

Documentation Projet Holodeck

Installation des outils de virtualisation

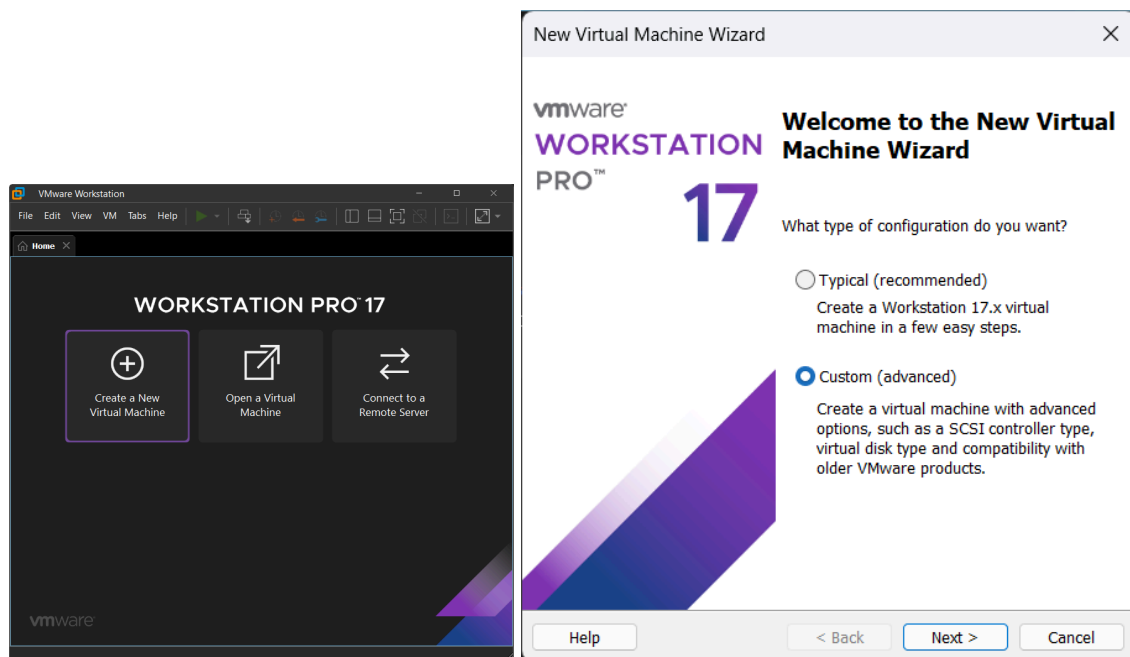
...

Installation de la machine virtuelle serveur

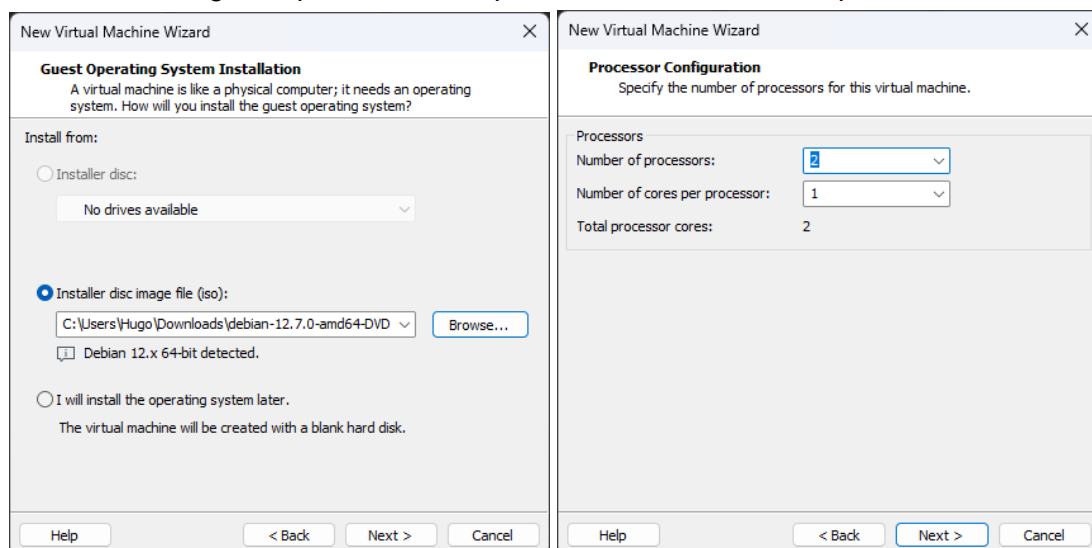
Ouvrir votre Hyperviseur, puis créer une machine virtuelle. En l'espèce les spécification de la machine sont :

Debian de base sans interface Graphique

2 Go RAM – 2vpcu – Disque 32 Go. Avec 2 cartes réseaux (une WAN et une LAN). Pour les cartes réseaux l'une sera en NAT et l'autre en LAN-Segment.



Choisir une image disque de Debian, puis définir le nombres de processeurs:



Définir la taille de la mémoire et une première carte réseau en NAT :

The image displays two side-by-side screenshots of the 'New Virtual Machine Wizard' interface.

Left Screenshot: Memory for the Virtual Machine
The title is 'Memory for the Virtual Machine' with the subtitle 'How much memory would you like to use for this virtual machine?'. It instructs the user to 'Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.' A vertical slider on the left shows memory options from 4 MB to 128 GB. A text box on the right shows 'Memory for this virtual machine: 2048 MB'. To the right of the slider, three memory recommendations are listed: 'Maximum recommended memory: 12.9 GB' (blue bar), 'Recommended memory: 2 GB' (green bar), and 'Guest OS recommended minimum: 1 GB' (yellow bar). Navigation buttons at the bottom include 'Help', '< Back', 'Next >', and 'Cancel'.

Right Screenshot: Network Type
The title is 'Network Type' with the subtitle 'What type of network do you want to add?'. It lists four network connection options under the heading 'Network connection':

- ☐ Use bridged networking: Give the guest operating system direct access to an external Ethernet network. The guest must have its own IP address on the external network.
- ☒ Use network address translation (NAT): Give the guest operating system access to the host computer's dial-up or external Ethernet network connection using the host's IP address.
- ☐ Use host-only networking: Connect the guest operating system to a private virtual network on the host computer.
- ☐ Do not use a network connection

Navigation buttons at the bottom include 'Help', '< Back', 'Next >', and 'Cancel'.

