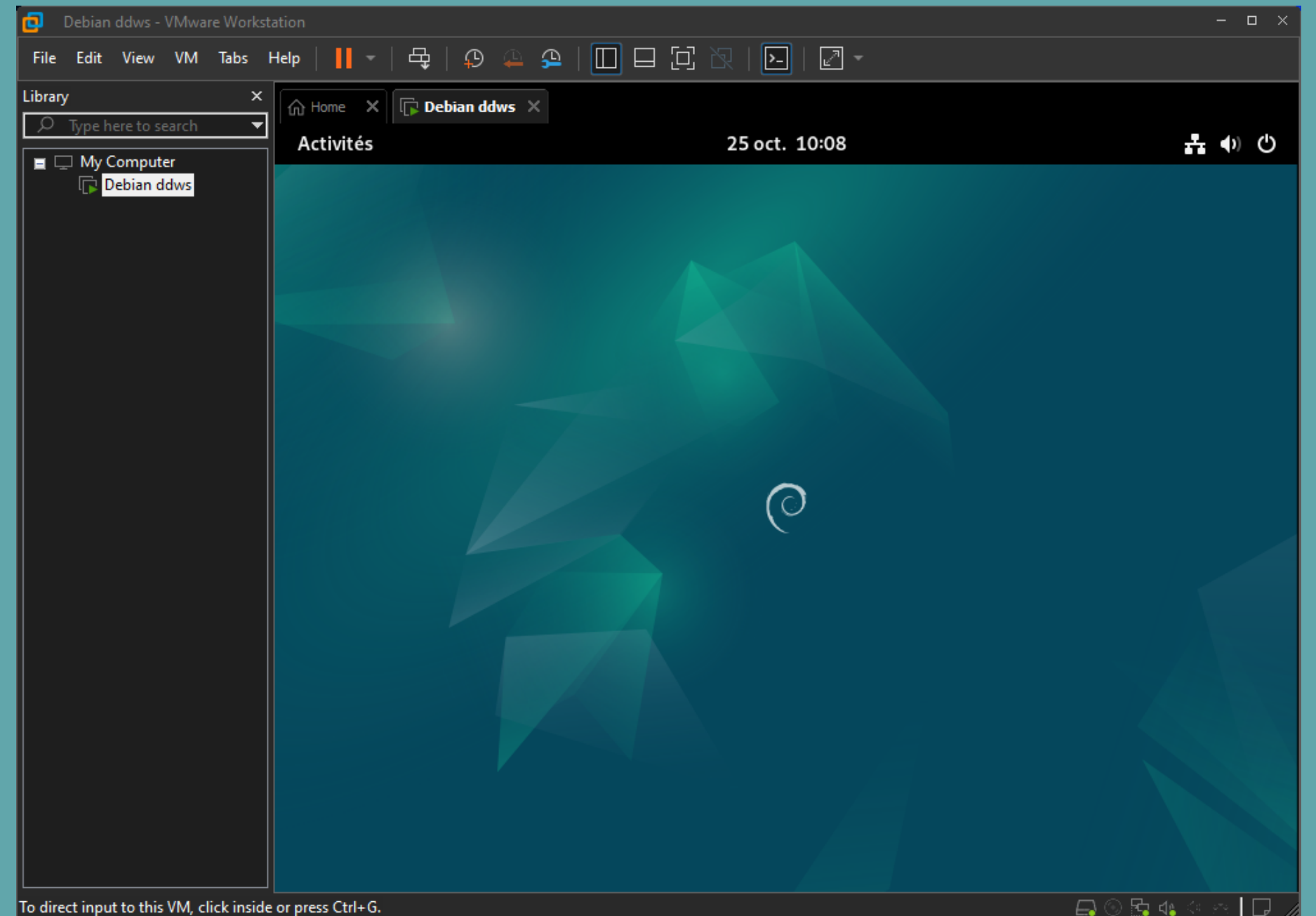


# Projet Ddws

## APACHE WEB SERVER

# Job 1 : installation Debian

## Installation debian en mode graphique



# Job 2 : installation serveur Web Apache2

En tant qu'administrateur,

- mettre à jour les paquets :  
`sudo apt update`
- installer Apache2 :  
`sudo apt install apache2`
- vérifier l'état du serveur :  
`sudo systemctl status apache2`

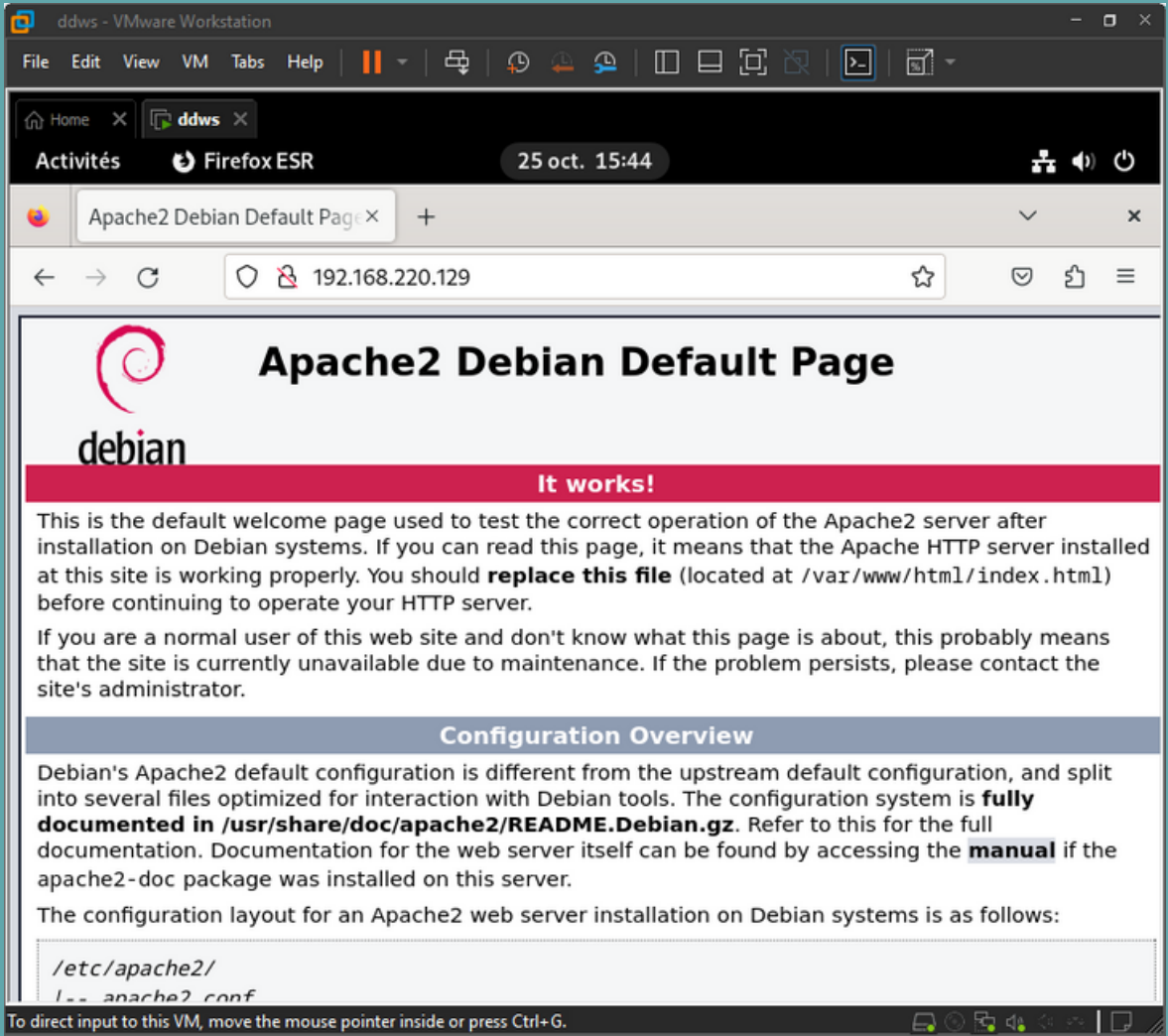
```
hugo@ddws:~$ sudo systemctl status apache2
• apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled)
   Active: active (running) since Wed 2023-10-25 15:31:39 CEST; 31s ago
     Docs: https://httpd.apache.org/docs/2.4/
  Main PID: 3285 (apache2)
    Tasks: 55 (limit: 9421)
   Memory: 10.8M
      CPU: 32ms
   CGroup: /system.slice/apache2.service
           └─3285 /usr/sbin/apache2 -k start
             └─3287 /usr/sbin/apache2 -k start
               └─3288 /usr/sbin/apache2 -k start

oct. 25 15:31:39 ddws systemd[1]: Starting apache2.service - The Apache HTTP Server...
oct. 25 15:31:39 ddws apache2[3284]: AH00558: apache2: Could not reliably determine >
oct. 25 15:31:39 ddws systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-16/16 (END)
```

