Colombelle Malone
Bardet Arthur
BTS SIO 2

Document de validation de compétences

ArchiSite

06/10 /2026-13/11

Equipe4

1. Présentation du contexte d'entreprise

Un Hyperviseur est déjà présent dans la DMZ et administré à distance par l'ensemble des membres du groupe.

Les différents services seront virtualisés au sein d'une ou plusieurs zones DMZ.
Un serveur virtuel par membre du groupe.
Un compte d'administration par membre du groupe.
L'environnement du serveur devra reposer sur une solution Linux.

Les utilisateurs sont sous Windows 11.

2. Objectifs attendus

- Un serveur Web sécurisé (HTTPS, SSL/TLS) exécutant des pages de script côté serveur
- Un serveur de Base de données (MySQL, MariaDB ou autre)
- Choix du service Web (Apache, Nginx ou autre)
  Un serveur FTPS

3. Plan de travail

Planification du projet / Mise en place d'une nouvelle zone DMZ avec Switch.

Réalisation du planning prévisionnel : Diagramme de Gantt à réaliser intégralement avant de commencer : <u>à faire en groupe</u>
<u>Par le chef de projet :</u> Réalisation de la répartition des tâches avec Trello en cohérence avec le diagramme de Gantt ET Suivi régulier du projet et du planning réel

Installation des Serveurs Web, Bases de données et FTPS

Paramétrage IP des machines virtuelles
Installation des services

Paramétrage de l'accès entrant vers les ressources

Accès au site web et au service FTPS
Accès à la base de données
Création des différents comptes pour les développeurs
Communication des identifiants et paramètres d'accès en respectant la date de mise en production fixée au : 03/11 17h30
Tests de validation

Sécurisation du serveur web

Installation du service
Création de l'autorité de certification
Gestion des certificats

Tests de validation

Installation du serveur FTPS

Installation du service FTPS et paramétrage d'un accès réservé aux développeurs du site
Tests de validation avec le client

Ajout \ modification des règles d'accès aux différents services

Configuration des différents accès Web, Base de données et FTP
Tests de validation

