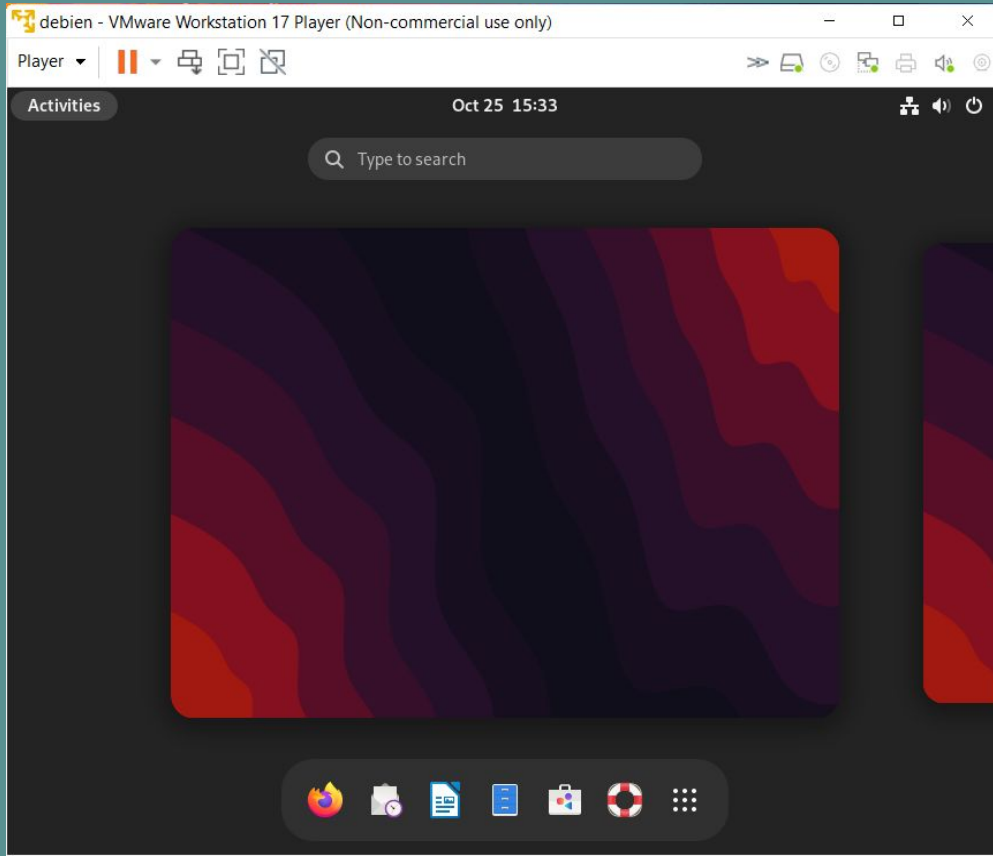


DDWS

DHCP DNS Web server Samba !

BY (ALYSON)HE.YU-COOPER





Installation Debian en mode graphique

JOB 01

1. Apache HTTP Server

Apache est le serveur Web le plus populaire et environ 60% des machines de serveur Web dans le monde utilisent ce serveur.

Avantages:

- Il est rapide, sécurisé et peut être facilement personnalisé pour différents environnements en utilisant des extensions et des modules.
- Il fonctionne sans problème sur les systèmes d'exploitation Windows et Linux.
- Il est open source, ce qui signifie que son code peut être consulté et modifié gratuitement.

Inconvénients :

- Sa vitesse de traitement des requêtes est quelque peu plus lente par rapport à ses concurrents.
- La flexibilité du serveur Web nuit à la performance dans certains cas. Par exemple, Apache doit lire plusieurs fichiers de configuration sur le serveur à chaque fois, consommant des ressources système et du temps.

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.

2. Nginx

Nginx est un serveur Web open source, performant, lancé en 2004. Il est devenu l'un des serveurs Web les plus utilisés, avec Apache.

Avantages :

- Il peut gérer plusieurs connexions simultanées tout en utilisant un minimum de ressources serveur.
- Il consomme moins de mémoire, prend moins d'espace et fonctionne sur des serveurs moins puissants.

Inconvénients :

- Liste moins étendue de modules.
- Prend en charge les systèmes d'exploitation Linux et Unix - le support de Windows est limité.
- Nginx ne prend pas en charge quelque chose comme le fichier .htaccess d'Apache.

3. Microsoft Internet Information Services (IIS)

IIS (Internet Information Services) est un serveur Web performant développé par Microsoft.

Avantages :

- Il est fortement uni au système d'exploitation et est donc relativement plus facile à administrer.
- Il a une bonne intégration avec Performance Monitor, ce qui permet un accès facile à des statistiques d'utilisation étendues.

Inconvénients :

- IIS n'est pas robuste et peut facilement être amené à 'se bloquer' de sorte que le serveur doit être redémarré pour récupérer.

4. LiteSpeed

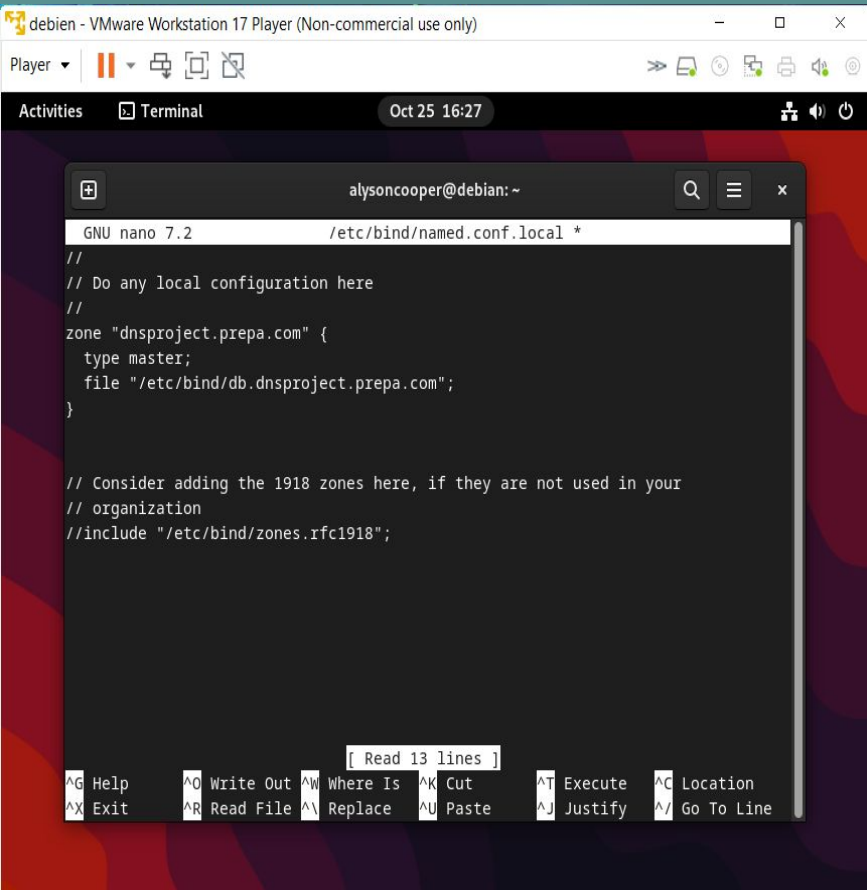
LiteSpeed Web Server (LSWS) est un logiciel de serveur Web propriétaire connu pour fournir des performances rapides et une haute évolutivité.

