

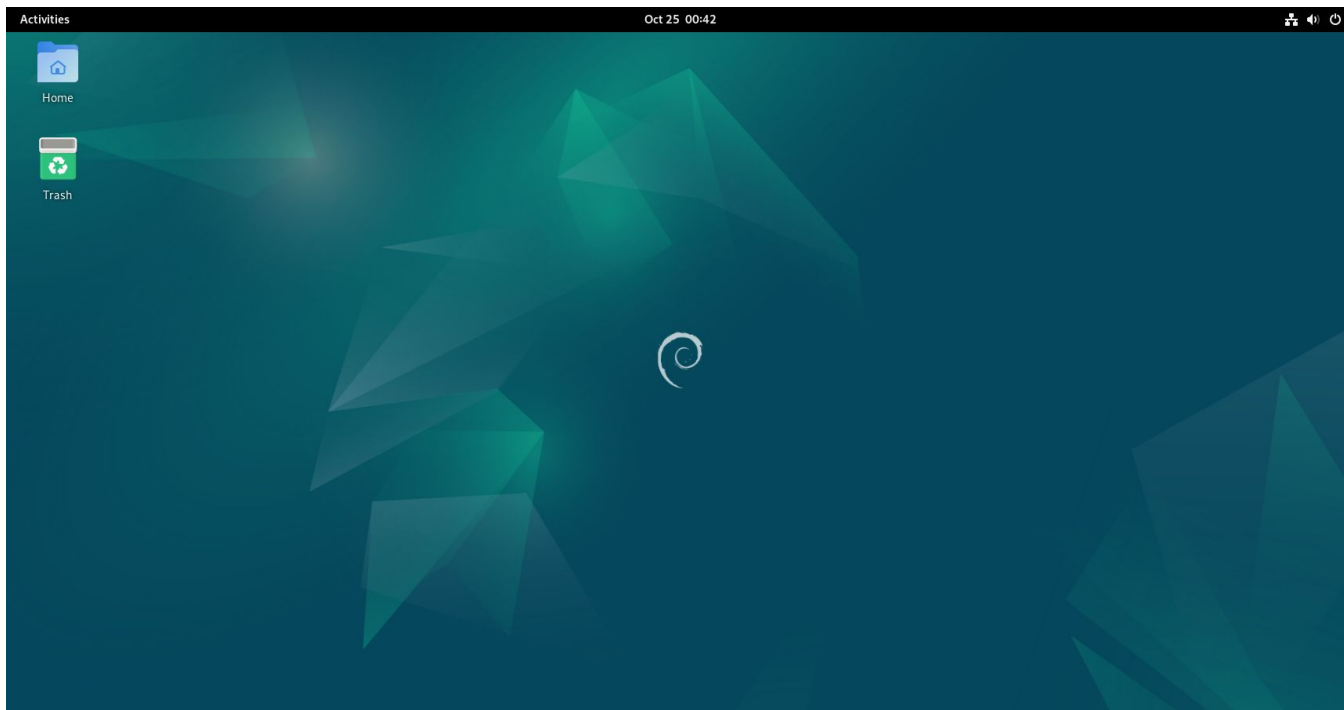


La Plateforme

DDWS-DOC

SAID ALI TSARAVELONA ALLAQUI

JOB 01 – INSTALLER DEBIAN AVEC INTERFACE GRAPHIQUE



Dans le cadre de cette activité, j'opte pour une machine virtuelle Debian dotée d'une interface graphique.

Avec comme hyperviseur VMWare.

JOB 2 – METTRE EN PLACE APACHE2 ET DÉMARRER LE SERVICE.

Installer Apache2 en utilisant la commande suivante : *sudo apt install apache2*

```
root@debian:/home/goldroger# sudo apt install apache2
```

Ensuite, nous installerons **ufw** pour cela, la commande à utiliser est : *sudo apt install ufw*.

```
root@debian:/home/goldroger# apt install ufw
```

Une fois installé, nous autoriserons les ports **TCP 80** et **443** dans le **pare-feu** en utilisant les commandes suivantes : *sudo ufw allow 80/tcp* et *sudo ufw allow 443/tcp*.

```
root@debian:/home/goldroger# sudo ufw allow 80/tcp
Rules updated
Rules updated (v6)
root@debian:/home/goldroger# sudo ufw allow 443/tcp
Rules updated
Rules updated (v6)
root@debian:/home/goldroger# █
```

ufw (**Uncomplicated Firewall**), un programme permettant de gérer le pare-feu.

pare-feu, un dispositif logiciel ou matériel qui contrôle et filtre le trafic réseau entre un réseau privé et public. Son rôle principal est de protéger un système informatique en régulant les communications entrantes et sortantes, autorisant ou bloquant le trafic en fonction de règles prédéfinies.

Ensuite, nous vérifierons si Apache2 est en cours d'exécution avec la commande :
sudo systemctl status apache2.

Si le statut affiche "**active (running)**", cela signifie qu'Apache2 est en cours d'exécution.

```
root@debian:/home/goldroger# 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 00:50:28 CEST; 7min ago
     Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 30238 (apache2)
    Tasks: 55 (limit: 9452)
   Memory: 18.9M
      CPU: 126ms
   CGroup: /system.slice/apache2.service
           └─30238 /usr/sbin/apache2 -k start
             └─30239 /usr/sbin/apache2 -k start
               └─30240 /usr/sbin/apache2 -k start

Oct 25 00:50:28 debian systemd[1]: Starting apache2.service - The Apache HTTP Server...
Oct 25 00:50:28 debian apachectl[30237]: AH00558: apache2: Could not reliably determine the server's fully
Oct 25 00:50:28 debian systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-16/16 (END)
```