Installation du serveur DNS dans la DMZ

Ajout du service DNS
Configuration du service DNS
Tests de validation

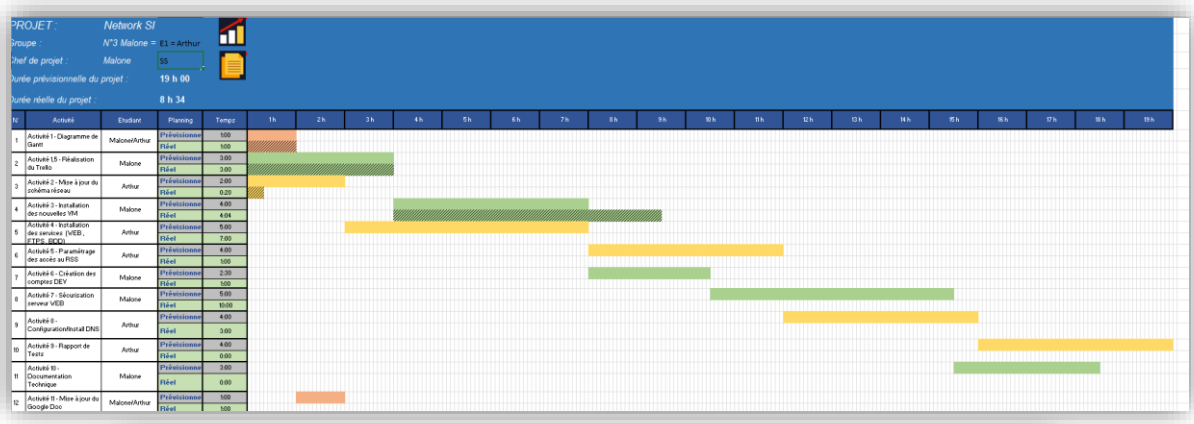
Rédaction de la documentation

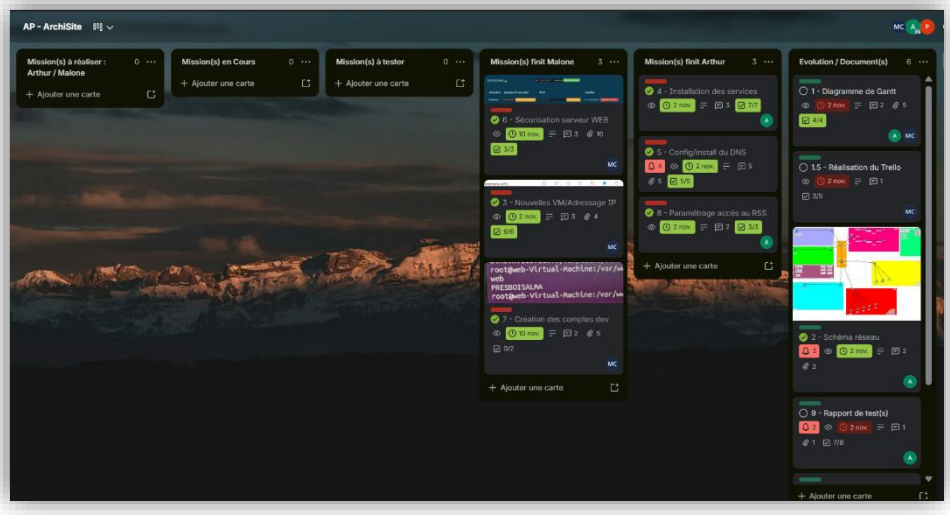
Fichiers de configuration commentés
Rapport de tests
Schéma réseau modifié

4. Réalisation

Activité 1 - Planification du Projet :

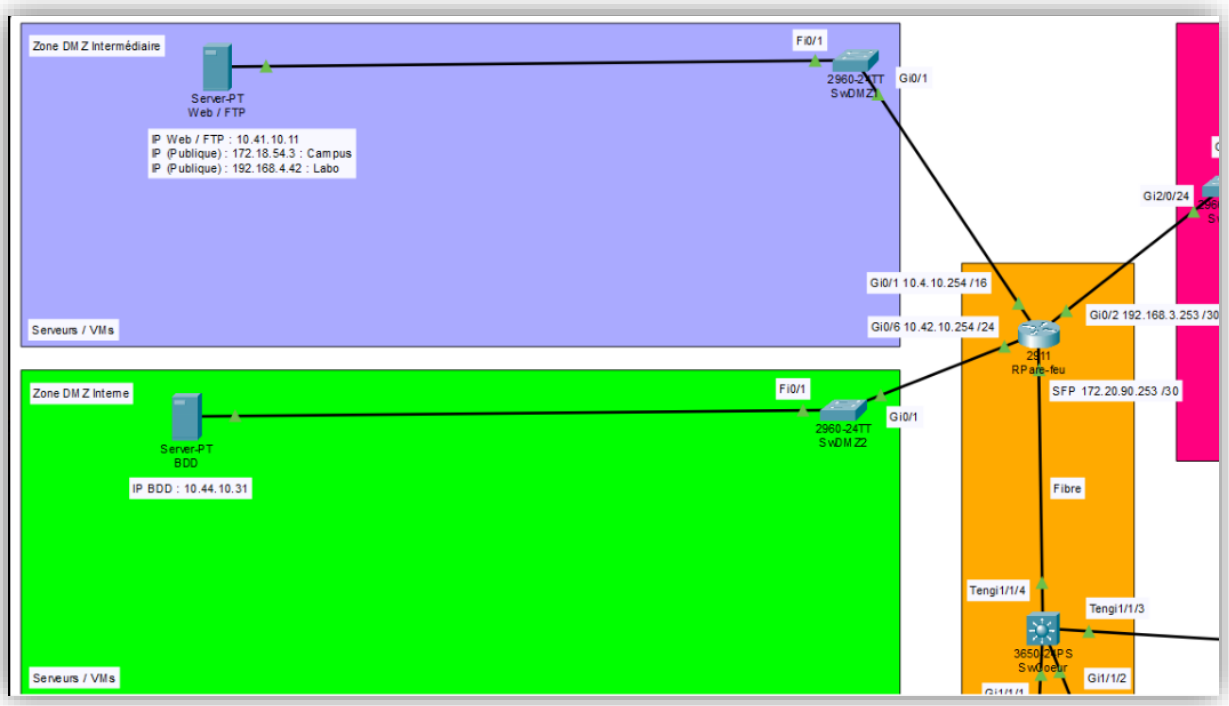
Création d'un GANTT afin de nous organiser, et un TRELLO afin de suivre de plus l'actualité des activités.