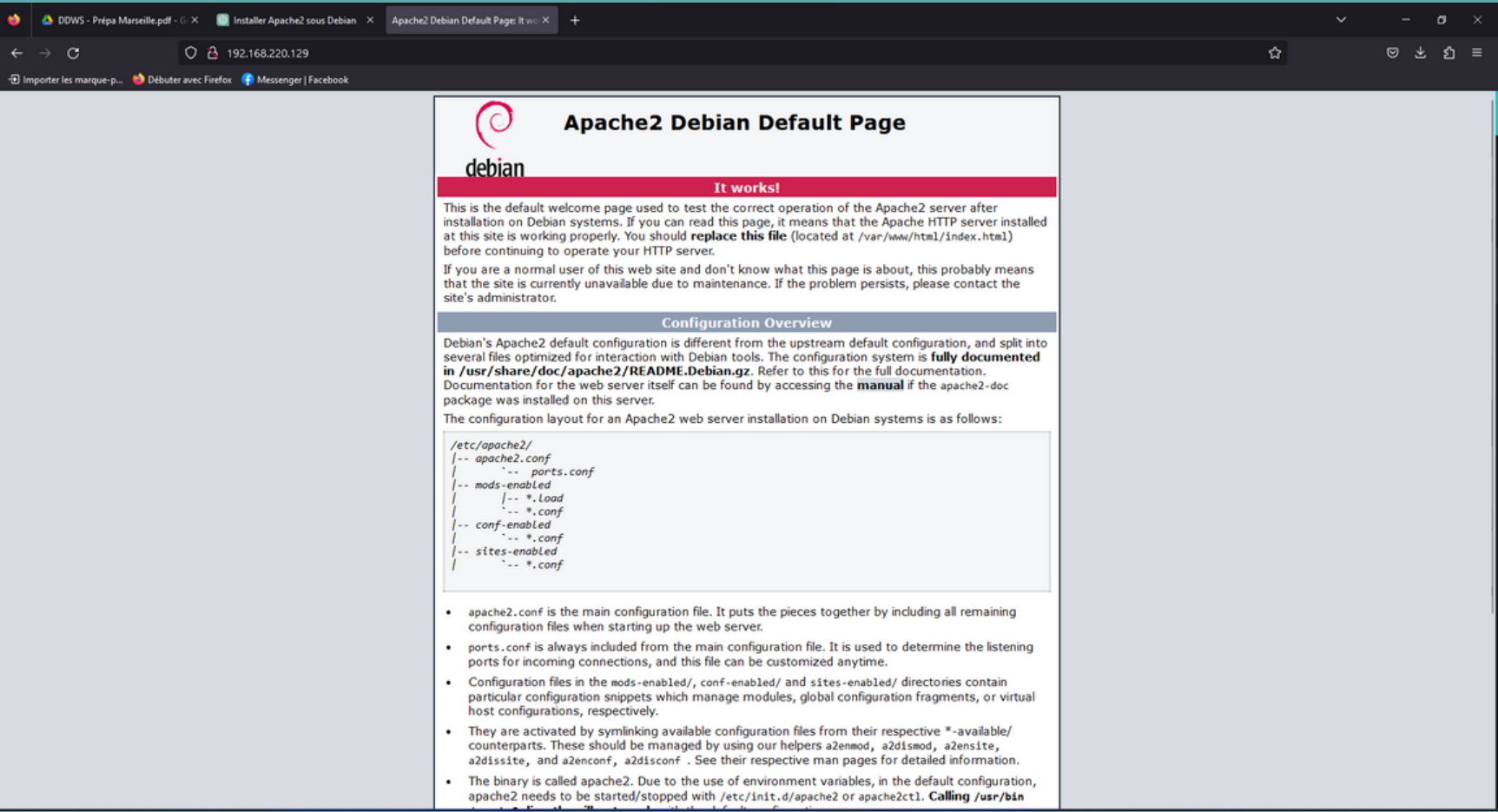
Statut du serveur

# Connexion au serveur depuis la machine hôte

Pour ce connecter au serveur il faut ouvrir un navigateur web  
et entré l'adresse IP du serveur.



Depuis la machine virtuelle



Depuis la machine hôte

# Job 3 : recherches

Il existe au moins **neuf** serveurs web différents: **Apache HTTP**, **Nginx**, **Microsoft IIS**, **LiteSpeed**, **caddy Cherokee**, **Lighttpd**, **Tomcat** et **Node.js**.

On va se concentrer sur les quatre plus connus qui sont :  
**Apache**, **Nginx**, **IIS** et **Lighttpd**





**Apache HTTP Server** (Apache) : Apache est l'un des serveurs web les plus populaires et les plus anciens. Il est open source et largement utilisé sur de nombreuses plateformes.

**Avantages :**

- Stable et éprouvé.
- Grande communauté d'utilisateurs et de développeurs.
- Supporte de nombreux modules et extensions.

**Inconvénients :**

- Peut être moins performant que d'autres serveurs web pour les charges très élevées.
- La configuration peut sembler complexe pour les débutants.





**Nginx** : Nginx est un serveur web et proxy inverse open source réputé pour sa performance, sa légèreté et sa capacité à gérer de nombreuses connexions simultanées.

**Avantages :**

- Excellente performance, notamment pour les charges élevées et les connexions simultanées.
- Gestion efficace des serveurs proxy et des répartiteurs de charge.

**Inconvénients :**

- La configuration peut sembler moins intuitive pour les débutants.
- Moins de modules que ceux disponibles pour Apache.



# Microsoft IIS

**Microsoft Internet Information Services (IIS)** : IIS est le serveur web de Microsoft pour les systèmes Windows. Il est souvent utilisé avec des technologies Microsoft telles que ASP.NET.

## **Avantages :**

- Intégration transparente avec d'autres produits Microsoft.
- Prise en charge d'ASP.NET et d'autres technologies Microsoft.

## **Inconvénients :**

- Principalement destiné aux systèmes Windows, ce qui limite la portabilité.
- Moins couramment utilisé pour l'hébergement web non-Microsoft.





**lighttpd (Lighty)** : Lighttpd est un serveur web open source léger et conçu pour la performance. Il est souvent utilisé pour servir des fichiers statiques.

