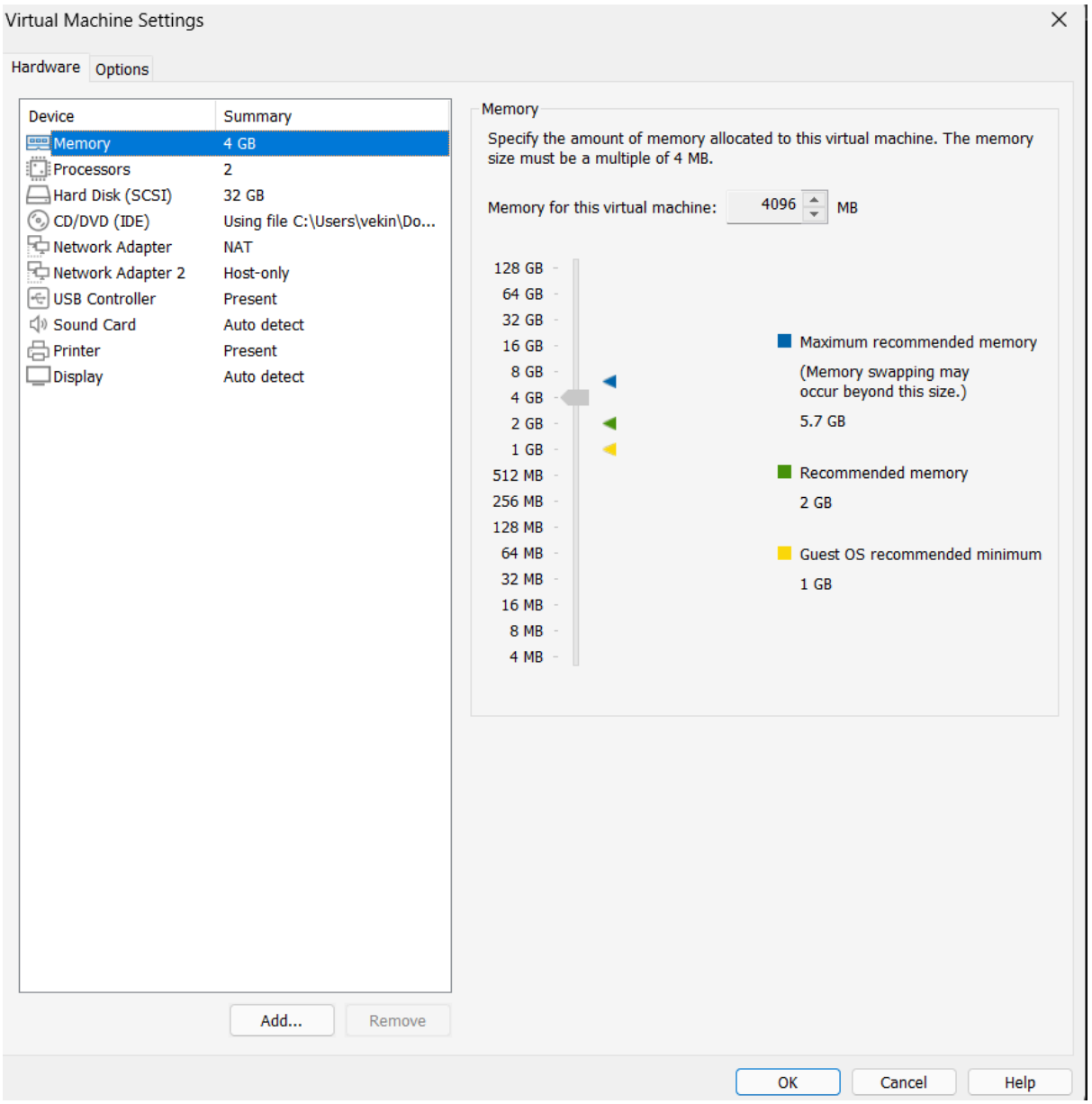
Notice d’installation et d’utilisation chez Starfleet

Installation des deux VM

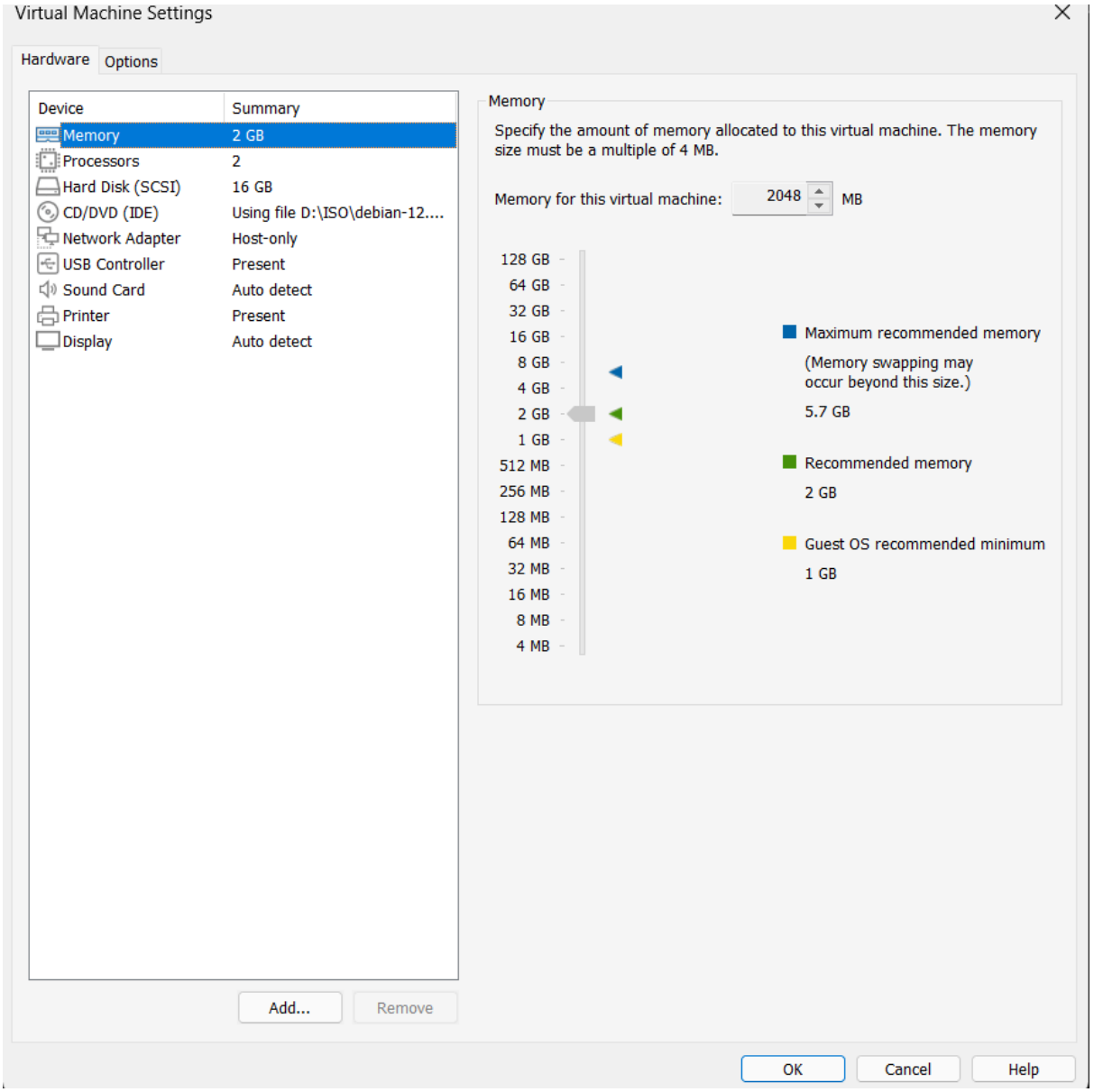
Configuration de la VM Serveur :

Pour la VM Serveur : Debian de base sans interface Graphique – 2 Go RAM – 2vpcu – Disque 32 Go. Avec 2 cartes réseaux (une WAN et une LAN).



Configuration de la VM Client :

Pour la VM Cliente : une Debian avec GUI – 2 Go RAM – 2vcpu – Disque 16 Go et connecté sur le «LAN» de la VM serveur et un navigateur web.



Sans utiliser Sudo :
On va devoir se mettre en root soit : su -

```
serveurr@serveurrevision:/root$ su -
Mot de passe :
root@serveurrevision:~#
```

IP Statique

Avant toute configuration et installation des serveurs, il faut configurer notre ip de l'interface réseau Lan pour qu'il soit statique !

