Universidad Nacional Autónoma de México
Facultad de Ciencias

Fundamentos de Bases de Datos

Práctica 8

Creación y Manejo de Usuarios (Privilegios y Roles)

Autor: Arroyo Martínez Erick Daniel

Introducción

El manejo de usuarios y permisos es una parte fundamental en la administración de bases de datos, ya que garantiza la seguridad y el acceso controlado a los datos. En esta práctica, aprenderás a crear usuarios en un sistema de gestión de bases de datos (SGBD) y a asignarles roles y permisos específicos sobre las tablas, consultas, y otras operaciones del esquema que hemos utilizado previamente en las prácticas anteriores.

Trabajarás con la creación y administración de roles que simplifican la gestión de permisos, permitiendo que varios usuarios compartan permisos de acuerdo con sus responsabilidades. Además, explorarás cómo revocar permisos cuando sea necesario para mantener la integridad y seguridad de la base de datos.

Nota: `Si bien no podemos crear usuarios o roles en ciertos entornos como Oracle Live SQL debido a limitaciones de privilegios, esta práctica asume que estás trabajando en un entorno donde tienes privilegios suficientes, como una instalación local o un entorno de producción controlado.`

Objetivos

- Crear usuarios en una base de datos relacional y asignarles permisos específicos sobre distintas entidades del esquema proporcionado.
- Asignar y manejar roles para facilitar la gestión de permisos a múltiples usuarios.
- Controlar el acceso de los usuarios a tablas, consultas y transacciones, limitando o permitiendo las operaciones que pueden realizar.
- Revocar permisos para usuarios específicos o roles, manteniendo la seguridad y la integridad del sistema.
- Garantizar que las transacciones y acciones realizadas por diferentes usuarios mantengan la consistencia y seguridad de la base de datos, utilizando los conceptos de privilegios y roles.

Especificaciones de Desarrollo

En esta continuación de la práctica anterior, se creará y gestionará el acceso de dos usuarios a la base de datos, donde cada uno tendrá diferentes niveles de privilegios. Uno de ellos será capaz de ejecutar los procedimientos almacenados (las transacciones diseñadas previamente) y el otro solo podrá realizar consultas básicas (`SELECT`) sobre las tablas. El propósito es reforzar la seguridad del sistema de base de datos a través de la asignación controlada de privilegios.

Creación de Usuarios

- `user_manager`: Este usuario tendrá los permisos necesarios para ejecutar las transacciones diseñadas en la práctica anterior. Podrá modificar, insertar, y ejecutar cualquier procedimiento almacenado en la base de datos.
- `user_viewer`: Este usuario solo tendrá permisos para realizar consultas SELECT sobre las tablas de la base de datos. No podrá modificar, insertar, o ejecutar procedimientos almacenados.

`Nota:` Los usuarios deben ser creados con una contraseña segura y, si el entorno lo permite, debe asignarles una política de expiración de contraseña distinta a cada usuario.

Asignación de Privilegios

- `user_manager debe tener los siguientes permisos:`
  - Permisos para ejecutar procedimientos almacenados (transacciones).
  - Permisos para realizar operaciones `INSERT`, `UPDATE`, y `DELETE` en las tablas involucradas en las transacciones.
  - Acceso completo a todas las tablas y a los índices creados.
  - Permisos para manejar transacciones.
- `user_viewer debe tener los siguientes permisos`
  - Permisos solo de lectura (SELECT) sobre todas las tablas en la base de datos.
  - Sin permisos para modificar datos o ejecutar procedimientos almacenados.

Configuración de Privilegios por Roles

Para cada usuario, utiliza la creación y asignación de roles, de modo que, se llegue al mismo estado que el paso anterior. Además, debes designar estos roles como predeterminados cuando los usuarios inicien sesión.

Entregables

- Archivo `.sql` de la creación de usuarios, pruebas de privilegios y comentarios.
- El archivo debe además debe exhibir el resultado de realizar pruebas de **DDL** y **DML**, así como la llamada a procedimientos.
- Explica brevemente la relación entre roles y privilegios.
- Los comentarios deben mostrar el error, la razón del mismo, cómo corregirlo (o evitarlo) y argumentación respecto impacto tiene esto en la seguridad del esquema, así como explicar en que contextos es adecuado designar los permisos solicitados a usuarios (de ser necesario, argumentar la asignación de política de expiración).

`Nota: Se espera que el script estregado este diseñado por bloques sobre el esquema, es decir, para la revisión de su implementación deberán entregar un script comentado y en orden de ejecución con el objetivo de que el evaluador solo tenga que ejecutar los bloques en secuencia, si por alguna razón surge un error, entonces no se evaluará el trabajo hasta que sea corregido (solo se admiten errores de denegación de operaciones por privilegios), por lo que se les sugiere verificar antes de entregar.`

Importante

La práctica se centra en la creación y administración de usuarios, roles y privilegios en MySQL, fundamentales para el control de acceso y la seguridad en sistemas de bases de datos. Aunque el alcance es relativamente más corto que el de los trabajos previos, esto no disminuye la importancia de los temas abordados. De hecho, dado que el ejercicio está diseñado para poner a prueba la comprensión y aplicación de conceptos críticos, se evaluará con un mayor rigor.

La concisión de las especificaciones fomenta un enfoque en la precisión y el razonamiento crítico, donde los estudiantes deben discernir y justificar sus elecciones de diseño y configuración de privilegios. Al dejar margen para la interpretación, se espera que los estudiantes opten por soluciones óptimas que respondan al contexto del esquema y a las mejores prácticas de seguridad en la administración de bases de datos. De esta manera, los participantes no solo demostrarán su habilidad técnica, sino también su capacidad para argumentar y defender sus implementaciones.

La evaluación incluirá tanto la correcta implementación de los usuarios y permisos como la calidad de la justificación proporcionada para cada elección. Este enfoque exigente asegura que los estudiantes no solo realicen las tareas de manera funcional, sino que también demuestren un entendimiento profundo de los principios subyacentes a una gestión segura y eficiente de los recursos en MySQL.

Rúbrica de Evaluación

Criterio	**Puntos**
Creación de usuarios	25 %
Configuración de privilegios	20 %
Creación y Configuración de Roles a Usuarios	20 %
Pruebas de privilegios	10 %
Argumentación de Implementación	25 %
Política de Expiración	+10 %

Recursos

- Live SQL
- SQL Language Reference
- SQL Tutorial
- mockaroo
- MySQL Documentation