



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE INGENIERÍA

BASE DE DATOS
PRIVILEGIOS EN POSTGRESQL

Análisis de la base de datos

INTEGRANTE
CRUZ VARGAS EMILIO

PROFESOR
ING. FERNANDO ARREOLA FRANCO

GRUPO

Índice

1. El rol predeterminado	2
2. Privilegios	2
3. Referencias	3

1. El rol predeterminado

Al empezar una instalación de PostgreSQL, el manejador de base de datos relacionales se conoce como el rol predeterminado o "superusuario" llamado "postgres". También es llamado "manejador" tiene varios privilegios especiales que le permiten administrar y controlar el sistema de bases de datos. Como se mencionó, este rol sirve para representar un usuario o un grupo de usuarios, y ayudan a determinar quiénes pueden acceder a la base de datos y qué operaciones pueden realizar. Esto es crucial para la seguridad e integridad de la información. Entre los roles más conocidos están:

1. **Superusuario (Superuser):** Tiene todos los privilegios en todas las bases de datos del sistema y puede realizar cualquier operación.
2. **Rol de base de datos (Database Role):** Es un rol de usuario regular que tiene ciertos privilegios en las bases de datos a las que se le asigna.
3. **Rol de inicio de sesión (Login Role):** Puede autenticarse en el servidor. Este rol puede ser un superusuario o un rol de base de datos, y está destinado a permitir el acceso de usuarios a la base de datos.

Hay más roles muy importantes para la correcta administración de los permisos y accesos en la base de datos, pero la intención es entender los privilegios que tiene el rol "postgres".

2. Privilegios

Lo primero que se debe entender antes de hablar de los privilegios es a qué se les llama privilegios en el contexto de las bases de datos. Estos son derechos o permisos otorgados a un rol para realizar ciertas acciones específicas dentro de la base de datos. Algunos de los más importantes son:

1. **SELECT:** Permite al usuario recuperar datos de una tabla.
2. **INSERT:** Permite al usuario agregar nuevos registros a la tabla.
3. **UPDATE:** Permite al usuario modificar los valores existentes y actualizarlos.
4. **DELETE:** Permite al usuario eliminar registros de las tablas.
5. **CREATE:** Permite al usuario crear nuevos objetos, como tablas.
6. **ALTER:** Permite al usuario modificar la estructura de un objeto ya existente.
7. **DROP:** Permite al usuario eliminar objetos, como eliminar una tabla.
8. **GRANT:** Permite al usuario otorgar privilegios a otros usuarios.
9. **REVOKE:** Permite al usuario revocar privilegios previamente asignados a un usuario.
10. **USAGE:** Permite al usuario utilizar un esquema o una secuencia.

Los privilegios se otorgan y gestionan para garantizar que los usuarios tengan el acceso adecuado a los datos y las funciones, manteniendo la seguridad y la integridad de la base de datos.

3. Referencias

1. IBM documentation. (s. f.). <https://www.ibm.com/docs/es/bpm/8.6.0?topic=privileges-sql-server-database>
2. Privilegios para geodatabases en SQL Server—ArcMap — Documentación. (s. f.). <https://desktop.arcgis.com/es/arcmap/latest/manage-data/gdbs-in-sql-server/privileges-sqlserver.htm>