Avantages:

- LiteSpeed sert du contenu statique plus rapidement que tout autre serveur Web.
- Il augmente les performances de PHP grâce à son PHP LSAPI personnalisé.
- Il peut gérer plusieurs sites Web à partir du même serveur.

Inconvénients :

- OpenLiteSpeed, la version open source de LiteSpeed, n'est pas compatible avec Apache.
- Les nouvelles fonctionnalités sont souvent ajoutées à LiteSpeed avant OpenLiteSpeed. Par conséquent, la version gratuite peut être moins fiable et efficace que la version entreprise.



The screenshot shows a VMware Workstation 17 Player window titled 'debian - VMware Workstation 17 Player (Non-commercial use only)'. Inside the VM, the 'Terminal' application is open, displaying a nano 7.2 editor session. The user 'alysoncooper@debian: ~' is editing the file '/etc/bind/named.conf.local'. The configuration file content is as follows:

```
GNU nano 7.2 /etc/bind/named.conf.local *
//
// Do any local configuration here
//
zone "dnsproject.prepa.com" {
    type master;
    file "/etc/bind/db.dnsproject.prepa.com";
}

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

At the bottom of the terminal window, a status bar shows '[Read 13 lines]' and a list of keyboard shortcuts: ^G Help, ^O Write Out, ^W Where Is, ^K Cut, ^T Execute, ^C Location, ^X Exit, ^R Read File, ^\ Replace, ^P Paste, ^J Justify, and ^_ Go To Line.

Tout d'abord, il faut installer BIND sur mon serveur. Ouvrez un terminal et exécutez la commande suivante :

Cela installera BIND sur votre serveur Linux.

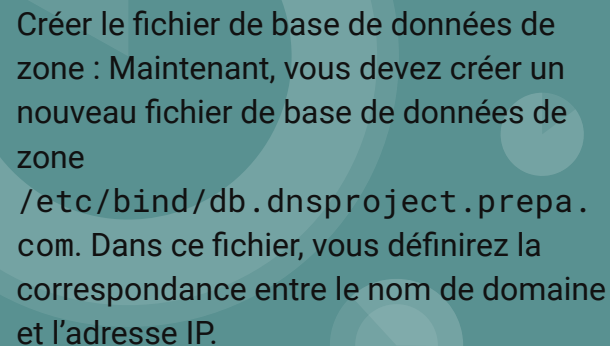
sudo apt install bind9

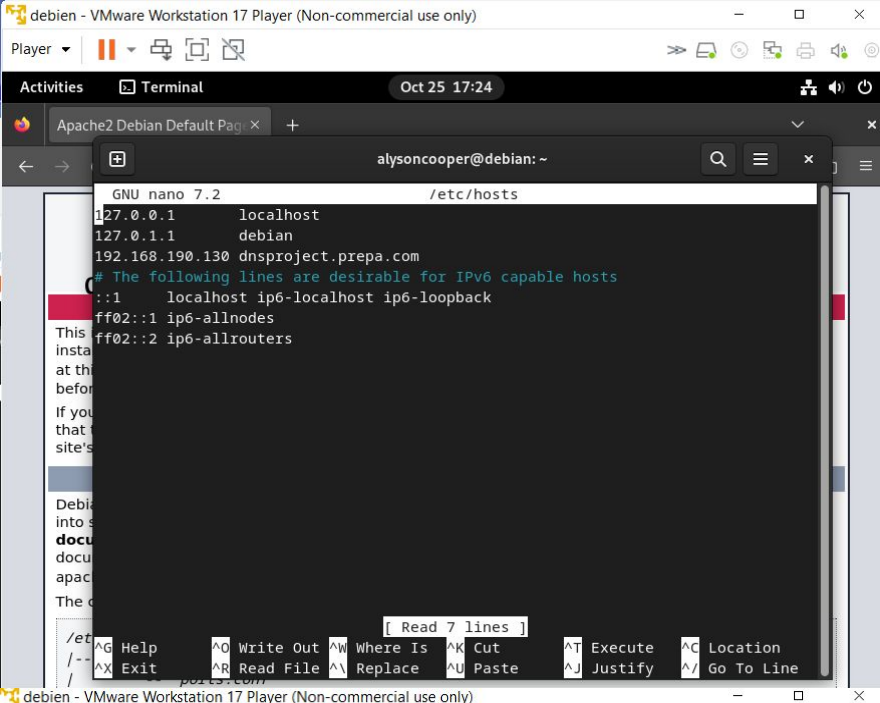
Configurer le fichier de zone : Ensuite, vous devez ajouter une zone à la configuration de BIND pour le transformer en serveur principal. Éditez le fichier

/etc/bind/named.conf.local et ajoutez le contenu suivant :

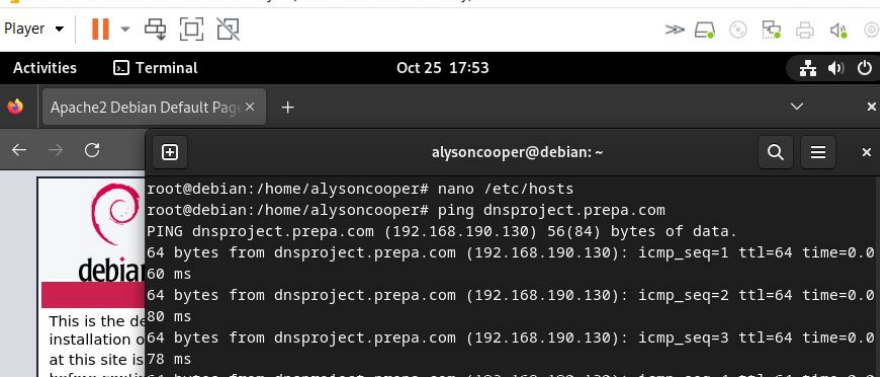
sudo nano /etc/bind/named.conf.local

JOB 04





```
GNU nano 7.2 /etc/hosts
127.0.0.1    localhost
127.0.1.1    debian
192.168.190.130 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
```



