Sistemas de Bases de Datos 2

2024

Ing. Luis Alberto Arias Solórzano

Unidad 4

Seguridad

Limitaciones de la autorización SQL

- Las normas SQL actuales de autorización tienen algunas deficiencias. Por ejemplo, supóngase que se desea que todos los estudiantes sean capaces de ver sus propias notas, pero no las del resto. La autorización debe estar en el nivel de las tuplas, lo cual no es posible en los estándares de autorización de SQL. Más aún, con el crecimiento de Web, los accesos a bases de datos vienen principalmente de los servidores de aplicaciones Web. Los usuarios finales puede que no tengan identificadores de usuario individuales en la base de datos y realmente puede que haya sólo un único identificador de usuario en la base de datos que corresponda a todos los usuarios del servidor de aplicaciones.

- La tarea de la autorización recae entonces sobre el servidor de aplicaciones; el esquema completo de autorización de SQL se omite. El beneficio es que la aplicación puede implementar las autorizaciones de grano fino, como las de las tuplas individuales. Estos son los problemas:

1. El código para comprobar la autorización se entremezcla con el resto del código de la aplicación.
2. La implementación de la autorización mediante código de aplicación, en lugar de realizarlo declarativamente con SQL, hace que sea difícil asegurar la ausencia de agujeros de seguridad. debido a un descuido, uno de los programas de aplicación podría no comprobar la autorización, permitiendo el acceso de usuarios no autorizados a datos confidenciales. La verificación de que todos los programas de aplicación realizan todas las comprobaciones de autorización implica la lectura de todo el código del servidor de la aplicación, una tarea formidable en un gran sistema.

Autorizaciones

Los usuarios pueden tener varios tipos de autorización para diferentes partes de la base de datos. Entre ellas están las siguientes:

- **La autorización de lectura** permite la lectura de los datos, pero no su modificación.
- **La autorización de inserción** permite la inserción de datos nuevos, pero no la modificación de los existentes.
- **La autorización de actualización** permite la modificación de los datos, pero no su borrado.
- **La autorización de borrado** permite el borrado de los datos.

Autorizaciones

- Además de estas formas de autorización para el acceso a los datos, los usuarios pueden recibir autorización para modificar el esquema de la base de datos:
  - **La autorización de índices** permite la creación y borrado de índices.
  - **La autorización de recursos** permite la creación de relaciones nuevas.
  - **La autorización de alteración** permite el añadido o el borrado de atributos de las relaciones.
  - **La autorización de eliminación** permite el borrado de relaciones.

- Las autorizaciones de **eliminación** y de **borrado** se diferencian en que la autorización de borrado sólo permite el borrado de tuplas. Si un usuario borra todas las tuplas de una relación, la relación sigue existiendo, pero está vacía. Si se elimina una relación, deja de existir. La capacidad de crear nuevas relaciones queda regulada mediante la autorización de **recursos**. El usuario con la autorización de **recursos** que crea una relación nueva recibe automáticamente todos los privilegios sobre la misma.

Seguridad

Otras características

- El creador de un objeto (relación, vista o papel) obtiene todos los privilegios sobre el objeto, incluyendo el privilegio de conceder privilegios a otros.

- La norma SQL especifica un mecanismo primitivo de autorización para el esquema de la base de datos: sólo el propietario del esquema puede ejecutar cualquier modificación del esquema. Por tanto, las modificaciones del esquema —como la creación o borrado de las relaciones, la adición o eliminación de atributos de las relaciones y la adición o eliminación de índices— sólo pueden ser ejecutadas por el propietario del mismo.

- Varias implementaciones de las bases de datos tienen mecanismos de autorización más potentes para los esquemas de las bases de datos, parecidos a los discutidos anteriormente, pero esos mecanismos no son estándar.

Registros de Auditoría

Un registro de auditoría es un archivo o base de datos especial en el que el sistema lleva automáticamente la cuenta de todas las operaciones realizadas por los usuarios sobre los datos normales. En algunos sistemas el registro de auditoria puede estar integrado físicamente con la bitácora de recuperación, mientras que en otros, los dos pueden ser distintos pero los usuarios deben —de cualquier forma— tener la posibilidad de consultar el registro de auditoría usando su lenguaje de consulta normal (por supuesto, siempre y cuando tengan autorización). Un registro de auditoría típico podría contener la siguiente información:

- Petición (texto de origen)
- Terminal desde la que se llamó a la operación
- Usuario que llamó a la operación
- Fecha y hora de la operación
- Varrels, tupias, atributos afectados
- Valores antiguos Valores nuevos

El simple hecho de mantener un registro de auditoría puede ser suficiente para disuadir en algunas situaciones a un posible infiltrador.

Virtual Private Databases

- Una base de datos privada o VPD enmascara la información de una base de datos mas grande de tal manera que pareciera que solo una parte de ella existiera, sin necesidad de segregar información en diferentes tablas, esquemas o bases de datos.

- Una aplicación típica es la restricción de sitios, departamentos, individuos, etc. que necesitan operar solamente con sus propios registros y al mismo tiempo permitir usuarios privilegiados tener acceso toda la información.

- Ejemplo: Oracle DBMS, donde la implementación es muy general: tablas pueden ser asociadas con funciones propias de SQL que puedan devolver las consultas propias para el acceso de dicha información. Para este caso SELECT, INSERT, UPDATE y DELETE pueden tener diferentes reglas.

- Las VPD permiten a múltiples usuarios el acceso a un esquema en particular mientras no les permita también el acceso a información que no es relevante para estos usuarios.

Clasificación de datos

Un esquema de clasificación de restricciones

- Clasificamos las restricciones de integridad en general en cuatro grandes categorías: restricciones de tipo (dominio), de atributo, de varrel y de base de datos.

En esencia:

■ Una restricción de *tipo* especifica los valores válidos para un tipo dado. Empleamos "tipo" para referirnos específicamente a un tipo *escalar.*

Por supuesto, los tipos de relación también están sujetos a las restricciones de tipo, pero dichas restricciones son básicamente sólo una consecuencia lógica de las restricciones de tipo que se aplican a los tipos escalares en términos de los cuales esos tipos de relación están (en ú tima instancia) definidos.

Clasificación de datos

- Una restricción de *atributo* especifica el valor válido de un atributo dado.
- Una restricción de *varrel* especifica los valores válidos de una varrel determinada.
- Una restricción de *base de datos* especifica el valor válido de una base de datos dada.

Los tipos comunes de restricciones incluyen las siguientes:

- - NOT NULL
- - UNIQUE
- - CHECK
- - Clave primaria
- - Clave externa (extranjera, foránea)

Gracias