ACTIVIDAD 5 – SEGURIDAD Y CUMPLIMIENTO

Cristóbal Suárez Abad

ADMINISTRACIÓN DE SISTEMAS GESTORES DE BASES DE DATOS - 2º ASIR

Contenido

Actividad 5 – Seguridad y cumplimiento

Configuración de políticas de seguridad

- Activa el registro (`logging_collector = on`) y revisa el archivo `postgresql.conf`.

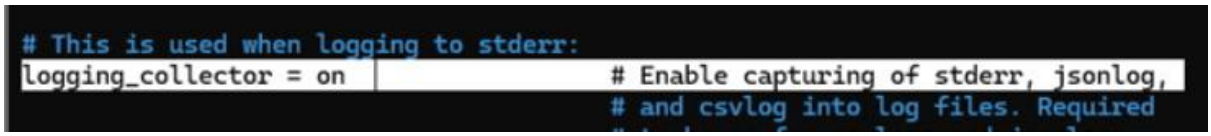
Modificamos el archivo "**postgresql.conf**". Debemos poner:

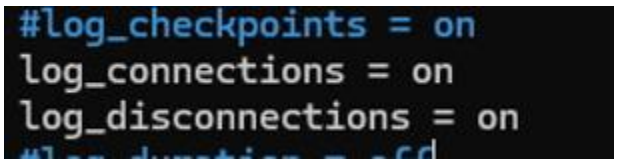
logging_collector = on

Y activar también las opciones:

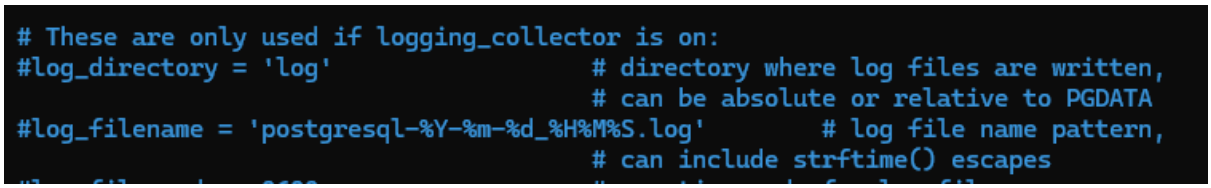
log_connections = on

log_disconnections = on

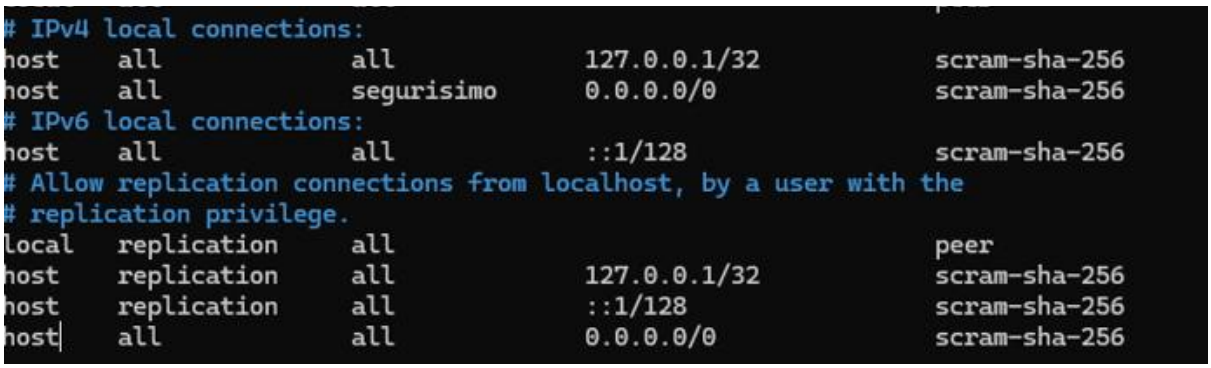




Algunos compañeros han dicho que han tenido que "**descomentar**" las siguientes líneas para que les funcione el registro. A mi no me ha hecho falta.



- Cambia la política de autenticación de `md5` a `scram-sha-256` en `pg_hba.conf`.



Auditoría de accesos

- Conéctate con distintos usuarios y revisa los logs.

