Entregable 0: pg_hba.conf

Autor: Francisco Javier Molina Rojas

El archivo pg_hba.conf (**p**ostgr**e** **h**ost-**b**ased **a**uthentication) es un archivo de configuración de postgre, que como podemos ver en la Figura 1, esta almacenado en el directorio "/etc/postgresql/14/main/".

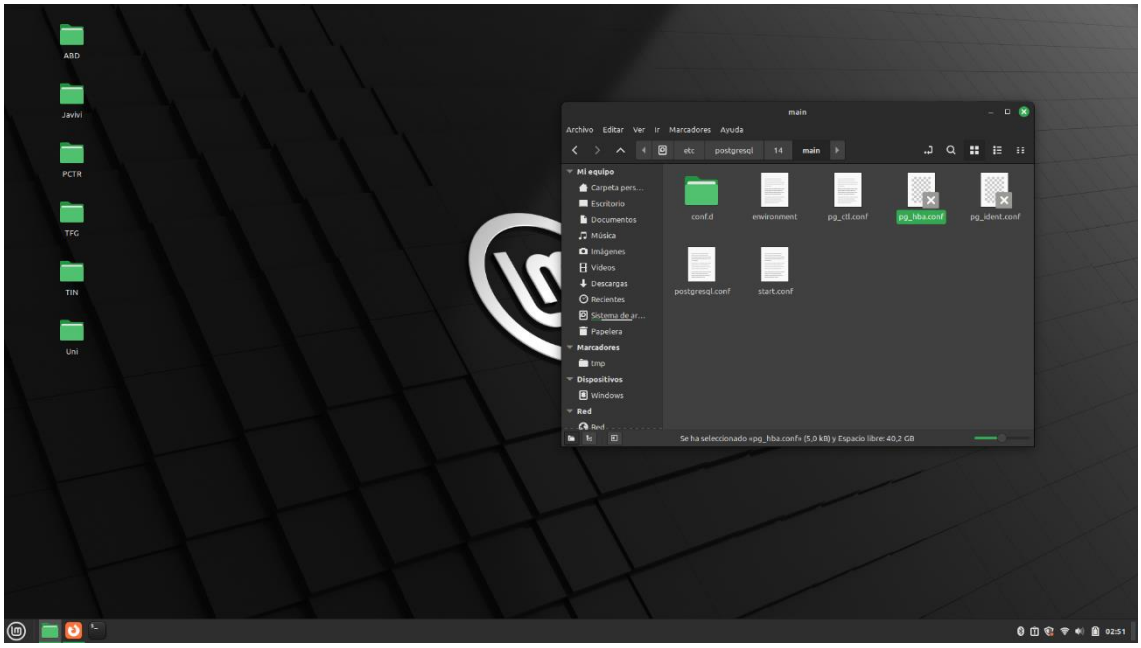

Figura 1 Ubicación de pg_hba.conf

Si intentamos abrir el archivo, veremos que no tenemos permiso para hacerlo. Para solucionarlo, usamos la orden "chmod 777" con sudo para conceder los permisos de lectura al archivo. Su contenido es visible en la Figura 2.

