
ORACLE
ACADEMY

Programación de bases de datos con SQL

17-2
Creación y Revocación de Privilegios de Objeto

ORACLE ACADEMY

Objetivos

En esta lección se abordan los siguientes objetivos:

- Explicar qué es un ROL y cuáles son sus ventajas
- Crear una sentencia para crear un ROL y OTORGARLE privilegios
- Crear una sentencia GRANT .. ON .. TO.. WITH GRANT OPTION para asignar privilegios a objetos de su esquema para otros usuarios y/o a PUBLIC
- Crear y ejecutar una sentencia para REVOCAR los privilegios de objeto a otros usuarios y/o PUBLIC

Objetivos

En esta lección se abordan los siguientes objetivos:

- Distinción entre Privilegios y Roles
- Explicar el objetivo de un enlace de base de datos

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 esos objetos de base de datos.

Funciones

- Un rol es un grupo con nombre de privilegios relacionados que se pueden otorgar a un usuario.
- Este método facilita la revocación y el mantenimiento de los privilegios.
- Un usuario puede tener acceso a diferentes roles y el mismo rol se puede asignar a diferentes usuarios.
- Los roles normalmente se crean para una aplicación de base de datos.

El uso de roles hace que el proceso de otorgar privilegios sea mucho más fácil. En lugar de asignar privilegios individuales a cientos de usuarios, el DBA puede crear un rol, asignar privilegios al rol y, a continuación, otorgar el rol a los usuarios.

Funciones

- Para crear y asignar un rol, en primer lugar el DBA debe crear el rol.
- A continuación, el DBA puede asignar privilegios al rol, y dicho rol a los usuarios.

```
CREATE ROLE manager;
```

```
Role created.
```

```
GRANT create table, create view TO manager;
```

```
Grant succeeded.
```

```
GRANT manager TO jennifer_cho;
```

```
Grant succeeded.
```

Funciones

- Utilice la sintaxis siguiente para crear un rol:

```
CREATE ROLE role_name;
```

- Después de crear el rol, el DBA puede utilizar la sentencia GRANT para asignar el rol a los usuarios, así como asignar privilegios al rol.

Funciones

- En el ejemplo que se muestra se crea un rol manager y, a continuación, se permite a los gestores crear tablas y vistas.
- A continuación, se otorga el rol a un usuario.
- Ahora el usuario puede crear tablas y vistas.

```
CREATE ROLE manager;
```

```
Role created.
```

```
GRANT create table, create view TO manager;
```

```
Grant succeeded.
```

```
GRANT manager TO jennifer_cho;
```

```
Grant succeeded.
```

Funciones

- Si los usuarios tiene varios roles otorgados, reciben todos los privilegios asociados a todos los roles.
- Nota: CREATE ROLE es un privilegio del sistema que no se ha emitido para las clases de Academy.

```
CREATE ROLE manager;
```

```
Role created.
```

```
GRANT create table, create view TO manager;
```

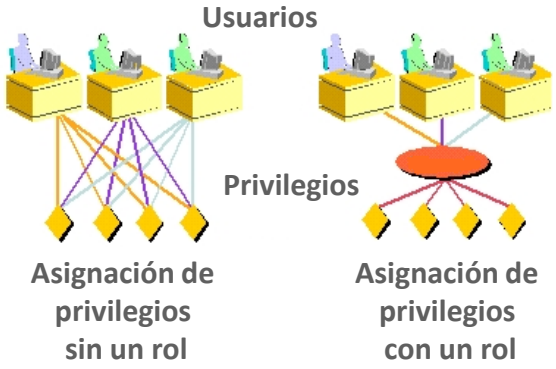
```
Grant succeeded.
```

```
GRANT manager TO jennifer_cho;
```

```
Grant succeeded.
```

Características de los Roles

- Los roles son grupos con nombre de privilegios relacionados.
- Se pueden otorgar a usuarios.
- Simplifican el proceso de otorgamiento y revocación de privilegios.
- Los crea un DBA.



