DCL. CREACION DE USUARIOS

Desde la versión 12c debemos usar

```
alter session set "_ORACLE_SCRIPT"=true;
```

cada vez que vayamos a crear usuarios.

CREATE USER statement

The `CREATE USER` statement allows you to create a new database user which you can use to log in to the Oracle database.

The basic syntax of the `CREATE USER` statement is as follows:

```
CREATE USER username
   IDENTIFIED BY password
   [DEFAULT TABLESPACE tablespace]
   [QUOTA {size | UNLIMITED} ON tablespace]
   [PROFILE profile]
   [PASSWORD EXPIRE]
   [ACCOUNT {LOCK | UNLOCK}];Code language: SQL (Structured Query Language) (sql)
```

In this syntax:

`CREATE USER` username

Specify the name of the user to be created.

`IDENTIFIED BY` password

Specify a password for the local user to use to log on to the database. Note that you can create an external or global user, which is not covered in this tutorial.

`DEFAULT TABLESPACE`

Specify the tablespace of the objects such as tables and views that the user will create.

If you skip this clause, the user's objects will be stored in the database default tablespace if available, typically it is `USERS` tablespace; or the `SYSTEM` tablespace in case there is no database default tablespace.

`QUOTA`

Specify the maximum space in the tablespace that the user can use. You can have multiple `QUOTA` clauses, each for a tablespace.

Use `UNLIMITED` if you don't want to restrict the size of the tablespace that the user can use.

`PROFILE` profile

A user profile limits the database resources or password that the user cannot exceed. You can assign a profile to a newly created user. If you skip this clause, Oracle will assign the `DEFAULT` profile to the user.

`PASSWORD EXPIRE`

Use the `PASSWORD EXPIRE` if you want to force the user to change the password for the first time the user logs in to the database.

`ACCOUNT {LOCK | UNLOCK}`

Use `ACCOUNT LOCK` if you want to lock the user and disable access. On the other hand, specify `ACCOUNT UNLOCK` to unlock user and enable access.

To execute the `CREATE USER` statement, you must have the `CREATE USER` system privilege. Once you create the new user, the privilege domain of the user will be empty.

Therefore, if you want the user to be able to login to the database, you should grant the `CREATE SESSION` system privilege to the user.

Oracle `CREATE USER` examples

Let's practice with the `CREATE USER` statement.

1) Using Oracle `CREATE USER` statement to create a new local user example

This example uses the `CREATE USER` statement to create a new local user named `john` with the password `abcd1234`:

```
CREATE USER john IDENTIFIED BY abcd1234;
```
Code language: SQL (Structured Query Language) (sql)

Oracle issues the following output indicating that the user `john` has been created successfully.

```
User JOHN created.
```
Code language: SQL (Structured Query Language) (sql)

To find a list of users with the `OPEN` status, you query the information from the `dba_users`:

```
SELECT
    username,
    default_tablespace,
    profile,
    authentication_type
FROM
    dba_users
WHERE
    account_status = 'OPEN';
```

```
Code language: SQL (Structured Query Language) (sql)
```

USERNAME	DEFAULT_TABLESPACE	PROFILE	AUTHENTICATION_TYPE
JOHN	USERS	DEFAULT	PASSWORD
OT	USERS	DEFAULT	PASSWORD
PDBADMIN	USERS	DEFAULT	PASSWORD
SYS	SYSTEM	DEFAULT	PASSWORD
SYSTEM	SYSTEM	DEFAULT	PASSWORD

As you can see from the output, the user `john` has a default tablespace as `USERS`, profile as `DEFAULT`, and log in to the database using a `PASSWORD`.

Tambien podremos modificar y borrar usuarios de la siguiente manera

```
ALTER USER Antonio QUOTA UNLIMITED ON usuarios
```

```
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.´

GESTION DE PRIVILEGIOS

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.

1. PRIVILEGIOS DEL 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.

Privilegio	Significado
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

Privilegio	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

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

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 cualquie 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

CONCEDER y REVOCAR 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 VIEW, CREATE VIEW TO ANTONIO;

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.

2. GESTION DE PRIVILEGIOS SOBRE OBJETOS

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 de otros usuarios.

Los privilegios permiten definir el modo en que otros usuarios van a tratar los objetos de otros usuarios.

```
GRANT {privilegio [(listaColumnas)] [,privilegio
[(listaColumnas)] [,…]] |
ALL [PRIVILEGES]}
ON [esquema.]objeto
TO {usuario | rol | PUBLIC} [,{usuario | rol | PUBLIC} [,…]]
[WITH GRANT OPTION]
```

El privilegio sobre un objeto lo otorga el propietario del objeto, es decir, aquel que lo creó. También lo puede otorgar un usuario con el rol DBA.

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:

Privilegio	Aplicable a
SELECT	Tablas, vistas, instantáneas, secuencias
INSERT	Tablas, vistas,
UPDATE	Tablas, vistas
DELETE	Tablas, vistas
ALTER	Tablas, secuencias
EXECUTE	Procedimientos, funciones, paquetes, sinónimos, programas en directorios
INDEX	Tablas (para crear índices en la misma)
REFERENCES	Tablas (para crear claves secundarias, FOREIGN KEY)
UNDER	Vistas, para crear subvistas
DEBUG	Depurar procedimientos y funciones mediante programa externo
ON COMMIT REFRESH	Actualizar la vista materializada (o instantánea) al realizar un COMMIT
QUERY REWRITE	Escribir en la vista materializada (o instantánea)
READ	Directorios
WRITE	Directorios

Para otorgar al usuario David que pueda insertar registros en la tabla Producto, se ejecutará el siguiente comando:

```
GRANT INSERT ON Producto TO David;
```

Si se quiere asignar todos los privilegios posibles que se pueden asignar a un objeto dependiendo de su tipo, se usa la opción ALL [PRIVILEGES]. La palabra PRIVILEGES es opcional.

Como ya se dijo anteriormente, se pueden asignar privilegios a algunas columnas de algunas tablas. Por ejemplo, supóngase la tabla Precio con los campos CodProd, fecha, precioVenta, precioCoste, tipoIVA. Si se desea que el usuario Antonio no pueda ver la columna precioCoste, el comando sería el siguiente:

```
GRANT SELECT(CodProd, fecha, precioVenta, tipoIVA) ON Precio TO Antonio;
```

Se ha asignado al usuario Antonio el privilegio de consulta, privilegio SELECT, a todas las columnas de la tabla Precio excepto la columna precioCoste.

La tarea para la gestión de los privilegios es fácil, solo basta conocer todos los posibles privilegios asignables a cada tipo de objeto.

Para revocar los privilegios sobre objetos se usa también el comando `REVOKE`, con la sintaxis

Para revocar los privilegios sobre objetos se usa también el comando `REVOKE`, con la sintaxis

```
REVOKE {ALL [PRIVILEGES] | privilegio} ON objeto FROM usuario [WITH GRANT OPTION];
```

Para revocar al usuario David los privilegios de consultas e inserción sobre la tabla Productos se ejecutaría el comando

```
REVOKE SELECT, INSERT ON Productos FROM David;
```

Para quitar todos los permisos al usuario Paco se ejecutaría el comando

```
REVOKE ALL PRIVILEGES FROM Paco;
```

```
REVOKE {privilegio1  [,privilegio2] [,…]] |
ALL [PRIVILEGES]}
ON [esquema.]objeto
FROM {usuario | rol | PUBLIC} [,{usuario | rol | PUBLIC} [,…]]
[CASCADE CONSTRAINTS]
```

CASCADE CONSTRAINTS elimina cualquier restricción que impida el borrado del privilegio.

Sólo puede revocar los privilegios de objeto concedidos, el usuario que concedió dichos privilegios.

Las vistas que permiten mostrar información sobre privilegios son:

Vista	Significado
DBA_SYS_PRIVS	Privilegios de sistema asignados a usuarios y roles
DBA_TAB_PRIVS	Lista de todos los privilegios de todos los objetos de la base de datos
DBA_COL_PRIVS	Lista de todos los privilegios aplicados a columnas de la base de datos
SESSION_PRIVS	Privilegios en activo para el usuario y sesión actuales
USER_SYS_PRIVS	Privilegios de sistema asignados al usuario
USER_TAB_PRIVS_MADE	Privilegios de objeto asignados a los objetos del usuario actual
USER_TAB_PRIVS_RECD	Privilegios de objeto (de otros usuarios) concedidos al usuario actual
USER_COL_PRIVS_MADE	Privilegios de objeto asignados a columnas de objetos del usuario actual
USER_COL_PRIVS_RECD	Privilegios asignados a columnas de objetos (de otros usuarios) y concedidos al usuario actual

3. OTORGA R PRIVILEGIOS A UN ROL

Los roles son privilegios aglutinados sobre un mismo nombre, bajo la idea de que ese conjunto denote un uso habitual sobre la base de datos.
Gracias a los roles se facilita la asignación de privilegios a los usuarios. Un usuario puede tener asignados varios roles y viceversa.
Se puede crear un rol con el comando:

```
CREATE ROLE rol
```

```
GRANT nombre_rol TO cuenta_usuario [IDENTIFIED BY contraseña] [WITH ADMIN OPTION];
```

Nos permite asignar permisos a un usuario o a un rol.

La cláusula IDENTIFIED BY es opcional y se usa para indicar la contraseña de la cuenta de usuario. La opción WITH ADMIN OPTION se utiliza para que el usuario al que se le asigna un rol determinado puede asignar también el mismo rol a otros usuarios.

Por ejemplo, el siguiente comando asigna el rol CONNECT al usuario Alejandro:

```
GRANT CONNECT TO Alejandro;
```

Existe un gran número de posibles roles preestablecidos. Los más importantes son:

Nombre del rol	Detalles
AUDIT_ADMIN	Permite que el usuario pueda realizar políticas de auditorías a través de `AUDIT` y `NOAUDIT`.
AUDIT_VIEWER	Permite ver y analizar las auditorías de datos.
CAPTURE_ADMIN	Permite crear y gestionar privilegios de análisis de políticas.
DBFS_ROLE	Para el acceso a los objetos y paquetes del sistema de ficheros.
DELETE_CATALOG_ROLE	Se puede borrar registros en la tabla de auditoría del sistema (AUD$).
EXECUTE_CATALOG_ROLE	Se puede usar `EXECUTE` sobre los objetos del diccionario de datos.
EXP_FULL_DATABASE	Permite exportar copias completas e incrementales.
JAVA_ADMIN	Permite administrar las tablas de políticas para las aplicaciones Java.
OLAP_DBA	Permite administrar los objetos dimensionados para Oracle OLAP.
OLAP_USER	Permite desarrollar aplicaciones que crean objetos dimensionados en esquemas propios para Oracle OLAP.