

INSTALACION Y CONFIGURACION DE SSL

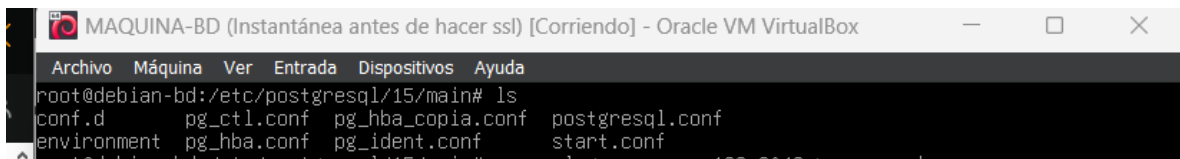
Comprovacions:

- PostgreSQL instal·lat
 - Comprovar connexió a internet (adaptador pont) a la base de dades
 - Actualitzar repositoris (apt update + apt upgrade)
 -
1. Configuració de PostgreSQL per ssl

Primer generarem un certificat SSL amb una eina anomenada openssl:

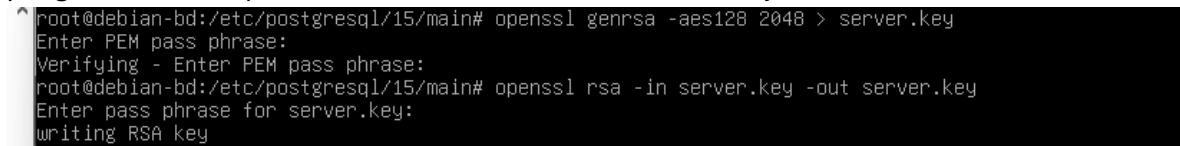
PROCES DE CREACIO DE CERTIFICAT:

Anem a la ruta on es troba el fitxer de configuració de postgresql, una vegada a dins podem crear una carpeta i dins d'ella crear els certificats. En el meu cas no la creu sinó que els vaig fer al main on hi ha el fitxer de configuració.



```
MAQUINA-BD (Instantánea antes de hacer ssl) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
root@debian-bd:/etc/postgresql/15/main# ls
conf.d          pg_ctl.conf    pg_hba_copia.conf  postgresql.conf
environment     pg_hba.conf    pg_ident.conf       start.conf
```

per generar la clau privada executem les comandes a la ruta ja esmentada:



```
root@debian-bd:/etc/postgresql/15/main# openssl genrsa -aes128 2048 > server.key
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
root@debian-bd:/etc/postgresql/15/main# openssl rsa -in server.key -out server.key
Enter pass phrase for server.key:
writing RSA key
```

openssl genrsa -aes128 2048 > server.key

aquesta ordre genera la clau privada amb l'opció d'encryptació especificada que és -aes128 i en mida de la clau privada que es genera en bits que són 2048 tot això ho generarà amb el nom i l'extensió especificat que és server.key.

```
openssl rsa -in server.key -out server.key
```

Això especifica el nom del fitxer d'entrada per llegir una clau un cop feta amb l'opció -out podrem escriure una clau per a aquest.

Un cop fet aquest procediment canviarem els permisos del fitxer i el propietari com es mostra a la imatge:

```
root@debian-bd:/etc/postgresql/15/main# chmod 400 server.key
root@debian-bd:/etc/postgresql/15/main# chown postgres:postgres server.key
root@debian-bd:/etc/postgresql/15/main# openssl req -new -key server.key -days 365 -out server.crt -x509
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Blanes
Locality Name (eg, city) []:Blanes
Organization Name (eg, company) [Internet Widgits Pty Ltd]:sapalomera
Organizational Unit Name (eg, section) []:bd
Common Name (e.g. server FQDN or YOUR name) []:arley
Email Address []:
root@debian-bd:/etc/postgresql/15/main# cp server.crt root.crt
root@debian-bd:/etc/postgresql/15/main#
```

Chmod 400 server.key : amb aquesta comanda canviem els permisos perquè el propietari del fitxer té permisos de lectura.

chown postgres:postgres server.key : canvia el propietari i el grup a l'usuari postgres.