```
root@debian: /home/alysoncooper# nano /etc/hosts
root@debian: /home/alysoncooper# ping dnsproject.prepa.com
PING dnsproject.prepa.com (192.168.190.130): 56(84) bytes of data:
64 bytes from dnsproject.prepa.com (192.168.190.130): icmp_seq=1 ttl=64 time=0.060 ms
64 bytes from dnsproject.prepa.com (192.168.190.130): icmp_seq=2 ttl=64 time=0.080 ms
64 bytes from dnsproject.prepa.com (192.168.190.130): icmp_seq=3 ttl=64 time=0.078 ms
```

Et puis taper la commande :

nano /etc/hosts

- **nano /etc/hosts** est une commande qui permet d'ouvrir et d'éditer le fichier /etc/hosts dans un système Linux.
- **nano** est un éditeur de texte couramment utilisé dans les systèmes Linux et Unix. **/etc/hosts** est un fichier système spécial, utilisé pour mapper des noms d'hôtes (par exemple, des noms de domaine de sites Web) à leurs adresses IP correspondantes. Ce fichier est généralement utilisé pour le débogage et les tests réseau, ou comme solution de secours lorsque les serveurs DNS ne sont pas disponibles.
- Lorsque vous exécutez la commande **sudo nano /etc/hosts** dans le terminal, vous ouvrez l'éditeur nano avec les droits de superutilisateur (root) pour éditer le fichier **/etc/hosts**. Dans ce fichier, vous pouvez ajouter, modifier ou supprimer des mappages de noms d'hôtes vers des adresses IP.

Enfin taper la commande dans terminal :

ping dnsproject.prepa.com

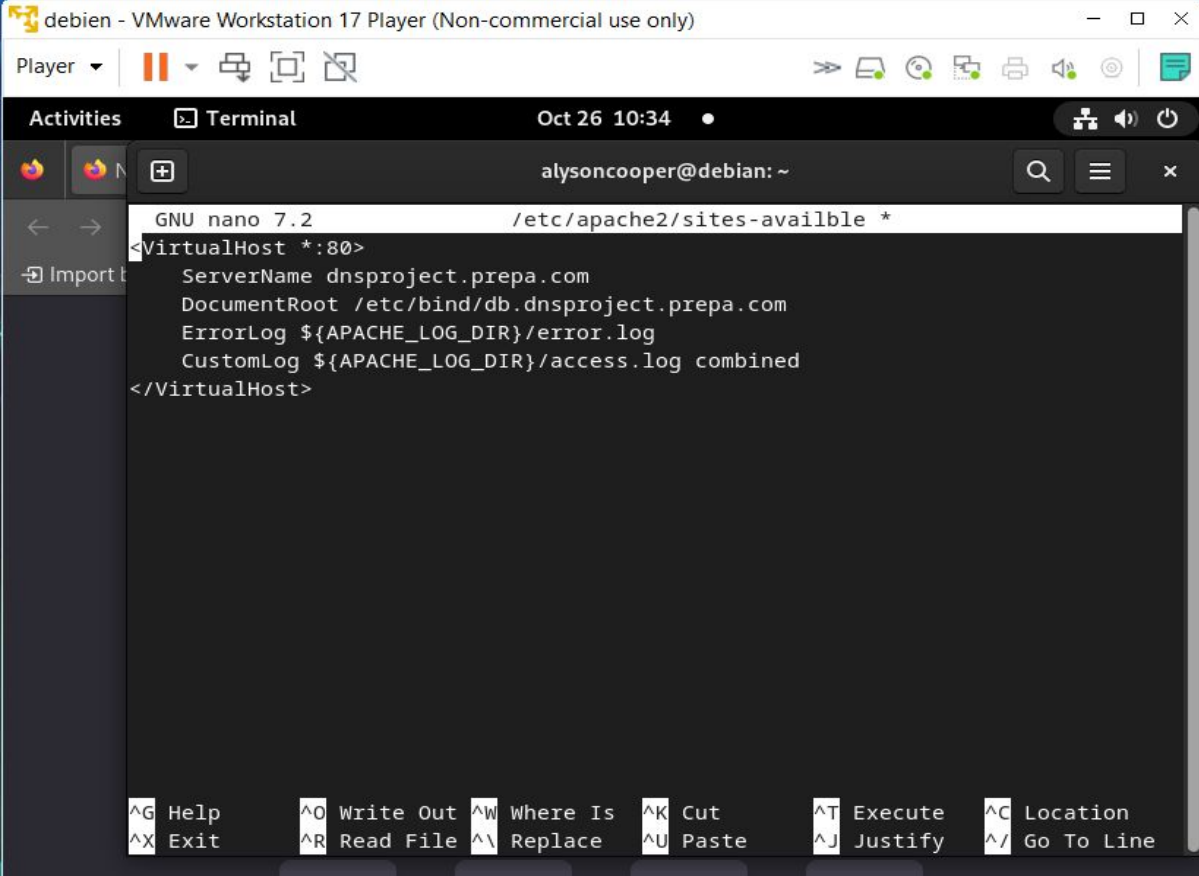
Pour venez voir si mon serveur peut être ping via ce nom de domaine.

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

1. **Choisissez un registraire de noms de domaine** : Il existe de nombreux registraires de noms de domaine disponibles, comme GoDaddy, Namecheap, et Wix.
2. **Recherchez votre nom de domaine** : Utilisez l'outil de recherche du registraire pour voir si le nom de domaine que vous souhaitez est disponible.
3. **Finalisez votre choix de nom de domaine** : Choisissez un nom qui représente bien votre marque ou votre entreprise.
4. **Choisissez une extension de nom de domaine** : Les extensions les plus courantes sont .com, .net, .org, .co et .us. Cependant, il existe de nombreuses autres extensions disponibles.
5. **Achetez le nom de domaine** : Une fois que vous avez choisi votre nom de domaine et son extension, vous pouvez l'acheter auprès du registraire.

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

1. **Aider à la marque** : Certaines extensions sont conçues pour aider à la marque d'une entreprise individuelle ou d'une industrie entière, comme .aarp ou .realtor.
2. **Indiquer l'emplacement d'un site web** : Certaines extensions sont réservées aux organisations spécifiques à une zone géographique, comme .us ou .ca.
3. **Servir une communauté spécifique** : Certaines extensions sont destinées à servir une communauté spécifique, basée sur la localisation géographique, l'ethnie, la technique ou d'autres catégories.
4. **Restreindre l'utilisation du domaine de premier niveau** : Certaines extensions sont réservées aux personnes ou organisations appartenant à un certain groupe.



The screenshot shows a terminal window titled 'alysoncooper@debian: ~' with the date 'Oct 26 10:34'. The terminal is running the GNU nano 7.2 editor, editing the file `/etc/apache2/sites-available *`. The content of the file is as follows:

```
<VirtualHost *:80>
    ServerName dnsproject.prepa.com
    DocumentRoot /etc/bind/db.dnsproject.prepa.com
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

At the bottom of the terminal, there is a row of keyboard shortcuts: `^G Help`, `^O Write Out`, `^W Where Is`, `^K Cut`, `^T Execute`, `^C Location`, `^X Exit`, `^R Read File`, `^_ Replace`, `^U Paste`, `^J Justify`, and `^_ Go To Line`.

Configurer Apache pour utiliser le nom de domaine : Il faut configurer Apache pour utiliser ce nom de domaine. Pour cela, on peut créer un nouveau fichier de configuration virtuel dans le répertoire `/etc/apache2/sites-available`. Par exemple, vous pouvez créer un fichier appelé `dnsproject.prepa.com.conf` avec le contenu suivant :
Taper la commande :
`nano /etc/apache2/sites-available`

Redémarrer Apache : Il faut redémarrer Apache pour que les modifications prennent effet avec la commande :
`sudo systemctl restart apache2`

