



# 1. Gestió d'usuari

## NF5. Llenguatge SQL: DCL

UF3 - Llenguatges SQL: DCL i extensió procedimental

Desenvolupament d'Aplicacions Multiplataforma

M02 – Bases de dades Versió 1.0

© M<sup>a</sup> Carmen Brito Ruiz



- 1.1. Seguridad en la base de datos
- 1.2. Gestión de usuarios
  - 1.2.1. Creación de usuarios
    - 1.2.1.1. Tablespace
    - 1.2.1.2. Autenticación
  - 1.2.2. Eliminación de usuarios
- 1.3. Modificación de atributos de cuentas de usuarios
- 1.4. Perfil de usuario
- 1.5. Privilegios
  - 1.5.1. Privilegios del sistema
  - 1.5.2. Privilegios de objetos
  - 1.5.3. Listar privilegios otorgados
- 1.6. Roles
- 1.7. Catálogo de Oracle

## 1.1. Seguridad en la base de datos

### *Seguridad de Cuentas:*

Para acceder a los datos en una base de datos de Oracle, se debe tener acceso a una cuenta en la base de datos.

### *Seguridad de Objetos:*

El acceso a los objetos de la base de datos se realiza con privilegios. Estos permiten que determinados comandos sean utilizados contra determinados objetos de la BD. Esto se especifica con el comando GRANT, conceder.

### *Roles del Sistema*

Los roles se pueden utilizar para gestionar los comandos de sistema (CREATE TABLE o SELECT ANY TABLE) disponibles para los usuarios. Todos los usuarios que quieran acceder a la BD deben tener el rol CONNECT. Un usuario con el rol DBA tiene derecho para ver y manejar todos los datos de la BD.

## 1.2. Gestión de usuarios

Hay dos usuarios que se crean cuando se crea la base de datos y que tienen el rol de DBA.

SYS ⇒ clave inicial es `change_on_install`,.

Habitualmente se usa para arrancar y parar la base de datos, así como para modificar los componentes de la misma (como instalar nuevas opciones).

SYSTEM ⇒ clave inicial `manager`.

Es el DBA por excelencia. Se usara para las tareas administrativas habituales: alta de usuarios, creación de tablespaces, etc.

Una de las tareas del Administrador de la base de datos (DBA) es la gestión de los usuarios.

El DBA tiene privilegios del sistema de alto nivel, para poder realizar tareas como:

- Crear nuevos usuarios (CREATE USER),
- Eliminar usuarios (DROP USER),
- Eliminar tablas,
- Realizar copias de seguridad de las tablas, etc.



Los objetos del diccionario de datos a los que un usuario puede acceder se encuentran en la vista `DICTIONARY`, que es propiedad del usuario `SYS`.

```
DESC DICTIONARY;
```

Con la orden:

```
SELECT * FROM DICTIONARY;
```

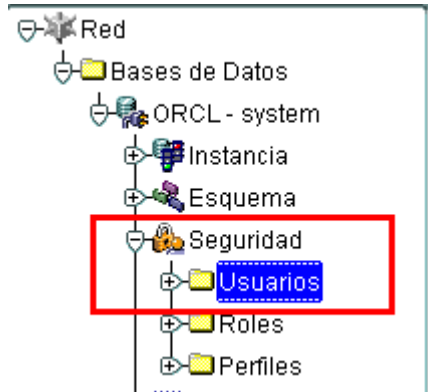
Se visualizan los objetos del diccionario de datos a los que se puede acceder y la descripción del mismo.

### 1.2.1. Creación de usuarios

Crear un usuario, es establecer una cuenta segura y útil, que tenga los privilegios adecuados y los valores por defecto apropiados.

Cuando se crea una cuenta...

- como mínimo tienes que asignar un único nombre (username) y una contraseña para poder autenticarse.
- el nombre de usuario no debe superar 30 caracteres, no debe tener caracteres especiales y debe iniciar con una letra.



Desenvolupament d'Aplicacions Multiplataforma – M02 Bases de dades

UF3: Llenguatges SQL: DCL i extensió procedimental - NF5: Gestió d'usuaris (Llenguatge DCL) -

EA 3.5.1. Gestió d'usuaris

Versió 1.0 - © M<sup>a</sup> Carmen Brito



### 1.2.1.1. Tablespace

Un tablespace es una unidad lógica de almacenamiento dentro de una base de datos Oracle. Cada tabla o índice de Oracle pertenece a un tablespace, es decir cuando se crea una tabla o índice se crea en un tablespace determinado.

- Tablespace default,:  
es donde el usuario va a poder crear sus objetos por defecto. Aunque no siempre puede crear objetos, o que tener una cuota de espacio. Los permisos se asignan de forma separada, salvo si utiliza el privilegio RESOURCE (que asigna una *quota unlimited*. incluso en el Tablespace SYSTEM).
- Tablespace temporal,  
el usuario crea sus objetos temporales y hace los sorts ('ordenamientos').

➤ Asignación de un usuario a un Tablespace (Default Tablespace)

Se le asigna un tablespace cuando se crea el usuario.