Activité 2.1 - Mise en place d'une nouvelle Zone DMZ :

L'objectif de cette AP autre que d'avoir un serveur WEB est de mettre en place une nouvelle ZONE DMZ dont une qui contiendra notre BDD et une qui contiendra notre FTPS / Serveur WEB, soit nous aurons une installation de ce Type pour notre infrastructure côté DMZ :



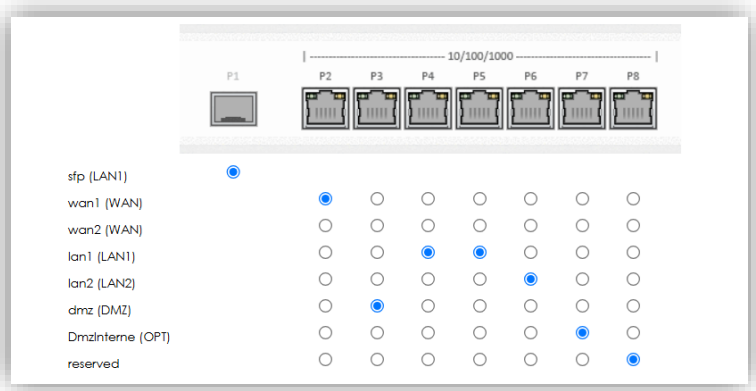
Soit, le nouvelle adressage IP sera celui-ci :

BDD -> 10.42.10.31
Serveur WEB / FTPS -> 10.41.10.11 avec un nat Statique en 192.168.4.46 côtés LAB et 172.18.54.3 côtés Campus
Interface Pare Feu vers DMZIntermédiaire -> 10.41.10.254
Interface DMZIntermédiaire vers pare Feu -> 10.41.10.253
Interface Pare Feu vers DMZInterne -> 10.42.10.254
Interface DMZInterne vers Pare Feu -> 10.42.10.253

Ensuite nous avons l'application en Deux Zone dmz sur le Pare Feu soit comme ceci :



Voici pour les Interface et voici pour les Ports :



Ensuite nous allons configurer le nouveau Switch soit hors adresse IP le SSH et La Sauvegarde Automatique vers le Serveur TFTP (172.20.100.4). Pour le SSH voici les commandes :

Configure Terminal

hostname SWDMZI

ip domain-name presbois.local

username admin privilege 15 secret Admin123

enable secret Admin123 (Passer en enable)

crypto key generate rsa modulus 2048

banner motd #

-------Nouvelle Session SSH -------

\#

line vty 0 15

login local

transport input ssh

exit

Et pour la sauvegarde Automatique nous faisons ces commandes :

kron policy list SAUVEGARDE

cli write

cli copy running-config tftp://172.20.100.4/swdmz2

Et nous mettons des « occurrence » permettant de répéter la sauvegarde à des moments données :

```
kron occurrence SAUVEGARDEM at 17:30 Tue recurring
 policy-list SAUVEGARDE
!
kron occurrence SAUVEGARDEJ at 17:30 Thu recurring
 policy-list SAUVEGARDE
!
kron occurrence SAUVEGARDEV at 12:30 Fri recurring
 policy-list SAUVEGARDE
```

Ensuite nous allons nous occuper des règles de Pare Feu pour autoriser la communication entre les deux service soit Service WEB et le Service BDD et la communication sur le port 3306 pour les relier soit nous allons créer premièrement une ip statique sur le Pare feu soit :

12	bddftpsHyperV	SUBNET	10.42.10.0/24
14	web1	HOST	10.41.10.11

Et pour les règles de Pare feu premièrement le port 3306 puis la communication :

14	BDDWEBTCP	DMZ	OPT	web1	bddftps...	BDDWEB...	any	an
15	DMZ_to_WAN	DMZ	WAN	any	any	any		an
16	BDDFTPSWAN	OPT	WAN	any	any	MES		an
17	SSHDENY	any	any (Excl...	any	any	SSH		an
18	BDDDD	DMZ	any (Excl...	web1	bddftps...	MES		an

