

SESION III – MODULO III

Especialización Oracle



Ing. Cesar Hajar
Instructor

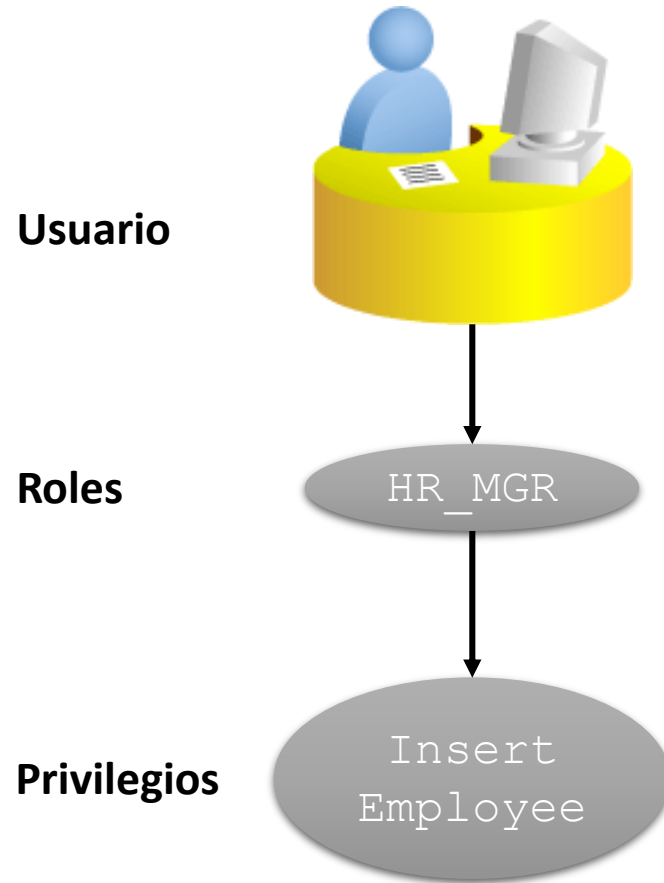
SESION 3

1. Creación de usuario-esquema.
2. Gestión de roles y perfiles.
3. Privilegios de objeto y de sistema
4. Asignación y revocación de privilegios de objeto y de sistema.
5. Visualización de privilegios a través de vistas dinámicas.
6. Taller práctico.



Usuario-esquema

Administración de usuarios: Vista general



- Crear un usuario asignado a un área de almacenamiento
- Asignar una cuota para limitar el uso de almacenamiento
- Limitar el uso de recursos con perfiles
- Autenticar usuarios con un password
- Administrar reglas de password rules con perfiles (expirar password y bloquear cuenta)
- Asignar privilegios a roles y roles a usuarios

Esquemas

- Un esquema es una colección de datos pertenecientes a un usuario
- Username y schema son a menudo usados intercambiabilmente
- Un usuario puede ser asociado con un solo esquema, pero él o ella pueden usar objetos desde varios esquemas con permisos apropiados

Schema Objects:

- Tables
- Triggers
- Indexes
- Views
- Sequences
- Stored program units
- Synonyms
- User-defined data types
- Database links

Características de los usuarios

- Cada cuenta de usuario de base de datos tiene:
 - Un nombre de usuario único
 - Un método de autenticación
 - Un espacio de tablespace
 - Un espacio de tabla temporal
 - Un perfil de usuario
 - Un grupo consumidor
 - Un estado de bloqueo

Cuentas predefinidas: SYS y SYSTEM

- La cuenta SYS:
 - Tiene otorgado el rol DBA
 - Tiene todos los privilegios con ADMIN OPTION
 - Es requerido para arrancar, apagar y ejecutar comandos de mantenimiento.
 - Dueño del diccionario de datos
- La cuenta SYSTEM:
 - Tiene otorgado el rol DBA
 - No tiene acceso a las tablas X\$ (estructura interna de Oracle)
 - No puede realizar tareas de backup y recovery o upgrade
- Estas cuentas no deben ser utilizadas para operaciones de rutina.

Autenticando usuarios

- Password
- External
- Global (Oracle Internet Directory)

Edit User: HR

Actions: [Create Like](#) [Go](#) [Show SQL](#) [Revert](#) [Apply](#)

General [Roles](#) [System Privileges](#) [Object Privileges](#) [Quotas](#) [Consumer Group Privileges](#) [Proxy Users](#)

Name **HR**

Profile **DEFAULT**

Authentication **Password**

* Enter Password

* Confirm Password


For Password choice, the role is authorized via password.

