**Universidad Tecnológica de Panamá**

**Facultad de Ingeniería de Sistemas Computacionales**

**Licenciatura en Ingeniería de Sistemas de Información**

**Departamento de Sistemas de Información**

Sistemas de Bases de Datos II

Equipo #2

INVESTIGACION

Aseguramiento del Acceso a la Base de Datos

Facilitador:

Ing. Henry Lezcano

Integrantes grupo 2:

Karen Cabrera 20-14-5403

Medardo Logreira 8-879-1679

Sebastian Zamora 20-15-4392

Grupo:

1IF131

II Semestre, 2020

**UNIVERSIDAD TECNOLOGICA DE PANAMA**

**FACULTAD DE INGENIERIA DE SISTEMAS COMPUTACIONES**

**LICENCIATURA EN INGENIERIA DE SISTEMAS DE INFORMACION**

**SISTEMAS DE BASE DE DATOS II**

INVESTIGACION

ASEGURAMIENTO DEL ACCESO A LA BASE DE DATOS

2.ADMINISTRACIÓN DE PRIVILEGIOS Y FUNCIONES:

Oracle pone al alcance del DBA varios niveles de seguridad:

* Seguridad de cuentas para la validación de usuarios.
* Seguridad en el acceso a los objetos de la base de datos.
* Seguridad a nivel de sistema para la gestión de privilegios globales.

**2.2 Seguridad de Objetos**

El acceso a los objetos de la BD se realiza via privilegios. Estos permiten que determinados comandos sean utilizados contra determinados objetos de la BD. Esto se especifica con el comando GRANT, *conceder*. Los privilegios se pueden agrupar formando lo que se conoce por roles. La utilización de los roles simplifica la administración de los privilegios cuando tenemos muchos usuarios. Los roles pueden ser protegidos con *passwords*, y pueden activarse y desactivarse dinámicamente, con lo que constituyen una capa más de seguridad en el sistema.

**Privilegios de Sistema y de Objetos**

En Oracle existen dos tipos de privilegios de usuario.

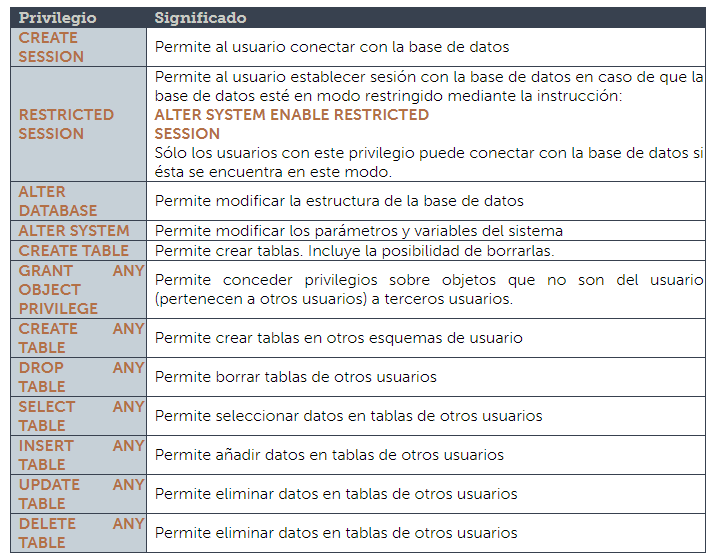
**2.2.1System:** Que permite al usuario hacer ciertas tareas sobre la BD, como por ejemplo crear un Tablespace. Estos permisos son otorgados por el administrador o por alguien que haya recibido el permiso para administrar ese tipo de privilegio. Existen como 100 tipos distintos de privilegios de este tipo.

En general los permisos de sistema, permiten ejecutar comandos del tipo DDL (Data definition Language), como CREATE, ALTER y DROP o del tipo DML (Data Manipulation Language). Oracle 10g tiene mas de 170 privilegios de sistema los cuales pueden ser vistos consultando la vista: SYSTEM\_PRIVILEGE\_MAP

Entre todos los privilegios de sistema que existen, hay dos que son los importantes: SYSDBA y SYSOPER. Estos son dados a otros usuarios que serán administradores de base de datos.