Faisons ip a pour voir le nom de l'interface réseau Lan (ici ens37)

```
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:29:9a:06:f7 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.116.129/24 brd 192.168.116.255 scope global dynamic ens33
       valid_lft 1452sec preferred_lft 1452sec
    inet6 fe80::20c:29ff:fe9a:6f7/64 scope link
       valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:0c:29:9a:06:01 brd ff:ff:ff:ff:ff:ff
    altname enp2s5
root@serveurrevision:~#
```

Modifions le fichier /etc/network/interfaces et rentrer une ip statique

```
 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 dhcp

allow-hotplug ens37
auto ens37
iface ens37 inet static
        address 192.168.10.26
        netmask 255.255.255.0
        gateway 192.168.10.1
```

Installation DHCP

Installer le paquet

```
root@serveurrevision:~# apt install isc-dhcp-server
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
isc-dhcp-server est déjà la version la plus récente (4.4.3-P1-2).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
root@serveurrevision:~#
```

Modifier le fichier dhcpd.conf selon notre réseau Lan qu'on a modifié :

```
  GNU nano 7.2                                                  /etc/dhcp/dhcpd.conf

# 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 10.254.239.0 netmask 255.255.255.224 {
#  range 10.254.239.10 10.254.239.20;
#  option routers rtr-239-0-1.example.org, rtr-239-0-2.example.org;
#}

# This declaration allows BOOTP clients to get dynamic addresses,
# which we don't really recommend.

# A slightly different configuration for an internal subnet.
subnet 192.168.10.0 netmask 255.255.255.0 {
  range 192.168.10.10 192.168.10.100;
  option domain-name-servers 192.168.10.1;
  option domain-name "local";
  option routers 192.168.10.1;
  option broadcast-address 192.168.10.255;
  default-lease-time 600;
  max-lease-time 7200;
}
```

Mettre le nom de notre interface réseau qu'on utilise pour le DHCP (ici le LAN) dans le fichier /etc/default/isc-dhcp-server

```
  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="ens37"
INTERFACESv6=""
```

On redémarre pour vérifier si notre configuration est bonne et sans erreur.

```
root@serveurrevision:~# systemctl restart isc-dhcp-server.service
```

```
root@serveurrevision:~# systemctl status isc-dhcp-server.service
● isc-dhcp-server.service - LSB: DHCP server
     Loaded: loaded (/etc/init.d/isc-dhcp-server; generated)
     Active: active (running) since Wed 2024-09-04 14:47:54 CEST; 1h 5min ago
       Docs: man:systemd-sysv-generator(8)
    Process: 3021 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, status=0/SUCCESS)
      Tasks: 1 (limit: 4611)
     Memory: 4.4M
        CPU: 104ms
     CGroup: /system.slice/isc-dhcp-server.service
             └─3033 /usr/sbin/dhcpd -4 -q -cf /etc/dhcp/dhcpd.conf ens37

sept. 04 14:47:52 serveurrevision systemd[1]: Starting isc-dhcp-server.service - LSB: DHCP server...
sept. 04 14:47:52 serveurrevision isc-dhcp-server[3021]: Launching IPv4 server only.
sept. 04 14:47:52 serveurrevision dhcpd[3033]: Wrote 0 leases to leases file.
sept. 04 14:47:52 serveurrevision dhcpd[3033]: Server starting service.
sept. 04 14:47:54 serveurrevision isc-dhcp-server[3021]: Starting ISC DHCPv4 server: dhcpd.
sept. 04 14:47:54 serveurrevision systemd[1]: Started isc-dhcp-server.service - LSB: DHCP server.
```

Et voici que la configuration du DHCP est finalisée.

Testons sur la VM Cliente si il a pris la plage d'adresse ip de notre réseau Lan

Une fois dessus nous allons libérer l'ancien bail DHCP et mettre le nouveau avec :

```
clientt@client-revision:~$ su -
Mot de passe :
root@client-revision:~# dhclient -r
root@client-revision:~# dhclient

root@client-revision:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t 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 grc
up default qlen 1000
    link/ether 00:0c:29:33:4e:a9 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.96.135/24 brd 192.168.96.255 scope global dynamic noprefixroute
 ens33
       valid_lft 1533sec preferred_lft 1533sec
    inet 192.168.10.11/24 brd 192.168.10.255 scope global dynamic ens33
       valid_lft 547sec preferred_lft 547sec
    inet6 fe80::20c:29ff:fe33:4ea9/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Installation DNS

Installation du paquet bind9 (DNS)

```
root@serveurrevision:~# apt install bind9
```

Modifions le fichier /etc/bind/named.conf.options comme en bas

```
root@serveurrevision:~# nano /etc/bind/named.conf.options
```

```
 GNU nano 7.2                                                  /etc/bind/named.co
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.
        listen-on { 192.168.10.26; };

        allow-query { 192.168.10.0/24; };

        forwarders {
                8.8.8.8;
                8.8.4.4;
         };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation auto;
        auth-nxdomain no;
        listen-on-v6 { none; };
};
```

Modifions ce fichier en mettant notre nom de domaine de nos serveurs webs

```
root@serveurrevision:~# nano /etc/bind/named.conf.local
```

```
 GNU nano 7.2                                          /etc/bind/named.conf.local
zone "localdomain" {
        type master;
        file "/etc/bind/db.localdomain";
};

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

```
root@serveurrevision:~/nginx-ldap-auth# cp /etc/bind/db.local /etc/bind/db.starfleet.lan
```

Le fichier créé soit db.starfleet.lan, on va le modifier avec toutes nos formats de nos pages

```
  GNU nano 7.2                                                /etc/bind/db.starfleet.lan
$TTL    604800
@       IN      SOA     ns.starfleet.lan. admin.starfleet.lan. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns.starfleet.lan.
@       IN      A       192.168.10.26
@       IN      AAAA    ::1
ns      IN      A       192.168.10.26

www7    IN      A       192.168.10.26
www8    IN      A       192.168.10.26
php     IN      A       192.168.10.26
admin   IN      A       192.168.10.26
client1 IN      A       192.168.10.11
```

On vérifie si nos configurations sont bien écrites et configurées.

```
root@serveurrevision:~# named-checkconf
root@serveurrevision:~# named-checkzone localdomain /etc/bind/db.localdomain
zone localdomain/IN: loaded serial 2
OK
root@serveurrevision:~# systemctl restart bind9
root@serveurrevision:~#
```

On active le pare-feu pour autoriser le port DNS.

```
root@serveurrevision:~# ufw allow "DNS"
Rule added
Rule added (v6)
```

Une fois avoir tout installé et configuré, on va aller sur la Vm client pour voir si tout fonctionne :

Test DNS :

```
root@client-revision:~# nslookup localdomain
Server:         192.168.10.26
Address:        192.168.10.26#53

Name:   localdomain
Address: 192.168.10.26
Name:   localdomain
Address: ::1

root@client-revision:~#
```

```
root@client-revision:~# nslookup www7.starfleet.lan
Server:         192.168.10.26
Address:        192.168.10.26#53

Name:   www7.starfleet.lan
Address: 192.168.10.26
```

Installation FTPS (SSL/TLS)

```
root@serveurrevision:~# apt install proftpd proftpd-mod-crypto
```

Configurons le fichier en enlevant les commentaires de ces lignes dans le fichier /etc/proftpd/proftpd.conf

```
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
```

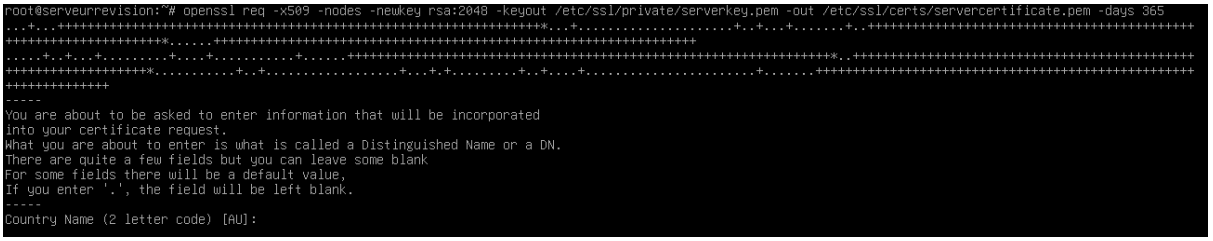
```
chroot_local_user=YES
```

```
Include /etc/proftpd/tls.conf
```

Chrooté sur les dossiers web

```
DefaultRoot /var/www_
```

Installation des certificats/clés openssl pour le SSL/TLS



Une fois les clés installé, nous allons configurer le fichier tls.conf pour mettre les certificats et activé FTPS en mettant bien le chemin des certificats créé

```
<IfModule mod_tls.c>
TLSEngine                               on
TLSLog                                  /var/log/proftpd/tls.log
TLSProtocol                             TLSv1.2 TLSv1.3
Port 21

TLSRSACertificateFile                   /etc/ssl/certs/proftpd.crt
TLSRSACertificateKeyFile                /etc/ssl/private/proftpd.key
#
# CA the server trusts...
#TLSCACertificateFile                    /etc/ssl/certs/CA.pem
# ...or avoid CA cert and be verbose
TLSOptions                          NoCertRequest
# ... or the same with relaxed session use for some clients (e.g. FireFtp)
#TLSOptions                          NoCertRequest EnableDiags NoSessionReuseRequi
#
#
# Per default drop connection if client tries to start a renegotiate
# This is a fix for CVE-2009-3555 but could break some clients.
#
#TLSOptions                             NoCertRequest
#
# Authenticate clients that want to use FTP over TLS?
#
TLSVerifyClient                         off
#
```

On ouvre les ports pour le FTPS

```
root@serveurrevision:~# ufw allow from any to any port 20,21 proto tcp
Rules updated
Rules updated (v6)
root@serveurrevision:~# ufw allow from any to any port 1024:1048 proto tcp
Rules updated
Rules updated (v6)
root@serveurrevision:~#
```

```
root@serveurrevision:~# systemctl restart proftpd
```

Forçons le SSL à chaque connexion du FTP avec la commande lftp dans le fichier ./lftprc :

```
  GNU nano 7.2                                                    ./lftprc *
set ftp:ssl-auth TLS
set ftp:ssl-force true
set ftp:ssl-protect-list yes
set ftp:ssl-protect-data yes
set ssl:verify-certificate no
```

