Seguridad en las BBDD

Bernat Costa

Ser Rancios

En seguridad, no vamos a hacer amigos. Seamos rancios. Seamos tacaños con los permisos

Si nos piden permisos para que un usuario consulte una tabla de una BBDD, no le vamos a dar las claves de admin de nuestro motor de BBDD.

Usuarios y logins

- SQL Server diferencia los logins para conectarte de los usuarios a los que damos permiso en una bbdd en concreto.
  - Crear login (usuario clave)
    - **CREATE LOGIN** alumno **WITH PASSWORD** = '12345Ab##'
  - Añadir crear usuario para añadirlo a los permisos de una bbdd
    - USE Arepazo
    - **CREATE USER** alu **FOR LOGIN** alumno

Añadir y revocar permisos

GRANT Y REVOKE

Los permisos se añaden sobre los usuarios. Primero hay que añadir el usuario a la bbdd, y luego podemos darle el permiso que queramos

- Select/insert/update/Delete (para poder ejecutar consultas DML)
- ALTER -> modificar nombres, eliminar campos, añadir campos...
- EXECUTE -> Para poder ejecutar un procedimiento/funcion

ámbito de los permisos

- Los permisos, los podremos dar por tabla, vista, sinónimo, bbdd entera...
- Ejemplo: Podemos crear un usuario en la BBDD Arepazo, que sólo pueda ver el menú. (dar al usuario alu, el permiso de select en la tabla menu)
  - USE arepazo
  - **GRANT SELECT ON OBJECT::menu TO alu;**

Que son las vistas y los sinonimos?

- Una vista es una forma de nombrar una consulta. Podemos hacer una vista especial para darle permisos a un usuario sobre algunos datos de nuestra tabla.
  - **CREATE VIEW** menusimplificado
    AS
    SELECT id,nombre,descripcion FROM menu
- Los sinónimos es darle otro nombre a una tabla
  - **CREATE SYNONYM** m **FOR** Menu

Roles de usuario

- Igual que en el Active Directory de Windows, podemos agrupar a usuarios por grupos y asignar permisos a ese grupo.
- En SQL SERVER, los grupos se llaman ROLES
- Para crearlos usaremos CREATE ROLE desde una BBDD
  - USE arepazo
    CREATE ROLE developers
    GRANT SELECT clientes to developers
- Para añadir a un usuario a un rol:
  - **ALTER ROLE** developers **ADD MEMBER** alu
    ;

Permisos Arepazo 1

Sobre la BBDD del Arepazo y SOLO CON INSTRUCCIONES SQL:

1) Crea un grupo cocineros que tenga permisos de select sobre las tablas menu, recetas,ingredientes.
   - Crea un usuario y añadelo al grupo cocineros
   - Logueate con ese usuario y comprueba que solo puedes consultar esas tablas. (intenta un select a otra tabla y un delete sobre la tabla menu)
2) Crea un grupo Camareros, con permisos de lectura sobre la tabla menu. Añade también permisos de para poder ver y añadir y modificar las tablas de pedidos y pedidoslinea. No debe tener permisos para borrar registros.
   - Añade un usuario al grupo camareros y comprueba que efectivamente puedes añadir pedidos, pero no borrarlos.

Permisos Arepazo 2

Sobre la BBDD del Arepazo y SOLO CON INSTRUCCIONES SQL:

1. Añade un usuario Jefe, que los mismos permisos que los cocineros y los camareros, pero que además pueda borrar pedidos y pueda modificar el menú a su antojo (añadir, borrar y modificar).
   - Logueate con el usuario jefe y añade un elemento al menu, borra un pedido y modifica aumenta el precio de todo el menú un 5%.
2. Crea un usuario invitado con permisos de lectura sobre una vista de la tabla menú donde en lugar de la foreingkey de tipo y categoria, vea el nombre del tipo y la categoria.
   - Logueate como invitado, y comprueba que no puedes ver nada más que esa vista.

Ejercicio

- Crea un usuario en el arepazo sin permisos para select ni update ni insert ni delete.
- Crea un procedimiento que haga una select sobre el menu.
- Dale permisos de execute al usuario en ese procedimiento
- Logueate con ese usuario e intenta hacer un select al menu. Luego intenta ejecutar el procedimiento.

Ejercicio Documentación

Documenta cómo hacer los ejercicios anteriores desde el entorno gráfico del SQL SERVER MANAGEMENT STUDIO

Haz un PDF con esa documentación.