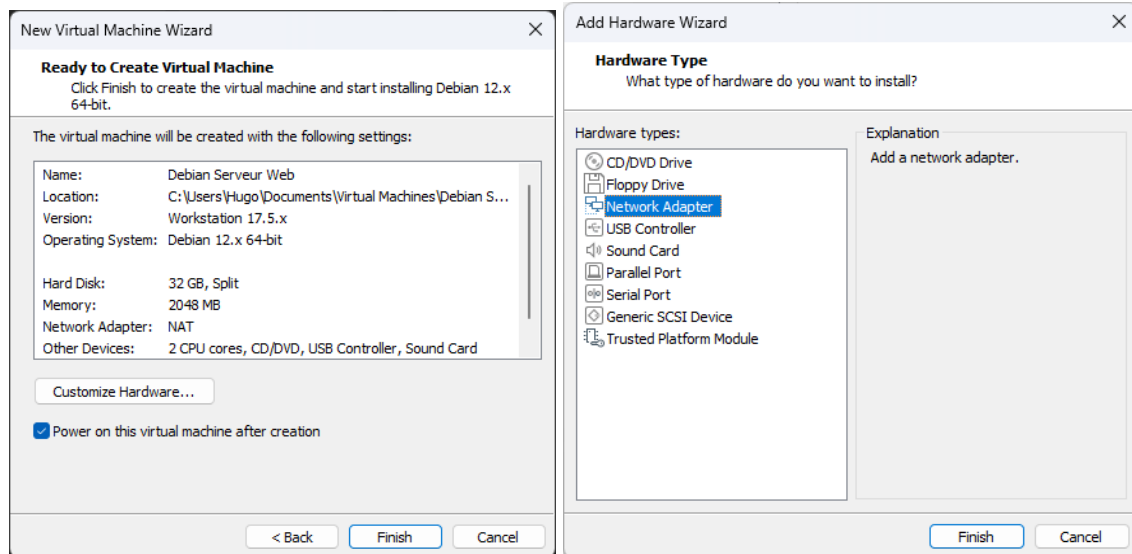
Suivre les recommandations puis définir la taille du disque

The image shows a screenshot of the 'New Virtual Machine Wizard' at the 'Specify Disk Capacity' step. The title is 'Specify Disk Capacity' with the subtitle 'How large do you want this disk to be?'. It shows 'Maximum disk size (GB): 32.0' in a text box. Below this, it states 'Recommended size for Debian 12.x 64-bit: 20 GB'. There are two main options for disk allocation:

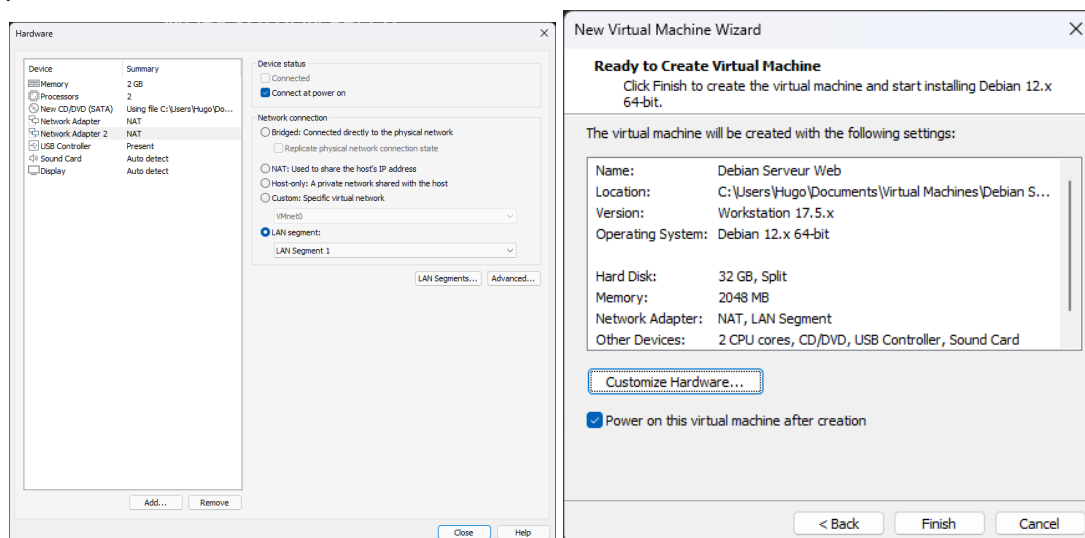
- ☐ Allocate all disk space now. Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it.
- ☒ Split virtual disk into multiple files. Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

Navigation buttons at the bottom include 'Help', '< Back', 'Next >', and 'Cancel'.