Puis on teste :

```
root@serveurrevision:~# ftp ftpuser@192.168.116.129
Connected to 192.168.116.129.
220 ProFTPD Server (Starfleet) [::ffff:192.168.116.129]
331 Mot de passe requis pour ftpuser
Password:
230 Utilisateur ftpuser authentifié
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

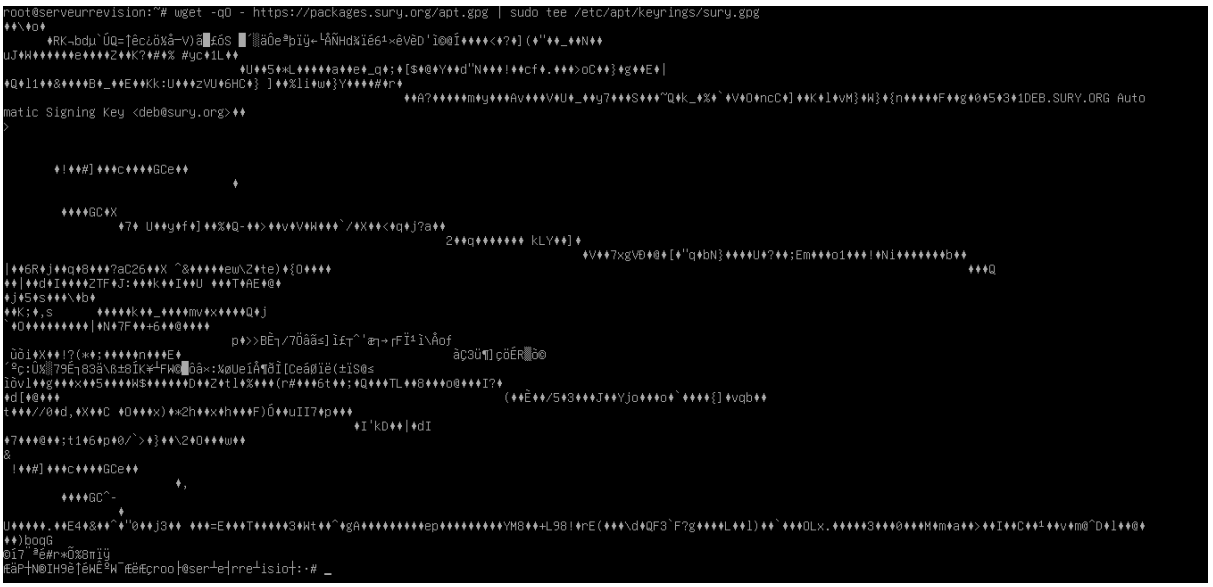
```
(myenv) root@serveurrevision:~/nginx-ldap-auth# lftp -u ftpuser ftp://192.168.116.129
Mot de passe :
lftp ftpuser@192.168.116.129:~> ls
drwxr-xr-x   2 root     root         4096 Sep 12 15:40 admin
drwxr-xr-x   2 root     root         4096 Sep 10 15:12 html
drwxr-xr-x   2 root     root         4096 Sep 11 22:21 php7
drwxr-xr-x   2 root     root         4096 Sep 11 22:20 php8
drwxr-xr-x   2 root     root         4096 Sep 12 12:29 phpmyadmin
lftp ftpuser@192.168.116.129:/>
```

```
root@serveurrevision:~# ftp localhost
Trying [::1]:21 ...
Connected to localhost.
220 ProFTPD Server (Starfleet) [::1]
```

```
root@serveurrevision:~# ftp 192.168.116.129
Connected to 192.168.116.129.
220 ProFTPD Server (Starfleet) [::ffff:192.168.116.129]
Name (192.168.116.129:serveurr): _
```

Installation de la dernière version de Nginx

installer Nginx avec Sury pour avoir la dernière version :




```
root@serveurrevision:~# echo "deb [signed-by=/etc/apt/keyrings/sury.gpg] https://packages.sury.org/nginx bookworm main" | sudo tee /etc/apt/sources.list.d/nginx
.list_
```

```
root@serveurrevision:~# nano /etc/apt/preferences.d/nginx.pref
```

```
  GNU nano 7.2
Package: *
Pin: origin packages.sury.org
Pin-Priority: 1000
```

```
root@serveurrevision:~# apt update
```

```
root@serveurrevision:~# apt upgrade
```

Une fois avoir installé et mis dans la sources.list nous pouvons installer le paquet nginx :

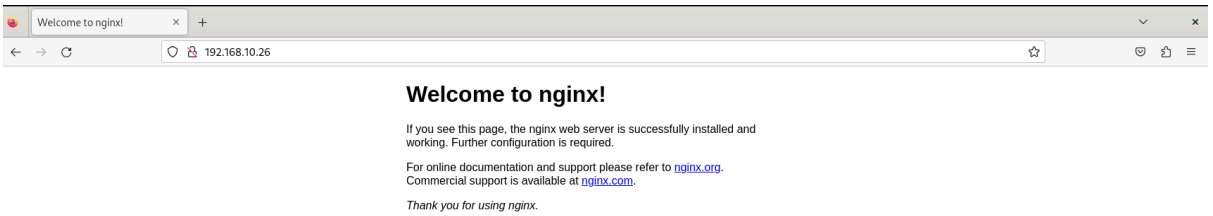
```
root@serveurrevision:~# apt install nginx-full
```

```
root@serveurrevision:~# nginx -v
nginx version: nginx/1.26.2
```

Ouvrons les ports pour nginx :

```
root@serveurrevision:~# ufw allow "Nginx HTTP"
Rule added
Rule added (v6)
root@serveurrevision:~# ufw allow "Nginx HTTPS"
Rule added
Rule added (v6)
root@serveurrevision:~#
```

Testons déjà, la page de base de nginx en tapant sur le navigateur de notre VM Cliente : http://192.168.10.26 soit l'ip de notre VM serveur :

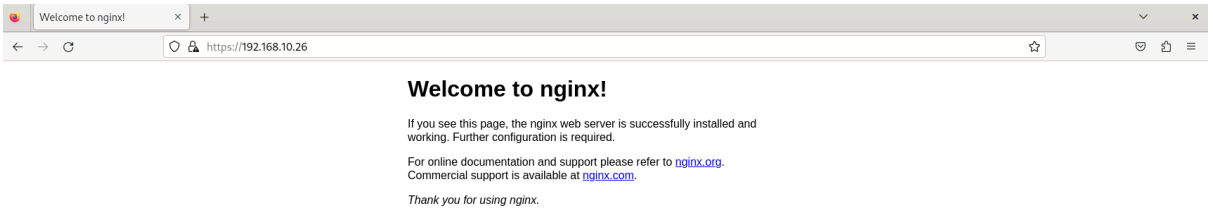


Activons la sécurisation HTTP :

Nous allons sur le fichier de notre serveur web soit /etc/nginx/sites-available/default :

```
 GNU nano 7.2                                                /etc/nginx/sites-available/default
# applications, such as Drupal or Wordpress. These applications will be made
# available underneath a path with that package name, such as /drupal8.
#
# Please see /usr/share/doc/nginx-doc/examples/ for more detailed examples.
##

# Default server configuration
#
server {
        listen 80 default_server;
        listen [::]:80 default_server;
        server_name _;
        return 301 https://$host$request_uri;
}

server {
        listen 443 ssl default_server;
        listen [::]:443 ssl default_server;
        # SSL configuration
        #
        # listen 443 ssl default_server;
        # listen [::]:443 ssl default_server;
        #
        # Note: You should disable gzip for SSL traffic.
        # See: https://bugs.debian.org/773332
        #
        # Read up on ssl_ciphers to ensure a secure configuration.
        # See: https://bugs.debian.org/765782
        #
        # Self signed certs generated by the ssl-cert package
        # Don't use them in a production server!
        #
        # include snippets/snakeoil.conf;
        ssl_certificate /etc/ssl/certs/servercertificate.pem;
        ssl_certificate_key /etc/ssl/private/serverkey.pem;
        root /var/www/html;

        # Add index.php to the list if you are using PHP
        index index.nginx-debian.html;

        server_name _;

        location / {
                # First attempt to serve request as file, then
                # as directory, then fall back to displaying a 404.
```

Maintenant testons une nouvelle fois mais maintenant avec https://192.168.10.26



NGINX PHP

Installons les 2 PHP avec la dernière version pour faire deux pages PHP :

Dernière version PHP8 et PHP7 :

```
root@serveurrevision:~# wget -O /etc/apt/trusted.gpg.d/php.gpg https://packages.sury.org/php/apt.gp_
```

```
root@serveurrevision:~# echo "deb https://packages.sury.org/php/ $(lsb_release -sc) main" | sudo tee /etc/apt/sources.list.d/php.list
```

apt update et upgrade

```
root@serveurrevision:~# apt update
Réception de :1 http://security.debian.org/debian-security bookworm-security InRelease [48,0 kB]
Atteint :2 http://deb.debian.org/debian bookworm InRelease
Réception de :3 http://deb.debian.org/debian bookworm-updates InRelease [55,4 kB]
Atteint :4 https://packages.sury.org/nginx bookworm InRelease
Réception de :5 https://packages.sury.org/php bookworm InRelease [7 551 B]
Réception de :6 https://packages.sury.org/php bookworm/main amd64 Packages [242 kB]
352 ko réceptionnés en 3s (139 ko/s)
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
4 paquets peuvent être mis à jour. Exécutez « apt list --upgradable » pour les voir.
root@serveurrevision:~# apt upgrade
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Calcul de la mise à jour... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  apache2-bin apache2-data apache2-utils inetutils-syslogd libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.3-0 libsodium23
Veuillez utiliser « apt autoremove » pour les supprimer.
Les NOUVEAUX paquets suivants seront installés :
  libfribidi0 libgomp1 libgraphite2-3 libharfbuzz0b libimagequant0 libraqm0
Les paquets suivants seront mis à jour :
  libgd3 libhashkit2 libmemcached11 libmemcachedutil2
4 mis à jour, 6 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 2 489 ko dans les archives.
Après cette opération, 3 502 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n]
```