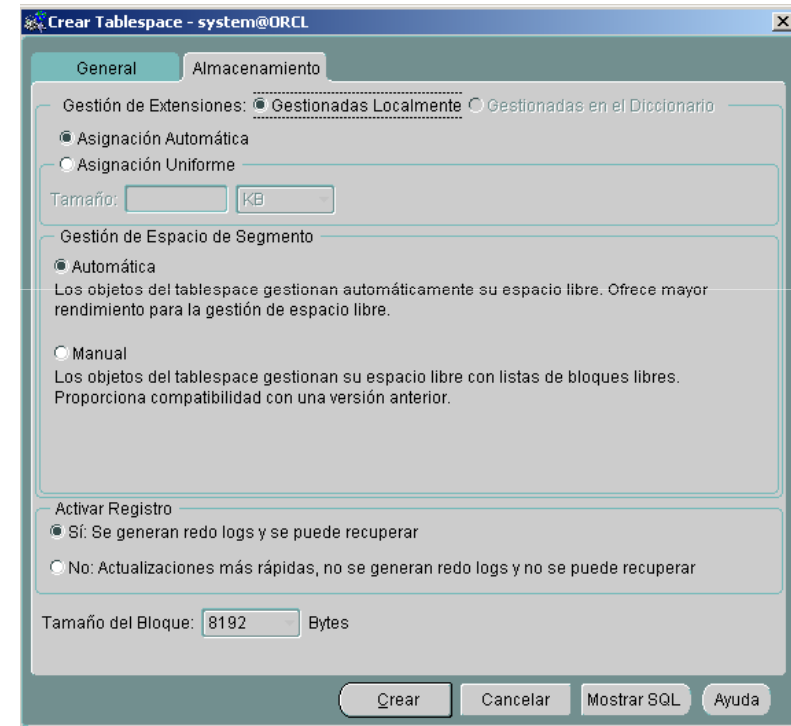
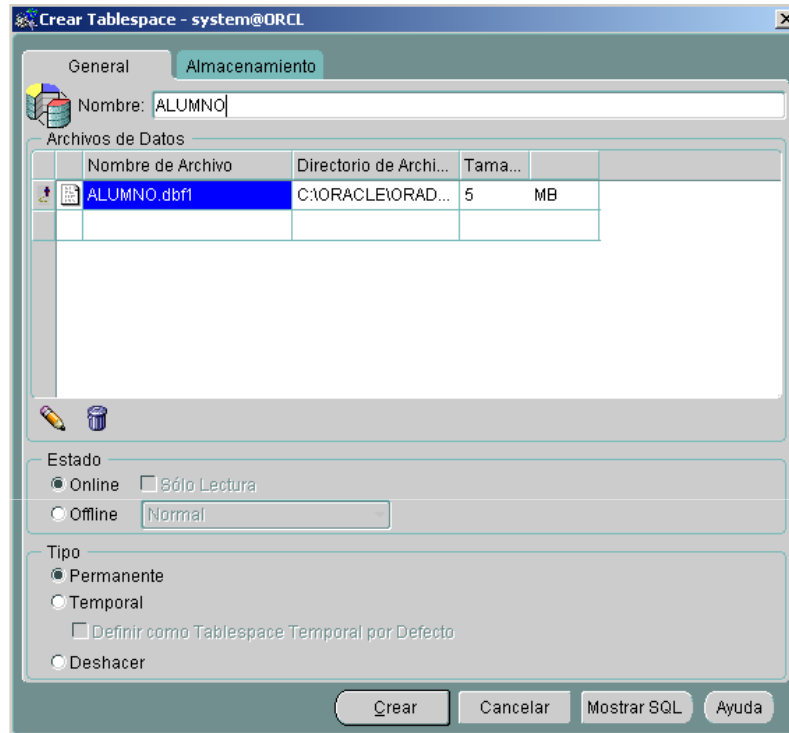
### ➤ Asignación de un usuario a un Tablespace Temporal

Un tablespace temporal se utiliza para almacenar “segmentos” temporales que son creados durante operaciones como ORDER BY, SELECT DISTINCT, MERGE JOIN o CREATE INDEX.

Cuando se asocia un tablespace temporal para realizar este tipo de operaciones, cuando finalizan las operaciones, este segmento temporal desaparece.

En primer lugar se ha de crear:





### 1.2.1.2. Autenticación

Cuando un usuario se conecta con una instancia de una base de datos la cuenta de usuario debe de estar autenticada.

ORACLE provee tres métodos de autenticación para nuestra cuenta de usuario, el más común es mediante una clave o password, aunque Oracle 10g soporta otros métodos (como biométrico, certificado y autenticación por medio de token).

Tipos de autenticación:

- Autenticación mediante password o clave
- Autenticación externa
- Autenticación global

The screenshot shows the Oracle User Management console with the 'General' tab selected. The 'Nombre:' field is empty. The 'Perfil:' dropdown is set to 'DEFAULT'. The 'Autenticación' dropdown is open, showing three options: 'Contraseña' (highlighted in blue), 'Externo', and 'Global'. Below the dropdown, there are fields for 'Introducir Contraseña:' and 'Confirmar Contraseña:'.

➤ Autenticación mediante password:

Cuando un usuario conecta con una base de datos verifica que este usuario y la contraseña introducida almacenada en la base de datos, sea correcta. Las contraseñas se guardan encriptadas en la base de datos (en el data dictionary).

➤ Autenticación Externa:

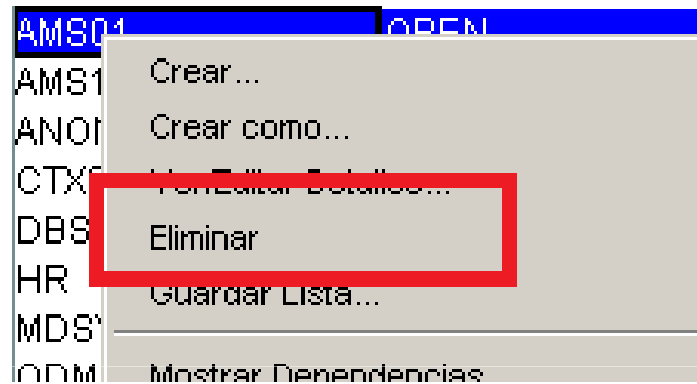
Cuando un usuario conecta con la base de datos se verifica que el nombre de usuario es el mismo que el nombre de usuario del sistema operativo para permitir la validación.