Asignación de Privilegios de Objeto

- Utilice la siguiente sintaxis para otorgar privilegios de objeto:

```
GRANT object_priv [(column_list)]
ON object_name
TO {user|role|PUBLIC}
[WITH GRANT OPTION];
```

Sintaxis	Definida
object_priv	es un privilegio de objeto que se va a otorgar
column_list	especifica la columna de una tabla o vista en la que se otorgan los privilegios
ON object_name	es el objeto sobre el que se otorgan los privilegios
TO user|role	identifica el usuario o rol al que se le otorga el privilegio
PUBLIC	otorga privilegios de objeto a todos los usuarios
WITH GRANT OPTION	permite al usuario con privilegios otorgar privilegios de objeto a otros usuarios y roles

Directrices de Privilegios de Objeto

- Para otorgar privilegios en un objeto, el objeto debe estar en el propio esquema o debe otorgar el privilegio con WITH GRANT OPTION.
- Un propietario de objeto puede otorgar privilegios de objeto en el objeto a cualquier otro usuario o rol de la base de datos.
- El propietario de un objeto adquiere automáticamente todos los privilegios de objeto en dicho objeto.

Ejemplos de GRANT

- Scott King (nombre de usuario scott_king) ha creado una tabla de clientes.
- En el ejemplo 1 de la derecha, a todos los usuarios se les ha otorgado permiso para SELECCIONAR en la tabla de clientes de Scott.
- En el ejemplo 2 se otorgan privilegios UPDATE a Jennifer y al rol de gestor en columnas específicas de la tabla de clientes de Scott.

```
1. GRANT SELECT
   ON clients
   TO PUBLIC;

2. GRANT UPDATE(first_name,
       last_name)
   ON clients
   TO jennifer_cho, manager;

3. SELECT  *
   FROM scott_king.clients;

4. CREATE SYNONYM clients
   FOR scott_king.clients;

5. SELECT *
   FROM clients;
```

Ejemplos de GRANT

- Si Jennifer ahora desea SELECCIONAR datos de la tabla de Scott, la sintaxis que debe utilizar se muestra en el ejemplo 3.
- Asimismo, Jennifer puede crear un sinónimo para la tabla de Scott y SELECCIONAR en el sinónimo.
- Consulte la sintaxis en los ejemplos 4 y 5.

```
1. GRANT SELECT
   ON clients
   TO PUBLIC;

2. GRANT UPDATE(first_name,
       last_name)
   ON clients
   TO jennifer_cho, manager;

3. SELECT  *
   FROM scott_king.clients;

4. CREATE SYNONYM clients
   FOR scott_king.clients;

5. SELECT *
   FROM clients;
```

Ejemplos de GRANT

- Hay disponibles diferentes privilegios de objeto para distintos tipos de objetos de esquema.
- Un usuario automáticamente tiene todos los privilegios de objeto para los objetos de esquema que están en su esquema.
- Un usuario puede otorgar privilegios de objeto sobre cualquier objeto de esquema que el usuario posea a otro usuario o rol.

```
1. GRANT SELECT
   ON clients
   TO PUBLIC;

2. GRANT UPDATE(first_name,
       last_name)
   ON clients
   TO jennifer_cho, manager;

3. SELECT  *
   FROM scott_king.clients;

4. CREATE SYNONYM clients
   FOR scott_king.clients;

5. SELECT *
   FROM clients;
```

WITH GRANT OPTION

- El usuario con privilegios puede transferir un privilegio que se otorga con la cláusula WITH GRANT OPTION a otros usuarios y roles.
- Los privilegios de objeto otorgados con la cláusula WITH GRANT OPTION se revocan si se revoca el privilegio del otorgante.

WITH GRANT OPTION

- En el ejemplo siguiente se proporciona al usuario Scott acceso a la tabla de clientes con los privilegios para consultar la tabla y agregar filas a la tabla.
- En el ejemplo también se permite a Scott otorgar a otros usuarios estos privilegios:

```
GRANT  SELECT, INSERT
ON   clients
TO   scott_king
WITH GRANT OPTION;
```

Palabra Clave PUBLIC

- Un propietario de una tabla puede otorgar acceso a todos los usuarios mediante la palabra clave PUBLIC.
- El segundo ejemplo de la diapositiva permite a todos los usuarios del sistema consultar datos de la tabla de clientes de Jason.

```
GRANT  SELECT
ON   jason_tsang.clients
TO   PUBLIC;
```

Objeto DELETE

- Si intenta realizar una operación no autorizada, como la supresión de una fila de una tabla en la que no tiene el privilegio DELETE, Oracle Server 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:
  - Hacer referencia a una tabla o vista que no existe
  - Intentar realizar una operación en una tabla o vista para la que no tiene los privilegios adecuados

Revocación de Privilegios de Objeto

- Puede eliminar los privilegios otorgados a otros usuarios mediante la sentencia REVOKE.
- Al utilizar la sentencia REVOKE, los privilegios que especifique se revocarán a los usuarios que designe y a otros usuarios a los que se haya otorgado estos privilegios con las palabras clave WITH GRANT OPTION.

