Índice

Bibliografía

- Sistemas de bases de datos. Conceptos fundamentales. 3ª Edición
  R. Elmasri y S.B. Navathe. Addison Wesley, 2001
  Capítulo 22
- Database: Principles, Programming, and Performance, 2ª Edición
  P. O'Neil y E. O'Neil. Morgan Kaufmann, 2000
  Capítulo 7
- Oracle 10g: Manual del administrador
  K. Loney. McGraw-Hill, 2005
  Capítulo 10

2.1 Objetivos y requerimientos

- Objetivo:
  - Controlar quién y cómo accede a los datos almacenados

- Requerimientos:
  1. Quién puede acceder a la base de datos
  2. A qué datos puede acceder un usuario determinado
  3. Acceso a ciertos valores de un mismo dato (ver tu sueldo pero no el de los compañeros)
  4. Qué operaciones se pueden realizar sobre los datos (lectura,modificación o eliminación)
  5. Permitir consultas estadísticas pero no consultas de datos concretos
  6. Los privilegios pueden o no ser transferibles
  7. Los accesos pueden restringirse según cuándo o desde dónde se hagan

- Mecanismos:
  - Identificación de usuarios
  - Asignación de privilegios
  - Asignación de recursos
  - Auditorías

2.2 Identificación del usuario

- Para determinar qué privilegios tiene un usuario, antes hay que identificarlo
- Por base de datos o por sistema operativo (autentificación externa)
- Técnicas:
  - username + password
  - identificación por preguntas (útil en aplicaciones de internet)
  - identificación por tarjetas o llaves
    - –DNI Electrónico
    - – Servidor RADIUS
  - identificación por características físicas
    - – Huella dactilar
    - – Iris
- Determinación de los privilegios
  - Estrategia D*iscretionary Access Control* (DAC): cada usuario tiene una lista de privilegios
  - Estrategia *Mandatory Access Control* (MAC): cada usuario pertenece a un nivel de prioridad y cada nivel de prioridad tiene asignada una lista de privilegios

2.3 Gestión de privilegios

- **Privilegio**: Derecho a ejecutar un tipo determinado de sentencia SQL o a acceder a un objeto de otro usuario. Pueden asignarse a usuarios o, preferiblemente, a roles
- Algunos privilegios pueden ser transferidos y otros no
- La concesión de un privilegio a un determinado usuario puede revocarse
- Un mismo privilegio puede haber sido obtenido por concesiones distintas y dado por usuarios distintos
- Al revocar un privilegio hay que revocar todos aquellos que se deriven de él

2.4 Asignación y Control de los Recursos del Sistema

- Espacio de disco
  - espacio de almacenamiento principal
  - espacio de almacenamiento temporal
  - cuotas de disco en cada espacio de almacenamiento

- Límites de recursos: básico en grandes sistemas multiusuario (recursos caros)
  - tiempo de CPU: provocado por sentencias SQL, PL/SQL, ...
  - operaciones de E/S: operación más costosa
  - número de sesiones concurrentes
  - tiempo de ocio por sesión
  - tiempo de conexión

2.5 Auditoría

Consiste en mantener un fichero especial donde el sistema registra de forma automática, toda interacción de los usuarios con la información almacenada en la base de datos

- ¿Qué auditamos?
  - usuario: quién accede a los datos
  - fecha y hora: cuándo se accedió a los datos
  - puesto: desde qué tipo de dispositivo/aplicación
  - ubicación: desde qué ubicación en la Red
  - operación: cuál fue la sentencia SQL ejecutada
  - objetos afectados: cuál fue el efecto del acceso a la base de datos

- Tipos de auditorias:
  - De sentencias
  - De privilegios
  - De esquema
  - De grano fino

2.6 Seguridad en SQL (Oracle) (i)

- Oracle distingue entre dos tipos de privilegios:
  - Del sistema: qué tipo de cosas podemos hacer sobre la base de datos: conectarnos, crear objetos, administrarla, modificar sesiones de usuario.
  - De objetos: qué sentencias SQL puedo realizar sobre esquemas de usuario.

Privilegio Objeto	Tabla	Vista	Secuencia	Procedimiento
ALTER	XXX	XXX	XXX	XXX
DELETE	XXX	XXX		
EXECUTE				XXX
INDEX	XXX	XXX		
INSERT	XXX	XXX		
REFERENCES	XXX			
SELECT	XXX	XXX	XXX	
UPDATE	XXX	XXX		

2.6 Seguridad en SQL (Oracle) (ii)

- Gestión de privilegios
  - De sistema:

```
GRANT system_priv(s) TO {user, | role, |PUBLIC}
[IDENTIFIED BY password] [WITH ADMIN OPTION];
REVOKE privilegio ...
FROM {user | role | PUBLIC} ...;
```

  - De objeto:

```
GRANT privilegio [ (column [, column] ...) ] ...
ON objeto
TO {usuario | role | PUBLIC} ...
[WITH GRANT OPTION];
```

  - Revocar privilegio:

```
REVOKE privilegio ...
ON objeto
FROM {user | role | PUBLIC} ...
[CASCADE CONSTRAINT];
```

2.6 Seguridad en SQL (Oracle) (iii)

- Política de transmisión/revocación de privilegios en ORACLE:
  - Para perder un privilegio es necesario que lo revoquen todos aquellos que lo dieron.
  - Los privilegios de tipo sistema no se elimina en cascada (hay que revocarlos explícitamente a cada usuario).
  - Los privilegios de tipo objeto sí se eliminan en cascada, siempre, sin tener en cuenta el momento en que se concedieron.
  - Los privilegios de tipo objeto solo pueden ser revocados por el mismo usuario que los transmitió (`with grant option`).

