

Gestión de roles

Roles predefinidos

1. Sobre la base de datos Oracle conéctate como usuario **system**.
2. Consulta los roles predefinidos en Oracle.

SELECT * FROM DBA_ROLE_PRIVS;

	GRANTEE	GRANTED_ROLE	ADMIN_OPTION	DELEGATE_OPTION	DEFAULT_ROLE	COMMON	INHERITED
1	C##E12V2	RESOURCE	NO	NO	YES	NO	NO
2	SERG10	CONNECT	NO	NO	YES	NO	NO
3	C##E12V2	CONNECT	NO	NO	YES	NO	NO
4	SERG10	RESOURCE	NO	NO	YES	NO	NO
5	GSUSER_ROLE	CONNECT	NO	NO	YES	YES	NO
6	INSTITUTO12	CONNECT	NO	NO	YES	YES	NO
7	E12V2	RESOURCE	NO	NO	YES	YES	NO
8	EMPRESA12	RESOURCE	NO	NO	YES	YES	NO
9	EMPRESA12-2	RESOURCE	NO	NO	YES	YES	NO
10	PEDIDOS12	RESOURCE	NO	NO	YES	YES	NO
11	SYSTEM	DBA	NO	NO	YES	YES	NO
12	SYS	AUDIT_VIEWER	YES	NO	YES	YES	NO

Hay muchos más resultado, pero solo he capturado la imagen hasta aquí

3. Consulta los privilegios de sistema concedidos a los roles **CONNECT** y **RESOURCE**.

IMPORTANTE: Cuando se asigna el rol **RESOURCE** a un usuario Oracle internamente también le asigna al usuario el privilegio **UNLIMITED TABLESPACE** (lo hace con un trigger, no a través del rol ya que este privilegio no se puede asignar a un rol).

Recuerda que a los usuarios les asignamos en prácticas anteriores el rol **RESOURCE**. Consulta sus privilegios de sistema.

SELECT * FROM DBA_SYS_PRIVS WHERE GRANTEE = 'CONNECT' OR GRANTEE = 'RESOURCE';

	GRANTEE	PRIVILEGE	ADMIN_OPTION	COMMON	INHERITED
1	RESOURCE	CREATE SEQUENCE	NO	YES	NO
2	RESOURCE	CREATE PROCEDURE	NO	YES	NO
3	CONNECT	SET CONTAINER	NO	YES	NO
4	RESOURCE	CREATE CLUSTER	NO	YES	NO
5	CONNECT	CREATE SESSION	NO	YES	NO
6	RESOURCE	CREATE INDEXTYPE	NO	YES	NO
7	RESOURCE	CREATE OPERATOR	NO	YES	NO
8	RESOURCE	CREATE TYPE	NO	YES	NO
9	RESOURCE	CREATE TRIGGER	NO	YES	NO
10	RESOURCE	CREATE TABLE	NO	YES	NO

4. Consulta los privilegios de sistema concedidos al rol DBA.

```
SELECT * FROM DBA_SYS_PRIVS WHERE GRANTEE = 'DBA';
```

	GRANTEE	PRIVILEGE	ADMIN_OPTION	COMMON	INHERITED
1	DBA	CREATE ANALYTIC VIEW	NO	YES	NO
2	DBA	ALTER ANY CUBE BUILD PROCESS	NO	YES	NO
3	DBA	CREATE LOCKDOWN PROFILE	NO	YES	NO
4	DBA	EM EXPRESS CONNECT	NO	YES	NO
5	DBA	DROP ANY SQL TRANSLATION PROFILE	NO	YES	NO
6	DBA	UPDATE ANY CUBE DIMENSION	NO	YES	NO
7	DBA	DELETE ANY CUBE DIMENSION	NO	YES	NO
8	DBA	SELECT ANY MINING MODEL	NO	YES	NO
9	DBA	ALTER ANY ASSEMBLY	NO	YES	NO
10	DBA	MANAGE FILE GROUP	NO	YES	NO

Hay muchos más resultado, pero solo he capturado la imagen hasta aquí

5. Consulta los privilegios sobre objetos concedidos a los roles CONNECT y RESOURCE.

```
SELECT * FROM DBA_TAB_PRIVS WHERE GRANTEE = 'RESOURCE';
```

-- no sale nada?? exactooo, se comprueba con el siguiente apartado

```
SELECT * FROM DBA_TAB_PRIVS WHERE GRANTEE = 'CONNECT'; -- no sale nada
```

