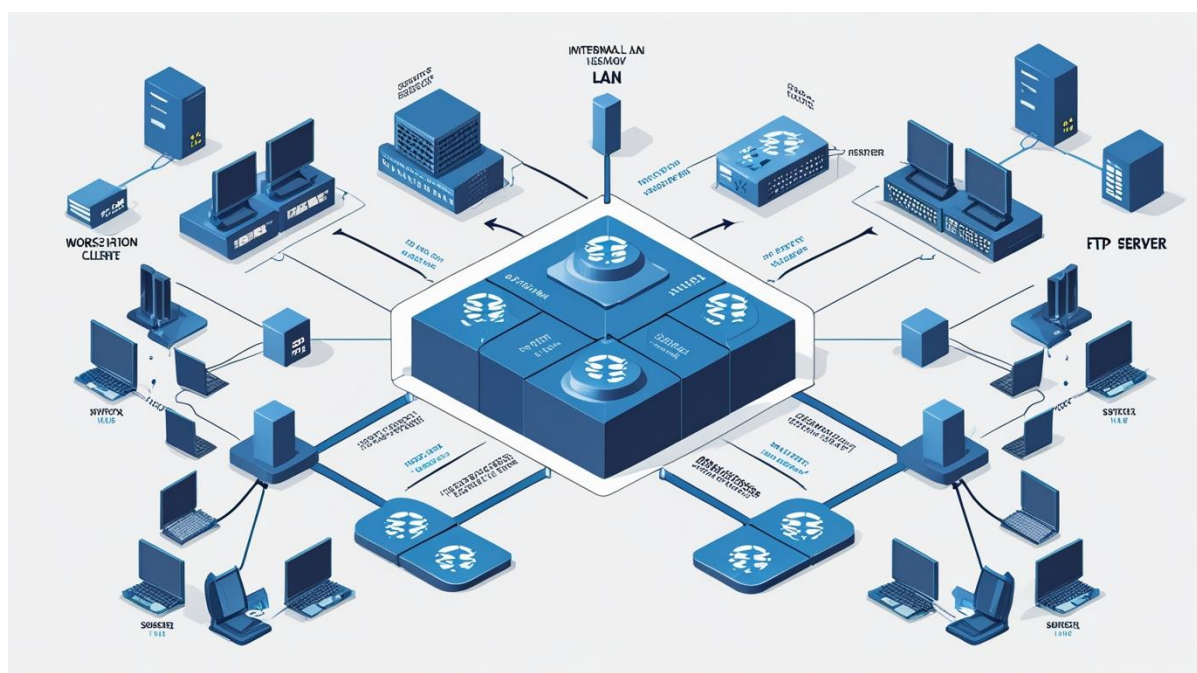


Document technique

AP2 – SISR

Mise en place de solutions techniques sur un réseau d'entreprise, à l'aide de serveurs LAMP et FTP



Dates du projet :
Début le 06/02/2026
Fin le 06/03/2026

Equipe 4
Bardet Arthur
Vallée Estéban

Sommaire

Table des matières

Document technique.....	1
Sommaire.....	2
Présentation du contexte de l'entreprise	3
Les objectifs attendus	4
Voici ci-dessous la liste de nos différentes tâches :.....	5
Comment travailler en binôme ?.....	6
A.1 Installation de l'environnement.....	8
A.2 Paramétrage IP	10
A.3 Configuration de l'accès à distance SSH au serveur	11
A.4 Installation du serveur web	13
A.5 Fiche de configuration et rapport de tests du service web	14
A.6 Installation du serveur FTP	15
A.7 Sécurisation du serveur FTP	17
A.9 Résolution du nom « gestion.mdl.local » grâce au DNS Windows Server	18

Présentation du contexte de l'entreprise

La maison des ligues fait appel à l'entreprise NetworkSI qui est une SSII dont nous sommes employés. On a pu déjà mettre en place une solution de centralisation réseau des accès utilisateurs ainsi qu'un serveur de fichiers à l'aide d'un contrôleur de domaine Active Directory. La maison des ligues souhaite à présent mettre en place un nouvel outil de gestion des adhérents qui sera une solution web Intranet à destination du service comptabilité ainsi qu'un accès FTP pour ses développeurs afin de réaliser les mises à jour du site. L'entreprise a choisi d'héberger en interne les serveurs. Cette solution sera intégrée au réseau existant déjà mis en place.