```
root@serveurrevision:~# apt install -y php8.3_
```

```
root@serveurrevision:~# apt install php8.3-fpm
```

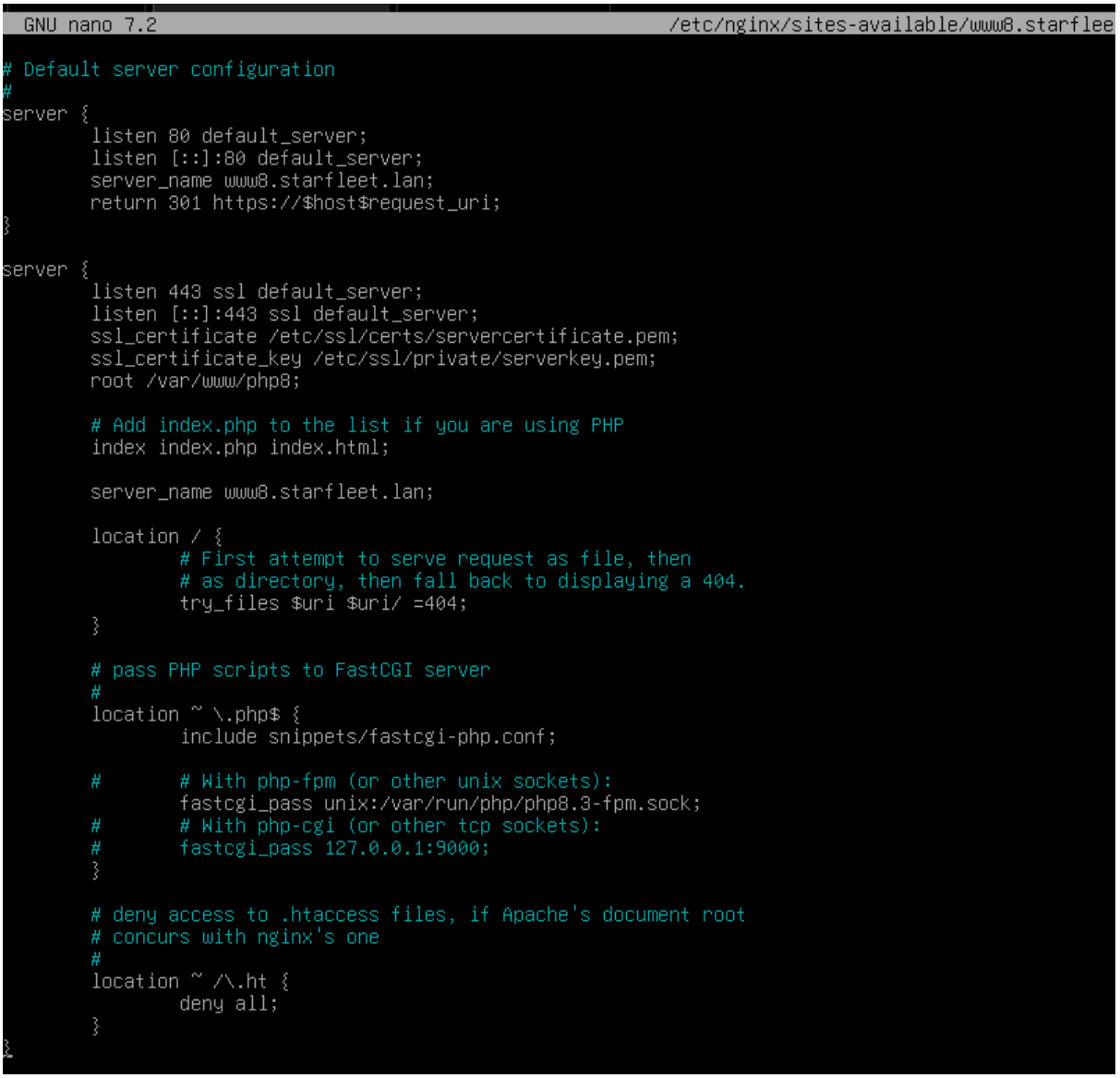
```
root@serveurrevision:~# apt install -y php7.4
```

```
root@serveurrevision:~# apt install php7.4-fpm
```

```
root@serveurrevision:~# mkdir -p /var/www/php7
root@serveurrevision:~# mkdir -p /var/www/php8
```

Créations de nos 2 fichiers configurations pour chaque serveur web php

PHP8 www8.starfleet.lan



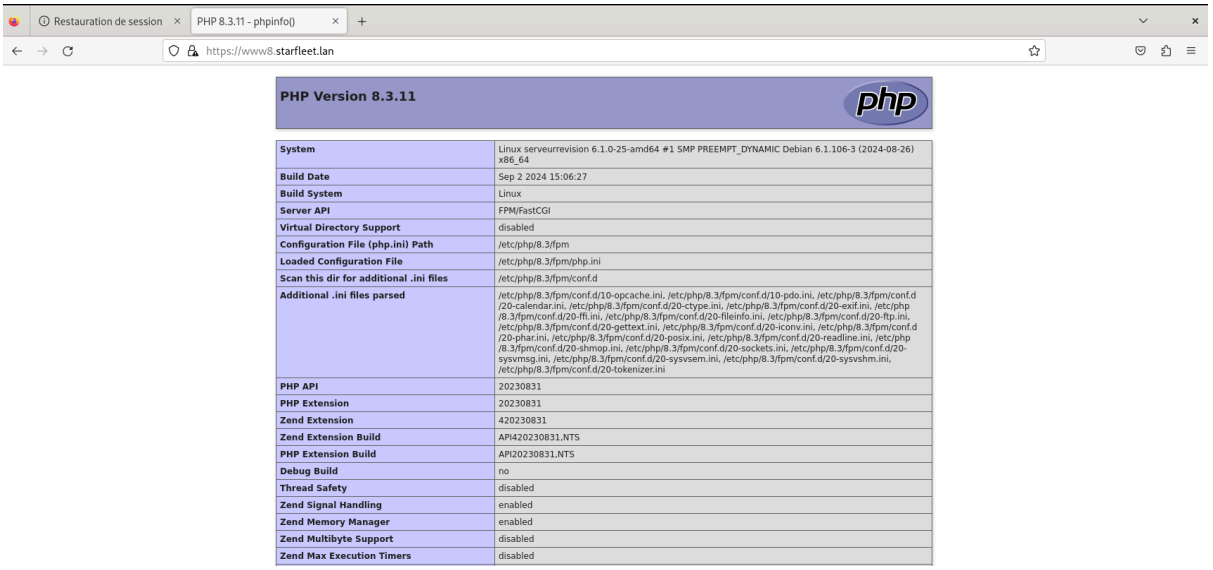
PHP7 www7.starfleet.lan

```
server {
        listen 80 default_server;
        listen [::]:80 default_server;
        server_name www7.starfleet.lan;
        return 301 https://$host$request_uri;
}

server {
        listen 443 ssl default_server;
        listen [::]:443 ssl default_server;
        ssl_certificate /etc/ssl/certs/servercertificate.pem;
        ssl_certificate_key /etc/ssl/private/serverkey.pem;
        root /var/www/php7;

        # Add index.php to the list if you are using PHP
        index index.php index.html;

        server_name www7.starfleet.lan;

        location / {
                # First attempt to serve request as file, then
                # as directory, then fall back to displaying a 404.
                try_files $uri $uri/ =404;
        }

        # pass PHP scripts to FastCGI server
        #
        location ~ \.php$ {
                include snippets/fastcgi-php.conf;

        #       # With php-fpm (or other unix sockets):
                fastcgi_pass unix:/var/run/php/php7.4-fpm.sock;
        #       # With php-cgi (or other tcp sockets):
        #       fastcgi_pass 127.0.0.1:9000;
        }

        # deny access to .htaccess files, if Apache's document root
        # concurs with nginx's one
        #
        location ~ /\.ht {
                deny all;
        }
}
```

Nous allons lier les fichiers pour qu’ils aient un lien avec sites-enabled

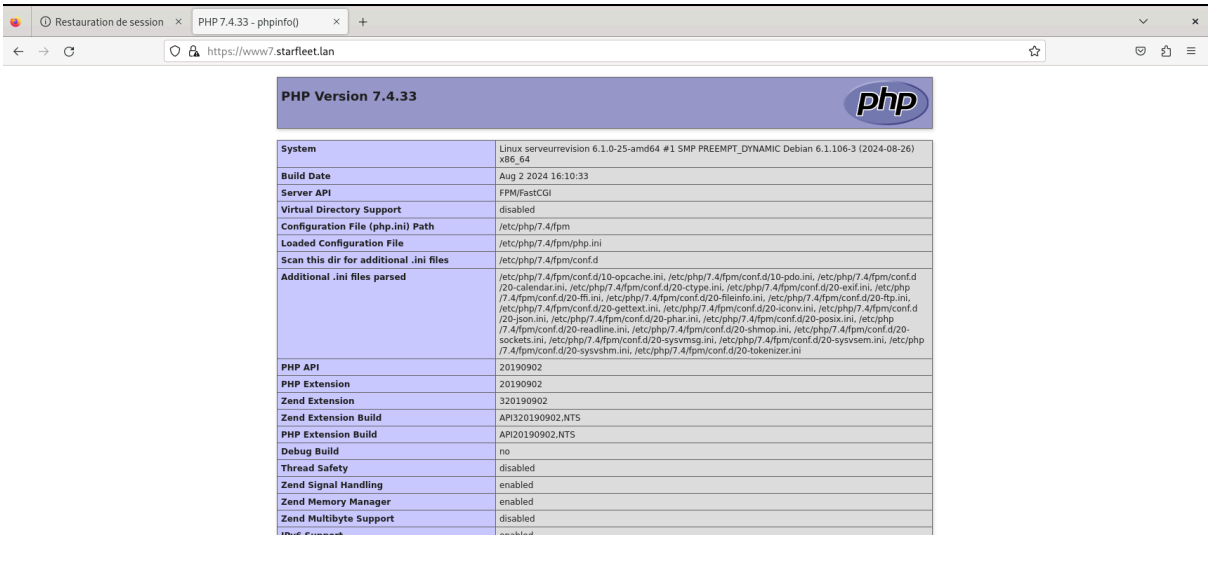
```
root@serveurrevision:~# ln -s /etc/nginx/sites-available/www8.starfleet.lan /etc/nginx/sites-enabled/
```