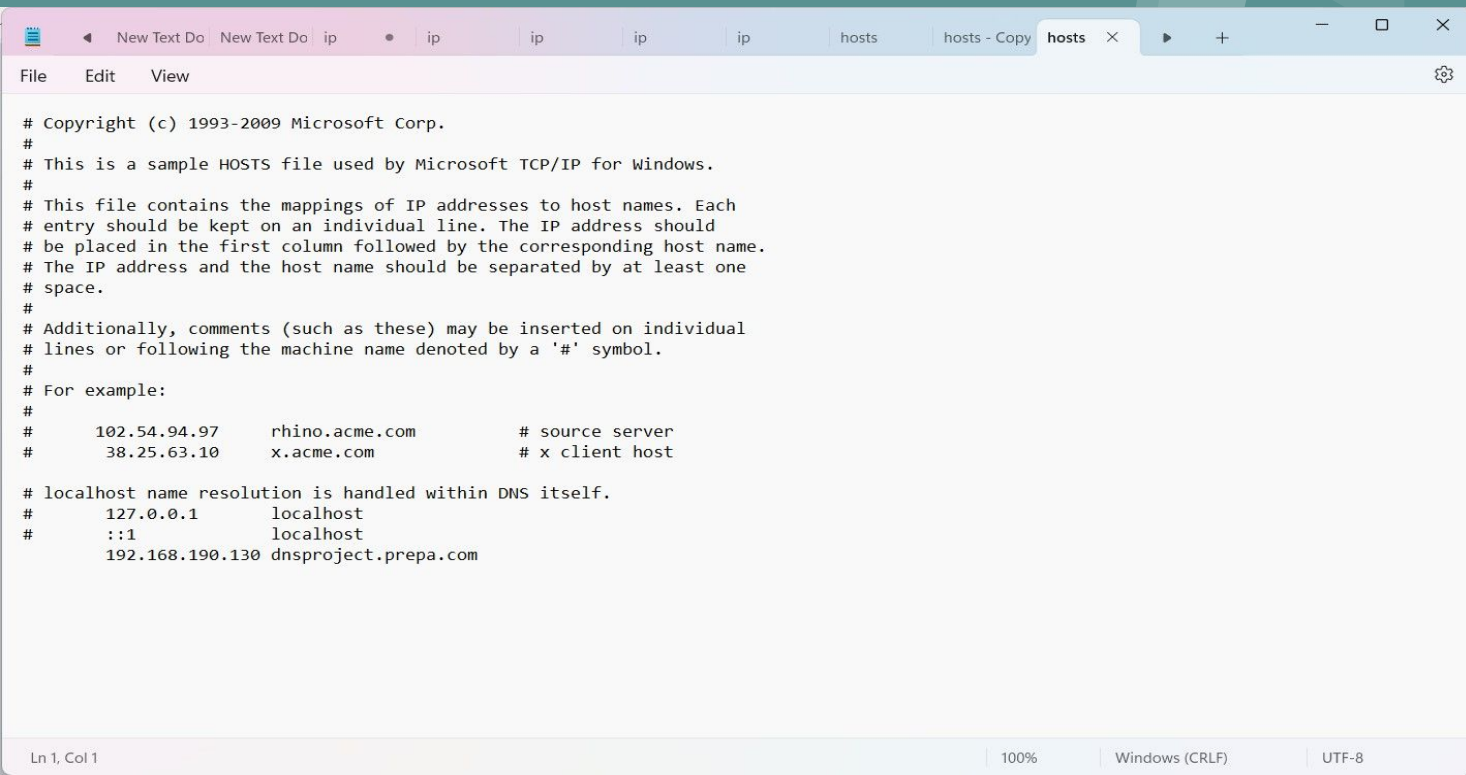
Activer le site : Une fois que on peut créé le fichier de configuration, vous pouvez activer le site en utilisant la commande `a2ensite` :

`sudo a2ensite dnsproject.prepa.com`
(même si on écrit pas tout ça, c'est pas grave parce que on a déjà créé dans le job 4).

JOB 06

```
root@debian:/home/alysoncooper# sudo a2ensite dnsproject.prepa.com
Site dnsproject.prepa.com already enabled
```

Modifier le fichier hosts dans windows : Ajoutez votre nom de domaine et l'adresse IP de votre serveur à votre fichier /etc/hosts. Par exemple, si votre nom de domaine est dnsproject.prepa.com et que l'adresse IP de mon serveur est 192.168.190.130, vous pouvez ajouter la ligne suivante à votre fichier [/etc/hosts](#) dans mon windows :
dans le chemin [windows /system32/drivers/etc/hosts](#)
copier le hosts sur le desktop et ouvrir l'éditeur de texte, copier l'adresse IP de mon serveur et l'adresse IP, puis remplacer le hosts dans /etc/hosts.



The screenshot shows a Notepad++ window with the file 'hosts' open. The window has a menu bar with 'File', 'Edit', and 'View'. The title bar shows the file path 'C:\Windows\System32\drivers\etc\hosts'. The text content of the file is as follows:

```
# 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
192.168.190.130 dnsproject.prepa.com
```

The status bar at the bottom indicates 'Ln 1, Col 1', '100%', 'Windows (CRLF)', and 'UTF-8'.

Windows PowerShell

Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! <https://aka.ms/PSWindows>

PS C:\Users\alyso\Desktop> ping dnsproject.prepa.com

Ping request could not find host dnsproject.prepa.com. Please check the name and try again.

PS C:\Users\alyso\Desktop> ping 192.168.190.130

Pinging 192.168.190.130 with 32 bytes of data:

Reply from 192.168.190.130: bytes=32 time=2ms TTL=64

Reply from 192.168.190.130: bytes=32 time=8ms TTL=64

Reply from 192.168.190.130: bytes=32 time<1ms TTL=64

Reply from 192.168.190.130: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.190.130:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 8ms, Average = 2ms

PS C:\Users\alyso\Desktop> ping dnsproject.prepa.com

Pinging dnsproject.prepa.com [192.168.190.130] with 32 bytes of data:

Reply from 192.168.190.130: bytes=32 time<1ms TTL=64

Reply from 192.168.190.130: bytes=32 time=2ms TTL=64

Reply from 192.168.190.130: bytes=32 time=1ms TTL=64

Reply from 192.168.190.130: bytes=32 time=4ms TTL=64

Ping statistics for 192.168.190.130:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

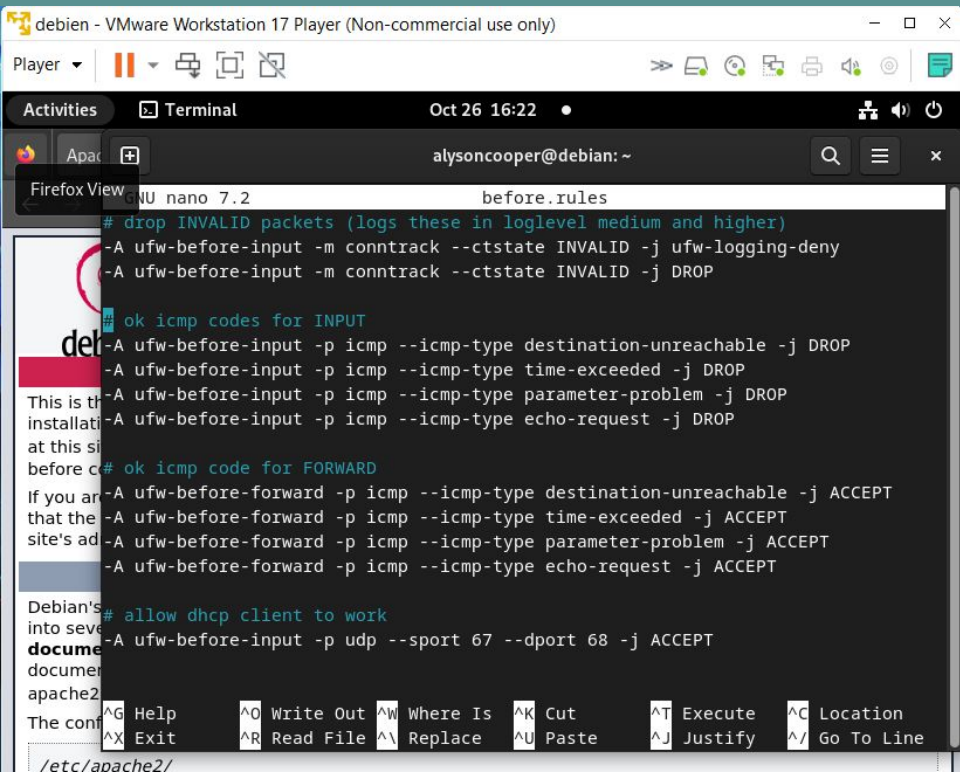
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/  
|-- apache2.conf  
|   |-- ports.conf  
|-- mods-enabled  
|   |-- *.load  
|   |-- *.conf  
|-- conf-enabled  
|   |-- *.conf  
|-- sites-enabled  
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective `*-available/`

