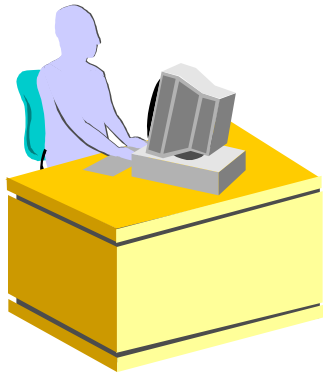
SQL

Seguridad

Noviembre 2012

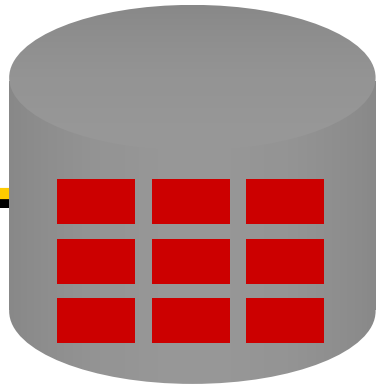
Acceso a usuarios

DBA



Usuario y password

privilegios



Usuarios

Privilegios

Privilegios del sistema: Acceso a la base de datos.

Privilegios Objetos: Acceso a la manipulación del contenido de los objetos de la base.

Privilegios Esquema: Acceso a la manipulación de objetos, como tablas, vistas y secuencias.

Privilegios del sistema

- Existen más de 80 privilegios.
- El DBA tiene el nivel más alto de privilegios
  - Crear nuevos usuarios
  - Borrar usuarios
  - Borrar tablas
  - Respaldar tablas

CREATE USER

```
CREATE USER     user
IDENTIFIED BY   password;
```

```
SQL> CREATE   USER   scott
  2   IDENTIFIED BY tiger;
User created.
```

Seguridad

Una vez que se crea un usuario, el DBA debe asignarle privilegios

```
GRANT privilege [, privilege...]
TO user [, user...];
```

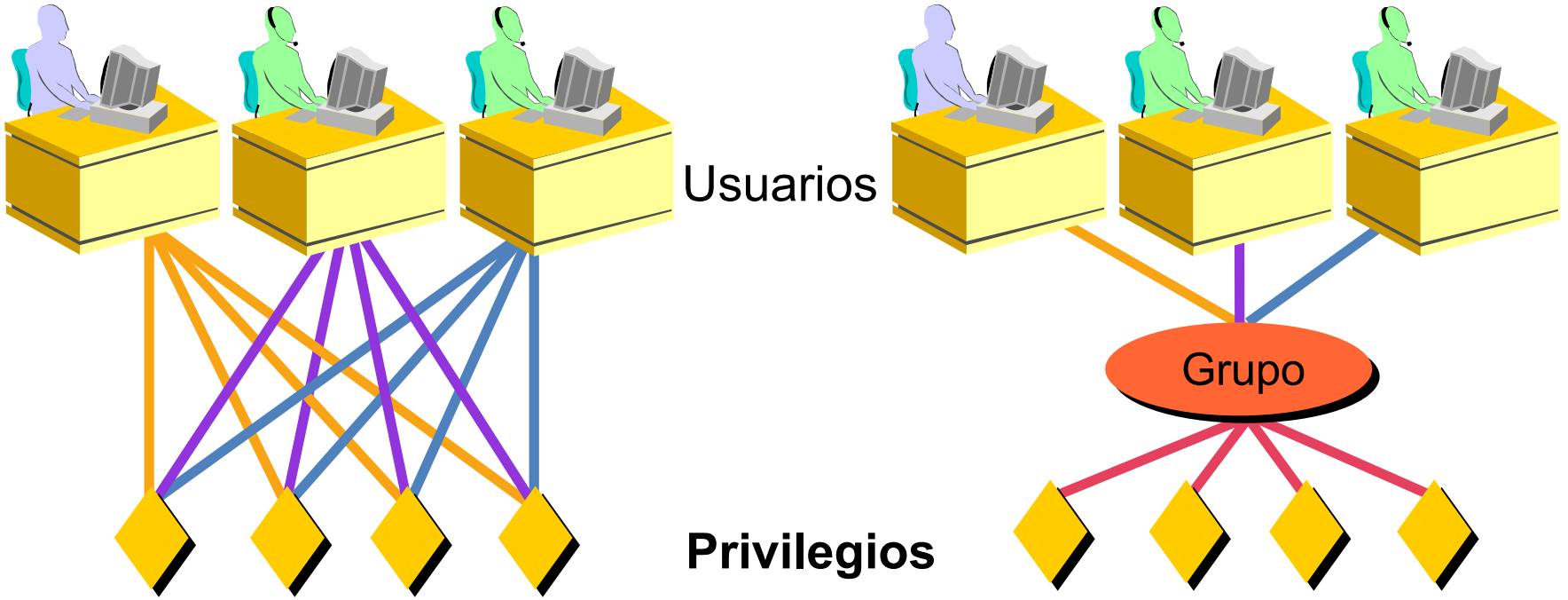
Un desarrollador de aplicaciones debe tener los privilegios siguientes