Un cop fet això s'executa la comanda : openssl req -new -key server.key -days 365 -out server.crt -x509:

Després d'executar la comanda no demanarà emplenar unes dades, emplenem les que creiem convenientes.

Después de terminar de rellenar, copiamos el fichero server.crt y creamos una copia con otro nombre:

Cp server.crt root.crt

Un cop generats els canvis anteriors, procedim a configurar perquè s'utilitzi el certificat i la clau generats.

```
Archivo Maquina Ver Entrada Dispositivos Ayuda
GNU nano 7.2 postgresql.conf

# - SSL -

ssl = on
ssl_ca_file = '/etc/postgresql/15/main/root.crt'
ssl_cert_file = '/etc/postgresql/15/main/server.crt'
#ssl_crl_file = ''
#ssl_crl_dir = ''
ssl_key_file = '/etc/postgresql/15/main/server.key'
ssl_ciphers = 'HIGH:MEDIUM:+3DES:!aNULL' # allowed SSL ciphers
ssl_prefer_server_ciphers = on
#ssl_ecdh_curve = 'prime256v1'
#ssl_min_protocol_version = 'TLSv1.2'
#ssl_max_protocol_version = ''
#ssl_dh_params_file = ''
#ssl_passphrase_command = ''
#ssl_passphrase_command_supports_reload = off

#-----
# RESOURCE USAGE (except WAL)
#-----
```

IMPORTANT:

Dins del fitxer busquem l'apartat - SSL – i verifiquem si el ssl és a on, on posa ssl_ca_file posem la ruta del fitxer root.crt, al ssl_cert_file posem la ruta del fitxer server.crt i per últim posem a ssl_key_file la ruta del fitxer server.key, després descomentem el ssl_ciphers, ssl_prefer_server_ciphers i guardem.

Ara configurem el fitxer pg_hba.conf i afegim al final del fitxer la següent línia:

```
#
# Database administrative login by Unix domain socket
local all postgres peer

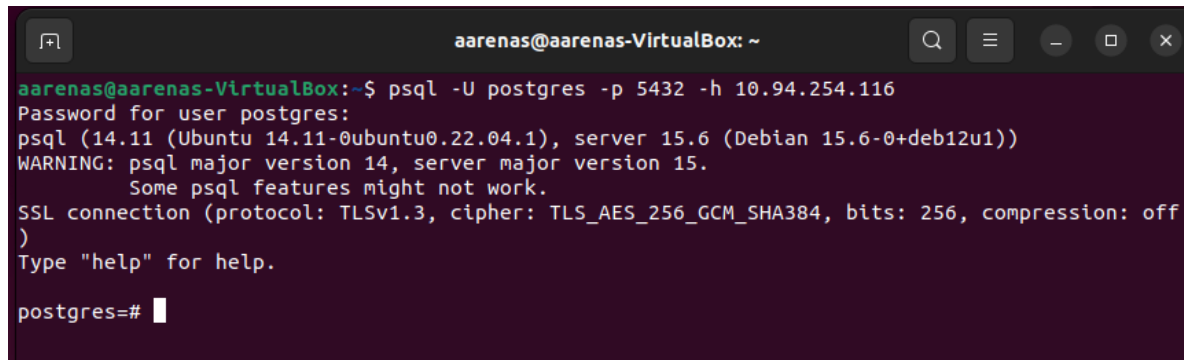
# TYPE DATABASE USER ADDRESS METHOD
# "local" is for Unix domain socket connections only
local all all peer
# IPv4 local connections:
host all all 127.0.0.1/32 scram-sha-256
host all all 0.0.0.0/0 scram-sha-256
# IPv6 local connections:
host all all ::1/128 scram-sha-256
# Allow replication connections from localhost, by a user with the
# replication privilege.
local replication all peer
host replication all 127.0.0.1/32 scram-sha-256
host replication all ::1/128 scram-sha-256
hostssl all all 0.0.0.0/0 md5
```

Un cop modificat i guardat reiniciem el servei de postgres.