BDDWEBTCP

IP Protocol: TCP
Starting Port: 3306
Ending Port: 3306
Reference: 1

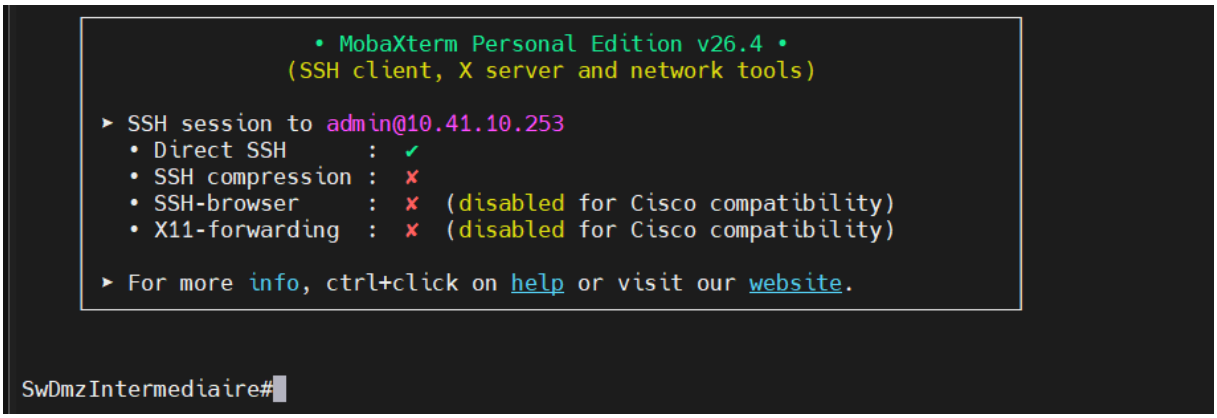
18		BDDDD	DMZ	any (Excl...	web1	bddftps...	MESUR
19		LANVERSINTERNET	any	WAN	any	any	MESUR
20		IPSec_VPN_Out...	IPSec_VPN	any (Excl...	any	any	any
21		SSL VPN Outgoi	SSL VPN	any (Excl	any	any	any

Description:

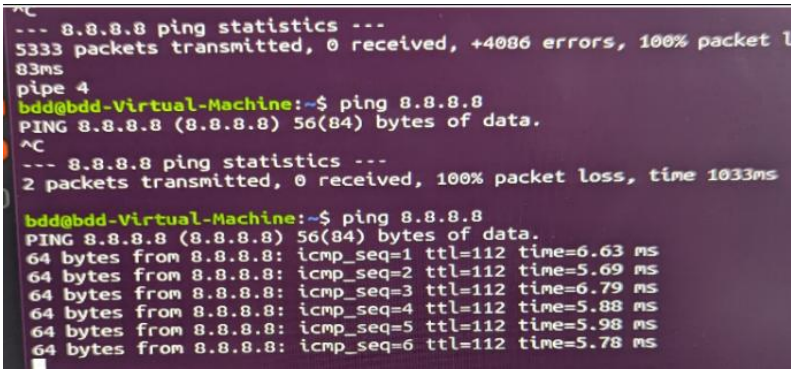
Members:

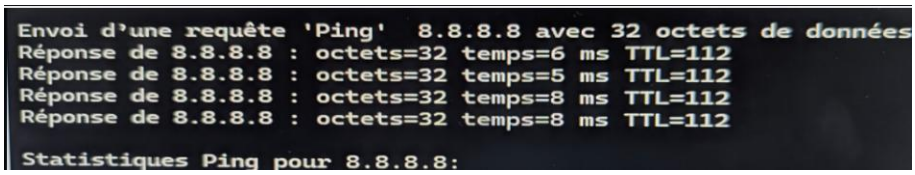
Name	Content
HTTP	TCP 80-80
PING	ICMP 8-8

Et comme nous pouvons le voir, le SSH marche :



Et voici pour les pings :





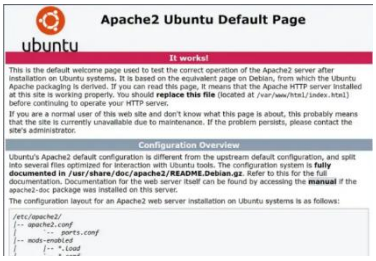
Et nous vérifierons le port 3306 juste après.

Activité 2.2 – Installation des Service BDD/FTPS/Web :

Nous allons commencer par l'installation du Service WEB :

- Sudo apt update
- Sudo apt install apache2 -y
- Sudo systemctl status apache2

Et nous allons le configurer juste après mais si nous mettons l'adresse IP soit 10.41.10.11 nous tombons sur la page de base d'apache 2 :



Ensuite nous allons installer le service BDD sur le serveur BDD :

- *sudo apt install mariadb-server -y*
- *sudo systemctl status mariadb*

Ensuite nous allons installer le service FTPS :

- *sudo apt install vsftpd -y*
- *sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem*
- *sudo nano /etc/vsftpd.conf*

Et ce qui est obligé à mettre c'est dans ce fameux fichier vsftpd.conf le :

- *local_enable = Yes*
- *write_enable = Yes*

Puis nous allons faire un :

- *sudo systemctl restart vsftpd*
- *sudo systemctl enable vsftpd*

Voici pour l'installaton des Services.