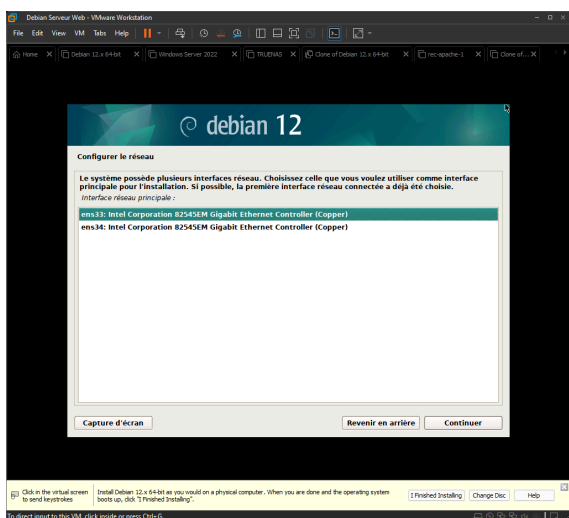
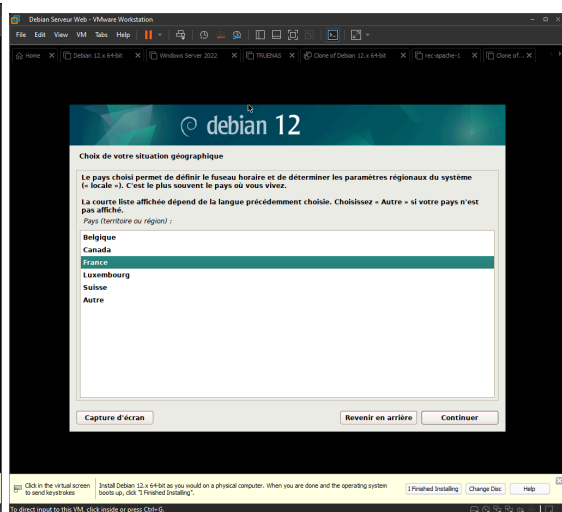
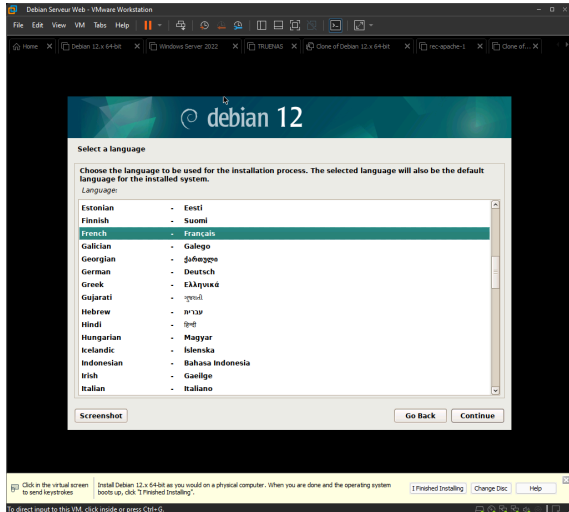
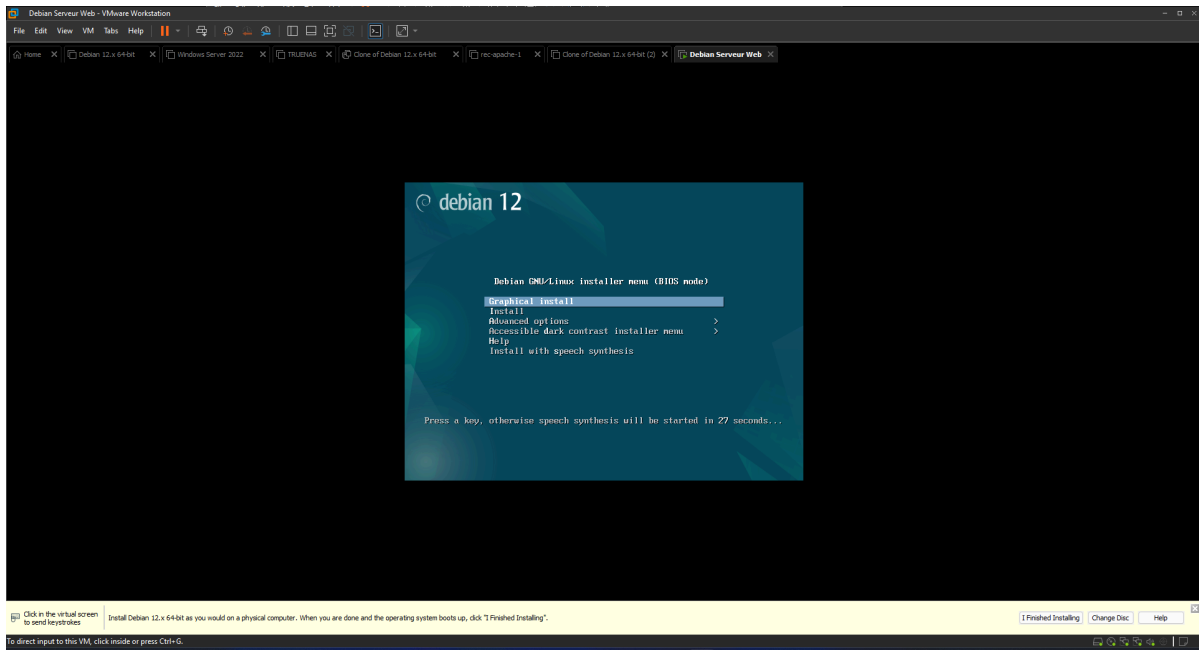
Pour ajouter une deuxième carte réseau cliquez sur customize hardware, Add, Network adapter, finish.



Ensuite configurer la carte réseau pour la mettre en LAN-Segment, puis cliquez sur close puis sur finish.

