TAREA 2 - Conexión y control de accesos en bases de datos

Vences Santillán Carlos Eduardo

22 de agosto de 2025

1. ¿Qué requiero para conectarme a una base de datos?

Desde el punto de vista teórico, una conexión a una base de datos requiere varios elementos interrelacionados:

- **Mecanismo de comunicación**: el gestor de bases de datos (DBMS) expone una interfaz de conexión, usualmente mediante un puerto de red y un protocolo definido.
- **Cliente**: puede ser un programa (como `psql`, `MySQL Workbench`, `SQL Server Management Studio`) o una librería (`ODBC`, `JDBC`).
- **Credenciales de autenticación**: el sistema debe identificar a la entidad que solicita acceso, ya sea mediante usuario y contraseña, autenticación integrada o certificados digitales.
- **Parámetros de conexión**: servidor, puerto, base de datos y, en algunos casos, el esquema.
- **Permisos adecuados**: aunque la conexión sea exitosa, solo se podrá interactuar si el DBMS concede los privilegios necesarios.

En términos teóricos, la conexión es un proceso de **autenticación** (verificación de identidad) seguido por una **autorización** (definición de lo que se permite hacer).

2. Permisos a nivel sistema y a nivel objeto

La teoría de control de acceso distingue dos grandes niveles:

- **Permisos de nivel sistema**: privilegios globales que afectan al DBMS completo o a la base en su conjunto. Permiten crear usuarios, crear bases de datos, modificar parámetros del servidor o realizar copias de seguridad.
- **Permisos de nivel objeto**: se otorgan sobre entidades específicas (tablas, vistas, funciones, procedimientos). Regulan operaciones concretas como leer datos (`SELECT`), modificarlos (`INSERT`, `UPDATE`, `DELETE`), ejecutar funciones (`EXECUTE`) o referenciar tablas en claves foráneas (`REFERENCES`).

Esta división responde al principio de **jerarquía de control**, que evita que un usuario con privilegios de consulta pueda alterar la estructura de la base.

3. ¿Cómo dar o quitar permisos?

En el plano teórico, los sistemas de bases de datos implementan un **modelo de control de acceso discrecional (DAC, Discretionary Access Control)**.

- `GRANT`: otorga a un usuario o rol la capacidad de realizar una acción determinada.
- `REVOKE`: retira un permiso previamente concedido.
- `DENY`: en algunos sistemas (como SQL Server), establece explícitamente la prohibición de un privilegio, incluso si este ha sido concedido por otro medio.

Este mecanismo aplica el principio del **mínimo privilegio**, que establece que cada usuario debe tener solo los permisos necesarios para realizar su función.

4. Diferencia entre *role* y *usuario*

- **Usuario**: es una identidad individual, que representa a una persona, aplicación o servicio. Es la unidad básica de autenticación (quién eres).
- **Rol**: es una entidad colectiva que agrupa un conjunto de permisos y puede asignarse a uno o varios usuarios. Representa un perfil de autorización (qué puedes hacer).

La diferencia radica en que el usuario es una instancia de acceso, mientras que el rol es un mecanismo de abstracción que facilita la administración. Este modelo se conoce como **control de acceso basado en roles (RBAC, Role-Based Access Control)**.

Conclusión

Para conectarse a una base de datos no basta con tener acceso técnico, sino que es necesario comprender la estructura jerárquica de permisos (sistema vs objeto) y la abstracción roles/usuarios. La concesión y revocación de permisos reflejan modelos teóricos de control de acceso que buscan equilibrar **usabilidad** y **seguridad** en la gestión de datos.

Referencias

[1] R. Elmasri and S. B. Navathe, *Fundamentals of Database Systems*, 7th ed. Boston, MA, USA: Pearson, 2017.

[2] A. Silberschatz, H. F. Korth, and S. Sudarshan, *Database System Concepts*, 7th ed. New York, NY, USA: McGraw-Hill, 2020.

[3] C. J. Date, *An Introduction to Database Systems*, 8th ed. Boston, MA, USA: Addison-Wesley, 2003.

[4] E. Ferrari and B. Thuraisingham, "Database Security Concepts, Approaches, and Challenges," *IEEE Transactions on Knowledge and Data Engineering*, vol. 8, no. 1, pp. 4–19, Feb. 1996.

[5] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, "Role-Based Access Control Models," *IEEE Computer*, vol. 29, no. 2, pp. 38–47, 1996.