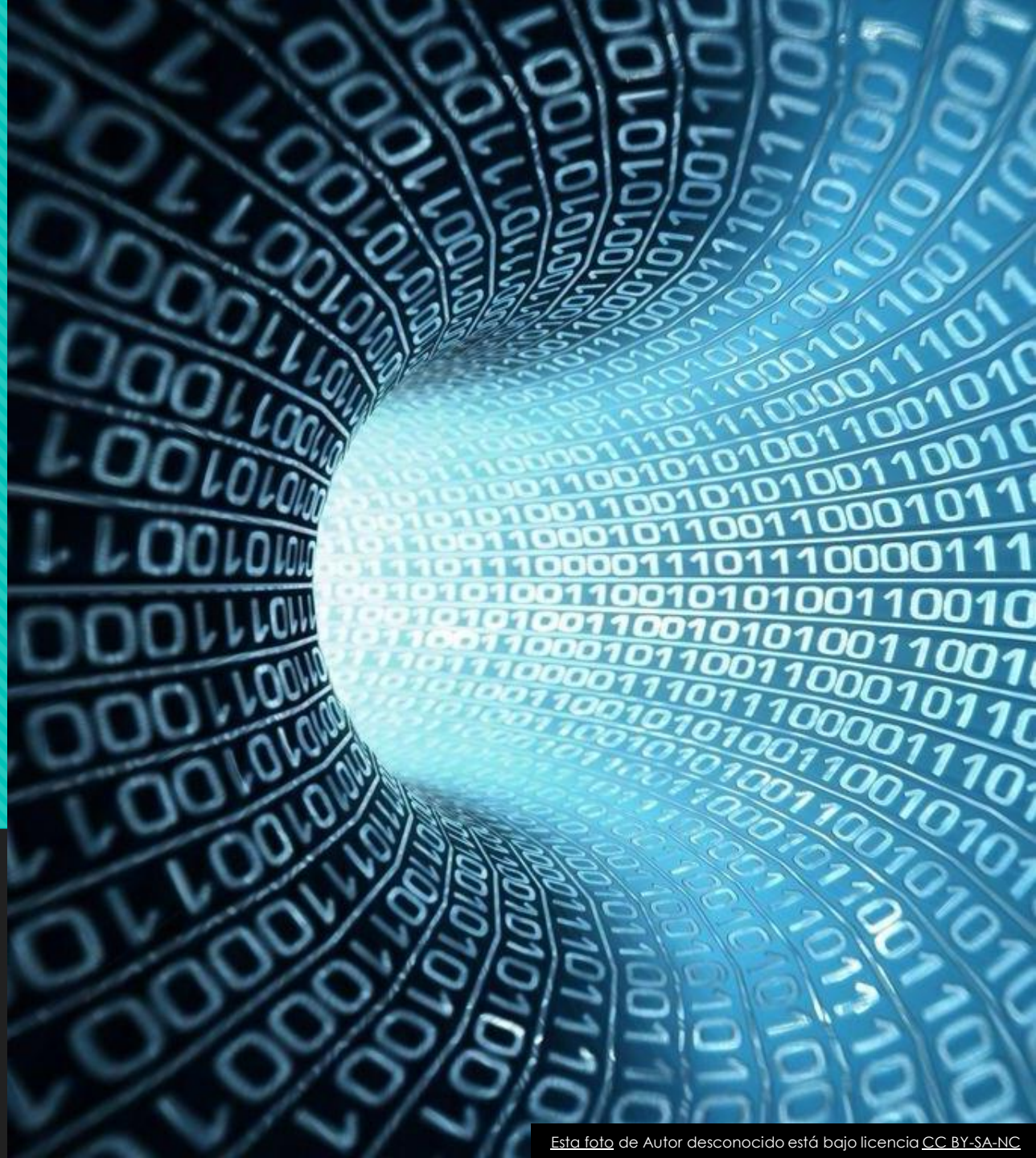
Bases de datos 2

Clase 3

Kevin Morán

bases2.fiusac@gmaill.com



SEGURIDAD

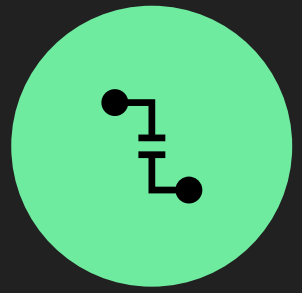
Administración de usuarios

Introducción

- Todo acceso a una base de datos requiere conectar mediante un usuario y contraseña. Dicho usuario dará derecho a utilizar ciertos objetos de la base de datos, pero tendrá restringido (salvo que se trate de un superadministrador) el uso de otros.
- A los usuarios se les asigna una serie de **privilegios** que son los que dan permiso de uso a ciertos objetos. Estos privilegios suelen agruparse en lo que se conoce como **roles**, que permiten estructurar mejor los permisos que se conceden a los usuarios. El **perfil** del usuario será el conjunto de permisos y restricciones que se aplican a dicho usuario.
- Por ello cuando un usuario conecta debe probar que es quien dice ser (normalmente mediante una contraseña), es decir se autentifica. Por otro lado esta autentificación dará lugar a unos privilegios (unos derechos) y unas restricciones
- Todo lo que se explica en esta presentación se refiere a la gestión de usuarios en la base de datos **Oracle 11g**.

Cuentas y permisos administrativos

Cuentas administrativas



SYS. Inicialmente posee la contraseña **CHANGE_ON_INSTALL** que, lógicamente, hay que cambiar inmediatamente en la instalación. SYS toma rol de DBA (es decir, de superadministrador) y es en su esquema donde se crea el diccionario de datos; por lo que no conviene de ninguna manera crear otro tipo de elementos en su esquema; es decir, el usuario SYS no debe crear tablas, ni vistas no ningún otro objeto de la base de datos.

SYSTEM. Posee también el rol DBA y se crea durante la instalación. Como antes, la contraseña **MANAGER** que tiene por defecto se debería cambiar en la instalación. En su esquema se suelen crear tablas y vistas administrativas (pero no se deberían crear otro tipo de tablas).

SYSMAN. Usado para realizar tareas administrativas con la aplicación **Database Control** del**Enterprise Manager**.

DBSMNP. Usuario que tiene permisos para monitorizar Enterprise Manager.

ROLES administrativos

