

Documentation Technique

Installation et automatisation d'un Wordpress

(Projet AP portfolio)

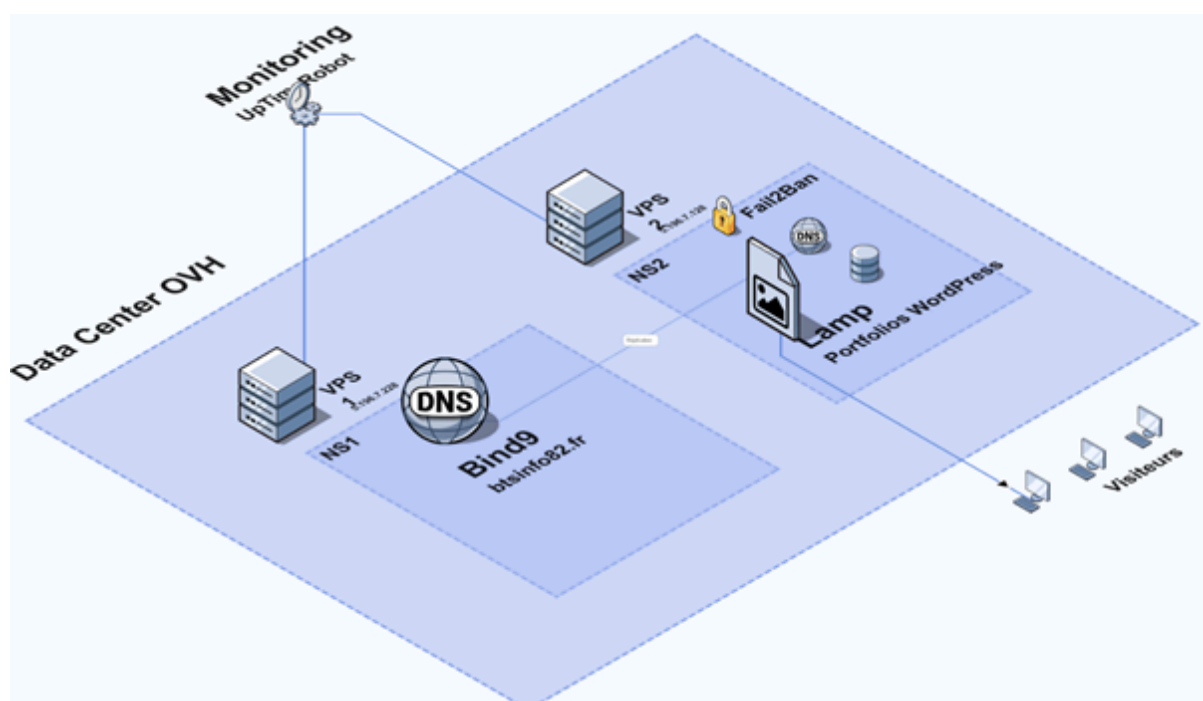


A. Présentation du projet

Le projet à pour but de créer des portfolios pour les élèves de BTS SIO mais pour y parvenir il fallait faire toute l'infrastructure

Du Serveur jusqu'à la connexion partout dans le monde au portfolio

Donc voici le schéma qu'on à créé pour bien expliquer tous les objectifs



Maintenant que l'objectif est présenté nous allons passer vous expliquer chaque étape qui nous à permit d'atteindre ceci

