windows. Ça nous permettra de ne pas désactiver notre firewall.

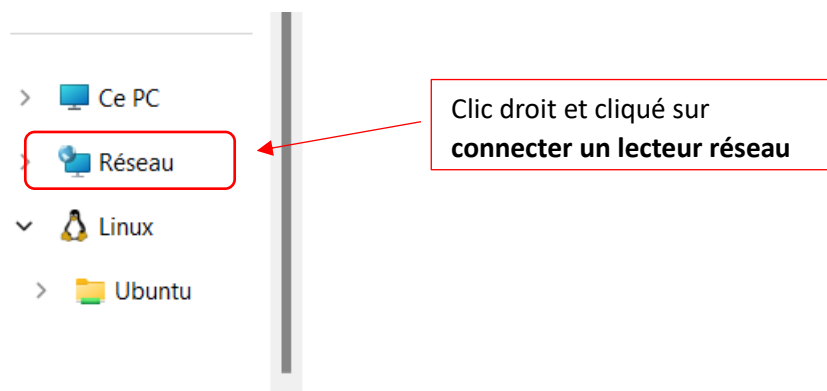
```
manon@debian:~$ sudo ufw allow 139
```

Le port 139 est associé au service de partage de fichiers Windows, appelé SMB (Server Message Block). En autorisant le port 139, vous permettez à d'autres ordinateurs de se connecter au vôtre pour partager des fichiers ou des imprimantes, généralement dans un réseau Windows.

```
manon@debian:~$ sudo ufw allow 445
```

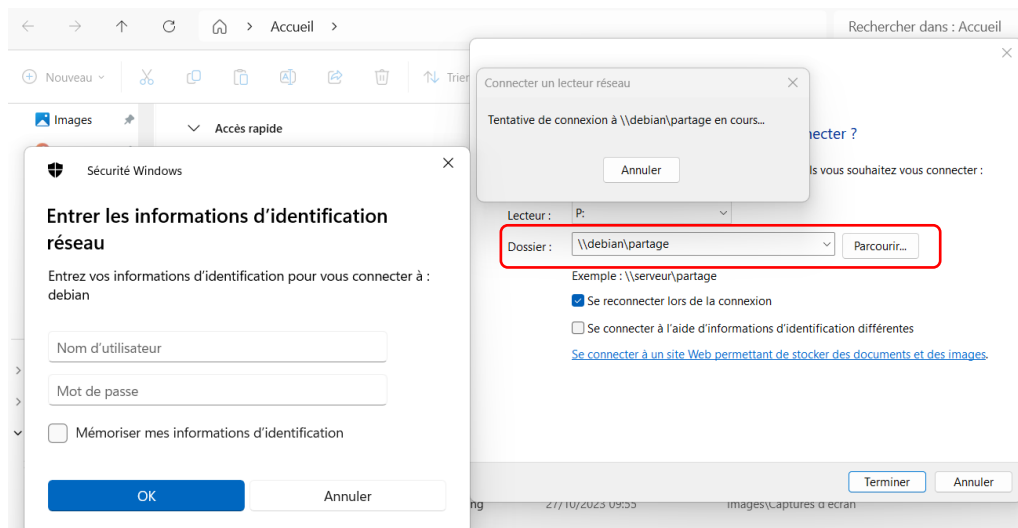
Le port 445 est utilisé pour partager des fichiers et des imprimantes sur un réseau, principalement avec des ordinateurs Windows. Il permet aux ordinateurs de se connecter pour accéder à des fichiers, des dossiers, des imprimantes, et d'autres ressources partagées. Il est également utilisé pour gérer des ordinateurs à distance et effectuer des tâches de maintenance.

Ensuite il suffit d'aller dans les paramètres de Windows



Dans connecter un lecteur réseau, choisir un lecteur disponible et mettre dans dossier le chemin avec le nom de la machine et le dossier partage.

Puis rentré le nom d'utilisateur que l'on a ajouté dans samba avec les autorisations pour le partage.



Pour aller plus loin...

Tout d'abord il faut s'assurer que openssl soit bien installé pour cela faire la commande suivante

```
manon@debian:~$ sudo openssl version
```

```
[sudo] Mot de passe de manon :
```

```
OpenSSL 3.0.11 19 Sep 2023 (Library: OpenSSL 3.0.11 19 Sep 2023)
```

- Ensuite généré une clé privée avec la commande suivante :

```
manon@debian:~$ sudo openssl genrsa -out dnsproject.prepa.com key 2048
```

Ça permet de générer une clé privée RSA et l'enregistré dans le fichier nommé **dnsproject.prepa.com.key** avec une longueur de clé de 2048 bits.

- Générez un certificat auto-signé

```
manon@debian:~$ openssl req -out dnsproject.prepa.com.crs -newkey rsa:2048 -nodes -keyout dnsproject.prepa.com.key
```

La commande crée un certificat SSL auto-signé avec une clé privée.