No se almacenan las cuentas en la base de datos de ninguna forma. Estas cuentas están siempre referidas con OPS\$ .

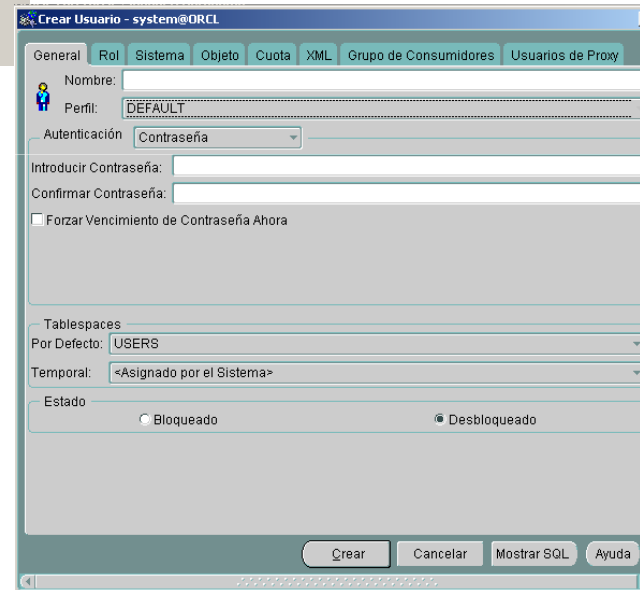
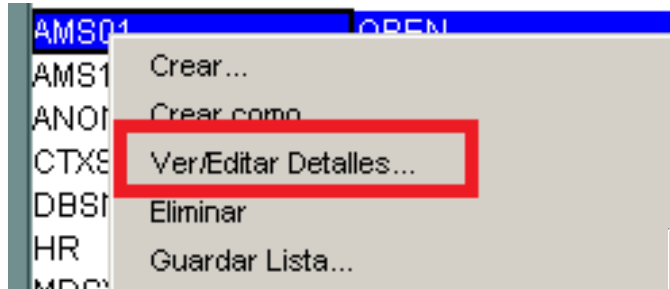
➤ Autenticación Global:

Cuando un usuario se conecta con la base de datos se verifica globalmente cuando la información pasa por una opción avanzada de seguridad (ADVANCED SECURITY OPTION ) para la autenticación tal como Kerberos, RADIUS ....

### 1.2.2. Eliminación de usuarios



### 1.3. Modificación de atributos de cuentas de usuarios





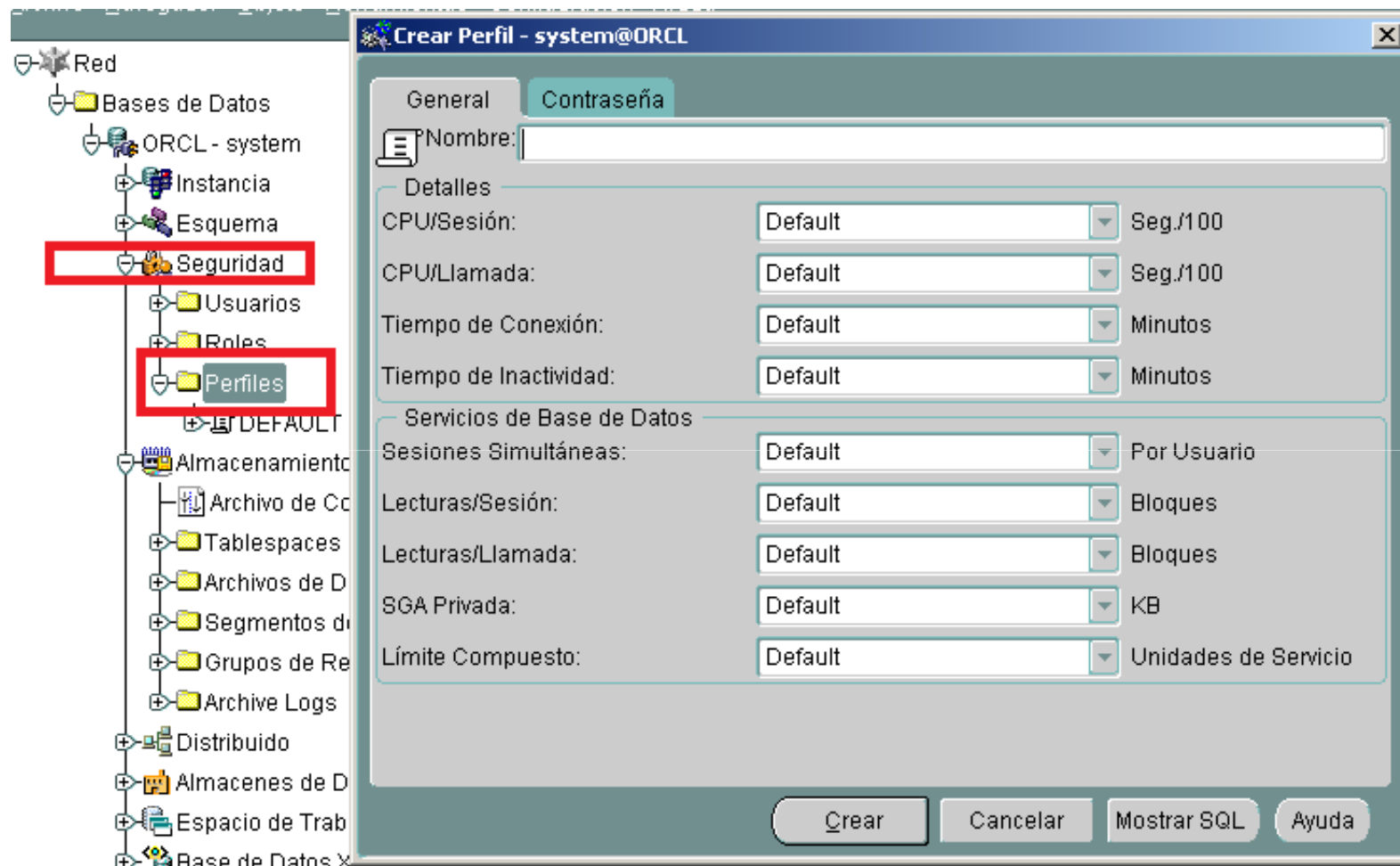
## 1.4. Perfil de usuario

Un perfil o profile de usuario, es una:

- agrupación que tiene características especiales, es decir, en cada perfil se asignan los privilegios de acceso y/o restricciones que puede tener la cuenta de usuario.
- forma de limitar los recursos que puede utilizar un usuario en la base de datos.