6. Consulta los privilegios sobre objetos concedidos al rol DBA.

	GRANTEE	OWNER	TABLE_NAME	GRANTOR	PRIVILEGE	GRANTABLE	HIERARCHY	COMMON	TYPE	INHERITED
1	DBA	SYS	MAP_OBJECT	SYS	DELETE	NO	NO	YES	TABLE	NO
2	DBA	SYS	MAP_OBJECT	SYS	INSERT	NO	NO	YES	TABLE	NO
3	DBA	SYS	MAP_OBJECT	SYS	SELECT	NO	NO	YES	TABLE	NO
4	DBA	SYS	MAP_OBJECT	SYS	UPDATE	NO	NO	YES	TABLE	NO
5	DBA	SYS	X\$SDB4SCHEMA_ACL	SYS	INSERT	NO	NO	YES	TABLE	NO
6	DBA	SYS	X\$SDB4SCHEMA_ACL	SYS	SELECT	NO	NO	YES	TABLE	NO
7	DBA	SYS	X\$SDB4SCHEMA_ACL	SYS	UPDATE	NO	NO	YES	TABLE	NO
8	DBA	SYS	DBMS_LOGSTDBY	SYS	EXECUTE	NO	NO	YES	PACKAGE	NO
9	DBA	SYS	ADR_HOME_T	SYS	EXECUTE	NO	NO	YES	TYPE	NO
10	DBA	SYS	ADR_INCIDENT_CORP_KEYS_T	SYS	EXECUTE	NO	NO	YES	TYPE	NO

Hay muchos más resultado, pero solo he capturado la imagen hasta aquí

Crear roles**7. Crea el usuario `alumno1` con contraseña `alumno1`.**

```
ALTER SESSION SET "_ORACLE_SCRIPT" = TRUE;
CREATE USER ALUMNO1 IDENTIFIED BY ALUMNO1;
ALTER USER ALUMNO1 QUOTA 5M ON USERS;
```

```

Permisos_Roles.sql
Hoja de Trabajo  Generador de Consultas
102  -- 7.  Crea el usuario alumno1 con contraseña alumno1.
103
104  ALTER SESSION SET "_ORACLE_SCRIPT" = TRUE;
105
106  CREATE USER ALUMNO1 IDENTIFIED BY ALUMNO1;
107
108  ALTER USER ALUMNO1 QUOTA 5M ON USERS;
Resultado de la Consulta  Salida de Script
Tarea terminada en 0,173 segundos

Session alterado.

User ALUMNO1 creado.

Error que empieza en la linea: 108 del comando :
ALTER USER ALUMNO1 QUOTA 5M ON USER
Informe de error -
ORA-02156: identificador de tablespace TEMPORARY no válido
02156. 00000 - "invalid TEMPORARY tablespace identifier"
*Cause:   An identifier does not follow TEMPORARY TABLESPACE.
*Action:   Place a tablespace name after TEMPORARY TABLESPACE.

User ALUMNO1 alterado.

```

8. Crea el usuario `alumno2` con contraseña `alumno2`.

```
ALTER SESSION SET "_ORACLE_SCRIPT" = TRUE;
CREATE USER ALUMNO2 IDENTIFIED BY ALUMNO2;
ALTER USER ALUMNO2 QUOTA 5M ON USERS;
```

```

Permisos_Roles.sql
Hoja de Trabajo  Generador de Consultas
109
110  -- 8.  Crea el usuario alumno2 con contraseña alumno2.
111
112  ALTER SESSION SET "_ORACLE_SCRIPT" = TRUE;
113
114  CREATE USER ALUMNO2 IDENTIFIED BY ALUMNO2;
115
116  ALTER USER ALUMNO2 QUOTA 5M ON USERS;
117
Salida de Script
Tarea terminada en 0,035 segundos

Session alterado.

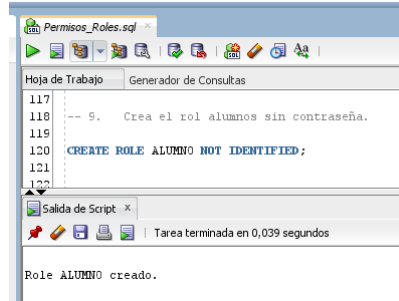
User ALUMNO2 creado.

User ALUMNO2 alterado.

```

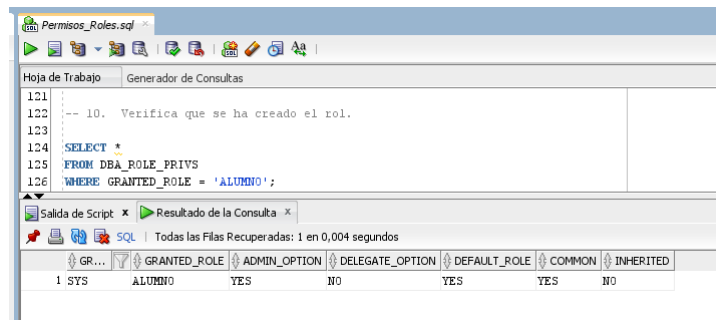
9. Crea el rol **alumnos** sin contraseña.

