**Documentation de la configuration du serveur pour gereboul.net**

**Informations générales**

* **Domaine** : gereboul.net et [www.gereboul.net](http://www.gereboul.net)
* **Serveur** : VPS Ubuntu
* **Application** : Next.js (port 3000)
* **Serveur web** : Apache

**Configuration actuelle**

**Architecture**

L'application Next.js fonctionne sur le port 3000. Apache agit comme proxy inverse, redirigeant le trafic HTTP vers HTTPS et transmettant les requêtes à l'application Next.js.

**Certificat SSL**

Un certificat SSL auto-signé est utilisé pour le chiffrement HTTPS. Les fichiers sont stockés dans :

* Certificat : /etc/ssl/gereboul/server.crt
* Clé privée : /etc/ssl/gereboul/server.key

**Configuration Apache**

Le fichier de configuration principal est /etc/apache2/sites-available/gereboul.conf :

apache

Copier

<VirtualHost \*:80>

ServerName gereboul.net

ServerAlias www.gereboul.net

# Rediriger vers HTTPS

RewriteEngine On

RewriteRule ^(.\*)$ https://%{HTTP\_HOST}$1 [R=301,L]

</VirtualHost>

<VirtualHost \*:443>

ServerName gereboul.net

ServerAlias www.gereboul.net

# SSL Configuration

SSLEngine on

SSLCertificateFile /etc/ssl/gereboul/server.crt

SSLCertificateKeyFile /etc/ssl/gereboul/server.key

# Logs

ErrorLog ${APACHE\_LOG\_DIR}/gereboul-error.log

CustomLog ${APACHE\_LOG\_DIR}/gereboul-access.log combined

# Proxy vers Next.js

ProxyRequests Off

ProxyPreserveHost On

ProxyPass / http://localhost:3000/

ProxyPassReverse / http://localhost:3000/

# WebSockets pour Next.js

RewriteEngine On

RewriteCond %{HTTP:Upgrade} =websocket [NC]

RewriteRule /(.\*) ws://localhost:3001/$1 [P,L]

</VirtualHost>

**Modules Apache activés**

Les modules suivants sont activés :

* ssl
* proxy
* proxy\_http
* proxy\_wstunnel
* rewrite

**Étapes de mise en place (historique)**

**1. Préparation de l'environnement**

bash

Copier

# Désactivation de Nginx qui était en conflit

sudo systemctl stop nginx

sudo systemctl disable nginx

# Installation des modules Apache nécessaires

sudo a2enmod ssl proxy proxy\_http proxy\_wstunnel rewrite

**2. Création des certificats SSL**

bash

Copier

# Création du répertoire pour les certificats

sudo mkdir -p /etc/ssl/gereboul

# Génération du certificat auto-signé

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 \

-keyout /etc/ssl/gereboul/server.key \

-out /etc/ssl/gereboul/server.crt \

-subj "/CN=gereboul.net"

**3. Configuration d'Apache**

bash

Copier

# Création du fichier de configuration

sudo nano /etc/apache2/sites-available/gereboul.conf

# [Contenu du fichier ajouté comme indiqué ci-dessus]

# Activation du site

sudo a2ensite gereboul.conf

# Test de la configuration

sudo apache2ctl configtest

# Démarrage d'Apache

sudo systemctl start apache2

sudo systemctl enable apache2

**Maintenance et dépannage**

**Vérification du statut d'Apache**

bash

Copier

sudo systemctl status apache2

**Vérification des ports utilisés**

bash

Copier

sudo lsof -i :80

sudo lsof -i :443

**Consultation des logs Apache**

bash

Copier

# Logs d'erreur

sudo tail -f /var/log/apache2/gereboul-error.log

# Logs d'accès

sudo tail -f /var/log/apache2/gereboul-access.log

**Redémarrage d'Apache après modification**

bash

Copier

sudo systemctl restart apache2

**Améliorations futures**

**Installation d'un certificat SSL valide avec Let's Encrypt**

bash

Copier

# Installation de Certbot via snap

sudo snap install core

sudo snap refresh core

sudo snap install --classic certbot

sudo ln -sf /snap/bin/certbot /usr/bin/certbot

# Obtention d'un certificat

sudo certbot --apache -d gereboul.net -d www.gereboul.net

**Sauvegarde des fichiers importants**

Pour une restauration rapide en cas de problème, sauvegardez régulièrement :

1. /etc/apache2/sites-available/gereboul.conf
2. /etc/ssl/gereboul/server.crt
3. /etc/ssl/gereboul/server.key

**Sécurité**

* Le certificat auto-signé actuel devrait être remplacé par un certificat validé par une autorité de certification (comme Let's Encrypt).
* Vérifiez régulièrement les mises à jour de sécurité avec sudo apt update && sudo apt upgrade.
* Examinez périodiquement les logs pour détecter les tentatives d'intrusion.