```
root@serveurrevision:~# ln -s /etc/nginx/sites-available/www7.starfleet.lan /etc/nginx/sites-enabled/
```



PHP Version 8.3.11

System	Linux serveurrevision 6.1.0-25-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.106-3 (2024-08-26) x86_64
Build Date	Sep 2 2024 15:06:27
Build System	Linux
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/8.3/fpm
Loaded Configuration File	/etc/php/8.3/fpm/php.ini
Scan this dir for additional .ini files	/etc/php/8.3/fpm/conf.d
Additional .ini files parsed	/etc/php/8.3/fpm/conf.d/10-opcache.ini, /etc/php/8.3/fpm/conf.d/10-pdo.ini, /etc/php/8.3/fpm/conf.d/20-calendar.ini, /etc/php/8.3/fpm/conf.d/20-ctype.ini, /etc/php/8.3/fpm/conf.d/20-exif.ini, /etc/php/8.3/fpm/conf.d/20-ffi.ini, /etc/php/8.3/fpm/conf.d/20-fileinfo.ini, /etc/php/8.3/fpm/conf.d/20-ftp.ini, /etc/php/8.3/fpm/conf.d/20-gettext.ini, /etc/php/8.3/fpm/conf.d/20-iconv.ini, /etc/php/8.3/fpm/conf.d/20-phar.ini, /etc/php/8.3/fpm/conf.d/20-posix.ini, /etc/php/8.3/fpm/conf.d/20-readline.ini, /etc/php/8.3/fpm/conf.d/20-shmop.ini, /etc/php/8.3/fpm/conf.d/20-sockets.ini, /etc/php/8.3/fpm/conf.d/20-sysvmsg.ini, /etc/php/8.3/fpm/conf.d/20-sysvsem.ini, /etc/php/8.3/fpm/conf.d/20-sysvshm.ini, /etc/php/8.3/fpm/conf.d/20-tokenizer.ini
PHP API	20230831
PHP Extension	20230831
Zend Extension	420230831
Zend Extension Build	API420230831,NTS
PHP Extension Build	API20230831,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
Zend Max Execution Timers	disabled



PHP Version 7.4.33

System	Linux serveurrevision 6.1.0-25-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.106-3 (2024-08-26) x86_64
Build Date	Aug 2 2024 16:10:33
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/fpm
Loaded Configuration File	/etc/php/7.4/fpm/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/fpm/conf.d
Additional .ini files parsed	/etc/php/7.4/fpm/conf.d/10-opcache.ini, /etc/php/7.4/fpm/conf.d/10-pdo.ini, /etc/php/7.4/fpm/conf.d/20-calendar.ini, /etc/php/7.4/fpm/conf.d/20-ctype.ini, /etc/php/7.4/fpm/conf.d/20-exif.ini, /etc/php/7.4/fpm/conf.d/20-ffi.ini, /etc/php/7.4/fpm/conf.d/20-fileinfo.ini, /etc/php/7.4/fpm/conf.d/20-ftp.ini, /etc/php/7.4/fpm/conf.d/20-gettext.ini, /etc/php/7.4/fpm/conf.d/20-iconv.ini, /etc/php/7.4/fpm/conf.d/20-json.ini, /etc/php/7.4/fpm/conf.d/20-phar.ini, /etc/php/7.4/fpm/conf.d/20-posix.ini, /etc/php/7.4/fpm/conf.d/20-readline.ini, /etc/php/7.4/fpm/conf.d/20-shmop.ini, /etc/php/7.4/fpm/conf.d/20-sockets.ini, /etc/php/7.4/fpm/conf.d/20-sysvmsg.ini, /etc/php/7.4/fpm/conf.d/20-sysvsem.ini, /etc/php/7.4/fpm/conf.d/20-sysvshm.ini, /etc/php/7.4/fpm/conf.d/20-tokenizer.ini
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902,NTS
PHP Extension Build	API20190902,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled

NGINX MariaDB PhpMyAdmin

MariaDB Server | MariaDB Server Repositories | Connectors

MariaDB Foundation provides packages for MariaDB versions newer than the version provided by the distribution only.

Choose a distribution

Debian 12 "Bookworm"

Choose a MariaDB Server version

11.4

Mirror

Renater - France

Here are the commands to run to import the MariaDB repository key on your Debian system:

```
sudo apt-get install apt-transport-https curl
sudo mkdir -p /etc/apt/keyrings
sudo curl -o /etc/apt/keyrings/mariadb-keyring.pgp 'https://mariadb.org/mariadb_rele
```

Once the key is imported, copy and paste the following into a file under `/etc/apt/sources.list.d` (for instance `/etc/apt/sources.list.d/mariadb.sources`):

Installation de la dernière version de mariaDB (sur le site de mariadb, tout est écrit)

```
root@serveurrevision:~# curl -o /etc/apt/keyrings/mariadb-keyrings.pgp "https://mariadb.org/mariadb_release_signing_key.pgp"
```

```
root@serveurrevision:~# echo "deb [signed-by=/usr/share/keyrings/mariadb-archive-keyring.gpg] http://mirrors.ircam.fr/pub/mariadb/repo/11.4/debian bookworm main" | sudo tee /etc/apt/sources.list.d/mariadb.list
```

```
root@serveurrevision:~# mariadb --version
mariadb from 11.4.3-MariaDB, client 15.2 for debian-linux-gnu (x86_64) using  EditLine wrapper
```

```
root@serveurrevision:~# mysql_secure_installation
/usr/bin/mysql_secure_installation: Deprecated program name. It will be removed in a future release, use 'mariadb-secure
-installation' instead

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
haven't set the root password yet, you should just press enter here.

Enter current password for root (enter for none):
```

Installer le paquet phpmyadmin

```
root@serveurrevision:~# sudo apt install phpmyadmin php-mbstring php-zip php-gd php-json php-curl
```

```
root@serveurrevision:~# sudo ln -s /usr/share/phpmyadmin/ /var/www/phpmyadmin
```

Créons notre première base de données :

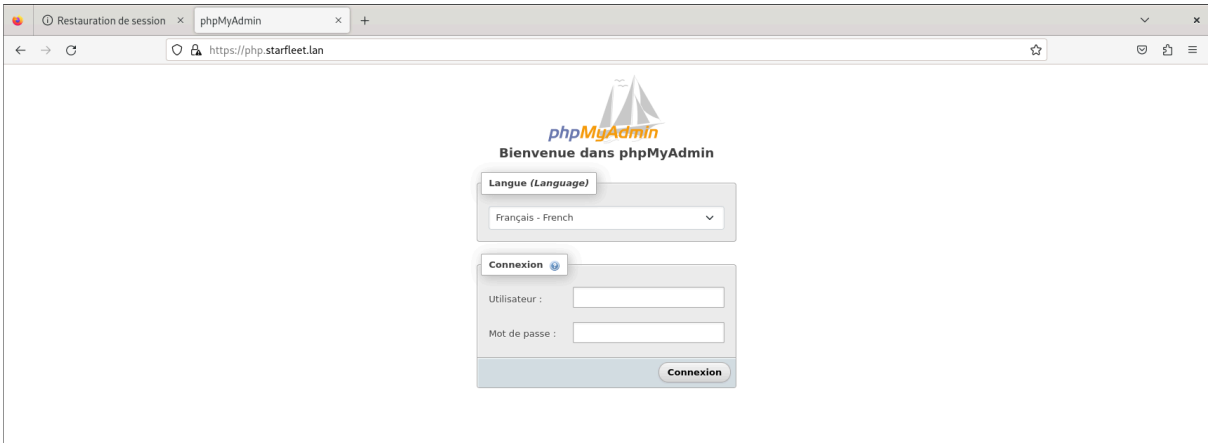
```
root@serveurrevision:~# mysql -u root -p
```

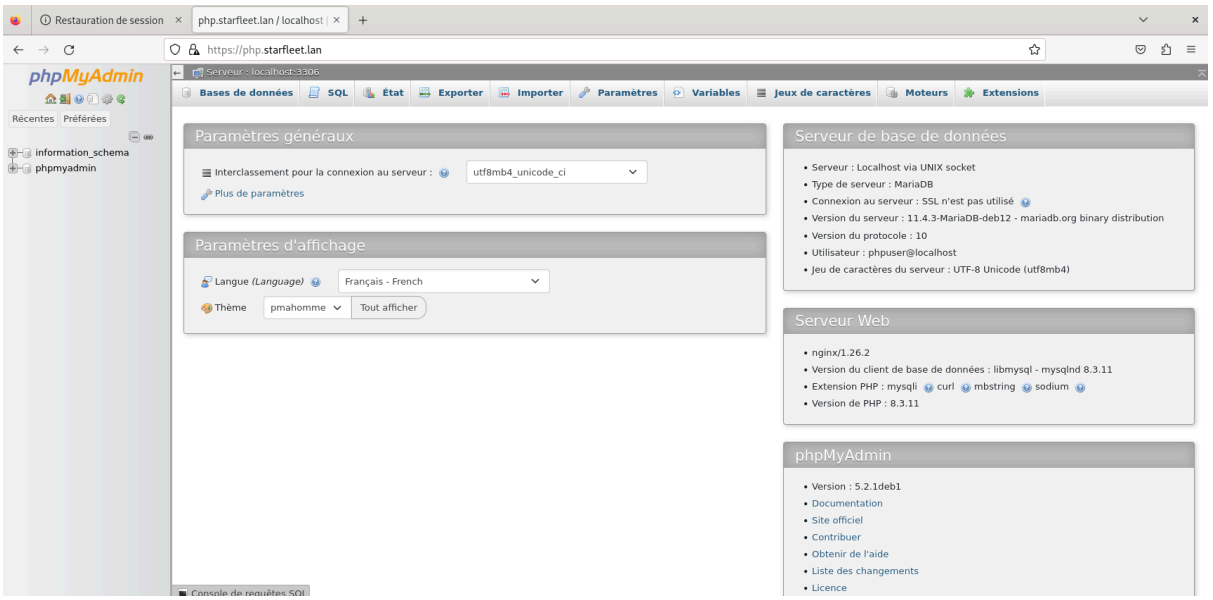
```
MariaDB [(none)]> CREATE DATABASE phpmyadmin;
Query OK, 1 row affected (0,001 sec)