CREATE ROLE ALUMNO NOT IDENTIFIED;



10. Verifica que se ha creado el rol.

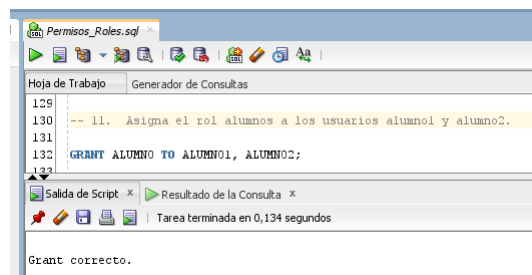
SELECT *
FROM DBA_ROLE_PRIVS
WHERE GRANTED_ROLE = 'ALUMNO';



Asignar roles a usuarios

11. Asigna el rol **alumnos** a los usuarios **alumno1** y **alumno2**.

GRANT ALUMNO TO ALUMNO1, ALUMNO2;



12. Verifica que el rol se ha asignado a los usuarios.

```
SELECT *
FROM DBA_ROLE_PRIVS
WHERE GRANTED_ROLE = 'ALUMNO';
```

Hoja de Trabajo: Generador de Consultas

```

133
134 -- 12. Verifica que el rol se ha asignado a los usuarios.
135
136 SELECT *
137 FROM DBA_ROLE_PRIVS
138 WHERE GRANTED_ROLE = 'ALUMNO';

```

Salida de Script x Resultado de la Consulta x

Todas las Filas Recuperadas: 3 en 0,006 segundos

	GRANTEE	GRANTED_ROLE	ADMIN_OPTION	DELEGATE_OPTION	DEFAULT_ROLE	COMMON	INHERITED
1	ALUMNO02	ALUMNO	NO	NO	YES	YES	NO
2	SYS	ALUMNO	YES	NO	YES	YES	NO
3	ALUMNO01	ALUMNO	NO	NO	YES	YES	NO

Asignar privilegios a roles

Privilegios de sistema

13. Asigna los privilegios de sistema **CREATE SESSION**, **CREATE TABLE** y **CREATE VIEW** al rol **alumnos**.

```
GRANT CREATE SESSION, CREATE TABLE, CREATE VIEW TO ALUMNO;
```

Hoja de Trabajo: Generador de Consultas

```

141
142 -- 13. Asigna los privilegios de sistema CREATE SESSION, CREATE TABLE y CREATE VIEW al rol alumnos.
143
144 GRANT CREATE SESSION, CREATE TABLE, CREATE VIEW TO ALUMNO;
145
146

```

Salida de Script x Resultado de la Consulta x

Tarea terminada en 0,12 segundos

Grant correcto.

Grant correcto.

14. Verifica que se han asignado los privilegios

```
SELECT * FROM DBA_SYS_PRIVS WHERE GRANTEE = 'ALUMNO';
```

Hoja de Trabajo: Generador de Consultas

```

145
146 -- 14. Verifica que se han asignado los privilegios
147
148 SELECT * FROM DBA_SYS_PRIVS WHERE GRANTEE = 'ALUMNO';
149

```

Salida de Script x Resultado de la Consulta x

Todas las Filas Recuperadas: 3 en 0,047 segundos

	GRANTEE	PRIVILEGE	ADMIN_OPTION	COMMON	INHERITED
1	ALUMNO	CREATE TABLE	NO	YES	NO
2	ALUMNO	CREATE VIEW	NO	YES	NO
3	ALUMNO	CREATE SESSION	NO	YES	NO

15. Establece una conexión como **alumno1** y verifica los **privilegios de sistema y roles** que tiene disponibles en su sesión.

```
SELECT * FROM USER_SYS_PRIVS;
SELECT * FROM USER_ROLE_PRIVS;
```

The screenshot shows the SQL Developer interface with a script named 'Permisos_Roles.sql'. The script contains two SQL queries: 'SELECT * FROM USER_SYS_PRIVS;' and 'SELECT * FROM USER_ROLE_PRIVS;'. The results are displayed in a table with the following columns: USERNAME, GRANTED_ROLE, ADMIN_OPTION, DELEGATE_OPTION, DEFAULT_ROLE, OS_GRANTED, COMMON, and INHERITED. The results show that user ALUMNO1 has the role ALUMNO and no system privileges.

USERNAME	GRANTED_ROLE	ADMIN_OPTION	DELEGATE_OPTION	DEFAULT_ROLE	OS_GRANTED	COMMON	INHERITED
1 ALUMNO1	ALUMNO	NO	NO	YES	NO	YES	NO

Privilegios sobre objetos.

