#### **Task 1 - HW: creating and managing roles**

**Task 1. Figure out what security precautions are already used in your 'dvd\_rental' database. Prepare description**

Data security in DBMS consist of end user authentication, access control, data encryption and database auditing tools. To evaluate the security precautions in the dvd\_rental database, I will analyze the aforementioned key aspects of database security:

1. **Authentication:** PostgreSQL supports a variety of authentication methods, including password authentication, certificate-based authentication, and external authentication via LDAP or Kerberos. By default, PostgreSQL requires users to authenticate using a password. The PostgreSQL Client Authentication Configuration File (pg\_hba.conf) specifies how clients are authenticated, which PostgreSQL user names they can use and which databases they can access.
2. **Access control:** PostgreSQL provides a strong authorization system that allows database administrators to control access to various database objects, including tables, views, and functions. To analyze the roles and privileges we can use a query to list the users in the database and their granted permissions:

SELECT \* FROM pg\_roles;  
 SELECT \* FROM information\_schema.role\_table\_grants;

1. PostgreSQL supports **encryption**, including network encryption, data encryption, and encryption of stored passwords:  
   Password encryption ensures that user credentials are securely stored in the database and the method can be checked using the following query:   
   SHOW password\_encryption;  
   Network encryption is also crucial for protecting data as it travels between the client and the PostgreSQL server and it can be checked using the following query:   
   SHOW ssl;
2. Database auditing features in Postgresql help detect and track security breaches by logging all the activities in the database. This can be achieved by reviewing the activities in the Session manager or the pg\_stat activity (Select \* from pg\_stat\_activity) or enabling PostgreSQL logging.

**Summary:**

Findings in the dvd\_rental database is that:

* password\_encryption was set to scram-sha-256
* SSL encryption is turned off which means that the data between the client and the database server is sent in plain text without encryption
* logging\_collector is enabled to track all the database activity