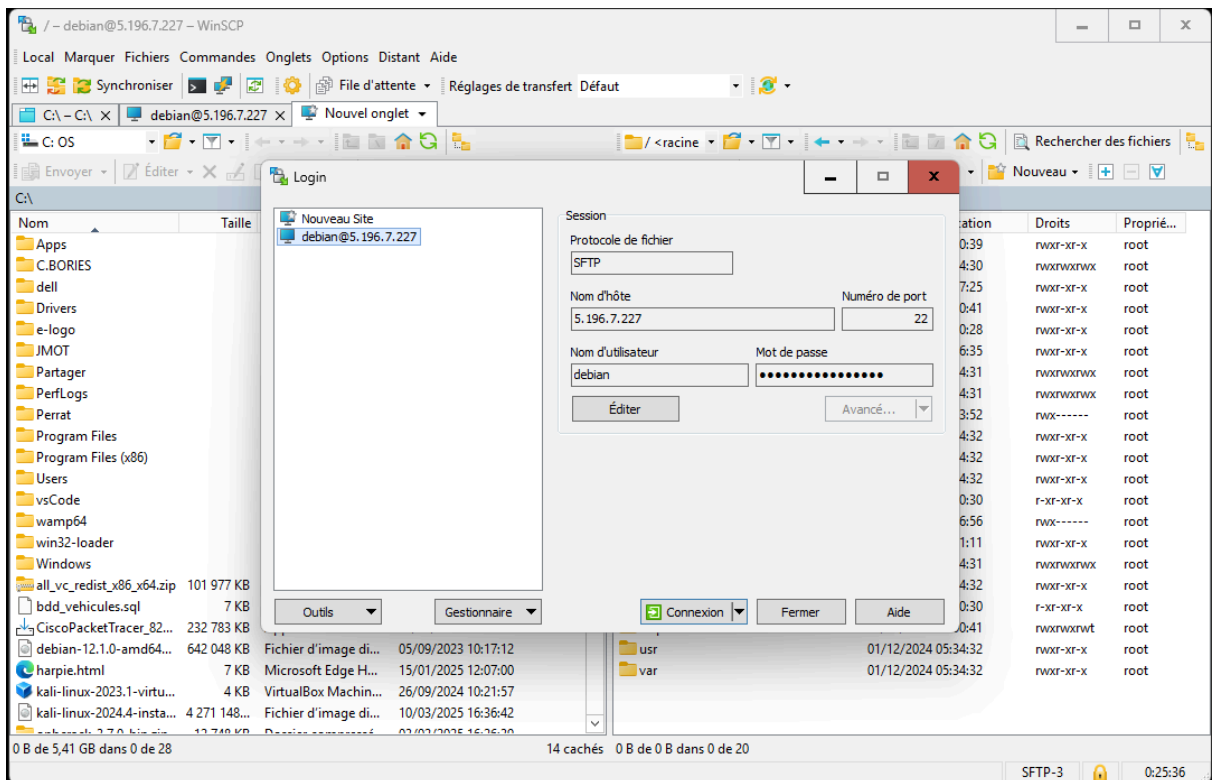
Chapitre n°1: Installation DNS

Tout d'abord nous avons fait appel à hostinger afin de nous fournir des serveurs virtuels pour que l'on puisse travailler dessus

Les serveurs étaient intégrés à un serveur DNS donc nous n'avons plus qu'à juste nous connecter pour commencer

/-> pour avoir tous les dossiers (WinSCP)

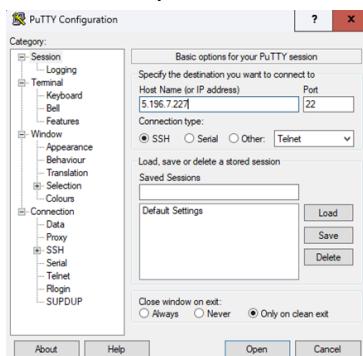
Connexion sur WinSCP :



Cliquez sur cette icône pour y accéder par PUTTY

/-> Maintenant vous devriez être dans le terminal de votre serveur

Sinon vous pouvez utiliser PUTTY



→ Cliquez sur "open"

Installation BIND9 :

```
sudo apt-get update  
sudo apt-get install bind9 dnsutils
```

systemctl status bind9 vérifier si l'install fonctionne.

cp -R /etc/bind{,.save} sauvegarder le fichier Bind en cas de mauvaise manip.

Configuration de la Zone:

Pour créer la zone nous devons éditer le fichier de configuration

```
sudo nano /etc/bind/named.conf.local
```

/-> C'est la commande pour y accéder

Une fois dans le fichier des paramètres ajouter en bas les lignes

/-> Ajouter un fichier **zones** et mettre db.**btsinfo82.fr** dedans

```
zone "btsinfo82.fr" {  
    type master;  
    file "/etc/bind/zones/db.btsinfo82.fr";  
    allow-update { none; };  
};
```

Maintenant que ça est fait nous devons récupérer le fichier nommé **"db.local"** pour l'utiliser pour base

```
sudo cp /etc/bind/db.local/etc/bind/zones/db.btsinfo82.fr
```

Maintenant on peut aller modifier le fichier de zone et créer les premiers enregistrement DNS

En premier on ouvre le fichier de zone

```
sudo nano /etc/bind/zones/db.btsinfo82.fr
```

Nous déclarons également la zone avec l'adresse IP du serveur DNS, à savoir "5.196.7.227".

A chaque fois que le fichier de zone est modifier le numéro de **"Serial"** doit être augmenter de +1

Ne pas oublier de changer le DNS dans sa configuration sur un ordinateur afin de pouvoir y accéder (Dans Windows / Paramètre / Réseau et Internet / Attribution du serveur DNS)

Création d'hôtes:

Ouvrir la doc DNS

```
sudo nano /etc/bind/zones/db.btsinfo82.fr
```

puis on ajoute la nomenclature avec l'adresse ip de ns2. Eet penser à incrémenter le Serial

```
GNU nano 7.2 /etc/bind/zones/db.btsinfo82.fr *
        604800      ; Refresh
        86400      ; Retry
        2419200    ; Expire
        604800 )    ; Negative Cache TTL

;Name Servers:
@      IN      NS      ns1.btsinfo82.fr.
@      IN      NS      ns2.btsinfo82.fr.

;Record for name servers:
ns1     IN      A       5.196.7.227
ns2     IN      A       5.196.7.128

;Others records:
www     IN      CNAME    btsinfo82.fr.
@       IN      A        5.196.7.128
dorsainvils  IN      A        5.196.7.128
moinec  IN      A        5.196.7.128
cremouxm  IN      A        5.196.7.128
pione   IN      A        5.196.7.128

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

Une fois cela fait on reload Bind9

```
sudo systemctl reload bind9
```

Reverse:

On doit d'abord commencer par éditer le fichier "named.conf.local"

```
sudo nano /etc/bind/named.conf.local
```

Ensuite dans le fichier on déclare la zone inversée

```
zone "227.7.196.5.in-addr.arpa" {
    type master;
    file "/etc/bind/zones/db.reverse.btsinfo82.fr";
    allow-update { none; };
};
```

Copiez le fichier de la zone "btsinfo82.fr" pour l'utiliser comme base. Le fichier de la zone inverse sera "db.reverse.btsinfo82.fr". Puis, éditez ce fichier.

```
sudo cp/etc/bind/db.btsinfo82.fr/etc/bind/db.reverse.btsinfo82.fr
sudo nano /etc/bind/db.reverse.btsinfo82.fr
```

Une fois dans le fichier voici comment doit être remplie le fichier (Avec vos infos à vous)

```
;
; BIND data file for reverse btsinfo82.fr
;
$TTL 604800
@      IN      SOA      ns1.btsinfo82.fr. contact.btsinfo82.fr. (
                                1          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
;Name Servers:
@      IN      NS       ns1.btsinfo82.fr.