**Avantages :**

- Léger et performant pour servir des fichiers statiques.
- Utilisé dans des environnements à faible consommation de ressources.

**Inconvénients :**

- Moins polyvalent que certains autres serveurs web.
- Peut nécessiter des solutions tierces pour des fonctionnalités avancées.

# Job 4 : Serveur DNS

## L'installation se fait en 4 étapes

Étape 1: **Installation** du serveur DNS Bind9

Étape 2: **configuration** du fichier de zone

Étape 3: **redémarrage** du serveur DNS

Étape 4: **Configuration** du DNS **local** sur les clients

# Étape 1: Installation du serveur DNS Bind9

L'installation se fait en deux ligne de commandes :

- `sudo apt update`
- `sudo apt install bind9` (confirmer l'installation avec o)

```
hugo@ddws:~$ sudo 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.
Après cette opération, 2 024 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://deb.debian.org/debian bookworm/main amd64 bind9-utils amd64 1:9.18.19-1~deb12u1 [406 kB]
Réception de :2 http://deb.debian.org/debian bookworm/main amd64 bind9 amd64 1:9.18.19-1~deb12u1 [494 kB]
900 ko réceptionnés en 0s (8 774 ko/s)
Sélection du paquet bind9-utils précédemment désélectionné.
(Lecture de la base de données... 150359 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../bind9-utils_1%3a9.18.19-1~deb12u1_amd64.deb ...
Dépaquetage de bind9-utils (1:9.18.19-1~deb12u1) ...
Sélection du paquet bind9 précédemment désélectionné.
Préparation du dépaquetage de .../bind9_1%3a9.18.19-1~deb12u1_amd64.deb ...
Dépaquetage de bind9 (1:9.18.19-1~deb12u1) ...
Paramétrage de bind9-utils (1:9.18.19-1~deb12u1) ...
Paramétrage de bind9 (1:9.18.19-1~deb12u1) ...
Ajout du groupe « bind » (GID 122)...
Fait.
Ajout de l'utilisateur système « bind » (UID 114) ...
Ajout du nouvel utilisateur « bind » (UID 114) avec pour groupe d'appartenance « bind »
...
Pas de création du répertoire personnel « /var/cache/bind ».
wrote key file "/etc/bind/rndc.key"
named-resolvconf.service is a disabled or a static unit, not starting it.
Created symlink /etc/systemd/system/bind9.service → /lib/systemd/system/named.service.
Created symlink /etc/systemd/system/multi-user.target.wants/named.service → /lib/system
d/system/named.service.
Traitement des actions différées (« triggers ») pour man-db (2.11.2-2) ...
```

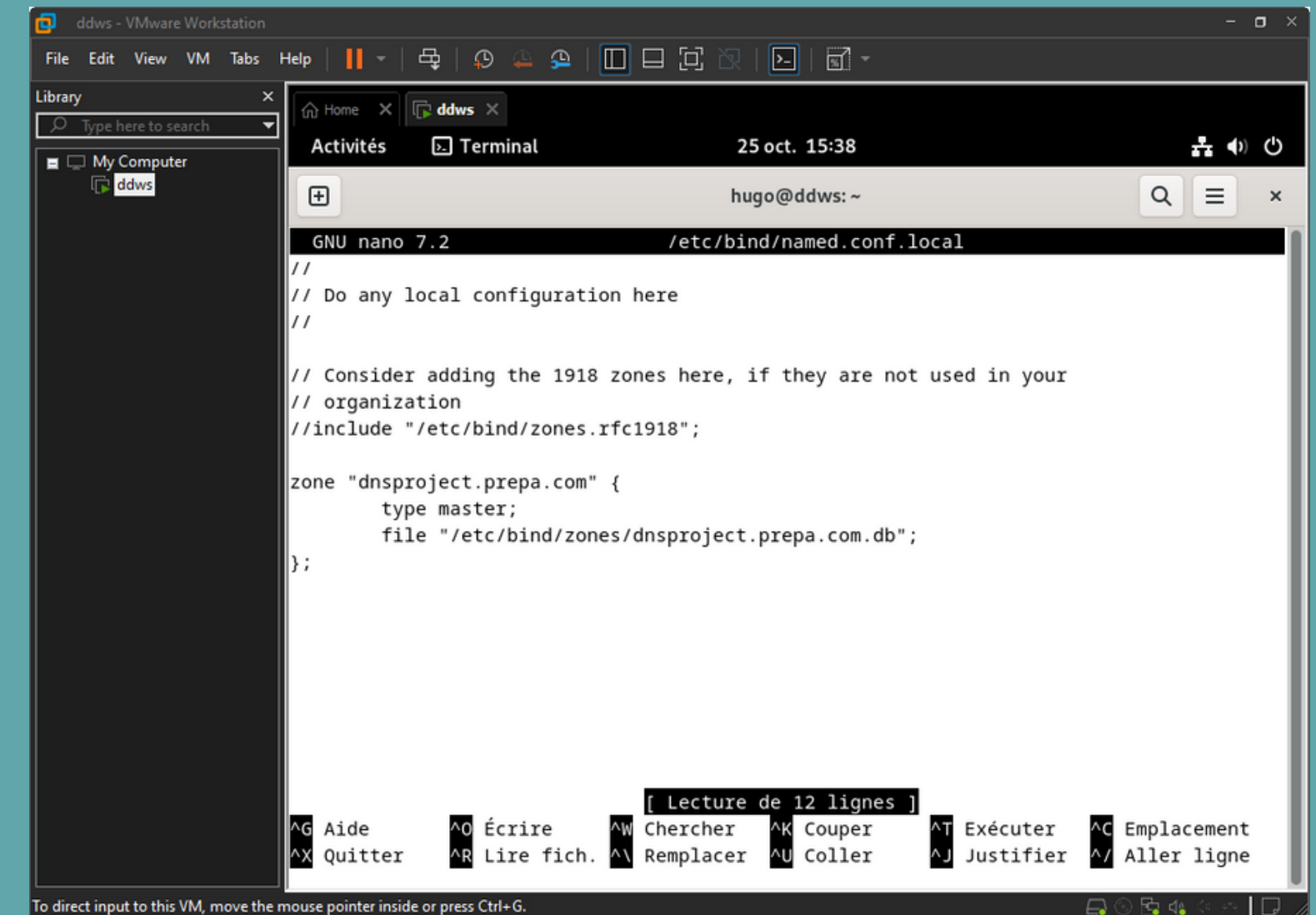
# Étape 2 : configuration du fichier de zone

Il faut alors ouvrir le fichier de configuration de Bind9 :

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

Puis ajouter une zone pour le domaine :

```
zone "dnsproject.prepa.com" {  
    type master;  
    file "/etc/bind/zones/dnsproject.prepa.com.db";  
};
```



The screenshot shows a VMware Workstation window titled 'ddws - VMware Workstation'. Inside, a terminal window is open with the prompt 'hugo@ddws: ~'. The terminal is running the GNU nano 7.2 editor, editing the file '/etc/bind/named.conf.local'. The file content is as follows:

```
//  
// 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 "dnsproject.prepa.com" {  
    type master;  
    file "/etc/bind/zones/dnsproject.prepa.com.db";  
};
```

At the bottom of the terminal window, there is a status bar with various keyboard shortcuts for nano, such as '^G Aide', '^O Écrire', '^W Chercher', '^K Couper', '^T Exécuter', '^C Emplacement', '^X Quitter', '^R Lire fich.', '^\_ Remplacer', '^U Coller', '^J Justifier', and '^\_ Aller ligne'. A message at the bottom of the terminal says 'To direct input to this VM, move the mouse pointer inside or press Ctrl+G.'