L'adresse IP associée à cette machine sera dans la continuité des précédentes : 172.18.40.3

Le site doit être accessible depuis le nom « gestion.mdl.local » qui sera présent sur le réseau local.

L'application qui nous permettra de réaliser cette AP sera hébergée sur un serveur virtuel sur Hyper-V. Le serveur sera sous « Ubuntu server 22.04 » et les utilisateurs seront sur Windows 10 et 11. Les machines Windows ainsi que le serveur Ubuntu seront ajoutés au domaine MDL.LOCAL.

L'environnement devra être accessible aux seuls acteurs de l'entreprise, la mise en place d'un mot de passe sécurisé et donc obligatoire. Les connexions devront être identifiées à l'aide d'un nom d'utilisateur.

Il y aura des fonctionnalités à mettre en place comme : un serveur Web sécurisé, ainsi qu'un serveur FTP sécurisé (Prot FTPD).

Les objectifs attendus

Cet atelier va nous permettre de découvrir de nouvelles compétences comme la mise en place d'un site internet sur Ubuntu 22.04, le travail de groupe, puis par la suite toutes nos compétences apprises en cours tout au long de l'année.

Pour réaliser ce travail, nous avons un cahier des charges, qui nous explique comment faire et avec quelles conditions ainsi que du matériel (serveur, Pc avec VM).

L'avancée de l'Atelier Professionnel sera renseignée sur une application, « Trello ». Cette application nous permet de savoir les tâches en cours de traitement, celles qui ne sont pas encore démarrées ou encore celles qui sont terminées.

Un autre logiciel nous sera utile : Gantt. Ce dernier permet de mesurer le temps utilisé pour chaque étape de l'AP pour comparer ce temps avec celui prévu à la base.

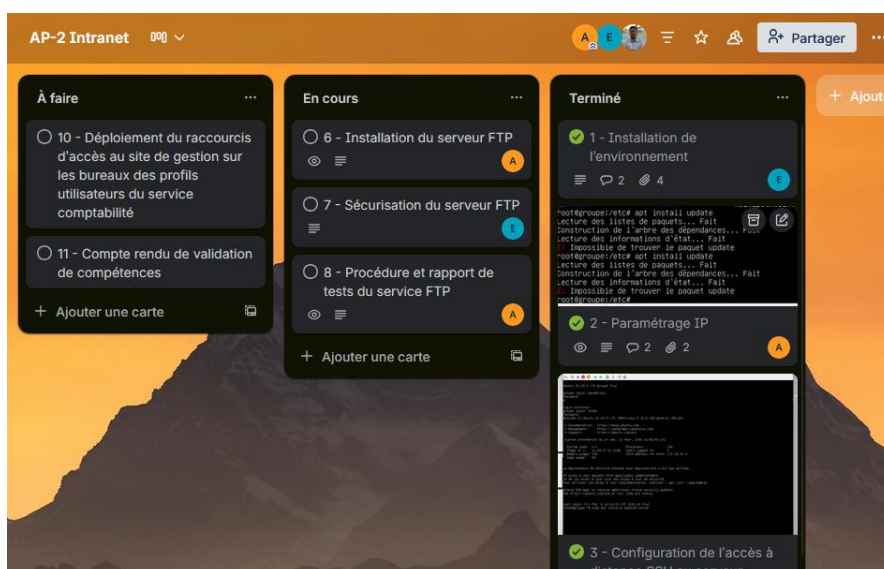
Voici ci-dessous la liste de nos différentes tâches :