Cada usuario puede tener un único perfil y antes de asignar un perfil a un usuario es necesario que este perfil exista en la base de datos.

Si no se definen perfiles para un usuario se utiliza el perfil por defecto, que especifica recursos ilimitados.



**Crear Perfil - system@ORCL**

**General** **Contraseña**

☒ **Forzar Vencimiento de Contraseña**

Vencer en: Default días

Bloquear: Default días después de vencimiento

☒ **Mantener Historial de Contraseñas**

Mantener: Default contraseñas

Mantener durante: Default días

☒ **Forzar Complejidad de Contraseña**

Función de Complejidad: Default

☒ **Bloquear Cuenta al Fallar Conexión**

Bloquear despu... Default fallos de conexión

Bloquear durante: Default días

Crear Cancelar Mostrar SQL Ayuda

Los recursos que pueden ser limitados son:

Recurso	Descripción
SESSIONES_PER_USER	Número de sesiones concurrentes que el usuario puede tener en una instancia.
CPU_PER_SESSION	Tiempo de CPU (en centenas de segundos) que un sesión puede usar.
CONNECT_TIME	Número de minutos que una sesión puede permanecer activa.
IDLE_TIME	Número de minutos que un sesión puede permanecer sin que sea usada de manera activa.
LOGICAL_READS_PER_SESSION	Número de bloques de datos que se pueden leer en una sesión.
LOGICAL_READS_PER_CALL	Número de bloques de datos que pueden leer en una operación.
PRIVATE_SGA	Cantidad de espacio privado que una sesión puede reservar en la zona de SQL compartido de la SGA <sup>1</sup> (System Global Area).
COMPOSITE_LIMIT	Número total de recursos por sesión, en unidades de servicio.

1- Es el área de memoria que Oracle asigna durante el inicio de sesión y que contiene las estructuras de memoria que se utilizan para almacenar datos y para controlar la información.

Desenvolupament d'Aplicacions Multiplataforma – M02 Bases de dades

UF3: Llenguatges SQL: DCL i extensió procedimental - NF5: Gestió d'usuaris (Llenguatge DCL) -

EA 3.5.1. Gestió d'usuaris

Versió 1.0 - © M<sup>a</sup> Carmen Brito

## 1.5. Privilegios

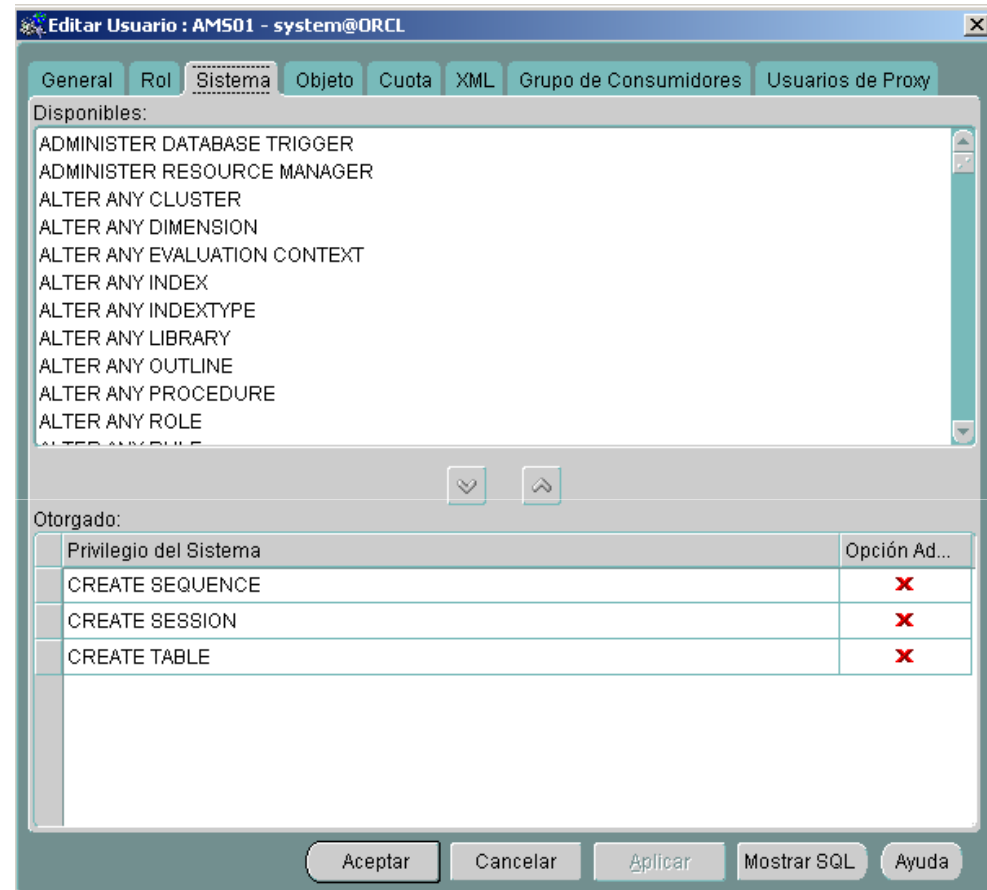
Un permiso, en Oracle, es un derecho a ejecutar una sentencia (`system privileges`) o a acceder a un objeto de otro usuario (`object privileges`).