;PTR records:
5.196.7.227 IN    PTR    ns1.btsinfo82.fr.
5.196.7.128 IN    PTR    ns2.btsinfo82.fr.
```

Une fois terminé enregistré, vérifié si ce que vous avez fait fonctionne en utilisant cette commande

```
named-checkzone 227.7.196.5.in-addr.arpa /etc/bind/zones/db.reverse.btsinfo.fr
```

Si vous obtenez une réponse comme ça c'est que cela fonctionne

```
named-checkzone 227.7.196.5.in-addr.arpa/etc/bind/zones/db.reverse.btsinfo82.fr
zone 227.7.196.5.in-addr.arpa/IN: loaded serial 1
OK
```

Ensuite redémarré les services de bind9

```
sudo systemctl restart bind9
```

GLUE:



Zone DNS

Serveurs DNS

Redirection

DynHost

GLUE

Personnalisez ici vos serveurs DNS avec votre nom de domaine afin qu'ils s'affichent dans les bases WHOIS.

Vous pouvez créer vos propres serveurs DNS en IPv4.

Hôte	Cible(s)	
ns2.btsinfo82.fr	["5.196.7.128"]	
ns1.btsinfo82.fr	["5.196.7.227"]	

25 sur 2 résultats



/-> C'est super si vous avez ceci c'est que tout fonctionne parfaitement

Maintenant nous allons passer à autre chose

Chapitre n°2: Installation Lamp

APACHE :

Comme à chaque fois on commence par faire:

```
sudo apt update
sudo apt upgrade -y
```

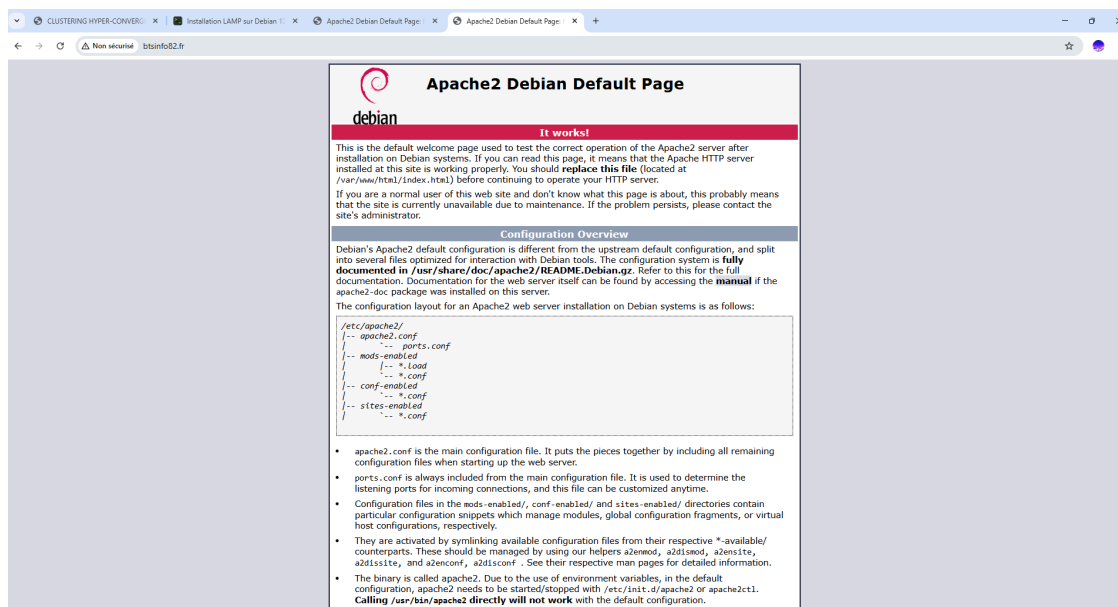
Ensuite on installe apache sur votre serveur Linux

```
sudo apt-get install apache2 -y
```

On peut vérifier que apache ce soit bien installé

```
systemctl status apache2
```

Taper ensuite l'adresse sur une page web si tout est bien installé cette page devrait s'afficher (c'est la page de base d'un apache fonctionnel)



MARIA DB:

On commence par installer mariadb grâce à cette commande

```
sudo apt-get install mariadb-server -y
```

On peut ensuite l'exécuter en faisant On doit configurer un mot de passe pour y accéder

```
sudo systemctl start mariadb  
sudo mysql_secure_installation
```

Suivez les instructions à l'écran et choisissez-y pour toutes les options proposées.

Maintenant on peut utiliser cette commande pour y accéder

```
sudo mysql -u root -p
```



PHP :

Pour installer PHP on doit utiliser la commande