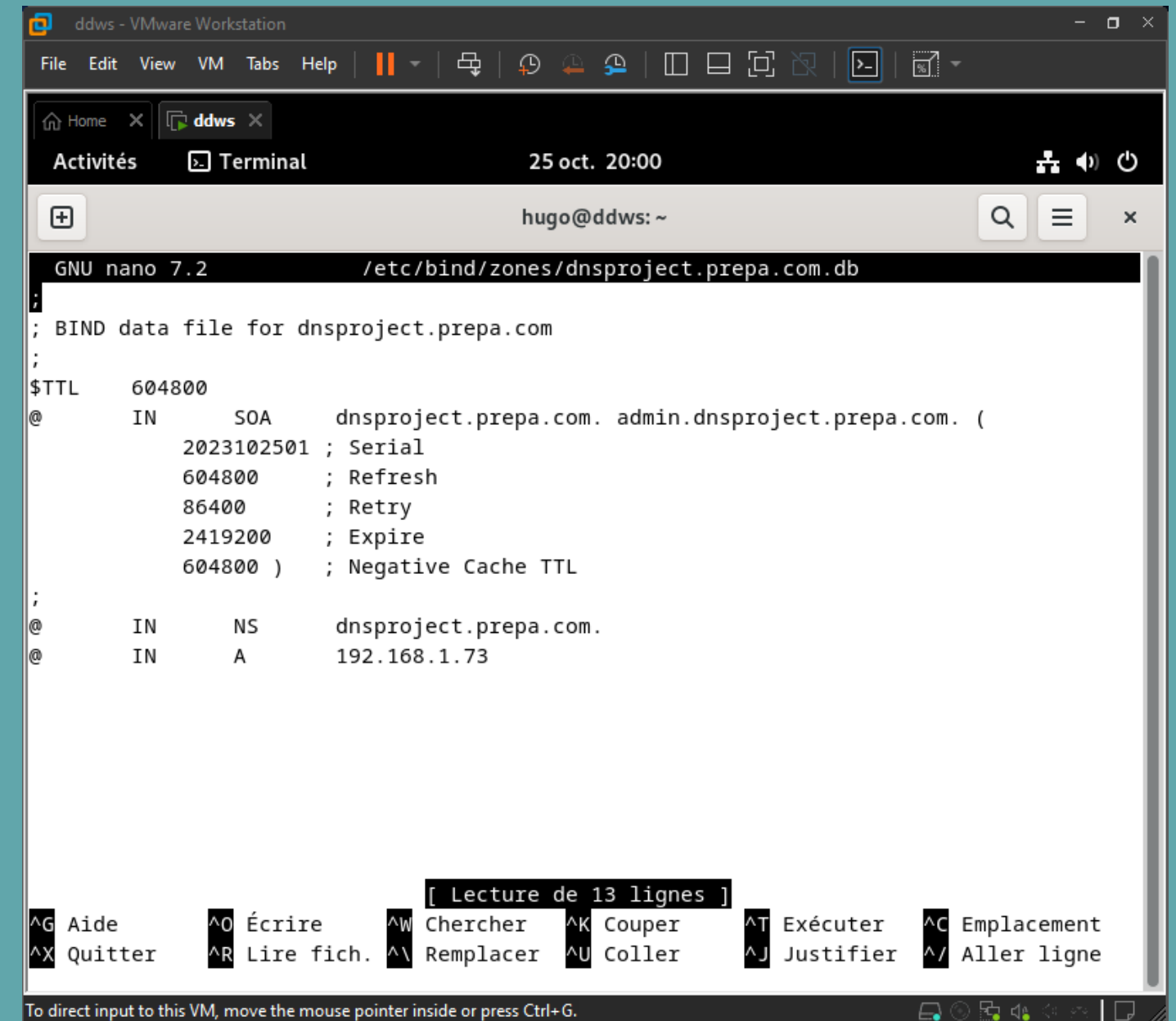
# Étape 2 : configuration du fichier de zone

Créer le dossier et le fichier zone :

```
sudo mkdir /etc/bind/zones
```

```
sudo nano /etc/bind/zones/dnsproject.prepra.com.db
```

Puis ajouter des enregistrements DNS dans le fichier avec la bonne adresse IP:



The screenshot shows a terminal window titled 'ddws - VMware Workstation'. The terminal is running the nano text editor, editing the file '/etc/bind/zones/dnsproject.prepra.com.db'. The file content is as follows:

```
; BIND data file for dnsproject.prepra.com
;
$TTL      604800
@         IN      SOA      dnsproject.prepra.com. admin.dnsproject.prepra.com. (
                                2023102501 ; Serial
                                604800      ; Refresh
                                86400       ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
;
@         IN      NS       dnsproject.prepra.com.
@         IN      A        192.168.1.73
```

The terminal window also shows the nano editor's help menu at the bottom, which includes options like Aide, Écrire, Chercher, Couper, Exécuter, Emplacement, Quitter, Lire fich., Remplacer, Coller, Justifier, and Aller ligne. The status bar at the bottom indicates 'To direct input to this VM, move the mouse pointer inside or press Ctrl+G.'

# Étape 3 : redémarrage du serveur DNS

Redémarrer le service Bind9 pour appliquer les modification avec la commande

```
sudo systemctl restart bind9
```





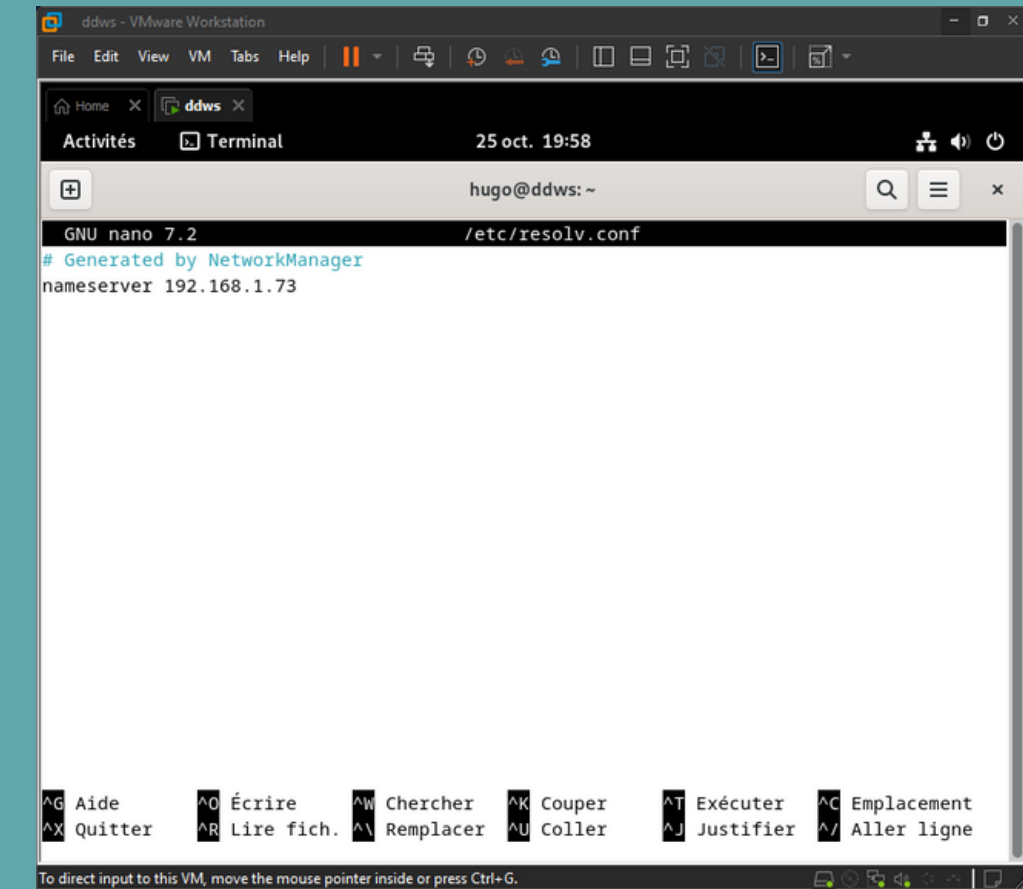
# Étape 4 : Configuration du DNS local sur les clients

