

¿Qué requiero para conectarme a una BD?

Para poder conectarse a una base de datos se necesitan varios elementos básicos. Primero, el servidor de base de datos debe estar instalado y en funcionamiento. Después, es necesario contar con credenciales válidas, es decir, un nombre de usuario y una contraseña (o algún método de autenticación autorizado).

Además de las credenciales, el usuario debe tener el permiso para conectarse. En muchos sistemas gestores de bases de datos este permiso se conoce como CONNECT o CREATE SESSION. Si el usuario no tiene este privilegio, aunque su contraseña sea correcta, no podrá iniciar sesión.

También es necesario conocer los datos de conexión, como el nombre del servidor, el puerto y el nombre de la base de datos a la que se desea acceder.

Permisos a nivel sistema y objeto

Los permisos en una base de datos se clasifican principalmente en permisos a nivel sistema y permisos a nivel objeto.

Los permisos a nivel sistema permiten realizar acciones generales dentro del gestor de base de datos. Por ejemplo, crear tablas, crear usuarios, crear roles o administrar otros elementos del sistema. Estos privilegios afectan al entorno completo y normalmente los tiene un administrador.

En cambio, los permisos a nivel objeto se aplican a elementos específicos dentro de la base de datos, como tablas, vistas o procedimientos almacenados. Algunos ejemplos comunes son: SELECT (consultar datos), INSERT (agregar datos), UPDATE (modificar datos), DELETE (eliminar datos).

Estos permisos determinan exactamente qué operaciones puede realizar un usuario sobre un objeto en particular.

¿Cómo dar/quitar permisos?

Para administrar permisos se utilizan comandos del Lenguaje de Control de Datos (DCL).

El comando GRANT se usa para otorgar permisos a un usuario o a un rol. Por ejemplo, se puede conceder permiso para consultar una tabla o para crear objetos dentro del sistema.

Por otro lado, el comando REVOKE se utiliza para retirar permisos previamente otorgados. Esto permite controlar el acceso en caso de que un usuario ya no necesite ciertos privilegios o haya cambiado de funciones.

De esta manera, el administrador puede controlar quién puede hacer qué dentro de la base de datos.

Diferencia entre role y usuario

Un usuario es una identidad individual dentro de la base de datos. Tiene credenciales propias (nombre y contraseña) y puede iniciar sesión en el sistema si tiene los permisos necesarios.

Un role (rol) es un conjunto de permisos agrupados. No representa necesariamente a una persona, sino a un conjunto de privilegios que pueden asignarse a varios usuarios.

La principal diferencia es que el usuario es quien se conecta a la base de datos, mientras que el rol facilita la administración de permisos. En lugar de asignar permisos uno por uno a cada usuario, se asignan al rol y después ese rol se otorga a los usuarios que lo necesiten.

Bibliografía

[1] R. Elmasri and S. B. Navathe, *Fundamentals of Database Systems*, 7th ed. Boston, MA, USA: Pearson, 2016.

[2] A. Silberschatz, H. F. Korth and S. Sudarshan, *Database System Concepts*, 7th ed. New York, NY, USA: McGraw-Hill, 2019.

[3] Oracle, “Managing User Privileges and Roles,” Oracle Database Documentation. [Online]. Available: <https://docs.oracle.com/>

[4] Microsoft, “Getting Started with Database Engine Permissions,” Microsoft Learn. [Online]. Available: <https://learn.microsoft.com/>

[5] PostgreSQL Global Development Group, “Database Roles and Privileges,” PostgreSQL Documentation. [Online]. Available: <https://www.postgresql.org/docs/>