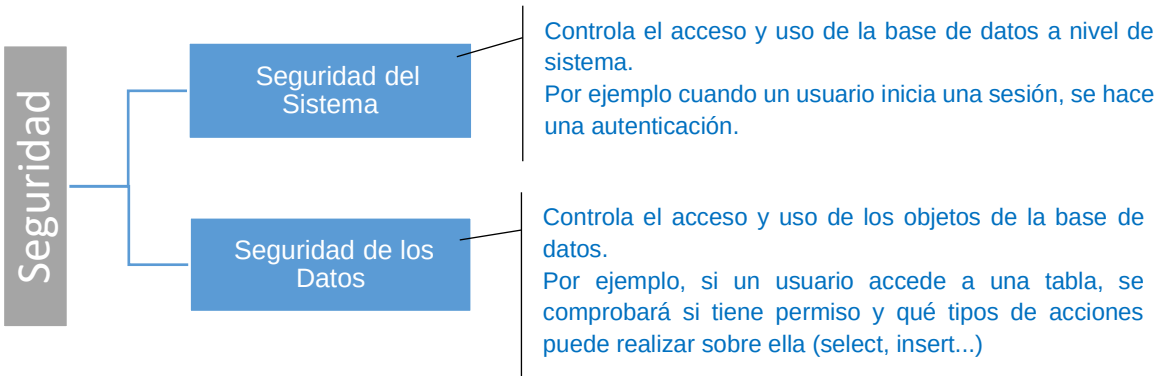
Seguridad en una Base de Datos Relacional

ÍNDICE

En este documento, a no ser que se indique lo contrario, se reflejan los comandos SQL referidos al Sistema Gestos de Base de Datos (SGBD) Oracle Database.

1. Gestión de seguridad

El administrador de la base de datos es el responsable de permitir o denegar el acceso a los usuarios a los objetos y recursos de la base de datos.

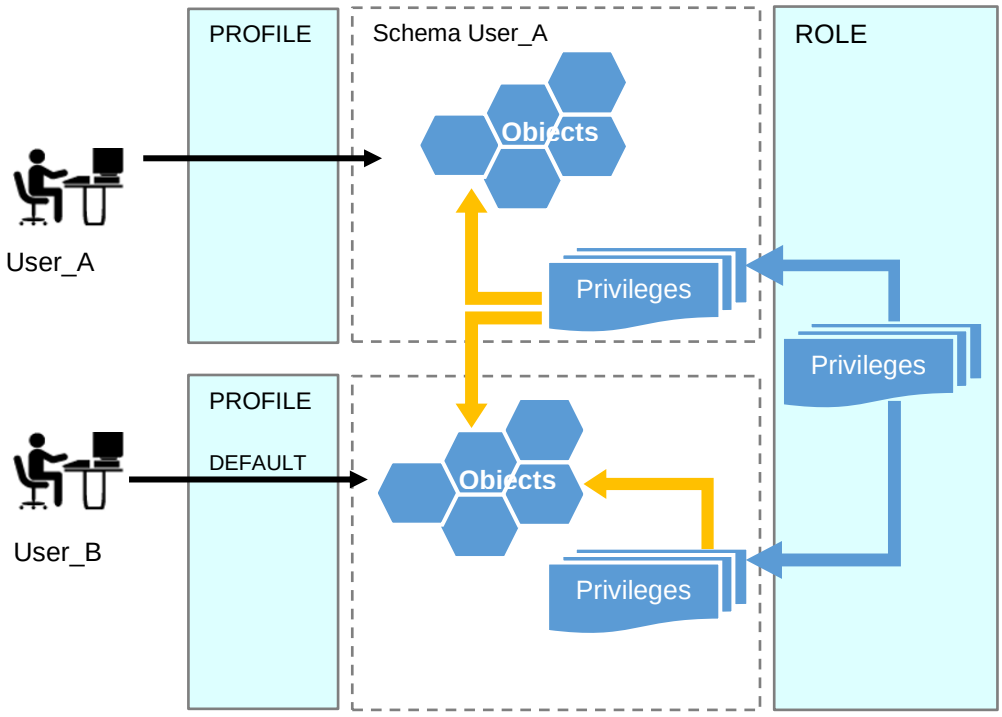


En el siguiente esquema se representan dos usuarios, A y B. **Cada uno tiene su esquema correspondiente en la base de datos, donde están todos los objetos que ha creado** (tablas, índices, secuencias, procedimientos…).

El usuario A accede a sus objetos a través de un perfil (profile) determinado, lo que establece las condiciones de conexión a la base de datos. El usuario B tiene asignado el perfil por defecto.

Cada usuario tiene asignados una serie de permisos que le permiten acceder y operar con sus objetos. El usuario A tiene incluso permisos que le permiten acceder y operar objetos del esquema del usuario B.