Revocación de Privilegios de Objeto

- Utilice la siguiente sintaxis para revocar privilegios de objeto:

```
REVOKE {privilege [, privilege...]|ALL}
ON  object
FROM {user[, user...]|role|PUBLIC}
[CASCADE CONSTRAINTS];
```

- CASCADE CONSTRAINTS es obligatorio para eliminar todas las restricciones de integridad referenciales realizadas sobre el objeto mediante el privilegio REFERENCES.

With Grant Option

- En el ejemplo siguiente, se revocan los privilegios SELECT e INSERT proporcionados al usuario Scott en la tabla de clientes.

```
REVOKE SELECT, INSERT
ON clients
FROM scott_king;
```

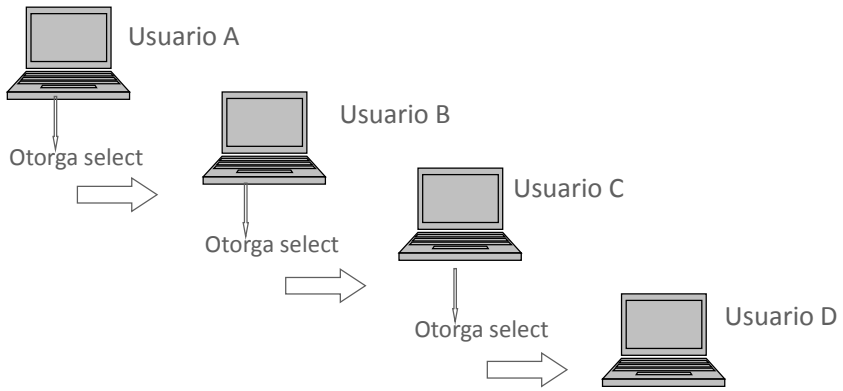
- Si se otorga a un usuario un privilegio con la cláusula WITH GRANT OPTION, dicho usuario también puede otorgar el privilegio mediante la cláusula WITH GRANT OPTION.
- Esto significa que es posible una larga cadena de usuarios con privilegios, pero no se permiten otorgar permisos de forma circular.

With Grant Option

- Si el propietario revoca un privilegio de un usuario que ha otorgado privilegios a otros usuarios, la sentencia de revocación tiene un efecto en cascada en todos los privilegios otorgados.

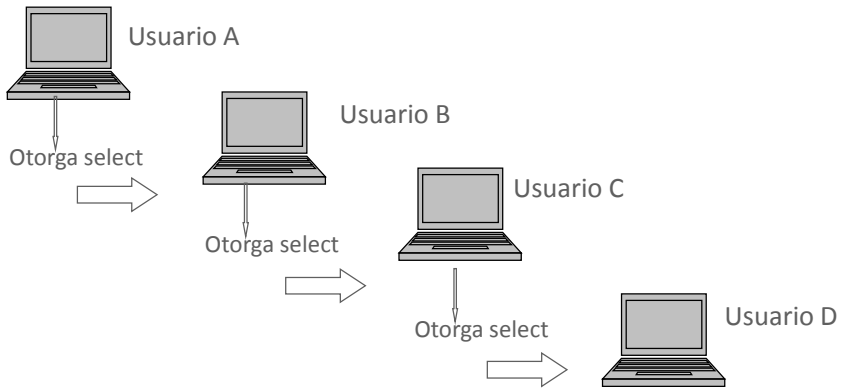
With Grant Option

- Por ejemplo, si el usuario A otorga un privilegio SELECT en una tabla al usuario B, con la cláusula WITH GRANT OPTION, el usuario B puede otorgar al usuario C el privilegio SELECT también con la cláusula WITH GRANT OPTION.