- A.1 Installation de l'environnement**
- A.2 Paramétrage IP**
- A.3 Configuration de l'accès à distance SSH au serveur**
- A.4 Installation du serveur web**
- A.5 Fiche de configuration et rapport de tests du service web**
- A.6 Installation du serveur FTP**
- A.7 Sécurisation du serveur FTP**
- A.8 Procédure et rapport de tests du service FTP**
- A.9 Résolution du nom « gestion.mdl.local » grâce au DNS Windows Server**
- A.10 Déploiement du raccourcis d'accès au site de gestion sur les bureaux des profils utilisateurs du service comptabilité**
- A.11 Compte rendu de validation de compétences**

Comment travailler en binôme ?

Pour réaliser ce travail, il faut répartir les tâches entre les membres du groupe de travail. Comme vu ci-dessus, on va utiliser le logiciel « Trello » qui va nous permettre de faire cela. La répartition des tâches se fait également à l'aide des compétences déjà acquises.

« Capture d'écran de l'appli Trello et de nos activités »



Notre deuxième outil a été Gantt qui nous a servi à nous repérer dans le temps. C'est-à-dire qu'il nous a permis de nous fixer un planning de travail. Puis au fur et à mesure, on renseigne le temps que l'on a réellement utilisé pour savoir ou l'on en a perdu.

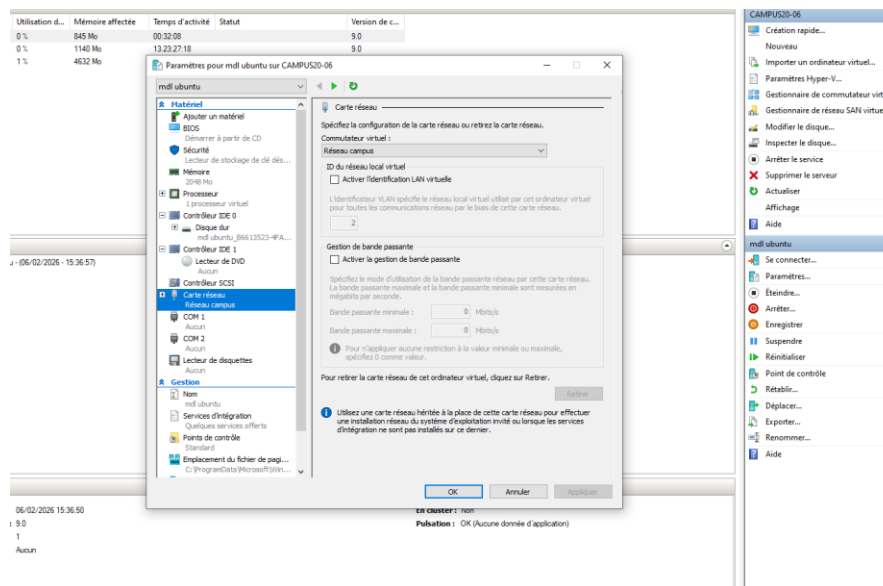
« Capture d'écran de notre Gantt »



A.1 Installation de l'environnement

Avant de commencer, on vérifie quelques paramètres. Ici on voit que notre serveur est bien sur le réseau campus, ce qui permettra la communication avec notre serveur Ubuntu. On peut maintenant continuer.

« Capture, vérification des paramètres réseaux »



Maintenant il faut télécharger Ubuntu. L'environnement Ubuntu a été téléchargé depuis le site officiel, il nous est demandé d'installer la version 22.04 d'Ubuntu. Puis une fois le téléchargement effectué, on installe une nouvelle machine sur notre hyperviseur de type 1. On la configure pour qu'elle soit dans le bon domaine, ici réseau campus.

Il faut continuer le long de l'installation. Puis on crée un identifiant "stban", un mot de passe et le nom du serveur sera groupe4.

