
ORACLE
ACADEMY

Programación de bases de datos con SQL

17-1
Control del Acceso de los Usuarios

ORACLE ACADEMY

Objetivos

En esta lección se abordan los siguientes objetivos:

- Comparar la diferencia entre privilegios de objeto y privilegios del sistema
- Construir los dos comandos necesarios para permitir que un usuario tenga acceso a una base de datos
- Construir y ejecutar una sentencia GRANT… ON …TO para asignar privilegios a objetos de un esquema para otros usuarios y/o a PUBLIC
- Consultar el diccionario de datos para confirmar los privilegios otorgados

Objetivo

- Si comparte una computadora con otros usuarios, ya sea en la escuela o en casa, probablemente otra persona haya visto, cambiado o suprimido algo con lo que haya trabajado.
- ¿No sería fantástico poder controlar los privilegios que otros usuarios tienen a sus archivos personales?
- En el caso de bases de datos, al igual que en la escuela o en casa, la seguridad de los datos es muy importante.
- En esta lección, aprenderá a otorgar o quitar acceso a los objetos de base de datos como un medio para controlar quién puede modificar, suprimir, actualizar, insertar, indexar o hacer referencia a los objetos de base de datos.

Control del Acceso de los Usuarios

- En un entorno de varios usuarios, desea mantener la seguridad del uso y acceso a la base de datos.
- Con la seguridad de la base de datos del servidor de Oracle, puede realizar lo siguiente:
  - Controlar el acceso a la base de datos
  - Proporcionar acceso a objetos específicos en la base de datos
  - Confirmar los privilegios asignados y recibidos en el diccionario de datos de Oracle
  - Crear sinónimos para objetos de bases de datos

Seguridad de la Base de Datos

- La seguridad de la base de datos se puede clasificar en dos categorías:
  - Seguridad del sistema
  - Seguridad de datos
- La seguridad del sistema abarca el acceso a la base de datos en el nivel del sistema, como la creación de usuarios, nombres de usuario y contraseñas, la asignación de espacio en disco a los usuarios y la concesión de los privilegios del sistema que los usuarios pueden llevar a cabo, como crear tablas, vistas y secuencias.
- Existen más de 100 privilegios del sistema distintos.

Seguridad de la Base de Datos

- La seguridad de datos (también denominada seguridad de objetos) está relacionada con los privilegios de objeto que abarca el acceso y el uso de los objetos de base de datos, así como las acciones que los usuarios pueden realizar sobre los objetos.
- Estos privilegios incluyen poder ejecutar sentencias DML.

Privilegios y Esquemas

- Los privilegios son el derecho a ejecutar sentencias SQL determinadas.
- El DBA es un usuario de alto nivel con capacidad para otorgar a los usuarios acceso a la base de datos y sus objetos.
- Los usuarios necesitan privilegios del sistema para obtener acceso a la base de datos.
- Necesitan privilegios de objeto para manipular el contenido de los objetos de la base de datos.
- A los usuarios también se les da el privilegio de otorgar privilegios adicionales a otros usuarios o a los roles, que son grupos con nombres de privilegios relacionados.

Privilegios y Esquemas

- Un esquema es una recopilación de objetos, como tablas, vistas y secuencias.
- El esquema es propiedad de un usuario de base de datos y tiene el mismo nombre que el usuario.
- En este curso, su nombre de esquema es una combinación de su país/estado, escuela, curso y número de alumno.
- Por ejemplo: uswa_skhs_sql01_s22

Seguridad del Sistema

- Este nivel de seguridad abarca el acceso y uso de la base de datos en el nivel del sistema.
- Existen más de 100 privilegios del sistema distintos.
- Los privilegios del sistema, como la capacidad de crear o eliminar usuarios, eliminar tablas o realizar copias de seguridad de tablas, solo los suele tener el DBA.

Seguridad del Sistema

- En esta tabla se muestran algunos de los privilegios del sistema que el DBA normalmente no otorga a otros usuarios.
- ¿Desea que otro usuario pueda para borrar sus tablas?