SYSDBA. Con capacidad de parar e iniciar (instrucciones **SHUTDOWN** y **STARTUP**) la instancia de base de datos; modificar la base de datos (**ALTER DATABASE**), crear y borrar bases de datos (**CREATE** y **DROP DATABASE**), Crear el archivo de parámetros (**CREATE SPFILE**), cambiar el modo de archivado de la base de datos, recuperar la base de datos y además incluye el privilegio de sistema **RESTRICTED SESSION**. En la práctica sus capacidades son las asociadas al usuario **SYS**.

SYSOPER. Permite lo mismo que el anterior salvo: crear y borrar la base de datos y recuperar en todas las formas la base de datos (hay modos de recuperación que requieren el privilegio anterior).

Propiedades de los usuarios

- **Nombre de usuario**. No puede repetirse y como máximo debe tener 30 caracteres que sólo podrán contener letras del alfabeto inglés, números, el signo dólar y el signo de guión bajo (_). Además el nombre no puede comenzar con un número.
- **Configuración física**. Se refiere al espacio asociado al usuario para almacenar sus datos (lo que Oracle llama **tablespace**) y la cuota (límite de almacenamiento) que se le asigna a dicho usuario y mediante la que se establece el espacio máximo que el usuario puede gastar en el tablespace.
- **Perfil asociado**. El perfil del usuario indica los recursos y configuración que tomará el usuario al sistema
- **Privilegios y roles**. Permiten especificar los permisos que posee el usuario.
- **Estado de la cuenta de usuario**:
  - **Abierta**. El usuario puede conectar y realizar sus acciones habituales
  - **Bloqueada**. El usuario no podrá conectar mientras siga en estado bloqueado. El bloqueo lo realiza el DBA:
    - **AL TER USER** usuario **ACCOUNT LOCK**
  - **Expirada**. La cuenta agotó el tiempo máximo asignado a ella. Para salir de este estado, el usuario/a debe resetear su contraseña de usuario.
  - **Expirada y bloqueada**.
  - **Expirada en periodo de gracia**. Está en los últimos momentos de uso antes de pasar a estado de expirada

Autentificación

Autentificación por sistema operativo

- Se permite el uso sólo en usuarios con privilegios administrativos. En el sistema operativo en el que se instale Oracle se crean dos **grupos** de usuarios relacionados con los dos privilegios de sistema **SYDBA** y **SYSOPER**. En Windows se llaman **ORA_DBA** y **ORA_OPER** respectivamente, en Linux normalmente son **dba** y **oper**.
- Los usuarios de esos grupos conectarían mediante **CONNECT / AS SYSDBA** o **CONNECT / AS SYSOPER**.