Une fois Ubuntu installé, on s'assure qu'il soit à jour avec les commandes « apt update » et « apt install », nous avons cependant rencontré une erreur

lors de l'exécution de cette dernière, c'est pour cela qu'on a effectué apt-get upgrade --fix-missing;

« Capture, commande de correction des bugs »

```
root@groupe:/etc# apt-get upgrade --fix-missing
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 conservés :
  linux-generic linux-headers-generic sosreport
Les paquets suivants seront mis à jour :
  amd64-microcode apparmor apport apt apt-utils bind9-dnsutils bind9-host bind9-libs binutils binutils-common
  binutils-x86-64-linux-gnu ca-certificates cloud-init cryptsetup cryptsetup-bin cryptsetup-initramfs curl dirmngr
  distro-info-data dmeventd dmidecode dmsetup dpkg ethtool gcc-12-base gir1.2-packagekitglib-1.0 git git-man gnupg gnupg-l10n
  gnupg-utils gpg gpg-agent gpg-wks-client gpg-wks-server gpgconf gpgsm gpgv initramfs-tools initramfs-tools-bin
  initramfs-tools-core intel-microcode iputils-ping iputils-tracepath klibc-utils landscape-common libapparmor1 libapt-pkg6.0
  libarchive13 libbinutils libblockdev-crypto2 libblockdev-fs2 libblockdev-loop2 libblockdev-part-err2 libblockdev-part2
  libblockdev-swap2 libblockdev-utils2 libblockdev2 libc-bin libc6 libc6-dev libc6-i386 libc6-dev libc6-dev-bin libcryptsetup12 libctf-nobfd0 libctf0
  libcurl3-gnutls libcurl4 libdevmapper-event1.02.1 libdevmapper1.02.1 libdw1 libelf1 libexpat1 libfreetype6 libgcc-s1
  libgl1.0-0 libgl1.0-bin libgl1.0-data libgnutls30 libgssapi-krb5-2 libgstreamer1.0-0 libk5crypto3 libklibc libkrb5-3
  libkrb5support0 libldap-2.5-0 libldap-common liblvm2cmd2.03 libmbim-glib4 libmbim-proxy libmm-glib0 libmodule-scandeps-perl
  libnss-systemd libopeniscsiusr libpackagekit-glib2-18 libpam-cap libpam-modules libpam-modules-bin libpam-runtime
  libpam-systemd libpam0g libpcap0.8 libperl5.34 libpng16-16 libpython3.10 libpython3.10-minimal libpython3.10-stdlib
  libseccomp2 libsodium23 libsqlite3-0 libssh-4 libssl3 libstdc++6 libsystemd0 libtasn1-6 libudev1 libudisks2-0 libxml2
  libxslt1.1 linux-base linux-firmware locales lvm2 modemmanager nano needrestart open-iscsi open-vm-tools openssh-client
  openssl packagekit packagekit-tools pci.ids perl perl-base perl-modules-5.34 pollinate powermgmt-base python-apt-common
  python3-apparmor python3-apt python3-attr python3-configobj python3-jinja2 python3-pkg-resources python3-problem-report
  python3-pyasn1 python3-requests python3-setuptools python3-twisted python3-update-manager python3-urllib3 python3.10
  python3.10-minimal rsync screen snapd sudo systemd systemd-hwe-hwdb systemd-sysv systemd-timesyncd tzdata
  ubuntu-advantage-tools ubuntu-drivers-common ubuntu-minimal ubuntu-pro-client ubuntu-pro-client-l10n ubuntu-server
  ubuntu-server-minimal ubuntu-standard udev udisks2 update-manager-core usbmuxd vim vim-common vim-runtime vim-tiny
  wireless-regdb xfsprogs xxd
181 mis à jour, 0 nouvellement installés, 0 à enlever et 4 non mis à jour.
Il est nécessaire de prendre 447 Mo dans les archives.
Après cette opération, 102 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n]
```

Une fois la correction effectuée, on peut continuer de faire la configuration de Ubuntu. La prochaine étape est de faire la mise à jour d'Ubuntu.