- Copiez le fichier avec la clé privé dans le dossier ssl

```
manon@debian:~$ sudo cp dnsproject.prepa.com /etc/ssl
```

- Configurer Apache pour utiliser le certificat : Modifiez la configuration d'Apache pour activer le support SSL

```
manon@debian:/etc/apache2/sites-enabled$ ls
000-default.conf  dnsproject.prepa.com.conf
```

```
GNU nano 7.2      dnsproject.prepa.com.conf
<VirtualHost *:443>

    ServerName dnsproject.prepa.com
    DocumentRoot /var/www/html

    SSLEngine on
    SSLCertificateFile /etc/ssl/dnsproject.prepa.com.crt
    SSLCertificateKeyFile /etc/ssl/dnsproject.prepa.com.key

</VirtualHost>

[ Lecture de 10 lignes ]
^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter   ^C Emplacement
^X Quitter   ^R Lire fich.^M Remplacer  ^U Coller    ^J Justifier  ^_ Aller ligne
```

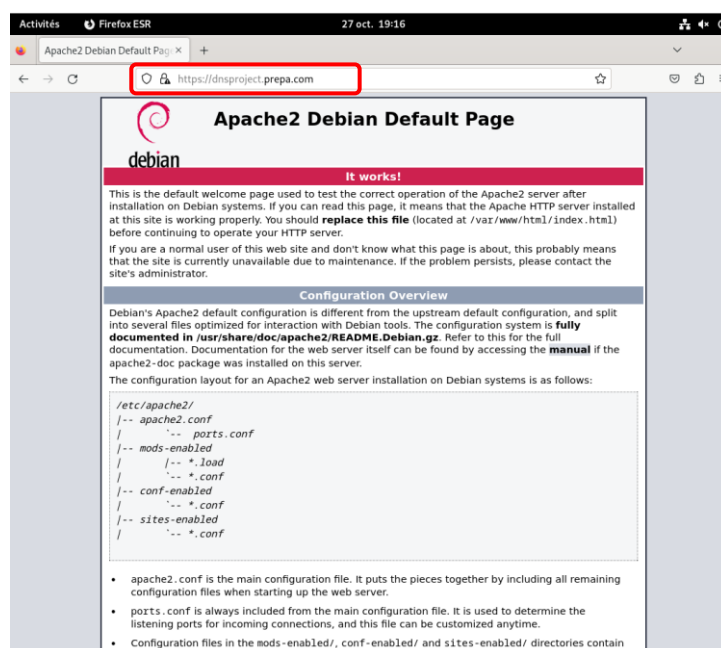
Explication :

Il définit les paramètres pour un site web qui utilise HTTPS pour sécuriser les communications. Il spécifie le nom de domaine, le répertoire racine du site, et les fichiers de certificat et de clé privée nécessaires pour activer la sécurité SSL

Rechargez apache pour appliquer les modifications

```
manon@debian:/etc/apache2/sites-enabled$ sudo systemctl reload apache2
```

- Vérifier que sa fonctionne sur le navigateur Mozilla en entrant l'url en commençant par https



Renseignez-vous aussi sur la différence entre les certificats SSL donnés par des organismes extérieurs et le vôtre auto-signé ?

Certificats SSL délivrés par des organismes externes (CA) :

-Ces certificats sont émis par des entités appelées Autorités de Certification (CA), qui sont des organismes de confiance.

-Pour obtenir un tel certificat, un site web doit passer par un processus de vérification rigoureux, où la CA s'assure que le site est bien la propriété de l'entité qui demande le certificat.

-Les navigateurs web font confiance aux CA, ce qui signifie que lorsqu'un navigateur se connecte à un site web sécurisé avec un certificat d'une CA, il sait que la communication est chiffrée et que le site est ce qu'il prétend être.

-Les visiteurs du site ne voient généralement aucun avertissement de sécurité et ont confiance dans la sécurité de la connexion.

Certificats SSL auto-signés :

Ces certificats sont générés par l'administrateur du serveur lui-même, sans implication d'une CA externe.

Il n'y a pas de vérification d'identité formelle par une tierce partie. Le certificat est signé par la clé privée du serveur, et le serveur déclare qu'il est la source de confiance.

Les navigateurs web, n'ayant aucune relation de confiance avec le serveur, affichent généralement des avertissements de sécurité aux visiteurs lorsqu'ils accèdent à un site utilisant un certificat auto-signé.

Les certificats auto-signés sont souvent utilisés pour des besoins internes ou de développement, mais ne sont pas recommandés pour les sites web publics, car ils peuvent décourager les visiteurs en raison des avertissements de sécurité.

Pourquoi votre certificat apparaît-il comme non sécurisé dans votre navigateur ?

Notre certificat apparaît comme non sécurisé car il a un certificat sll auto-signé. Le certificat auto-signé n'est pas émis par une autorité de certification de confiance (CA), ce qui fait qu'il n'a pas de validation et donc pas vérifier donc crée des avertissements de sécurité.