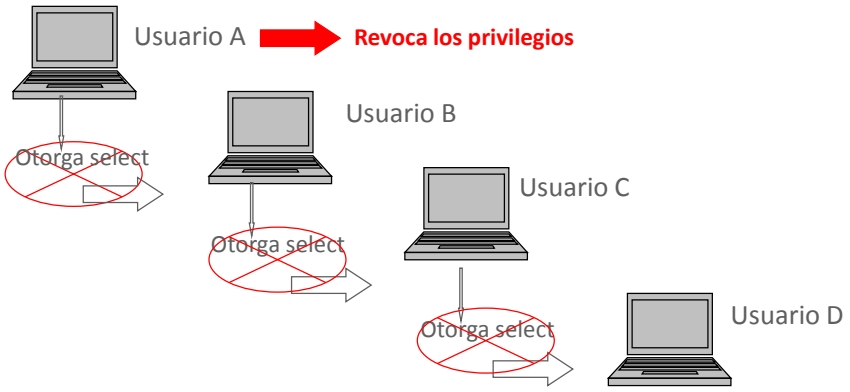
With Grant Option

- Ahora, el usuario C puede otorgar al usuario D el privilegio SELECT.



With Grant Option

- Sin embargo, si el usuario A revoca los privilegios del usuario B, los privilegios otorgados a los usuarios C y D también se revocan.



Sinónimos Privados y Públicos

- Como se ha mencionado anteriormente en esta lección, puede crear un sinónimo para eliminar la necesidad de cualificar el nombre del objeto con el esquema y se ofrecen nombres alternativos para tablas, vistas, secuencias, procedimientos u otros objetos.
- Los sinónimos pueden ser privados (valor por defecto) o públicos.

Sinónimos Privados y Públicos

- Un sinónimo público lo pueden crear los administradores de base de datos o usuarios de base de datos a los que se haya dado los privilegios para hacerlo, pero no todo el mundo puede crear automáticamente sinónimos públicos.
- Nota: el privilegio CREATE PUBLIC SYNONYM no se ha otorgado a los alumnos de Academy.

Roles y Privilegios

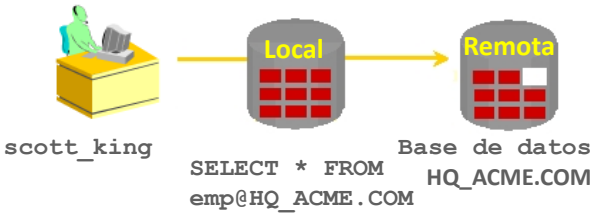
- Los roles y privilegios difieren de varias formas:
  - Un privilegio de usuario es un derecho para ejecutar un tipo concreto de sentencia SQL o un derecho para acceder a un objeto de otro usuario.
  - Oracle define todos los privilegios.
  - Los roles, por otra parte, los crean los usuarios (normalmente administradores) y se utilizan para agrupar los privilegios u otros roles.
  - Se crean para que sea más fácil gestionar el otorgamiento de varios privilegios o roles a los usuarios.
  - Los privilegios se incluyen con la base de datos y los roles los realizan los administradores de base de datos o los usuarios de una base de datos concreta

Enlaces de Base de Datos

- Un enlace de base de datos es un puntero que define una ruta de acceso de comunicación unidireccional de una base de datos Oracle a otra base de datos.
- El puntero del enlace se define realmente como una entrada en la tabla del diccionario de datos.
- Para acceder al enlace, debe estar conectado a la base de datos local que contiene la entrada del diccionario de datos.

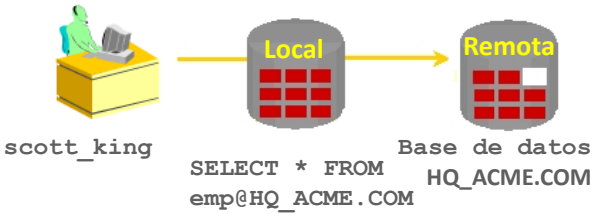
Enlaces de Base de Datos

- Una conexión de enlace de base de datos es "unidireccional" en el sentido de que un cliente conectado a la base de datos local A puede utilizar un enlace almacenado en la base de datos A para acceder a información de la base de datos remota B, pero los usuarios conectados a la base de datos B no pueden utilizar el mismo enlace para acceder a los datos de la base de datos A.