« Capture de la maj d'Ubuntu »

```
root@groupe:/etc# apt install update
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
E: Impossible de trouver le paquet update
root@groupe:/etc# apt install update
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
E: Impossible de trouver le paquet update
root@groupe:/etc#
```

A.2 Paramétrage IP

Tout d'abord il faut installer les fichiers de config. Pour installer ce service nous nous aiderons d'une commande. Cette dernière est : « nano /etc/netplan/00-installer-config.yaml ».

« Capture, commande d'installation »

```
root@groupe:/etc# nano /etc/netplan/00-installer-config.yaml
```

Puis une fois le service installé et après avoir vérifié l'installation on peut maintenant configurer les paramètres réseaux. Il nous suffit d'aller dans les paramètres réseaux et de renseigner toutes les informations de configuration nécessaire.

« Capture, des paramètres réseaux »

```
# This is the network config written by 'subiquity'
network:
  version: 2
  ethernets:
    eth0:
      dhcp4: false
      addresses:
        - 172.18.40.3/16
      routes:
        - to: default
          via: 172.18.255.254
      nameservers:
        addresses:
          - 172.18.40.2
```

A.3 Configuration de l'accès à distance SSH au serveur

En premier lieu, il a fallu installer le “ssh” avec la commande “sudo apt install openssh-server”. Puis on peut vérifier avec la commande, “sudo systemctl status ssh”, elle nous permet d'être sûr que le “ssh” fonctionne correctement.

« Capture de l'installation de SSH »

```
Ubuntu 22.04.5 LTS groupe tty1
groupe login: bardetvall
Password:
g
Login incorrect
groupe login: stban
Password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-168-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of ven. 13 févr. 2026 12:58:54 UTC

System load:  0.0               Processes:    106
Usage of /:   10.5% of 61.21GB   Users logged in:  0
Memory usage: 20%              IPv4 address for eth0: 172.18.40.3
Swap usage:   0%

La maintenance de sécurité étendue pour Applications n'est pas activée.
20 mises à jour peuvent être appliquées immédiatement.
10 de ces mises à jour sont des mises à jour de sécurité.
Pour afficher ces mises à jour supplémentaires, exécuter : apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Fri Feb  6 16:14:02 UTC 2026 on tty1
stban@groupe:~$ sudo apt install openssh-server
```

Puis par la suite après avoir configuré le SSH on va pouvoir commencer les tests. Dans un premier temps il faut lancer un PowerShell. A l'aide de ce dernier on va se connecter à distance à l'aide d'un client, par exemple un wind 11, machine virtuelle.

« Capture du test de connexion SSH »

```
* Management:      https://landscape.canonical.com
* Support:         https://ubuntu.com/pro

System information as of ven. 13 févr. 2026 13:25:33 UTC

System load: 0.0          Processes:            113
Usage of /:  10.5% of 61.21GB Users logged in:        1
Memory usage: 20%        IPv4 address for eth0: 172.18.40.3
Swap usage:  0%

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
  just raised the bar for easy, resilient and secure K8s cluster deployment.

  https://ubuntu.com/engage/secure-kubernetes-at-the-edge

La maintenance de sécurité étendue pour Applications n'est pas activée.

20 mises à jour peuvent être appliquées immédiatement.
10 de ces mises à jour sont des mises à jour de sécurité.
Pour afficher ces mises à jour supplémentaires, exécuter : apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

New release '24.04.4 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Feb 13 13:22:42 2026 from 172.18.0.83
stban@groupe:~$
```

A.4 Installation du serveur web

Installation d'apache2 et de PHP sur la VM Ubuntu

Création du dossier contenant le PHP et l'html du site.

Copie de la configuration du site conf pour notre site mdl.

Activation de ce même site.

« Capture, installation du service PHP »

```
stban@groupe:~$ sudo apt-get install php -y
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :

```

Ensuite après avoir installé le service PHP, il faut créer un répertoire pour héberger notre site internet.

« Capture, création du répertoire pour notre site »

```
stban@groupe:~$ sudo mkdir /var/www/site
```

A.5 Fiche de configuration et rapport de tests du service web

A.6 Installation du serveur FTP

Avant de commencer, il faut déjà installer le protocole vsftpd. On le fera à l'aide d'une commande comme ci-dessous.