Activité 3 – Paramétrage de l'accès entrant vers les ressources :

Pour relier le serveur Web et le BDD nous allons utiliser PHPmyadmin et nous allons l'installer avec ces commandes :

- sudo apt install phpmyadmin php-mbstring php-zip php-gd php-json php-curl -y

Pendant l'installation, une fenêtre bleue de configuration apparaît dans le terminal :

1. Utilise les flèches pour sélectionner **apache2**
2. Valide avec **Entrée**.
3. Lorsque l'assistant demande s'il faut configurer la base de données avec dbconfig-common, choisissez **Oui** (Yes) et saisissez le mot de passe root(Utilisateur Dev que nous allons créer donc faite cette tache après la création du compte développeur BDD de notre base de données (ou laisse-le générer un mot de passe automatique). *Verification:* L'installation se poursuit et s'achève avec succès après la configuration de la base

Et pour terminer nous allons mettre ces commandes :

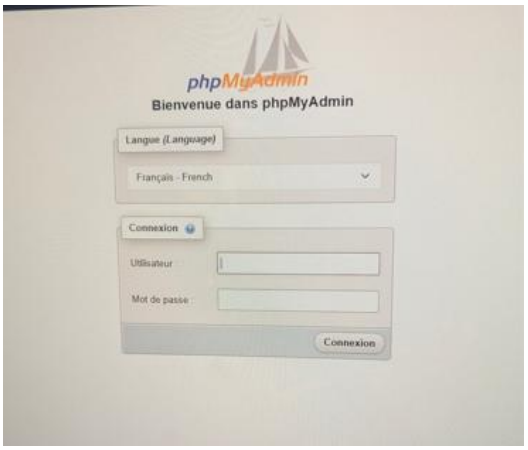
- sudo phpenmod mbstring
- sudo systemctl restart apache2

Et notre PHPmyadmin est opérationnel (le port 3306 est utilisé pour cette liaison).

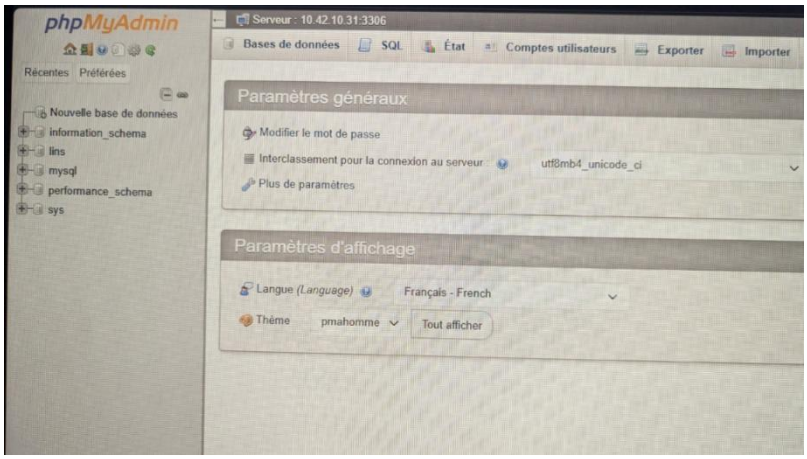
Ensuite nous allons créer le compte BDD soit :

- sudo mariadb
- CREATE USER 'PRESBOISALMA'@'10.41.10.11' IDENTIFIED BY 'Admin123';
- GRANT ALL PRIVILEGES ON nom_de_la_base.* TO 'PRESBOISALMA'@'Admin123';
- FLUSH PRIVILEGES;

Et pour verifier nous faisons 10.41.10.11\phpmyadmin et nous tombons sur cette page :



Puis après connexion nous tombons sur cette page :