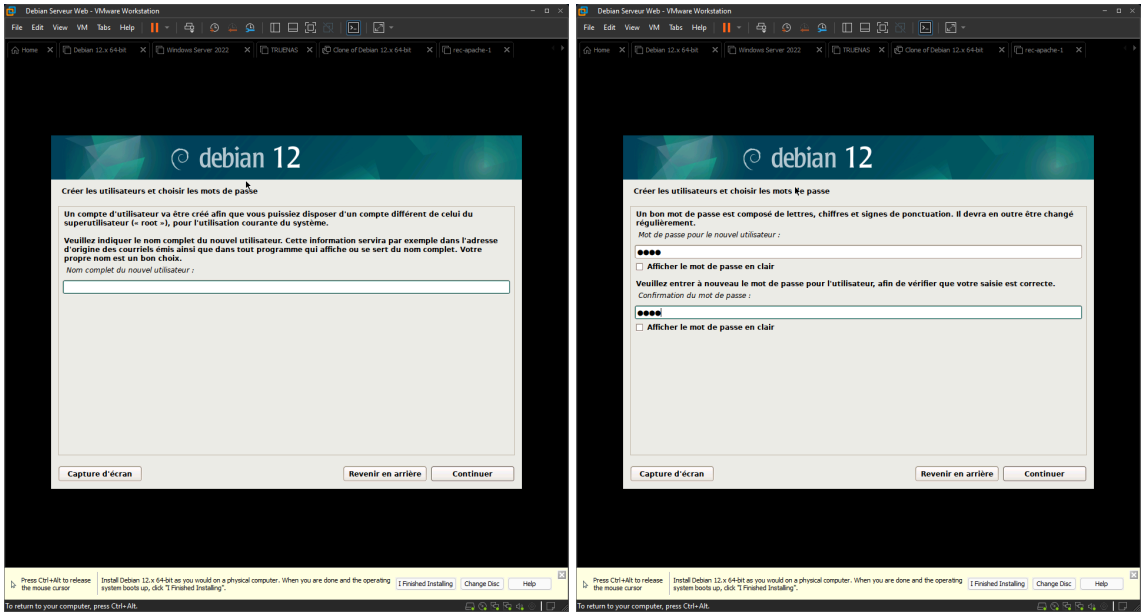


Installation de Debian

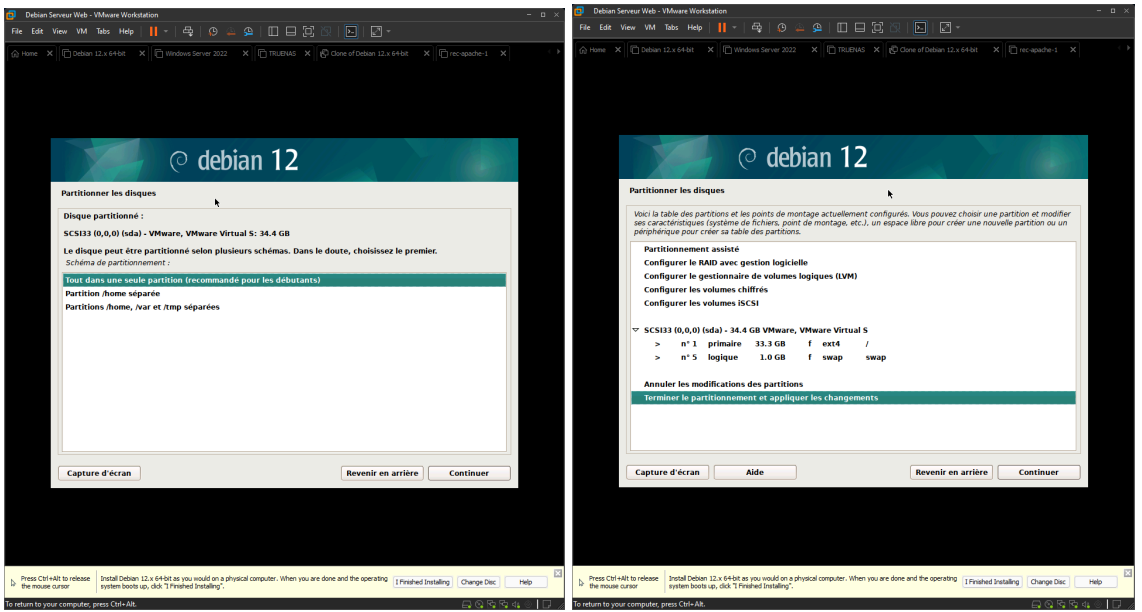


Donner un nom à la machine, laisser le nom de domaine vide. Définissez un mot de passe robuste pour l'utilisateur root.

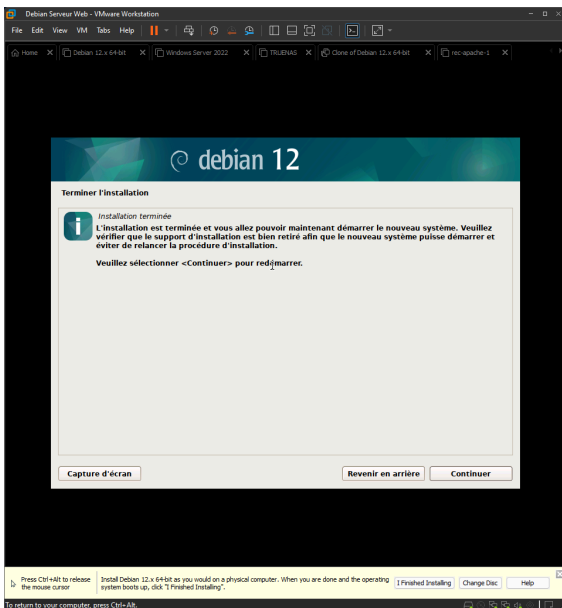
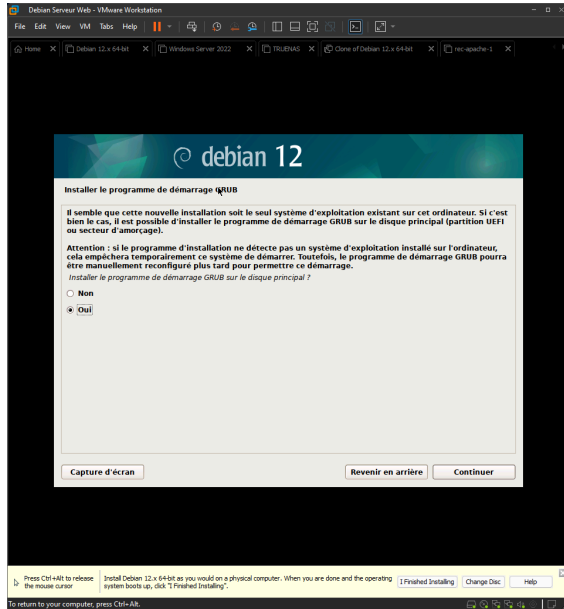
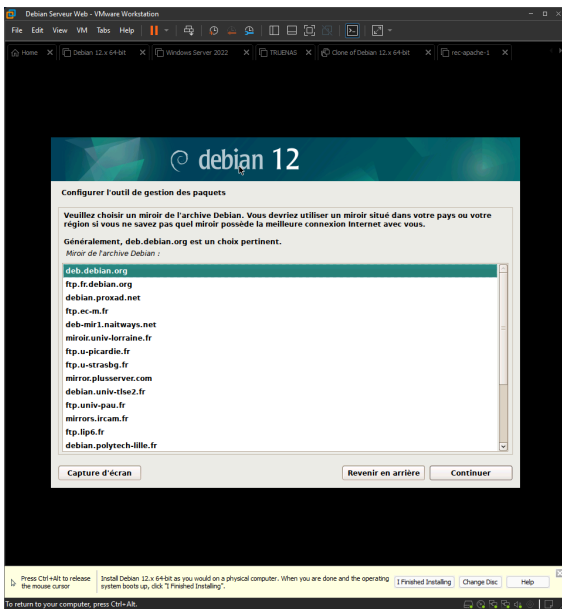
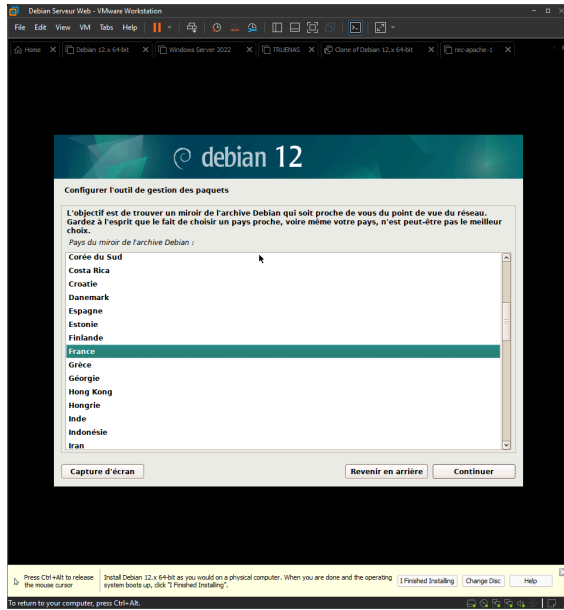
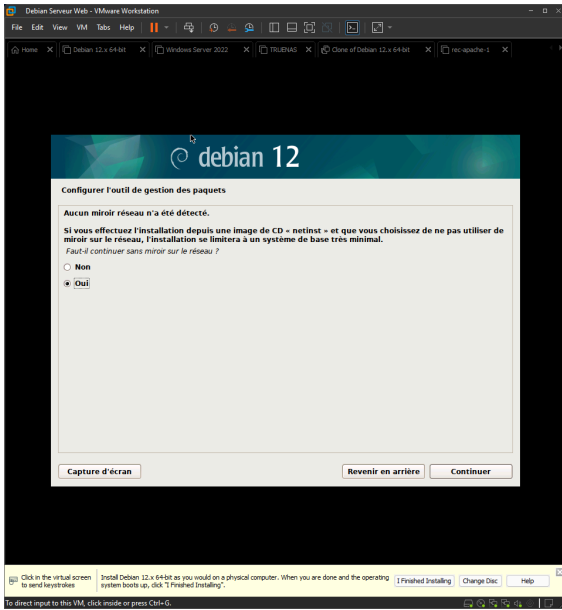
Définissez le nom de votre utilisateur puis son mot de passe.