« Capture de l'installation de vsftpd »

```
rtt min/avg/max/mdev = 0.680/1.052/1.204/0.094 ms
root@groupe:/home/stban# nano /etc/hosts
root@groupe:/home/stban# nano /etc/hosts
root@groupe:/home/stban#
root@groupe:/home/stban# sudo apt install vsftpd
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  libclone-perl libencode-locale-perl libhtml-tagset-perl libhttp-date-perl liblwp-mediatypes-perl libtimedate-perl
  liburi-perl
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
Les NOUVEAUX paquets suivants seront installés :
  vsftpd
0 mis à jour, 1 nouvellement installés, 0 à enlever et 14 non mis à jour.
Il est nécessaire de prendre 123 ko dans les archives.
Après cette opération, 326 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 vsftpd amd64 3.0.5-0ubuntu1.1 [123 kB]
123 ko réceptionnés en 0s (467 ko/s)
Préconfiguration des paquets...
Sélection du paquet vsftpd précédemment désélectionné.
(Lecture de la base de données... 112710 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../vsftpd_3.0.5-0ubuntu1.1_amd64.deb ...
Dépaquetage de vsftpd (3.0.5-0ubuntu1.1) ...
Paramétrage de vsftpd (3.0.5-0ubuntu1.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /lib/systemd/system/vsftpd.service.
Traitement des actions différées (« triggers ») pour man-db (2.10.2-1) ...
Scanning processes...
```

Dans le fichier de configuration il y a de nombreuses commandes à utiliser, nous allons les voir ici. La commande « local... » permet d'autoriser les connexions locales en ftp. Ensuite, « write... » permet aux utilisateurs de pouvoir écrire ce qui est normalement pas possible.

« Capture des commande de configuration »

```
#
# Uncomment this to allow
local_enable=YES
#
# Uncomment this to enable
write_enable=YES
#
# Default umask for local
# if your users expect th
```

Puis dans le fichier des paramètres vsftpd on peut désormais les modifier. Ici dans ce screen on voit plusieurs lignes : « ssl... » sert à activer le cryptage du mot de passe, pour des questions de sécurité évidentes. Ensuite « pasv_en... » elle sert à activer le mode passif ce qui permet au client d'ouvrir des connexions vers le serveur. Puis les lignes avec les ports servent à attribuer des ports pour les connexions.

« Capture des paramètres vsftpd »

```
ssl_enable=YES

#
# Uncomment this to indicate that vsftpd use a utf8
#utf8_filesystem=YES

pasv_enable=YES
pasv_min_port=10000
pasv_max_port=10100

local_enable=YES
allow_writeable_chroot=YES
```

Maintenant on doit vérifier que le service FTP est fonctionnel. On vérifie cela à l'aide de la commande « sudo systemctl status vsftpd ».

« Capture de la vérification du statu VSFTPD »

```
root@groupe:/home/stban# sudo systemctl status vsftpd
• vsftpd.service - vsftpd FTP server
   Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2026-02-13 16:05:28 UTC; 2 weeks 4 days ago
     Process: 698 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/
   Main PID: 699 (vsftpd)
      Tasks: 1 (limit: 2143)
     Memory: 1.3M
        CPU: 5ms
    CGroup: /system.slice/vsftpd.service
            └─699 /usr/sbin/vsftpd /etc/vsftpd.conf

févr. 13 16:05:28 groupe systemd[1]: Starting vsftpd FTP server...
févr. 13 16:05:28 groupe systemd[1]: Started vsftpd FTP server.
```

A.7 Sécurisation du serveur FTP

Un des enjeux de ce travail pratique est l'aspect sécurité des données. Ici en ftp il est obligatoire de sécuriser les informations qui transitent. Dans notre cas en quelques étapes nous pouvons faire cela, à l'aide de commandes. Avec la commande en plus de « configurer » la sécurité, il faudra rentrer quelques informations facultatives.