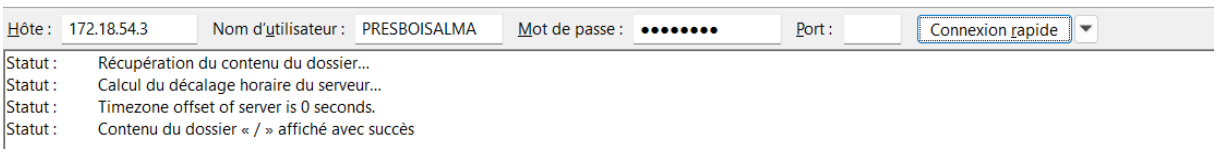
Ensuite nous allons créer le nom d'utilisateur pour le vsftpd soit :

- *sudo adduser PRESBOISALMA*
- *sudo passwd PRESBOISALMA puis Admin123*
- *sudo usermod -d /var/www/html PRESBOISALMA*
- *sudo chown -R mon_user_ftp:www-data /var/www/html*
- *sudo chmod -R 775 /var/www/html*

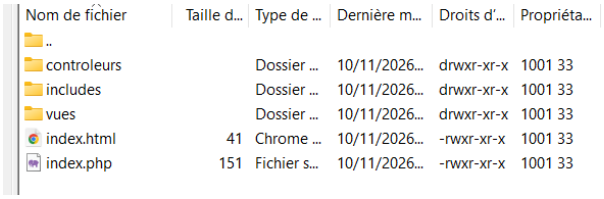
Pour bloquer l'utilisateur dans un dossier donné soit HTML dans notre cas vous allez dans votre vsftpd.conf vous mettez/décommenter ceci :

- *chroot_local_user=YES*
- *allow_writeable_chroot=YES*

Et quand nous essayons avec Filezilla client , nous voyons premièrement pour nous connecter c'est en fonction d'où vous êtes si nous prenons depuis le campus vous mettez 172.18.54.3 et nous voyons que ça marche :



Puis nous avons accès à ces dossiers :



Et si nous essayons d'y sortir nous avons cette erreur :

```
Réponse :    550 Failed to change directory.
Erreur :     Impossible de récupérer le contenu du dossier
```

Notre utilisateur est donc bien configurer , nous avons accès au FTP et si nous tapons l'adresse IP soit 172.18.54.3 nous avons accès au serveur WEB

Et donc nous avons fait un document qui contient toutes les informations pour nos développeurs :



Document de communication équipe développeurs

Contexte : PRESBOIS

Connexion au site :

- url du site web : www.presbois.com
- IP du site Web : 10.41.10.11
- Identifiant /mot de passe interface administration (à remplir par les développeurs) :

Connexion ftp :

- IP du serveur FTP : 10.41.10.11
- Identifiant / mot de passe : Identifiant : PRESBOISALMA et MDP : Admin123

Connexion au serveur de base de données :

- IP du serveur de base de données : 10.42.10.31
- Identifiant / mot de passe : PRESBOISALMA et Admin123

Activité 4 – Sécurisation du Serveur WEB :

Nous sommes sur un Site Externe servant au commerce donc nous avons premièrement besoin d'une autorité de certification Publique et non auto-signé. Soit nous allons faire ce processus pour sécuriser :

Nous allons utiliser **Let's Encrypt** (via l'outil **Certbot** sur ton serveur Apache). qui est une autorité de certification publique cohérente avec notre site qui est un site externe commercial.

Ensuite nous allons sur la VM Serveur WEB et nous allons taper ces commandes :

- sudo apt install -y certbot python3-certbot-apache

Nous rappelons adresse IP côtés campus -> 172.18.54.3 et côtés LAB -> 192.168.4.46

Ensuite nous allons aller sur DUCKDNS et nous allons publier un nom de domaine soit pour notre contexte ce sera celui-ci :



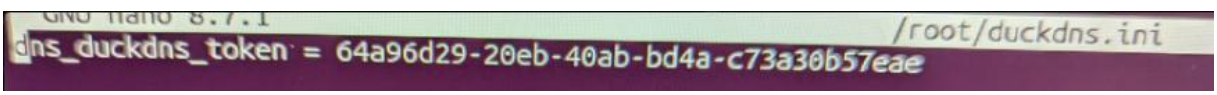
Ensuite nous allons repartir sur la VMServeur WEB et nous allons installer DuckDNS sur le serveur web soit avec la commande suivante :

- apt install python3-venv

Et ensuite nous allons aller dans le fichier de configuration de duckdns soit

- nano /root/duckdns.ini

Ensuite nous allons modifier l'intérieur pour y mettre notre token et ceci :



Ensuite nous allons faire la commande suivante :

- a2enmod ssl

Pour annoncer à apache2 que nous utilisons le mode ssl
Ensuite nous allons générer notre certificat soit avec cette commande :

```
root@web-Virtual-Machine:/etc/letsencrypt/live# sudo /opt/certbot-duckdns/bin/certbot certonly --authenticator dns-duc
kdns --dns-duckdns-credentials /root/duckdns.ini --dns-duckdns-propagation-second 60 -d www.presbois.duckdns.org
```

On devrait voir un “Succès” apparaître après cette commande.

