MANEJO DE USUARIOS

Valeria Beratto Ulloa

Qué involucra la seguridad?

- Una aplicación de BD debe cumplir tres objetivos de seguridad:
  - *Secreto: La información no se debe dar a conocer a usuarios no autorizados*
  - *Integridad: Sólo se debe permitir modificar los datos a los usuarios autorizados*
  - *Disponibilidad: No se debe impedir el acceso a los usuarios autorizados*

Seguridad en BD

- El SGBD ofrece dos mecanismos de control de acceso:
  - *Control discrecional de acceso basado en privilegios*
  - *Control obligatorio de acceso*
- Estos controles se logran a través del *Manejo de Usuarios* de la Base de Datos.

Manejo de Usuarios

- Todo acceso a una base de datos requiere conectar mediante un *usuario y contraseña*.
- 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.

Cuentas por Defecto en ORACLE

- **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
- **SYSTEM:** Similar SYS, pero algunas operaciones no las puede realizar.
- **SYSMAN:** Usado para realizar tareas administrativas con la aplicación **Database Control** del **Enterprise Manager.**
- **DBSMNP:** Usuario que tiene permisos para monitorizar Enterprise Manager.

Crear Usuarios en ORACLE (1/4)

- **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 guion 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

Crear Usuarios en ORACLE (2/4)

- **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:

    ALTER 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

Crear Usuarios en ORACLE (3/4)

- Creación básica (Toma valores por defecto)

```
CREATE USER Nombre_usuario IDENTIFIED BY Contraseña
```

Para la contraseña, si no se usan comillas dobles, no puede tener espacios en blanco, ni caracteres nacionales como la eñe.

Crear Usuarios en ORACLE (4/4)

- Creación con definición de parámetros

```
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}]
```

Modificar /Borrar un Usuario

- **`ALTER USER Nombre_usuario  Modificación;`**
- **`DROP USER Nombre_usuario [CASCADE];`**

La opción **CASCADE** elimina los objetos del esquema del usuario antes de eliminar al propio usuario. Es obligatorio si el esquema contiene objetos

- Podemos consultar los usuarios existentes en la tabla DBA_USERS
- Podemos ver con qué usuario estoy conectado con SHOW USER

Privilegios

- Son permisos que se dan a los usuarios para que puedan realizar ciertas operaciones con la base de datos
- **GRANT:** concede a los usuarios privilegios a un objeto
- **REVOKE:** Quita un privilegio de un objeto de la BD a un usuario
- Para conocer los privilegios que tiene el usuario se debe consultar SESSION_PRIVS

```
GRANT privileges [ON object] TO users [WITH GRANT OPTION]
```

```
REVOKE privileges [ON object] FROM users
```

- [WITH GRANT OPTION]: el usuario puede transmitir a otro usuario los privilegios recibidos
- [ON object]: para asignar/quitar los privilegios a un determinado objeto.

Tipos de Privilegios o permisos

- **Sistemas:** Que permite al usuario hacer ciertas tareas sobre la BD, como por ejemplo crear un Tablespace. Pueden ser vistos consultando la vista: SYSTEM_PRIVILEGE_MAP
- **Objetos:** Este tipo de permiso le permite al usuario realizar ciertas acciones en objetos de la BD, como una tabla, vista, procedimiento, 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 dueño del objeto, el administrador o alguien que haya recibido este permiso explícitamente (con Grant Option).

Privilegios del sistema

- Más de 200 privilegios. Algunos de ellos son:

CLUSTERS:

CREATE CLUSTER	Crear un cluster (agrupamiento) en el esquema del usuario
CREATE ANY CLUSTER	Crear un agrupamiento en cualquier esquema
ALTER ANY CLUSTER	Alterar agrupamientos en cualquier esquema
DROP ANY CLUSTER	Eliminar agrupamientos en cualquier esquema

DATABASE:

ALTER DATABASE	Alterar la base de datos
ALTER SYSTEM	Usar la sentencia ALTER SYSTEM
AUDIT SYSTEM	Usar las sentencias de auditoria

DATABASE LINKS:

CREATE DATABASE LINK	Crear enlaces de bases de datos privados en el esquema del usuario
CREATE PUBLIC DATABASE LINK	Crear enlaces de bases de datos públicos
DROP PUBLIC DATABASE LINK	Eliminar enlaces de bases de datos públicos

DIMENSIONS:

CREATE DIMENSION	Crear dimensiones en el esquema del usuario
CREATE ANY DIMENSION	Crear dimensiones en cualquier esquema
ALTER ANY DIMENSION	Alterar dimensiones en cualquier esquema
DROP ANY DIMENSION	Eliminar dimensiones en cualquier esquema

Privilegios del sistema

INDEXES:

CREATE ANY INDEX	Crear un índice o un índice de dominio de aplicación (índice sobre datos complejos como documentos, imágenes satelitales, clips de video entre otros) en una tabla de cualquier esquema
ALTER ANY INDEX	Alterar un índice en cualquier esquema
DROP ANY INDEX	Eliminar un índice en cualquier esquema
QUERY REWRITE	Crear índices basados en funciones y habilitar la re-escritura en una vista materializada (snapshot) en el esquema del usuario
GLOBAL QUERY REWRITE	Crear índices basados en funciones y habilitar la re-escritura en una vista materializada (snapshot) en cualquier esquema

PROCEDURES:

CREATE PROCEDURE	Crear procedimientos almacenados, funciones y paquetes en el esquema del usuario
CREATE ANY PROCEDURE	Crear procedimientos almacenados, funciones y paquetes en cualquier esquema
ALTER ANY PROCEDURE	Alterar procedimientos almacenados, funciones y paquetes en cualquier esquema
DROP ANY PROCEDURE	Eliminar procedimientos almacenados, funciones y paquetes en cualquier esquema
EXECUTE ANY PROCEDURE	Ejecutar procedimientos o funciones (independientes o empaquetados) y referenciar variables publicas de paquetes en cualquier esquema

PROFILES:

CREATE PROFILE	Crear perfiles de usuario
ALTER PROFILE	Alterar perfiles de usuario
DROP PROFILE	Eliminar perfiles de usuario

Privilegios del sistema

ROLES:

CREATE ROLE	Crear roles en la base de datos
ALTER ANY ROLE	Alterar cualquier rol en la base de datos
DROP ANY ROLE	Eliminar roles
GRANT ANY ROLE	Conceder cualquier rol a un usuario de la base de datos

ROLLBACK SEGMENTS:

CREATE ROLLBACK SEGMENT	Crear segmentos de restauración
ALTER ROLLBACK SEGMENT	Alterar segmentos de restauración
DROP ROLLBACK SEGMENT	Eliminar segmentos de restauración

SEQUENCES:

CREATE SEQUENCE	Crear secuencias en el esquema del usuario
CREATE ANY SEQUENCE	Crear secuencias en cualquier esquema
ALTER ANY SEQUENCE	Alterar secuencias en cualquier esquema
DROP ANY SEQUENCE	Eliminar secuencias en cualquier esquema
SELECT ANY SEQUENCE	Referenciar (consultar) secuencias en cualquier esquema

SESSIONS:

CREATE SESSION	Conectarse a la base de datos
ALTER RESOURCE COST	Fijar los costos de los recursos para una sesión
ALTER SESSION	Usar la sentencia ALTER SESSION
RESTRICTED SESSION	Entrar al sistema (Logon) después de que la instancia ha sido arrancada usando la sentencia STARTUP RESTRICT

Privilegios del sistema

SYNONYMS:

CREATE SYNONYM	Crear sinónimos en el esquema del usuario
CREATE ANY SYNONYM	Crear sinónimos privados en cualquier esquema
CREATE PUBLIC SYNONYM	Crear sinónimos públicos
DROP ANY SYNONYM	Eliminar sinónimos privados en cualquier esquema
DROP PUBLIC SYNONYM	Eliminar sinónimos públicos

TABLES:

CREATE TABLE	Crear tablas en el esquema del usuario
CREATE ANY TABLE	Crear tablas en cualquier esquema. El dueño del esquema que contiene la tabla debe tener una cuota de espacio sobre el espacio de tablas (tablespace) que se almacena la tabla
ALTER ANY TABLE	Alterar cualquier tabla o vista en cualquier esquema
BACKUP ANY TABLE	Usar la utilidad EXPORT para exportar objetos de cualquier esquema
DELETE ANY TABLE	Eliminar filas de tablas, particiones de tablas o vistas de cualquier esquema
DROP ANY TABLE	Eliminar o truncar tablas o particiones de tablas de cualquier esquema
INSERT ANY TABLE	Insertar filas en tablas o vistas de cualquier esquema
LOCK ANY TABLE	Bloquear tablas y vistas en cualquier esquema
SELECT ANY TABLE	Consultar tablas, vistas o vistas materializadas en cualquier esquema
FLASHBACK ANY TABLE	Usar una consulta SQL histórica o de retroceso (flashback query) en una tabla, vista o vista materializada en cualquier esquema. Este privilegio no se necesita para ejecutar el procedimiento DBMS_FLASHBACK) SELECT * FROM Departamentos AS OF TIMESTAMP(SYSTIMESTAMP - INTERVAL '1' DAY)
UPDATE ANY TABLE	Modificar filas en tablas y vistas de cualquier esquema

Privilegios del sistema

TABLESPACES:

CREATE TABLESPACE	Crear espacios de tablas
ALTER TABLESPACE	Alterar espacios de tablas
DROP TABLESPACE	Eliminar espacios de tablas
MANAGE TABLESPACE	Manejar el estado de un espacio de tablas, en línea, fuera de línea, iniciando copia de seguridad y finalizando copia de seguridad
UNLIMITED TABLESPACE	Usar una cantidad ilimitada de espacio en cualquier espacio de tablas. Este privilegio es superior a cualquier cuota establecida en un espacio de tablas. Si a un usuario se le revoca este permiso, los objetos y datos existentes permanecen en el sistema, pero no se le asignará más espacio hasta que se le asigne una cuota especifica en el espacio de tablas. Este privilegio de sistema NO se puede asignar a un rol.