☐ Expire Password now

Default Tablespace **USERS**

Temporary Tablespace **TEMP**

Status ☐ Locked ☒ Unlocked



Creando usuarios

- El DBA crea usuarios con la sentencia **CREATE USER**

```
SQL> CREATE USER user  
      2 IDENTIFIED BY password;
```

```
SQL> CREATE USER bob  
      2 IDENTIFIED BY oracle;  
User created.
```

```
SQL> CREATE USER hans  
      2 IDENTIFIED BY oracle  
      3 PASSWORD EXPIRE;  
User created.
```

Autenticación del Administrador

- Seguridad del sistema operativo:
 - Los DBAs deben tener privilegios del sistema operativo para crear y eliminar archivos.
 - Los usuarios comunes de base de datos no deberían tener privilegios de sistema operativo para crear o eliminar archivos de base de datos
- Seguridad del Administrador:
 - El usuario DBA por su nombre es auditado por el archivo de contraseñas y métodos de autenticación fuerte
 - El nombre de cuenta de SO es auditado por la autenticación de SO
 - La autenticación de sistema operativo tiene prioridad sobre la autenticación por archivo de contraseña para los usuarios con privilegios
 - El archivo de contraseñas reconoce mayúsculas y minúsculas

Desbloqueando cuentas de usuario y reseteando contraseñas

- El DBA puede desbloquear cuentas de usuarios con la sentencia **ALTER USER**

```
SQL> ALTER USER rob  
      2      ACCOUNT UNLOCK;  
User created.
```

Cambio de contraseña

- El DBA crea la cuenta de usuario e inicializa su contraseña.
- Usted puede cambiar su contraseña utilizando la sentencia ALTER USER.

```
SQL> ALTER USER bob  
      2 IDENTIFIED BY olink;  
User altered.
```

Eliminar un usuario

- El DBA puede eliminar cuentas de usuario

```
SQL> DROP USER username CASCADE;
```

```
SQL> DROP USER bob;  
User dropped.
```

*Specify **CASCADE** to drop all objects in the user's schema before dropping the user.
You must specify this clause to drop a user whose schema contains any objects.*

Bloqueo y desbloqueo de cuentas

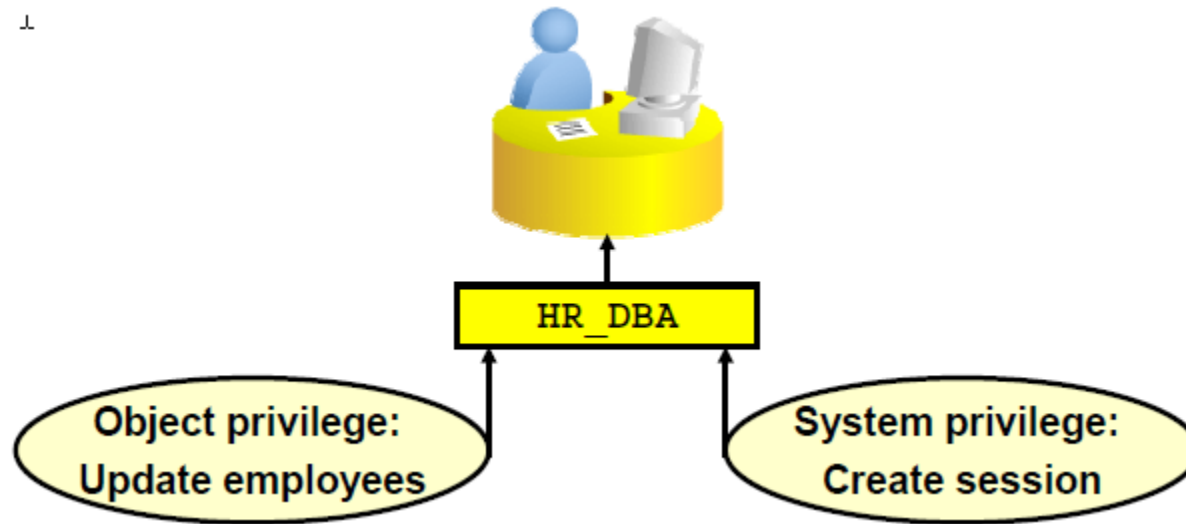
```
SQL> ALTER USER username ACCOUNT UNLOCK;
```

```
SQL> ALTER USER username ACCOUNT LOCK;
```

Privilegios de objeto y de sistema

Privilegios

- Existen dos tipos de privilegios:
 - De sistema: habilita a los usuarios a ejecutar acciones particulares en la base de datos
 - De objeto: habilita a los usuarios a acceder y manipular un objeto específico