Et commande nous allons vérifier les certificats avec cette commande :

- cd /etc/letsencrypt/live puis ls -l

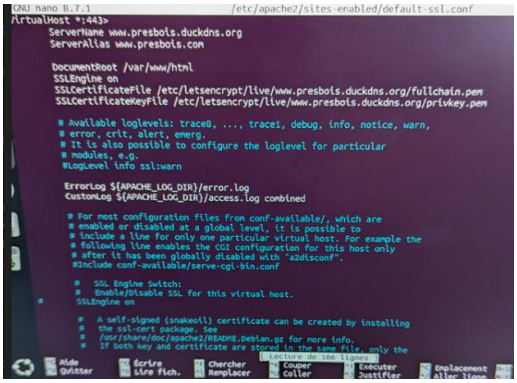
Nous devrions obtenir ceci :

```
-Virtual-Machine:/etc/letsencrypt/live# ls -l

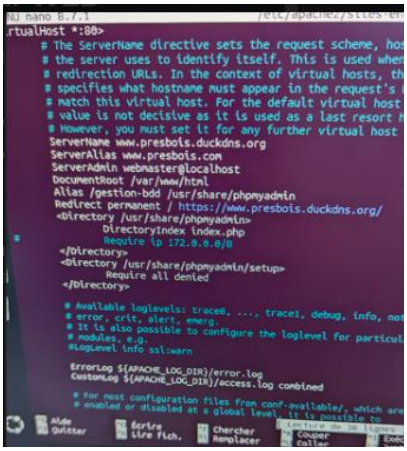
--- 1 root root  740 Nov 12 17:07 README
r-x 2 root root 4096 Nov 12 17:07 presbois.duckdns.org
xr-x 2 root root 4096 Nov 13 09:17 www.presbois.duckdns.org
eb-Virtual-Machine:/etc/letsencrypt/live#
```

Ensuite nous allons ouvrir nos fichiers de configurations soit 000-default.conf et default-ssl.conf et nous allons y mettre ces informations :

Default-SSL.conf :



000-default.conf :



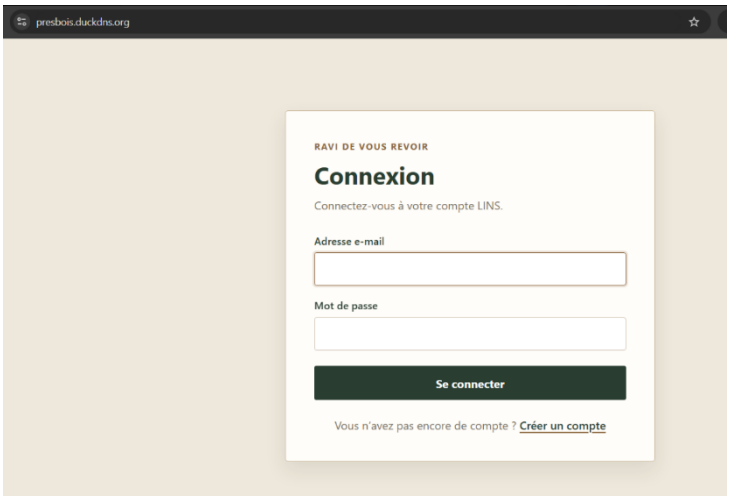
Après ceci nous faisons deux commandes soit :

- apache2ctl configtest (Pour voir les eventuels erreurs de syntaxe)

Puis :

- systemctl restart apache2

Et quand nous allons voir le site désormais peut importe si vous marquez “presbois.com” ou “https://www.presbois.duckdns.org” vous tomberez sur ceci :



Et voici , nous avons sécurisé notre site internet.