Tout d'abord : Il faut installer UFW sur mon serveur. Ouvrez le terminal et exécutez la commande : `sudo apt install ufw`
Une fois finir installer UFW , taper le commande : `sudo nano before.rules` Pour interdire les requêtes ping, On doit éditer le fichier `/etc/ufw/before.rules` , trouver la ligne de `#ok icmp codes for INPUT` : Changer tous les ACCEPT EN DROP.
Enfin utiliser la commande : `sudo ufw reload` pour Firewall reloaded.
Maintenant on peut ping uniquement dans le debien vmware.

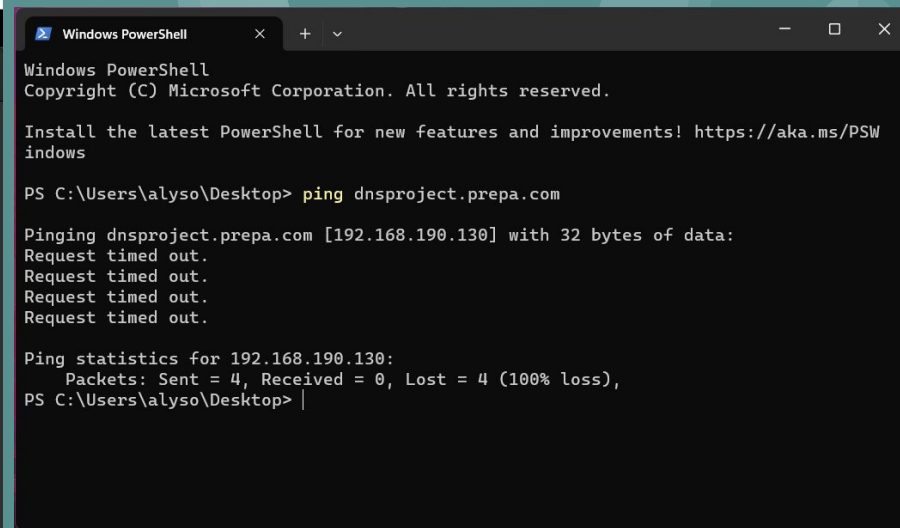


```
debien - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities Terminal Oct 26 16:22
alysoncooper@debian: ~
$ sudo apt install ufw
$ sudo nano before.rules
# drop INVALID packets (logs these in loglevel medium and higher)
-A ufw-before-input -m conntrack --ctstate INVALID -j ufw-logging-deny
-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

# ok icmp code for FORWARD
-A ufw-before-forward -p icmp --icmp-type destination-unreachable -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type time-exceeded -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type parameter-problem -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type echo-request -j ACCEPT

# allow dhcp client to work
-A ufw-before-input -p udp --sport 67 --dport 68 -j ACCEPT
```



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSW
indows

PS C:\Users\alyso\Desktop> ping dnsproject.prepa.com

Pinging dnsproject.prepa.com [192.168.190.130] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.190.130:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\alyso\Desktop>
```

JOB 07

Tout d'abord faut sur linux et mettez à jour la liste des paquets avec la commande :

```
root@debian:/home/alysoncooper# sudo apt-get update
```

Ensuite, installer le paquet "Samba" avec la commande :

```
root@debian:/home/alysoncooper# sudo apt-get install -y samba
```

Suite à l'installation, on peut afficher la version actuelle de Samba via la commande `smbd` :

```
root@debian:/home/alysoncooper# sudo smbd --version
Version 4.17.12-Debian
```

Pour afficher le statut du serveur Samba, et voir s'il est démarré ou arrêté, la commande à exécuter :

```
root@debian:/home/alysoncooper# 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 19:34:25 CEST; 34s ago
     Docs: man:smbd(8)
           man:samba(7)
           man:smb.conf(5)
  Process: 3343 ExecCondition=/usr/share/samba/is-configured smb (code=exited, status=0/SUCCESS)
  Process: 3345 ExecStartPre=/usr/share/samba/update-apparmor-samba-profile (code=exited, status=0/SUCCESS)
 Main PID: 3354 (smbd)
   Status: "smbd: ready to serve connections..."
    Tasks: 3 (limit: 9413)
  Memory: 8.9M
     CPU: 376ms
   CGroup: /system.slice/smbd.service
           └─3354 /usr/sbin/smbd --foreground --no-process-group
             └─3356 /usr/sbin/smbd --foreground --no-process-group
               └─3357 /usr/sbin/smbd --foreground --no-process-group

Oct 26 19:34:25 debian systemd[1]: Starting smbd.service - Samba SMB Daemon...
Oct 26 19:34:25 debian update-apparmor-samba-profile[3348]: grep: /etc/apparmor.d/samba: No such file or directory
Oct 26 19:34:25 debian update-apparmor-samba-profile[3351]: diff: /etc/apparmor.d/samba: No such file or directory
Oct 26 19:34:25 debian systemd[1]: Started smbd.service - Samba SMB Daemon.
```

JOB 08

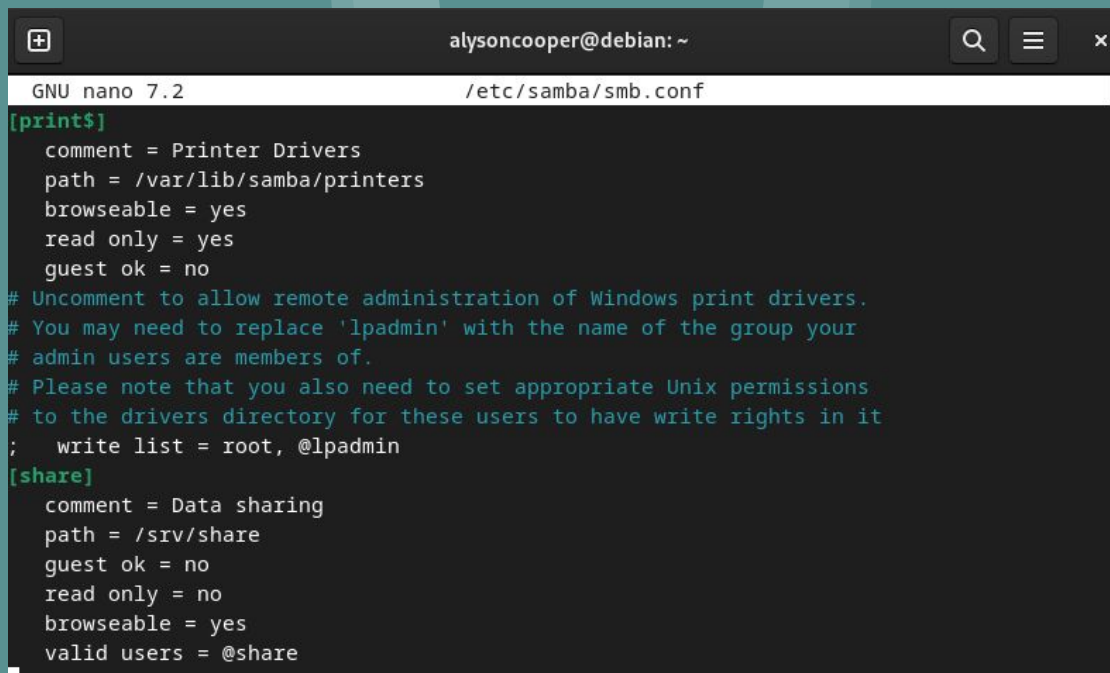
activer le démarrage automatique de *smbd* (Samba) :