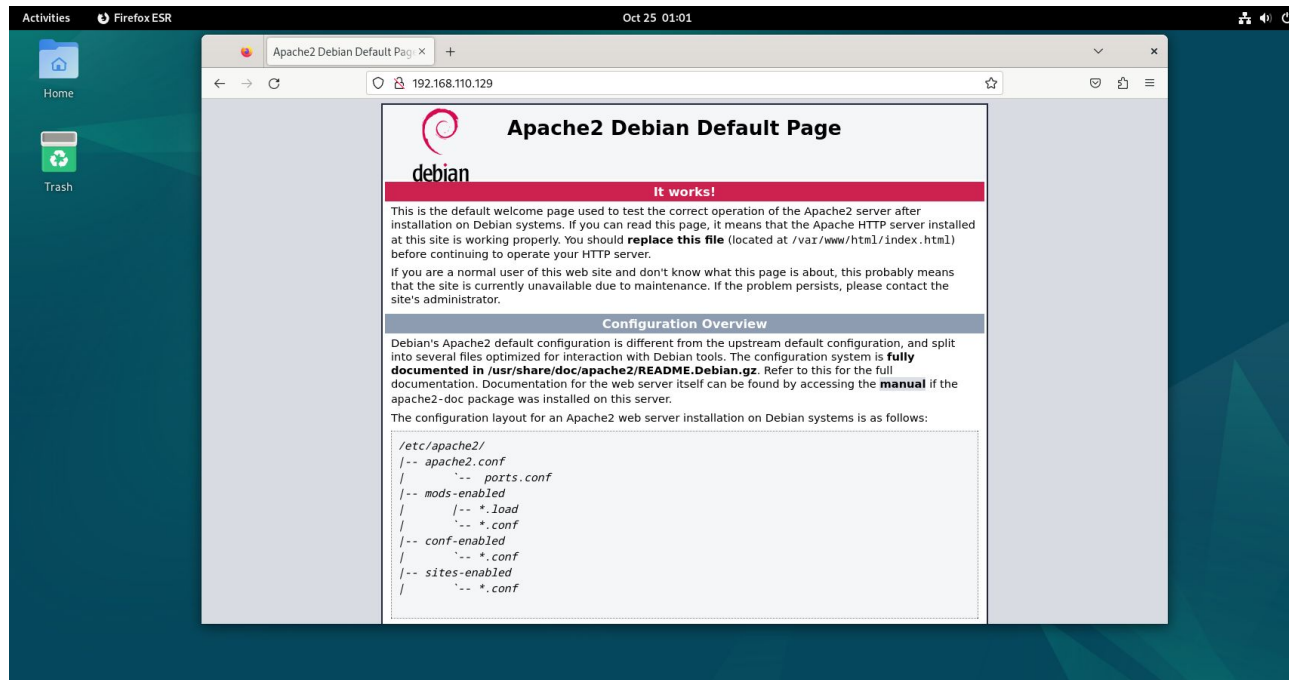
Enfin, pour obtenir l'adresse IP du serveur, nous utiliserons la commande : *hostname -I*

```
root@debian:/home/goldroger# hostname -I
192.168.110.129
root@debian:/home/goldroger#
```

hostname (*nom d'hôte*), un label assigné à un périphérique sur un réseau, permettant de l'identifier de manière unique. C'est souvent associé à une adresse IP pour faciliter la communication au sein du réseau.

Par exemple : **192.168.110.129**

Vous pouvez ensuite copier cette adresse IP (**192.168.110.129**) et la saisir dans votre navigateur pour accéder au serveur.



JOB 03 – AVANTAGES ET INCONVÉNIENTS DES DIFFÉRENTS SERVEURS WEB

Il existe plusieurs serveurs web populaires, chacun ayant ses propres avantages et inconvénients. Voici une liste de quelques-uns d'entre eux :

1. Apache HTTP Server :

Apache est l'un des serveurs web les plus anciens et les plus utilisés. Il est open source et fonctionne sur la plupart des systèmes d'exploitation, y compris Linux, Unix, Windows, et plus encore.

Avantages : Stabilité, robustesse, modularité grâce à des modules tiers, une grande communauté de soutien.

Inconvénients : Peut être un peu plus lourd en termes de consommation de ressources comparé à certains autres serveurs web.

2. Nginx :

Nginx est un serveur web open source et un serveur proxy inverse. Il est connu pour sa légèreté et sa capacité à gérer de nombreux utilisateurs simultanément.

Avantages : Hautement performant, capable de gérer de nombreuses connexions simultanées, excellent pour servir du contenu statique, supporte les technologies modernes comme WebSocket

Inconvénients : Moins flexible pour le traitement de contenu dynamique par rapport à Apache.



3. Microsoft Internet Information Services (IIS) :

IIS est le serveur web de Microsoft, principalement utilisé sur les systèmes d'exploitation Windows Server.

Avantages : Intégration étroite avec d'autres produits Microsoft, support natif pour les technologies Microsoft comme ASP.NET.

Inconvénients : Moins couramment utilisé en dehors des environnements Windows, peut ne pas être aussi performant que certains serveurs web open source.



4. LiteSpeed Web Server :

LiteSpeed est un serveur web commercial qui se vante d'être un remplaçant direct d'Apache, offrant une meilleure performance.

Avantages : Haute performance, compatibilité avec les configurations Apache, consommation de ressources relativement faible.

Inconvénients : Licence commerciale avec une version gratuite limitée.

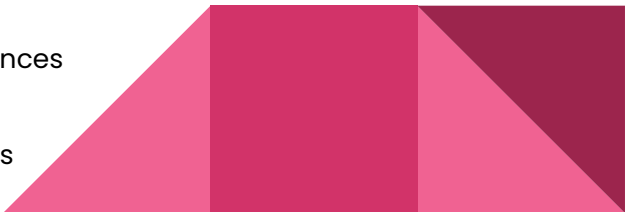


5. Caddy :

Caddy est un serveur web open source qui se distingue par sa configuration automatique, la gestion automatique du certificat SSL et son utilisation facile.

Avantages : Configuration automatique, gestion facile des certificats SSL, performances solides.

Inconvénients : Peut ne pas être aussi adapté pour des scénarios complexes ou des configurations très spécifiques.



JOB 04 – MISE EN PLACE D'UNE CONFIGURATION DNS

Pour associer l'adresse IP de notre serveur à un nom de domaine, on commence par installer **Bind9**, en utilisant la commande suivante : `sudo apt install bind9`

```
goldroger@debian:~$ sudo apt install bind9
```

Ensuite, on procède à la configuration du serveur DNS. Pour cela on va éditer le fichier de configuration de **Bind** en utilisant la commande : `sudo nano /etc/bind/named.conf.local`

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

On va ajouter la zone de notre domaine dans le fichier de configuration, enregistrez les modifications, puis quittez.

bind9 ou simplement **BIND** (**Berkeley Internet Name Domain**), est un logiciel serveur DNS (Domain Name System) open source largement utilisé sur Internet.