2.6 Seguridad en SQL (Oracle) (iv)

- Gestión de privilegios a través de ROLES
  - Rol: grupo de privilegios, de sistema o sobre objetos, a los que se les da un nombre y pueden ser asignados a otros usuarios y roles.
  - Pueden otorgarse a cualquier usuario o rol, pero no a si mismo y tampoco de forma circular.
  - Pueden tener contraseña.
  - Su nombre es único en la bd, distinto a cualquier otro nombre de usuario o rol.
  - No pertenecen a ningún esquema.
  - Si un rol cambia automáticamente cambian los privilegios de sus usuarios.
  - Es posible activar/desactivar temporalmente un rol para un conjunto de usuarios.

```
CREATE ROLE nombre_role [IDENTIFIED BY <CONTRASEÑA> | NOT IDENTIFIED];
```

```
Ej.:    CREATE ROLE Rmecanico;
        CREATE ROLE Radmin;

        GRANT select,insert,update ON trabajo TO Rmecanico;
        GRANT select,insert,update ON mecanico TO Radmin;
        GRANT select,insert,update ON trabajo  TO Radmin;
        GRANT Rmecanico TO antonio,lola;
        GRANT Radmin TO luis;
        GRANT select,insert,update ON coche TO Radmin;
```

2.6 Seguridad en SQL (Oracle) (v)

- Asignación y control de recursos del sistema

  – Profile: Conjunto, con nombre, de límites de utilización de recursos

```
CREATE PROFILE perfil
LIMIT    [SESSIONS_PER_USER          {núm_entero | UNLIMITED | DEFAULT}]
         [CPU_PER_SESSION            {núm_entero | UNLIMITED | DEFAULT}]
         [CPU_PER_CALL               {núm_entero | UNLIMITED | DEFAULT}]
         [CONNECT_TIME               {núm_entero | UNLIMITED | DEFAULT}]
         [IDLE_TIME                  {núm_entero | UNLIMITED | DEFAULT}]
         [LOGICAL_READS_PER_SESSION  {núm_entero | UNLIMITED | DEFAULT}]
         [LOGICAL_READS_PER_CALL     {núm_entero | UNLIMITED | DEFAULT}]
         [PRIVATE_SGA                {núm_entero | UNLIMITED | DEFAULT}]
         [COMPOSITE_LIMIT            {núm_entero | UNLIMITED | DEFAULT}]
         [FAILED_LOGIN_ATTEMPTS      {núm_entero | UNLIMITED | DEFAULT}]
         [PASSWORD_LIFE_TIME         {núm_entero | UNLIMITED | DEFAULT}]
         [PASSWORD_GRACE_TIME        {núm_entero | UNLIMITED | DEFAULT}]
         [PASSWORD_REUSE_TIME        {núm_entero | UNLIMITED | DEFAULT}]
         [PASSWORD_LOCK_TIME         {núm_entero | UNLIMITED | DEFAULT}]
         [PASSWORD_VERIFY_FUNCTION   {núm_entero | UNLIMITED | DEFAULT}]
;
```

2.6 Seguridad en SQL (Oracle) (y vi)

- Asignación y control de recursos del sistema
  – Espacio de almacenamiento y cuotas

```
CREATE USER usuario
IDENTIFIED {BY password | EXTERNALLY}
[DEFAULT TABLESPACE tablespace]
[TEMPORARY TABLESPACE tablespace]
[QUOTA {número_entero [K|M] | UNLIMITED} ON tablespace] ...
[PROFILE perfil];
```

Ejemplo:

```
create profile LIMITED_PROFILE
   limit FAILED_LOGIN_ATTEMPTS 5
         SESSION_PER_USER 2
         CONNECT TIME 30
         IDLE_TIME 5

create user JANE identified by EYRE
   profile LIMITED_PROFILE;

grant CREATE SESSION to JANE;
```

2.7 Vistas

- Tabla virtual que obtiene sus datos de otra/s tabla/s de la base de datos
- Principales usos desde el punto de vista de la seguridad:
  - Mostrar sólo determinados atributos:
    - Ej.: No permitir el acceso a los sueldos

```
CREATE VIEW v_mec AS
    SELECT nombre,puesto
    FROM mecanico;
```