Privilegios de sistema

- Están disponibles más de 100 privilegios.
- El administrador de base de datos tiene privilegios de sistema de alto nivel para tareas tales como:
 - Creación de nuevos usuarios
 - Eliminación de usuarios
 - Eliminación de tablas
 - Copia de seguridad de las tablas

Otorgando privilegios de sistema

- Utilizar el comando **GRANT** para otorgar privilegios de sistema.
- El beneficiario puede conceder privilegios del sistema con la opción **ADMIN**.

```
GRANT {system_privilege|role}  
      TO {user|role|PUBLIC}  
      [WITH ADMIN OPTION]
```

```
GRANT CREATE SESSION TO emi;
```

```
GRANT CREATE SESSION TO emi WITH ADMIN OPTION;
```

Privilegios de objeto

- Los privilegios de objetos varían de un objeto a otro.
- Un propietario tiene todos los privilegios sobre el objeto.
- Un propietario puede dar privilegios específicos sobre el objeto del que es propietario.

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

Privilegios de objeto

| Privilegio de objeto | Tabla | Vista | Secuencia | Procedimiento |
|----------------------|-------|-------|-----------|---------------|
| ALTER | ✓ | | ✓ | |
| DELETE | ✓ | ✓ | | |
| EXECUTE | | | | ✓ |
| INDEX | ✓ | | | |
| INSERT | ✓ | ✓ | | |
| REFERENCES | ✓ | | | |
| SELECT | ✓ | ✓ | ✓ | |
| UPDATE | ✓ | ✓ | | |

Asignación y revocación de privilegios de objeto y de sistema

Otorgando privilegios de objeto

- Conceder privilegios de consulta en la tabla empleados.

```
GRANT  select
ON      employees
TO      sue, rich;
Grant succeeded.
```

- Conceder privilegios para actualizar columnas específicas para usuarios y roles.

```
GRANT  update (department_name, location_id)
ON      departments
TO      scott, manager;
Grant succeeded.
```

Dando permisos para asignar sus privilegios

- Dar al usuario autoridad para pasar los privilegios.

```
GRANT  select, insert
ON     departments
TO     scott
WITH   GRANT OPTION;
Grant succeeded.
```

- Permitir que todos los usuarios del sistema consultar los datos de la tabla DEPARTAMENTOS de Alice.

```
GRANT  select
ON     alice.departments
TO     PUBLIC;
Grant succeeded.
```

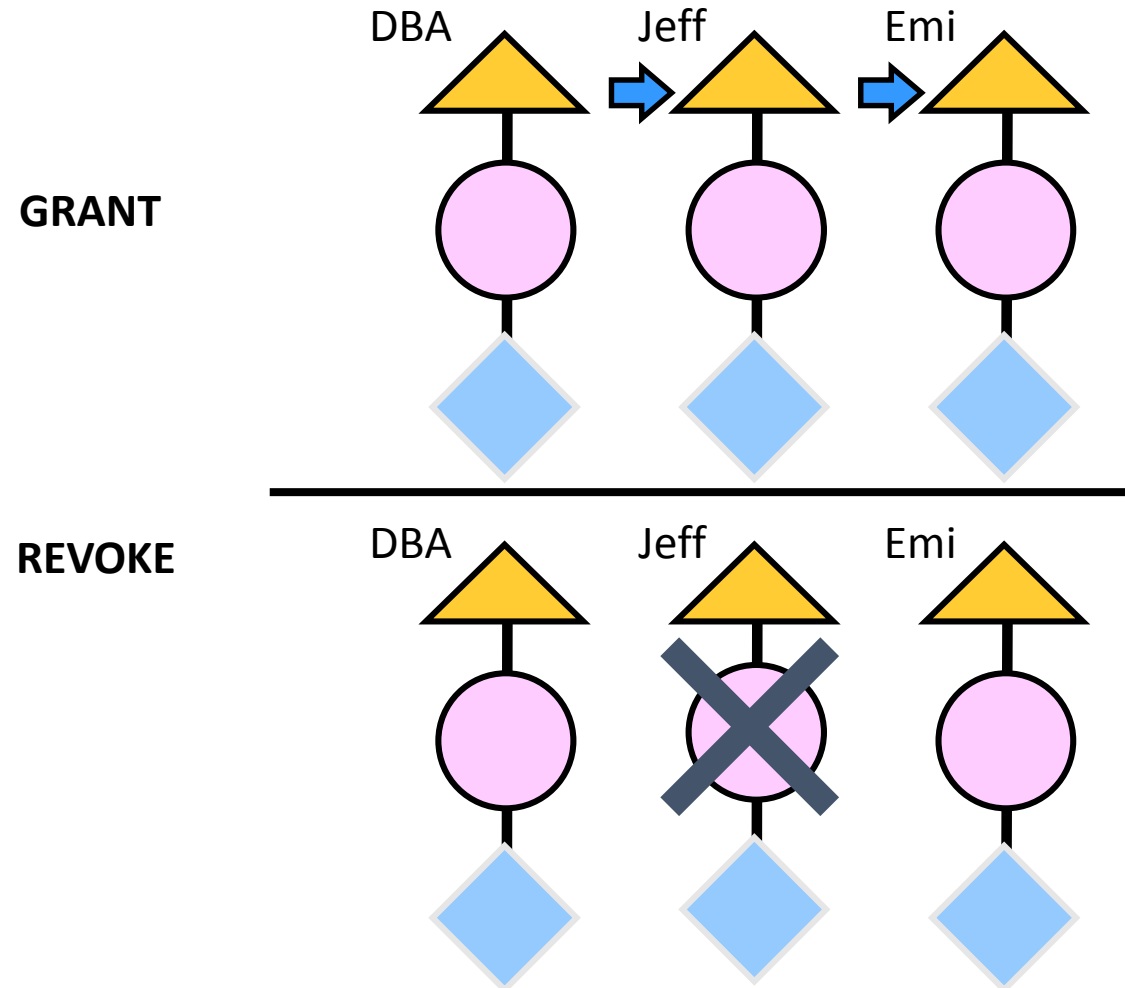
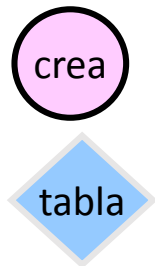
Revocando privilegios de objeto