Ambos tienen asignado un rol, que les concede permisos adicionales.

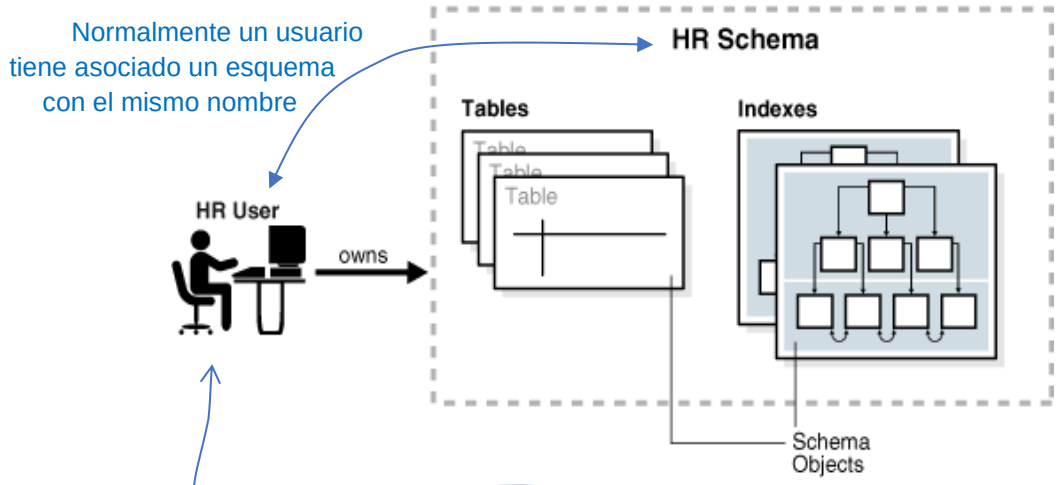


2. Usuarios

2.1. Esquema (schema)

Usuario: nombre definido en la base de datos que se puede conectar a ella y puede acceder a determinados objetos según ciertas condiciones definidas por el administrador.

Esquema: conjunto de objetos de base de datos

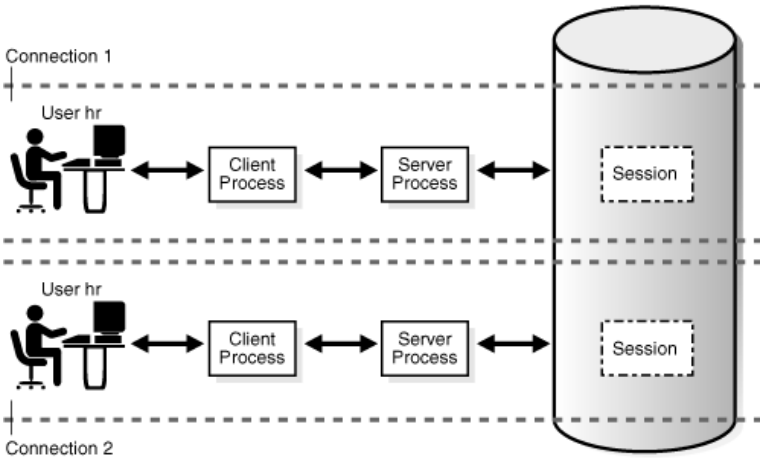


Por defecto, un usuario tiene acceso a todos los objetos de su esquema.

Un usuario tendrá permiso para acceder a objetos de otros esquemas solo si se lo han concedido.

2.2. Sesión

Conexión a la base de datos por parte de un usuario o proceso.



2.3. Usuarios de instalación

Al instalar la base de datos se crean dos usuarios administradores (DBA), ambos con una password introducida durante la instalación: SYS y SYSTEM.

- **Usuario SYS**

Al usuario SYS se le concede el privilegio SYSDBA, que le permite realizar tareas administrativas de alto nivel, como copia de seguridad y recuperación. Puede realizar todas las funciones administrativas.

Todas las tablas base y las vistas del diccionario de datos, fundamentales para el funcionamiento de Oracle, son propiedad de SYS (se almacenan en el esquema SYS). En ellas se almacena información del resto de la estructura de la base de datos.

Para mantener la integridad del diccionario de datos, las tablas del esquema SYS solo son manipuladas por la base de datos. Nunca deben ser modificadas por ningún usuario o administrador de base de datos. No se debe crear ninguna tabla en el esquema SYS.

- **Usuario SYSTEM**

Es un usuario que se emplea para administrar la base de datos. Puede realizar todas las funciones administrativas excepto las siguientes:

  - Copia de seguridad y recuperación.
  - Actualización de la base de datos.

Si bien esta cuenta puede utilizarse para realizar tareas administrativas diarias, Oracle recomienda la creación de cuentas de usuarios con nombre para administrar la base de datos, permitiendo el seguimiento de la actividad de la base de datos.