Il est principalement utilisé pour la résolution de noms de domaine en adresses IP et pour la gestion des zones DNS.



```

goldroger@debian: ~
GNU nano 7.2 /etc/bind/named.conf.local
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

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

[Read 12 lines]

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

```

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


On va maintenant créer et éditer le fichier de zone avec la commande : `sudo nano /etc/bind/db.dnsproject.prepa.com`

```
goldroger@debian:~$ sudo nano /etc/bind/db.dnsproject.prepa.com
```

On va ajouter les enregistrements de zone dans le fichier, enregistrer les modifications, puis quitter.



```
goldroger@debian: ~
GNU nano 7.2 /etc/bind/db.dnsproject.prepa.com *
$TTL      604800
@         IN      SOA      dnsproject.prepa.com. admin.dnsproject.prepa.com. (
                                2023102501 ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
;
@         IN      NS       dnsproject.prepa.com.
@         IN      A        192.168.110.129

^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
```

Redémarrez le service bind9 pour appliquer les modifications :
`sudo systemctl restart bind9`

```
goldroger@debian:~$ sudo systemctl restart bind9
```

Ensuite on va ajouter l'adresse IP du serveur DNS dans le fichier `/etc/resolv.conf` en utilisant la commande :
`sudo nano /etc/resolv.conf`

```
goldroger@debian:~$ sudo nano /etc/resolv.conf
```

On va ajouter la ligne "nameserver + adresse IP du serveur", enregistrer les modifications, puis quitter.

```
nameserver 192.168.110.129
```

Enfin, on va maintenant tester la résolution DNS en effectuant un ping sur le nom de domaine : dnsproject.prepa.com

Si tout est configuré correctement, le ping devrait réussir et aboutir à notre adresse IP.

```
goldroger@debian:~$ ping dnsproject.prepa.com
PING dnsproject.prepa.com (192.168.110.129) 56(84) bytes of data.
64 bytes from debian (192.168.110.129): icmp_seq=1 ttl=64 time=0.053 ms
64 bytes from debian (192.168.110.129): icmp_seq=2 ttl=64 time=0.083 ms
64 bytes from debian (192.168.110.129): icmp_seq=3 ttl=64 time=0.063 ms
64 bytes from debian (192.168.110.129): icmp_seq=4 ttl=64 time=0.052 ms
64 bytes from debian (192.168.110.129): icmp_seq=5 ttl=64 time=0.044 ms
64 bytes from debian (192.168.110.129): icmp_seq=6 ttl=64 time=0.065 ms
64 bytes from debian (192.168.110.129): icmp_seq=7 ttl=64 time=0.027 ms
64 bytes from debian (192.168.110.129): icmp_seq=8 ttl=64 time=0.066 ms
64 bytes from debian (192.168.110.129): icmp_seq=9 ttl=64 time=0.033 ms
64 bytes from debian (192.168.110.129): icmp_seq=10 ttl=64 time=0.053 ms
64 bytes from debian (192.168.110.129): icmp_seq=11 ttl=64 time=0.068 ms
^C
--- dnsproject.prepa.com ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10076ms
rtt min/avg/max/mdev = 0.027/0.055/0.083/0.015 ms
goldroger@debian:~$
```

BINGO, ÇA PING SUR NOTRE IP ! 🚀



JOB 05 – COMMENT OBTIENT-ON UN NOM DE DOMAINE PUBLIC ?

Pour réserver un nom de domaine, le processus implique plusieurs étapes clés qui mettent en jeu différents acteurs du domaine de l'enregistrement des noms de domaine. Voici une procédure détaillée :

1. Sélection du Nom de Domaine :

Commencez par choisir un nom de domaine pertinent et représentatif de votre site ou entreprise. Assurez-vous qu'il est facilement mémorisable et qu'il correspond à vos objectifs.

2. Choix du Registraire :

Un registraire est un intermédiaire entre le propriétaire du nom de domaine (le registrant) et l'organisme de gestion des noms de domaine (le registre). Choisissez un registraire de confiance réputé pour ses services et sa conformité aux normes.

3. Vérification de la Disponibilité :

Utilisez l'interface en ligne du registraire pour vérifier la disponibilité du nom de domaine souhaité. Respectez les règles de syntaxe et de droits spécifiques à chaque extension.

4. Fourniture des Informations et Documents :

Entamez le processus d'enregistrement en fournissant les informations requises. Celles-ci incluent généralement les coordonnées du registrant (vous, en tant que propriétaire du domaine) et du contact administratif. Certains registrars peuvent également demander des documents supplémentaires pour des extensions spécifiques ou pour des raisons de vérification.

nom de domaine public, C'est une adresse unique sur Internet qui permet d'identifier un site web, et de la rendre accessible en ligne. Il sert de lien entre les utilisateurs et les serveurs hébergeant le contenu associé à ce nom de domaine.

Les noms de domaine publics sont enregistrés auprès de registrars et sont soumis à une gestion centralisée pour assurer leur unicité et leur fonctionnement dans le système de noms de domaine (DNS)

5. Paiement de la Transaction :

Une fois les détails fournis, procédez au paiement de la transaction. Les registrars acceptent généralement diverses méthodes de paiement. Assurez-vous de suivre les protocoles de sécurité pour protéger vos informations financières.

6. Options de Services Complémentaires :

Certains registrars proposent des services complémentaires tels que l'hébergement web, la protection de la vie privée du domaine, des certificats SSL, ou encore la création d'adresses email associées au domaine. Explorez ces options selon vos besoins.

7. Configuration des Paramètres DNS :

Accédez à votre compte chez le registraire pour configurer les paramètres DNS de votre domaine. Cela peut inclure la gestion des enregistrements MX, CNAME, et d'autres configurations nécessaires à votre site.

8. Renouvellement Périodique :

Les noms de domaine sont généralement enregistrés pour une période déterminée (par exemple, un an). Assurez-vous de renouveler votre enregistrement avant l'expiration pour éviter de perdre la propriété de votre domaine.

registrar , Un registrar est essentiellement un intermédiaire agréé qui facilite l'enregistrement et la gestion des noms de domaine.

Ces entreprises sont autorisées par les organismes de réglementation des domaines (comme l'ICANN) et permettent aux individus et aux entreprises d'acheter, renouveler et gérer leurs noms de domaine.

En gros, ils sont comme des courtiers pour les adresses web.

QUELLES PARTICULARITÉS PEUVENT ÊTRE ASSOCIÉES À CERTAINES EXTENSIONS DE NOMS DE DOMAINE ?

L'extension d'un nom de domaine constitue la dernière partie de celui-ci et joue un rôle crucial tant pour les visiteurs que pour les moteurs de recherche. Voici les points à considérer, classés par ordre d'importance :

1. Confiance des visiteurs :

- Les extensions courantes comme ".com", ".net" et ".org" renforcent la confiance des visiteurs.
- Les extensions moins connues telles que ".zip", ".biz", ou ".info" peuvent susciter la méfiance en raison de leur utilisation fréquente par des spammeurs et des cybercriminels.