Modifier le fichier de configuration réseau :  
`sudo nano /etc/resolv.conf`

ajouter le serveur DNS à la liste:

`nameserver 192.168.1.73`

le serveur peut maintenant se ping :



```
hugo@ddws:~$ ping dnsproject.prepa.com
PING dnsproject.prepa.com (192.168.1.73) 56(84) bytes of data.
64 bytes from ddws (192.168.1.73): icmp_seq=1 ttl=64 time=0.011 ms
64 bytes from ddws (192.168.1.73): icmp_seq=2 ttl=64 time=0.023 ms
64 bytes from ddws (192.168.1.73): icmp_seq=3 ttl=64 time=0.026 ms
64 bytes from ddws (192.168.1.73): icmp_seq=4 ttl=64 time=0.023 ms
64 bytes from ddws (192.168.1.73): icmp_seq=5 ttl=64 time=0.025 ms
64 bytes from ddws (192.168.1.73): icmp_seq=6 ttl=64 time=0.025 ms
64 bytes from ddws (192.168.1.73): icmp_seq=7 ttl=64 time=0.023 ms
64 bytes from ddws (192.168.1.73): icmp_seq=8 ttl=64 time=0.023 ms
64 bytes from ddws (192.168.1.73): icmp_seq=9 ttl=64 time=0.021 ms
64 bytes from ddws (192.168.1.73): icmp_seq=10 ttl=64 time=0.024 ms
^C
--- dnsproject.prepa.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9219ms
rtt min/avg/max/mdev = 0.011/0.022/0.026/0.004 ms
```

# Job 5 : Nom de domaine

Pour obtenir un nom de domaine il faut dans un premier temps **choisir un nom** et en **vérifier la disponibilité**. Puis il faut choisir une **extension de domaine**, ce choix dépend de la nature du site.

Par la suite il faut **enregistrer** son nom de domaine au près du **registar** (bureau d'enregistrement) accrédité de son choix. Il faut alors fournir des informations de contact précises.

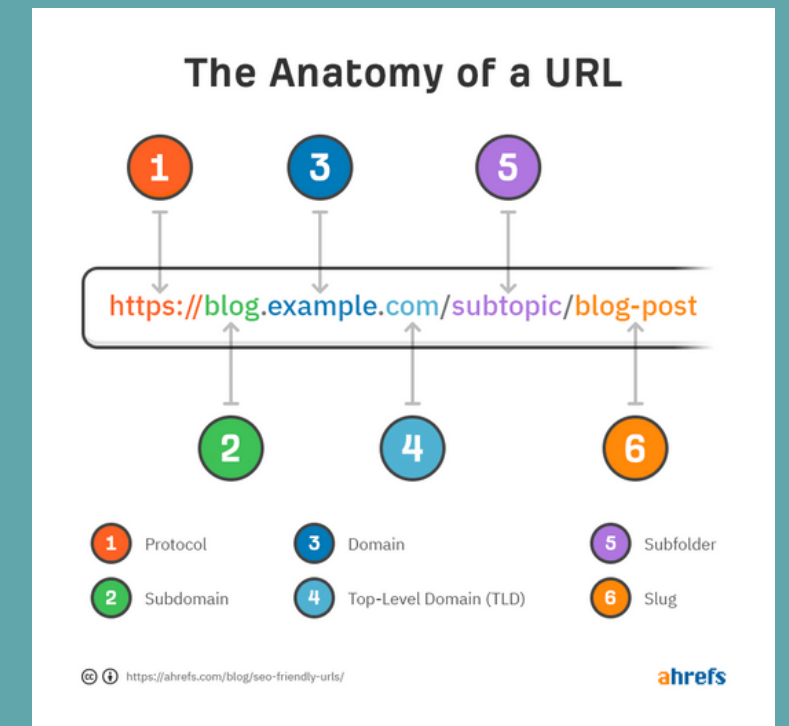
Enfin il faut **payer les frais d'enregistrement** pour réserver le nom de domaine, la plus part des domaines sont enregistré pour une durée d'un an renouvelable.

# Les extensions de domaines

Il existe trois types d'extension de domaines : les Top-Level domaine génériques, les TLD sponsorisés et les TLD avec code pays.

## Les TLD génériques :

Elle comprend les extension connues tel que : .com, .org, .net. Elle sont "génériques" par opposition aux extension à code pays. En 2011, l'ICANN autorise les organisations a enregistrer leurs extensions de domaines génériques.



# Les TLD Sponsorisés

**Les TLD sponsorisés** sont des extensions utilisé par des entités spécifiques, des entreprises, une branche du gouvernement ou un autre type de groupe. On retrouve dans cette catégorie : .gouv, .edu.

## Les TLD avec code pays

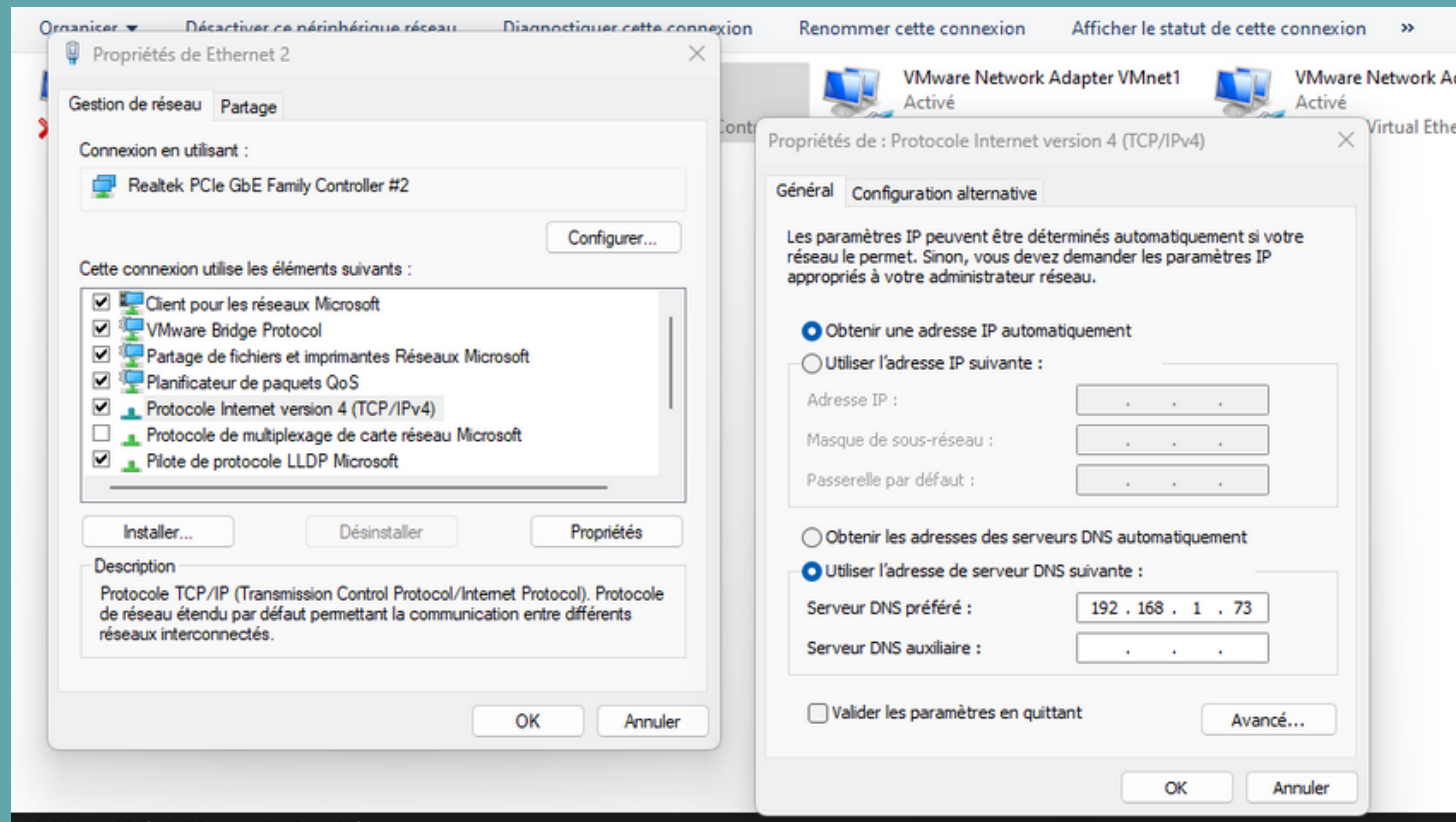
Elles représentent un pays spécifique, comme .ru pour la Russie. Certaines sont réservées auxx organisation du pays, d'autres sont accessible à tous.