Para saber dónde están los logs:

Te metes en **postgresql:**

Encuentra el Directorio de Datos (PGDATA): **SHOW data_directory**;

Verifica el Directorio de Logs: **SHOW log_directory;**

Determina el Nombre del Archivo de Log Actual (si el servidor está en ejecución): **SELECT pg_current_logfile();**

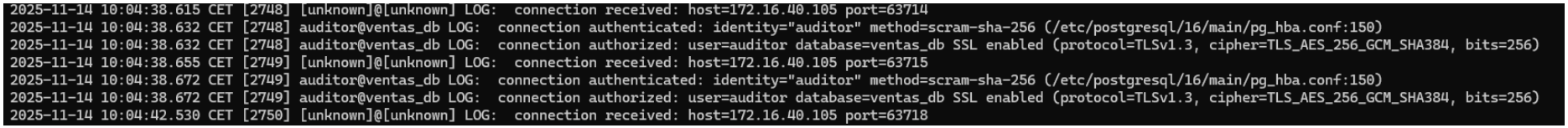
```
postgres=# SHOW data_directory;
       data_directory
-----------------------------
 /var/lib/postgresql/16/main
(1 row)

postgres=# SHOW log_directory;
 log_directory
---------------
 log
(1 row)

postgres=# SELECT pg_current_logfile();
          pg_current_logfile
---------------------------------------
 log/postgresql-2025-11-14_095314.log
(1 row)
```

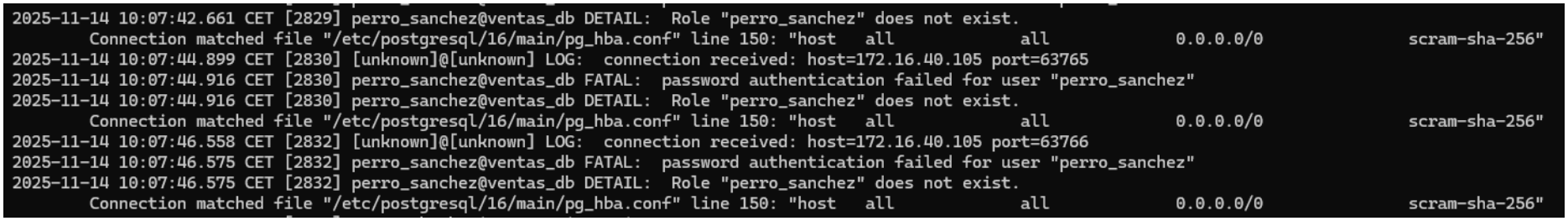
En “**/var/lib/postgresql/16/main/log/**”:

“Logeo” **exitoso**:



- Identifica intentos fallidos de conexión. Explica que ves

“Logeo” **fallido**:



Me indica hora, IP y nombre del usuario que intenta conectarse, también la conexión configurada en “**pg_hba.conf**” que se le aplicaría.

Comprobación de seguridad

- Verifica los privilegios de cada usuario (`\du` y `\z`).

```
postgres=# \du
                                   List of roles
    Role name    |                         Attributes
-----------------+------------------------------------------------------------
 admin_ventas    | Create role, Create DB                                    +
                 | Password valid until 2026-12-31 00:00:00+01
 auditor         | No inheritance                                            +
                 | 15 connections
 cristobal       |
 empleado_ventas | 3 connections
 postgres        | Superuser, Create role, Create DB, Replication, Bypass RLS
 segurisimo      | Superuser, Create role, Create DB, Replication, Bypass RLS
 solo_lectura    | Cannot login
 ventas_acceso   | 10 connections
 ventas_grupo    | Cannot login
```

```
postgres=# \z
                                    Access privileges
 Schema |      Name       |     Type      |     Access privileges     | Column privileges | Policies
--------+-----------------+---------------+---------------------------+-------------------+----------
 public | clientes        | table         |                           |                   |
 public | clientes_id_seq | sequence      |                           |                   |
 public | pedidos         | table         |                           |                   |
 public | pedidos_id_seq  | sequence      |                           |                   |
 public | productos       | foreign table | postgres=arwdDxt/postgres |                   |
(5 rows)
```

- Elabora un informe final indicando qué medidas garantizan la seguridad.

- **Vistas personalizadas**: Cada usuario solo accede a las columnas y datos esenciales para su función, ocultando información sensible (DNI, Email).
- **Revocación de Permisos Directos**: Se fuerza a los usuarios a usar las vistas, asegurando que las políticas de filtrado y exposición de datos se cumplan.
- **Restricción de Conexiones:** Previene el abuso o el uso excesivo de recursos por parte de cuentas individuales.
- **Asignación de Permisos de Manipulación Detallada**: Solo admin_ventas tiene el poder de eliminar registros, mientras que empleado_ventas solo puede insertar/actualizar.
- **Rol solo_lectura**: Centraliza y simplifica la concesión de acceso de solo lectura para la auditoría.
- **Autenticación scram-sha-256**: Mejora la seguridad de las contraseñas almacenadas, haciéndolas menos susceptibles a ataques que la política md5.
- **Registro de Actividad**: Permite detectar y rastrear intentos fallidos, accesos no autorizados y actividades sospechosas, garantizando el cumplimiento.