2. Particularités géographiques :

- Les extensions reflètent parfois la zone géographique, comme ".fr" pour la France ou ".be" pour la Belgique.
- Les extensions géographiques peuvent favoriser le trafic localisé, augmentant ainsi les chances de conversion en prospects ou clients.



3. Score de confiance élevé :

- Pour les institutions telles que les universités ou les organismes gouvernementaux, l'utilisation d'extensions comme ".edu" ou ".org" peut améliorer le score de confiance auprès des moteurs de recherche.
- Cependant, il est crucial de ne pas abuser de ces extensions pour éviter de tromper les internautes et les moteurs de recherche.

4. Types d'extensions :

- Extensions génériques : Comme ".com", ".org", ou ".net", largement utilisées sans exigences particulières.
- Extensions géographiques : Représentant des pays, villes ou régions spécifiques, telles que ".fr" ou ".paris".
- Extensions spécifiques : Réservées à des secteurs ou entreprises spécifiques, comme ".news" pour l'information, ".blog" pour les blogs, ou ".tech" pour des activités particulières.
- Extensions restreintes : Dédiées à des entités spécifiques, comme ".gouv" pour les branches gouvernementales ou ".edu" pour les institutions éducatives.
- Extensions de marque : La propriété d'une entreprise ou d'une marque, comme ".google", ".apple" ou ".amazon", avec des conditions d'enregistrement strictes.

En conclusion, le choix de l'extension de domaine est crucial, influençant la confiance des visiteurs, la pertinence géographique, le score de confiance, et s'alignant avec la nature spécifique d'une entité, qu'elle soit une institution, une entreprise sectorielle, ou une marque.



JOB 06 – ÉTABLIR LA CONNEXION ENTRE NOTRE HÔTE ET LE DOMAINE LOCAL

Pour associer l'adresse IP de notre serveur à un nom de domaine, la première étape consiste à modifier le fichier `hosts` en y ajoutant l'adresse IP et le nom de domaine.

Pour ce faire, utilisez la commande suivante : `sudo nano /etc/hosts` et ajoutez l'IP ainsi que le nom de domaine.

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

Ensuite, on redémarre le service DNS avec la commande : `sudo systemctl restart networking`

```
goldroger@debian:~$ sudo systemctl restart networking
```

Passons maintenant à la configuration d'Apache sur notre serveur. Accédez au répertoire de configuration d'Apache en utilisant la commande : `cd /etc/apache2/sites-available`

```
goldroger@debian:~$ cd /etc/apache2/sites-available
goldroger@debian:/etc/apache2/sites-available$ ls
000-default.conf default-ssl.conf
```

hosts, un fichier texte local qui associe des adresses IP à des noms de domaine.

Il est utilisé pour résoudre les noms de domaine en adresses IP localement, contournant ainsi le besoin de consulter un serveur DNS distant.

Lorsque vous essayez d'accéder à un site Web, votre système d'exploitation vérifie d'abord le fichier `hosts` pour voir s'il contient une entrée correspondant au nom de domaine que vous essayez d'atteindre.

On va maintenant créer et éditer un fichier de virtual host pour notre serveur en utilisant la commande : `dnsproject.prepa.com.conf` et ajoutez une configuration de base.



```
goldroger@debian: /etc/apache2/sites-available
GNU nano 7.2 dnsproject.prepa.com.conf
<VirtualHost *:80>
    ServerAdmin webmaster@dnsproject.prepa.com
    ServerName dnsproject.prepa.com
    DocumentRoot /var/www/html
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Ensuite, activez le site et redémarrez Apache avec les commandes suivantes : `sudo a2ensite dnsproject.prepa.com.conf` suivi de `sudo systemctl restart apache2`



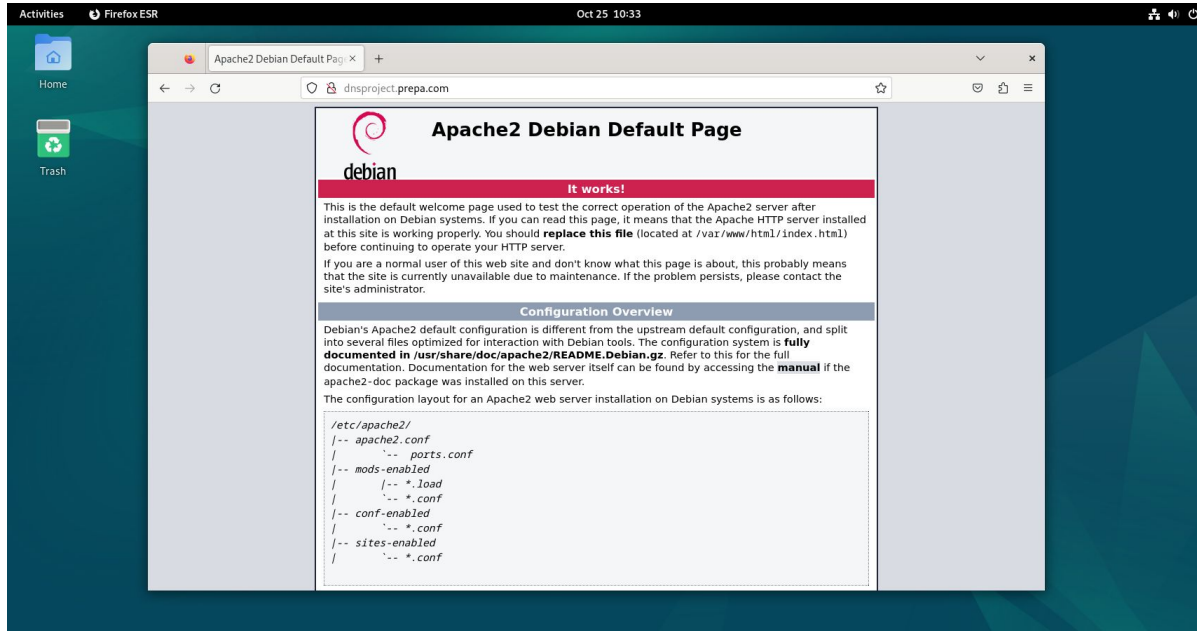
```
goldroger@debian: /etc/apache2/sites-available$ sudo a2ensite dnsproject.prepa.com.conf
Enabling site dnsproject.prepa.com.
To activate the new configuration, you need to run:
    systemctl reload apache2
goldroger@debian: /etc/apache2/sites-available$ sudo systemctl restart apache2
goldroger@debian: /etc/apache2/sites-available$
```

a2ensite, une commande utilisée sur les systèmes d'exploitation basés sur Apache, tels que Linux, pour activer un site web spécifique (virtual host) configuré dans Apache.

Lorsque vous exécutez la commande **sudo a2ensite nom_du_site.conf**, elle crée un lien symbolique du fichier de configuration du site depuis le répertoire sites-available vers le répertoire sites-enabled.

Cela permet à Apache de prendre en compte la configuration du site lors de son fonctionnement.

Vérifions maintenant si notre configuration a été appliquée en accédant à notre nom de domaine : **dnsproject.prepa.com**



Tout semble fonctionner correctement !



JOB 07 – CONFIGURER UN PARE-FEU SUR NOTRE SERVEUR AFIN D'EMPÊCHER LES REQUÊTES DE PING.

En premier lieu, l'étape initiale consiste à installer **ufw**, cependant, comme nous l'avons déjà installé antérieurement et avons autorisé les ports, nous allons sauter cette étape.

Pour bloquer les requêtes ping, nous nous rendrons dans le répertoire **/etc/ufw/** et éditerons le fichier **before.rules** en utilisant la commande **sudo nano before.rules**

Ensuite, en parcourant le fichier jusqu'au paramètre **INPUT**, situé à la quatrième ligne où **echo-request** est défini en **ACCEPT**

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

On le modifie en le remplaçant par **DROP**

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

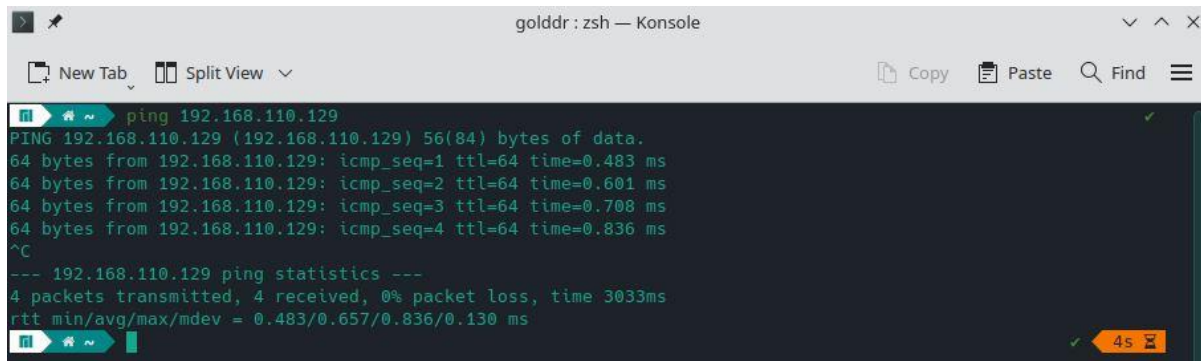


Après avoir effectué cette modification, on sauvegarde le fichier.

Il est crucial de recharger le pare-feu pour appliquer ces changements, ce que nous ferons en utilisant la commande : **sudo ufw reload**