- Se utiliza la sentencia REVOKE para revocar privilegios concedidos a otros usuarios.
- Privilegios concedidos a los demás a través de la cláusula WITH GRANT OPTION también se revocan.

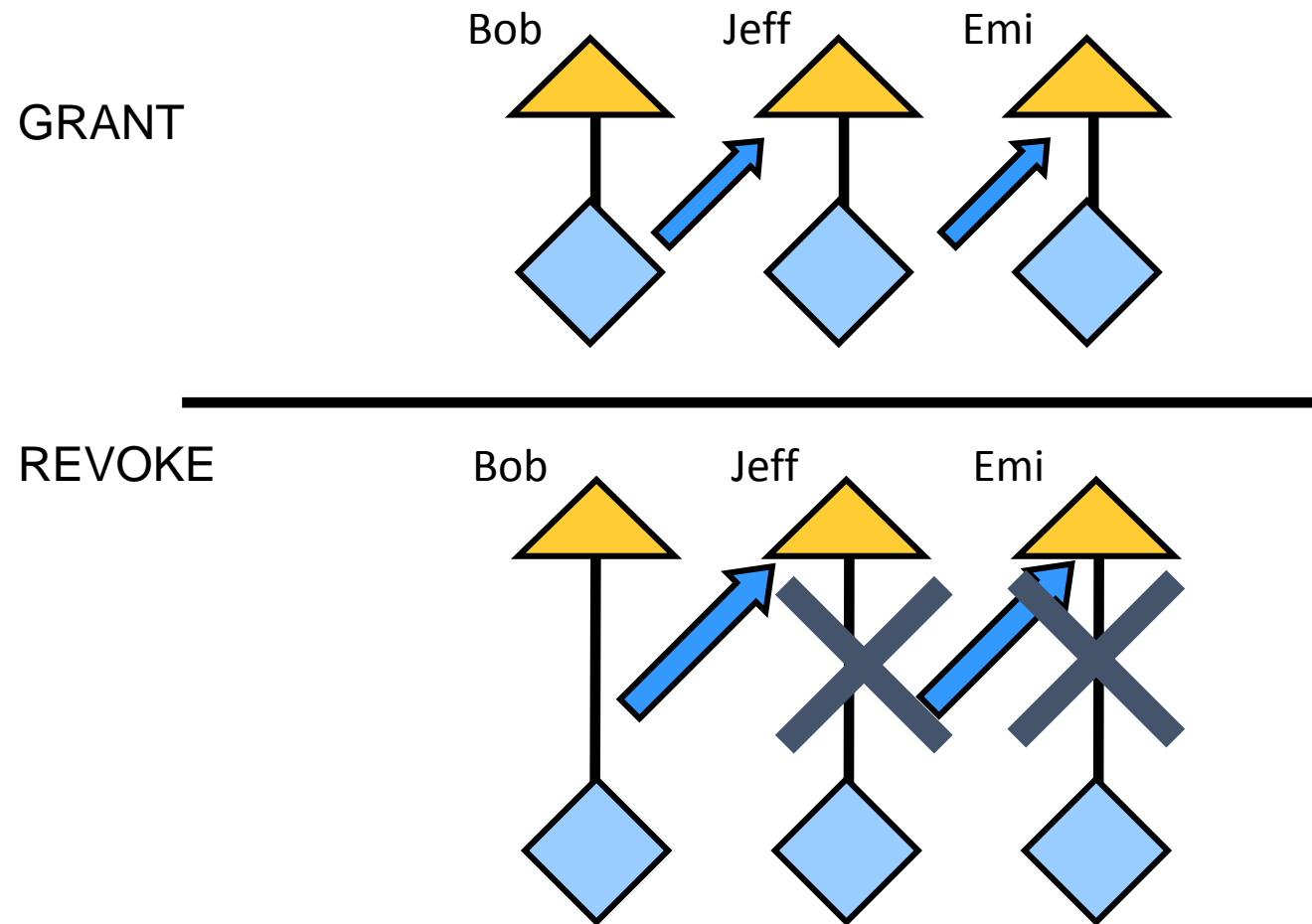
```
REVOKE {privilege [, privilege...] | ALL}
ON      object
FROM    {user[, user...] | role | PUBLIC}
[CASCADE CONSTRAINTS];
```