```
root@debian:/home/alysoncooper# 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
```

Le fichier de configuration de Samba est "*/etc/samba/smb.conf*", on doit l'éditer : `root@debian:/home/alysoncooper# nano /etc/samba/smb.conf`

La configuration étant terminée, sauvegardez le fichier et redémarrez le service *smbd* :

```
root@debian:/home/alysoncooper# sudo systemctl restart smbd
```



```
alysoncooper@debian: ~
GNU nano 7.2 /etc/samba/smb.conf
[print$]
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
[share]
comment = Data sharing
path = /srv/share
guest ok = no
read only = no
browseable = yes
valid users = @share
```


Créez l'utilisateur "*alysoncoo*" et définissez son mot de passe :

```
root@debian:/home/alysoncooper# sudo adduser alysoncoo
Adding user `alysoncoo' ...
Adding new group `alysoncoo' (1001) ...
Adding new user `alysoncoo' (1001) with group `alysoncoo (1001)' ...
adduser: The home directory `/home/alysoncoo' already exists. Not touching this directory.
adduser: Warning: The home directory `/home/alysoncoo' does not belong to the user you are currently creating.
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for alysoncoo
Enter the new value, or press ENTER for the default
    Full Name []: alysoncoo
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
Adding new user `alysoncoo' to supplemental / extra groups `users' ...
Adding user `alysoncoo' to group `users' ...
```

Lorsqu'un utilisateur exécute lui-même la commande "*smbpasswd*", cela lui permet de modifier lui-même son mot de passe Samba :

```
root@debian:/home/alysoncooper# sudo smbpasswd -a alysoncoo
New SMB password:
Retype new SMB password:
```

L'utilisateur étant prêt, nous allons créer le groupe **<share>** Avec **gpsswd** ou **usermod**, ajoutez l'utilisateur "*alysoncoo*" au groupe "*share*" :

```
root@debian:/home/alysoncooper# sudo groupadd share
root@debian:/home/alysoncooper# sudo gpsswd -a alysoncoo share
Adding user alysoncoo to group share
```

Le partage va être hébergé à l'emplacement "*/srv/share*" de notre serveur. Commençons par créer le dossier :

```
root@debian:/home/alysoncooper# mkdir /srv/share
```

Ensuite, on va attribuer le groupe "*share*" comme groupe propriétaire de ce dossier :

```
root@debian:/home/alysoncooper# sudo chgrp -R share /srv/share
```

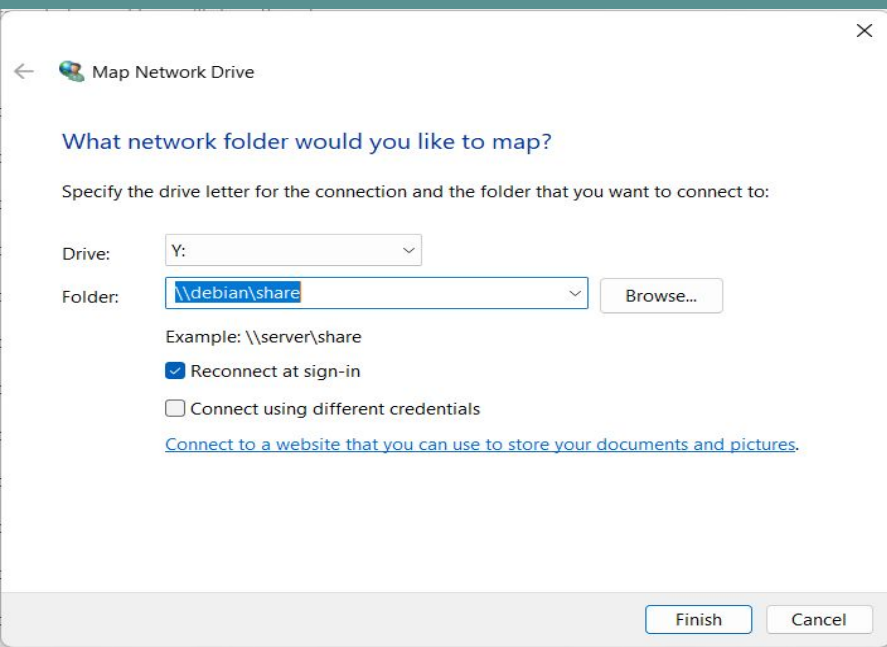
Puis, nous allons ajouter les droits de lecture/écriture à ce groupe sur ce dossier :

```
root@debian:/home/alysoncooper# sudo chmod -R g+rw /srv/share
```

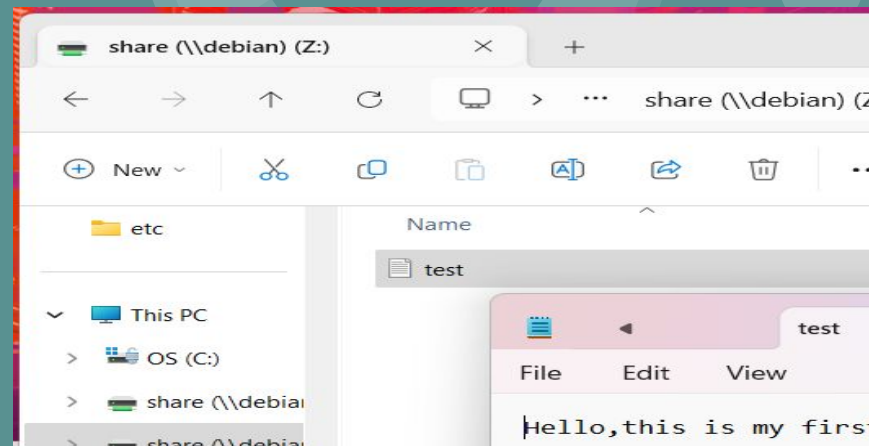
On peut vérifier la configuration des droits avec la commande suivante :

