Universidad Nacional Autónoma de México

Facultad de Ingeniería

Bases de Datos (1644)

Grupo 1

Tarea 2

Profesor: Ing. Fernando Arreola Franco

Alumno: Medina Guzmán Santiago

Semestre: 2025-2

¿Qué requiero para conectarme a una base de datos?

Una conexión de base de datos le permite trabajar con tablas de bases de datos directamente en Insights. Se pueden crear conexiones de base de datos para las bases de datos compatibles y bases de datos relacionales adicionales que utilizan el controlador Java Database Connectivity (JDBC).

Antes de crear una conexión de base de datos, se deben cumplir los siguientes requisitos:

- Se debe agregar el conector adecuado para poder crear una conexión de base de datos. Para obtener más información, consulte archivos de proveedor requeridos y administrar tipos de conectores.
- Debe disponer de los privilegios adecuados para la base de datos a la que desea conectarse. Si no tiene privilegios para la base de datos, póngase en contacto con el administrador de la base de datos.
- Debe ser capaz de autentificar la conexión. En la mayoría de las bases de datos, se utiliza un nombre de usuario y una contraseña para la autenticación. SQL Server y BigQuery utilizan los siguientes métodos alternativos de autenticación:
    - SQL Server puede utilizar la autenticación de SQL Server (nombre de usuario y contraseña) o la autenticación del SO. Para obtener más información, consulte Habilitar OS de autenticación.
    - BigQuery utiliza la autenticación de cuentas de servicio. Para obtener más información, consulte Crear una cuenta de servicio y una clave privada.

Permisos a nivel sistema y objeto

Los permisos determinan qué tipos de acciones pueden realizar los usuarios en el ObjectServer.

Se asignan permisos a los roles utilizando el mandato GRANT. Hay dos tipos de permisos:

- *Permisos de sistema*, que controlan los mandatos que pueden ejecutarse en el ObjectServer
- *Permisos de objeto*, que controlan el acceso a objetos individuales, como por ejemplo tablas

Los permisos de sistema incluyen la capacidad de utilizar la interfaz interactiva de SQL, crear una base de datos y concluir el ObjectServer. Por ejemplo:

- El permiso ISQL es necesario para conectar al ObjectServer utilizando la interfaz interactiva de SQL.
- El permiso ISQLWrite es necesario para modificar datos del ObjectServer utilizando la interfaz interactiva de SQL.

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 quitar permisos

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.

Con la siguiente query darías todos los permisos **(excepto WITH GRANT OPTION)** a un usuario sobre una base de datos especificada:

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

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;
```

Cabe destacar que esto no es aconsejable, y es altamente inseguro ya que únicamente el usuario administrador debería poder agregar o eliminar privilegios.

De la siguiente forma únicamente le darías permiso para realizar algunas querys sobre la base de datos. Cabe destacar que el usuario no podría crear nuevas tablas ni nuevas bases de datos:

```
GRANT select,insert,update,delete ON BD.* TO USER@localhost IDENTIFIED BY "PASSWORD";
```

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
```

De este modo quitarías todos los permisos del usuario.

```
REVOKE ALL ON BD.* from USER@localhost
```

Diferencia entre role y usuario

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 desea revocar privilegios para un usuario, simplemente se tiene que revocar la autorización de rol del usuario, en vez de revocar cada privilegio individual.

Los roles se crean y se descartan utilizando el mismo proceso que para realizar cualquier cambio de objeto de base de datos.

Referencias

“Crear una conexión de base de datos,” *ArcGIS*. https://doc.arcgis.com/es/insights/latest/get-started/create-a-database-connection.htm (accessed Feb. 19, 2025).

“Permisos de objeto y sistema,” *IBM*, Jan. 30, 2025. https://www.ibm.com/docs/es/netcoolomnibus/8.1?topic=roles-system-object-permissions (accessed Feb. 19, 2025).

P. Armesto, “MySQL: Cómo conceder y quitar privilegios en esta base de datos,” *https://help.clouding.io/hc/es/articles/360011519919-MySQL-c%C3%B3mo-conceder-y-quitar-privilegios-en-esta-base-de-datos*, 2020. https://help.clouding.io/hc/es/articles/360011519919-MySQL-c%C3%B3mo-conceder-y-quitar-privilegios-en-esta-base-de-datos (accessed Feb. 19, 2025).