El conjunto de permisos es fijo, no se pueden crear nuevos tipos de permisos. Y son:

- Privilegios del Sistema ( `System privileges` ): permisos sobre “niveles de la base de datos” como pueden ser conexión a la base de datos, creación de usuarios, limitar cuentas.
- Privilegios sobre Objetos ( `Object privileges` ): permisos sobre vistas, tablas, secuencias, procedimientos, paquetes.

### 1.5.1. Privilegios del sistema

Los privilegios de sistema son permisos para realizar ciertas operaciones en la base de datos, donde para poder asignarlos se usa la instrucción GRANT y para cancelarlos REVOKE.



Privilegios de  
manejo de objetos

Parámetro	Descripción
CREATE ANY INDEX	Crear cualquier índice
CREATE [PUBLIC] SYNONYM	Crear sinónimos (públicos)
CREATE [ANY] TABLE	Crear tablas. El usuario ha de tener cuota en el espacio de tablas o asignar el privilegio UNLIMITED TABLESPACE.
CREATE [ANY] VIEW	Crear vistas
ALTER ANY INDEX	Alterar cualquier índice
ALTER ANY TABLE	Alterar cualquier tabla
DROP ANY INDEX	Borrar cualquier índice
DROP ANY SYNONYM	Borrar cualquier sinónimo
DROP PUBLIC SYNONYM	Borrar sinónimos públicos
DROP ANY VIEW	Borrar cualquier vista
DROP ANY TABLE	Borrar cualquier tabla
SELECT ANY TABLE	Efectuar selecciones de cualquier tabla o vista
INSERT ANY TABLE	Insertar en cualquier tabla o vista.
DELETE ANY TABLE	Borrar filas de cualquier tabla o vista (también truncar).
ALTER SESSION	Alterar los parámetros de la sesión.
CREATE SESSION	Conectarse a la base de datos.

Privilegios  
Gestión de la  
Base de Datos

Parámetro	Descripción
CREATE PROFILE	Crear perfiles de usuario
CREATE ROLE	Crear roles
CREATE ROLLBACK SEGMENT	Creación de segmentos de rollback
CREATE TABLESPACE	Creación espacios de tablas
CREATE USER	Creación usuarios
ALTER PROFILE	Alterar perfiles de usuario
ALTER ANY ROLE	Alterar cualquier rol
ALTER ROLLBACK SEGMENT	Alterar segmentos de rollback
ALTER TABLESPACE	Alterar espacios de tablas
ALTER USER	Alterar usuarios



## Privilegios

Gestión de la  
Base de Datos

Parámetro	Descripción
DROP PROFILE	Borrar un perfil existente
DROP ANY ROLE	Borrar cualquier rol
DROP ROLLBACK SEGMENT	Borrar un segmento de rollback
DROP TABLESPACE	Borrar un espacio de tablas
DROP USER	Borrar un usuario. Si se desea eliminar los objetos del usuario, se ha de añadir CASCADE.
ALTER DATABASE	Permite una sentencia ALTER DATABASE
GRANT ANY PRIVILEGE	Otorgar cualquiera de estos privilegios.
GRANT ANY ROLE	Otorgar cualquier rol a un usuario.
UNLIMITED TABLESPACE	Puede usar una cantidad de almacenamiento ilimitada.
DROP PROFILE	Borrar un perfil existente

### 1.5.2. Privilegios de objetos

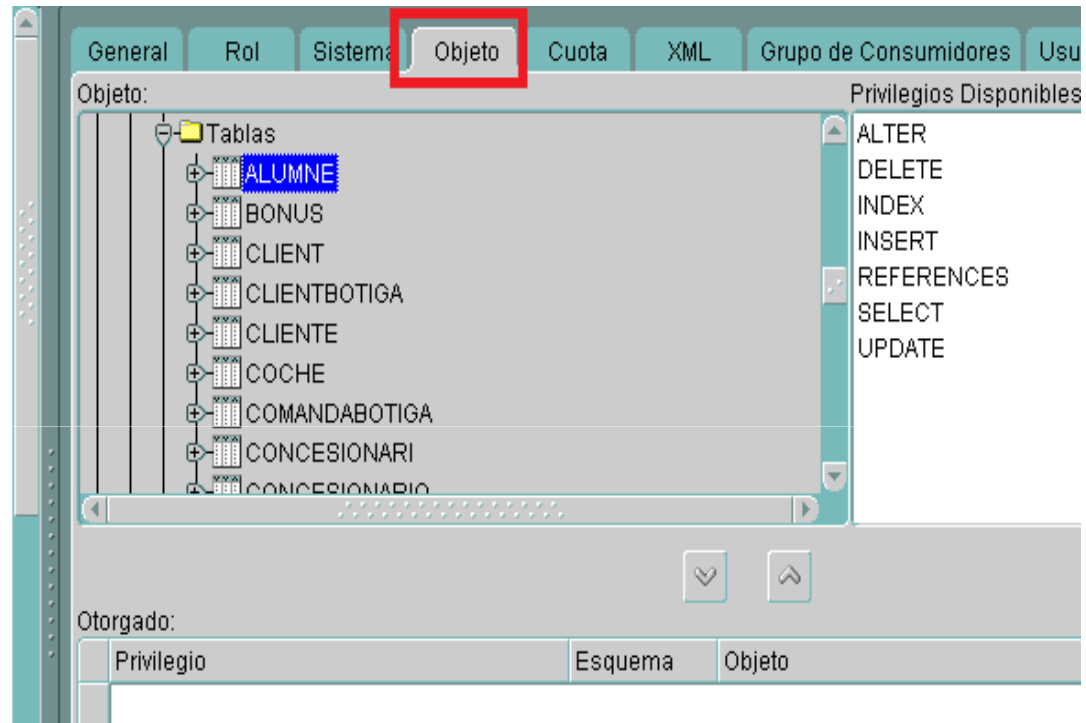
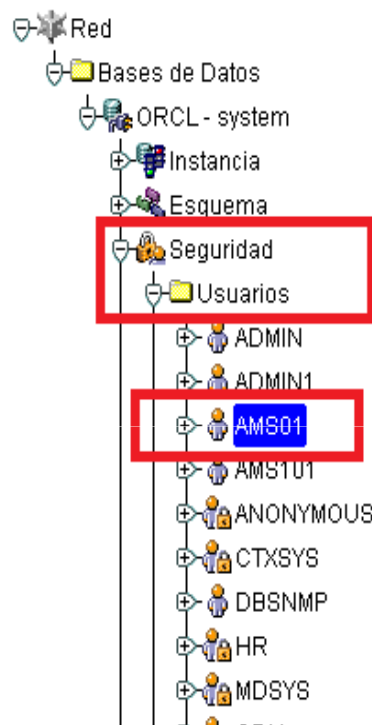
Los privilegios de objetos consienten que un objeto (creado por un usuario) pueda ser accedido por otros usuarios. Y el nivel de acceso depende del permiso que puede ser de SELECT, de UPDATE, de DELETE, de INSERT o de todos ellos.