Sudo systemctl restart postgresql o sudo service postgresql restart

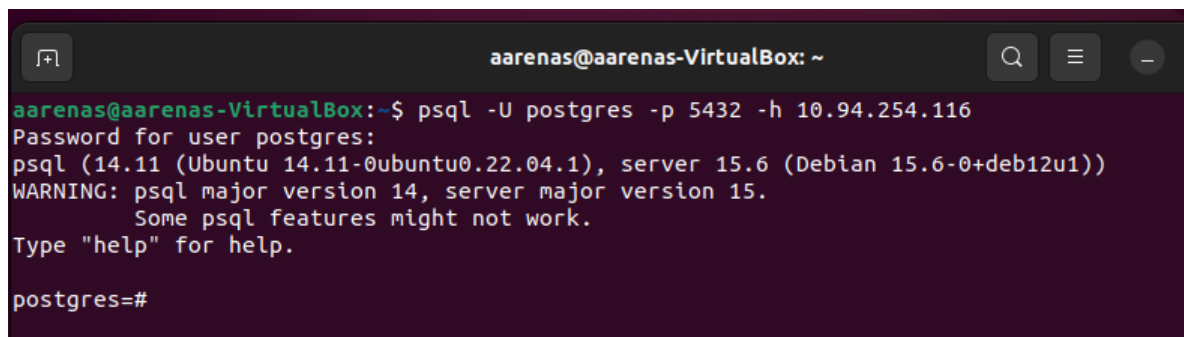
COMPROBACIONS:

SSL ON:



```
aarenas@aarenas-VirtualBox: ~  
aarenas@aarenas-VirtualBox:~$ psql -U postgres -p 5432 -h 10.94.254.116  
Password for user postgres:  
psql (14.11 (Ubuntu 14.11-0ubuntu0.22.04.1), server 15.6 (Debian 15.6-0+deb12u1))  
WARNING: psql major version 14, server major version 15.  
Some psql features might not work.  
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, bits: 256, compression: off)  
)  
Type "help" for help.  
postgres=#
```

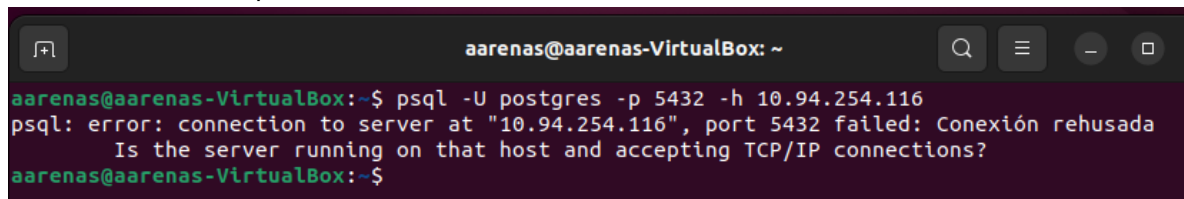
SSL OFF:



```
aarenas@aarenas-VirtualBox: ~  
aarenas@aarenas-VirtualBox:~$ psql -U postgres -p 5432 -h 10.94.254.116  
Password for user postgres:  
psql (14.11 (Ubuntu 14.11-0ubuntu0.22.04.1), server 15.6 (Debian 15.6-0+deb12u1))  
WARNING: psql major version 14, server major version 15.  
Some psql features might not work.  
Type "help" for help.  
postgres=#
```

SSL ON AMB RUTA ERRONEA:

Nota: es recomana posar la ruta absoluta on hi ha les claus.



```
aarenas@aarenas-VirtualBox: ~  
aarenas@aarenas-VirtualBox:~$ psql -U postgres -p 5432 -h 10.94.254.116  
psql: error: connection to server at "10.94.254.116", port 5432 failed: Conexión rehusada  
Is the server running on that host and accepting TCP/IP connections?  
aarenas@aarenas-VirtualBox:~$
```

WEBGRAFIA:

[OPENSSL RSA](#)

[OPENSSL GENRSA](#)

[PAGINA1 DE AYUDA DE CONFIGURACION DE SSL](#)

[PAGINA2 DE AYUDA DE CONFIGURACION DE SSL](#)