Activité 5 – Installation du Serveur DNS dans la DMZ :

Nous allons installer Bind9 si on ne l’a pas déjà avec ces commandes :

- sudo apt update
- sudo apt install bind9 bind9utils bind9-doc -y

Ensuite nous allons dedans et nous allons créer un fichier pour chaque nom de domaine dans notre cas

- sudo nano /etc/bind/db.presbois.duckdns.org

Et nous allons le remplir ici :

Fichier 1 : /etc/bind/db.presbois.duckdns.org

$TTL 6040800
@ IN SOA ns1.presbois.duckdns.org. admin.presbois.duckdns.org. (
1
6040800
86400
2419200
6040800)

@ IN NS ns1.presbois.duckdns.org.
ns1 IN A 10.41.10.11
www IN A 10.41.10.11

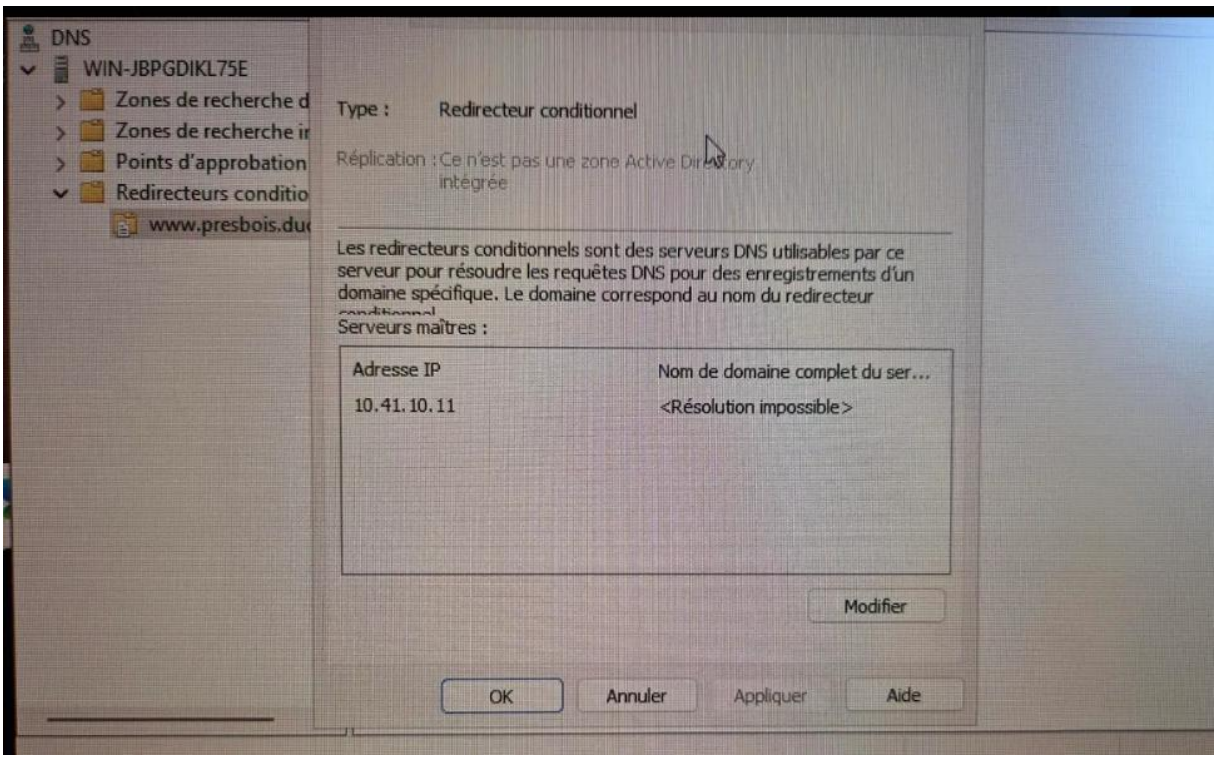
Puis pour le Fichier 2 :

Fichier 2 : /etc/bind/db.presbois.com

$TTL 6040800
@ IN SOA ns1.presbois.com. admin.presbois.com. (
1 ; Serial
6040800 ; Refresh
86400 ; Retry
2419200 ; Expire
4800) ; Negatif cache TTL

@ IN NS ns1.presbois.com.
ns1 IN A 10.41.10.11
www IN A 10.41.10.11

Ensuite nous allons faire une redirection vers www.presbois.duckdns.org dans l'active Directory soit ici :



Et voici nous avons accès à notre site depuis le LAN et depuis le WAN des deux réseaux.

Et voici nous avons Terminé l'AP.