5.5 Control de usuarios en Oracle

# 5.5.1 Creación de usuarios en Oracle

La sentencia de creación de usuarios (que es compatible con SQL estándar) es:  
  
CREATE USER nombre IDENTIFIED BY contraseña [opciones]  
El formato completo de la instrucción con todas sus cláusulas es:  
  
CREATE USER nombre {IDENTIFIED BY contraseña |   
 EXTERNALLY |   
 GLOBALLY AS nombreGlobal}  
[DEFAULT TABLESPACE tableSpacePorDefecto]  
[TEMPORARY TABLESPACE tableSpacetTemporal]  
[QUOTA {cantidad [K|M] | UNLIMITED} ON tablespace  
 [QUOTA {cantidad [K|M] | UNLIMITED} ON tablespace […]]  
]  
[PASSWORD EXPIRE]  
[ACCOUNT {UNLOCK|LOCK}];  
[PROFILE {perfil | DEFAULT}]  
Sólo la primera línea es obligatoria, el resto posee opciones por defecto que se aplican si no se especifica cada apartado (no hace falta especificar todos, sólo las líneas que nos interesen).  
  
Ejemplo:  
  
CREATE USER jsanchez IDENTIFIED BY Caracola   
DEFAULT TABLESPACE Usuarios  
QUOTA 15M ON Usuarios //Se dan 15MBytes de espacio en el tablespace  
ACCOUNT LOCK; //La cuenta estará bloqueada  
  
La contraseña, si no se usan comillas dobles, no puede tener ni espacios en blanco ni caracteres nacionales como la eñe. En caso de querer usar estos símbolos se usan comillas dobles, lo que permitirá establecer contraseñas más complejas.

## 5.5.2 Modificación de usuarios

Cada parámetro indicado anteriormente se puede modificar mediante la instrucción ALTER USER que se utiliza igual que CREATE USER. Ejemplo:  
  
ALTER USER jsanchez QUOTA UNLIMITED ON usuarios

## 5.5.3 Borrado de usuarios

Se realiza mediante:  
  
DROP USER usuario [CASCADE]  
La opción CASCADE elimina los objetos del esquema del usuario antes de eliminar al propio usuario. Es obligatorio si el esquema contiene objetos.

## 5.5.4 Consultar usuarios

La vista administrativa DBA\_USERS muestra la lista y configuración de todos los usuarios del sistema. Para observar la estructura de la vista, siempre es conveniente usar DESCRIBE DBA\_USERS con el fin de consultar las columnas que nos interesen más

# 5.6 Control de privilegios en Oracle

Los privilegios son permisos que damos a los usuarios para que puedan realizar ciertas operaciones con la base de datos. En Oracle hay más de cien posibles privilegios. Se dividen en:  
  
Privilegios de sistema. Son permisos para modificar el funcionamiento de la base de datos. Son cambios, en definitiva, que afectan a todos los usuarios y usuarias.  
Privilegios de objeto. Son permisos que se aplican a un objeto concreto de la base de datos.

## 5.6.1 Privilegios de sistema

Se comentan algunos de los privilegios de sistema más importantes  
  
Privilegio | Significado  
------------------------|------------------------------------------------  
CREATE SESSION | Permite al usuario conectar con la base de datos  
RESTRICTED SESSION | Permite al usuario establecer sesión con la base de datos en caso de que la base de datos esté en modo restringido mediante la instrucción:  
  
 ALTER SYSTEM ENABLE RESTRICTED SESSION  
  
 Sólo los usuarios con este privilegio puede conectar con la base de datos si ésta se encuentra en este modo.  
  
ALTER DATABASE | Permite modificar la estructura de la base de datos  
ALTER SYSTEM | Permite modificar los parámetros y variables del sistema  
CREATE TABLE | Permite crear tablas. Incluye la posibilidad de borrarlas.  
GRANT ANY OBJECT PRIVILEGE | Permite conceder privilegios sobre objetos que no son del usuario (pertenecen a otros usuarios) a terceros usuarios.  
CREATE ANY TABLE | Permite crear tablas en otros esquemas de usuario  
DROP ANY TABLE | Permite borrar tablas de otros usuarios  
SELECT ANY TABLE | Permite seleccionar datos en tablas de otros usuarios  
INSERT ANY TABLE | Permite añadir datos en tablas de otros usuarios  
UPDATE ANY TABLE | Permite eliminar datos en tablas de otros usuarios  
DELETE ANY TABLE | Permite eliminar datos en tablas de otros usuarios

En la tabla anterior se ha hecho hincapié en los privilegios referidos a las tablas, para otros objetos el funcionamiento es similar: igual que hay **CREATE** **TABLE**, se puede usar **CREATE** **VIEW** para las vistas o **INDEX**, **TRIGGER**, **PROCEDURE**, **SEQUENCE**, **SYNONYM**, **TYPE**,… y de esa forma podemos conceder privilegio de creación de otros objetos. Lo mismo con el resto de operaciones

Hay dos privilegios especiales que permiten conceder nivel de DBA, son: SYSDBA y SYSOPER.

