**UNIVERSIDAD TECNOLÓGICA DE PANAMÁ**

**FACULTAD DE INGENIERÍA DE SISTEMAS COMPUTACIONALES**

**DEPARTAMENTO DE SISTEMAS DE INFORMACIÓN, CONTROL Y EVALUACIÓN DE RECURSOS INFORMÁTICOS**

**LIC. EN ING. DE SISTEMAS DE INFORMACIÓN**

**SISTEMAS DE BASE DE DATOS II**

**Asignación 2**

**Profesor:**

**Ing. Henry Lezcano**

**Integrantes:**

Cutire, Fernando (8-972-906)

Díaz, Gabriel (20-53-5198)

Escobar, Jorge (2-747-1772)

Feng, William (8-977-446)

**Grupo: 1IF131**

Indice

[**Tipos de privilegios de base de datos**](#_ki4z9zsuto3q) **3**

[Privilegios del Sistema](#_wyilfcteo2jw) 3

[Privilegios sobre Objetos](#_59cbyf3mds0y) 3

[Roles de usuario](#_yuszuxd17cnp) 4

[**Conceder y restaurar privilegios de usuario**](#_a4mc12ldynwm) **5**

[Comando GRANT:](#_q0xwtm6je8xa) 5

[Comando REVOKE:](#_g00p6vjgxdr7) 5

[Efecto cascada](#_ehkice6hld6v) 6

[¿Cuándo entran en vigor las subvenciones y las revocaciones**?**](#_v3oufa79rh27) **7**

[**Administración de privilegios con tareas**](#_wdeyey1qo4ha) **8**

[Manejando privilegios mediante usuarios de oracle](#_9kyngokarqfa) 8

[Manejando privilegios mediante perfiles](#_yjtt3qcbtpot) 9

[Manejando privilegios mediante roles](#_2tpzmuxq2pdr) **9**

[**Conclusión**](#_zb9alqr0frfe) **10**

[**Referencias**](#_ezyrm08fb86c) **11**

Administración de privilegios y funciones en bases de datos

Un privilegio de usuario es el derecho a ejecutar un tipo particular de instrucción SQL, o el derecho a acceder a un objeto que pertenece a otro usuario, ejecutar un paquete PL/SQL, etc. Los tipos de privilegios son definidos por Oracle Database.

Los roles son creados por los usuarios (generalmente administradores) para agrupar privilegios u otros roles. Son un medio para facilitar la concesión de múltiples privilegios o roles a los usuarios.

# Tipos de privilegios de base de datos

## Privilegios del Sistema

Los permisos a niveles de la base de datos como pueden ser conexión a la base de datos, creación de usuarios, limitar cuentas. Privilegios del sistema:

| **ALTER** **ANY** **INDEX**, **ALTER** **ANY** **ROLE**, **ALTER** **ANY** **TABLE** ,**ALTER** **DATABASE**, **ALTER** PROFILE, **ALTER** **USER**, **BACKUP** **ANY** **TABLE**, BECOME **USER**, **COMMENT** **ANY** **TABLE**, **CREATE** PROFILE, **CREATE** **ROLE**, **CREATE** **TABLE**, **CREATE** **USER**, **CREATE** **VIEW**, **DELETE** **ANY** **TABLE**, **DROP** **ANY** **INDEX**, **DROP** **ANY** **ROLE**, **DROP** **ANY** **VIEW**, **DROP** PROFILE, **DROP** **USER**, **EXECUTE** **ANY** **PROCEDURE**, **EXECUTE** **ANY** **TYPE**, **FORCE** **ANY** **TRANSACTION**, **FORCE** **TRANSACTION**, **GRANT** **ANY** PRIVILEGE, **GRANT** **ANY** **ROLE**, **INSERT** **ANY** **TABLE**, **LOCK** **ANY** **TABLE**, **UPDATE** **ANY** **TABLE** |
| --- |