MariaDB [(none)]> CREATE USER 'phpuser'@'localhost' IDENTIFIED BY 'azerty';
Query OK, 0 rows affected (0,004 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON phpmyadmin.* TO 'phpuser'@'localhost';
Query OK, 0 rows affected (0,004 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,002 sec)
```

Et créons le fichier php.starfleet.lan

```
nano /etc/nginx/sites-available/php.starfleet.lan
```

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

server {
        listen 443 ssl;
        listen [::]:443 ssl;
        ssl_certificate /etc/ssl/certs/servercertificate.pem;
        ssl_certificate_key /etc/ssl/private/serverkey.pem;
        root /var/www/phpmyadmin/phpmyadmin;

        # Add index.php to the list if you are using PHP
        index index.php index.html;

        server_name php.starfleet.lan;

        location / {
                # First attempt to serve request as file, then
                # as directory, then fall back to displaying a 404.
                try_files $uri $uri/ =404;
        }
```





Serveur Web d’administration des VM

Installons cockpit qui sera notre serveur d'administration :

```
root@serveurrevision:~# apt install cockpit
```

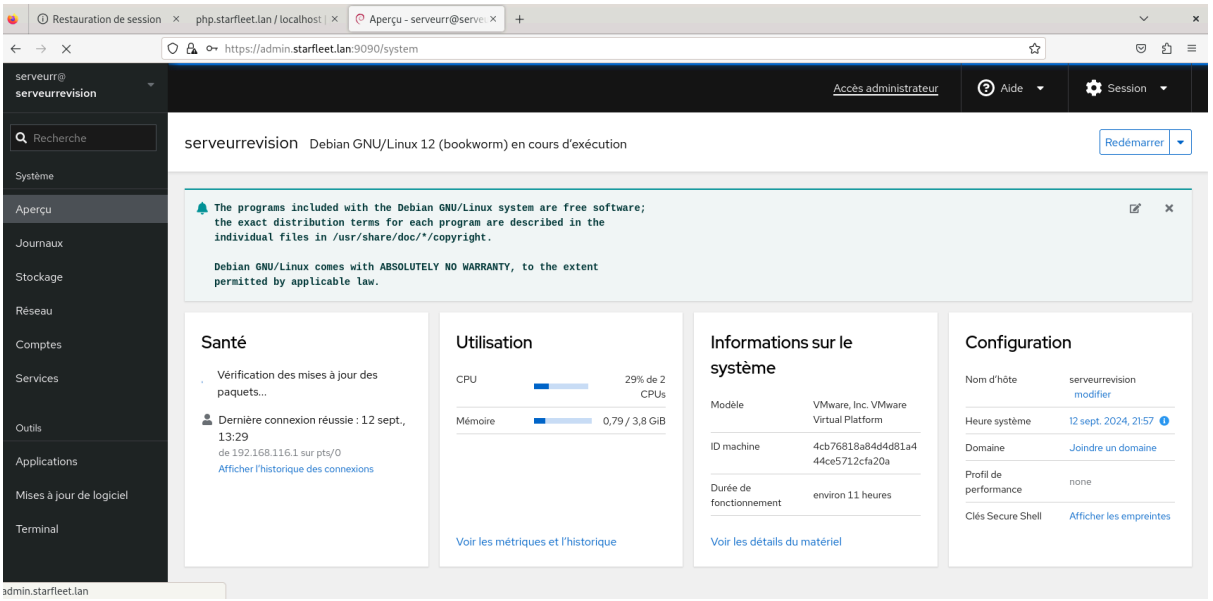
Ouvrons les ports de cockpit soit 9090

```
root@serveurrevision:~# ufw allow 9090
Rule added
Rule added (v6)
```

Configurons le fichier /etc/nginx/sites-available/admin.starfleet.lan pour qu'il se connecte au proxy de cockpit

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

server {
        listen 443 ssl;
        listen [::]:443 ssl;
        ssl_certificate /etc/ssl/certs/servercertificate.pem;
        ssl_certificate_key /etc/ssl/private/serverkey.pem;
        root /var/www/admin;

        # Add index.php to the list if you are using PHP
        index index.php index.html;

        server_name admin.starfleet.lan;

        location / {
                # First attempt to serve request as file, then
                # as directory, then fall back to displaying a 404.
                try_files $uri $uri/ =404;
                proxy_pass https://localhost: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_buffering off;
        }
        # pass PHP scripts to FastCGI server
        #
```

Testons sur la VM cliente :



LDAP NGINX

Ldap nginx module n'est pas disponible sur le dépot de sury et debian. Pour ce faire, on va aller cloner un github qui est fait pour le ldap nginx