Vistas con información de usuarios:

→ `user_users`	Información sobre el usuario actual
→ `all_users`	Información sobre todos los usuarios de la base de datos
→ `dba_users`	Información de administración de los usuarios de la base de datos

Realiza las siguientes acciones:

- Ver información del propio usuario:

```
select * from user_users;
```

- Ver información de todos los usuarios:

```
select * from all_users;
```

- Ver información de administración de los usuarios (solo si se tienen permisos de administrador):

```
select * from dba_users;
```

2.4. SQL. Comandos LCD (Lenguaje Control de Datos) para usuarios

```
CREATE USER nombreUsuario
   IDENTIFIED BY claveAcceso
   [DEFAULT TABLESPACE nombreTablespace]
   [TEMPORARY TABLESPACE nombreTablespace]
   [QUOTA {entero {K|M} | UNLIMITED} ON nombreTablespace]
   [PROFILE nombrePerfil];
```

Tablespace o "espacio de tablas": estructura lógica que se asocia con uno o varios ficheros físicos (datafiles) en los que se almacenarán los datos de los objetos (tablas, vistas, índices, etc)

[IDENTIFY BY] permite dar una clave de acceso al usuario. Esta clave se indica sin comillas.

[DEFAULT nombreTablespace] indica el tablespace en el que se almacenarán los objetos del usuario. Si no se indica ninguno, por defecto será USERS.

[TEMPORARY nombreTablespace] indica el tablespace en el que se almacenarán los datos temporales del usuario. Si no se indica ninguno, por defecto será TEMP.

[QUOTA] asigna un espacio en kilobytes (K) o megabytes (M) en el tablespace asignado, o bien un espacio ilimitado con UNLIMITED.

[PROFILE] asigna un perfil al usuario. Si se omite, se asignará el perfil por defecto.

Nota: al crear un usuario nuevo, por defecto no tiene permiso para iniciar sesión.

```
ALTER USER nombreUsuario
   [IDENTIFIED BY claveAcceso]
   [DEFAULT TABLESPACE nombreTablespace]
   [TEMPORARY TABLESPACE nombreTablespace]
   [QUOTA {entero {K|M} | UNLIMITED} ON nombreTablespace]
   [PROFILE nombrePerfil]
   [DEFAULT ROLE nombreRol];
```

Un usuario puede cambiarse así mismo solamente la clave de acceso, a no ser que tenga el privilegio ALTER_USER.

```
ALTER USER nombreUsuario ACCOUNT {LOCK|UNLOCK};
```

Bloquea/desbloquea una cuenta de usuario.

```
DROP USER nombreUsuario [CASCADE];
```

CASCADE: borra todos los objetos del usuario.

Nota: si un usuario ha creado objetos en su esquema, no puede borrarse (deben borrarse previamente los objetos o utilizar el parámetro CASCADE)

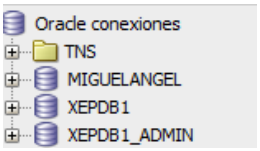
Actividad. Crear un usuario

Para hacer esta actividad se requiere un usuario administrador. No vamos a utilizar el usuario SYS, que reservamos para tareas de alto nivel. En su lugar, de momento, emplearemos el usuario **SYSTEM** a través de línea de comandos o sqlDeveloper.

a) Dentro de la PDB XEPDB1 Crea un usuario MIGUELANGEL que tenga una cuota ilimitada en el tablespace USERS y una contraseña 12345.

b) Inicia una sesión con MIGUELANGEL, solucionando si es necesario problemas de privilegios para ello.

Si estás usando sqlDeveloper guarda la conexión para poder utilizarla más adelante.



Una vez iniciada la sesión, con el propio usuario MIGUELANGEL, comprueba cuales son los parámetros principales de usuario que tiene asignados (vista USER_USERS).

c) El usuario MIGUELANGEL se cambia su propia contraseña a “miguela”.

d) ¿Puede MIGUELANGEL crear una tabla nueva? Haz una prueba.

3. Perfiles

3.1. Definición de perfil

Un perfil es un conjunto de límites a los recursos de la base de datos, que se puede imponer a los usuarios.
Se emplean para:

- Limitar el espacio disponible para un usuario
- Imponer restricciones de contraseña

El perfil por defecto es **DEFAULT**, que otorga recursos ilimitados.

→ **dba_profiles** Vista con información sobre perfiles.