## Privilegios sobre Objetos

Este tipo de permiso le permite al usuario realizar ciertas acciones en objetos de la Base de Datos, como una Tabla, Vista, un Procedure o Función, etc. Si a un usuario no se le dan estos permisos sólo puede acceder a sus propios objetos. Este tipo de permisos los da el owner o dueño del objeto, el administrador o alguien que haya recibido este permiso explícitamente (con Grant Option).

| **ALTER**, **EXECUTE**, **INDEX**, **INSERT**, **READ**, **REFERENCES**, **SELECT**, **UPDATE**, ALL ó ALL **PRIVILEGES** |
| --- |

## Roles de usuario

Se emplean para asignar los privilegios relacionados con los usuarios finales de las aplicaciones de un sistema o para asignar roles a otros roles. Los roles de la base de datos tienen la siguiente funcionalidad:

* Un rol puede tener privilegios del sistema y privilegios de objetos del schema.
* Un rol se puede asignar a otro roles (excepto a sí mismo directa o indirectamente).
* A cualquier usuario de la base de datos se le puede asignar cualquier rol.
* Un rol asignado a un usuario se puede habilitar o inhabilitar en cualquier momento.
* Un rol garantizado indirectamente puede ser explícitamente habilitado o inhabilitado al usuario.

En Oracle database podemos crear roles administrativos por medio de los siguientes comandos:

El concesionario puede conceder o revocar el privilegio o rol del sistema a o desde cualquier usuario u otro rol en la base de datos. Los usuarios no pueden revocar un rol de sí mismos.

| //Creación de roles **CREATE** **ROLE** manager **IDENTIFIED** **BY** morework;  //Creación de un rol global **CREATE** **ROLE** supervisor **IDENTIFIED** **GLOBALLY**;  //Creación de un rol externo **CREATE** **ROLE** accts\_rec **IDENTIFIED** **EXTERNALLY**;  //Conceder permisos al grupo de administradores a un usuario **GRANT** new\_dba **TO** michael **WITH** **ADMIN** **OPTION**; |
| --- |

# Conceder y restaurar privilegios de usuario

Para otorgar privilegios utilizamos la sentencia GRANT, para quitar un privilegio o permiso a un usuario utilizamos la sentencia REVOKE.

## Comando GRANT:

Se utiliza para concederle privilegios al usuario La sintaxis general del comando GRANT es la siguiente:

| /\*CONCEDER PERMISOS\*/ **GRANT** **CREATE** **SESSION** **TO** usuario; **GRANT** **CONNECT** **TO** usuario; **GRANT** **RESOURCE** **TO** usuario; **GRANT** **CREATE** **VIEW** **TO** usuario; |
| --- |

## Comando REVOKE:

Es la cláusula predefinida para la remoción de un privilegio. Se utiliza la siguiente sentencia para remover un privilegio a un usuario:

| /\*REVOCAR PERMISOS\*/ **REVOKE** **CREATE** **SESSION** **TO** usuario; **REVOKE** **CONNECT** **TO** usuario; **REVOKE** **RESOURCE** **TO** usuario; **REVOKE** **CREATE** **VIEW** **TO** usuario; |
| --- |

### 

Para otorgar privilegios y roles del sistema a otros usuarios y roles mediante la declaración GRANT se requieren los siguientes privilegios:

* Para otorgar un privilegio del sistema, se le debe haber otorgado el privilegio del sistema con ADMIN OPTION o se le debe haber otorgado el privilegio del sistema GRANT ANY PRIVILEGE.
* Para otorgar un rol, se le debe haber otorgado el rol con la ADMIN OPTION o se le debe haber otorgado el privilegio del sistema GRANT ANY ROLE.

Un usuario o rol al que se le otorga un privilegio o rol, que especifica la cláusula WITH ADMIN OPTION, tiene varias capacidades:

* El beneficiario puede otorgar o revocar el privilegio o rol del sistema.
* Puede otorgar además el privilegio o rol del sistema con ADMIN OPTION.
* El beneficiario de un rol puede alterarlo o abandonarlo.