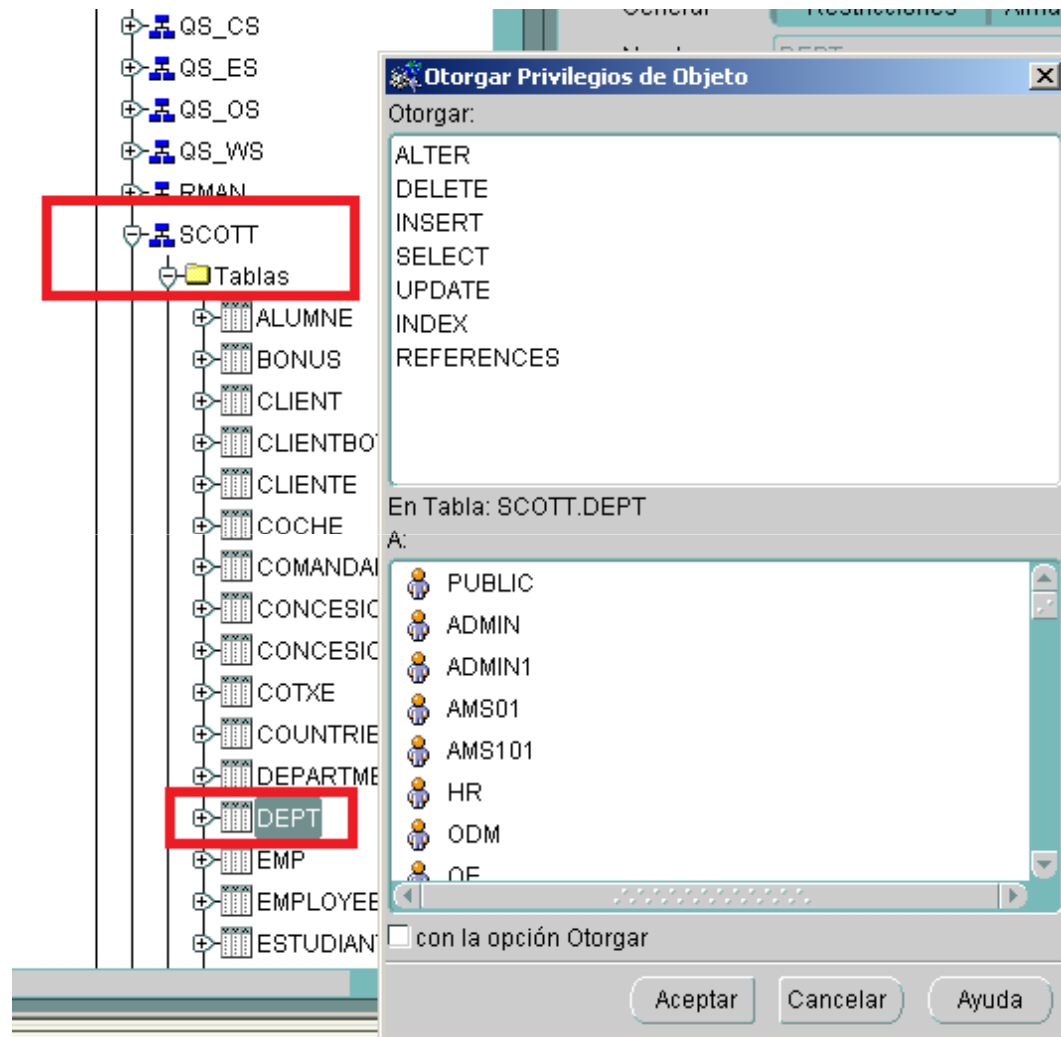
Los privilegios que pueden otorgarse sobre objetos son los siguientes:

Privilegio	Descripción
SELECT	Consultar un objeto.
INSERT	Insertar filas en una tabla o vista.
UPDATE	Actualizar filas en una tabla o vista.
DELETE	Borrar filas de una tabla o vista.
ALTER	Alterar la tabla.
INDEX	Crear índices de una tabla.
REFERENCES	Crear claves ajenas para referenciar otras tablas.
EXECUTE	Ejecutar un procedimiento, función o paquete.