Revocando privilegios de sistema

There are no cascading effects when a system privilege is revoked, regardless of whether it was given the ADMIN OPTION.



Revocando privilegios de objeto



Cascading effects can be observed when revoking a object privilege that is related to a DML operation.

Revocando privilegios de objeto

- Como usuario de Alice, revocar los privilegios de SELECT e INSERT dadas a usuario Scott en la tabla DEPARTAMENTOS.

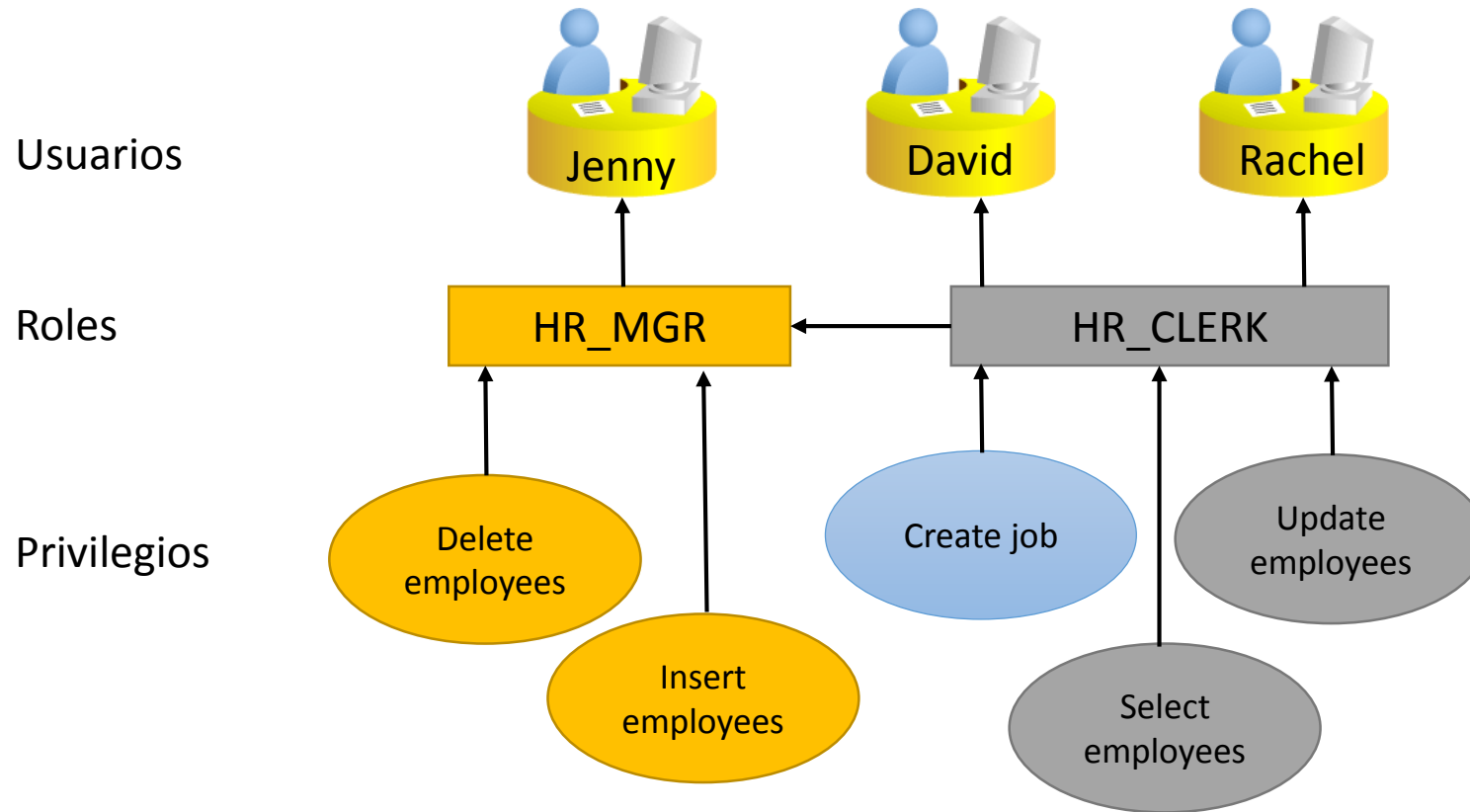
```
REVOKE  select, insert
ON      departments
FROM    scott;
Revoke succeeded.
```