Parmi les plus courants on retrouve : .jp, .cn, .fr, .de

# Job 6 : Connexion de la machine hôte

Sous windows :

1. Ouvrez les "**Paramètres**" puis allez dans "**Réseau et Internet**".
2. Cliquez sur "**Modifier les options de l'adaptateur**".
3. Cliquez avec le bouton droit de la souris sur votre connexion réseau active et sélectionnez "**Propriétés**".
4. Cochez "**Protocole Internet version 4 (TCP/IPv4)**" et cliquez sur "**Propriétés**".
5. Sélectionnez "**Utiliser l'adresse de serveur DNS suivante**" et ajoutez l'adresse IP de votre machine virtuelle.





# Job 7 : Pare-feu

Pour installer le pare-feu :

- `sudo apt update`
- `sudo apt install ufw`
- `sudo ufw allow 80/tcp`
- `sudo ufw allow 443/tcp`

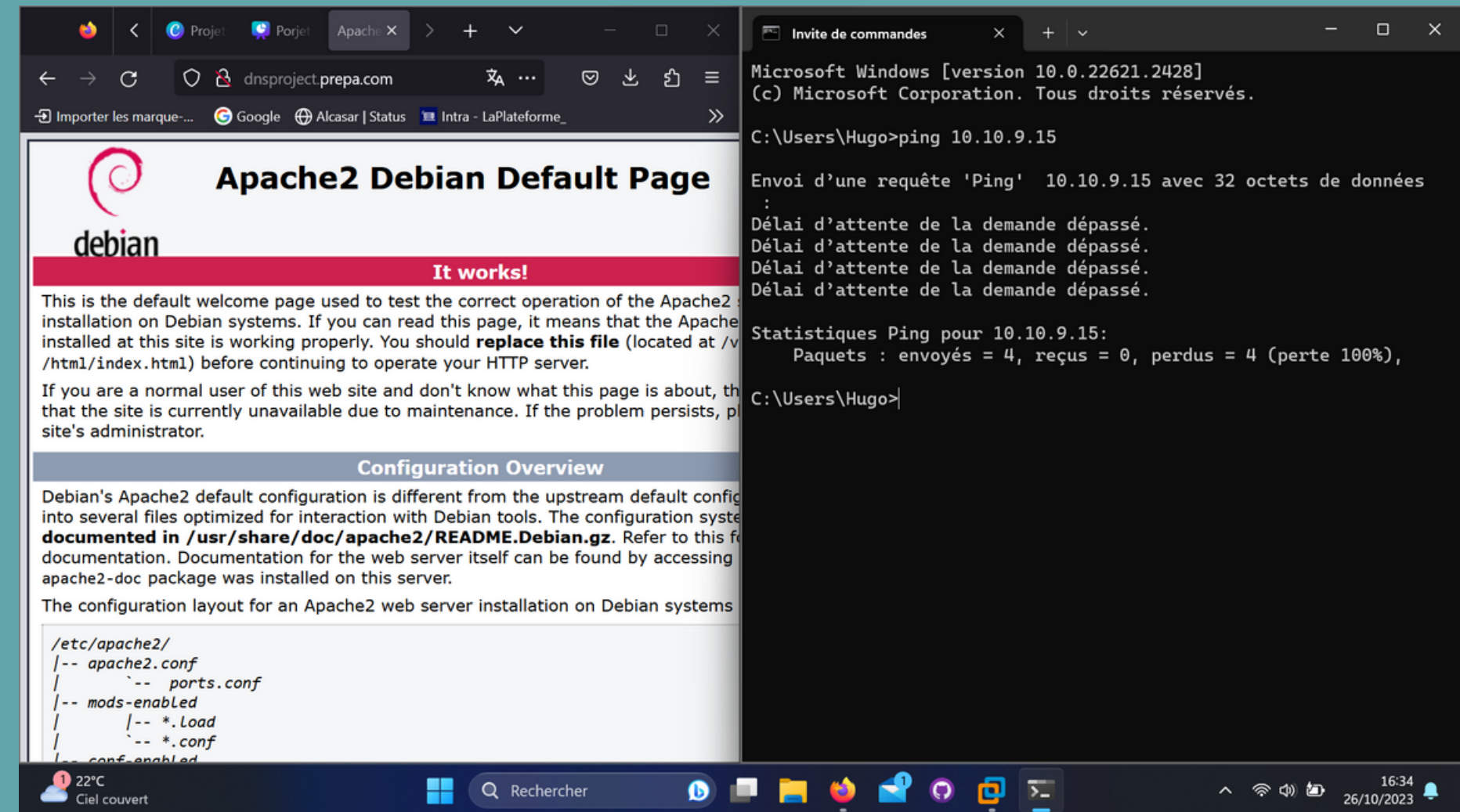
pour bloquer les ping :

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

Là, nous allons localiser les codes ok icmp pour la section INPUT et modifier la ligne suivante:

- A ufw-before-input -p icmp --icmp-type echo-request -j **DROP**

- `ufw disable && ufw enable`





# Job 8 : Dossier partagé

Pour mettre en place un fichier partagé on va utiliser Samba.

pour installer Samba :

- `sudo apt update`
- `sudo apt install samba`

Pour vérifier le statut du serveur Samba :

- `systemctl status smbd`

Pour activer le démarrage automatique de SMBD :

- `systemctl enable smbd`



# Créer le partage sous Samba

Il faut configurer le partage dans smb.conf:

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

Ajouter le paragraphe suivant :  
cf capture d'écran

Puis redémarrez le service smbd:

- `sudo systemctl restart smbd`

```
[partage]
comment = Partage de fichiers
path = /home/srv/partage
guest ok = no
read only = no
browseable = yes
valid users = @partage
create mask = 0660
directory mask = 0770
force group = partage
```

# Créer un utilisateur et le groupe “partage”

Créer l'utilisateur “user” :