Suivez la recommandation pour la partition des disques.



Définir les miroires sur le réseau



Serveur DHCP sur Linux

Prérequis :

- une machine Debian avec une IP fixe.
- Aucun autre serveur DHCP actif afin d'éviter les conflits.
- Une machine cliente (par exemple Debian) sans configuration IP afin de tester.
- Une connexion Internet.

Définir les adresses IP fixes

On va donc définir des IP fixes pour les interfaces réseaux:

On modifie le fichier "interfaces"

- nano /etc/network/interfaces

Dans ce fichier on définit les adresses IP en fonction des interfaces:

```
allow-hotplug ens33
```

```
iface ens33 inet static
```

```
    address 192.168.140.100/24
```

```
    gateway 192.168.140.2
```

```
    dns-nameserver 8.8.8.8
```

```
allow-hotplus ens34
```

```
iface ens34 inet static
```

```
    address 192.168.1.1/24
```

```
    dns-nameservers 192.168.10.1
```

```
Debian Server Web - VMware Workstation
File Edit View VM Tabs Help
Debian 12.x 64-bit Windows Server 2022 TRUENAS Clone of Debian 12.x 64-bit rec-apache-1 Clone of Debian 12.x 64-bit (2)
GNU nano 7.2 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens33
iface ens33 inet static
    address 192.168.140.100/24
    gateway 192.168.140.2
    dns-nameservers 0.0.0.0

allow-hotplug ens34
iface ens34 inet static
    address 192.168.1.1/24

Lecture de 20 lignes
Aide Quitter Écrire Écr. Ligne fich. Chercher Remplacer Couper Coller Exécuter Exécuter Emplacement M-U Annuler M-A Marc
To direct input to this VM, click inside or press Ctrl+G.
```

Mise en place du DHCP

On installe le paquet isc-dhcp-server avec la commande suivante

- apt install isc-dhcp-server

On configure la plage d'adresses IP du réseaux en modifiant le fichier de configuration "dhcpd.conf".