En la siguiente declaración, el administrador de seguridad otorga el rol new\_dba a gabriel:

| GRANT new\_dba TO gabriel WITH ADMIN OPTION; |
| --- |

El usuario gabriel no solo puede usar todos los privilegios implícitos en el rol new\_dba, sino que también puede otorgar, revocar y eliminar el rol new\_dba según lo considere necesario. Debido a estas poderosas capacidades, tenga cuidado al otorgar privilegios o roles del sistema con la ADMIN OPTION. Estos privilegios generalmente se reservan para un administrador de seguridad y rara vez se otorgan a otros administradores o usuarios del sistema.

Oracle proporciona el rol de dba y, por lo tanto, se otorga (con ADMIN OPTION) a cualquier usuario que se conecte como SYSDBA (usuario SYS).

Si se desea revocar no tiene que ser el usuario que originalmente otorgó el privilegio o el rol mientras tenga los privilegios de ADMIN OPTION.

## Efecto cascada

Privilegios del sistema

No hay efectos en cascada cuando se revoca un privilegio del sistema relacionado con las operaciones DDL, independientemente de si el privilegio se otorgó con o sin la ADMIN OPTION. Por ejemplo, suponga lo siguiente:

1. El administrador de seguridad otorga el privilegio del sistema CREATE TABLE a fernando con la ADMIN OPTION.
2. El usuario fernando crea una tabla.
3. El usuario fernando otorga el privilegio del sistema CREATE TABLE a escobar.
4. El usuario escobar crea una tabla.
5. El administrador de seguridad revoca el privilegio del sistema CREATE TABLE de fernando.
6. La tabla creada por el usuario fernando sigue existiendo. El usuario escobar todavía tiene la tabla y el privilegio del sistema CREATE TABLE.

Se pueden observar efectos en cascada al revocar un privilegio del sistema relacionado con una operación DML. Si SELECT ANY TABLE se revoca a un usuario, todos los procedimientos contenidos en el esquema de usuarios que dependen de este privilegio fallarán hasta que se vuelva a autorizar el privilegio.

Privilegios de objeto

Revocar un privilegio de objeto puede tener efectos en cascada que deben investigarse antes de emitir una declaración REVOKE. Ejemplo: Las definiciones de objeto que dependen de un privilegio de objeto DML pueden verse afectadas si se revoca el privilegio de objeto DML. Por ejemplo, suponga que el cuerpo del procedimiento de Prueba incluye una declaración SQL que consulta datos de la tabla temp. Si el privilegio SELECT en la tabla temp se revoca al propietario del procedimiento de prueba, entonces el procedimiento ya no se puede ejecutar con éxito.

### ¿Cuándo entran en vigor las subvenciones y las revocaciones?

Dependiendo de lo que se conceda o revoque, una concesión o revocación entra en vigor en diferentes momentos:

* Todas las concesiones y revocaciones de privilegios de objetos y sistemas sobre cualquier cosa (usuarios, roles y PUBLIC) tienen efecto inmediato.
* Todas las concesiones y revocaciones de roles a cualquier cosa (usuarios, otros roles, PUBLIC) entran en vigencia sólo cuando una sesión de usuario actual emite una declaración SET ROLE para volver a habilitar el rol después de la concesión y revocación, o cuando se crea una nueva sesión de usuario después de la concesión y revocar.

# Administración de privilegios con tareas

Muchas tareas, con muchas consideraciones entrelazadas, están involucradas en la administración de privilegios, roles y perfiles de usuario. Estas operaciones y principios necesarios se analizan en las siguientes secciones:

Para entender la administración de privilegios, se introduce el concepto de SQL Dinámico.