```
sudo apt-get install php
```

On peut vérifier si PHP c'est bien installer

```
echo "<?php phpinfo(); ?>" | sudo tee /var/www/html/info.php
```

PHP Version 8.2.28		
System	Linux ns2.btsinfo82.fr 6.1.0-32-cloud-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.129-1 (2025-03-06)	
Build Date	Mar 13 2025 18:21:38	
Build System	Linux	
Server API	Apache 2.0 Handler	
Virtual Directory Support	disabled	
Configuration File (php.ini) Path	/etc/php/8.2/apache2	
Loaded Configuration File	/etc/php/8.2/apache2/php.ini	
Scan this dir for additional .ini files	/etc/php/8.2/apache2/conf.d	
Additional .ini files parsed	/etc/php/8.2/apache2/conf.d/10-opcache.ini, /etc/php/8.2/apache2/conf.d/10-pdo.ini, /etc/php/8.2/apache2/conf.d/20-calendar.ini, /etc/php/8.2/apache2/conf.d/20-type.ini, /etc/php/8.2/apache2/conf.d/20-xml.ini, /etc/php/8.2/apache2/conf.d/20-ffi.ini, /etc/php/8.2/apache2/conf.d/20-fileinfo.ini, /etc/php/8.2/apache2/conf.d/20-ftp.ini, /etc/php/8.2/apache2/conf.d/20-gettext.ini, /etc/php/8.2/apache2/conf.d/20-iconv.ini, /etc/php/8.2/apache2/conf.d/20-ldap.ini, /etc/php/8.2/apache2/conf.d/20-mbstring.ini, /etc/php/8.2/apache2/conf.d/20-mysqlnd.ini, /etc/php/8.2/apache2/conf.d/20-openssl.ini, /etc/php/8.2/apache2/conf.d/20-readline.ini, /etc/php/8.2/apache2/conf.d/20-shmop.ini, /etc/php/8.2/apache2/conf.d/20-sockets.ini, /etc/php/8.2/apache2/conf.d/20-sysvmsg.ini, /etc/php/8.2/apache2/conf.d/20-sysvsem.ini, /etc/php/8.2/apache2/conf.d/20-sysvshm.ini, /etc/php/8.2/apache2/conf.d/20-tokenizer.ini	
PHP API	20220829	
PHP Extension	20220829	
Zend Extension	420220829	
Zend Extension Build	API420220829.NTS	
PHP Extension Build	API20220829.NTS	
Debug Build	no	
Thread Safety	disabled	
Zend Signal Handling	enabled	
Zend Memory Manager	enabled	
Zend Multibyte Support	disabled	
Zend Max Execution Timers	disabled	
IPv6 Support	enabled	
DTrace Support	available, disabled	
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar	
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3	
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, convert.*, consumed, dechunk, convert.iconv.*	
This program makes use of the Zend Scripting Language Engine: Zend Engine v4.2.28, Copyright (c) Zend Technologies with Zend OPcache v8.2.28, Copyright (c), by Zend Technologies		

Accédez ensuite à ce fichier via votre navigateur à l'adresse <http://btsinfo82.fr/info.php>. Vous devriez voir une page avec des informations sur PHP.

Dans notre cas:

<http://192.168.0.242/info.php>

Chapitre n°3 : Installation Wordpress :

Étape 1 : Préparation de la Base de Données pour WordPress

On commence par créer la base de données

```
sudo mysql -u root -p  
  
CREATE DATABASE Nom_de_la_base;
```

Maintenant on peut commencer à créer un utilisateur

```
CREATE USER 'Nom_de_l'utilisateur'@'localhost' IDENTIFIED BY  
'MDP';
```

On peut accorder les privilèges :

```
GRANT ALL PRIVILEGES ON Nom_de_la_base.* TO  
'Nom_de_l'utilisateur'@'localhost';
```

Appliquer les modifications :

```
FLUSH PRIVILEGES;
```

Maintenant vous pouvez quitter mysql

```
EXIT;
```

Étape 2 : Télécharger et Configurer WordPress

Maintenant que ça est fait déplacer vous dans le répertoire par défaut de APACHE, là où les fichier de votre site seront stockés

```
cd /home/debian
```

Télécharger WordPress : Utiliser *wget* pour télécharger la dernière version de WordPress depuis le site officiel :

```
sudo wget https://wordpress.org/latest.tar.gz
```

Extraire le fichier :

```
sudo tar -xzf latest.tar.gz
```

Créer le dossier pour pouvoir le déplacer :

```
sudo mkdir /var/www/nom.btsinfo82.fr  
sudo cp -r wordpress/* /var/www/nom.btsinfo82.fr  
sudo chown -R www-data:www-data /var/www/nom.btsinfo82.fr  
sudo chmod -R 755 /var/www/nom.btsinfo82.fr
```

Déplacer les fichiers de WordPress : Déplacez tous les fichiers du dossier wordpress dans le répertoire racine /var/www/html

```
sudo cp -r wordpress/* /var/www/nom.btsinfo82.fr
```

Changer les permissions des fichiers : Assurez-vous qu'Apache possède les permissions nécessaires pour accéder aux fichiers :

```
sudo chown -R www-data:www-data /var/www/nom.btsinfo82.fr  
sudo chmod -R 755 /var/www/nom.btsinfo82.fr
```

Étape 3 : Configurer un virtualhost

```
cd /etc/apache2/sites-available
```

On crée un fichier de configuration nom. btsinfo82.fr.conf

```
<VirtualHost *:80>
    ServerName moinec.btsinfo82.fr
    DocumentRoot /var/www/nom.btsinfo82.fr
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
    RewriteEngine on
    RewriteCond %{SERVER_NAME} =nom.btsinfo82.fr
    RewriteRule ^ https://%{SERVER_NAME}%{REQUEST_URI}
    [END,NE,R=permanent]
</VirtualHost>
```

On active le site .

```
sudo a2ensite nom.btsinfo82.fr.conf
```

On redémarre apache

```
sudo systemctl restart apache2
```

Etape 4 : Activation du HTTPS

bonjour, vous venez de mettre en place votre virtualhost et nous allons mettre en place le https grâce à

Certbot est un client utilisé pour demander un certificat à partir de Let's Encrypt(association qui fournit des certificats gratuits) et le déployer sur un serveur Web.

Sécurisation https:

```
sudo apt install certbot python3-certbot-apache
```

```
sudo certbot --apache
```

(Entrez son e-mail pour possible expiration de son certificat).

