



Universidad Nacional Autónoma de México

Facultad de Ingeniería División de Ingeniería Eléctrica **Bases de Datos**

Profesor(a): Ing. Fernando Arreola Franco
Semestre 2025-1

Proyecto de Investigación

Nombre del Trabajo
Tarea II
Bases de Datos

Grupo: 1

Alumno:

Nava Benitez David Emilio

Requerimientos para conectarse a una Base de Datos [1]

La forma de conectarse depende de la herramienta o protocolo cliente que se use, el propósito de la conexión y como esté configurada la su red en la nube.

Prerrequisitos:

Para usar la consola o la API para obtener las cadenas de conexión del servicio de administración predeterminado, se le debe otorgar el tipo de acceso requerido en una política escrita por un administrador, ya sea que este usando la consola o a API REST con SDK.

Para conectarse a la base de datos, se necesitará la dirección IP publica o privada del sistema de base de datos.

Para acceder mediante Secure Shell (SSH) al sistema de base de datos, se necesitará la ruta completa al archivo que contiene la clave privada asociada con la clave publica utilizada cuando se inicio el sistema de base de datos.

Permisos a nivel sistema y objeto [2]

Estos son dos tipos de privilegios o permisos. El primero a nivel sistema o administrados son lo que controlan la creación de objetos y la administración del sistema. Mientras que, los privilegios de objeto acceden a objetos de base de datos específicos. Algunos privilegios de administrador son globales en cuanto al alcance, independientemente de la base de datos actual.

En los privilegios a nivel sistema, permite al usuario crear bases de datos. El permiso para operar en base de datos existentes está controlado por los privilegios de objeto.

Mientras que los permisos de objeto, que controlan el acceso a objetos individuales, por ejemplo, tablas. Los permisos del sistema incluyen desde utilizar la interfaz interactiva de SQL, crear una base de datos y concluir el ObjectServer, todo esto para el caso de usuarios en el ObjectServer.

Los permisos de objeto especifican las acciones que cada rol tiene autorización para realizar sobre un objeto concreto. Cada objeto tiene un conjunto de acciones asociadas. Por ejemplo, las acciones que puede realizar en una base de datos de ObjectServer son:

- DROP
- CREATE TABLE
- CREATE VIEW

¿Cómo dar y/o quitar permisos? [3]

La función GRANT de MySQL es la utilizada para facilitar privilegios:

```
GRANT privilegios  
ON base/tabla  
TO usuario [IDENTIFIED by 'contraseña']  
[WITH GRANT OPTION];
```

La opción WITH GRANT OPTION facilita al usuario el poder de darle a otros usuarios sus mismos privilegios.

Para dar todos los permisos, incluido el WITH GRANT OPTION, debe de indicarse con su opción pertinente:

```
GRANT ALL ON BD.* TO USER@localhost IDENTIFIED BY "PASSWORD"  
WITH GRANT OPTION;
```

La función REVOKE es empleada para retirar privilegios a los usuarios. Su sintaxis es muy similar a la de GRANT:

```
REVOKE privilegios  
ON base/tabla  
FROM usuario
```

Diferencia entre role y usuario [4]

Los conceptos de rol y usuarios están estrechamente relacionados. En PostgreSQL, un usuario es esencialmente un rol que tiene la capacidad de iniciar sesión en la base de datos.

Un usuario puede ser propietario de objetos de base de datos (como tablas, vistas, etc.). Cada usuario tiene un nombre de usuario único y puede tener una contraseña para la autenticación.

En el caso de los roles, en PostgreSQL es un concepto más general que abarca tanto a usuarios como a grupos. Un rol puede representar a un solo usuario o a una colección de usuario (un grupo).

Los roles pueden tener varios atributos como LOGIN, SUPERUSER, etc.

A los roles se les puede otorgar permisos sobre objetos de base de datos y pueden heredar permisos de otros roles.

Los roles de base de datos simplifican el proceso de gestión de privilegios, ya que se pueden otorgar privilegios a un rol y luego otorgar el rol a usuarios. Cuando se desee revocar privilegios para un usuario, simplemente se tiene que revocar la autorización de rol de usuario, en vez de revocar cada privilegio individual.

Referencias:

- [1] "Overview of Connecting to a DB System". Oracle Help Center. Accedido el 12 de febrero de 2025. [En línea]. Disponible: <https://docs.oracle.com/en/cloud/paas/base-database/connect/index.html#articletitle>
- [2] "Tivoli Netcool/OMNIBus 8.1.0". IBM - United States. Accedido el 12 de febrero de 2025. [En línea]. Disponible: <https://www.ibm.com/docs/es/netcoolomnibus/8.1?topic=roles-system-object-permissions>
- [3] P. Armesto. "MySQL: cómo conceder y quitar privilegios en esta base de datos". clouding.io. Accedido el 12 de febrero de 2025. [En línea]. Disponible: <https://help.clouding.io/hc/es/articles/360011519919-MySQL-cómo-conceder-y-quitar-privilegios-en-esta-base-de-datos>
- [4] "IBM Data Studio 4.1.1". IBM - United States. Accedido el 12 de febrero de 2025. [En línea]. Disponible: <https://www.ibm.com/docs/es/data-studio/4.1.1?topic=management-database-roles>