SQL dinámico se refiere a sentencias de SQL que se construyen y ejecutan en tiempo de ejecución. Dinámico es lo opuesto a estático. SQL estático se refiere a declaraciones SQL que están completamente especificadas, o fijas, en el momento en que se compila el código que contiene esas declaraciones. PL / SQL dinámico se refiere a bloques de código PL / SQL completos que se construyen dinámicamente, luego se compilan y ejecutan.

Para ver una lista de privilegios que ha otorgado a otros usuarios y roles, puede consultar la vista del diccionario de datos USER\_TAB\_PRIVS\_MADE. Algo contrario a la intuición, los nombres de los programas PL / SQL aparecen en la columna table\_name:

| /\*Listar Privilegios\*/ **SELECT table\_name, grantee, privilege**  **FROM USER\_TAB\_PRIVS\_MADE**  **WHERE table\_name = 'WORDCOUNT';** |
| --- |

### 

## Manejando privilegios mediante usuarios de oracle

Cada base de datos de Oracle tiene una lista de usuarios válidos. Para acceder a una base de datos, un usuario debe ejecutar una aplicación de base de datos y conectarse a la instancia de la base de datos utilizando un nombre de usuario válido definido en la base de datos. Contiene los siguientes temas:

Creando Usuarios

Modificando Usuarios

Eliminando Usuarios

## Manejando privilegios mediante perfiles

Presentan las mismas utilidades que los usuarios, pero estos perfiles son especiales en darle ciertos roles a ciertos usuarios.

Un perfil puede ser creado, asignado a usuarios, alterado y eliminado en cualquier momento (usando CREAR USUARIO o ALTERAR USUARIO) por cualquier usuario de base de datos autorizado. Los perfiles se pueden asignar solo a usuarios y no a roles u otros perfiles. Las asignaciones de perfiles no afectan a las sesiones actuales, sino que solo entran en vigor en sesiones posteriores.

Creando Perfiles

Modificando Perfiles

Eliminando Perfiles

## Manejando privilegios mediante roles

Crear un rol

Especificar la autorización del rol

Eliminando roles

# Conclusión

Los privilegios en las bases de datos, permiten al administrador, entre muchas cosas, a administrar de mejor forma la seguridad e integridad y optimización de una base de datos, llevando el control total de las opciones que tiene cada rol o usuario, permitiendoles poder hacer o no hacer alguna tarea, viendo las múltiples opciones de privilegios que nos permite usar para los roles o usuarios, se puede personalizar a necesidad de cada caso.

# Referencias

IBM. (2020). Otorgar privilegios necesarios a usuarios de Oracle mediante scripts SQL en el directorio /samples. <https://www.ibm.com/docs/es/idr/11.3.3?topic=ccreod-granting-required-privileges-oracle-users-using-sql-scripts-in-samples-directory>

Olave, E. (2011, 17 noviembre). Ayuda con Query para consultar los privilegios que tiene asignado un grupo de PACKAGE (Oracle) | Dataprix TI. Dataprix. <https://www.dataprix.com/es/forum/oracle-database/ayuda-query-consultar-privilegios-tiene-asignado-un-grupo-package-oracle>

Feuerstein, S., Pribyl, B., & Dawes, C. (2015). Oracle PL/SQL Language Pocket Reference: A Guide to Oracle’s PL/SQL Language Fundamentals (5th ed.). O’Reilly Media.

Oracle Help Center (2021). *Database Security Guide*. Obtenido de: <https://docs.oracle.com/cd/B19306_01/network.102/b14266/admusers.htm#DBSEG10000>

Unixpad. (2017, 17 enero). Listar privilegios de un usuario en Oracle – Memorias de un Sysadmin. <https://blog.unixpad.com/2017/01/17/listar-privilegios-de-un-usuario-en-oracle/>

Informática, R. E. (2020, 30 junio). Roles en SQL SERVER. Blogger. Recuperado 19 de noviembre de 2021, de http://www.respuestasit.com.mx/2020/06/roles-en-sql-server.html