UT 3

GESTION DE LA SEGURIDAD

ÍNDICE UNIDAD 3

- Creación, modificación y eliminación de usuarios
- Asignación y retirada de permisos a usuarios
- Creación y eliminación de roles
- Asignación y retirada de permisos de roles

Creación, modificación y eliminación de usuarios

- Puede haber varios usuarios diferentes de la base de datos. Cada uno es propietario de sus objetos.
- Para crear un usuario debemos conectarnos a la base datos como administradores (por ejemplo "system").
- Consulta los usuarios de una BD

  SELECT USERNAME FROM DBA_USERS;

- Sintaxis básica para crear un usuario:

create user NOMBREUSUARIO identified by CONTRASEÑA;

- default tablespace NOMBRETABLESPACEPORDEFECTO
- quota CANTIDAD on TABLEESPACE;
- default role ROLE, ALL;

Creación, modificación y eliminación de usuarios

- La cláusula "default tablespace" será el tablespace (espacio de tablas) por defecto en la creación de objetos del usuario. Si se omite se utilizará el tablespace SYSTEM. Los tablespaces son unidades lógicas en las cuales de divide una base de datos, en las cuales se almacenan los objetos (tablas, secuencias, etc.); todos los objetos están almacenados dentro de un tablespace.
- La cláusula "quota" permite configurar un espacio en bytes, Kb o Mb en la base de datos. Si no se especifica, por defecto es cero y no podrá crear objetos. Se puede indicar UNLIMITED.
- La cláusula "default role" permite asignar roles de permisos durante la creación del usuario.

Creación, modificación y eliminación de usuarios

- La modificación de usuarios se hace utilizando la cláusula ALTER

Alter user USUARIO identified by nuevacontraseña;
ALTER USER username ACCOUNT LOCK / UNLOCK;

- Para borrar un usuario realizamos la siguiente instrucción:

  Drop user “usuario”;

En caso de que tenga tablas y estén relacionadas colocamos:

  Drop user “usuario” cascade;

Asignación y retirada de permisos a usuarios

- En Oracle existen dos tipos de privilegios de usuario.
- **Sistema**: Permite al usuario hacer ciertas tareas sobre la BD, como por ejemplo crear un Tablespace. Estos permisos son otorgados por el administrador o por alguien que haya recibido el permiso para administrar ese tipo de privilegio. Existen como 100 tipos distintos de privilegios de este tipo.
- En general los permisos de sistema, permiten ejecutar comandos del tipo DDL (Data definition Language), como CREATE, ALTER y DROP o del tipo DML (Data Manipulation Language). Oracle tiene más de 200 privilegios de sistema los cuales pueden ser vistos consultando la vista: SYSTEM_PRIVILEGE_MAP
- Entre todos los privilegios de sistema que existen, hay dos que son los importantes: SYSDBA y SYSOPER. Estos son dados a otros usuarios que serán administradores de base de datos.
- Para otorgar varios permisos a la vez, se hace de la siguiente manera:

```
GRANT CREATE USER, ALTER USER, DROP USER TO usuario;
```

Asignación y retirada de permisos a usuarios

- **Objecto**: Este tipo de permiso le permite al usuario realizar ciertas acciones en objetos de la BD, como una Tabla, Vista, un Procedure o Función, etc. Si a un usuario no se le dan estos permisos sólo puede acceder a sus propios objetos (véase USER_OBJECTS). Este tipo de permisos los da el owner o dueño del objeto, el administrador o alguien que haya recibido este permiso explícitamente (con Grant Option).

- Por ejemplo, para otorgar permisos a una tabla Ventas para un usuario particular:

- GRANT SELECT,INSERT,UPDATE ON HR.JOBS TO usuario;

- Adicionalmente, podemos restringir los DML a una columna de la tabla mencionada. Si quisiéramos que este usuario pueda dar permisos sobre la tabla JOBS a otros usuarios, utilizamos la cláusula WITH GRANT OPTION. Ejemplo:

- GRANT SELECT,INSERT,UPDATE,DELETE ON HR.JOBS TO usuario2 WITH GRANT OPTION;

Asignación / retirada de permisos a usuarios

- Los permisos se asignan a los usuarios con la instrucción **GRANT** y se quitan con la instrucción **REVOKE.**

```
REVOKE ALL PRIVILEGES FROM usuario;

REVOKE <derecho1>, <derecho2>, ...
ON TABLE <nombre tabla>
FROM <usuario1>, <usuario2> ...;

REVOKE CREATE TABLE FROM usuario;
```

Creación y eliminación de roles

- Los roles son un conjunto de privilegios que se pueden otorgar a un usuario o a otro Rol. De esa forma se simplifica el trabajo del DBA en esta tarea.
  - Al crear el rol se puede incluir la cláusula IDENTIFIED e incluir una password u otro tipo de autenticación.
- Un usuario puede tener múltiples roles.
- A un rol se le pueden asignar otros roles.
- Para crear / eliminar un Rol se hace de la siguiente manera:

  CREATE / DROP ROLE appl_dba;

- Para asignar este Rol a un usuario / rol:

  GRANT appl_dba TO usuario / rol;

Asignación / retirada de permisos a roles

- Los permisos sobre roles se asignan y se retiran de igual manera que usuarios, con la misma sintaxis sustituyendo el usuario por el rol (GRANT / REVOKE).
- Para consultar los roles definidos y los privilegios otorgados a través de ellos, utilize las vistas:

  select * from DBA_ROLES;
  select * from DBA_ROLE_PRIVS order by GRANTEE (meter condición en el where para filtrar por un usuario);

