1. Usuarios

Un **usuario** es un nombre definido en la base de datos que se puede conectar a ella y acceder a determinados objetos según ciertas condiciones que define el administrador.

Asociado al usuario hay un **esquema** con el mismo nombre que contiene los objetos (tablas, vistas, secuencias, sinónimos, índices, procedures, funciones, clusters, paquetes y database links) propios del usuario.

Un usuario tiene acceso a los objetos de otro usuario si tiene los privilegios suficientes.

Al instalar Oracle se crean automáticamente los usuarios

- SYS
- SYSTEM

Ambos con privilegios de DBA

SYS es propietario del **diccionario de datos** (tablas y vistas donde se guarda toda la información sobre el resto de estructuras de datos; contiene nombres de usuarios, derechos, autorizaciones, restricciones, información de espacio, objetos de BD...)

Nadie, ni un administrador, puede modificar las tablas del SYS

SYSTEM es el usuario encargado de realizar las tareas de administración de la BD, tiene entre otros el privilegio de crear usuarios

VISTAS USER y ALL accesibles a todos los usuarios

VISTAS DBA solo accesibles al administrador

Creación de usuarios

Creación de nuevos usuarios de base de datos

Hay que realizar los siguientes pasos:

1. Seleccionar un nombre de usuario y un mecanismo de autenticación
2. Identificar los tablespaces en los que el usuario debe almacenar los objetos
3. Decidir acerca de las cuotas para cada tablespace
4. Asignar un tablespace por defecto y uno temporal
5. Crear el usuario
6. Otorgar privilegios y roles al usuario.

CREATE USER nombre_usuario

IDENTIFIED BY clave_acceso

[DEFAULT TABLESPACE espacio_tabla]

[TEMPORARY TABLESPACE espacio_tabla]

[QUOTA {entero {K|M} | UNLIMITED} ON espacio_tabla]

[QUOTA {entero {K|M} | UNLIMITED} ON espacio_tabla]

[PASSWORD EXPIRE]

[ACCOUNT (LOCK | UNLOCK)]

[PROFILE perfil];

DEFAULT TABLESPACE espacio_tabla
Especifica el nombre del tablespace para los objetos que cree el usuario.
Si no se especifica será por defecto el tablespace SYSTEM

TEMPORARY TABLESPACE espacio_tabla
Especifica el nombre del tablespace para trabajos temporales
Si no se especifica será por defecto el tablespace TEMP

QUOTA {entero {K|M} | UNLIMITED} ON espacio_tabla
Asigna un espacio en megabytes o kilobytes en el tablespace que se indique (no para los temporales)
Si no tiene cuota no podrá crear objetos en dicho tablespace (si se le da el rol RESOURCE si podrá porque tiene el privilegio unlimited tablespace)

PASSWORD EXPIRE
fuerza a que el usuario cambie su password cuando se conecte mediante SQL

PROFILE perfil
asigna un perfil al usuario
si no se pone, asigna el perfil por omisión
un perfil limita el nº de sesiones concurrentes del usuario, uso de CPU, tiempo de sesión...

Para ver la información de los usuarios que hay en la BD podemos acceder a la vista
DBA_USERS

(Ver qué usuarios hay actualmente)

EJEMPLO 1:

La siguiente orden crea un usuario de nombre USUARIO1. La clave es la misma. El *tablespace* para sus objetos es TRABAJO, en el cual se han asignado 500 kilobytes. El *tablespace* para trabajos temporales es TEMP (ya que no se indica en la orden):

```
CREATE USER USUARIO1
  IDENTIFIED BY USUARIO1
    DEFAULT TABLESPACE TRABAJO
      QUOTA 500K ON TRABAJO;
```

EJEMPLO 2:

La siguiente orden crea un usuario de nombre USUARIO2, la clave es la misma. El *tablespace* por defecto es TRABAJO al cual se han asignado 1 megabyte. El *tablespace* para trabajos temporales es TEMPORAL1 . Se crea con la cuenta bloqueada y que el usuario tenga que cambiar la contraseña cuando acceda por primera vez.

```
CREATE USER USUARIO2 IDENTIFIED BY USUARIO2
        DEFAULT TABLESPACE TRABAJO
        TEMPORARY TABLESPACE TEMPORAL
        QUOTA 1M ON TRABAJO
         PASSWORD EXPIRE
        ACCOUNT LOCK ;
```

