Tema 3
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.

SQL Server

Usuarios y logins

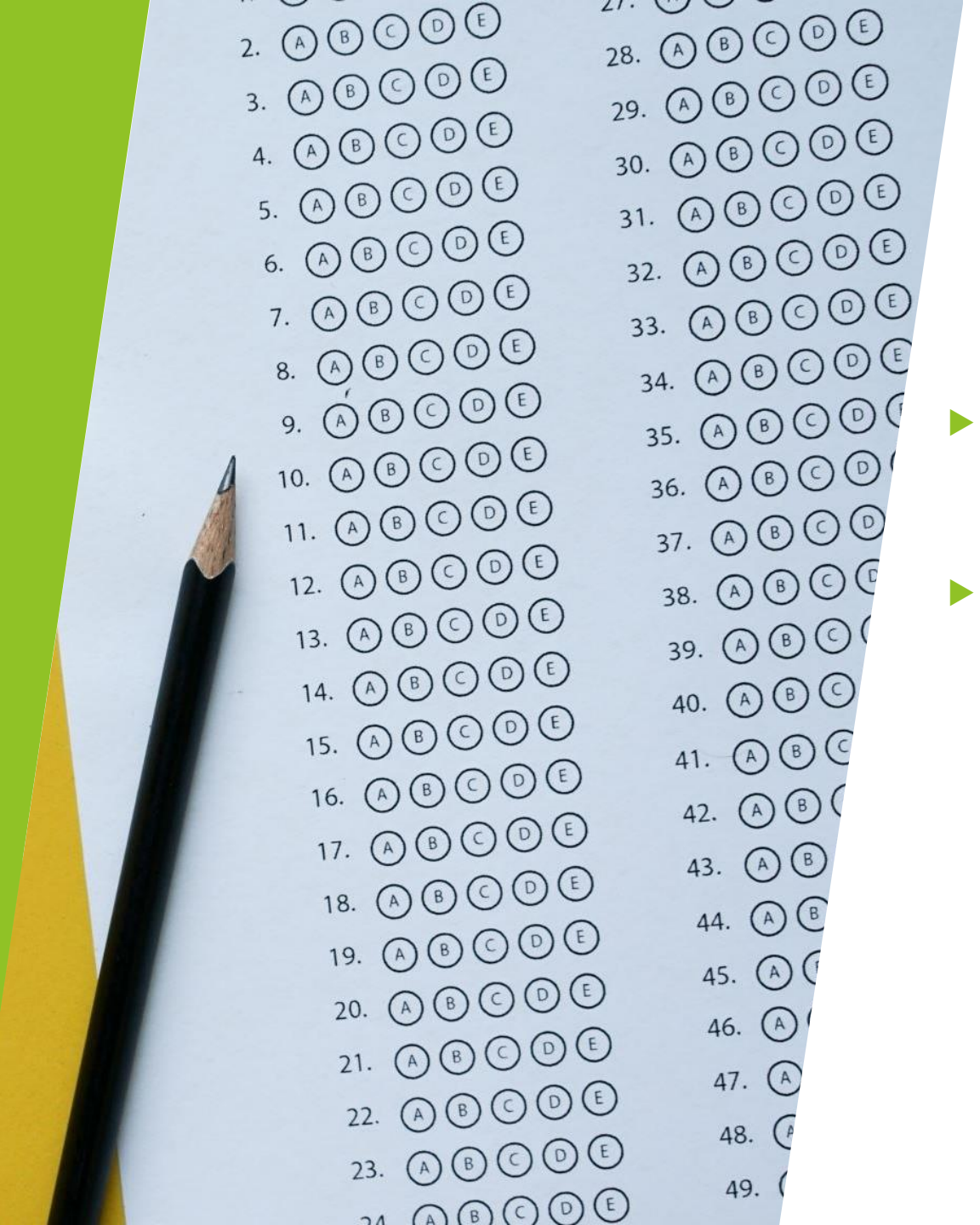
- SQL Server diferencia los logins para conectarte de los usuarios a los que damos permiso en una bbdd en concreto.
  - Crear login (usuario clave)
    - **CREATE LOGIN** alumno **WITH PASSWORD** = '12345Ab##'
  - Añadir crear usuario para añadirlo a los permisos de una bbdd
    - USE Arepazo
    - **CREATE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

¿Qué 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 ;

TABLAS CON LA INFORMACIÓN DE LOS USUARIOS Y LOGINS

- SELECT * FROM master.sys.syslogins
  - En la BBDD Master, se guarda la información de los logins. En esta información por ejemplo, podriamos ver las fechas de creación, modificación y acceso de un login.
- SELECT * FROM sys.sysusers u
  - En cada BBDD, hay una tabla con los usuarios de dicha bbdd. Donde podremos ver la info de esos usuarios
- SELECT * FROM arepazo.sys.sysusers u
  INNER JOIN master.sys.syslogins l ON u.sid=l.sid
  - Consulta para ver los logins y los usuarios de la BBDD arepazo.

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:

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%.

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 Documentación

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

Haz un PDF con esa documentación.

Autenticación con Active Directory

- SQL Server nos permite crear logins con autenticación de Windows.
- Si tenemos un Active Directory, podremos dar permisos a los usuarios de nuestro AD o usuarios de nuestro Windows (En el que esté instalado el SQL Server).
- El login desde el cliente SSMS será con la opción de Windows Autentication.

Seguridad en Azure

- En azure, a parte de la seguridad del usuario como en cualquier SQL, tenemos un firewall que nos permitirá añadir una capa de seguridad anterior.
- Podremos configurar desde que IPs nos conectamos
- Podremos también ver la actividad de nuestra BBDD en un log de actividad para ver "cosas raras".

Ejercicio

Crea un login y un usuario en la bbdd del arepazo con permisos para consultas y modificaciones de datos (select,insert,delete,update) (usa los roles ya prefijados de writer y reader) con tu usuario de windows.

Dale permisos al usuario de windows de algun compañer@ de clase. Dile que se conecte y conéctate tu a su base de datos. Debéis asignarle el rol de camarero a ese usuario de un compañer@.

Ejercicio

Ves a azure, y añade alguna regla en el firewall de algún servidor de BBDD.

Bichera el log de actividad e intenta entender lo que ves.

MySQL o MariaDB

El host en el usuario

- La creación de usuarios en los sistemas MySQL o MariaDB es muy parecido a SQL Server, pero con una importante diferencia.
- **A cada usuario, le asignamos una IP desde la que puede conectarse.**
- A este usuario le llamamos host, y en la tabla mysql.users podemos verlos
  - Select * from mysql.users
- Podremos usar el comodín % para decirle que ese usuario se puede conectar desde cualquier máquina.
- También podremos usar la palabra localhost para indicar que solo permitiremos accesos locales.

Ejercio MySQL

- Crea una bbdd con una tabla en MySQL o MariaDb con Docker
- Crea un usuario con host localhost que pueda acceder a la tabla
- Crea otro usuario con host % que NO pueda acceder
- Accede desde el "infierno" con docker exec –it /bin/sh nombredelcotenedor
  - Una vez dentro, del contenedor lanza mysql –u nombreusuario –p
- Comprueba la diferencia entre los permisos del mismo usuario desde localhost y desde fuera con el cliente que quieras.