```
root@debian:/etc/ufw# sudo ufw reload
Firewall reloaded
```

AVANT LE BLOCAGE - Les pings à partir d'une machine externe sont autorisés.



```
golddr: zsh — Konsole
New Tab Split View
Copy Paste Find
ping 192.168.110.129
PING 192.168.110.129 (192.168.110.129) 56(84) bytes of data.
64 bytes from 192.168.110.129: icmp_seq=1 ttl=64 time=0.483 ms
64 bytes from 192.168.110.129: icmp_seq=2 ttl=64 time=0.601 ms
64 bytes from 192.168.110.129: icmp_seq=3 ttl=64 time=0.708 ms
64 bytes from 192.168.110.129: icmp_seq=4 ttl=64 time=0.836 ms
^C
--- 192.168.110.129 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3033ms
rtt min/avg/max/mdev = 0.483/0.657/0.836/0.130 ms
4s
```



APRÈS LE BLOCAGE - Aucune communication n'est établie.



```
golddr: zsh — Konsole
New Tab Split View
Copy Paste Find
ping 192.168.110.129
PING 192.168.110.129 (192.168.110.129) 56(84) bytes of data.
^C
--- 192.168.110.129 ping statistics ---
11 packets transmitted, 0 received, 100% packet loss, time 10129ms
1 X 11s
```



JOB 08 – CRÉATION D'UN DOSSIER RÉSEAU PARTAGÉ

Nous allons mettre en place notre dossier partagé en utilisant **Samba**,
Pour commencer l'installation, exécutez la commande suivante : **sudo apt install samba**

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

Ensuite, créons un répertoire qu'on va nommer "**shared_folder**", que nous partagerons en réseau. Utilisez la commande : **mkdir shared_folder**

```
goldroger@debian:~$ mkdir shared_folder
```

```
goldroger@debian:~$ ls
```

Desktop	Downloads	Music	Public	shell	Templates
Documents	le_reseau	Pictures	shared_folder	shell-exe	Videos

Afin de permettre aux membres du réseau de lire et écrire dans notre répertoire, ajustons les autorisations avec la commande : **chmod -R 777 shared_folder**

```
goldroger@debian:~$ chmod -R 777 shared_folder
```

```
goldroger@debian:~$ ls -l
```

```
total 48
```

```
drwxrwxrwx  2 goldroger goldroger 4096 Oct 25 22:08 shared_folder
```

Samba est une suite de logiciels open source permettant le partage de fichiers et d'imprimantes entre systèmes d'exploitation différents, notamment entre Linux et Windows

Ajoutons notre utilisateur à la base de données de Samba et définissons un mot de passe avec la commande : `sudo smbpasswd -a + user`

```
goldroger@debian:~$ sudo smbpasswd -a goldroger
[sudo] password for goldroger:
New SMB password:
Retype new SMB password:
goldroger@debian:~$
```

Maintenant, modifions le fichier de configuration de Samba situé à `/etc/samba/smb.conf` en utilisant la commande : `sudo nano /etc/samba/smb.conf`

```
goldroger@debian:~$ sudo nano /etc/samba/smb.conf
```

Ajoutons notre configuration en bas du fichier