Comprobar en DBA_USERS qué información se almacena de estos usuarios

```
SELECT * FROM DBA_USERS
  WHERE USERNAME LIKE 'USUARIO%';
```

Script Output | Query Result | SQL | All Rows Fetched: 2 in 0.042 seconds

	USERNAME	USER_ID	PASSWORD	ACCOUNT_STATUS	LOCK_DATE	EXPIRY_DATE	DEFAULT_TABLESPACE	TEMPORARY_TABLESPACE	CREATED	PROFILE
1	USUARIO1	54	(null)	OPEN	(null)	09-MAY-21	TRABAJO	TEMP	10-NOV-20	DEFAULT
2	USUARIO2	59	(null)	EXPIRED & LOCKED	10-NOV-20	10-NOV-20	TRABAJO	TEMPORAL1	10-NOV-20	DEFAULT

Importante

Una vez creado un usuario hay que darle privilegios para que pueda acceder a la BD, para iniciar una sesión

GRANT CREATE SESSION TO nombre_usuario;
GRANT CONNECT TO nombre_usuario;

```
SQL> connect system/manager
Conectado.
SQL> desc all_users
 Nombre                                    ¿Nulo?   Tipo
 ----------------------------------------- -------- ----------------
 USERNAME                                  NOT NULL VARCHAR2(30)
 USER_ID                                   NOT NULL NUMBER
 CREATED                                   NOT NULL DATE

 SQL> desc dba_users
  Nombre                                    ¿Nulo?   Tipo
  ----------------------------------------- -------- ----------------
  USERNAME                                  NOT NULL VARCHAR2(30)
  USER_ID                                   NOT NULL NUMBER
  PASSWORD                                           VARCHAR2(30)
  ACCOUNT_STATUS                            NOT NULL VARCHAR2(32)
  LOCK_DATE                                          DATE
  EXPIRY_DATE                                        DATE
  DEFAULT_TABLESPACE                        NOT NULL VARCHAR2(30)
  TEMPORARY_TABLESPACE                      NOT NULL VARCHAR2(30)
  CREATED                                   NOT NULL DATE
  PROFILE                                   NOT NULL VARCHAR2(30)
  INITIAL_RSRC_CONSUMER_GROUP                        VARCHAR2(30)
  EXTERNAL_NAME                                      VARCHAR2(4000)
```

Modificación de usuarios

ALTER USER nombre_usuario
IDENTIFIED BY clave_acceso
[
todo lo que aparece al crear
];

- En principio un usuario solo puede cambiar su clave de acceso
- Si tiene privilegio ALTER USER podrá modificar lo demás

EJEMPLO 3:

Desbloquear la cuenta USUARIO2

ALTER USER USUARIO2 ACCOUNT UNLOCK;

Cambiar la contraseña a USUARIO2 por OTRA

ALTER USER USUARIO2 IDENTIFIED BY OTRA;

Borrado de usuarios

DROP USER nombre_usuario;

Si tiene objetos dará error, tendremos que poner

DROP USER nombre_usuario CASCADE;

que borrará el usuario y sus objetos

- Es necesario tener privilegio DROP USER
- No se puede borrar un usuario que esté conectado

Privilegios

Un **privilegio** es la capacidad de un usuario dentro de la BD de realizar determinadas operaciones o acceder a determinados objetos de otros usuarios.

Al crear un usuario es necesario otorgarle privilegios para que pueda hacer algo

Un **rol** (o función) es un conjunto de privilegios

Se puede otorgar a un usuario privilegios o roles

ROLES	PRIVILEGIOS
CONNECT	**Alter session** Create cluster Create database Link Create sequence **Create session** Create synonym **Create table** Create view
RESOURCE	Create cluster **Create procedure** **Create table** Create sequence **Create trigger** **Unlimited tablespace** Create type Create operator Create indextype
DBA	Posee todos los privilegios

➢ Privilegios sobre los objetos

Permiten acceder y realizar cambios en los datos de otros usuarios. Por ejemplo, el privilegio de consultar la tabla de otro usuario es un privilegio sobre objetos