Para otorgar varios permisos a la vez, se hace de la siguiente manera:

SQL> GRANT CREATE USER, ALTER USER, DROP USER TO ahernandez;



**2.2.2 Object:** Este tipo de permiso le permite al usuario realizar ciertas acciones en objetos de la BD, 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 (véase USER\_OBJECTS). 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).

Por ejemplo, para otorgar permisos a una tabla Ventas para un usuario particular:

SQL> GRANT SELECT,INSERT,UPDATE, ON analista.venta TO jperez;

Adicionalmente, podemos restringir los DML a una columna de la tabla mencionada. Si quisieramos que este usuario pueda dar permisos sobre la tabla Factura a otros usuarios, utilizamos la cláusula WITH GRANT OPTION. Ejemplo:

SQL> GRANT SELECT,INSERT,UPDATE,DELETE ON venta TO mgarcia WITH GRANT OPTION;

---------------------------------------------------------------

SYSDBA. Con capacidad de parar e iniciar (instrucciones SHUTDOWN y STARTUP) la instancia de base de datos; modificar la base de datos (ALTER DATABASE), crear y borrar bases de datos (CREATE y DROP DATABASE), Crear el archivo de parámetros (CREATE SPFILE), cambiar el modo de archivado de la base de datos, recuperar la base de datos y además incluye el privilegio de sistema RESTRICTED SESSION. En la práctica sus capacidades son las asociadas al usuario SYS.

SYSOPER. Permite lo mismo que el anterior salvo: crear y borrar la base de datos y recuperar en todas las formas la base de datos (hay modos de recuperación que requieren el privilegio anterior).

La vista V$PWFILE\_USERS nos permite examinar a los usuarios administrativos.

<https://youtu.be/f4LJg4qEp40>

**Conceder Privilegios**

Se usa con la instrucción GRANT que funciona así:

***GRANT privilegio1 [,privilegio2[,…]] TO usuario***

***[WITH ADMIN OPTION];***

La opción WITH ADMIN OPTION permite que el usuario al que se le concede el privilegio puede conceder dicho privilegio a otros usuarios. Es, por tanto, una opción a utilizar con cautela.

**Ejemplo:**

**GRANT CREATE SESSION, ALTER SESSION, CREATE TABLE,**

**CREATE VIEW, CREATE SYNONYM, CREATE SEQUENCE,**

**CREATE TRIGGER, CREATE PROCEDURE, CREATE TYPE**

**TO Hlezcano;**

**Revocar Privilegios**

Retira privilegios concedidos a un usuario. Se realiza con la instrucción REVOKE que funciona de esta forma:

REVOKE privilegio1 [,privilegio2 [,…]] FROM usuario;

Al revocar los privilegios, las acciones llevadas a cabo con ellos (borrar, modificar,…) no se anulan.

**CREACIÓN DE ROLES**

Los roles se crean usando esta sintaxis

**CREATE ROLE rol [NOT IDENTIFIED |**

**IDENTIFIED {BY password | EXTERNALLY | GLOBALLY | USING package}];**

Por defecto un rol no requiere identificación.

**MODIFICACIÓN DE ROLES**

Disponemos de la instrucción ALTER ROLE permite modificar la configuración del rol. Tiene las mismas opciones que CREATE ROLE y sólo se usa si deseamos establecer un nuevo método para autentificarnos.

**ASIGNAR Y RETIRAR PRIVILEGIOS A ROLES**

Se realiza con la instrucción GRANT y se usa igual que cuando establecemos permisos a los usuarios, en la sintaxis de los comandos GRANT y REVOKE vistas anteriormente, simplemente se indicaría un nombre de rol en lugar de un nombre de usuario. Por ejemplo si deseamos asignar los privilegios CREATE TABLE y CONNECT a un rol llamado rol1. Se haría:

GRANT CREATE TABLE, CONNECT TO rol1;

De la misma forma, podemos quitar privilegios asignados a un rol mediante el comandol REVOKE:

REVOKE CREATE TABLE FROM rol1;

[5.6.11]asignar roles a usuarios

La sintaxis completa para asignar roles a un usuario es:

GRANT rol1 [,rol2 [,…]]

TO {usuario|rol|PUBLIC [,{usuario|rol|PUBLIC} [,…] }

[WITH ADMIN OPTION]

Al igual que en las instrucciones anteriores, PUBLIC asigna el rol a todos los usuarios y WITH ADMIN OPTION permite al usuario al que se le concede el rol, conceder él dicho rol a otros usuarios/as.