Roles y perfiles

Beneficio de los Roles

- Facilita la administración de privilegios
- Administración dinámica de privilegios
- Disponibilidad selectiva de privilegios

Asignando privilegios a roles y asignando roles a usuarios



Roles predefinidos

| Rol | Privilegios incluidos |
|---------------------|---|
| CONNECT | CREATE SESSION |
| RESOURCE | CREATE CLUSTER, CREATE INDEXTYPE, CREATE OPERATOR, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER, CREATE TYPE |
| SCHEDULER_ADMIN | CREATE ANY JOB, CREATE EXTERNAL JOB, CREATE JOB, EXECUTE ANY CLASS, EXECUTE ANY PROGRAM, MANAGE SCHEDULER |
| DBA | La mayoría de los privilegios del sistema; varias otras funciones. No lo otorgue para no administradores |
| SELECT_CATALOG_ROLE | No hay privilegios del sistema; HS_ADMIN_ROLE y más de 1.700 privilegios de objeto en el diccionario de datos |

Creando y asignando privilegios a roles

- Crear un rol

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

- Conceder privilegios a un rol

```
GRANT create table, create view  
TO manager;  
Grant succeeded.
```

- Asignar un rol a un usuario

```
GRANT manager TO DE HAAN, KOCHHAR;  
Grant succeeded.
```