Asignación / retirada de permisos a roles

- Los roles que tiene asignado un usuario en una sesión se pueden consultar haciendo una Select sobre la vista session_roles

- 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

Asignación / retirada de permisos a 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). Su sintaxis es:

```
SET ROLE
{ rol1 [IDENTIFIED BY contraseña]
 [,rol2 [IDENTIFIED BY contraseña] [,…]]
 | ALL [EXCEPT rol1 [,rol2 [,…]]]
 | NONE
  };
```

- Las posibilidades son:
  - Indicar una lista de roles que serán los que se activen (se usa cuando se habían desactivado)
  - Indicar ALL para activar todos los roles, excepto aquellos que se indiquen en la cláusula EXCEPT que quedarán sin activar.
  - NONE desactiva todos los roles (incluido el rol por defecto). Sólo quedarán activados los privilegios individuales marcados explícitamente.
  - La activación y desactivación sólo sirve para la sesión actual, en la siguiente sesión volverán a estar activados sólo los roles por defecto

Anexo - Resumén

USUARIOS	CREATE USER “X” IDENTIFIED BY “Y” [TABLESPACE / ROLE / PROFILE/QUOTA] DROP USER “X” [CASCADE] ALTER USER “X”
PRIVILEGIOS	GRANT “PRIV” [ON “OBJETO”] TO “USUARIO/ROL” [WITH GRANT OPTION] REVOKE “PRIV” [ON “OBJETO”] FROM “USUARIO/ROL”
ROLES	CREATE ROLE “ROL” DROP ROLE “ROL”
TABLESPACE	CREATE TABLESPACE DROP TABLESPACE ALTER TABLESPACE

No es fácil comprobar todos los privilegios asociados a un usuario. Link a una página con una utilidad para hacerlo:

http://www.petefinnigan.com/find_all_privs.sql

Anexo - Descripción de privilegios

Veamos 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.
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

Anexo - Descripción de privilegios

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

Anexo - Descripción de privilegios

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

Anexo - Descripción de privilegios

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

Anexo - Descripción de privilegios

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
ADMINISTER DATABASE TRIGGER	Crear triggers de sistema (requiere además el privilegio **CREATE TRIGGER**)

Anexo - Descripción de privilegios

DROP ANY TRIGGER	Borrar cualquier trigger
DROP LIBRARY	Borrar librería de procedimientos y funciones en el esquema de usuario
DROP ANY LIBRARY	Borrar librerías de procedimientos y funciones en cualquier esquema
EXECUTE ANY LIBRARY	Ejecutar cualquier librería
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 cualquier 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

Anexo - Descripción de privilegios

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
SELECT ANY SEQUENCE	Seleccionar cualquier secuencia de cualquier esquema

Anexo - Descripción de privilegios

Programación de tareas	
CREATE JOB	Crear trabajo planificado en el esquema actual
CREATE ANY JOB	Crea, modifica y elimina tareas, programas y credenciales de cualquier esquema (excepto SYS). Esto permite ejecutar código en cualquier esquema de cualquier usuario.
CREATE EXTERNAL JOB	Crear un trabajo en el esquema de usuario procedente del planificador de tareas del sistema operativo
EXECUTE ANY PROGRAM	Ejecutar cualquier programa presente en un trabajo planificado del esquema de usuario.
EXECUTE ANY CLASS	Asignar cualquier clase a un trbajo en el esquema de usuario.
MANAGE SCHEDULER	Administrar el planificador de tareas,

Diferencia entre un Schema y un tablespace

- Un Schema(Esquema) son el conjunto de objetos que le pertenecen a un usuario, por ejemplo, teniendo al usuario HR todos los objetos que este crea (tablas, indices, vistas, procedimientos almacenados, triggers) le pertenecen a el y unicamente a el, esto es le pertenecen al schema HR, cualquier otro usuario puede tener acceso a estos objetos siempre y cuando el usuario HR se los otorgue y podrá utilizarlos anteponiendo el nombre del schema ejemplo.

- Un Tablespace es a nivel Oracle el segundo nivel de almacenamiento, a primer nivel de almacenamiento de datos se encuentra las tablas(ejemplo employees), un tablespace se refiere a un nivel del tipo Oracle Operating system si así lo pudiéramos llamar, este a su vez esta constituido a nivel Sistema operativo como tal (ya sea Linux, Unix o windows) por uno o más datafiles, que son archivos visibles al usuario con extensión .DBF, un tablespace almacena, a nivel instancia de oracle, objetos pertenecientes al sistema en si mismo u objetos que un usuario genera, estos objetos pueden ser una vez más tablas, vistas, indices, procedimientos almacenados etc.

Diferencia entre un Schema y un tablespace

- Los objetos propios del sistema se almacenan en los tablespaces system y sysaux, existe un tablespace para guardar las transacciones que no han recibido un commit llamada UNDO, por default existe un tablespace llamada USERS donde por default cualquier usuario creado (a menos que se especifique lo contrario) generara sus objetos y por último un tablespace llamado TEMP que su nombre lo indica todo…

```
BEGIN
    FOR t IN (SELECT * FROM DBA_TABLES where OWNER =
‘HR’) LOOP
        EXECUTE IMMEDIATE 'GRANT SELECT ON ' ||
t.table_name || ' TO DEST_USER';
    END LOOP;
END;
```