Privilegios asociado a objeto.

Privilegio	Tabla	Vista	Secuencia	Procedimiento
ALTER	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
DELETE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
EXECUTE				
INDEX	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
INSERT	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
REFERENCES	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
SELECT	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
UPDATE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		





Desenvolupament d'Aplicacions Multiplataforma – M02 Bases de dades

UF3: Llenguatges SQL: DCL i extensió procedimental - NF5: Gestió d'usuaris (Llenguatge DCL) -

EA 3.5.1. Gestió d'usuaris

Versió 1.0 - © M<sup>a</sup> Carmen Brito

### 1.5.3. Listar privilegios otorgados

La información de los privilegios otorgados se almacena en el diccionario de datos.

Estos datos son accesibles a través de las siguientes vistas del diccionario de datos:

Vista	Contenidos
DBA_ROLE	Nombre de los roles y su estado del password.
DBA_ROLE_PRIVS	Usuarios a los que han sido otorgados roles.
DBA_SYS_PRIVS	Usuarios a los que han sido otorgados privilegios del sistema.
DBA_TAB_PRIVS	Usuarios a los que han sido otorgados privilegios sobre objetos.
DBA_COL_PRIVS	Usuarios a los que han sido otorgados privilegios sobre columnas de las tablas.
ROLE_ROLE_PRIVS	Roles que han sido otorgados a otros roles.
ROLE_SYS_PRIVS	Privilegios de sistema que han sido otorgados a roles.
ROLE_TAB_PRIVS	Privilegios de tabla que han sido otorgados a roles.

Los privilegios se pueden agrupar en `roles`, para así satisfacer a distintos tipos de usuarios.

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.

En la instalación se crea un rol llamado `OSOPER` que sirve para los operarios de la máquina donde está la BD y permite realizar copias de seguridad en frío y en caliente.

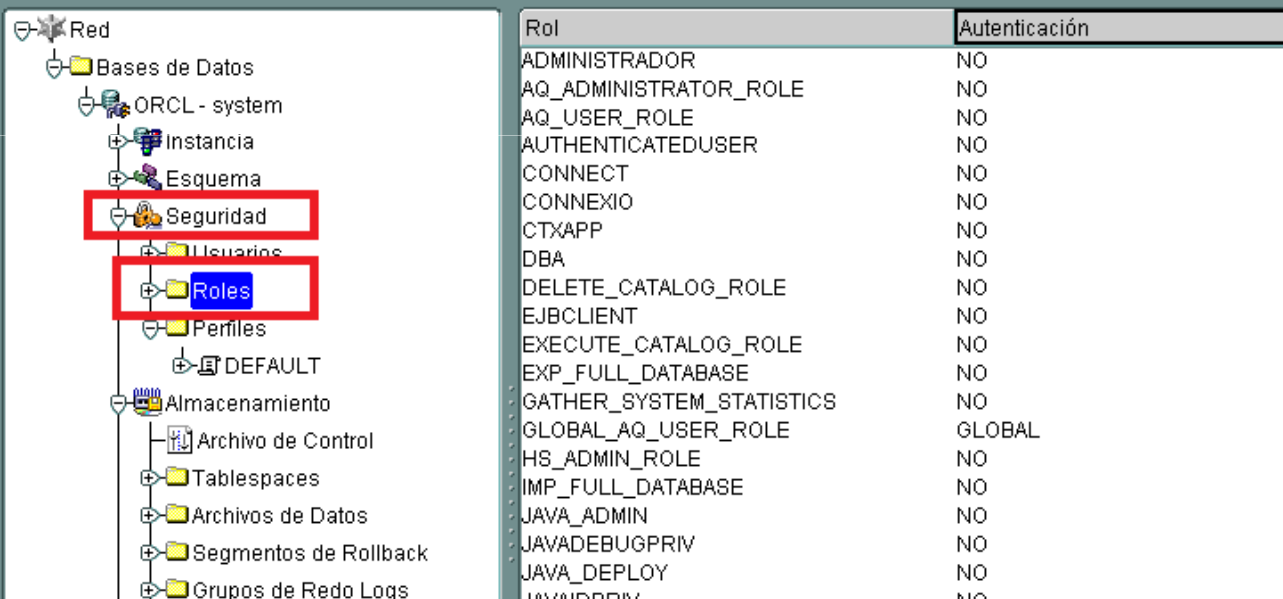
Los privilegios de `OSOPER` son `STARTUP`, `SHUTDOWN`, `ALTER DATABASE OPEN/MOUNT`, `ALTER DATABASE BACKUP`, `ARCHIVE LOG`, `RECOVER` y `RESTRICTED SESSION`.

## 1.6. Roles

Es un grupo específico de privilegios relacionados que se pueden otorgar al usuario.

Un usuario puede tener acceso a varios roles, y se puede asignar el mismo rol a varios usuarios.

Los roles se crean normalmente para una aplicación de base de datos.



The screenshot shows the Oracle Enterprise Manager (OEM) interface. On the left, a tree view displays the database structure. The 'Seguridad' (Security) folder is highlighted with a red box, and the 'Roles' folder is also highlighted with a red box. On the right, a table lists the roles and their authentication methods.