Comprueba los límites definidos en el perfil DEFAULT (con un usuario administrador):

```
select * from dba_profiles where profile='DEFAULT';
```

Actividad. Ver perfil de un usuario

a) En la vista DBA_USERS existe información de administración de los usuarios. Comprueba, con el usuario administrador, qué perfil tiene asociado el usuario MIGUELANGEL con el comando:

```
select * from dba_users where username='MIGUELANGEL';
```

b) En la vista DBA_PROFILES existe información de administración de los perfiles. Revisa cómo está configurado el perfil (los recursos) mediante el comando:

```
select * from dba_profiles where profile='DEFAULT';
```

3.2. SQL. Comandos LCD (Lenguaje Control de Datos) para perfiles

```
ALTER SYSTEM SET RESOURCE_LIMIT=TRUE;
```

Activa el uso de perfiles en el sistema. Si no está activado, los perfiles se pueden utilizar, pero no tienen efecto.

```
CREATE PROFILE nombrePerfil LIMIT
  {parámetrosRecursos | parámetrosContraseña}
  {entero [K|M] | UNLIMITED | DEFAULT};
```

ParámetrosRecursos (ver tabla más abajo): SESSIONS_PER_USER, CPU_PER_SESSION, CPU_PER_CALL, CONNECT_TIME, IDLE_TIME, LOGICAL_READS_PER_SESSION, LOGICAL_READS_PER_CALL, PRIVATE_SGA, COMPOSITE_LIMIT.

ParámetrosContraseña (ver tabla más abajo): FAILED_LOGIN_ATTEMPTS, PASSWORD_LIFE_TIME, PASSWORD_REUSE_TIME, PASSWORD_REUSE_MAX, PASSWORD_LOCK_TIME, PASSWORD_GRACE_TIME, PASSWORD_VERIFY_FUNCTION

Entero [K|M] asigna un espacio en kilobytes (K) o megabytes (M) en el tablespace asignado, o bien un espacio ilimitado con UNLIMITED. Si se indica DEFAULT, se toma el espacio del perfil DEFAULT.

```
ALTER USER nombreUsuario PROFILE nombre_Perfil;
```

Asigna un perfil a un usuario.

```
ALTER PROFILE nombrePerfil LIMIT
  {parámetrosRecursos | parámetrosContraseña}
  {entero [K|M] | UNLIMITED | DEFAULT};
```

```
DROP PROFILE nombrePerfil [CASCADE];
```

[CASCADE] borra la asignación del perfil que se quiere borrar a los usuarios.

RECURSO	FUNCIÓN
SESSIONS_PER_USER	Número de sesiones múltiples concurrentes permitidas por nombre de usuario.
CONNECT_TIME	Indica el número de minutos que puede estar una sesión conectada.
IDLE_TIME	Indica el número de minutos que puede estar una sesión conectada sin ser utilizada de forma activa.
CPU_PER_SESSION	Limita el tiempo máximo de CPU por sesión. Este valor se expresa en centésimas de segundo.
CPU_PER_CALL	Limita el tiempo máximo de CPU por llamada (de análisis, ejecución o búsqueda). Se expresa en centésimas de segundo.
LOGICAL_READS_PER_SESSION	Limita el número de bloques de datos leídos en una sesión.
LOGICAL_READS_PER_CALL	Limita el número de bloques de datos leídos por llamada (de análisis, ejecución o búsqueda).
PRIVATE_SGA	Indica la cantidad de espacio privado que una sesión puede reservar en el área SQL compartida de la SGA (para la opción servidor compartido).
COMPOSITE_LIMIT	Indica un límite compuesto basado en los límites anteriores.
FAILED_LOGIN_ATTEMPTS	Número de intentos de acceso sin éxito consecutivos que producirá el bloqueo de la cuenta.
PASSWORD_LIFE_TIME	Número de días que puede utilizarse una contraseña antes de que caduque.
PASSWORD_REUSE_TIME	Número de días que deben pasar antes de que se pueda reutilizar una contraseña.
PASSWORD_REUSE_MAX	Número de veces que debe cambiarse una contraseña antes de poder reutilizarla.
PASSWORD_LOCK_TIME	Número de días que quedará bloqueada una cuenta si se sobrepasa el valor del parámetro FAILED_LOGIN_ATTEMPTS.
PASSWORD_GRACE_TIME	La duración en días del periodo de gracia durante el cual una contraseña puede cambiarse cuando ha alcanzado su valor PASSWORD_LIFE_TIME.

Actividad. Crear un perfil y asignarlo a un usuario

a) Crea un perfil nuevo que se llame REPONEDOR que limite a 1 el número de sesiones concurrentes por usuario y a dos minutos el tiempo de conexión permitido por sesión.

b) Asígnale al usuario MIGUELANGEL dicho perfil.

c) Comprueba que no puede iniciar dos sesiones simultáneas.

d) Comprueba que, trascurridos 2 minutos, se cierra la sesión de MIGUELANGEL. Si utilizas sqlDeveloper debes intentar mandar un comando transcurrido el tiempo.

Actividad. Modificar un perfil

a) Modifica el perfil REPONEDOR para que limite a 3 el número de intentos fallidos de conexión.

Comprueba con el usuario MIGUELANGEL, que si falla tres veces al introducir su contraseña en un inicio de sesión, su cuenta se bloquea.