Privilegio del Sistema	Operaciones Autorizadas
CREATE USER	Los usuarios con privilegios pueden crear otros usuarios de Oracle (privilegio necesario para el rol DBA).
DROP USER	El usuario con privilegios puede borrar otro usuario.
DROP ANY TABLE	El usuario con privilegios puede borrar una tabla en cualquier esquema.
BACKUP ANY TABLE	El usuario con privilegios puede realizar una copia de seguridad de tablas en cualquier esquema con la utilidad de exportación.
SELECT ANY TABLE	El usuario con privilegios puede consultar las tablas, vistas o instantáneas en cualquier esquema.
CREATE ANY TABLE	El usuario con privilegios puede crear una tabla en cualquier esquema.

Privilegios del Sistema

- El DBA crea el usuario mediante la ejecución de la sentenciaCREATE USER.
- El usuario no tiene ningún privilegio en este punto.
- El DBA puede otorgar privilegios necesarios a dicho usuario.
- Sintaxis:

```
CREATE USER user
IDENTIFIED BY password;
```

- Ejemplo:

```
CREATE USER  scott
IDENTIFIED BY ur35scott;
```

Privilegios del Sistema

- Mediante la sentencia ALTER USER, un usuario puede cambiar su contraseña.
- Ejemplo:

```
ALTER USER scott
IDENTIFIED BY imscott35;
```

Los alumnos no podrán probar estos privilegios en APEX, debido a privilegios insuficientes.

Privilegios del Sistema de Usuario

- El DBA utiliza la sentencia GRANT para asignar privilegios del sistema al usuario.
- Estos privilegios del sistema determinan lo que el usuario puede realizar en el nivel de base de datos.
- Una vez que el usuario ha otorgado los privilegios, el usuario puede utilizar estos privilegios inmediatamente.

```
GRANT privilege [, privilege...]
TO user [, user| role, PUBLIC...];
```

```
GRANT  create session, create table, create sequence, create view
TO scott;
```

Privilegios del Sistema de Usuario

- Un usuario debe tener un privilegio CREATE SESSION y un identificador de usuario si debe poder acceder a una base de datos.
- No puede emitir el comando CREATE SESSION en Oracle Application Express; esto se produce de forma automática en segundo plano.

Privilegio del Sistema	Operaciones Autorizadas
CREATE SESSION	Conectar a la base de datos.
CREATE TABLE	Crear tablas en el esquema del usuario.
CREATE SEQUENCE	Crear una secuencia en el esquema del usuario.
CREATE VIEW	Crear una vista en el esquema del usuario.
CREATE PROCEDURE	Crear un paquete, función o procedimiento en el esquema del usuario.

Seguridad de Objetos

- Este nivel de seguridad abarca el acceso y el uso de los objetos de la base de datos así como las acciones que los usuarios puedan realizar en dichos objetos.

Privilegios de Objeto

- Cada objeto tiene un juego determinado de privilegios que se pueden otorgar.
- En la tabla siguiente se muestran los privilegios para varios objetos.

Privilegio de Objeto	Tabla	Ver	Secuencia	Procedimiento
ALTER	X		X	
DELETE	X	X		
EXECUTE				X
INDEX	X	X		
INSERT	X	X		
REFERENCES	X			
SELECT	X	X	X	
UPDATE	X	X		

Privilegios de Objeto

- Es importante tener en cuenta los siguientes cuatro puntos sobre los privilegios de objeto:
  - Los únicos privilegios que se aplican a una secuencia son SELECT y ALTER.
  - Recuerde que una secuencia utiliza ALTER para cambiar las opciones INCREMENT, MAXVALUE, CACHE/NOCACHE o CYCLE/NOCYCLE.
  - La opción START WITH no se puede cambiar mediante ALTER.

Privilegios de Objeto

- Puede otorgar los privilegios UPDATE, REFERENCES e INSERT en columnas individuales de una tabla.
- Por ejemplo:

```
GRANT UPDATE (salary)
  ON employees TO steven_king
```

- Un privilegio SELECT se puede restringir mediante la creación de una vista con un subjuego y otorgamiento del privilegio SELECT solo en la vista.
- No puede otorgar SELECT en columnas individuales.