Rol	Autenticación
ADMINISTRADOR	NO
AQ_ADMINISTRATOR_ROLE	NO
AQ_USER_ROLE	NO
AUTHENTICATEDUSER	NO
CONNECT	NO
CONNEXIO	NO
CTXAPP	NO
DBA	NO
DELETE_CATALOG_ROLE	NO
EJBCLIENT	NO
EXECUTE_CATALOG_ROLE	NO
EXP_FULL_DATABASE	NO
GATHER_SYSTEM_STATISTICS	NO
GLOBAL_AQ_USER_ROLE	GLOBAL
HS_ADMIN_ROLE	NO
IMP_FULL_DATABASE	NO
JAVA_ADMIN	NO
JAVADEBUGPRIV	NO
JAVA_DEPLOY	NO
JAVASERVER	NO

Desenvolupament d'Aplicacions Multiplataforma – M02 Bases de dades

UF3: Llenguatges SQL: DCL i extensió procedimental - NF5: Gestió d'usuaris (Llenguatge DCL) -

EA 3.5.1. Gestió d'usuaris

Versió 1.0 - © M<sup>a</sup> Carmen Brito





### ROL vs. Perfil:

ROL: actividad que realiza un usuario en la base de datos.

Perfil: son los requerimientos o requisitos que necesita una persona para que se le asigne un rol dentro de la base de datos. Cabe destacar que una persona puede tener varios roles.

Otros roles de sistema:

Rol	Privilegios
CONNECT	Son los permisos necesarios para iniciar la sesión en Oracle. ALTER SESSION, CREATE SESSION, CREATE CLUSTER, CREATE TABLE, CREATE VIEW, CREATE SYNONYM, CREATE SEQUENCE, CREATE DATABASE LINK
RESOURCE	Son los permisos necesarios para tener recursos para crear objetos. CREATE CLUSTER, CREATE TABLE, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TRIGGER
DBA	Todos los privilegios del sistema con la opción with admin option.
EXP_FULL_DATABASE	Son los permisos para poder exportar toda la base de datos.
IMP_FULL_DATABASE	Son los permisos para poder importar toda la base de datos.



## 1.7. Catálogo de Oracle

Oracle cuenta con una serie de tablas y vistas que conforman una estructura denominada catálogo.

La principal función del catálogo de Oracle es almacenar toda la información de la estructura lógica y física de la base de datos, desde los objetos existentes, la situación de los datafiles, la configuración de los usuarios, etc.

El catàlego sigue un estándar de nomenclatura para que su memorización sea más fácil y son una serie de prefijos, que son:

Prefijo	Privilegios
DBA_	Objetos del administrador. Accesibles por usuarios DBA.
USER_	Objetos del usuario que está conectado. Accesible desde todos los usuarios. La información que retorna es menor que la de los objetos DBA.
ALL_	Todos los objetos de la base de datos.
V_\$ o V\$	Tablas virtuales

Para acceder a los elementos del catàlego, se utiliza el respectivo prefijo que se necesite seguido del nombre del objeto en plural, por ejemplo, para acceder a la información de las tablas de los administradores: DBA\_TABLES.

### Ejemplo Usuarios – Tablespaces:

1. Crear los usuarios llamados AMS101 y AMS102 .
  - Tablespace por defecto.
  - Se autenticará mediante contraseña el AMS101 . Y la contraseña es 12.
  - Se autenticará mediante el sistema operativo el AMS102.
2. Crear una tablespace llamado ALUMNO y que será un tablespace temporal pero no sé el temporal por defecto.
3. Asignar al AMS102 el tablespace creado anteriormente.
4. Crear un nuevo usuario que tenga las mismas características que el AMS101 y se llamará AMS103.
5. Crear un usuario llamado ADMIN\_AMS.
  - Tablespace por defecto. Contraseña: ADMIN
  - Se autenticará mediante contraseña.
6. Modificar la contraseña del usuario AMS101 y que ahora sea AMS101 .
7. Eliminar el usuario AMS103.
8. Crear dos usuarios llamados PROFES1 y PROFES2. Las contraseñas son PROFES1 y PROFES2.

Desenvolupament d'Aplicacions Multiplataforma – M02 Bases de dades

UF3: Llenguatges SQL: DCL i extensió procedimental - NF5: Gestió d'usuaris (Llenguatge DCL) -

EA 3.5.1. Gestió d'usuaris

Versió 1.0 - © M<sup>a</sup> Carmen Brito

### Ejemplo Perfiles

1. Crear el perfil para asociarlo a los usuarios que son alumnos, se llamará ALUMNO. Las características que tendrá en cuenta este perfil será:
  - Detalles y Servicios de Base de Datos: todas las opciones por defecto.
  - Contraseña:
    - Forzar vencimiento de contraseña y vencer en 30 días.
    - No mantener el historial de contraseñas.
    - Forzar la complejidad de contraseña.
    - Bloquear la cuenta en caso de fallos y será tras 3 fallos de conexión y 5 días bloqueados.
2. Asignar a los alumnos AMS101 y AMS102 el perfil creado anteriormente.

### Ejemplo Perfiles

3. Crear el perfil para asociarlo a los usuarios que son profesores, se llamará PROFESOR.

Las características que tendrá en cuenta este perfil será:

- Detalles y Servicios de Base de Datos: todas las opciones por defecto.
- Contraseña:
  - No forzar vencimiento de contraseña.
  - Mantener el historial de contraseñas.
  - Forzar la complejidad de contraseña.
  - No bloquear la cuenta nunca.

4. Asignar a los profesores creados anteriormente al perfil PROFESOR.



### Ejemplo Rol

1. Crear el un rol llamada ALUMNOS\_AMS1.
2. Asignarle al rol creado los privilegios de crear tabla y vistas.
3. Otorgar el rol creado al usuario AMS101.
4. Asignar al usuario PROFES1 el rol creado por el sistema, el DBA.





### Ejemplo privilegios de objetos:

1. Permitir que todos los usuarios dados de alta en este ejercicio AMS101 y AMS102, pueda consultar la tabla `departments` del usuario SCOTT.
2. Otorga privilegios para que PROFES1 pueda gestionar las tablas del SCOTT, es decir, realizar cualquier operación sobre ella (borrar, insertar, consultar, etc.).

# Preguntes!!!!