La lista completa de privilegios es:

| **Significado** |
| --- |
| Sesiones | |
| **ALTER SESSION** | Modificar el funcionamiento de la sesión |
| **ALTER RESOURCE COST** | Modifica los parámetros de cálculo de coste de la sesión |
| **RESTRICTED SESSION** | Conectar aunque la base de datos se haya iniciado en modo restringido |
| Base de datos y sistema | |
| **ALTER DATABASE** | Modificar la base de datos (privilegio de gran capacidad administrativa) |
| **ALTER SYSTEM** | Modificar los parámetros del sistema |
| **AUDIT SYSTEM** | Auditar la base de datos |
| Usuarios, roles, privilegios y perfiles | |
| **CREATE USER** | Crear usuarios pudiendo indicar tablespace por defecto, cuotas y perfiles |
| **ALTER USER** | Modificar al usuario. Permite cambiar la contraseña y modo de autentificación, tablespace por defecto, cuota de uso de disco, roles y el perfil del usuario |
| **DROP USER** | Borrar usuario |
| **CREATE PROFILE** | Crear perfiles |
| **ALTER PROFILE** | Modificar perfiles |
| **DROP PROFILE** | Borrar perfiles |
| **CREATE ROLE** | Crear roles |
| **ALTER ANY ROLE** | Modificar roles |
| **GRANT ANY ROLE** | Conceder roles |
| **GRANT ANY PRIVILEGE** | Conceder privilegios de sistema |
| Directorios | |
| **CREATE ANY DIRECTORY** | Crear directorios |
| **DROP ANY DIRECTORY** | Borrar directorios |
| Tablespaces (espacios de tabla) | |
| **CREATE TABLESPACES** | Crear tablespaces |
| **ALTER TABLESPACE** | Modificar tablespaces |
| **DROP TABLESPACE** | Borrar tablespaces |
| **MANAGE TABLESPACE** | Administrar el espacio de tablas para poder hacer copia de seguridad o simplemente quedar online u offline el tablespace |
| **UNLIMITED TABLESPACE** | Usa cuota ilimitada al escribir en cualquier tablespace. Este privilegio elimina las cuotas establecidas sobre el usuario, si las hubiera. |
| Tablas | |
| **CREATE TABLE** | Crear tablas en el esquema del usuario, incluye insertar, modificar y eliminar datos de la misma; así como eliminar la propia tabla |
| **ALTER ANY TABLE** | Modificar tablas de cualquier usuario |
| **BACKUP ANY TABLE** | Utilizar la utilidad **Export** para copiar datos de otros esquemas. |
| **CREATE ANY TABLE** | Crear tablas en cualquier esquema |
| **DELETE ANY TABLE** | Borrar filas de tablas en cualquier esquema |
| **DROP ANY TABLE** | Borrar tablas en cualquier esquema |
| **INSERT ANY TABLE** | Añadir datos a cualquier tabla |
| **SELECT ANY TABLE** | Seleccionar datos de tablas en cualquier esquema |
| **UPDATE ANY TABLE** | Modificar datos de tablas de cualquier esquema |
| **LOCK ANY TABLE** | Bloquear tablas, vistas e instantáneas en cualquier esquema |
| **FLASHBACK ANY TABLE** | Realizar acción de flashback en tablas, vistas e instantáneas en cualquier esquema |
| Vistas | |
| **CREATE VIEW** | Crear vistas en el esquema del usuario |
| **CREATE ANY VIEW** | Crear vistas en cualquier esquema |
| **DROP ANY VIEW** | Borrar cualquier vista en cualquier esquema |
| **UNDER ANY VIEW** | Crear subvistas |
| Instantáneas (Snapshots o vistas materializadas) | |
| **CREATE MATERIALIZED VIEW** | Crear vistas materializadas (instantáneas) |
| **CREATE ANY MATERIALIZED VIEW** | Crear vistas materializadas (instantáneas) en cualquier esquema |
| **ALTER ANY MATERIALIZED VIEW** | Modificar vistas materializadas (instantáneas) en cualquier esquema |
| **DROP ANY MATERIALIZED VIEW** | Borrar vistas materializadas (instantáneas) en cualquier esquema |
| **GLOBAL QUERY REWRITE** | Permite realizar operaciones de lectura escritura en instantáneas que usan tablas de otros esquemas |