```
sudo apache2ctl configtest  
sudo systemctl reload apache2
```

```
sudo certbot renew --dry-run
```

connexion wordpress nomdedomain.fr/wp-admin

wordpress: plugin/extension: install wordfence , updraftplus

il faut configurer le firewall de wordfence pour assurer au maximum la sécurité.

Etape 5 : Finaliser l'installation via l'interface web

Accéder à l'interface d'installation de WordPress : Ouvrez votre navigateur et accédez à

```
http://nom.btsinfo82.fr
```

Maintenant vous devriez arriver sur une page fonctionnel de WORDPRESS

Remplir les informations de base :

- Titre du site.
- Nom d'utilisateur (pour accéder au tableau de bord de WordPress).
- Mot de passe.
- Adresse e-mail.



Vous devez saisir ci-dessous les détails de connexion à votre base de données. Si vous ne les connaissez pas, contactez votre hébergeur.

Nom de la base de données	<input type="text" value="wordpress"/>
Le nom de la base de données avec laquelle vous souhaitez utiliser WordPress.	
Identifiant	<input type="text" value="Identifiant"/>
Votre identifiant MySQL.	
Mot de passe	<input type="password" value="mot de passe"/> Afficher
Votre mot de passe de base de données.	
Adresse de la base de données	<input type="text" value="localhost"/>
Si localhost ne fonctionne pas, demandez cette information à l'hébergeur de votre site.	
Préfixe des tables	<input type="text" value="wp_"/>
Si vous souhaitez faire tourner plusieurs installations de WordPress sur une même base de données, modifiez ce réglage.	
<input type="button" value="Envoyer"/>	

Vous devez saisir ci-dessous les détails de connexion à votre base de données. Si vous ne les connaissez pas, contactez votre hébergeur.

Nom de la base de données	<input type="text" value="REDACTED"/>
Le nom de la base de données avec laquelle vous souhaitez utiliser WordPress.	
Identifiant	<input type="text" value="REDACTED"/>
Votre identifiant MySQL.	
Mot de passe	<input type="password" value="REDACTED"/> Afficher
Votre mot de passe de base de données.	
Adresse de la base de données	<input type="text" value="localhost"/>
Si localhost ne fonctionne pas, demandez cette information à l'hébergeur de votre site.	
Préfixe des tables	<input type="text" value="wp_"/>
Si vous souhaitez faire tourner plusieurs installations de WordPress sur une même base de données, modifiez ce réglage.	
<input type="button" value="Envoyer"/>	

Bienvenue

Bienvenue dans la très célèbre installation en 5 minutes de WordPress ! Vous n'avez qu'à remplir les informations demandées ci-dessous et vous serez prêt à utiliser la plus extensible et puissante plateforme de publication de contenu au monde.

Informations nécessaires

Veuillez renseigner les informations suivantes. Ne vous inquiétez pas, vous pourrez les modifier plus tard.

Titre du site

Identifiant

Les identifiants ne peuvent utiliser que des caractères alphanumériques, des espaces, des tirets bas ("_"), des traits d'union ("-"), des points et le symbole @.

Mot de passe

 Afficher

Forte

Important : Vous aurez besoin de ce mot de passe pour vous connecter. Pensez à le stocker dans un lieu sûr.

Votre e-mail

Vérifiez bien cette adresse e-mail avant de continuer.

Visibilité par les
moteurs de
recherche

☐ Demander aux moteurs de recherche de ne pas indexer ce site

Certains moteurs de recherche peuvent décider de l'indexer malgré tout.

Installer WordPress

Lancer l'installation : Cliquez sur le bouton **Installer WordPress**.

Erreur lors de la connexion à la base de données

Cela signifie soit que l'identifiant ou le mot de passe dans votre fichier `wp-config.php` n'est pas correct, soit que le serveur de base de données à l'adresse `5.196.7.128` ne peut pas être contacté. Cela peut signifier que votre serveur de base de données ne fonctionne plus.

- Confirmez-vous utiliser le bon identifiant et le bon mot de passe ?
- Confirmez-vous avoir saisi le bon nom d'hôte (hostname) ?
- Confirmez-vous que le serveur de la base de données fonctionne ?

Si vous ne connaissez pas ces termes, vous devriez probablement contacter votre hébergeur. Si vous avez toujours besoin d'aide, vous pouvez toujours vous rendre sur les [forums d'entraide de WordPress](#).

Recommencer

Pour Changer le mot de passe quand cette erreur survient :