Desbloquéala para que siga siendo operativa.

b) Modifica el perfil DEFAULT para que nunca caduquen las contraseñas.

4. Privilegios

4.1. Definición

Un privilegio es la capacidad de un usuario dentro de la base de datos para realizar determinadas acciones. Ningún usuario puede llevar a cabo una acción si no se le ha concedido permiso.

Mediante la asignación de privilegios se permite o restringe el acceso a los datos y su modificación.

→ `session_privs` Vista con los privilegios del usuario activo

Actividad. Ver permisos propios

Ejecuta el siguiente comando y compara los resultados:

```
select * from session_privs;
```

a) Con el usuario “alumno”.

b) Con el usuario administrador “system”.

c) Con el usuario “miguelangel”.

4.2. Clasificación de los privilegios:

- **Privilegios de sistema**

Dan permiso para ejecutar un tipo de comando sql o para realizar una acción sobre objetos de un tipo determinado (crear, borrar, modificar…).

Por ejemplo, se puede tener el privilegio CREATE TABLE pero no el privilegio ALTER ANY TABLE (se podrán crear tables, pero no modificar las existentes).

Algunos privilegios de sistema:

PRIVILEGIO DEL SISTEMA	OPERACIONES AUTORIZADAS
	INDEX
CREATE ANY INDEX	Crear un índice en cualquier esquema, en cualquier tabla.
ALTER ANY INDEX	Modificar cualquier índice de la base de datos.
DROP ANY INDEX	Borrar cualquier índice de la base de datos.
	PRIVILEGE
GRANT ANY PRIVILEGE	Conceder cualquier privilegio de sistema.
	PROCEDURE
CREATE ANY PROCEDURE	Crear procedimientos almacenados, funciones y paquetes en cualquier esquema.
CREATE PROCEDURE	Crear procedimientos almacenados, funciones y paquetes en nuestro esquema.
ALTER ANY PROCEDURE	Modificar procedimientos almacenados, funciones y paquetes en cualquier esquema.
DROP ANY PROCEDURE	Borrar procedimientos almacenados, funciones y paquetes en cualquier esquema.
EXECUTE ANY PROCEDURE	Ejecutar procedimientos, funciones o referencias a paquetes públicos en cualquier esquema.
	PROFILE
CREATE PROFILE	Crear un perfil de usuario.
ALTER PROFILE	Modificar cualquier perfil.
DROP PROFILE	Borrar cualquier perfil.
	ROLE
CREATE ROLE	Crear roles.
ALTER ANY ROLE	Modificar roles.
DROP ANY ROLE	Borrar cualquier rol.
GRANT ANY ROLE	Dar permisos para cualquier rol de la base.
	SEQUENCE
CREATE SEQUENCE	Crear secuencias en nuestro esquema.
ALTER ANY SEQUENCE	Modificar cualquier secuencia de la base.
DROP ANY SEQUENCE	Borrar secuencias de cualquier esquema.
SELECT ANY SEQUENCE	Referenciar secuencias de cualquier esquema.
	SESSION
CREATE SESSION	Conectarnos a la base de datos.
ALTER SESSION	Manejar la orden ALTER SESSION.
RESTRICTED SESSION	Conectarnos a la base de datos cuando se ha levantado con STARTUP RESTRICT.
	SYNONYM
CREATE SYNONYM	Crear sinónimos en nuestro esquema.
CREATE PUBLIC SYNONYM	Crear sinónimos públicos.
DROP PUBLIC SYNONYM	Borrar sinónimos públicos.
CREATE ANY SYNONYM	Crear sinónimos en cualquier esquema.
DROP ANY SYNONYM	Borrar sinónimos de cualquier esquema.
	TABLE
CREATE TABLE	Crear tablas en nuestro esquema y generar índices sobre las tablas del esquema.
CREATE ANY TABLE	Crear una tabla en cualquier esquema.
ALTER ANY TABLE	Modificar una tabla en cualquier esquema.