```
root@serveurrevision:~# git clone https://github.com/kvspb/nginx-auth-ldap.git
```

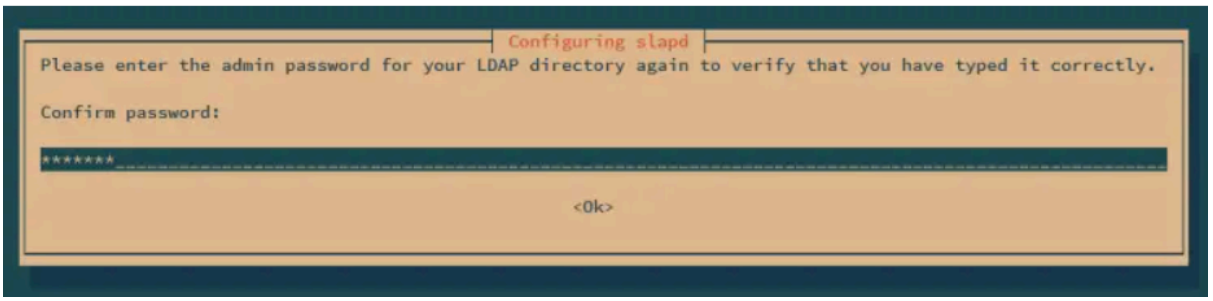
```
root@serveurrevision:~/nginx-auth-ldap# nginx -V
nginx version: nginx/1.26.2
```

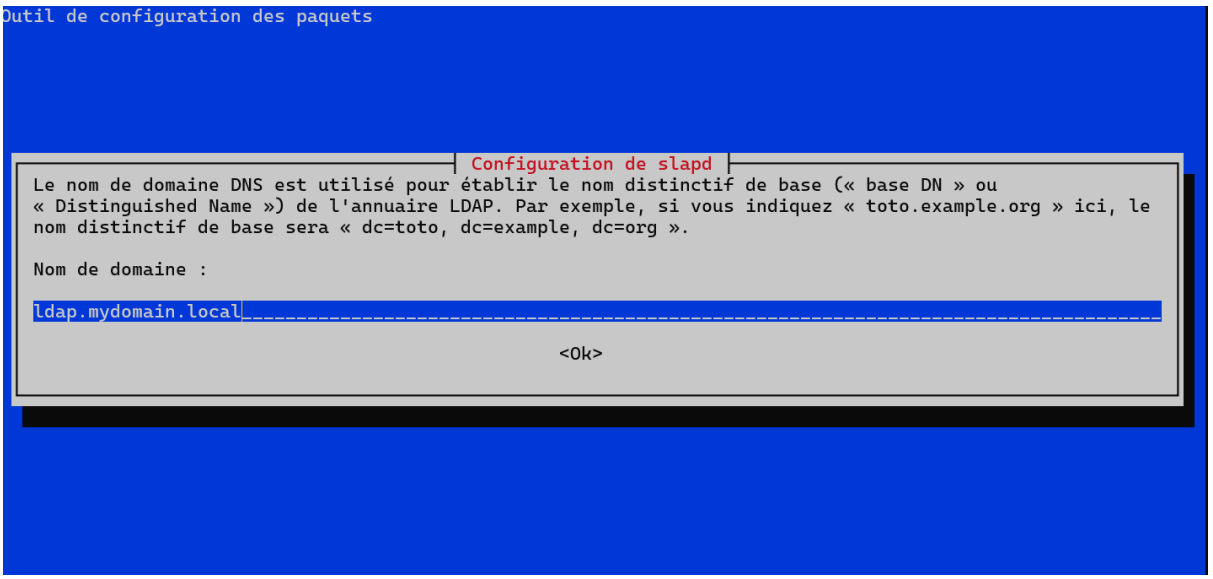
```
root@serveurrevision:~/nginx-auth-ldap# wget http://nginx.org/download/nginx-1.26.2.tar.gz
```

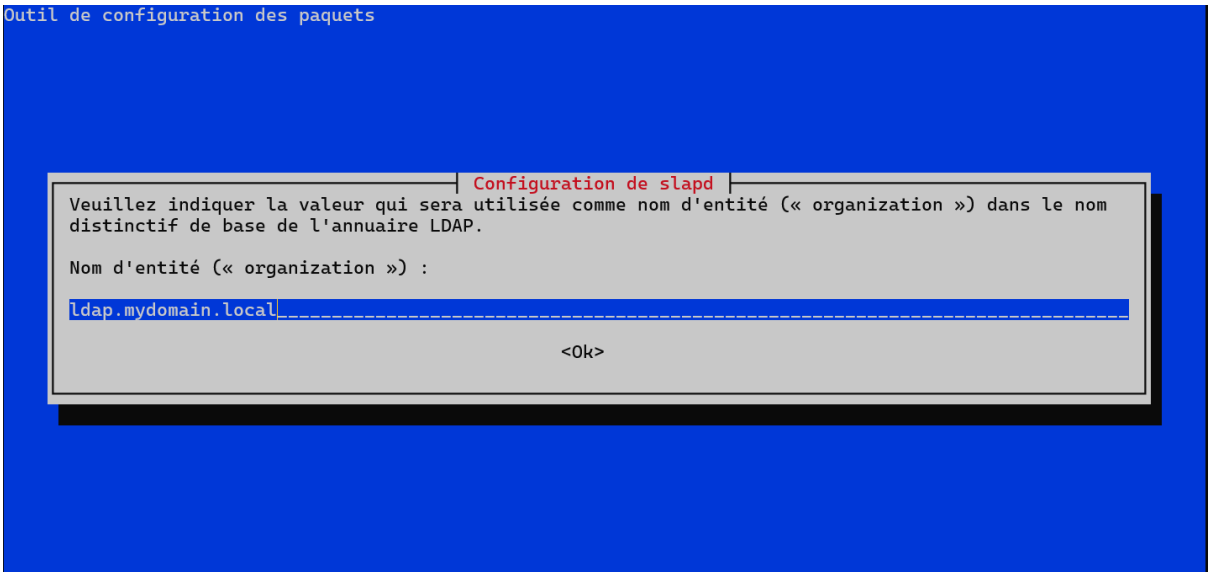
```
root@serveurrevision:~/nginx-auth-ldap# tar -zxvf nginx-1.26.2.tar.gz
```

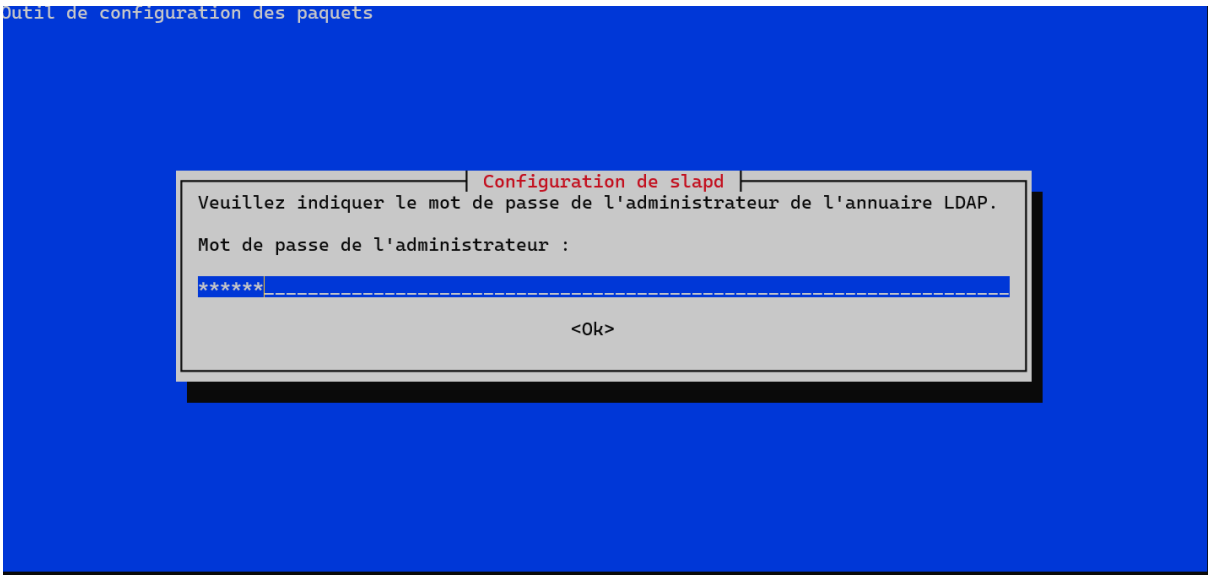
Une fois installé, nous allons installer Openldap qui sera notre serveur ldap :

```
root@serveurrevision:~# apt install slapd ldap-utils
```




Outil de configuration des paquets
Configuration de slapd
Le nom de domaine DNS est utilisé pour établir le nom distinctif de base (« base DN » ou « Distinguished Name ») de l'annuaire LDAP. Par exemple, si vous indiquez « toto.example.org » ici, le nom distinctif de base sera « dc=toto, dc=example, dc=org ».
Nom de domaine :
ldap.mydomain.local
<Ok>


Outil de configuration des paquets
Configuration de slapd
Veuillez indiquer la valeur qui sera utilisée comme nom d'entité (« organization ») dans le nom distinctif de base de l'annuaire LDAP.
Nom d'entité (« organization ») :
ldap.mydomain.local
<Ok>


Outil de configuration des paquets
Configuration de slapd
Veuillez indiquer le mot de passe de l'administrateur de l'annuaire LDAP.
Mot de passe de l'administrateur :
******
<Ok>


```
root@serveurrevision:~# sudo dpkg-reconfigure slapd
  Backing up /etc/ldap/slapd.d in /var/backups/slapd-2.5.13+dfsg-5... done.
  Moving old database directory to /var/backups:
  - directory unknown... done.
  Creating initial configuration... done.
  Creating LDAP directory... done.
```

Une fois bien configuré, ouvrons les ports pour le ldap :

```
root@serveurrevision:~# ufw allow OpenSSH
Rule added
Rule added (v6)
root@serveurrevision:~# ufw allow LDAP
Rule added
Rule added (v6)
root@serveurrevision:~# ufw allow LDAPS
Rule added
Rule added (v6)
root@serveurrevision:~# ufw allow "WWW Full"
Rule added
Rule added (v6)
```

Configurons notre premier DN Ldap :

```
root@serveurrevision:~# nano base.ldif
```

```
  GNU nano 7.2                                                  base.ldif *
dn: ou=users,dc=ldap,dc=mydomain,dc=local
objectClass: organizationalUnit
ou: users

dn: cn=admin,ou=users,dc=ldap,dc=mydomain,dc=local
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword: adminpassword
```

```
root@serveurrevision:~# ldapadd -x -D "cn=admin,dc=ldap,dc=mydomain,dc=local" -W -f base.ldif
Enter LDAP Password:
adding new entry "ou=users,dc=ldap,dc=mydomain,dc=local"

adding new entry "cn=admin,ou=users,dc=ldap,dc=mydomain,dc=local"
```

Testons si tout a bien fonctionné :

```
root@serveurrevision:~# ldapsearch -x -H ldap://localhost -b "dc=ldap,dc=mydomain,dc=local"
# extended LDIF
#
# LDAPv3
# base <dc=ldap,dc=mydomain,dc=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# ldap.mydomain.local
dn: dc=ldap,dc=mydomain,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: ldap.mydomain.local
dc: ldap
```

Ajoutons la fonctionnalité ldap sur notre fichier nginx.conf

```
 GNU nano 7.2                                    /etc/nginx/nginx.conf *
        gzip on;

        # gzip_vary on;
        # gzip_proxied any;
        # gzip_comp_level 6;
        # gzip_buffers 16 8k;
        # gzip_http_version 1.1;
        # gzip_types text/plain text/css application/json application/javascript text/xml applic

        ##
        # Virtual Host Configs
        ##
    ldap_server my_ldap {
        url ldap://localhost:389/DC=ldap,DC=mydomain,DC=local?sAMAccountName?sub?(objectClass=pe
        binddn "cn=admin,dc=ldap,dc=mydomain,dc=local";
        binddn_passwd "adminpassword";
        group_attribute memberOf;
        group_attribute_is_dn on;
        require valid_user;
    }
```

Le problème ,ici, est que la dernière version Nginx n'est plus du tout compatible avec le module ldap ce qui est un problème seul les anciennes versions fonctionnent

```
/nginx/modules/ngx_http_auth_ldap_module.so" is not binary compatible in /etc/nginx/nginx.conf:6
```

Donc nous allons essayé d'une autre manière selon un autre github (en utilisant docker)

```
root@serveurrevision:~# git clone https://github.com/nginxinc/nginx-ldap-auth.git
```