```
SET PASSWORD FOR 'user-name-here'@'localhost' =  
PASSWORD( 'new-password' );
```

Non sécurisé 5.196.7.128

Error establishing a database connection

Document Annexes :

Installé DNS :

/-> <https://www.it-connect.fr/dns-avec-bind-9/>

Installation WordPress :

/-> <https://oleks.ca/2024/09/30/installer-wordpress-sur-debian-12-avec-lamp/>

Installation LAMP :

/-> <https://oleks.ca/2024/09/28/installation-lamp-sur-debian-12/>

/-> <https://tutos-info.fr/wp-content/uploads/2023/08/TUTORIEL-INSTALLER-LAMP-SUR-DEBIAN-12.1.pdf>

Version :

/-> Linux : 6.14

/-> Apache : 2.4.63

/-> MariaDB : 11.7.1

/-> Php : 8.4.5

Adminer :

Outil pour utiliser une interface graphique pour les bases de données

Langue: Français ▼ MariaDB > Serveur > Créer une base de données Déconnexion

Adminer 5.2.0

Créer une base de données

BD: ▼

Requête SQL Importer Exporter

Access denied for user 'a264133admin'@'localhost' to database 'DB_dorsainvils' 09/29/24 Requête SQL

DB_dorsainvils utf8_general_ci Enregistrer +

Template du mail pour les accès

Nous avons fait un template qui s'envoie pour le déploiement de Wordpress avec tout les information important pour qu'il se connect

Objet : Accès à votre site WordPress


Bonjour [Prénom du client],

Comme convenu, voici vos identifiants pour accéder à votre site et à l'administration WordPress :

 **Adresse du site** : <https://.btsinfo82.fr>

 **Accès à l'administration** : <https://.btsinfo82.fr/wp-admin>

 **Nom d'utilisateur** : [adresse_mail]

 **Mot de passe** : [mot_de_passe]

Je vous conseille de modifier votre mot de passe dès votre première connexion pour plus de sécurité.

N'hésitez pas à me contacter si vous avez besoin d'assistance ou d'explications supplémentaires.

Bonne journée,
[Votre prénom]

Automatisation installation WordPress

Pour faciliter le déploiement de Wordpress pour des gens nous allons faire un script bash qui permet de tout automatiser, l'utilisateur aura juste à entrer les information qu'il veut pour que son Wordpress s'appelle d'une manière particulière ainsi que les tous ce qui est de la connection (utilisateur , mot de passe)

Donc voici toutes les étapes de ce qui nous à permit de le réaliser

lien/vidéo (it connect) pour script

<https://www.youtube.com/watch?v=gBCGeLjYBgQ>

<https://www.it-connect.fr/debuter-script-bash-linux/>

<https://www.hostinger.com/fr/tutoriels/script-bash>

<https://www.youtube.com/watch?v=0n0Ssc3dbll>

Etape 0 : Collecte d'information de l'utilisateur

Demander le nom, prénom et e-mail de l'utilisateur en script bash.

Mise en place de la nomenclature (nom et première lettre du prénom) des utilisateurs. Tout mettre en minuscule et sans accents

\$nom : nom

\$prenom : prénom

\$mail : e-mail

\$nomenclature : nomenclature

\$domaine : \$nomenclature.btsinfo82.fr

test et retour utilisateur.

```
#!/bin/bash

rep="n"

while [ "$rep" != "Y" ] && [ "$rep" != "y" ]; do
    read -p 'Nom: ' nom
    read -p 'Prenom: ' prenom
    read -p 'Mail: ' mail

    echo "Votre nom est $nom"
    echo "Votre prenom est $prenom"
    echo "Votre email est $mail"

    read -p 'Est-ce vrai? (Y/n) ' rep
done

nomenclature="${nom}${prenom:0:1}"
nomenclature=$(echo "$nomenclature" | tr '[:upper:]' '[:lower:]')
domaine= "${nomenclature}.btsinfo82.fr"
echo "Votre nomenclature est $nomenclature"
echo "Votre domaine est $domaine"
```

Etape 1 : DNS

Création d'un script bash pour ce SSH de NS2 à NS1 pour modifier le fichier de zone DNS.

après avoir créé une clef ssh

```
the key's randomart image is:
---[RSA 3072]-----+
|
|
o  ..  |
o ..oo. .. |
o .S == o...|
. + o++.* *oo|
o = o.=.+ *E|
o=.. =.o .+.|
o=++=...oo |
-----[SHA256]-----+
debian@ns2:~$ ssh-copy-id debian@5.196.7.227
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/debian/.ssh/id_rsa.pub"
The authenticity of host '5.196.7.227 (5.196.7.227)' can't be established.
D25519 key fingerprint is SHA256:CxS3u5i/oOucN8kIJ6VmJZF6I4LhPcT9BhWFY99Kf+Q.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
debian@5.196.7.227's password:

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'debian@5.196.7.227'"
and check to make sure that only the key(s) you wanted were added.
debian@ns2:~$
```

test et retour utilisateur.

```
#!/bin/bash

# --- CONFIGURATION ---
REMOTE_USER="debian"
REMOTE_HOST="ns1.btsinfo82.fr"
ZONE_FILE="/home/debian/adoutte/db.btsinfo82.fr"
ZONE_NAME="btsinfo82.fr"

# Enregistrement à ajouter

IP_ADDRESS="5.196.7.128"      # ex: 192.168.1.123

if [[ -z "$nomenclature" || -z "$IP_ADDRESS" ]]; then
    echo "Usage: $0 <hostname> <ip_address>"
    exit 1
fi

# --- SCRIPT ---
ssh ${REMOTE_USER}@${REMOTE_HOST} bash << EOF
# Début du script distant
set -e

# Sauvegarde du fichier de zone
cp ${ZONE_FILE} ${ZONE_FILE}.bak

# Incrémentation du serial
sed -i "/SOA/{n;s/[0-9]\\{1,\\}/$(date +%Y%m%d%H%M)/}" ${ZONE_FILE}

# Ajout de l'enregistrement A
echo "${nomenclature}      IN      A      ${IP_ADDRESS}" >> ${ZONE_FILE}

# Redémarrage Bind
sudo systemctl restart bind9

# Fin du script distant
EOF

echo "✅ Zone ${ZONE_NAME} mise à jour avec ${nomenclature} -> ${IP_ADDRESS}"

# --- Test de résolution DNS avec dig ---
for DNS_SERVER in 5.196.7.227 5.196.7.128 8.8.8.8; do
    echo "🔍 Test dig via le serveur DNS ${DNS_SERVER} pour ${domaine}:"
    dig +short @${DNS_SERVER} ${domaine}
done
```

Etape 2 : Bases de données

Création de bases de données + utilisateur + mdp :