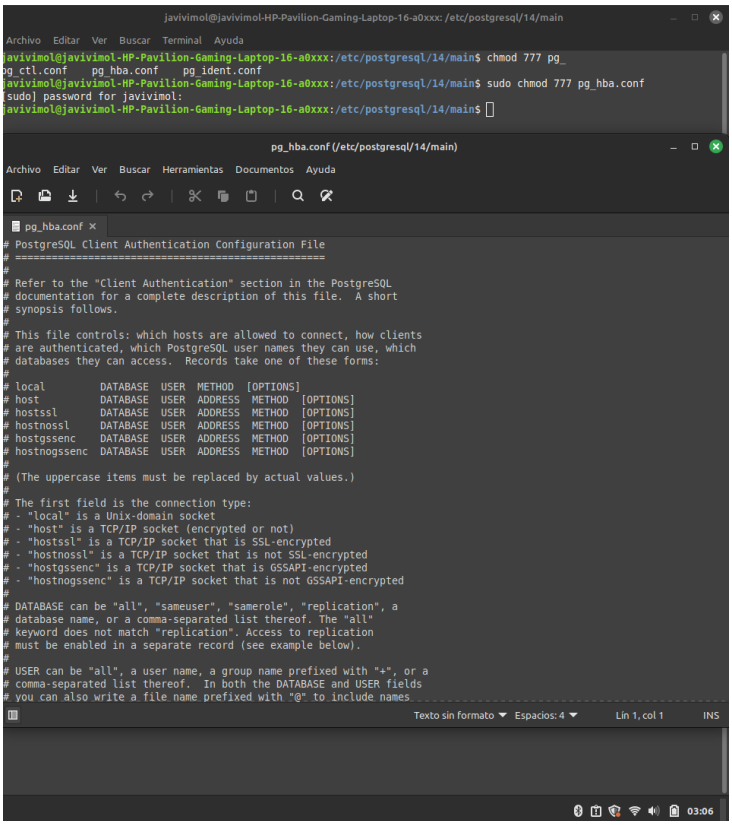

Figura 2 Contenido fichero

Como dice los comentarios del fichero, este es un fichero de configuración de autenticación de clientes. Este fichero controla (a través de registros), que host están autorizados a conectarse, como los clientes son autenticados, que usuarios pueden usar y a que bases de datos tienen acceso. El formato especifico de estos registros puede ser consultado en la Figura 2. Para resumir:

Si la conexión es local, el registro sigue la siguiente estructura:

- local DATABASE USER METHOD [OPTIONS]

Si la conexión es remota, el registro sigue las siguientes estructuras:

- host DATABASE USER ADDRESS METHOD [OPTIONS]
- hostssl DATABASE USER ADDRESS METHOD [OPTIONS]
- hostnossl DATABASE USER ADDRESS METHOD [OPTIONS]
- hostgssenc DATABASE USER ADDRESS METHOD [OPTIONS]
- hostnogssenc DATABASE USER ADDRESS METHOD [OPTIONS]

La primera palabra (local, host…) se refiere al tipo de conexión.

La segunda palabra (DATABASE) se refiere a la base de datos que se quiere usar.

La tercera palabra (USER) se refiere al **rol** (el concepto de tipo de usuario NO existe en ABD) que se quiere usar.

La cuarta palabra (necesaria para conexiones remotas, ADDRESS) se refiere a la dirección desde donde se va a establecer la conexión.

La quinta palabra (METHOD) se refiere al método que se usará para autenticar (como podemos leer en la documentación, si usamos el método “password”, la contraseña será mandada el texto claro). Esto puede ser un grave problema de seguridad ya que la contraseña es accesible.

Para evitar esto existe la opción "md5" o "scram-sha-256", que nos permite mandar las contraseñas encriptadas.

Por una parte, “md5” es uno de los algoritmos criptográficos mas conocidos y famosos. Sin embargo, tiene debilidades que hacen que su uso en un sistema sea inadecuado. Una de estas esta relacionadas con la facilidad de crear un certificado de autoridad con colisiones. A pesar de que tal y como esta previsto el uso de Postgre, no permitiría hacer uso de estas debilidades, es mejor evitar este método.

Esto lo soluciona usando el método “scram-sha-256”. Este tipo de algoritmo mejora la seguridad respecto al método “md5”, y aunque tenga problemas a la hora de implementarlo en el sistema, es una opción mas que recomendable el usar este método.

Por último, la sexta palabra ([OPTIONS]) se refiere al conjunto de opciones que pueden usar los registros.

Cuando realizamos cualquier tipo de cambio en el fichero (como, por ejemplo, para añadir una nueva conexión) debemos reiniciar el servicio de Postgre, para que los cambios tengan efectos.

Por último, como ejemplo de uso, podemos ver los distintos registros que trae este fichero por defecto cuando se instala Postgre, véase en Figura 3.

```
# 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
# 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
```

Figura 3 Registros por defecto