Universidad Nacional

Autónoma de México

Facultad de Ingeniería

Bases de Datos

Semestre: 2026-2

Tarea 2

Profesor: Fernando Arreola Franco

Alumno: Parra Bello Carlos Enrique

Número de cuenta: 321135344

Grupo: 01

¿Qué requiero para conectarme a una Base de Datos (BD)?

Para conectarse a una base de datos es necesario contar con varios elementos fundamentales. En primer lugar, se requiere un sistema gestor de bases de datos (SGBD), como Oracle, MySQL, PostgreSQL o SQL Server, el cual es el software encargado de almacenar, organizar y administrar la información. Este sistema puede estar instalado en una computadora local o en un servidor remoto.

Además, se necesita una herramienta cliente que permita establecer la conexión. Esta herramienta puede ser una interfaz gráfica, como SQL Developer o MySQL Workbench, o bien una herramienta de línea de comandos como SQL*Plus. También es posible conectarse desde aplicaciones desarrolladas en lenguajes de programación como Java, Python o C#, utilizando controladores o drivers específicos.

Para lograr la conexión se deben proporcionar ciertos datos obligatorios: la dirección del servidor (host o dirección IP), el número de puerto por el cual escucha el servicio (por ejemplo, 1521 en Oracle o 3306 en MySQL), el nombre de la base de datos o servicio, y finalmente un usuario con su respectiva contraseña. Estos datos permiten que el sistema valide la identidad del usuario y determine si tiene permisos para acceder.

Finalmente, es necesario que el usuario tenga privilegios de conexión otorgados dentro del sistema, como el privilegio CREATE SESSION en Oracle, y que la red permita el acceso al puerto correspondiente.

Permisos a nivel sistema y a nivel objeto

En los sistemas gestores de bases de datos existen distintos tipos de permisos que determinan qué acciones puede realizar un usuario. Estos permisos se dividen principalmente en privilegios a nivel sistema y privilegios a nivel objeto.

Los privilegios a nivel sistema permiten ejecutar acciones administrativas generales que afectan a toda la base de datos. Estos permisos incluyen operaciones como

crear usuarios, crear tablas, eliminar objetos o incluso administrar la base completa. Por ejemplo, el privilegio CREATE USER permite crear nuevas cuentas, mientras que CREATE TABLE permite crear tablas en el esquema del usuario. Estos privilegios son amplios y tienen un impacto global.

Por otro lado, los privilegios a nivel objeto permiten realizar operaciones específicas sobre objetos concretos dentro de la base de datos. Estos objetos pueden ser tablas, vistas, procedimientos almacenados, funciones o secuencias. Entre los permisos más comunes se encuentran SELECT (consultar datos), INSERT (insertar registros), UPDATE (modificar datos) y DELETE (eliminar registros). A diferencia de los privilegios de sistema, estos solo afectan al objeto específico sobre el cual se conceden.

¿Cómo dar o quitar permisos?

Para administrar los permisos en una base de datos se utilizan principalmente dos comandos del lenguaje SQL: GRANT y REVOKE.

El comando GRANT se utiliza para otorgar permisos a un usuario o rol. Mediante este comando se puede especificar qué privilegio se concede y sobre qué objeto o acción aplica. Por ejemplo, se puede otorgar permiso para consultar una tabla específica o para crear tablas dentro de la base de datos.

Por otro lado, el comando REVOKE se utiliza para retirar permisos previamente otorgados. Este comando elimina la autorización que tenía un usuario o rol para realizar determinada acción. La correcta administración de estos comandos es fundamental para garantizar la seguridad y el control de acceso dentro del sistema.

Diferencia entre usuario y rol

En una base de datos, un usuario es una cuenta individual que permite a una persona o aplicación autenticarse en el sistema. El usuario posee un nombre y una contraseña, puede conectarse a la base de datos y puede ser propietario de objetos

como tablas o vistas. Además, puede recibir permisos directamente o a través de roles.

Un rol, en cambio, es un conjunto de permisos agrupados que se asignan a uno o varios usuarios. Los roles no se utilizan para autenticarse, sino para facilitar la administración de privilegios. En lugar de asignar permisos uno por uno a cada usuario, se pueden crear roles con permisos específicos y luego asignarlos a los usuarios correspondientes. Esto simplifica la gestión y mejora la organización del control de acceso.

En resumen, el usuario es la entidad que se conecta al sistema, mientras que el rol es un mecanismo que agrupa permisos para asignarlos de manera más eficiente.

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*, 6th ed. New York, NY, USA: McGraw-Hill, 2011.

[3] Oracle Corporation, “Database Security Guide,” Oracle Documentation, 2023. [Online]. Available: https://docs.oracle.com

[4] P. Rob and C. Coronel, *Database Systems: Design, Implementation, and Management*, 12th ed. Boston, MA, USA: Cengage Learning, 2019.