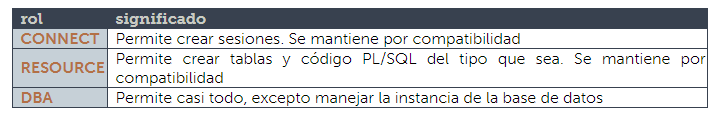
[5.6.12]roles por defecto

Los usuarios tienen una serie de roles por defecto, estos son aquellos roles que van unidos al usuario, de modo que en cuanto un usuario lanza una sesión, los privilegios que contienen sus roles por defecto, comienzan a funcionar.

Cuando asignamos un rol mediante el comando GRANT, este pasa a ser un rol por defecto.

**ROLES PREDEFINIDOS**

Oracle dispone de una serie de roles predefinidos que se pueden asignar a los usuarios. Hay más de cincuenta roles predefinidos. Los clásicos son:



**ACTIVAR Y DESACTIVAR ROLES**

La activación (y también la desactivación) de un rol se realiza mediante SET ROLE (sólo podemos activar y desactivar roles que el usuario tenga asignados mediante la instrucción GRANT). Su sintaxis es:

**SET ROLE**

**{ rol1 [IDENTIFIED BY contraseña]**

**[,rol2 [IDENTIFIED BY contraseña] [,…]]**

**| ALL [EXCEPT rol1 [,rol2 [,…]]]**

**| NONE**

**};**

Las posibilidades son:

* Indicar una lista de roles que serán los que se activen (se usa cuando se habían desactivado)
* Indicar ALL para activar todos los roles, excepto aquellos que se indiquen en la cláusula EXCEPT que quedarán sin activar.
* NONE desactiva todos los roles (incluido el rol por defecto). Sólo quedarán activados los privilegios individuales marcados explícitamente.

La activación y desactivación sólo sirve para la sesión actual, en la siguiente sesión volverán a estar activados sólo los roles por defecto.

[5.6.15]asignar a un usuario un rol por defecto

Cuando se crea un usuario mediante CREATE USER, no disponemos de la posibilidad de asignar un rol por defecto. De hecho se le asigna automáticamente la opción ALL que hace que todos los roles que se le asignen en el futuro (mediante GRANT) pasarán a ser roles por defecto.

Por ello la instrucción que administra los roles por defecto es ALTER USER:

ALTER USER usuario

DEFAULT ROLE {rol1 [,rol2 [,…]| ALL [EXCEPT rol1 [,rol2[,…]] |NONE ]};

La opción ALL coloca a todos los roles como roles por defecto, EXCEPT especifica una lista de roles que no serán colocados como roles por defecto. NONE hace que no haya ningún rol por defecto. Finalmente podemos simplemente especificar la lista de roles que quedarán como roles por defecto.

**BORRAR ROLES**

Lo hace la instrucción DROP ROLE, seguida del rol a borrar. Desde ese momento a los usuarios a los que se habían asignado el rol se les revoca.

**BIBLIOGRAFIA**

* Recuperado el 5 de noviembre de 2020, Guía de administración de dominios de E/S de Oracle: <https://docs.oracle.com/cd/E58626_01/E69681/html/E62192/z40015671104978.html>
* Recuperado el 5 de noviembre de 2020, Administración de usuarios en Oracle Database <https://jorgesanchez.net/manuales/abd/control-usuarios-oracle.html#h26>
* ORACLE: Seguridad - Mayo de 1998. Jesús Vegas – recuperado el 5 de noviembre de 2020 <https://www.infor.uva.es/~jvegas/cursos/bd/oraseg/oraseg.html>
* Video: SQL Tutorial - How to grant System and Object Privileges in Oracle Database <https://youtu.be/f4LJg4qEp40>