- nano /etc/dhcp/dhcpd.conf

On ajoute :

```
subnet 192.168.10.0 netmask 255.255.255.0 {
    range 192.168.10.20 192.168.10.30;
    option broadcast-address 192.168.10.255;
    option domaine-name-server 192.168.10.1;
}
```



```
GNU nano 7.2 /etc/dhcp/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;

default-lease-time 600;
max-lease-time 7200;

# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
ddns-update-style none;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
log-facility local7;

# No service will be given on this subnet, but declaring it helps the
# DHCP server to understand the network topology.

#subnet 10.152.187.0 netmask 255.255.255.0 {
#}

# This is a very basic subnet declaration.
subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.20 192.168.1.30;
    option broadcast-address 192.168.1.255;
}

# This declaration allows BOOTP clients to get dynamic addresses,
# which we don't really recommend.
#subnet 10.254.239.32 netmask 255.255.255.224 {
#    range dynamic-bootp 10.254.239.40 10.254.239.60;
#    option broadcast-address 10.254.239.31;
#    option routers rtr-239-32-1.example.org;
#}

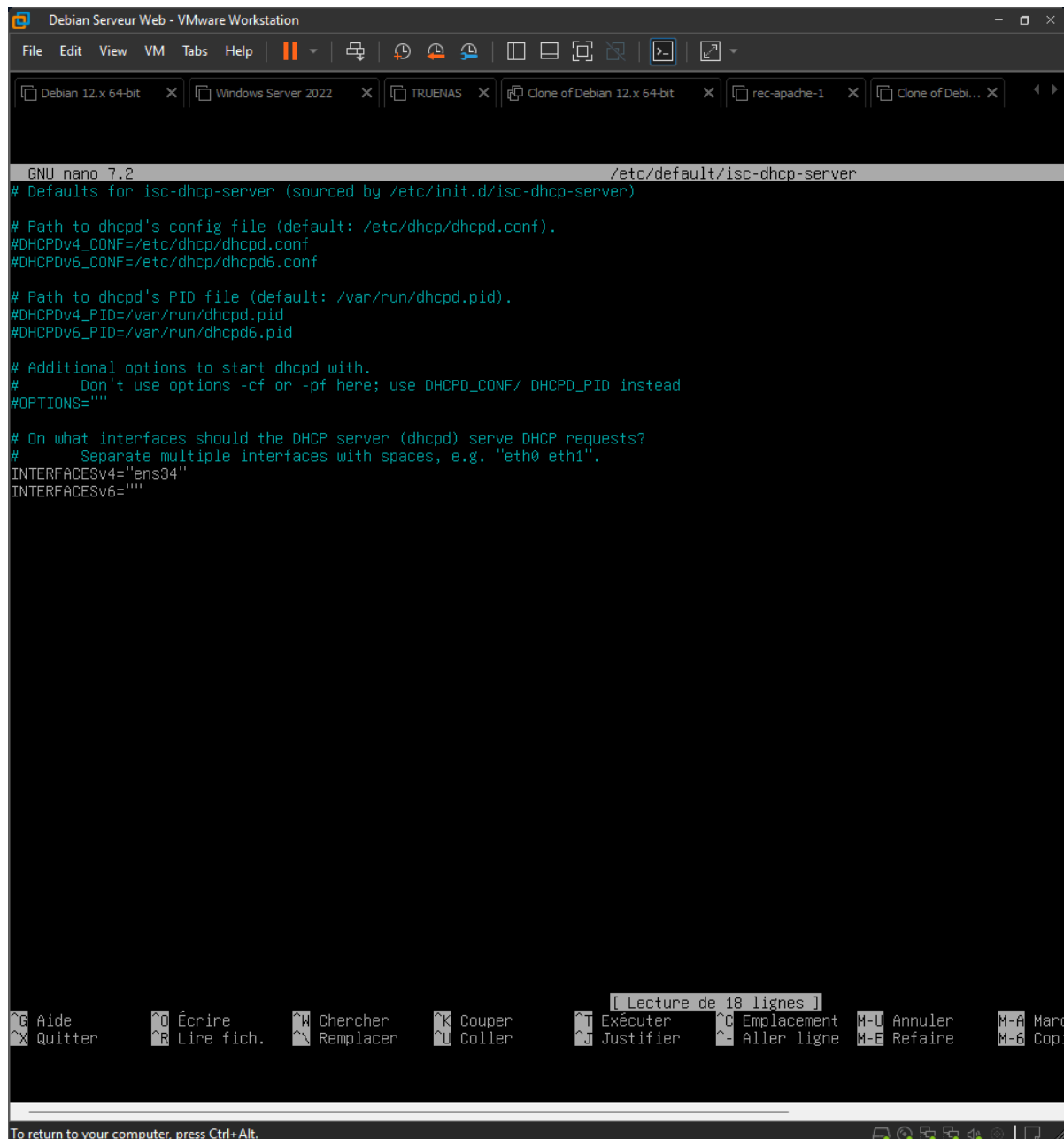
[[ Lecture de 107 lignes ]]
^G Aide          ^O Écrire      ^W Chercher    ^K Couper      ^T Exécuter    ^C Emplacement  M-U Annuler    M-A Marquer
^X Quitter       ^R Lire fich.  ^M Remplacer   ^J Coller      ^J Justifier   ^_ Aller ligne M-E Refaire    M-6 Copier
```

Il faut ensuite paramétrer l'interface réseaux sur laquelle opère le DHCP. On modifie le fichier "isc-dhcp-server".

- nano /etc/default/isc-dhcp-server

modifier la ligne suivante :

INTERFACESv4="ens34"



```
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="ens34"
INTERFACESv6=""

[ Lecture de 18 lignes ]
^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement M-U Annuler  M-A Marq
^X Quitter   ^R Lire fich. ^_ Remplacer ^U Coller    ^J Justifier ^_ Aller ligne M-E Refaire  M-6 Cop.
```

Création de certificat ssl

Créer un certificat auto-signé avec openssl :

- `openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/macle.key -out /etc/ssl/certs/moncertificat.crt`

Créer les utilisateurs des services SFTP et FTPS

Créer un groupe pour les utilisateurs sftp

- `addgroup ftpholodeck`

Créer un utilisateur et l'ajouter au groupe

- adduser utilisateur --ingroup ftpholodeck

Changer les droits des dossiers de transfert de fichier pour donner les droit d'écriture au groupe ftpholodeck

- chown root:ftpholodeck /home/web
- chmod 775 /home/web

Serveur SFTP

Vérifier la présence du service SSH

- systemctl status ssh

Configurer le fichier de configuration du server SSH

- nano /etc/ssh/sshd_config

Ajouter la configuration suivante

```
Match Group ftpholodeck
ForceCommand internal-sftp
PasswordAuthentication yes
ChrootDirectory /home/web
PermitTunnel no
AllowAgentForwarding no
AllowTcpForwarding no
X11Forwarding no
```

Redémarrer le service SSH

- systemctl restart sshd

Tester la configuration avec un client

Serveur FTPS

Installer vsftpd

- apt update && apt upgrade
- apt install vsftpd

Configurer vsftpd

- nano /etc/vsftpd.conf

Dans ce fichier éditer ces lignes

```
anonymous_logon=NO
local_enable=YES
write_enable=YES
download_enable=YES
ftpd_banner=Bienvenue sur le serveur FTP
local_root=/home/web
chroot_local_user=YES
allow_writeable_chroot=YES
```

Commentez la ligne suivante en ajoutant un '#' en début de ligne
Listen_ipv6=YES

Décommentez la ligne suivante
#Listen=YES

Ajoutez à la fin du fichier les éléments suivants. Utiliser le chemin de la paire clé certificat auto-signé.

```
rsa_cert_file=/etc/ssl/private/moncertificat.crt
rsa_private_key_file=/etc/ssl/private/macle.key
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
require_ssl_reuse=NO
ssl_ciphers=HIGH
debug_ssl=YES
```

Redémarrer le service vsftpd pour la prise en compte des modifications

- systemctl restart vsftpd.service

Assurez-vous que le service a démarré

- systemctl status vsftpd.service

Connectez-vous avec un client filezilla par exemple.

