

# Installation

## Pré-requis

- Une machine pouvant faire le proxy avec au moins 4 coeurs, 4 Gb de Ram et une connexion de 500 Mbps
- Un Nom de domaine

## Mise a jour des paquets

```
apt update -y
```

```
apt upgrade -y
```

## Installation des dépendances de base

```
apt install sudo nload htop tcpdump curl zip unzip net-tools screen ipset -y
```

## Installation de Nginx

```
apt install nginx -y
```

## Upgrade de Nginx en version Beta

```
sudo echo "deb http://nginx.org/packages/mainline/debian/ bullseye nginx deb-src  
http://nginx.org/packages/mainline/debian/ bullseye nginx" > /etc/apt/sources.list.d/nginx.list
```

```
apt install gnupg
```

```
wget -qO - https://nginx.org/keys/nginx\_signing.key | sudo apt-key add -
```

```
sudo apt update
```

```
sudo apt remove nginx-common -y
```

```
sudo apt install nginx
```

```
cd /etc/nginx && mkdir rproxy && cd rproxy && mkdir http http/available http/enabled stream  
stream/available stream/enabled
```

## On vérifie la version de Nginx

```
nginx -v (résultat au dessus de 19)
```

## Installation du certificat SSL avec Certbot

## Installation de Certbot avec python3 pour Nginx

```
sudo apt install -y python3-certbot-nginx
```

## Création du certificat SSL

```
certbot certonly --nginx -d proxy.johanpaam.fr
```

## Configuration de Nginx et du Proxy

## Se rendre dans /etc/nginx/sites-available

Crée le fichier se nomant "proxy-web.conf"

```

upstream backend {
    server your.fivem.server.ip:30120;
}

proxy_cache_path /srv/cache levels=1:2 keys_zone=assets:48m max_size=20g inactive=2h;

server {
    listen 443 ssl;
    listen [::]:443 ssl;

    server_name proxy.johanpaam.fr;

    # SSL is highly encouraged but optional. If not using SSL, comment the below and change the listen blocks
    # above.
    ssl_certificate /etc/letsencrypt/live/proxy.johanpaam.fr/cert.pem;
    ssl_certificate_key /etc/letsencrypt/live/proxy.johanpaam.fr/privkey.pem;

    location / {
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $remote_addr;
        proxy_pass_request_headers on;
        proxy_http_version 1.1;
        proxy_pass http://backend;
    }

    # if you do not wish to use the caching proxy, remove the below block
    location /files/ {
        proxy_pass http://backend$request_uri;
        add_header X-Cache-Status $upstream_cache_status;
        proxy_cache_lock on;
        proxy_cache assets;
        proxy_cache_valid 1y;
        proxy_cache_key $request_uri$is_args$args;
        proxy_cache_revalidate on;
        proxy_cache_min_uses 1;
    }
}

```

# Se rendre dans /etc/nginx

Crée le fichier se nomant "stream-proxy.conf"

```
stream {  
    upstream backend{  
        server ipdevotreserveurfivem:30120;  
    }  
    server {  
listen 30120;  
proxy_pass backend;  
}  
server {  
listen 30120 udp reuseport;  
proxy_pass backend;  
}  
}
```

## Remplacement fichier Nginx.conf

Remplacer le contenu du fichier nginx.conf par celui-ci

```
worker_rlimit_nofile 999999;  
  
user  nginx;  
worker_processes  1;  
  
error_log  /var/log/nginx/error.log warn;  
pid        /var/run/nginx.pid;  
  
include /etc/nginx/stream-proxy.conf;  
  
events {  
    worker_connections  999999;  
}
```

```
http {
    include      /etc/nginx/mime.types;
    default_type application/octet-stream;

    log_format  main  '$remote_addr - $remote_user [$time_local] "$request" '
                      '$status $body_bytes_sent "$http_referer" '
                      '"$http_user_agent" "$http_x_forwarded_for"';

    access_log  /var/log/nginx/access.log  main;

    proxy_cache_path /srv/cache levels=1:2 keys_zone=assets:48m max_size=20g inactive=2h;

    sendfile      on;
    #tcp_nopush    on;

    keepalive_timeout 65;

    #gzip on;

    include /etc/nginx/conf.d/*.conf;
}
```

# Augmentation du ulimit (max open files)

## Se rendre dans /etc/sysctl.conf

Ajouter a la fin du fichier cette ligne

```
fs.file-max = 999999
```

Faites cette commande pour mettre a jour avec la nouvelle configuration

```
sudo sysctl -p
```

## Se rendre dans /etc/security/limits.conf

Ajouter ces lignes a la fin du fichier

```
* soft nfile 999999
* hard nfile 999999
www-data soft nfile 999999
www-data hard nfile 999999
root soft nfile 999999
root hard nfile 999999
```

## Se rendre dans /etc/pam.d/common-session

Ajouter cette ligne

```
session required pam_limits.so
```

## Se rendre dans /etc/default/nginx

Ajouter cette ligne

```
ulimit -n 9999
```

## Config FXServer

```
sv_forceIndirectListing true
sv_listingHostOverride proxy.johanpaam.fr
sv_listingIpOverride "0.0.0.0"
sv_proxyIPRanges "0.0.0.0/32"
```

Si vous souhaitez utiliser plusieurs Proxy (minimum 8 pour que sa soit fonctionnel) remplacez `sv_proxyIPPranges` par `sv_proxyIPRanges` en mettant la liste de vos proxy après

A ajouter dans votre `server.cfg`, ensuite redémarrez votre serveur

Redémarrez Nginx avec la commande `service nginx restart`

Votre serveur passe désormais par le proxy !

# Utiliser plusieurs Proxys

Répéter l'installation sur plusieurs machines, pointer le domaine (exemple proxy.johanpaam.fr) vers chaque IPs

- Proxy.johanpaam.fr pointe sur 0.0.0.1 mais aussi sur 0.0.0.2, 0.0.0.3 etc

## Config FXServer Multiples Proxys

```
sv_listingHostOverride proxy.johanpaam.fr
sv_listingIpOverride "proxy.johanpaam.fr"
sv_proxyIPPranges "0.0.0.0/32 0.0.0.1/32 0.0.0.2/32 0.0.0.4/32 0.0.0.5/32"
```

---

Révision #2

Créé 21 mai 2024 13:22:01 par Johan

Mis à jour 21 mai 2024 13:23:15 par Johan