- `adduser user`

déclarer l'utilisateur et lui créer un mot de passe Samba :

- `smbpasswd -a user`

créer un groupe partage :

- `groupadd partage`

Ajouter l'utilisateur “user” au groupe “partage”

- `gpasswd -a user partage`

# Préparer le dossier du partage

Commençons par créer le dossier :

- `sudo mkdir /home/srv/partage`

Attribuer le groupe “partage” comme groupe propriétaire de ce dossier :

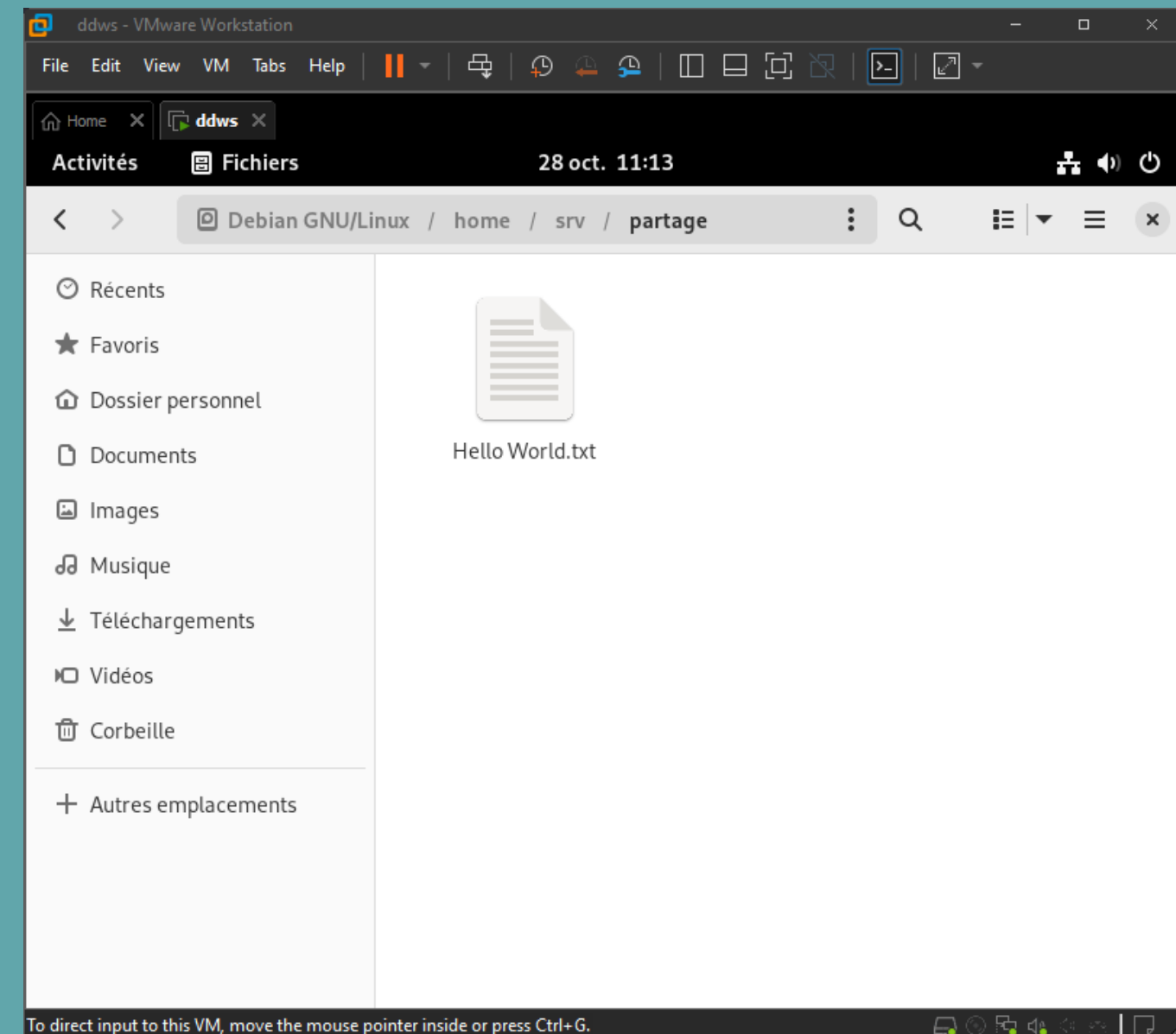
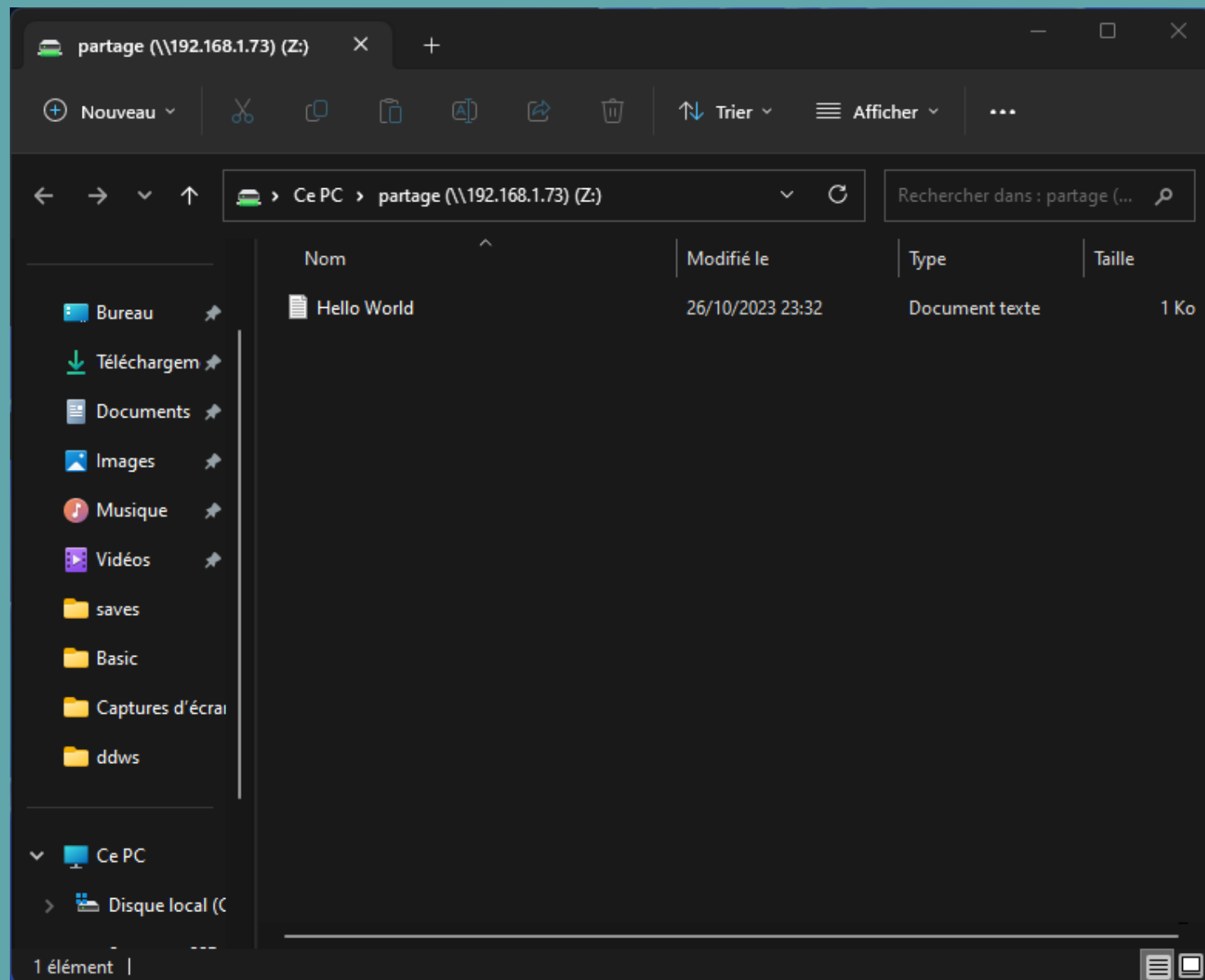
- `sudo chgrp -R partage /home/srv/partage/`

Ajouter les droits de lecture/écriture :

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

# Accéder au partage Samba depuis Windows

On peut se connecter au dossier via un chemin UNC directement dans la barre d'adresse de l'Explorateur de fichiers. Il faut ensuite s'authentifier avec le compte et le mot de passe mis en place avec la commande "smbpasswd".