Serveur DNS

Installation du serveur DNS

Installer Bind9:

- apt install bind9

Mise en place de la zone "starfleet.lan". Modifier le fichier "/etc/bind/named.conf.local":

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

Ajouter les lignes suivantes au fichier :

```
// Déclaration de la zone
zone "starfleet.lan" {
    type master;
    file "/etc/bind/db.starfleet.lan";
};
```

Créer et éditer le fichier “/etc/bind/db.starfleet.lan”:

- nano /etc/bind/db.starfleet.lan

éditer le fichier avec ces lignes :

```
$TTL 86400
@      IN      SOA  ns1.starfleet.lan. admin.starfleet.lan. (
                        3      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        86400 ) ; Minimum TTL
; Enregistrement DNS
```

```
@      IN      NS   ns1.starfleet.lan.
@      IN      A    192.168.10.1
```

```
ns1    IN      A    192.168.10.1
www    IN      A    192.168.10.1
www8   IN      A    192.168.10.1
www7   IN      A    192.168.10.1
php    IN      A    192.168.10.1
admin  IN      A    192.168.10.1
ldap   IN      A    192.168.10.1
```

Editer le fichier “/etc/resolv.conf” :

- nano /etc/resolv.conf

ajouter les lignes :

```
domain starfleet.lan
search starfleet.lan
nameserver 192.168.10.1
```

redémarrer le service Bind9:

- systemctl restart bind9

Installer les dernières versions de PHP, MariaDB et Nginx

Installer Nginx

Pour télécharger et installer la dernière version de Nginx sur Linux sans interface graphique, voici les étapes à suivre.

Mettez à jour votre liste de paquets :

- apt update

Installez les dépendances pour HTTPS :

- apt install curl gnupg2 ca-certificates lsb-release

Ajoutez la clé GPG pour le dépôt Nginx :

- curl -fsSL https://nginx.org/keys/nginx_signing.key | sudo tee /etc/apt/trusted.gpg.d/nginx_signing.asc

Ajoutez le dépôt Nginx officiel à votre fichier sources pour Debian :

- echo "deb http://nginx.org/packages/debian `lsb_release -cs` nginx" | sudo tee /etc/apt/sources.list.d/nginx.list

Mettez à jour à nouveau la liste des paquets :

- apt update

Installez Nginx :

- apt install nginx

Une fois Nginx installé, vous pouvez vérifier la version avec la commande :

- nginx -v

De plus, si vous utiliser debian, vous devez vérifier que l'utilisateur de Nginx est bien "www-data" dans le fichier "/etc/nginx/nginx.conf": user www-data;

Installer MariaDB

Les même étapes s'applique pour installer MariaDB

Installez les dépendances pour HTTPS :

- apt install curl software-properties-common dirmngr

Ajoutez le dépôt officiel MariaDB. Téléchargez la clé GPG de MariaDB :

- curl -Ls https://downloads.mariadb.com/MariaDB/mariadb_repo_setup | sudo bash

Cela ajoute automatiquement le dépôt MariaDB à vos sources et met à jour votre liste de paquets.

Mettez à jour la liste des paquets :

- apt update

Installez la dernière version de MariaDB :

- apt install mariadb-server

Vérifiez l'installation de MariaDB. Vous pouvez vérifier si MariaDB est installé correctement avec :

- systemctl status mariadb

Démarrez MariaDB (si nécessaire). Si MariaDB n'est pas déjà en cours d'exécution, démarrez-le avec :

- systemctl start mariadb

Activez MariaDB pour qu'il démarre au démarrage du système :

- `systemctl enable mariadb`

Post-installation MariaDB

Sécurisez l'installation de MariaDB. Utilisez le script suivant pour sécuriser votre installation (mot de passe root, suppression des utilisateurs anonymes, etc.) :

- `mysql_secure_installation`

Se connecter à mariadb

- `mariadb --password`

Créer un utilisateur pour la maintenance du service, remplacer "mariadb" par le nom d'utilisateur et "unmotdepasse" par votre mot de passe.

- `> grant all privileges on *.* to 'mariadb'@'localhost' identified by 'unmotdepasse';`
- `>exit`

installer PHP 7 et 8

Pour installer et faire cohabiter les dernières versions de PHP 7 et PHP 8 sur un système Linux, vous pouvez suivre ces étapes :

1. Mise à jour du système

Avant d'installer PHP, il est recommandé de mettre à jour votre système.

- `apt update && apt upgrade -y`

2. Installez les outils nécessaires pour ajouter des sources de dépôt :

- `apt install software-properties-common ca-certificates lsb-release apt-transport-https`

3. Ajouter la clé GPG du dépôt

Ajoutez la clé GPG pour le PPA d'Ondřej Surý (qui maintient les versions de PHP pour Debian et Ubuntu) :

- `wget -qO /usr/share/keyrings/sury-php.gpg https://packages.sury.org/php/apt.gpg`

4. Ajouter le dépôt

Ajoutez manuellement le dépôt à votre fichier sources. Utilisez la commande suivante pour ajouter la source du dépôt :

- `echo "deb [signed-by=/usr/share/keyrings/sury-php.gpg]
https://packages.sury.org/php/ $(lsb_release -sc) main" | sudo tee
/etc/apt/sources.list.d/sury-php.list`

5. Mettre à jour le système

Mettez à jour la liste des paquets :

- apt update

6. Installer PHP

Maintenant, vous pouvez installer PHP

- apt install php7.4 php7.4-fpm
- apt install php8.3 php8.3-fpm

Créer les site web pour le serveur

configuration pour un site web en php

Premièrement créer un dossier racine pour le site dans “/var/www” :

- mkdir /var/www/starfleet7.lan

Déterminer le propriétaire du dossier comme étant www-data :

- chown -R www-data:www-data /var/www/starfleet7.lan

définissez les droits de ce dossier :

- chmod 755 /var/www/starfleet7.lan

Ensuite on doit créer le fichier “index.html” qui correspond à la page d'accueil du site :