| **CREATE SNAPSHOT** | Crear instantáneas (obsoleto) |
| **ALTER ANY SNAPSHOT** | Modificar instantáneas de cualquier usuario (obsoleto) |
| **CREATE ANY SNAPSHOT** | Crear instantáneas a cualquier usuario (obsoleto) |
| **DROP ANY SNAPSHOT** | Borrar instantáneas (obsoleto) |
| PL/SQL | |
| **CREATE PROCEDURE** | Crear procedimientos y funciones PL/SQL |
| **ALTER ANY PROCEDURE** | Modificar procedimientos y funciones de cualquier usuario |
| **CREATE ANY PROCEDURE** | Crear funciones y procedimientos en cualquier esquema |
| **DROP ANY PROCEDURE** | Borrar cualquier procedimiento en cualquier esquema |
| **EXECUTE ANY PROCEDURE** | Ejecutar cualquier procedimiento en cualquier esquema |
| **CREATE TRIGGER** | Crear triggers |
| **ALTER ANY TRIGGER** | Modificar triggers de cualquier usuario |
| **CREATE ANY TRIGGER** | Crear triggers en cualquier esquema |
| **DROP ANY TRIGGER** | Borrar triggers de cualquier esquema |
| **ADMINISTER DATABASE TRIGGER** | Crear triggers de sistema (requiere además el privilegio **CREATE TRIGGER**) |
| **CREATE LIBRARY** | Crear librerías de procedimientos y funciones en el esquema de usuario |
| **CREATE ANY LIBRARY** | Crear librerías de procedimientos y funciones en cualquier esquema |
| **DROP ANY TRIGGER** | Borrar cualquier trigger |
| **DROP LIBRARY** | Borrar librería de procedimientos y funciones en el esquema de usuario |
| **DROP ANY LIBRARY** | Borrar librerías de procedimientos y funciones en cualquier esquema |
| **EXECUTE ANY LIBRARY** | Ejecutar cualquier librería |
| Tipos de datos | |
| **CREATE TYPE** | Crear tipos de datos personales |
| **ALTER ANY TYPE** | Modificar tipos de datos personales en cualquier usuario |
| **CREATE ANY TYPE** | Crear tipos de datos en cualquier esquema |
| **DROP ANY TYPE** | Borrar tipos de datos de cualquier esquema |
| **EXECUTE ANY TYPE** | Permite invocar a tipos de datos personales presentes en cualquier esquema |
| Índices | |
| **ALTER ANY INDEX** | Modificar índices de la base de datos (incluye modificar claves primarias, secundarias,…) |
| **CREATE ANY INDEX** | Crear índices en cualquier esquema |
| **DROP ANY INDEX** | Borrar índices en cualquier esquema |
| Secuencias y sinónimos | |
| **ALTER ANY SEQUENCE** | Modificar secuencias de cualquier usuario |
| **CREATE ANY SEQUENCE** | Crear secuencias en cualquier esquema |
| **CREATE ANY SYNONYM** | Crear sinónimos en cualquier esquema |
| **CREATE SEQUENCE** | Crear secuencias |
| **CREATE SYNONYM** | Crear sinónimos |
| **CREATE PUBLIC SYNONYM** | Crear sinónimos públicos |
| **DROP PUBLIC SYNONYM** | Borrar sinónimos públicos |
| **CREATE ANY SEQUENCE** | Crear secuencias en cualquier esquema |
| **DROP ANY SEQUENCE** | Borrar secuencias en cualquier esquema |
| **DROP ANY SYNONYM** | Borrar sinónimos en cualquier esquema |
| **SELECT ANY SEQUENCE** | Seleccionar cualquier secuencia de cualquier esquema |
| Clusters | |
| **CREATE CLUSTER** | Crea y modifica clusters en el esquema actual |
| **ALTER ANY CLUSTER** | Modificar clusters |
| **CREATE ANY CLUSTER** | Crear clusters en cualquier esquema |
| **DROP ANY CLUSTER** | Borrar cualquier cluster |
| Segmentos de rollback | |
| **CREATE ROLLBACK SEGMENT** | Crear segmentos de rollback |
| **ALTER ROLLBACK SEGMENT** | Modificar segmentos de rollback |
| **DROP ROLLBACK SEGMENT** | Borrar segmento de rollback |
| Enlaces a base de datos | |
| **CREATE DATABASE LINK** | Crear enlaces privados a bases de datos en el esquema del usuario |
