Síntesis conceptual

Grado: Administración de sistemas informáticos en red
Asignatura: Administración de Sistemas Gestores de Bases de Datos
Unidad: 3. Gestión de usuarios y permisos

Resumen

- La gestión de usuarios y permisos es común a todos los SGBD multiusuario y engloba la autenticación de usuarios, la cual se puede delegar bajo un sistema operativo distribuido, aunque no exime de la gestión en el SGDB.

- No es lo mismo la autenticación de una aplicación que accede a la base de datos que la autenticación sobre el SGBD y no siempre es necesario crear un usuario de la base de datos por cada usuario de la aplicación, especialmente si la aplicación está siendo utilizada por un gran número de usuarios con el mismo nivel de acceso a los datos. No obstante, es importante disponer de mecanismos que nos permitan auditar qué usuarios están haciendo uso del SGBD.

- Los roles nos permiten crear múltiples usuarios con determinados privilegios.

- El uso de perfiles nos va a permitir limitar el acceso a los recursos del sistema, que además también nos permiten definir políticas de seguridad en cuanto a autenticación.

- Usuarios, roles, permisos y perfiles pueden ser definidos tanto a nivel global como a nivel local (PDB), siguiendo un orden jerárquico.

- Hemos podido comprobar que la gestión de usuarios y permisos, así como la definición de esquemas externos son fundamentales para garantizar la confidencialidad de la información. Debemos asegurarnos de que solamente acceden a la información aquellos usuarios autorizados para ello.

- Tenemos que distinguir dos tipos de permisos: de sistema (acceso, administración, operaciones sobre el SGBD, etc. y permisos sobre los objetos (datos accesibles, modificación lectura, etc.).

- Mediante los esquemas externos, podemos garantizar una independencia lógica de los datos, utilizando mecanismos como los sinónimos y las vistas.

- Hemos aprendido como acceder a las vistas del diccionario de datos.

Conceptos fundamentales

- **Usuario**: Todos los SGBD multiusuario, incorporan un mecanismo interno de autenticación a través de usuarios, los cuales tendrán o no ciertas limitaciones tanto a nivel de administración (operaciones sobre el SGBD) como de acceso a la información (acceso a los datos). Los comandos SQL habituales son CREATE, ALTER ó DROP USER.

- **Permisos:** Van a determinar qué tipo de operaciones son las que pueden realizar los usuarios, tanto sobre el sistema como sobre los objetos de las bases de datos. Los comandos SQL para la gestión de permisos son GRANT y REVOKE.

- **Roles:** Son conjuntos de privilegios que permiten generar o modificar usuarios existentes con un mismo grupo de privilegios. Existen unos determinados roles por defecto, pero también se pueden crear o modificar roles, así como agregar o eliminar permisos asignados a cada rol.

- **Perfiles:** Los perfiles nos permiten limitar el acceso a los recursos del sistema, así como gestionar políticas de seguridad referentes a la autenticación de usuarios (fortaleza de la contraseña, expiración, número máximo de intentos de acceso, etc.)

- **Vistas:** Es una representación de datos almacenados en una tabla o conjunto de tablas. No se almacena la información como tal, sino la consulta. Hay tres tipos de vistas, horizontales, verticales o mixtas y permiten liminar la cantidad de información accesible para determinados usuarios.

- **Sinónimos:** Son accesos directos (enlaces) a determinados objetos de las bases de datos. Tanto las vistas como los sinónimos, nos permiten definir esquemas externos sobre los datos, aportando seguridad, facilidad de uso y homogeneidad.

Procesos fundamentales

Creación y configuración de usuarios.
Definición de un esquema externo de ejemplo mediante vistas y sinónimos.
Estructura de las vistas del diccionario de datos para el usuario SYS.