

Configuration pas à pas de SSL sur PostgreSQL

L'objectif est de sécuriser les connexions entre le client et le serveur PostgreSQL via SSL (Secure Sockets Layer). Voici une démarche pas à pas pour configurer et activer SSL sur PostgreSQL.

Appliquer cette routine à chaque nœud de serveur

1. Vérification de l'installation de PostgreSQL avec le support SSL

Avant de commencer, assurez-vous que PostgreSQL a été compilé avec le support SSL :

```
bash
Copier le code
psql -c "SHOW ssl;"
```

- Si `ssl` retourne `off`, vérifiez que PostgreSQL a été compilé avec `--with-openssl`.
- Installez les bibliothèques SSL si nécessaire :

```
bash
Copier le code
sudo apt-get install libssl-dev
```

2. Création des certificats SSL

a. Génération du certificat auto-signé

1. Créez un répertoire pour stocker les certificats :

```
bash
Copier le code
sudo mkdir /etc/postgresql
sudo chmod 700 /etc/postgresql
```

2. Créez une clé privée :

```
bash
Copier le code
sudo openssl genrsa -out /etc/postgresql/server.key 2048
```

3. Modifiez les permissions de la clé privée :

```
bash
Copier le code
```

```
sudo chmod 600 /etc/postgresql/server.key
```

4. Créez le certificat auto-signé :

```
bash
Copier le code
sudo openssl req -new -x509 -days 365 -key /etc/postgresql/server.key
-out /etc/postgresql/server.crt -subj
"/C=FR/ST=FRANCE/L=PARIS/O=ASTON/CN=postgresql.local"
```

3. Configuration du serveur PostgreSQL

a. Modifier le fichier `postgresql.conf`

Ouvrez le fichier de configuration PostgreSQL :

```
bash
Copier le code
sudo nano /etc/postgresql/<version>/main/postgresql.conf
```

Modifiez ou ajoutez les lignes suivantes :

```
conf
Copier le code
ssl = on
ssl_cert_file = '/etc/postgresql/ssl/server.crt'
ssl_key_file = '/etc/postgresql/ssl/server.key'
```

Remplacez `<version>` par la version PostgreSQL installée.

b. Modifier le fichier `pg_hba.conf`

Le fichier `pg_hba.conf` définit les règles d'accès. Ouvrez le fichier :

```
bash
Copier le code
sudo nano /etc/postgresql/<version>/main/pg_hba.conf
```

Ajoutez ou modifiez les lignes pour obliger l'utilisation du SSL :

hostssl	all	all	0.0.0.0/0	md5
hostssl	all	all	::/0	md5

4. Redémarrer PostgreSQL

Redémarrez le service PostgreSQL pour appliquer les changements :

```
bash
Copier le code
sudo systemctl restart postgresql
```

5. Connexion avec le client PostgreSQL (Optionnel)

Pour vous connecter avec SSL activé :

```
bash
Copier le code
psql "sslmode=require host=<adresse_ip_serveur> dbname=<nom_base>
user=<utilisateur>"
```

- **sslmode=require** : exige une connexion sécurisée.
- Vous pouvez également utiliser `sslmode=verify-full` pour une vérification complète du certificat si un certificat CA est disponible.

6. Tests et vérifications

a. Vérification du statut SSL dans PostgreSQL

Dans `psql`, exécutez :

```
sql
Copier le code
SHOW ssl;
```

Si la sortie est `on`, le SSL est activé.

b. Vérification des logs PostgreSQL

Vérifiez les logs pour voir les connexions :

```
bash
Copier le code
sudo tail -f /var/log/postgresql/postgresql-16-main.log
```