```
root@debian:/# ls -l /srv/  
share
```

Pour tester l'accès au partage, j'ai pris une machine Windows et j'ai aller dans le 'Map network drive '



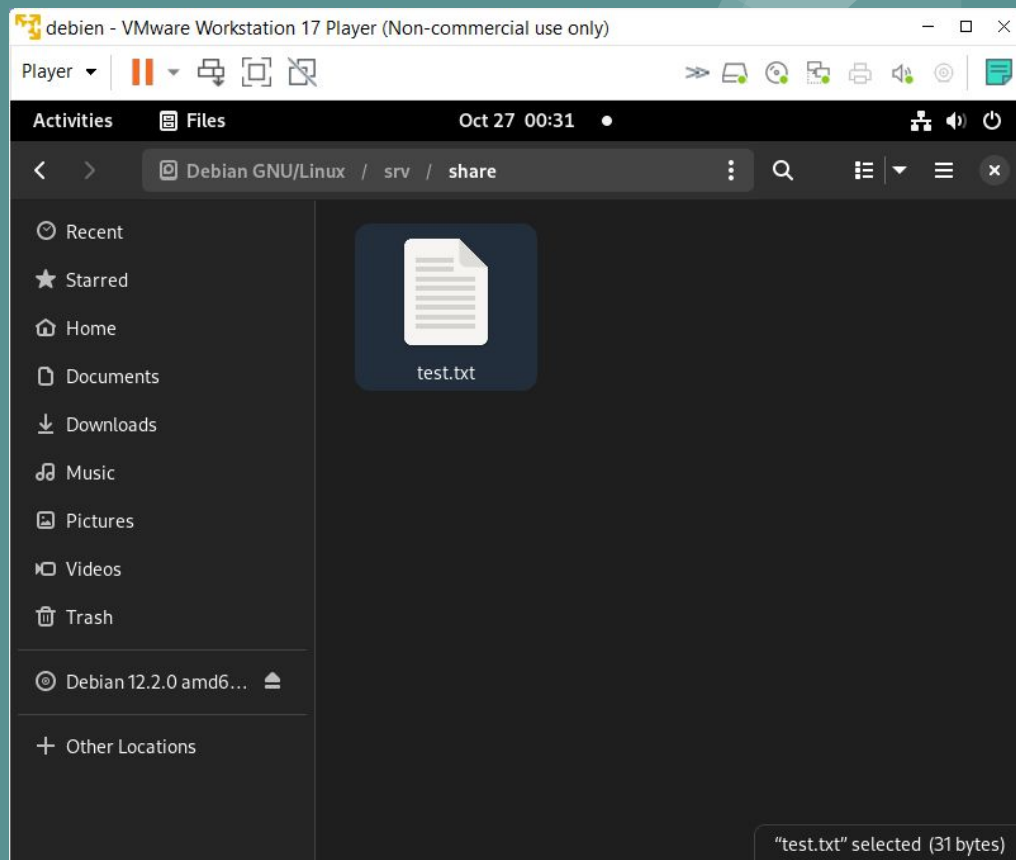
Le message accès refusé apparaît, c'est normal, car je dois m'authentifier, donc j'utilise le compte "alysoncoo" et le mot de passe saisi lors de l'exécution de la commande "smbpasswd".
J'accède bien à mon partage Samba depuis Windows ! Je peux même créer un fichier puisque j'ai accès en lecture / écriture.



Sur le serveur Linux, on peut lister le contenu de notre partage :

```
root@debian:/home/alysoncooper# ls -l /srv/share  
total 4  
-rwxr--r-- 1 alysoncoo alysoncoo 31 Oct 26 19:44 test.txt
```

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



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

La différence entre un certificat SSL auto-signé et un certificat SSL tiers réside dans le fait que le certificat SSL auto-signé est créé et signé par le propriétaire du site lui-même, tandis que le certificat SSL tiers est délivré par une autorité de certification (CA) tierce et de confiance. Bien que les certificats auto-signés soient gratuits et pratiques, ils ne sont généralement pas fiables car ils n'ont pas été vérifiés par une tierce partie, ce qui peut entraîner l'affichage d'un message d'avertissement par le navigateur. Par conséquent, l'utilisation de certificats auto-signés sur des sites web publics peut affecter l'expérience utilisateur et la crédibilité du site.

Si un navigateur marque un certificat SSL comme non sécurisé, cela peut être dû à plusieurs raisons :

Expiration du certificat : tous les certificats SSL ont une durée de validité. Une fois cette durée écoulée, le certificat expire. Si un site web utilise un certificat expiré, le navigateur affichera un message d'erreur. **L'autorité de certification n'est pas fiable :** si le certificat est délivré par une autorité non reconnue par le navigateur (par exemple, un certificat auto-signé), le navigateur affichera un message d'erreur. **Le certificat ne correspond pas au nom de domaine du site :** si le nom de domaine indiqué sur le certificat ne correspond pas au nom de domaine du site que l'utilisateur visite, le navigateur affichera un message d'erreur. **Problème de configuration du serveur :** si le serveur n'a pas correctement configuré SSL/TLS, par exemple s'il n'a pas fourni une chaîne de certificats complète ou s'il utilise une version de protocole ou une suite de chiffrement non prise en charge, le navigateur affichera un message d'erreur.

Pour aller plus loin...

1. Génération de la clé privée et du CSR : Tout d'abord, Je doit générer une clé privée et une demande de signature de certificat (CSR). On peut utiliser OpenSSL pour accomplir cette tâche. Par exemple, vous pouvez utiliser la commande suivante pour générer une nouvelle clé privée RSA:

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

```
alysoncooper@debian:~$ openssl req -new -key dnsproject.prepa.com.key -out dnsproject.prepa.com.csr
```

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
```

```
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:Provence-Alpes-Côte d'Azur
Locality Name (eg, city) []:Marseille
Organization Name (eg, company) [Internet Widgits Pty Ltd]:la plateforme
Organizational Unit Name (eg, section) []:Information Technology
Common Name (e.g. server FQDN or YOUR name) []:alysoncooper
Email Address []:he.yu-cooper@laplateforme.io
```

```
Please enter the following 'extra' attributes
to be sent with your certificate request
```

```
A challenge password []:814909
An optional company name []:814909
```

```
openssl req -new -key yourdomain.key -out yourdomain.csr
```

4. Installation du certificat SSL : Ensuite, on doit installer ce certificat SSL sur votre serveur web Apache. Tout d'abord, vous devez copier le fichier de certificat (.crt) et le fichier de clé privée (.key) dans le répertoire approprié du serveur Apache. Par exemple, vous pouvez les copier dans le répertoire /etc/httpd/ssl.

3.Obtention du certificat SSL : Ensuite, vous devez obtenir un certificat SSL. Vous pouvez choisir d'acheter un certificat ou de générer un certificat auto-signé. Si vous choisissez de générer un certificat auto-signé, vous pouvez utiliser la commande suivante :

debian - VMware Workstation 17 Player (Non-commercial use only)

Player ▾ | [Icons] | [Icons]

Activities | Terminal | Oct 27 10:08

alysoncooper@debian: ~

GNU nano 7.2 /etc/httpd/conf.d *

```
<VirtualHost *:443>
    DocumentRoot "/var/www/html"
    alysoncooper dnsproject.prepa.com:443
    SSLEngine on
    SSLCertificateFile "/etc/httpd/ssl/dnsproject.prepa.com.crt"
    SSLCertificateKeyFile "/etc/httpd/ssl/dnsproject.prepa.com.key"
    SSLCertificateChainFile /etc/httpd/ssl/root_bundle.crt
</VirtualHost>
```

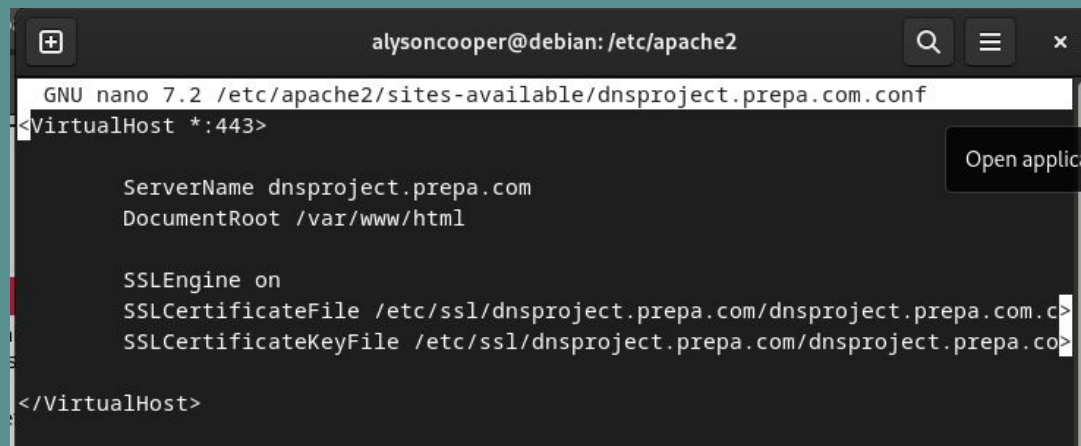
[Read 8 lines]