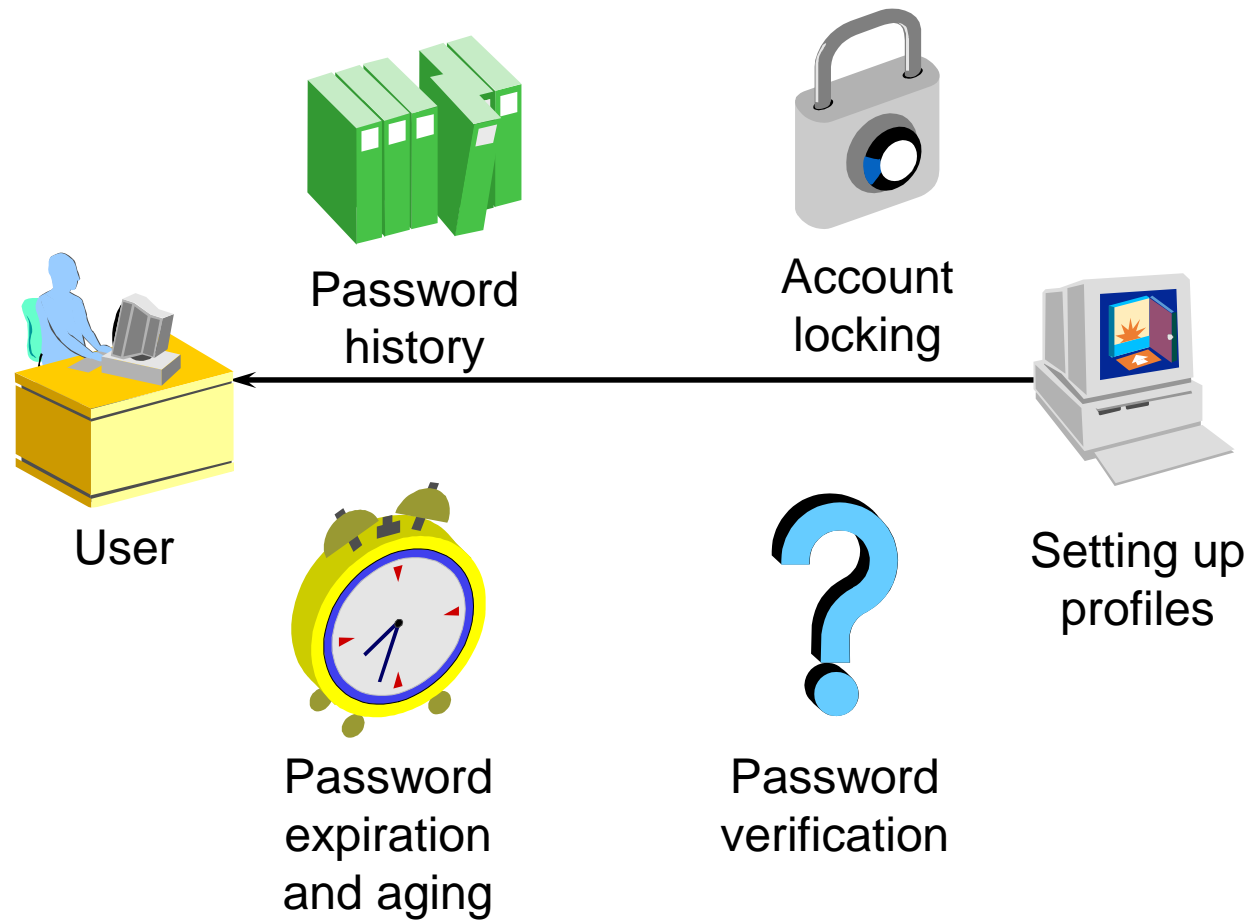

Confirmar los privilegios otorgados

| Vista del diccionario de datos | Descripción |
|--------------------------------|--|
| ROLE_SYS_PRIVS | Privilegios del sistema concedidos a los roles |
| ROLE_TAB_PRIVS | Privilegios sobre tablas concedidos a los roles |
| USER_ROLE_PRIVS | Roles accesibles por el usuario |
| USER_TAB_PRIVS_MADE | Privilegios concedidos a objetos en objetos del usuario |
| USER_TAB_PRIVS_RECD | Privilegios de objeto concedidos al usuario |
| USER_COL_PRIVS_MADE | Privilegios de objeto otorgadas en las columnas de los objetos del usuario |
| USER_COL_PRIVS_RECD | Privilegios de objeto concedidos al usuario en columnas específicas |
| USER_SYS_PRIVS | Privilegios del sistema concedidos al usuario |

Perfiles

- Un perfil es un conjunto de directivas que limita el uso de contraseñas y recursos.
- Los perfiles se asignan a los usuarios con el comando `CREATE USER` o `ALTER USER`.
- Los perfiles se pueden activar o desactivar.
- Los perfiles se pueden relacionar con el perfil `DEFAULT`.
- Los perfiles solo pueden ser asignados a usuario y no a roles u otros objetos.

Administración de contraseñas



Límites de contraseña

| | |
|--------------------------|--|
| FAILED_LOGIN_ATTEMPTS | Especifica el número de intentos fallidos para iniciar sesión en la cuenta de usuario antes de que la cuenta se bloquee. |
| PASSWORD_LIFE_TIME | Especifica el número de días que se puede usar la misma contraseña para la autenticación. Si también establece un valor para PASSWORD_GRACE_TIME, la contraseña caduca si no se modifica dentro del período de gracia y se rechazan las conexiones adicionales. Si no establece un valor para PASSWORD_GRACE_TIME, su valor predeterminado UNLIMITED hará que la base de datos emita una advertencia, pero permitirá que el usuario continúe conectándose indefinidamente. |
| PASSWORD_LOCK_TIME | Especifica el número de días que se bloqueará una cuenta después del número especificado de intentos de inicio de sesión fallidos consecutivos. |
| PASSWORD_GRACE_TIME | Especifica el número de días después de que comience el período de gracia durante el cual se emite una advertencia y se permite el inicio de sesión. Si la contraseña no se cambia durante el período de gracia, la contraseña caducará. |
| PASSWORD_VERIFY_FUNCTION | Permite que una secuencia de comandos de verificación de complejidad de contraseña PL / SQL se pase como un argumento a la declaración CREATE PROFILE |
| PASSWORD_REUSE_TIME | Especifica el número de días antes de que una contraseña no se pueda reutilizar. |
| PASSWORD_REUSE_MAX | Especifica el número de cambios de contraseña requeridos antes de que la contraseña actual pueda ser reutilizada. Para que estos parámetros tengan algún efecto, debe especificar un número entero para ambos. |