```
goldroger@debian: ~
GNU nano 7.2 /etc/samba/smb.conf
# printer drivers
[shared_folder]
  path = /home/goldroger/shared_folder
  read only = no
  writable = yes
  guest ok = yes

```

[^]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

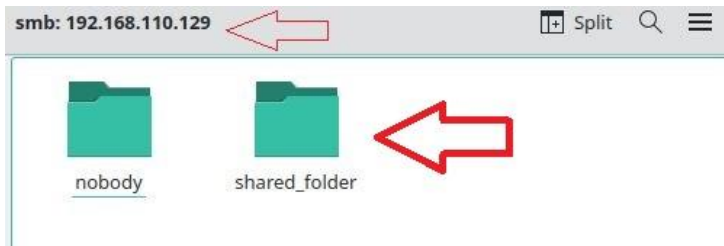


On enregistre les modifications, puis redémarrez le service Samba pour appliquer la configuration : `sudo service smb restart`

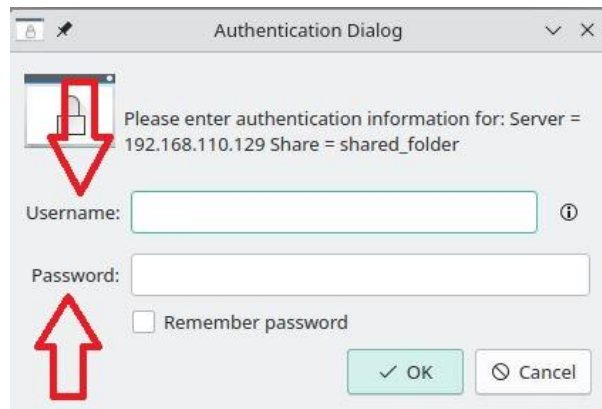
Testons si tout fonctionne. On peut accéder au dossier partagé en utilisant le gestionnaire de fichiers de notre environnement de bureau ou en utilisant l'adresse IP du serveur dans l'explorateur de fichiers : `smb://192.168.110.129`

Sous Manjaro

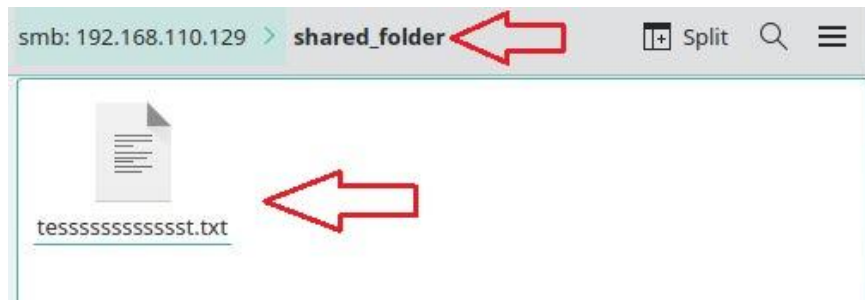
Nous sommes connectés à l'adresse IP du serveur et avons accès à notre dossier partagé.



Lorsqu'on vous demande de vous authentifier, entrez vos informations.



Si tout est configuré correctement, cela devrait fonctionner !



POUR ALLER PLUS LOIN...

Pour sécuriser notre serveur en activant le protocole HTTPS et installer un certificat, nous allons tout d'abord, installez **OpenSSL** en utilisant la commande suivante :

```
sudo apt install openssl
```

```
goldroger@debian:~$ sudo apt install openssl
[sudo] password for goldroger:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openssl is already the newest version (3.0.11-1~deb12u2).
openssl set to manually installed.
```

OpenSSL, une bibliothèque open source qui implémente les protocoles de sécurité SSL et TLS.

Elle est utilisée pour générer des certificats, assurer la sécurité des communications sur Internet, et offre des utilitaires en ligne de commande pour diverses opérations liées à la sécurité.

Dans le contexte d'un serveur web, OpenSSL est souvent utilisé pour créer des certificats SSL/TLS, permettant ainsi le chiffrement des données lors des connexions HTTPS.

Ensuite, générez un certificat auto-signé avec la commande suivante :

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout  
/etc/ssl/private/dnsproject.prepa.com.key -out /etc/ssl/certs/dnsproject.prepa.com.crt
```

```
goldroger@debian:~$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/dnsproject.prepa.com.key -out /etc/ssl/certs/dnsproject.prepa.com.crt
-----
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]:FR
Locality Name (eg, city) []:PARIS
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Plateformeurs
Organizational Unit Name (eg, section) []:Akatsuki
Common Name (e.g. server FQDN or YOUR name) []:Gol D Roger
Email Address []:pirate@king.ocean
goldroger@debian:~$
```



On va maintenant dans le répertoire `/etc/apache2/sites-available/` et modifiez le fichier `.conf` de notre site en ajoutant ces lignes :