Se dispone de los siguientes privilegios sobre tablas, vistas y procedures:

Privilegio sobre los objetos	Sentencia SQL permitida con cada privilegio
ALTER	ALTER objeto (tabla)
DELETE	DELETE FROM objeto (tabla o vista)
EXECUTE	EXECUTE objeto (procedimiento)
INSERT	INSERT INTO objeto (tabla o vista)
SELECT	SELECT ... FROM objeto (tabla o vista)
UPDATE	UPDATE objeto (tabla o vista)

La orden para dar privilegios sobre los objetos es **GRANT** con el siguiente formato:

GRANT {privilegio [, privilegio]... |ALL }
ON [usuario.]objeto
TO {usuario|rol|PUBLIC} [,{usuario|rol|PUBLIC} ...]
[**WITH GRANT OPTION**];

ON especifica el objeto sobre el que se dan los privilegios
TO identifica a los usuarios o roles a los que se conceden los privilegios
ALL concede todos los privilegios
WITH GRANT OPTION permite que el receptor del privilegio o rol se lo asigne a otros usuarios o roles
PUBLIC asigna los privilegios a todos los usuarios actuales y futuros

➢ Privilegios del sistema

Dan derecho a ejecutar un tipo de comando SQL o a realizar alguna acción sobre objetos de un tipo especificado

Por ejemplo: crear, modificar y borrar tablespaces, índices, clusters, links, procedimientos, profiles, sequences, synonim, tables, triggers, users, views

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.

(Continúa)

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

Para dar privilegios del sistema:

GRANT {privilegio|rol [, privilegio|rol]... }
TO {usuario|rol|PUBLIC} [,{usuario|rol|PUBLIC} ...]
[**WITH ADMIN OPTION**];

- **Retirada de privilegios**

Al igual que se otorgan, se pueden retirar privilegios o roles concedidos a usuarios.

Para privilegios de objetos:

REVOKE {privilegio [, privilegio]... |ALL }
ON [usuario.]objeto
FROM {usuario|rol|PUBLIC} [,{usuario|rol|PUBLIC} ...];

Para privilegios del sistema:

REVOKE {privilegio|rol [, privilegio|rol]... }
FROM {usuario|rol|PUBLIC} [,{usuario|rol|PUBLIC} ...];

Vistas con información de los privilegios:

SESSION_PRIVS	privilegios del usuario activo

(comprobar en system y en usuasir)

➢ Roles

Un rol o función es un conjunto de privilegios que recibe un nombre.

Los privilegios de un rol pueden ser del sistema o a nivel de objeto

Para crear un rol ha de ser un usuario DBA o tener privilegio CREATE ROL

Crear un rol:

CREATE ROLE nombre_rol
[IDENTIFIED BY contraseña];

Tras crearlo se le conceden privilegios:

GRANT privilegio,...privilegio **TO** nombre_rol;

Supresión de privilegios en un rol:

REVOKE privilegio,...privilegio **FROM** nombre_rol;

Supresión de un rol:

DROP ROLE nombre_rol;

Vistas con información de roles:

SESSION_ROLES	roles activos para el usuario
DBA_ROLES	todos los roles
DBA_ROLE_PRIVS	privilegios asignados a todos los usuarios y roles

➢ Perfiles

Create profile

Esta sentencia sirve para crear un perfil de usuario.

Un perfil de usuario es una forma de limitar los recursos que puede utilizar un usuario.

Cada usuario puede tener un único perfil.

Antes de asignar un perfil a un usuario es necesario que este perfil exista en la base de datos.

Un perfil se asigna en la creación de un usuario CREATE USER o modificandolo ALTER USER.

