



UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO
FACULTAD INGENIERIA
BASES DE DATOS

Profesor: Ing. Fernando Arreola Franco

Tarea 2

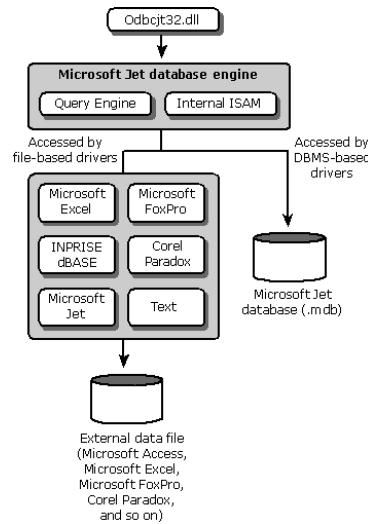
Rodrigo Jardón Marín

Fecha de entrega: 16/02/2026

1. ¿Qué requiero para conectarme a una Base de Datos?

Para poder conectarse a la mayoría de las bases de datos tales como MySQL, PostgreSQL, SQL Server, etc. Se tienen una serie de pasos y puntos que son casi casi universales los cuales son:

- Controlador: (Driver): Este es el software o librería la cual permitirá que el programa pueda interactuar y comunicarse con el mismo que tienen la base de datos. Ya que, si no hay un driver correcto para eso, no hará comunicación entre los lenguajes.



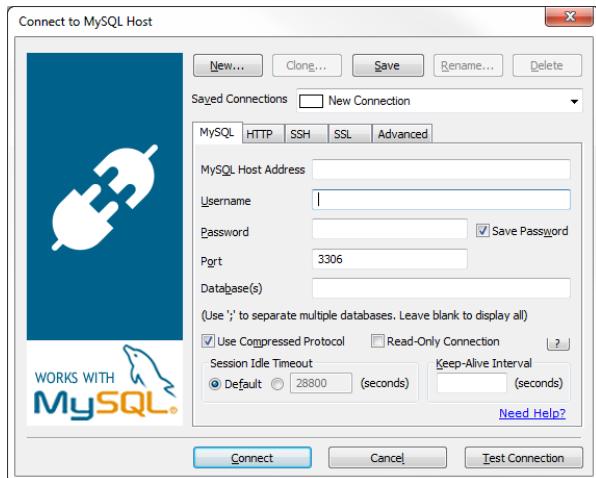
- Configuración de Seguridad: Se tiene que ver si la conexión es segura o no. Aquí es donde se decide si se usará una conexión cifrada tal como SSL, la cual funciona como un túnel seguro para que nadie intercepte ni lea información, en el caso de que se elija tener SSL se deberá tener un archivo llamado "certificado" para que se valide que la conexión es veraz y confiable antes de que se empiece a pasar información



- Acceso a Red y Puerto: Para que la conexión funcione, se necesita comprobar que el sistema de seguridad de red, no esté bloqueando ese número de puerto

específico, si el firewall no tiene permiso para dejar pasar el tráfico por ahí la conexión será rechazada de manera automática, aunque se tenga la contraseña correcta.

- Credenciales y Detalles del Host: Se recopila la dirección exacta de la computadora donde está la base de datos, y presentar las credenciales, tales como el nombre de usuario, contraseña, etc. Para que así el sistema pueda validar quién es y autorice para poder ver la información que se requiere.



2. Permisos a nivel de sistema

La seguridad en bases de datos se divide en dos categorías las cuales determinan la capacidad de acciones de un usuario y se asignan mediante la sintaxis 'GRANT'.

Primero, existen los permisos de sistema, que otorgan capacidades administrativas generales sobre el servidor completo, tales como la autorización para iniciar sesión, utilizar la interfaz interactiva, crear nuevas bases de datos o detener el servicio.

En segundo lugar, están los permisos de objeto, que son autorizaciones específicas y limitadas para interactuar con elementos concretos dentro de una base de datos que ya existe, estos definen si un usuario tiene derecho a realizar acciones puntuales como crear tablas, eliminar vistas o modificar estructuras internas, sin afectar al sistema global.



3. ¿Cómo dar/quitar permisos?

El dar y quitar permisos a un usuario consiste en dar o remover permisos que como se explico anteriormente dan a un usuario el derecho a realizar acciones puntuales.

Esto permitirá controlar el acceso y da seguridad.

Para asignar privilegios a un usuario en una base de datos, utilizamos la sintaxis GRANT, con el formato que se muestra en este ejemplo:

```
GRANT <privileges> ON <database>.<object> TO '<user>'@'<host>' ;
```

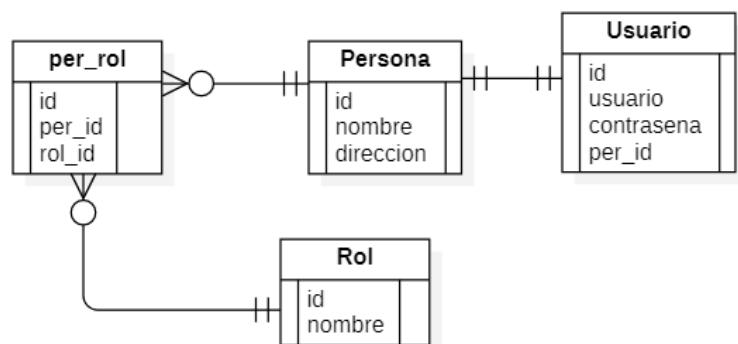
Y para quitar privilegios a un usuario en una base de datos, usamos la sintaxis REVOKE, con el formato que se muestra en este ejemplo:

```
REVOKE <privileges> ON <database>.<object> FROM '<user>'@'<host>' ;
```

4. Diferencia entre rol y usuario

La principal diferencia es que un usuario es la cuenta individual que se conecta a la base de datos, mientras que un rol es una entidad que funciona como un "contenedor" o conjunto de privilegios agrupados.

Básicamente, los roles existen para facilitar la gestión, en vez de configurar manualmente el nivel de acceso exacto para docenas de usuarios individuales, simplemente creas una agrupación de privilegios con nombre (el rol) y se lo asignas a quienes lo necesiten, como, por ejemplo, dar acceso al rol a todo el equipo de ventas de una sola vez.



Bibliografias:

[1] “IBM DB2 Warehouse as a service.” <https://www.ibm.com/docs/es/db2w-as-a-service?topic=ss6nhc-com-ibm-swg-im-dashdb-doc-connecting-connecting-applications-to-dashdb-database-html>

[2] “Netcool/OMNIbus.”

<https://www.ibm.com/docs/es/netcooolnibus/8.1.0?topic=roles-system-object-permissions>

[3] “Grant and Revoke MySQL Privileges using `GRANT` and `REVOKE`,” *Prisma’s Data Guide*. <https://www.prisma.io/dataguide/mysql/authentication-and-authorization/privilege-management>

[4] “Using roles to manage privileges for users with MySQL | Prisma,” *Prisma’s Data Guide*. <https://www.prisma.io/dataguide/mysql/authentication-and-authorization/role-management>