Administración de Bases de Datos (2023-24, Grado en Ingeniería Informática. Plan 2010 Todos los grupos y Grado en Matemáticas + Ingeniería Informática. Plan 2019 Todos los grupos)

SEGURIDAD

Pildora de conocimiento:: SEGURIDAD

Esquema del ejercicio

Debes conocer cómo crear usuarios y otorgarles permisos.

Vamos a trabajar accediendo a diferentes esquemas y dándoles permisos.

Debes escribir las instrucciones y preguntas en un script SQL y entregarlo en la tarea correspondiente. Utiliza comentarios para explicar todo lo que quieras y para responder a las preguntas de forma razonada.

Ten siempre en una ventana del navegador la referencia de SQL que puedes encontrar en el enlace proporcionado en el cv.

Necesitarás ...

Conceptos sobre usuarios y permisos.

Cómo crear un tablespace.

1. Conéctate a la base de datos como system.
2. Si tienes un problema de caducidad del password, utiliza el comando `password` (Se aconseja actualizar la contraseña sin cambiarla, para no tener problemas posteriormente de olvido. Por supuesto, esta recomendación solo es válida en un sistema de pruebas, **NUNCA EN PRODUCCIÓN**).
3. Comprueba que existe un tablespace denominado TS_LIFEFIT. Si no es así, créalo donde quieras. Que sea de 10M con el nombre de fichero de datos que quieras y autoextensible.
4. Crea un perfil denominado PERF_ADMINISTRATIVO con 3 intentos para bloquear la cuenta y que se desconecte después de 5 minutos de inactividad
5. Crea un perfil denominado PERF_USUARIO con 4 sesiones por usuario y con una password que caduca cada 30 días.
6. Asegúrate de que las limitaciones de recursos serán efectivas sin problemas. Y por supuesto, contesta a esta pregunta en tu script comentando cómo te has asegurado.
7. Crea un role R_ADMINISTRADOR_SUPER con permiso para conectarse y crear tablas.
8. Crea dos usuarios denominados USUARIO1 y USUARIO2 con perfil PERF_ADMINISTRATIVO y contraseña *usuario*. Otórgales el ROLE R_ADMINISTRADOR_SUPER. Asígneles Quota de 1 MB en el tablespace TS_LIFEFIT. Haz que éste sea un tablespace por defecto.
9. **En ambos** usuarios crear la tabla TABLA2:
   ```
   CREATE TABLE TABLA2
    (  CODIGO NUMBER   ) ;
   ```
10. Crea el procedimiento USUARIO1.PR_INSERTA_TABLA2. Como aún no hemos visto procedimientos en ORACLE, simplemente haz un copia y pega de lo siguiente (la barra final debe escribirse también):
    ```
    CREATE OR REPLACE PROCEDURE USUARIO1.PR_INSERTA_TABLA2 (
                              P_CODIGO IN NUMBER) AS
    BEGIN
        INSERT INTO TABLA2 VALUES (P_CODIGO);
    END PR_INSERTA_TABLA2;
    /
    ```
11. Conéctate como USUARIO1 y Ejecútalo. ¿Funciona?. Utiliza la instrucción `exec nombre_procedimiento(param)`; CONSEJO: Utiliza SQLPlus si no quieres crear otra conexión para el usuario en SQL Developer. Conocer SQLPlus es buena idea, porque en algunos entornos solo encontrarás el terminal SQLPlus de Oracle.
12. Otórgale permisos a USUARIO2 para ejecutarlo
13. Conéctate como **USUARIO2** y Ejecútalo. ¿Funciona? No olvides confirmar los cambios (commit)
14. En este último caso ¿dónde se inserta el dato en la tabla de USUARIO1 o en la de USUARIO2? ¿Por qué?
15. Cambiar el procedimiento para que el INSERT lo haga desde un EXECUTE IMMEDIATE. Es decir, vuelve a crear el procedimiento según vimos en el punto anterior pero sustituyendo la linea correspondiente al INSERT por `execute immediate 'INSERT INTO TABLA2 VALUES ('||P_CODIGO||')';`
16. Ejecutar desde USUARIO1. ¿Funciona?
17. Ejecutar desde USUARIO2. ¿Funciona?
18. Crear otro procedimiento en USUARIO1:
    ```
    CREATE OR REPLACE PROCEDURE PR_CREA_TABLA (
      P_TABLA IN VARCHAR2, P_ATRIBUTO IN VARCHAR2) AS
    BEGIN
      EXECUTE IMMEDIATE 'CREATE TABLE '||P_TABLA||'('||P_ATRIBUTO||' NUMBER(9))';
    END PR_CREA_TABLA;
    /
    ```
19. Ejecutar desde USUARIO1. ¿Funciona?¿Por qué?
20. Asignemos permisos explícitos (y no a través de un rol como está ahora) de creación de tablas al USUARIO1. Asignar permisos de ejecución sobre el procedimiento anterior al USUARIO2.
21. Ejecutar desde USUARIO2. ¿Funciona?¿Por qué? Piensa en los parámetros con los que se invoca.
22. Vamos ahora a comprobar cómo está la instalación de ORACLE que tenemos delante. En primer lugar, en una configuración óptima deberíamos conocer cuales son las cuentas que aún tienen su password por defecto (lo cual es una mala práctica desde el punto de vista de seguridad). Consulta para ello la vista de diccionario DBA_USERS_WITH_DEFPWD. Ahora, responde: ¿por qué hay tantas cuentas? ¿tan insegura es ORACLE tras la instalación? PISTA: Utiliza esa vista en combinación con otras que te permita estudiar el estado (si se pueden conectar, si están abiertas o bloqueadas, etc.) de esas cuentas.
23. Sabemos que existe un profile por defecto para la creación usuarios. Vamos a modificarlo de manera que todos los usuarios cumplan una política mínima para la gestión de contraseñas al ser creados por defecto.

    - En primer lugar consulta cuales son los parámetros existentes del profile por defecto (la vista DBA_PROFILES puede ayudarte). Cuales son?
    - Cambia el número de logins fallidos a 4 y el tiempo de gracia a 5 días.
    - Cambia el perfil del usuario1 al perfil por defecto y haz 5 logins fallidos. ¿Que ocurre la quinta vez? Para responder interpreta bien los mensajes que recibes.
    - Desbloquea la cuenta (alter user...)

- A pesar de que hayamos cambiado el parámetro de failed_login_attempts, como habrás visto, es posible que antes, aunque el usuario no se bloquee, si nos eche de la sesión. Si consultamos el parámetro de inicialización sec_max_failed_login_attempts (show parameter...) aparece un valor menor (si no lo has cambiado antes). Significan por tanto diferentes cosas. ¿Para qué es útil cada uno?
- Investiga si existe una forma de "quitar" los perfiles que hemos creado al principio. ¿Se puede hacer con todos los perfiles de oracle?

Una última pregunta. Algunos parámetros de inicialización son dinámicos, y otros estáticos. ¿Cual es la diferencia entre ellos?

Si has llegado hasta aquí..ENHORABUENA!!

Última modificación: viernes, 1 de marzo de 2024, 13:32

◄ Foro para las prácticas de seguridad

Saltar a...

Entrega de la práctica de seguridad (Grupo A1) ►