- nano /var/www/starfleet7.lan/index.php

dans ce fichier on peut insérer le code suivant :

```
<?php
phpinfo();
?>
```

Il faut maintenant créer le fichier de configuration du site internet, dans le dossier “conf.d” :

- nano /etc/nginx/conf.d/starfleet7.lan.conf

dans ce fichier il faut intégrer la configuration suivante :

```
server {
    listen 80;
    listen [::]:80;

    server_name www7.starfleet.lan;

    return 301 https://$server_name$request_uri;
```



```

}

server {
    listen 443 ssl;
    listen [::]:443 ssl;

    server_name www7.starfleet.lan;

    ssl_certificate /etc/ssl/certs/moncertificat.crt;
    ssl_certificate_key /etc/ssl/private/macle.key;

    root /var/www/starfleet7.lan;
    index index.php index.html index.htm;

    location / {
        try_files $uri $uri/ =404;
    }

    location ~ \.php$ {
        include fastcgi_params;
        fastcgi_pass unix:/var/run/php/php7.4-fpm.sock;
        fastcgi_index index.php;
        fastcgi_param SCRIPT_FILENAME
        $document_root$fastcgi_script_name;
    }
}

```

Vous pouvez vérifier la configuration avec cette commande :

- `nginx -t`

Redémarrer le service nginx :

- `systemctl restart nginx`

mise en place d'un reverse proxy pour accéder à cockpit

Installation de cockpit

- `apt install cockpit`
- `systemctl start cockpit`
- `systemctl enable cockpit`

Créer un fichier de configuration pour le domaine. En l'espèce "admin.starfleet.lan" :

- `nano /etc/nginx/conf.d/admin.starfleet.conf`

Ajouter la configuration suivante :

```

server {
    listen 80;

```

```

listen [::]:80;

server_name admin.starfleet.lan;

return 301 https://$host$request_uri;
}

server {
    listen 443 ssl;
    listen [::]:443 ssl;

    server_name admin.starfleet.lan;

    ssl_certificate /etc/ssl/certs/moncertificat.crt;
    ssl_certificate_key /etc/ssl/private/macle.key;
    ssl_protocols TLSv1.2 TLSv1.3;

    location / {
        proxy_pass https://127.0.0.1:9090;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection "upgrade";
        proxy_http_version 1.1;
        poxy_ssl_verify off;
    }
}

```

redémarrer Nginx :

- `systemctl restart nginx`

Installer phpMyAdmin

Sous Debian, le paquet s'appelle simplement `phpmyadmin`. Pendant l'installation, `apt` propose la configuration automatique du serveur web (Apache ou `lighttpd`). Comme cette configuration fonctionne avec Nginx, il est inutile de sélectionner un serveur web. Ensuite, `apt` propose la création d'une base de données pour stocker les paramètres de `phpMyAdmin` ; il est pratique de répondre `Yes`.

- `apt install phpmyadmin`

Configurer phpMyAdmin

Créez un fichier de configuration pour `phpMyAdmin`. Vous pouvez utiliser le fichier d'exemple fourni.

- `cp /usr/share/phpmyadmin/config.sample.inc.php /usr/share/phpmyadmin/config.inc.php`

Éditez “config.inc.php” pour ajouter une clé de sécurité. Ouvrez le fichier avec un éditeur de texte :

- `nano /usr/share/phpmyadmin/config.inc.php`

Recherchez la ligne contenant “blowfish_secret” et définissez une clé secrète aléatoire :

- `$cfg['blowfish_secret'] = 'votre_clé_secrète_ici';`

Configurer Nginx pour phpMyAdmin

modifier la propriété du fichier “/usr/share/phpmyadmin”

- `chown www-data:www-data /usr/share/phpmyadmin`

Créez un fichier de configuration pour phpMyAdmin dans le répertoire de configuration de Nginx.

- `nano /etc/nginx/conf.d/php.starfleet.lan.conf`

Ajoutez la configuration suivante :

```
server {
    listen 80;
    listen [::]:80;
    server_name php.starfleet.lan;
    return 301 https://$server_name$request_uri;
}

server {
    listen 443 ssl;
    listen [::]:443 ssl;

    server_name php.starfleet.lan;

    ssl_certificate /etc/ssl/certs/moncertificat.crt;
    ssl_certificate_key /etc/ssl/private/macle.key;

    root /usr/share/phpmyadmin;
    index index.php;

    location / {
        try_files $uri $uri/ =404;
    }

    location ~ \.php$ {
        include fastcgi_params;
        fastcgi_pass unix:/var/run/php/php8.3-fpm.sock;
        fastcgi_index index.php;
    }
}
```

```

        fastcgi_param SCRIPT_FILENAME
        $document_root$fastcgi_script_name;
    }
}

```

Redémarrer Nginx

- `systemctl restart nginx`

Serveur LDAP

Installer Le serveur OpenLDAP

- `apt update && apt upgrade`
- `apt install slapd ldap-utils`

Configuration du service d'annuaire

configurer le serveur à l'aide de la commande

- `dpkg-reconfigure slapd`

Répondez au questionnaire avec les bonnes informations

question 2 : starfleet.lan

question 3 : organization

question 4 : définir le mot de passe root

question 5 : confirmer le mot de passe

finir la configuration selon vos préférences

Activer slapd au démarrage et de le lancer

- `systemctl enable slapd`
- `systemctl start slapd`

Afficher les données de l'annuaire pour s'assurer de la présence de l'administrateur

- `ldapsearch -x -H ldap://starfleet.lan -b 'dc=starfleet,dc=lan'`

Si il n'y a pas d'administrateur créer le manuellement

Générer un mot de passe chiffré avec cette commande

- `slappasswd -s motdepasse`

copier le mot de passe chiffré et créer un fichier admin.ldif avec ces informations

dn: cn=admin,dc=starfleet,dc=lan

objectClass: simpleSecurityObject

objectClass: organizationalRole

cn: admin

description: LDAP administrator

userPassword: {SSHA}motdepasse_chiffré

Ajouter l'utilisateur administrateur dans LDAP en utilisant ldapadd

- `ldapadd -x -D "cn=admin,dc=starfleet,dc=lan" -W -f admin.ldif`