Autentificación por archivo de contraseñas

- Se usa también para usuarios administrativos, especialmente cuando no se confía la autentificación vista en el apartado anterior.
- Para usar esta forma de autentificación los usuarios de tipo SYSDBA o SYSOPER indican su nombre de usuario y contraseña al conectar (opcionalmente indican el host y/o nombre de servicio al que se desean conectar) esos datos se contrastarán con los del archivo de contraseñas utilizado.
- Esta forma (y la anterior) permite conectar la base de datos aunque no esté montada todavía la base de datos.

Autentificación por contraseña en el diccionario de datos

- Es la forma habitual de autentificarse de los usuarios normales (los que no son administradores). En este caso los usuarios son autentificados mediante una contraseña que se contrastará en el diccionario de datos, que es donde se almacenan estas contraseñas.
- Está configuración requiere la base de datos montada y abierta (al tener que usar el diccionario de datos).
- La contraseña se pasa encriptada desde el ordenador cliente al servidor mediante el algoritmo **AES**.

Auntentificación externa

- Oracle delega la autentificación a un servicio externo que se asociará a Oracle. Ejemplos de servicios externos son **Kerberos** o **RADIUS**, este último sólo disponible en Windows. Requiere el uso de las mejoras de seguridad avanzada de Oracle.

Control de usuarios

Creación

```
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}]
```

```
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
```

Modificación y borrado

```
ALTER USER jsanchez QUOTA UNLIMITED ON usuarios
```

```
DROP USER usuario [CASCADE]
```

Control 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.
- **Privilegios de objeto**. Son permisos que se aplican a un objeto concreto de la base de datos.

Privilegios de sistema

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: ALTERSYSTEM 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

Conceder y revocar privilegios

```
GRANT privilegio1 [,privilegio2[,…]] TO usuario
[WITH ADMIN OPTION];
```

```
GRANT   CREATE SESSION, ALTER SESSION, CREATE TABLE,
CREATE VIEW, CREATE SYNONYM, CREATE SEQUENCE,
CREATE TRIGGER, CREATE PROCEDURE, CREATE TYPE
TO jsanchez;
```

```
REVOKE privilegio1 [,privilegio2 [,…]]  FROM usuario;
```

Privilegios de objeto

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

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

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

Administración de roles

```
CREATE ROLE rol  [NOT IDENTIFIED |
        IDENTIFIED {BY password  | EXTERNALLY | GLOBALLY | USING package}];
```

```
GRANT CREATE TABLE, CONNECT TO rol1;
```

```
REVOKE CREATE TABLE FROM rol1;
```

```
GRANT rol1 [,rol2 [,…]]
TO  {usuario|rol|PUBLIC [,{usuario|rol|PUBLIC} [,…] }
[WITH ADMIN OPTION]
```

Roles predefinidos

Oracle dispone de una serie de roles predefinidos que se pueden asignar a los usuarios. Hay más de cincuenta roles predefinidos. Los clásicos son:

rol	significado
CONNECT	Permite crear sesiones. Se mantiene por compatibilidad
RESOURCE	Permite crear tablas y código PL/SQL del tipo que sea. Se mantiene por compatibilidad
DBA	Permite casi todo, excepto manejar la instancia de la base de datos

Activar y desactivar roles

- No todos los roles aparecen activados. Para saber los roles que están activados en una sesión de usuario, bastará con consultar el contenido de la vista **SESSION_ROLES**.
- Al iniciar sesión cada usuario tendrá activados los privilegios que se le asignaron explícitamente y los roles por defecto.
- La activación (y también la desactivación) de un rol se realiza mediante **SET ROLE** (sólo podemos activar y desactivar roles que el usuario tenga asignados mediante la instrucción GRANT).

Administración de perfiles

- Los perfiles permiten limitar los recursos que los usuarios usan de la base de datos. Hay un perfil llamado **DEFAULT** que se aplica automáticamente a todos los usuarios y que les da recursos ilimitados sobre la base de datos. Para limitar el número de recursos se debe de activar (poniéndola el valor **TRUE)** la variable de sistema **RESOURCE_LIMIT** (que por defecto está a **FALSE**). Esto se hace así:

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

(Parámetros) Perfiles de manejo de contraseñas

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

(Parámetros) Perfiles relacionados con el uso de recursos

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

```
CREATE PROFILE perfil LIMIT parámetro1 valor1 [parametro2 valor [...]]
```

```
CREATE PROFILE programador LIMIT
                SESSIONS_PER_USER UNLIMITED
                CPU_PER_SESSION UNLIMITED
                IDLE_TIME 15
                CONNECT_TIME 150
                FAILED_LOGIN_ATTEMPTS 5
                PASSWORD_LOCK_TIME 2;
```

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

```
ALTER USER jsanchez PROFILE programador;
```