PRIVILEGIO DEL SISTEMA	OPERACIONES AUTORIZADAS
DROP ANY TABLE	Borrar una tabla en cualquier esquema.
LOCK ANY TABLE	Bloquear una tabla en cualquier esquema.
SELECT ANY TABLE	Hacer SELECT en cualquier tabla.
INSERT ANY TABLE	Insertar filas en cualquier tabla.
UPDATE ANY TABLE	Modificar filas en cualquier tabla.
DELETE ANY TABLE	Borrar filas de cualquier tabla.
	TABLESPACES
CREATE TABLESPACE	Crear espacios de tablas.
ALTER TABLESPACE	Modificar *tablespaces*.
MANAGE TABLESPACES	Poner *on-line* u *off-line* a cualquier *tablespace*.
DROP TABLESPACE	Eliminar tablespaces.
UNLIMITED TABLESPACE	Utilizar cualquier espacio de cualquier *tablespace*.
	TYPE
CREATE TYPE	Crea tipos de objeto y cuerpos de tipos de objeto en el propio esquema.
CREATE ANY TYPE	Crea tipos de objeto y cuerpos de tipos de objeto en cualquier esquema.
ALTER ANY TYPE	Modifica tipos de objeto en cualquier esquema.
DROP ANY TYPE	Elimina tipos de objeto y cuerpos de tipos de objeto en cualquier esquema.
EXECUTE ANY TYPE	Utiliza y hace referencia a tipos de objeto y tipos de colección en cualquier esquema.
UNDER ANY TYPE	Crea subtipos a partir de cualquier tipo de objeto no final.
	USER
CREATE USER	Crear usuarios y crear cuotas sobre cualquier espacio de tablas, establecer espacios de tablas por omisión y temporales.
ALTER USER	Modificar cualquier usuario. Este privilegio autoriza al que lo recibe a cambiar la contraseña de otro usuario, a cambiar cuotas sobre cualquier espacio de tablas, a establecer espacios de tablas por omisión, etcétera.
DROP USER	Eliminar usuarios.
	VIEW
CREATE VIEW	Crear vistas en el esquema propio.
CREATE ANY VIEW	Crear vistas en cualquier esquema.
DROP ANY VIEW	Borrar vistas en cualquier esquema.
	OTROS
SYSDBA	Ejecutar operaciones STARTUP y SHUTDOWN, ALTER DATABASE, CREATE DATABASE, ARCHIVELOG y RECOVERY, CREATE SPFILE
SYSOPER	Ejecutar operaciones STARTUP y SHUTDOWN, ALTER DATABASE, ARCHIVELOG y RECOVERY, CREATE SPFILE

- **Privilegios sobre objetos**

  Dan permiso para acceder y cambiar datos en objetos concretos de otros usuarios.

  Privilegios sobre objetos:

Privilegio sobre los objetos	Tabla	Vista	Secuencia	Procedure
ALTER	X		X	
DELETE	X	X		
EXECUTE				X
INDEX	X			
INSERT	X	X		
REFERENCES	X			
SELECT	X	X	X	
UPDATE	X	X		

4.3. SQL. Comandos LCD (Lenguaje Control de Datos) para privilegios

```
GRANT {privilegio [,{privilegio}…] … |ALL [PRIVILEGES]}
  [(nombreColumna [,nombreColumna]…)]
  [ ON {[usuario.]objeto} ]
  TO {nombreUsuario|PUBLIC [,{usuario|PUBLIC}…]
  [WITH (ADMIN|GRANT) OPTION];
```

Asigna uno o varios privilegios a uno o varios usuarios.

ON: objeto sobre el que se dan privilegios

TO: usuario/s a los que se le da/n permisos

PUBLIC: asigna los privilegios a todos los usuarios (incluso a los que se creen después)

[WITH ADMIN OPTION] permite que el usuario o usuarios que reciben este privilegio puedan concederlo a otros usuarios. Para privilegios de sistema

[WITH GRANT OPTION] permite que el usuario o usuarios que reciben este privilegio puedan concederlo a otros usuarios. Para privilegios de objeto

Ejemplos:

```
grant create session to aurelio;
grant select on empleados to aurelio;
grant all on empleados to aurelio;
```

```
REVOKE {privilegio [,{privilegio}…] … |ALL [PRIVILEGES]} [ON [usuario.]objeto}]
  FROM {nombreUsuario|PUBLIC} [,{nombreUsuario|PUBLIC}…];
```

Retira uno o varios privilegios a uno o varios usuarios.

Actividad. Asignar permisos a usuarios

Para trabajar más cómodamente con el usuario MIGUELANGEL modifica su perfil: alter user miguelangel profile default;

a) Concede a MIGUELANGEL el permiso para crear tablas.

b) Con el usuario MIGUELANGEL, crea dos tablas y sus datos con los comandos del fichero "TEMPER_ACT y TEMPER_HIST.txt".

En la tabla TEMPER_ACT se almacenan las temperaturas actuales de distintas ciudades y en TEMPER_HIST se almacenan temperaturas históricas.

c) El usuario MIGUELANGEL quiere dar permisos al usuario ALUMNO para que pueda consultar los datos de su tabla TEMPER_ACT (solo esa tabla y solo consulta). Ejecuta, desde una sesión del usuario MIGUELANGEL, un comando que otorgue ese permiso.