Creando un perfil: ajustes de contraseña

```
CREATE PROFILE grace_5 LIMIT  
  FAILED_LOGIN_ATTEMPTS 3  
  PASSWORD_LOCK_TIME UNLIMITED  
  PASSWORD_LIFE_TIME 30  
  PASSWORD_REUSE_TIME 30  
  PASSWORD_VERIFY_FUNCTION verify_function  
  PASSWORD_GRACE_TIME 5;
```

Administración de recursos

- Los límites de gestión de recursos se pueden hacer cumplir en el nivel de sesión, el nivel de llamada, o ambos.
- Los límites pueden ser definidos por los perfiles utilizando el comando **CREATE PROFILE**.
- Habilitar límites de recursos con:
 - Parámetro de inicialización **RESOURCE_LIMIT**
 - Comando **ALTER SYSTEM**

Habilitando los límites de recursos

- Establecer el parámetro de inicialización **RESOURCE_LIMIT** a **TRUE**.
- Hacer cumplir los límites de recursos habilitando el parámetro con el comando **ALTER SYSTEM**.

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

Limites de recursos

| | |
|---------------------------|---|
| SESSIONS_PER_USER | Especifica el número de sesiones simultáneas a las que desea limitar al usuario. |
| CPU_PER_SESSION | Especifica el límite de tiempo de CPU para una sesión, expresado en centésimas de segundos. |
| CPU_PER_CALL | Especifica el límite de tiempo de la CPU para una llamada (un análisis, ejecución o recuperación), expresado en centésimas de segundo. |
| CONNECT_TIME | Especifica el límite de tiempo transcurrido total para una sesión, expresado en minutos. |
| IDLE_TIME | Especifica los períodos permitidos de tiempo inactivo continuo durante una sesión, expresados en minutos. Las consultas de larga ejecución y otras operaciones no están sujetas a este límite. |
| LOGICAL_READS_PER_SESSION | Especifica el número permitido de bloques de datos leídos en una sesión, incluidos los bloques leídos de la memoria y el disco. |
| LOGICAL_READS_PER_CALL | Especifica el número permitido de bloques de datos leídos para que una llamada procese una declaración SQL (un análisis, ejecución o recuperación). |
| PRIVATE_SGA | Especifica la cantidad de espacio privado que una sesión puede asignar en el grupo compartido del área global del sistema (SGA). Consulte size_clause para obtener información sobre esa cláusula. |
| COMPOSITE_LIMIT | Especifica el costo total de recursos para una sesión, expresado en unidades de servicio. Oracle Database calcula las unidades de servicio totales como una suma ponderada de CPU_PER_SESSION, CONNECT_TIME, LOGICAL_READS_PER_SESSION y PRIVATE_SGA. |

Creando un perfil: límite de recursos

```
CREATE PROFILE developer_prof LIMIT  
  SESSIONS_PER_USER 2  
  CPU_PER_SESSION 10000  
  IDLE_TIME 60  
  CONNECT_TIME 480;
```

Ejercicio

- En este ejercicio usted creará el usuario INVENTORY que será dueño de la nueva aplicación Inventory. Debe crear un perfil que limite el tiempo de inactividad de los usuarios. Si un usuario está sin actividad u olvida desconectarse de la base de datos pasados los 3 minutos, la sesión debe terminar.

Visualización de privilegios a través de vistas

Consultando privilegios y otros objetos

- Db_users
- Db_profiles
- Db_roles
- Db_tab_privileges
- Db_sys_privs
- Db_roles_privs

Información adicional

- How to Grant and Revoke privileges in Oracle :
- http://www.oracle-dba-online.com/sql/grant_and_revoke_privileges.htm
- Administracion de Usuarios Oracle :
- <http://www.orasite.com/tutoriales/administracion-de-usuarios-oracle.html>
- Oracle System Privileges :
- http://psoug.org/reference/system_privs.html
- Oracle Object Privileges :
- http://psoug.org/reference/object_privs.html
- Oracle Roles :
- <http://psoug.org/reference/roles.html>
- Oracle Users :
- <http://psoug.org/reference/user.html>