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

```
GNU nano 7.2 /etc/apache2/sites-available/dnsproject.prepa.com.conf
<VirtualHost *:443>
    ServerAdmin webmaster@dnsproject.prepa.com
    ServerName dnsproject.prepa.com
    DocumentRoot /var/www/html

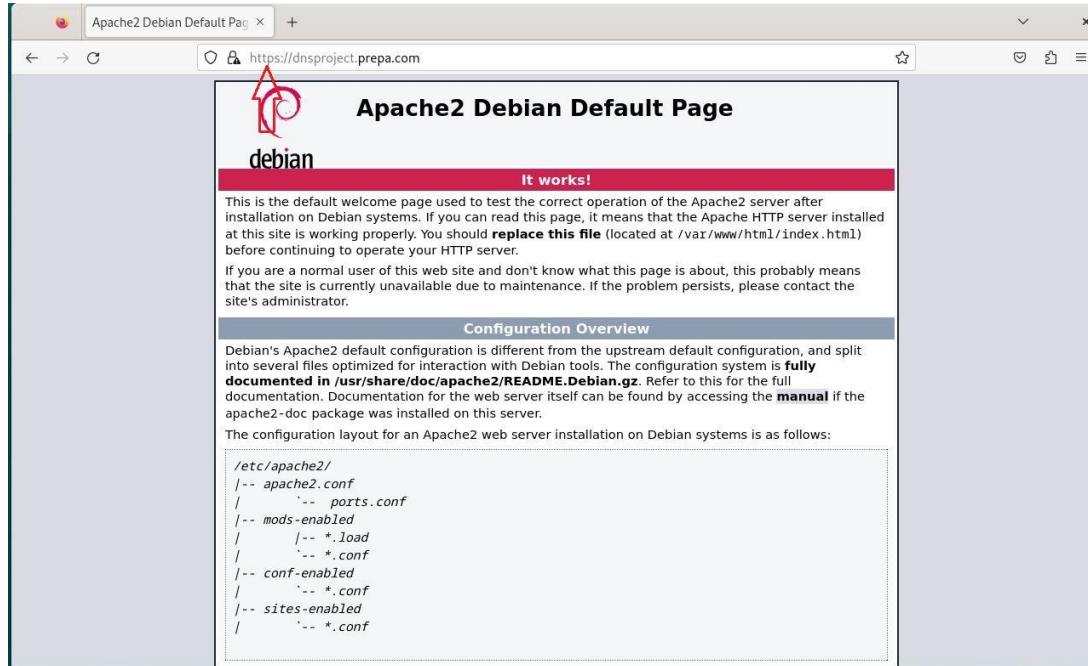
    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/dnsproject.prepa.com.crt
    SSLCertificateKeyFile /etc/ssl/private/dnsproject.prepa.com.key

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Sans oublier de remplacer le port 80 avec le port 443 pour activer la connexion https



Enfin, maintenant on active le module SSL avec la commande : `sudo a2enmod ssl` et redémarrez Apache pour appliquer les modifications : `sudo systemctl restart apache2`



systemctl, est une commande Linux utilisée pour contrôler les services système.

Elle permet de démarrer, arrêter, redémarrer des services, ainsi que d'activer ou désactiver leur démarrage automatique au boot

LA DIFFÉRENCE ENTRE LES CERTIFICATS SSL DONNÉS PAR DES ORGANISMES EXTÉRIEURS ET LE VÔTRE AUTO-SIGNÉ ?

Les certificats SSL, qu'ils soient délivrés par des organismes de certification externes (Certification Authorities - CA) ou auto-signés, sont utilisés pour sécuriser les communications sur Internet en établissant des connexions chiffrées entre les utilisateurs et les serveurs. Cependant, il y a des différences importantes entre ces deux types de certificats.

Certificats SSL délivrés par des organismes de certification externes :

1. Confiance universelle :

Les certificats SSL émis par des CA externes sont généralement inclus dans les listes de confiance des navigateurs. Cela signifie que lorsque vous utilisez un certificat émis par une CA, la plupart des navigateurs font confiance à ce certificat par défaut.

2. Validation approfondie :

Les CAs effectuent des vérifications approfondies pour s'assurer que le demandeur du certificat est légitime. Ces vérifications peuvent inclure des processus tels que la vérification du domaine, la vérification de l'organisation et d'autres procédures.



3. Coût :

Les certificats SSL émis par des CAs externes sont payants. Le coût peut varier en fonction du type de certificat et du niveau de validation effectué.

4. Durée de validité :

Les certificats SSL délivrés par des CAs ont une durée de validité limitée (généralement un an ou plus). Ils doivent être renouvelés régulièrement.

Certificats auto-signés :

1. Confiance limitée :

Les certificats auto-signés ne sont pas inclus dans les listes de confiance des navigateurs par défaut. Lorsqu'un utilisateur accède à un site utilisant un certificat auto-signé, le navigateur génère généralement un avertissement, indiquant que le certificat n'est pas de confiance.

2. Validation limitée :

Les certificats auto-signés ne subissent pas le même processus de validation approfondie que les certificats délivrés par des CAs externes. Le processus de génération d'un certificat auto-signé peut être réalisé par n'importe qui sans aucune vérification externe.



3. Coût :

Les certificats auto-signés sont gratuits à générer. Cela les rend attrayants pour des environnements de développement ou des tests.

4. Durée de validité :

Les certificats auto-signés peuvent avoir une durée de validité définie par l'utilisateur, mais cela dépend du logiciel utilisé pour les générer.

Recommandations :

- Production vs Développement :

En production, il est fortement recommandé d'utiliser des certificats émis par des CAs externes pour garantir la confiance des utilisateurs. Pour le développement ou des environnements locaux, les certificats auto-signés peuvent être utilisés.

- Confidentialité et Sécurité :

Les certificats délivrés par des CAs offrent un niveau plus élevé de confiance et de sécurité, ce qui les rend appropriés pour les sites web nécessitant une transmission sécurisée d'informations sensibles.

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

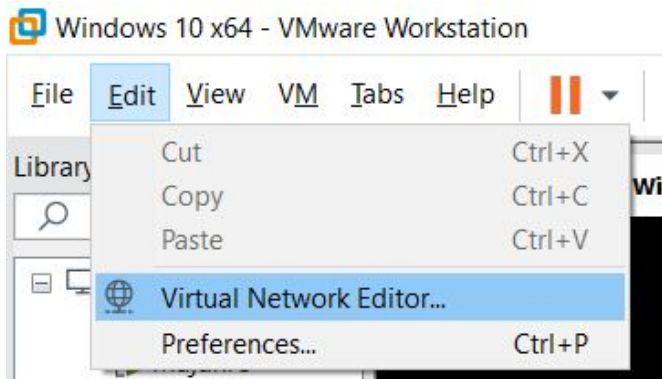
Un certificat auto-signé apparaît comme non sécurisé dans un navigateur principalement parce qu'il n'a pas été émis par une autorité de certification reconnue, ce qui conduit à un manque de confiance.



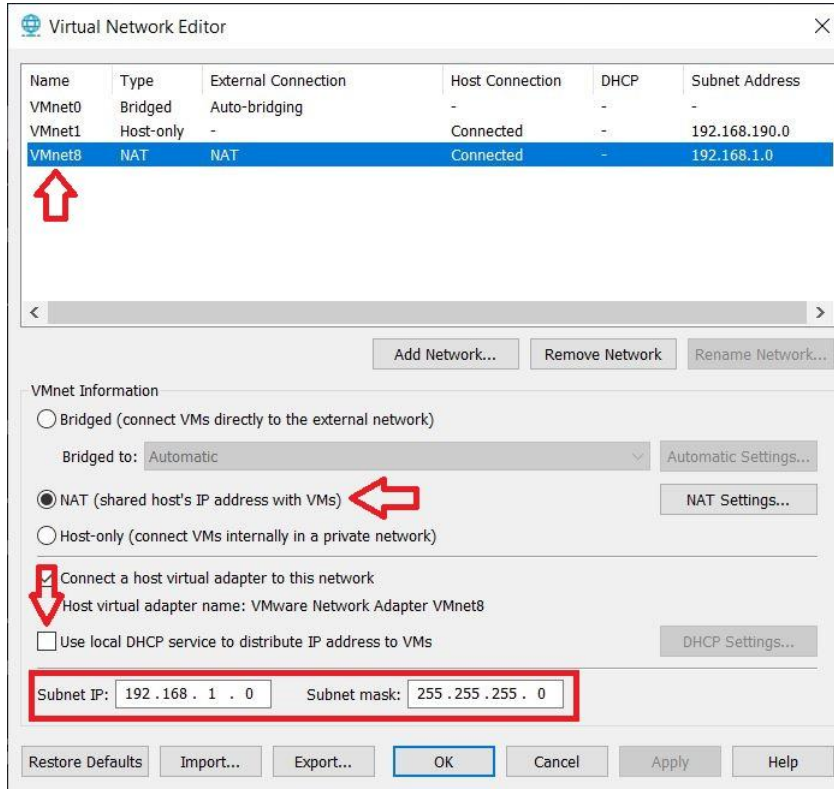
POUR ALLER ENCORE PLUS LOIN...

Configurer un serveur DHCP en dehors de l'environnement VMWare nécessite quelques étapes.

Tout d'abord, désactivez le service DHCP de votre machine virtuelle en accédant à "Edit > Virtual Network Editor".



Choisissez votre réseau, accédez à "VMnet Information" (en mode NAT), décochez "Use local DHCP...", puis spécifiez le réseau et le masque (par exemple, 192.168.1.0 255.255.255.0). Enregistrez les modifications.



The screenshot shows the Virtual Network Editor window. A table lists the networks, with VMnet8 selected. Below the table, the VMnet Information section shows the NAT configuration. The 'Connect a host virtual adapter to this network' checkbox is checked, and the 'Use local DHCP service to distribute IP address to VMs' checkbox is unchecked. The Subnet IP and Subnet mask fields are highlighted with a red box.

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Host-only	-	Connected	-	192.168.190.0
VMnet8	NAT	NAT	Connected	-	192.168.1.0

VMnet Information

☐ Bridged (connect VMs directly to the external network)

Bridged to: Automatic Automatic Settings...

☒ NAT (shared host's IP address with VMs) NAT Settings...

☐ Host-only (connect VMs internally in a private network)

☒ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet8

☐ Use local DHCP service to distribute IP address to VMs DHCP Settings...

Subnet IP: 192 . 168 . 1 . 0 Subnet mask: 255 . 255 . 255 . 0

Restore Defaults Import... Export... OK Cancel Apply Help



Sur Linux, installez le serveur **DHCP ISC-DHCP** avec la commande "sudo apt install isc-dhcp-server".