```
$db = "DB_$nomenclature"
$db_user = "DBuser_$nomenclature"
$db_pass = ""

sudo systemctl start mariadb
sudo mysql -e "CREATE DATABASE $db;"
sudo mysql -e "CREATE USER '$db_user' IDENTIFIED BY '$db_pass';"
sudo mysql -e "GRANT ALL PRIVILEGES ON $db.* TO '$db_user'@'localhost';"
sudo mysql -e "FLUSH PRIVILEGES;"
```

MDP aléatoire :

/-> Appel d'une fonction pour générer des mots de passe

```
genererMotDePasse()
{
    local longueur=16
    tr -dc 'A-Za-z0-9!@#$$%^&*()_+~`|}{[]:;?><.,/-=' < /dev/urandom | head -c "$longueur"
    echo
}
```

test et retour utilisateur. (base de données + user)

```
sudo mysql -e SHOW DATABASES ;
sudo mysql -e SELECT USER FROM mysql.user ;
```

Etape 3 : Installation et config fichier WordPress

Installer la dernière version de WordPress :

- wget de la dernière version ;
- décompresser ;
- créer le dossier /var/www/\$domaine;
- déplacer le fichier WordPress dans /var/www/\$domaine ;
- effacer le fichier .zip
- donner les droits aux utilisateurs : chmod et chown

```
cd /home/debian
sudo wget https://wordpress.org/latest.tar.gz
sudo tar -xzf latest.tar.gz
```



```
sudo mkdir /var/www/$domaine
sudo cp -r wordpress/* /var/www/$domaine
sudo chown -R www-data:www-data /var/www/$domaine
sudo chmod -R 755 /var/www/$domaine
```

```
touch ~/ScriptinstallWP.sh
read -p "Entrez le nom de domaine (ex: monsite.com): " domaine
cd /home/debian
sudo wget https://wordpress.org/latest.tar.gz
sudo tar -xvzf latest.tar.gz
sudo mkdir -p /var/www/$domaine
sudo cp -r wordpress/* /var/www/$domaine
sudo chown -R www-data:www-data /var/www/$domaine
sudo chmod -R 755 /var/www/$domaine
echo "Installation de WordPress terminée pour le domaine : $domaine"
chmod +x ScriptinstallWP.sh
```

Etape 4 : VirtualHosts

Création d'un fichier de configuration (\$domaine.conf) dans le dossier
/etc/apache2/sites-available/ :

```
sudo touch $domaine.conf
sudo nano $domaine.conf
```

Configurer le virtualhost dans le fichier de configuration :

```
<VirtualHost *:80>
ServerName $domaine
DocumentRoot /var/www/$domaine
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined
RewriteEngine on
RewriteCond %{SERVER_NAME} =$domaine
RewriteRule ^ https://%{SERVER_NAME}%{REQUEST_URI} [END,NE,R=permanent]
</VirtualHost>
```

Activer le site :

```
sudo a2ensite $domaine.conf
```

Redémarrer apache :

```
sudo systemctl restart apache2
```

```
#!/bin/bash
cd /etc/apache2/sites-available/

sudo touch /etc/apache2/sites-available/$domaine.conf
echo "<VirtualHost *:80>
ServerName $domaine
DocumentRoot /var/www/$domaine
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined
RewriteEngine on
RewriteCond %{SERVER_NAME} =$domaine
RewriteRule ^ https://%{SERVER_NAME}%{REQUEST_URI} [END,NE,R=permanent]
</VirtualHost>" > /etc/apache2/sites-available/$domaine.conf

sudo a2ensite /etc/apache2/sites-available/$domaine.conf

sudo systemctl restart apache2
```

Etape 5 : HTTPS

```
sudo certbot --apache -d $domain -m $mail --agree-tos
--non-interactive
sudo certbot renew --dry-run
sudo systemctl restart apache2
```

Sécurité WordPress (contrer une attaque)

[illegible]

Ce code PHP est **hautement obfusqué**, ce qui est une technique utilisée pour **cacher l'intention réelle du code**, souvent dans un but **malveillant** (comme du code **malicieux** ou **webshell**).

```
find /var/www/ -type f -newermt "2025-05-07"
```

Pour vérifier deux fichiers entre eux :

/-> diff -u fichier 1 fichier 2

[Information optionnel]

Installation WSL :

Si vous avez des problèmes lors du lancement de votre wsl faite ceci :

\rightarrow

```
wsl.exe --install Debian
wsl.exe -d Debian
```

Début du script :

```
#!/bin/bash

cd /home/debian/

read -p "Entrez votre nom et votre initiale : " nomenclature
if [ -z "$nomenclature" ]; then
    echo "Vous devez saisir une nomenclature."
    exit 1
fi

domaine="${nomenclature}.btsinfo82.fr"
echo "Domaine : $domaine"

db="DB_${nomenclature}"
db_user="DBuser_${nomenclature}"
db_pass=$(openssl rand -base64 24)
echo "${db_pass}"

systemctl start mariadb
mysql -e "CREATE DATABASE ${db};"
mysql -e "CREATE USER '${db_user}'@'localhost' IDENTIFIED BY
'${db_pass}';"
mysql -e "GRANT ALL PRIVILEGES ON ${db}.* TO '${db_user}'@'localhost';"
mysql -e "FLUSH PRIVILEGES;"
mysql -e "SHOW DATABASES;"
mysql -e "SELECT USER FROM mysql.user;"

rm -f latest.tar.gz
while ! wget https://wordpress.org/latest.tar.gz; do
    echo "Nouvel essai dans 10 seconde..."
    sleep 10
done

tar -xzf latest.tar.gz
mkdir -p "/var/www/$domaine"
cp -r wordpress/* "/var/www/$domaine"
chown -R www-data:www-data "/var/www/$domaine"
chmod -R 755 "/var/www/$domaine"
rm -rf wordpress latest.tar.gz

cat <<EOF > "/etc/apache2/sites-available/$domaine.conf"
<VirtualHost *:80>
    ServerName $domaine
```