TRIGGERS:

CREATE TRIGGER	Crear disparadores de base de datos en el esquema del usuario
CREATE ANY TRIGGER	Crear disparadores de base de datos en cualquier esquema
ALTER ANY TRIGGER	Habilitar, deshabilitar o compilar disparadores de base de datos en cualquier esquema
DROP ANY TRIGGER	Eliminar disparadores de base de datos cualquier esquema
ADMINISTER DATABASE TRIGGER	Crear disparadores para la base de datos (por ejemplo asociados a eventos de la base de datos como arrancar, detener; o a eventos de los usuarios como conectarse y desconectarse). Se debe tener el privilegio de CREATE TRIGGER o de CREATE ANY TRIGGER

Privilegios del sistema

USERS:

CREATE USER	Crear usuarios. Además permite asignar a un usuario su cuota en cualquier espacio de tablas, el espacio de tablas por defecto y el temporal y el perfil al momento en que se ejecuta la sentencia CREATE USER
ALTER USER	Alterar usuarios. Permite cambiar la clave del usuario y su método de identificación, asignar cuotas en cualquier espacio de tablas, el espacio de tablas por defecto y el temporal, el perfil y los roles por defecto
BECOME USER	Convertirse en otro usuario. Este privilegio se requiere para ejecutar una importación total de la base de datos
DROP USER	Eliminar usuarios de la base de datos

VIEWS:

CREATE VIEW	Crear vistas en el esquema del usuario
CREATE ANY VIEW	Crear vistas en cualquier esquema
DROP ANY VIEW	Eliminar vistas en cualquier esquema

Privilegios del sistema

OTROS:

COMMENT ANY TABLE	Comentar tablas, vistas o columnas de cualquier esquema
SELECT ANY DICTIONARY	Consultar cualquier objeto del diccionario de datos en el esquema SYS. Este privilegio permite que el administrador selectivamente sobre escriba el parámetro de inicialización O7_DICTIONARY_ACCESSIBILITY que por defecto esta en FALSE y no deja a ningún usuario consultar el diccionario de datos.
SYSDBA	Ejecutar las operaciones de STARTUP y SHUTDOWN Usar la sentencia ALTER DATABASE para abrir, montar, hacer copias o cambiar el conjunto de caracteres por defecto Usar la sentencia CREATE DATABASE Usar la sentencia ARCHIVELOG y RECOVERY Usar la sentencia CREATE SPFILE Incluye el privilegio de RESTRICTED SESSION
SYSOPER	Ejecutar las operaciones de STARTUP y SHUTDOWN Usar la sentencia ALTER DATABASE OPEN | MOUNT | BACKUP Usar la sentencia ARCHIVELOG y RECOVERY Usar la sentencia CREATE SPFILE Incluye el privilegio de RESTRICTED SESSION
CONNECT, RESOURCE, and DBA	Estos roles se conservan por compatibilidad con versiones anteriores de Oracle. Consultando la vista del diccionario de datos DBA_SYS_PRIVS puede ver los privilegios que tienen cada uno de ellos Nota: Oracle recomienda que no siga usando estos roles en el modelo de seguridad de su empresa, ya que no se espera que en futuras versiones se creen automáticamente

Privilegios a objetos

- Los permisos sobre objetos más importantes son: SELECT, UPDATE, INSERT, DELETE, ALTER, DEBUG, EXECUTE, INDEX, REFERENCES