Un ejemplo de script sería:

Copiar

```
CREATE PROFILE app_user LIMIT
  SESSIONS_PER_USER               2   --
  CPU_PER_SESSION             10000   -- decimas de segundo
  CPU_PER_CALL                    1   -- decimas de segundo
  CONNECT_TIME              UNLIMITED -- minutos
  IDLE_TIME                      30   -- minutos
  LOGICAL_READS_PER_SESSION   DEFAULT -- DB BLOCKS
  LOGICAL_READS_PER_CALL      DEFAULT -- DB BLOCKS
  -- COMPOSITE_LIMIT          DEFAULT --
  PRIVATE_SGA                    20M  --
  FAILED_LOGIN_ATTEMPTS           3   --
  PASSWORD_LIFE_TIME             30   -- dias
  PASSWORD_REUSE_TIME            12   --
  PASSWORD_REUSE_MAX        UNLIMITED --
  PASSWORD_LOCK_TIME          DEFAULT -- dias
  PASSWORD_GRACE_TIME             2   -- dias
  PASSWORD_VERIFY_FUNCTION       NULL;
```

Los recursos que limitamos son recursos del kernel: uso de la CPU, duración de sesion,...

Y tambien limites de uso de las claves de acceso (passwords): duración, intentos de acceso, reuso, ...

Por ejemplo:

Copiar

```
ALTER PROFILE default LIMIT IDLE_TIME  20;
```

Limita el perfil por defecto a 20 minutos. IDLE_TIME: Es el tiempo que puede estar una sesión sin hacer nada antes de ser cerrada.

El perfil por defecto de los usuarios es DEFAULT que da recursos ilimitados sobre la base de datos.

Los perfiles limitan los recursos de los usuarios, para que funcionen hay que poner a TRUE la variable del sistema RESOURCE_LIMIT que por defecto está a FALSE.

ALTER SYSTEM SET RESOURCE_LIMIT = TRUE;

En realidad hay dos tipos de parámetros de los perfiles:

- **Perfiles de manejo de contraseñas**, que gestionan el funcionamiento de las contraseñas para el usuario.

Variable de perfil	Significado
FAILED_LOGIN_ATTEMPTS	Número consecutivo de errores en las contraseñas antes de bloquear la cuenta. Por defecto son 10
PASSWORD_LOCK_TIME	Número de días hasta que se bloquea una cuenta si se supera el límite de intentos al meter una contraseña. Por defecto es uno
PASSWORD_LIFE_TIME	Números de días que tiene vigencia una contraseña. Por defecto es 180
PASSWORD_GRACE_TIME	Días que la contraseña se la concede un periodo extra de gracia tras consumir su tiempo de vida. Por defecto es 7
PASSWORD_REUSE_TIME	Número de días que una contraseña puede ser reutilizada
PASSWORD_VERIFY_FUNCTION	Función a la que se invoca cuando se modifica una contraseña con el fin de verificar su validez en base a las reglas de complejidad que deseemos

Perfiles relacionados con el uso de recursos. Establecen el máximo o mínimo uso de recursos de la base de datos por parte del usuario.

Variable de perfil	Significado
SESSIONS_PER_USER	Número de conexiones de usuario concurrentes que se permiten.
CPU_PER_SESSION	Límite de tiempo (en centésimas de segundo) que se permite a un usuario utilizar la CPU antes de ser echado del sistema. De esa forma se evitan peligros de rendimiento
CPU_PER_CALL	Como la anterior pero referida a cada proceso
PRIVATE_SGA	Para conexiones en instalaciones de servidor compartido, número de KB que puede consumir cada sesión en la zona de memoria compartida (SGA)
CONNECT_TIME	Minutos como máximo que se permite a una sesión
IDLE_TIME	Minutos máximos de inactividad de una sesión
LOGICAL_READS_PER_SESSION	Máximo número de bloques leídos en una sesión
LOGICAL_READS_PER_CALL	Máximo número de bloques leídos por un proceso
COMPOSITE_LIMIT	Máximo número de recursos consumidos por una sesión. Es la media ponderada de varios parámetros anteriores

La vista DBA_PROFILES contiene información sobre los límites.

La orden ALTER PROFILE permite modificar una determinada configuración de perfil. El formato es el mismo que el de la orden CREATE PROFILE.

Borrado de un perfil

Para borrar un perfil de la base de datos se usa la orden DROP PROFILE, que tiene el siguiente formato:

```
DROP PROFILE NombrePerfil [CASCADE];
```

Si algún usuario lo tiene asignado es necesario incluir la opción CASCADE. Ejemplo: `DROP PROFILE PERFIL2 CASCADE;`