- CREATE SESSION
- CREATE TABLE
- CREATE SEQUENCE
- CREATE VIEW
- CREATE PROCEDURE

Seguridad

```
SQL> GRANT  create table, create sequence, create view
  2  TO      scott;
Grant succeeded.
```

Seguridad



La asignación directa de privilegios

La asignación de privilegios por grupo

Crear y otorgar privilegios por grupo

```
SQL> CREATE ROLE manager;
Role created.
```

```
SQL> GRANT create table, create view
  2         to manager;
Grant succeeded.
```

```
SQL> GRANT manager to BLAKE, CLARK;
Grant succeeded.
```

Cambio de password

- Cuando la cuenta de usuario se crea, la contraseña se inicializa.

- Los usuarios pueden cambiar su contraseña utilizando la sentencia ALTER USER.

```
SQL> ALTER USER scott
  2         IDENTIFIED BY lion;
User altered.
```

Privilegios - Elementos

Elemento Privilegio	Tabla	Vista	Secuencia	Procedure
ALTER	√		√	
DELETE	√	√		
EXECUTE				√
INDEX	√			
INSERT	√	√		
REFERENCES	√			
SELECT	√	√	√	
UPDATE	√	√		

Control de Usuarios

Los privilegios pueden cambiar de un elemento a otro.

Un propietario tiene todos los privilegios sobre el objeto.

Un propietario puede dar privilegios específicos de sus objetos para otros usuarios

```
GRANT        object_priv [(columns)]
ON           object
TO           {user|role|PUBLIC}
[WITH GRANT OPTION];
```

Privilegios para consultar una tabla

```
SQL> GRANT    select
  2  ON       emp
  3  TO       sue, rich;
Grant succeeded.
```

Privilegios para modificar determinadas columnas

```
SQL> GRANT    update (dname, loc)
  2  ON       dept
  3  TO       scott, manager;
Grant succeeded.
```

Autorizar al usuario para pasar por alto los privilegios.

```
SQL> GRANT    select, insert
  2  ON       dept
  3  TO       scott
  4  WITH GRANT OPTION;
Grant succeeded.
```

Permitir a todos los usuarios del sistema consultar datos de una tabla

```
SQL> GRANT    select
  2  ON       alice.dept
  3  TO       PUBLIC;
Grant succeeded.
```

Tablas del Sistema que almacenan los privilegios

Data Dictionary Table	Descripción
ROLE_SYS_PRIVS	Relacionados con las funciones del sistema
ROLE_TAB_PRIVS	Relacionados con las Tablas
USER_ROLE_PRIVS	Relacionados con el acceso
USER_TAB_PRIVS_MADE	Relacionados con tablas de usuarios
USER_TAB_PRIVS_RECD	Relacionados con tablas especificas
USER_COL_PRIVS_MADE	Relacionados con columnas
USER_COL_PRIVS_RECD	Relacionados con columnas especificas

REVOKE

- Utilice el comando REVOKE para quitar los privilegios otorgados a otros usuarios.

- Los privilegios concedidos a los demás a través de la opción WITH GRANT también será revocada.

```
REVOKE {privilege [, privilege...]|ALL}
ON     object
FROM   {user[, user...]|role|PUBLIC}
[CASCADE CONSTRAINTS];
```

Eliminar Privilegios

```
SQL> REVOKE   select, insert
  2  ON       dept
  3  FROM     scott;
Revoke succeeded.
```