# Certificat pour serveur web

# Génération du certificats

Dans un premier temps installer le paquet OpenSSL si ce n'est pas déjà fait :

- `sudo apt update`
- `sudo apt install openssl`

Puis afin de générer le certificat sa clé saisir la commande suivante :

- `openssl req -x509 -nodes -days 365 -newkey rsa:2048 -sha256 -out /etc/apache2/server.crt -keyout /etc/apache2/server.key`

Cette commande permet d'obtenir un certificat valable un an et sa clé privé. la clé n'est en revanche pas crypté (-nodes). Sinon un mot de passe serait demandé à chaque démarrage du serveur.

Pendant la génération le service demande des informations sur votre identité :

On modifie en suite les permission dur la clé :

- `chmod 440 /etc/apache2/server.crt`

[illegible]



# Configuration d'Apache

Il faut indiquer à Apache les nouveaux fichiers de configuration. Pour ce faire il faut éditer le fichier `default-ssl.conf` :

- `sudo nano /etc/apache2/sites-available/default-ssl.conf`

Dans ce fichier modifier le chemin de ces deux options :

- `SSLCertificateFile`      `/etc/apache2/server.crt`
- `SSLCertificateKeyFile` `/etc/apache2/server.key`

```
#Include conf-available/serve-cgi-bin.conf

#   SSL Engine Switch:
#   Enable/Disable SSL for this virtual host.
SSLEngine on

#   A self-signed (snakeoil) certificate can be created by
#   the ssl-cert package. See
#   /usr/share/doc/apache2/README.Debian.gz for more info.
#   If both key and certificate are stored in the same file,
#   the SSLCertificateFile directive is needed.
SSLCertificateFile      /etc/apache2/server.crt
SSLCertificateKeyFile   /etc/apache2/server.key
```

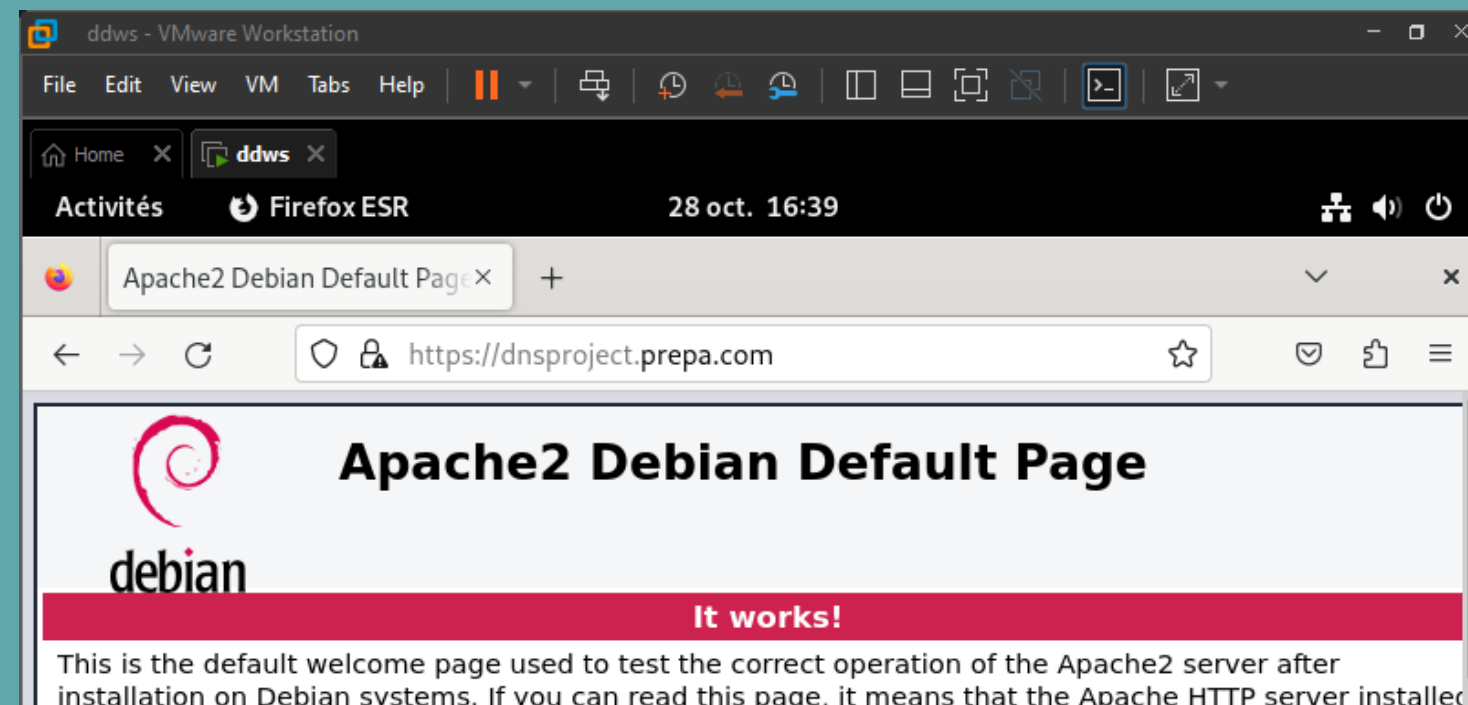
# Activer le module SSL et le site SSL

Les lignes de commandes suivantes permettent d'activer le module SSL, le site et de redémarrer le service

`a2enmod ssl`

`a2ensite default-ssl`

`systemctl reload apache2`



# La différence entre les certificats SSL donnés par des organismes extérieurs et le vôtre auto-signé ?

Un réel certificat doit être signé par **une autorité de certification** (CA) pour être **signé et valide**, comme par exemple Verisign, Thawte ou encore CertiSign. En ce qui nous concerne, nous avons généré un certificat **auto-signé** (**donc non certifié**) qui est gratuit et très bien pour une utilisation personnelle puisqu'il n'offre pas les mêmes garanties en terme de sécurité. Notamment parce que **n'importe qui peut auto-signer un certificat** donc ça ne vérifie pas l'identité de l'émetteur.

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

Comme expliqué précédemment n'importe qui peut générer un certificat auto-signé de ce fait le navigateur ne reconnaît pas l'autorité de certification(CA). Il n'y a pas de vérification tierce donc pas de garantie que le site soit légitime.

Un attaquant pourrait hypothétiquement utiliser un certificat auto-signé pour s'interposer entre le client et le serveur et déchiffrer le trafic. Sans tiers pour valider ce certificat ce n'est pas une méthode sûre d'authentification par le navigateur.

Enfin les certificats émis par les CA vérifient l'identité du serveur, l'utilisateur a alors la certitude qu'il se connecte au site qu'il prétend être.