^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

```
debien - VMware Workstation 17 Player (Non-commercial use only)
Player ▾ | [Icons] | Activities Terminal Oct 27 01:31 • [Icons]
alysoncooper@debian: ~
alysoncooper@debian: $ openssl req -x509 -newkey rsa:2048 -keyout dnsproject.prepa.com.key -out
dnsproject.prepa.com.crt -days 3650 -nodes
.....+.....*.....+.....
.....+.....*.....+.....
.....+.....*.....+.....
.....+.....*.....+.....
.....+.....*.....+.....
.....+.....*.....+.....
.....+.....*.....+.....
.....+.....*.....+.....
.....+.....*.....+.....
.....+.....*.....+.....
.....+.....*.....+.....
.....+.....*.....+.....
.....+.....*.....+.....
.....+.....*.....+.....
.....+.....*.....+.....
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:Provence-Alpes-Côte d'Azur
Locality Name (eg, city) []:Marseille
Organization Name (eg, company) [Internet Widgits Pty Ltd]:la plateforme
Organizational Unit Name (eg, section) []:Information Technology
Common Name (e.g. server FQDN or YOUR name) []:alysoncooper
Email Address []:he.yu-cooper@laplateforme.io
alysoncooper@debian: $
```


5. Configurer Apache pour utiliser SSL : Ensuite, vous devez configurer Apache pour utiliser SSL. Cela implique généralement de modifier les fichiers de configuration d'Apache (par exemple httpd.conf ou ssl.conf) et d'ajouter quelques directives pointant vers vos fichiers de certificat et de clé privée.

```
root@debian:/etc/apache2# nano /etc/apache2/sites-available/dnsproject.prepa.com.conf
```



The screenshot shows a terminal window with the nano text editor open. The title bar reads 'alysoncooper@debian: /etc/apache2'. The editor is editing the file '/etc/apache2/sites-available/dnsproject.prepa.com.conf'. The content of the file is as follows:

```
<VirtualHost *:443>

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

    SSLEngine on
    SSLCertificateFile /etc/ssl/dnsproject.prepa.com/dnsproject.prepa.com.c
    SSLCertificateKeyFile /etc/ssl/dnsproject.prepa.com/dnsproject.prepa.co
</VirtualHost>
```

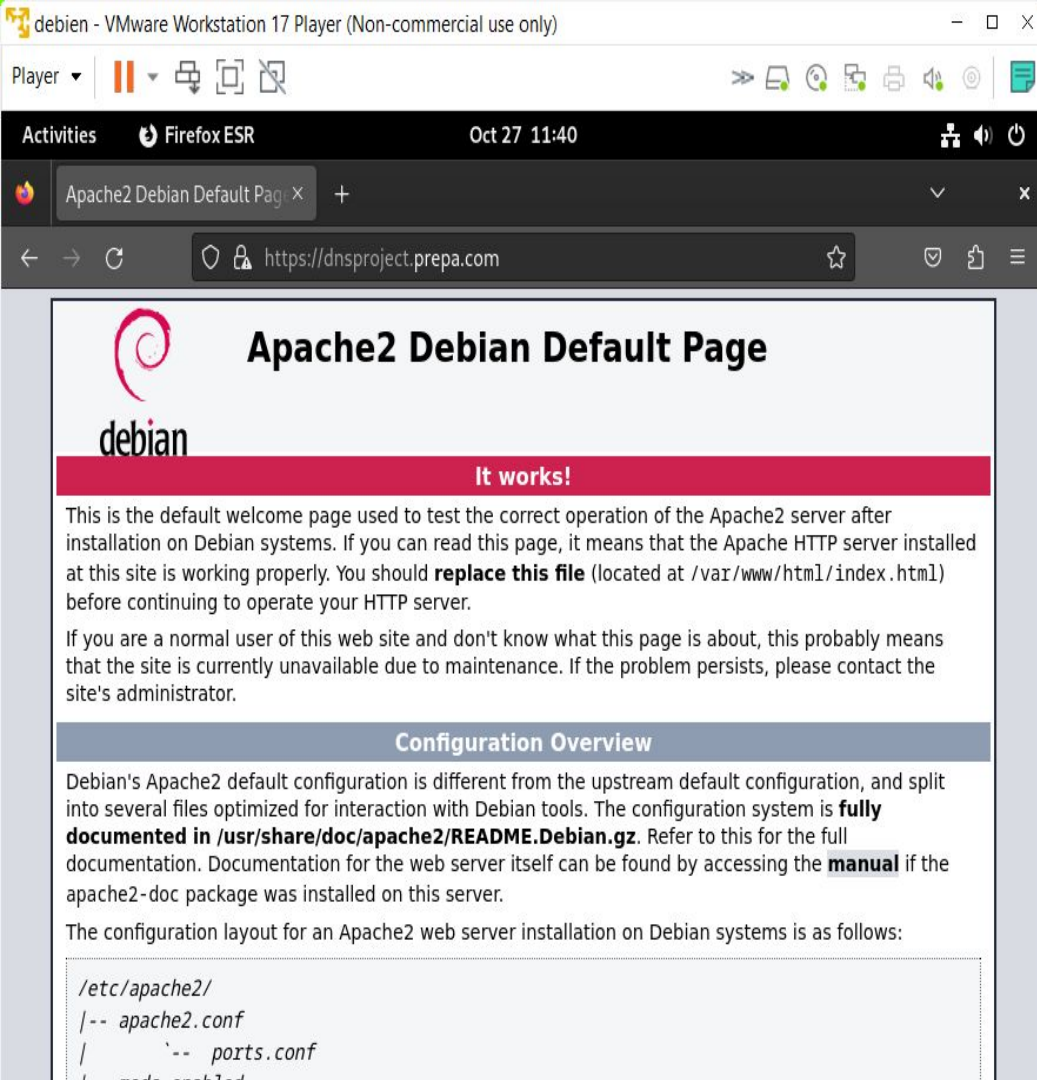
4.5 Je doit transférer un fichier **crt** et **key** vers SSL :

```
root@debian:/etc/apache2# cp /etc/httpd/ssl/dnsproject.prepa.com.crt /etc/ssl/dn
sproject.prepa.com/
```

```
root@debian:/etc/apache2# cp /etc/httpd/ssl/dnsproject.prepa.com.key /etc/ssl/dn
sproject.prepa.com/
```

Redémarrer Apache : Enfin, vous devez redémarrer Apache pour que les modifications prennent effet.

```
alysoncooper@debian:/etc/apache2$ sudo systemctl reload apache2
```



Maintenant, j'ai bien réussi ouvert la page avec https ! ! ! ! ! ! ! !

MERCI TO BE CONTINUE