```
root@serveurrevision:~# docker build -t nginx-ldap-auth-daemon .
```

```
root@serveurrevision:~# docker-compose up -d
```

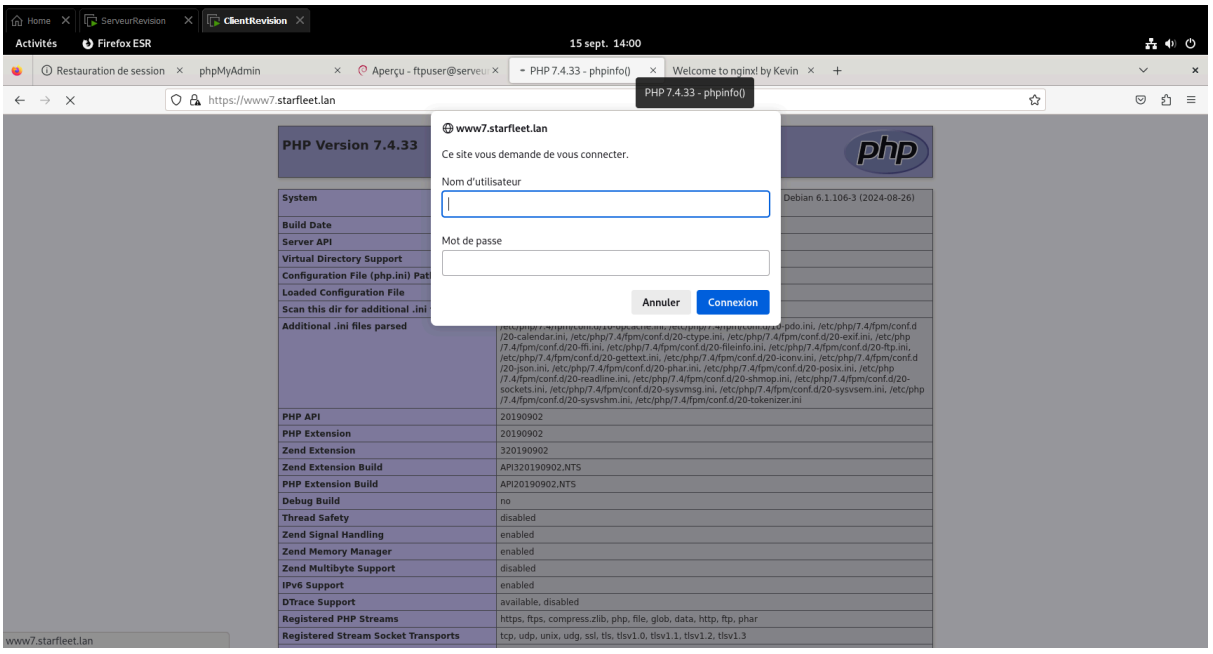
Activons le ldap du docker :

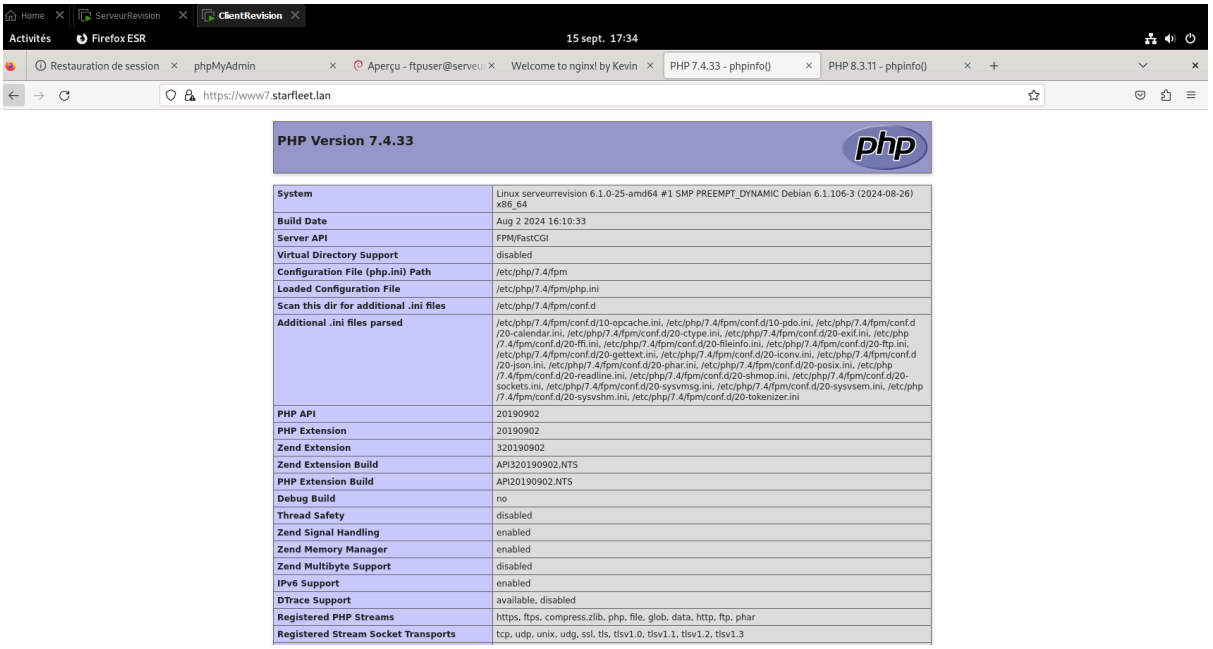
```
 GNU nano 7.2                                                  docker-compose.yml
version: '3.2'

services:
  nginx-ldap-auth:
    image: nginx-ldap-auth-daemon
    ports:
      - "8888:8888"
```

Configurons notre serveur web php7 et php8 pour l'authentification ldap

```
 GNU nano 7.2                                  /etc/nginx/sites-available/www7.starfleet.lan
server {
        listen 443 ssl;
        listen [::]:443 ssl;
        ssl_certificate /etc/ssl/certs/servercertificate.pem;
        ssl_certificate_key /etc/ssl/private/serverkey.pem;
        root /var/www/php7;
        # Add index.php to the list if you are using PHP
        index index.php index.html;
        server_name www7.starfleet.lan;
        location /{
                auth_request /auth-proxy;
                error_page 401 =200 /;
        # as directory, then fall back to displaying a 404.
                try_files $uri $uri/ =404;
                #auth_request http://192.168.10.26:9091/api/verify;
        }

        location = /auth-proxy {
                internal;
                proxy_pass http://localhost:8888;
                proxy_pass_request_body off;
                proxy_set_header Content-Length "";
                #proxy_cache auth_cache;
                #proxy_cache_valid 200 10m;
                proxy_cache_key "$http_authorization$cookie_nginxauth";
                proxy_set_header X-Ldap-URL "ldap://192.168.10.26";
                proxy_set_header X-Ldap-Starttls "false";
                proxy_set_header X-Ldap-BaseDN "dc=ldap,dc=mydomain,dc=local";
                proxy_set_header X-Ldap-BindDN "cn=admin,dc=ldap,dc=mydomain,dc=local";
                proxy_set_header X-Ldap-BindPass "azerty";
                proxy_set_header X-CookieName "nginxauth";
                proxy_set_header Cookie nginxauth=$cookie_nginxauth;
                proxy_set_header X-Ldap-Template "(uid=%(username)s)";
        }
```

Le test fonctionne, nous avons bien l'authentification ldap qui se montre quand nous voulons entrer sur le serveur web php7.

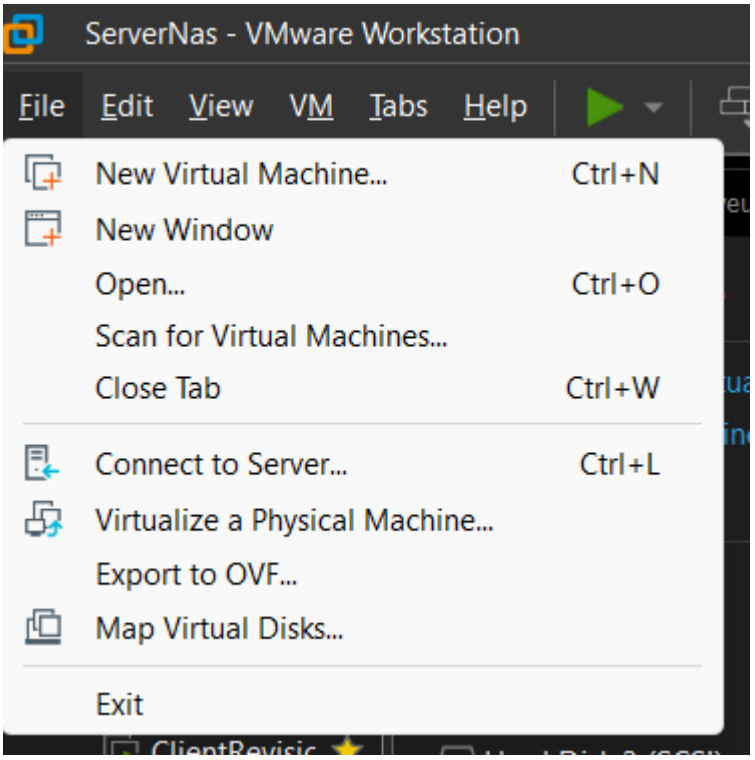


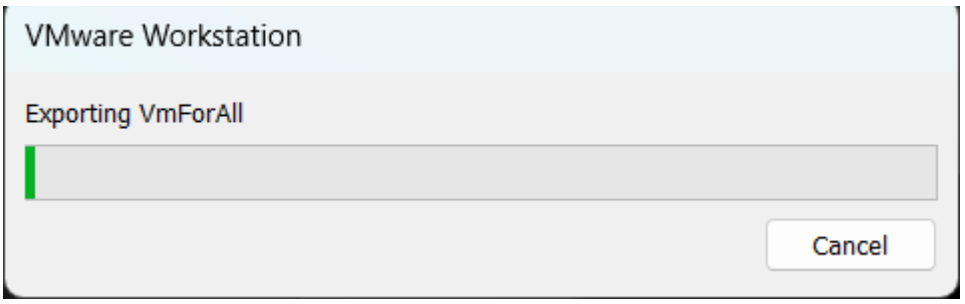


Export des VM

Cliquez sur la machine Vm que vous souhaitez exporter.

Exportation d’une Vm avec Export to OVF :





Voilà, vous avez exporté, maintenant pour l'importer rien de plus simple que d'ajouter une nouvelle VM et mettre la Vm exporter dans le format .ovf