« Capture de l'exécution de la commande de sécurisation »

```
root@sthan:/home/stban# sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 \
> -keyout /etc/ssl/private/vsftpd.pem \
> -out /etc/ssl/private/vsftpd.pem
.....+.....+...+.+.....+...+...+.....+.....+.....+.....+.....+
+.+..+++++++*....+....
+.+.....+.+.....+.....+.....+.....+.....+.....+.....+.....+.....+
.....+.+..+.+.....+.+.....+.+.....+.+.....+.+.....+.+.....+.+
.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+
+.+.....+.+.....+.+.....+.+.....+.+.....+.+.....+.+.....+.+.....+
+.+.....+.+.....+.+.....+.+.....+.+.....+.+.....+.+.....+.+.....+
.....+.....+.+.....+.+.....+.+.....+.+.....+.+.....+.+.....+.+.....+
.....+.....+.+.....+.+.....+.+.....+.+.....+.+.....+.+.....+.+.....+
-----
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]:EU
State or Province Name (full name) [Some-State]:FRANCE
Locality Name (eg, city) []:VERNON
Organization Name (eg, company) [Internet Widgits Pty Ltd]:company
Organizational Unit Name (eg, section) []:section
Common Name (e.g. server FQDN or YOUR name) []:sthan
```

Ensuite on doit activer l'encryptage des données au même endroit que précédemment, dans le fichier de configuration vsftpd. Tout cela pour ajouter plus de sécurité à notre serveur.

« Capture de l'encryptage de la clé »

```
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
rsa_cert_file=/etc/ssl/private/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
ssl_enable=YES

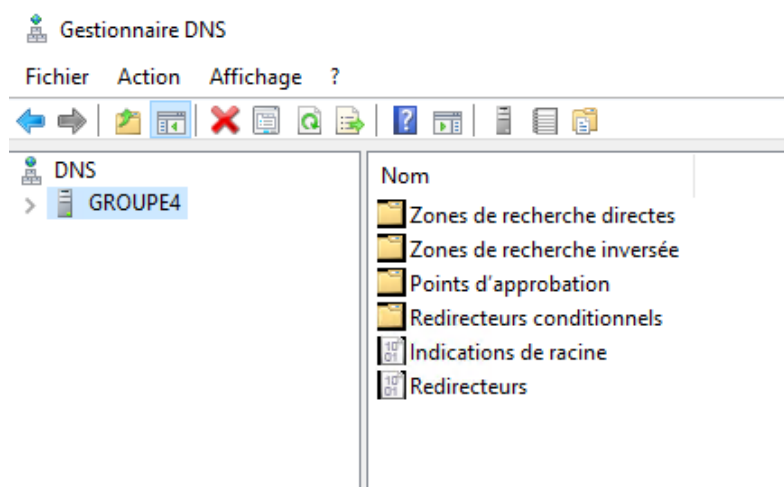
#
# Uncomment this to indicate that vsftpd use a utf8 filesystem.
#utf8 filesystem=YES
```

A.9 Résolution du nom « gestion.mdl.local » grâce au DNS Windows Server

Pour paramétrer le nom de domaine il faut nous rendre dans le Windows Serveur. Ici sera expliqué comment faire cela. Une fois dans l'accueil, il faut aller dans les paramètres. C'est ici que nous pourrons faire la configuration.

Une liste va apparaître il faut sélectionner « Gestionnaire DNS ». Une fois dedans vous aurez cette affichage :

« Captures écran du gestionnaire DNS »



Il faut maintenant cliquer sur le nom de votre serveur ici « GROUPE4 ». Un menu va s'ouvrir. Il faut cliquer sur votre nom de domaine, dans notre cas le nom est : « mdl.local ».

Il faut maintenant créer un nouvelle hôte qu'on a nommé « gestion ». Après l'avoir nommé on doit renseigner l'IP et cocher l'option « Créer un pointeur d'enregistrement PTR associé ».

« Capture de l'étape de création d'hôte »