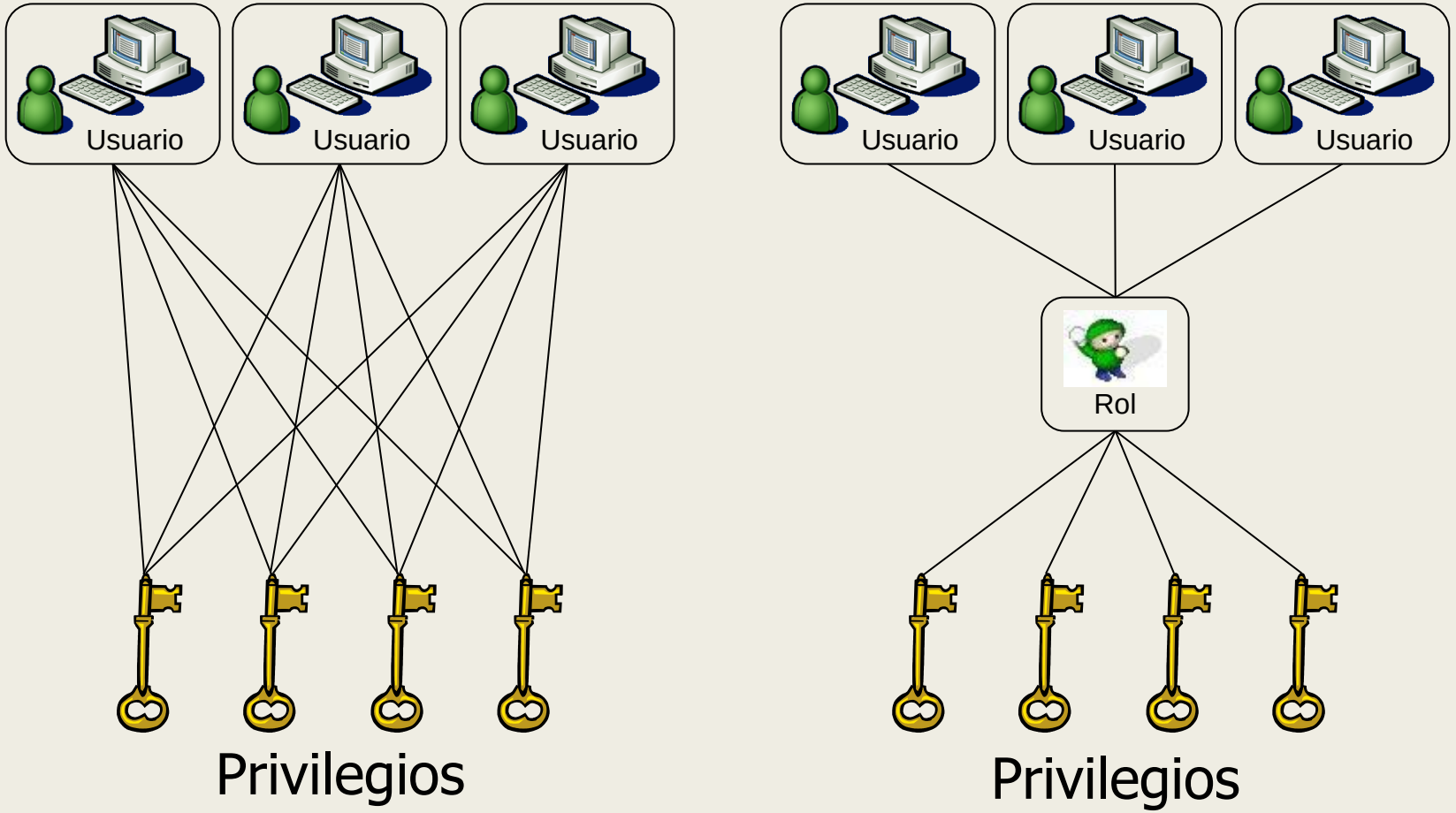
No olvidar

- Debemos asignar el privilegio CREATE SESSION

```
GRANT CREATE SESSION TO  Nombre_usuario
```

- Ahora podrá iniciar, pero no tiene privilegios para accionar la BD.
- Se recomienda asignar sólo los privilegios necesarios

Roles


Usuario
Usuario
Usuario
Privilegios
Usuario
Usuario
Usuario
Rol
Privilegios

Roles

- Un rol es un grupo de privilegios que reciben un nombre, este rol puede ser otorgado posteriormente a un usuario.
- Usar roles hace más fácil el manejo de los privilegios
- Un usuario puede tener asignados varios roles y varios usuarios pueden tener el mismo rol
- Los roles normalmente se crean debido a necesidades de las aplicaciones
- El DBA o un usuario con privilegios de crear roles, crea el rol y luego a ese rol se le asignan los privilegios

```
CREATE ROLE Nombre_rol
```

```
GRANT Privilegio TO Nombre_rol
```

Roles

- Asignar un rol

```
GRANT Nombre_rol TO  Nombre_usuario
```

- La vista USER_ROLE_PRIVS muestra los roles que se le han asignado a un usuario (el que esta actualmente conectado)

Ejercicios

- Cree un usuario1 que pueda administrar la base de datos
- Cree un usuario2 que pueda crear procedimientos almacenados
- Cree dos roles uno de diseñador (manipular tablas) y otro de consultor (sólo consultar).
- Al usuario2 quite el privilegio de crea procedimientos.
- Asigne al usuario2 el rol del consultor