Una vez hecho, abre una sesión con el usuario ALUMNO y ejecuta los siguientes comandos. El segundo debe fallar:

```
select * from miguelangel.temper_act;
insert into miguelangel.temper_act values('Madrid',12);
```

Nota: cuando se manipulan objetos, por ejemplo tablas, por defecto se supone que están en el mismo esquema del usuario que las manipula (ese usuario es su propietario).
En este caso, dado que las tablas están creadas por MIGUELANGEL, para que otro usuario pueda ejecutar comandos sobre ellas es necesario indicar el esquema al que pertenecen: **esquema.nombre_tabla** (miguelangel.temper_act)

d) El usuario MIGUELANGEL quiere dar permisos al usuario ALUMNO para que pueda insertar datos en su tabla TEMPER_HIST (solo insertar). Ejecuta, desde una sesión del usuario MIGUELANGEL, un comando que otorgue ese permiso.

Una vez hecho, abre una sesión con el usuario ALUMNO y ejecuta los siguientes comandos. El primero debe fallar:

```
select * from miguelangel.temper_hist;
insert into miguelangel.temper_hist values('Madrid','04/02/2021',12);
```

e) MIGUELANGEL da permisos a ALUMNO para poder hacer cualquier cosa en la tabla TEMPER_HIST.

Actividad. Dar permisos de administración

a) Con el usuario SYSTEM, convierte a MIGUELANGEL en usuario administrador. Para ello debes darle el privilegio de sistema “DBA” (realmente es un rol llamado “DBA”, se verá más adelante).

b) Con el usuario MIGUELANGEL, comprueba cuáles son sus permisos.

c) Con el usuario MIGUELANGEL, que ahora es administrador, da permisos a todos los usuarios (actuales y futuros) para que puedan hacer select de cualquier tabla (en su esquema propio o en otros).

Actividad. Revocar permisos

a) Según se ha configurado en actividades anteriores, ALUMNO tiene permiso para insertar registros en la tabla TEMPER_HIST de MIGUELANGEL. Compruébalo ejecutando con el usuario ALUMNO el comando:

```
insert into miguelangel.temper_hist values('Madrid','05/02/2021',15);
```

Ejecuta el comando adecuado con el usuario MIGUELANGEL para quitar a ALUMNO todos los permisos sobre la tabla TEMPER_HIST.

Compruébalo ejecutando con el usuario ALUMNO el siguiente comando, que debe fallar:

```
insert into miguelangel.temper_hist values('Madrid','10/02/2021',14);
```

b) SYSTEM hace que MIGUELANGEL deje de ser usuario administrador.

c) Cierra y abre de nuevo la sesión del usuario MIGUELANGEL. Comprueba cuáles son sus permisos.

5. Roles

5.1. Definición

Un rol o función se define como un conjunto de privilegios. No hay que confundirlo con un perfil.

Facilita la tarea de asignar los mismos permisos a varios usuarios, práctica muy frecuente. Por ejemplo, una empresa puede tener distintos departamentos formados por muchos usuarios, y puede ser necesario asignar los mismos privilegios a todos los usuarios de cada departamento.

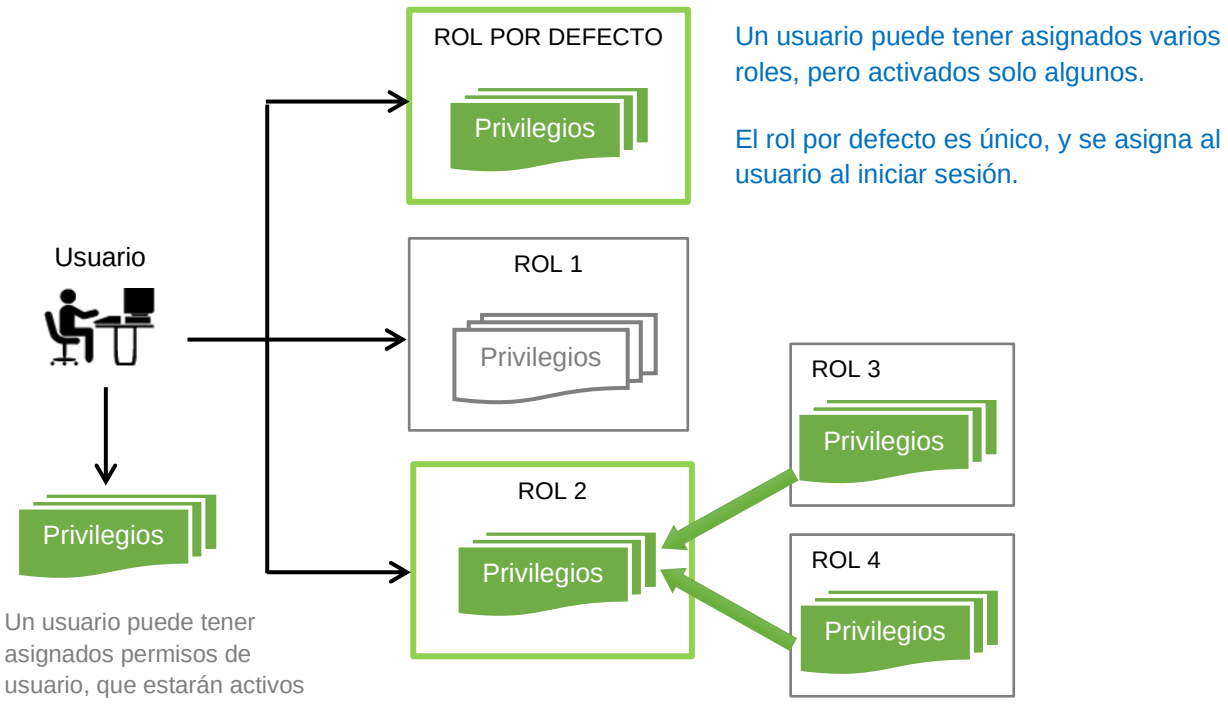
El procedimiento es el siguiente:

1) Se crea un rol
2) Se asignan privilegios al rol. Se pueden asignar privilegios de sistema o de objeto.
3) Se asigna el rol a uno o varios usuarios.

   Un usuario puede tener asignado más de un rol, pero sólo puede tener un rol por defecto, que es el que tendrá activo cuando inicie sesión.
4) El usuario puede tener varios roles asignados, pero no significa que estén activos. Pueden activarse uno o varios roles.

Notas:

- Sub-rol: puede asignarse un rol a otro rol (el segundo adquirirá los privilegios del primero)
- Puede existir la limitación de dar privilegios para crear objetos
- Con CREATE USER no puede asignarse un rol, debe usarse ALTER USER



En verde se muestran los permisos que tiene activos el usuario en este ejemplo

Vistas con información de roles:

→ `session_roles`	Roles activos del usuario
→ `role_sys_privs`	Privilegios de sistema de asignados a roles
→ `role_tab_privs`	Privilegios de roles sobre objetos del usuario

Actividad. Ver roles propios

a) Ejecuta el siguiente comando con el usuario ALUMNO, para ver sus roles:

```
select * from session_roles;
```

b) Ejecuta el siguiente comando con el usuario SYSTEM, para ver sus roles:

```
select * from session_roles;
```

c) Ejecuta el siguiente comando para ver los permisos de sistema y de objetos asociados al rol DBA:

```
select * from role_sys_privs where role='DBA';
select * from role_tab_privs where role='DBA';
```

5.2. SQL. Comandos LCD (Lenguaje Control de Datos) para roles

```
CREATE ROLE nombreRol;
```

GRANT Asigna uno o varios privilegios a uno o varios roles. El formato es similar a GRANT para un usuario, cambiando el usuario por el rol.

REVOKE Retira uno o varios privilegios a uno o varios roles. El formato es similar a REVOKE para un usuario, cambiando el usuario por el rol.

```
GRANT nombreRol TO nombreUsuario;
```
Asigna un rol a un usuario.

```
ALTER USER nombreUsuario DEFAULT ROLE nombreRol;
```
Asigna un rol por defecto a un usuario.

```
DROP ROLE nombreRol;
```

```
SET ROLE {nombreRol|ALL|NONE};
```
Activa un rol para un usuario (desactiva el resto). Debe ejecutarlo el propio usuario.
ALL: activa todos los roles asignados al usuario
NONE: desactiva todos los roles asignados al usuario

Ejemplos:

```
create role rol1;
grant insert any table to rol1; --asigna permisos de sistema a un rol
grant select on plsql.depart to rol1;--asigna permisos sobre objetos al rol
set role rol1;
drop role rol1;
```

Actividad. Crear rol y asignar a usuario

a) Con el usuario SYSTEM, crea el rol JEFE ya añade el privilegio de poder crear un índice en cualquier esquema, con los comandos:

```
create role jefe;
grant create any index to jefe;
```

b) Con el usuario SYSTEM, crea el rol SUPERVISION y añádele el privilegio de visualizar todas las tablas y el de actualizar los datos (UPDATE) en la tabla TEMPER_ACT en el esquema MIGUELANGEL.

c) Comprueba los privilegios de sistema y de objeto del rol JEFE y del rol SUPERVISOR.

d) Asigna los roles JEFE y SUPERVISOR al usuario ALUMNO

e) Haz que el rol SUPERVISOR sea el rol por defecto de alumno (el que tenga cuando inicie sesión).

f) Comprueba los roles activos del usuario ALUMNO. Desde ALUMNO ejecuta:

```
select * from session_roles;
```

Cierra la sesión con ALUMNO y vuelve a abrirla. Comprueba de nuevo los roles activos.

g) Desde el usuario ALUMNO, activa todos su roles. Después comprueba los roles activos.

h) Desde el usuario ALUMNO, desactiva todos su roles. Después comprueba los roles activos. Cierra la sesión con ALUMNO y vuelve a abrirla. Comprueba de nuevo los roles activos

Ejercicios: seguridad. Ejercicio 17.