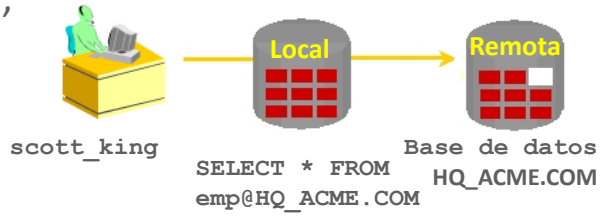
Enlaces de Base de Datos

- CREATE DATABASE LINK: en Oracle Application Express, no hay una conexión constante a la base de datos y, en consecuencia, esta función no está disponible.
- Si los usuarios locales de la base de datos B desean acceder a los datos de la base de datos A, deben definir un enlace que se almacena en el diccionario de datos de la base de datos B.
- Una conexión de enlace de base de datos proporciona a los usuarios locales acceso a los datos en una base de datos remota.



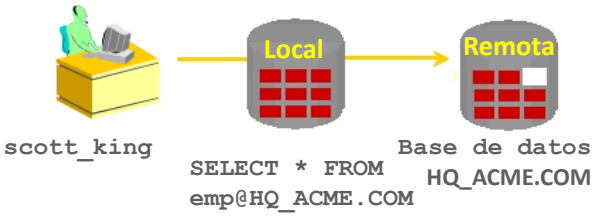
Enlaces de Base de Datos

- Para que se produzca esta conexión, cada base de datos del sistema distribuido debe tener un nombre de base de datos global único.
- El nombre de base de datos global identifica de forma única un servidor de base de datos en un sistema distribuido.
- La gran ventaja de los enlaces de base de datos es que permiten a los usuarios acceder a objetos de otros usuarios en una base de datos remota, para que estén limitados por el juego de privilegios del propietario del objeto.



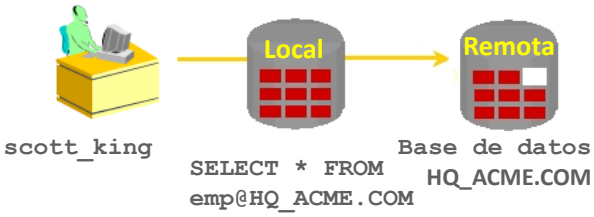
Enlaces de Base de Datos

- Es decir, un usuario local puede acceder a una base de datos remota sin tener que ser un usuario en la base de datos remota.
- En el ejemplo aparece un usuario scott_king que accede a la tabla EMP en la base de datos remota con el nombre global HQ.ACME.COM.
- Normalmente, el administrador de base de datos es el responsable de crear el enlace de la base de datos.



Enlaces de Base de Datos

- La vista del diccionario USER_DB_LINKS contiene información sobre los enlaces a los que tiene acceso un usuario.
- Una vez que se ha creado el enlace de base de datos, puede escribir sentencias SQL para los datos en el sitio remoto.
- Si se configura un sinónimo, puede escribir sentencias SQL mediante el sinónimo.



Enlaces de Base de Datos

- Por ejemplo:

```
CREATE PUBLIC SYNONYM HQ_EMP
 FOR emp@HQ.ACME.COM;
```

- A continuación, escriba la sentencia SQL que utiliza el sinónimo:

```
SELECT *
FROM HQ_EMP;
```

- no puede otorgar privilegios en objetos remotos.

Terminología

Entre los términos clave utilizados en esta lección se incluyen:

- Privilegio CREATE ROLE
- WITH GRANT OPTION
- Privilegio REVOKE
- Sentencia REVOKE
- PUBLIC SYNONYM
- PRIVATE SYNONYM
- Enlaces de Base de Datos

Resumen

En esta lección, debe haber aprendido lo siguiente:

- Explicar qué es un ROL y cuáles son sus ventajas
- Crear una sentencia para crear un ROL y OTORGARLE privilegios
- Crear una sentencia GRANT .. ON .. TO.. WITH GRANT OPTION para asignar privilegios a objetos de su esquema para otros usuarios y/o a PUBLIC
- Crear y ejecutar una sentencia para REVOCAR los privilegios de objeto a otros usuarios y/o PUBLIC

Resumen

En esta lección, debe haber aprendido lo siguiente:

- Distinción entre Privilegios y Roles
- Explicar el objetivo de un enlace de base de datos


ORACLE
ACADEMY