```

    DocumentRoot /var/www/$domaine
    ErrorLog \${APACHE_LOG_DIR}/error.log
    CustomLog \${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
EOF

a2enmod rewrite
a2ensite "$domaine.conf"
apache2ctl configtest && systemctl reload apache2

echo "Le site $domaine a été activé et WordPress installé."

```

Commande pour réparé

Cela permet de désactiver tout les site wordpress

```
/-> for site in *; do sudo a2dissite "$site"; done
```

Reprise sur incident :

```

cd /var/www

read -p "Entrez votre nom et votre initiale : " nomenclature
if [ -z "$nomenclature" ]; then
    echo "Vous devez saisir une nomenclature."
    exit 1
fi

sudo mkdir /var/www/${nomenclature}_backup
sudo mv /var/www/${nomenclature}.btsinfo82.fr/wp-config.php
/var/www/${nomenclature}_backup
sudo rm -r /var/www/${nomenclature}.btsinfo82.fr

sudo mkdir /var/www/${nomenclature}.btsinfo82.fr
sudo cp -r /home/debian/wordpress/* /var/www/${nomenclature}.btsinfo82.fr
sudo mv ${nomenclature}_backup/wp-config.php ${nomenclature}.btsinfo82.fr
sudo chown -R www-data:www-data /var/www/${nomenclature}.btsinfo82.fr
sudo chmod -R 755 /var/www/${nomenclature}.btsinfo82.fr

cd ${nomenclature}.btsinfo82.fr
sudo wp plugin install wordfence --activate --allow-root
sudo wp plugin install updraftplus --activate --allow-root

```

```
wp plugin auto-updates enable updraftplus
wp plugin auto-updates enable wordfence
sudo a2ensite ${nomenclature}.btsinfo82.fr.conf
sudo a2ensite ${nomenclature}.btsinfo82.fr-le-ssl.conf

sudo chown -R www-data:www-data /var/www/${nomenclature}.btsinfo82.fr
sudo chmod -R 755 /var/www/${nomenclature}.btsinfo82.fr

sudo systemctl reload apache2
```

Sécurisation après incident

Après l'incident survenu le 16 mai 2025 il est primordial de mettre en place une sécurité mais rajouter de la sécurité sur le serveur et non seulement l'extension Wordfence sur Wordpress

Deux solutions sont proposées:

- Fail2Ban

- AuditD

Installation Fail2Ban :

Installation Fail2Ban

```
sudo apt install -y fail2ban
```

Installation iptables

```
sudo apt install -y iptables
```

Création fichiers de conf

```
sudo cp /etc/fail2ban/jail.{conf,local}
```

Edition du fichier jail.local

```
sudo nano /etc/fail2ban/jail.local
```

Installation rsyslog

```
sudo apt install -y rsyslog
```

Dans la configuration de Fail2Ban changer la ligne backend

```
backend = systemd
```

Si vous voulez ignorer certains ip changer la ligne ignoreip(mettre des espaces entre chaque ip)

```
ignoreip = 127.0.0.1/8 :
```

Le temps du bannissement se gère dans la ligne bantime.

La durée pour comptabiliser le nombre de tentatives maximales avant de déclencher un ban dans la ligne findtime

Nombre de tentatives max dans la ligne maxretry.

Après ces modifications

```
sudo systemctl restart fail2ban.service
```

Vérifier le status

```
systemctl status fail2ban.service
```

Voir toutes les options disponibles

```
fail2ban-client -h
```

UnBan une adresse ip

```
sudo fail2ban-client set sshd unbanip [adresse ip]
```

Ban une adresse ip

```
sudo fail2ban-client set sshd banip [adresse ip]
```

source :

<https://slash-root.fr/fail2ban-installation-et-configuration/>

Sucuri VS WordFence

Nous allons comparer les différents plugin pour protéger notre wordpress

Sucuri	WordFence
Utilise un pare-feu d'application web (WAF) basé sur le cloud qui filtre le trafic avant qu'il n'atteigne votre serveur.	Offre un pare-feu basé sur le serveur qui fonctionne en installant le plugin directement sur votre site WordPress
Offre un service de nettoyage de malware professionnel sans frais supplémentaires avec certains plans, ce qui est un atout majeur pour les utilisateurs moins techniques.	Propose un scanner de malware puissant et des options de réparation de fichiers corrompus, mais le nettoyage manuel peut être requis.
N'a pas de version gratuite (sauf pour le scanner de site), et ses plans payants sont des abonnements qui incluent à la fois le WAF et les services de nettoyage de malware.	Propose une version gratuite robuste et une version premium avec des fonctionnalités supplémentaires.

Mettre à jour l'heure des serveurs

pour vérifier le statut des dates/heures des serveurs

```
timedatectl status
```

Pour avoir la liste de tous les time zone du monde (continents/pays)

```
timedatectl list-timezones
```


Et enfin pour sélectionner la time zone voulu

```
sudo timedatectl set-timezone Europe/Paris
```