| **CREATE PUBLIC DATABASE LINK** | Crear enlaces públicos a bases de datos |
| **CREATE DATABASE LINK** | Modificar enlaces privados a bases de datos |
| **CREATE PUBLIC DATABASE LINK** | Modificar enlaces públicos a bases de datos |
| **DROP PUBLIC DATABASE LINK** | Borrar enlaces públicos a bases de datos |
| Programación de tareas | |
| **CREATE JOB** | Crear trabajo planificado en el esquema actual |
| **CREATE ANY JOB** | Crea, modifica y elimina tareas, programas y credenciales de cualquier esquema (excepto SYS). Esto permite ejecutar código en cualquier esquema de cualquier usuario. |
| **CREATE EXTERNAL JOB** | Crear un trabajo en el esquema de usuario procedente del planificador de tareas del sistema operativo |
| **EXECUTE ANY PROGRAM** | Ejecutar cualquier programa presente en un trabajo planificado del esquema de usuario. |
| **EXECUTE ANY CLASS** | Asignar cualquier clase a un trbajo en el esquema de usuario. |
| **MANAGE SCHEDULER** | Administrar el planificador de tareas, |
| Varios | |
| **ANALYZE ANY** | Analizar cualquier tabla, clúster o índice en cualquier esquema. |
| **ANALYZE ANY DICTIONARY** | Analizar cualquier elemento del diccionario de datos |
| **SELECT ANY DICTIONARY** | Realizar SELECT sobre las vistas del diccionario de datos |
| **AUDIT ANY** | Auditar a cualquier objeto de la base de datos |
| **BECOME USER** | Convertirse en otro usuario al utilizar algunas de las utilidades de Oracle |
| **COMMENT ANY TABLE** | Realizar comentarios sobre tablas, columnas y vistas en cualquier esquema de la base de datos |
| **SELECT ANY TRANSACTION** | Seleccionar los datos de la vista **FLASHBACK\_TRANSACTION\_QUERY** que controla el proceso de la actual operación flashback. |
| **FORCE ANY TRANSACTION** | Forzar aceptar (**COMMIT**) las transacciones en duda en un sistema distribuido de bases de datos en cualquier conexión |
| **FORCE TRANSACTION** | Forzar aceptar (**COMMIT**) la transacción actual en caso de duda. |
| **SYSDBA** | Privilegio general de administrador |
| Varios | |
| **SYSOPER** | Privilegio general de administrador (más bajo que el anterior) |
| **FLASHBACK ARCHIVE ADMINISTER** | Crea, elimina o modifica cualquier archivo de flashback |
| **DEBUG CONNECT SESSION** | Conectar la sesión a un depurador |
| **DEBUG ANY PROCEDURE** | Conectar procedimientos, funciones y/o código Java a un depurador |

## [5.6.2]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** jsanchez; |

**[5.6.3]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.

**[5.6.4]privilegios de objeto**

Las instrucciones vistas anteriormente otorgan o quitan permisos generales, es decir dictan qué operaciones, en general, puede realizar un usuario.

Los privilegios de objeto marcan qué operaciones le están permitidas a un usuario realizar sobre el objeto

Gráfico

El contenido generado por IA puede ser incorrecto.

La opción **ALL** concede todos los privilegios posibles sobre el objeto. Se pueden asignar varios privilegios a la vez y también varios posibles usuarios. La opción **WITH GRANT OPTION** permite al usuario al que se le conceden los privilegios, que pueda, a su vez, conceder esos mismos privilegios a otro usuario.

Ejemplo de uso de GRANT con privilegios de objeto:

**GRANT UPDATE, INSERT ON** jsanchez.personas **TO** anozal**;**

En la siguiente tabla se enumeran los posibles privilegios que se pueden aplicar a un determinado objeto:

Tabla

El contenido generado por IA puede ser incorrecto.

**[5.6.5]quitar privilegios de objeto**