  - Mostrar sólo determinadas tuplas:
    - Ej.: Cada mecánico ve las reparaciones de su puesto

```
CREATE VIEW v_trab_chapa AS
   SELECT *
   FROM trabajos
   WHERE DNI IN (SELECT dni FROM mecanico WHERE puesto='CHAPA');
```

  - Generalmente, los usuarios de la base de datos sólo tienen privilegios sobre determinadas vistas (esquemas externos) y no sobre las tablas reales

```
GRANT select,insert,update ON v_mec TO Rmecanico;
GRANT select ON v_trab_chapa TO Rmecanico_chapa;
```

2.8 vistas en el diccionario de datos

Vista	Objeto
DBA_PROFILES	Perfiles en la base de datos
USER_RESOURCE_LIMITS	Parámetros de recursos asignados al usuario
DBA_ROLES	Roles existentes en la base de datos
DBA_USERS ALL_USERS USER_USERS	Usuarios de la base de datos Usuarios visibles por el usuario actual Describe al usuario actual
DBA_ROLE_PRIVS	Roles concedidos a usuarios
DBA_TAB_PRIVS	Permisos sobre objetos de la base de datos
DBA_SYS_PRIVS	Privilegios del sistema a usuarios y roles
SYSTEM_PRIVILEGE_MAP	Listado de todos los privilegios de sistema

2.9 Ejercicios

Dado el siguiente modelo lógico de datos:

```
create table al;
cod number(5,0) primary key,
dni varchar2(9) unique not null,
nombre varchar2(20) not null,
apellidos varchar2 (40) not null ,
email varchar2(20),
movil number(9),
direccion_postal varchar2(50) not null,
poblacion varchar2(50) not null
);

create table asignatura (
  cod number(5,0) primary key,
  nombre varchar2(40) not null,
  titulacion varchar2(40) not null,
  ct number(2,1) not null check (ct>=3 AND ct<=7.5),
  cp number(2,1) not null check (cp>=3 AND cp<=7.5),
  constraint ck_asignatura check (ct+cp<=9)
  );

create table alas (
    cod number(7,0) primary key,
    cod_al number not null references al,
    cod_as number not null references asignatura,
    fecha date,
    nota number(3,1),
    constraint ck_alas unique(cod_al,cod_as,fecha)
);
```

```
create table dpto (
 cod number(3,0) primary key,
 nombre varchar2(40) unique not null
);
create table prof (
 cod number(4,0) primary key,
 dni varchar2(9) unique not null,
 nombre varchar2(20) not null,
 apellidos varchar2 (40) not null ,
 email varchar2(20),
 telefono number(9),
 cod_dpto number references dpto
);


create table area_conocimiento (
 cod number(4,0) primary key,
 nombre varchar2(20) not null,
 cod_dpto number(3,0) references dpto
);

create table profas (
  cod_prof number(4,0) references prof,
  cod_as number(5,0) references asignatura,
  constraint pk_profas primary key(cod_prof, cod_as)
);
```

2.9 Ejercicios

Tema 2: seguridad de bases de datos

¿cómo definirías un modelo de seguridad adecuado para los siguientes supuestos?

1. Existen tres tipos de usuarios: alumnos, profesores, administración. La base de datos es propiedad del usuario “universidad”

2. Cualquier usuario debe poder listar la siguiente información:
   a. Listado de alumnos por titulación (nombre del alumno, nombre de titulación)
   b. Listado de profesores por departamento (nombre de profesor, departamento)

3. Los único que pueden modificar las notas son los profesores.

4. Los alumnos pueden acceder a las notas, pero no modificarlas

5. Un administrador puede asignar acceder a las asignaturas a alumnos, pero no poner notas

6. A partir de las decisiones tomadas ¿qué restricciones crees que deberían incluirse en el perfil de cada usuario?

2.9 Ejercicios

7. La gestión de privilegios en Oracle:
    1. Almacena el instante en que se concedió un privilegio a un usuario
    2. Es posible que un mismo privilegio sea asignado a un mismo usuario por varios usuarios
    3. Si un usuario A revoca un privilegio P a otro usuario B, entonces necesariamente B pierde el privilegio P y a su vez todos aquellos a los que B concedió el privilegio P
    4. Un usuario puede tener una cantidad indeterminada de privilegios

8. En Oracle, los privilegios de tipo objeto:
    1. Son necesarios para crear una tabla
    2. Pueden ser revocados exclusivamente por el mismo usuario que lo transmitió
    3. No es posible eliminarlos en cascada
    4. Pueden ser asignados a un role

9. En Oracle, los privilegios de tipo sistema:
    1. Son necesarios para crear una tabla
    2. Pueden ser revocados exclusivamente por el mismo usuario que lo transmitió
    3. No es posible eliminarlos en cascada
    4. Pueden ser asignados a un role

10. Un usuario en Oracle puede:
    1. Tener asignados varios roles y perfiles
    2. Tener asignados varios roles y un único perfil
    3. Tener asignados un único role y un único perfil
    4. Tener asignados un único role y varios perfiles