Privilegios de Objeto

- Un privilegio otorgado en un sinónimo se convierte en un privilegio en la tabla base a la que hace referencia el sinónimo.
- Es decir, un sinónimo es simplemente un nuevo nombre más fácil de utilizar.
- El uso de este nombre para otorgar un privilegio es lo mismo que otorga el privilegio en la propia tabla.

Palabra Clave PUBLIC

- Un propietario de una tabla puede otorgar acceso a todos los usuarios mediante la palabra clave PUBLIC.
- En el segundo ejemplo que se muestra a continuación, se permite a todos los usuarios del sistema consultar datos de la tabla DEPARTMENTS de Alice.

```
GRANT select
ON alice.departments
TO PUBLIC;
```

Palabra Clave PUBLIC

- Si una sentencia no utiliza el nombre completo de un objeto, Oracle Server incluye implícitamente en el nombre de objeto el nombre del usuario (o esquema) actual como prefijo.
- Si el usuario Scott consulta la tabla DEPARTMENTS, por ejemplo, el sistema selecciona en la tabla SCOTT.DEPARTMENTS.
- Si una sentencia no utiliza el nombre completo de un objeto y el usuario actual no es propietario de un objeto con ese nombre, el sistema incluye como prefijo PUBLIC en el nombre de objeto.

Palabra Clave PUBLIC

- Por ejemplo, si el usuario Scott consulta la vista USER_OBJECTS y Scott no es propietario de dicha tabla, el sistema realiza selecciones en la vista del diccionario de datos mediante el sinónimo público PUBLIC.USER_OBJECTS.

Confirmación de Privilegios Otorgados

- Si intenta realizar una operación no autorizada, como la supresión de una fila de una tabla para la que no tiene el privilegio DELETE, el servidor de Oracle no permite que se produzca la operación.
- Si recibe el mensaje de error de Oracle Server "table or view does not exist", es porque ha realizado una de las siguientes acciones:
  - Asignar un nombre a una tabla o vista que no existe
  - Intentar realizar una operación en una tabla o vista para la que no tiene el privilegio adecuado

Privilegios de Visualización

- Puede acceder al diccionario de datos para ver los privilegios que tiene.
- En el gráfico mostrado se describen varias vistas del diccionario de datos.
- Mediante Oracle Application Express Developer, acceda a SQL Workshop, Utilities, Object Reports.
- Los privilegios del usuario se pueden ver en la sección Security Reports.

Privilegios de Visualización

Vista del Diccionario de Datos	Description
ROLE_SYS_PRIVS	Privilegios del sistema otorgados a roles
ROLE_TAB_PRIVS	Privilegios de tabla otorgados a roles
USER_ROLE_PRIVS	Roles a los que puede acceder el usuario
USER_TAB_PRIVS_MADE	Privilegios de objeto otorgados a objetos del usuario
USER_TAB_PRIVS_RECD	Privilegios de objeto otorgados al usuario
USER_COL_PRIVS_MADE	Privilegios de objeto otorgados a columnas de objetos del usuario
USER_COL_PRIVS_RECD	Privilegios de objeto otorgados al usuario en columnas específicas
USER_SYS_PRIVS	Muestra privilegios del sistema otorgados al usuario

Terminología

Entre los términos clave utilizados en esta lección se incluyen:

- Privilegio CREATE SESSION
- Privilegio GRANT
- Privilegios de Objeto
- Seguridad de objetos
- de Objeto
- Privilegio PUBLIC
- Role

Terminología

Entre los términos clave utilizados en esta lección se incluyen:

- Esquema
- Privilegios del Sistema
- Seguridad del sistema

Resumen

En esta lección, debe haber aprendido lo siguiente:

- Comparar la diferencia entre privilegios de objeto y privilegios del sistema
- Construir los dos comandos necesarios para permitir que un usuario tenga acceso a una base de datos
- Construir y ejecutar una sentencia GRANT… ON …TO para asignar privilegios a objetos de un esquema para otros usuarios y/o a PUBLIC
- Consultar el diccionario de datos para confirmar los privilegios otorgados


ORACLE
ACADEMY