```
goldroger@debian:~$ sudo apt install isc-dhcp-server
[sudo] password for goldroger:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  linux-image-6.1.0-10-amd64
Use 'sudo apt autoremove' to remove it.
```

Modifiez la configuration réseau IPv4 de votre serveur en passant de "auto" à "manuel", attribuez-lui l'adresse IP 192.168.1.1 avec le masque 255.255.255.0.

IPv4 Method

- ☐ Automatic (DHCP) ☐ Link-Local Only
- ☒ Manual ☐ Disable
- ☐ Shared to other computers

Addresses

Address	Netmask	Gateway
192.168.1.1	255.255.255.0	<input type="button" value="x"/>
		<input type="button" value="x"/>



Dans le répertoire `"/etc/default/"`, ouvrez et modifiez le fichier `"isc-dhcp-server"` avec `"nano"`. Décommentez la ligne `DHCPDv4_CONF` et indiquez l'interface réseau sur laquelle écoute le serveur INTERFACESv4. Enregistrez les modifications.

```
GNU nano 7.2 /etc/default/isc-dhcp-server *
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpd with.
# Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="ens192"
INTERFACESv6=""
```

Accédez à `"/etc/dhcp/"` et ouvrez le fichier `"dhcpd.conf"` avec `"nano"`. Commentez les lignes `"option domain-name"` et `"domain-name-server"`.

```
GNU nano 7.2 dhcpd.conf *
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#

# option definitions common to all supported networks...
#option domain-name "example.org";
#option domain-name-servers ns1.example.org, ns2.example.org;
```



Décommentez la configuration pour un sous-réseau interne, puis configurez votre réseau.
Enregistrez et quittez.

```
goldroger@debian: /etc/dhcp
GNU nano 7.2          dhcpd.conf

# A slightly different configuration for an internal subnet.
subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.10 192.168.1.100;
    option domain-name-servers 192.168.1.1;
# option domain-name "dnsproject.prepa.com";
    option routers 192.168.1.1;
    option broadcast-address 192.168.1.255;
    default-lease-time 600;
    max-lease-time 7200;
}
```



Redémarrez et activez le serveur avec les commandes :

```
sudo systemctl restart isc-dhcp-server
sudo systemctl enable isc-dhcp-server
```

```
goldroger@debian:/$ sudo systemctl restart isc-dhcp-server
goldroger@debian:/$ sudo systemctl enable isc-dhcp-server
isc-dhcp-server.service is not a native service, redirecting to systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable isc-dhcp-server
goldroger@debian:/$
```



Vérifiez l'état du serveur avec : `sudo systemctl status isc-dhcp-server`

```
goldroger@debian:/$ sudo systemctl status isc-dhcp-server
● isc-dhcp-server.service - LSB: DHCP server
   Loaded: loaded (/etc/init.d/isc-dhcp-server; generated)
   Active: active (running) since Thu 2023-10-26 14:01:30 CEST; 1min 14s ago
     Docs: man:systemd-sysv-generator(8)
    Tasks: 1 (limit: 9452)
   Memory: 4.3M
      CPU: 68ms
   CGroup: /system.slice/isc-dhcp-server.service
           └─4601 /usr/sbin/dhcpd -4 -q -cf /etc/dhcp/dhcpd.conf ens192

Oct 26 14:01:28 debian systemd[1]: Starting isc-dhcp-server.service - LSB: DHCP server...
Oct 26 14:01:28 debian isc-dhcp-server[4588]: Launching IPv4 server only.
Oct 26 14:01:28 debian dhcpd[4601]: Wrote 3 leases to leases file.
Oct 26 14:01:28 debian dhcpd[4601]: Server starting service.
Oct 26 14:01:30 debian isc-dhcp-server[4588]: Starting ISC DHCPv4 server: dhcpd.
Oct 26 14:01:30 debian systemd[1]: Started isc-dhcp-server.service - LSB: DHCP server.
goldroger@debian:/$
```



Tout a l'air parfait maintenant vérifions sur mes autres VM si, une adresse leur ont été assignées !!

```
goldrr: zsh — Konsole
New Tab Split View
Copy Paste Find
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 00:0c:29:d7:12:bf brd ff:ff:ff:ff:ff:ff
   altname enp2s1
   inet 192.168.1.11/24 brd 192.168.1.255 scope global dynamic noprefixroute ens33
       valid_lft 450sec preferred_lft 450sec
   inet6 fe80::b904:8e28:9a3d:813b/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

CAPTURE D'ÉCRAN WINDOWS 7

Carte Ethernet Connexion au réseau local :

```
Suffixe DNS propre à la connexion. . . . :
Adresse IPv6 de liaison locale. . . . . : fe80::b4b8:aa5f:fc93:d864%11
Adresse IPv4. . . . . : 192.168.1.12
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 192.168.1.1
```

NOTRE DHCP FONCTIONNE !!