16. Desde el usuario **system** asigna los privilegios sobre objetos para **consultar e insertar** en las tablas **jugadores** y **equipos** de usuario **nbaxx** al rol **alumnos**.

```
GRANT SELECT, INSERT ON nba12.JUGADORES TO ALUMNO;
GRANT SELECT, INSERT ON nba12.EQUIPOS TO ALUMNO;
```

The screenshot shows the SQL Developer interface with a script named 'Permisos_Roles.sql'. The script contains two SQL queries: 'GRANT SELECT, INSERT ON nba12.JUGADORES TO ALUMNO;' and 'GRANT SELECT, INSERT ON nba12.EQUIPOS TO ALUMNO;'. The results are displayed in a table with the following columns: USERNAME, GRANTED_ROLE, ADMIN_OPTION, DELEGATE_OPTION, DEFAULT_ROLE, OS_GRANTED, COMMON, and INHERITED. The results show that user ALUMNO1 has the role ALUMNO and no system privileges.

USERNAME	GRANTED_ROLE	ADMIN_OPTION	DELEGATE_OPTION	DEFAULT_ROLE	OS_GRANTED	COMMON	INHERITED
1 ALUMNO1	ALUMNO	NO	NO	YES	NO	YES	NO

17. Verifica que se han asignado los privilegios.

```
SELECT * FROM DBA_SYS_PRIVS WHERE GRANTEE = 'ALUMNO';
```

Hoja de Trabajo de SQL | Historial

Hoja de Trabajo | Generador de Consultas

```
-- 17. Verifica que se han asignado los privilegios.

SELECT * FROM DBA_SYS_PRIVS WHERE GRANTEE = 'ALUMNO';

-- 18. Establece una conexión como alumno1 y verifica los privilegios de objetos y roles que tiene disponibles en su sesión.
-- Comprueba que puede consultar la tabla jugadores del usuario taller.
-- en realidad se refiere al nba12

SELECT * FROM USER_TAB_PRIVS;
SELECT * FROM USER_ROLE_PRIVS;

SELECT * FROM nba12.JUGADORES;
```

Salida de Script x | Resultado de la Consulta x

SQL | Se han recuperado 100 filas en 0,052 segundos

	CODIGO	NOMBRE	PROCEDENCIA	ALTURA	PESO	POSICION	NOMBRE_EQUIPO
1	604	Austin Croshere	Spain	6-10	235 F		Warriors
2	605	Baron Davis	Spain	6-3	215 G		Warriors
3	606	Monta Ellis	Spain	6-3	177 G		Warriors
4	607	Al Harrington	Spain	6-9	250 F-C		Warriors
5	608	Stephen Jackson	Spain	6-8	218 F		Warriors
6	609	Patrick O'Bryant	Spain	7-0	250 C		Warriors
7	610	Kosta Perovic	Spain	7-2	240 C		Warriors
8	611	Mickael Pietrus	Spain	6-6	215 F		Warriors
9	612	C.J. Watson	Spain	6-2	180 G		Warriors
10	613	Brandon Wright	Spain	6-9	205 F		Warriors

18. Establece una conexión como **alumno1** y verifica los privilegios de objetos y roles que tiene disponibles en su sesión. Comprueba que puede consultar la tabla jugadores del usuario taller.

```
SELECT * FROM USER_TAB_PRIVS;
SELECT * FROM USER_ROLE_PRIVS;
```

```
SELECT * FROM nba12.JUGADORES;
```

Hoja de Trabajo de SQL | Historial

Hoja de Trabajo | Generador de Consultas

```
-- 18. Establece una conexión como alumno1 y verifica los privilegios de objetos y roles que tiene disponibles en su sesión.
-- Comprueba que puede consultar la tabla jugadores del usuario taller.
-- en realidad se refiere al nba12

SELECT * FROM USER_TAB_PRIVS;
SELECT * FROM USER_ROLE_PRIVS;
```

Salida de Script x | Resultado de la Consulta x

SQL | Todas las Filas Recuperadas: 1 en 0,002 segundos

	USERNAME	GRANTED_ROLE	ADMIN_OPTION	DELEGATE_OPTION	DEFAULT_ROLE	OS_GRANTED	COMMON	INHERITED
1	ALUMNO1	ALUMNO	NO	NO	YES	NO	YES	NO

The screenshot shows a SQL Developer window with a script named 'Permisos_Roles.sql'. The script contains the following SQL queries:

```
-- 18. Establece una conexión como alumno1 y verifica los privilegios de objetos y roles que tiene disponibles en su sesión.
-- Comprueba que puede consultar la tabla jugadores del usuario taller.
-- en realidad se refiere al nba12

SELECT * FROM USER_TAB_PRIVS;
SELECT * FROM USER_ROLE_PRIVS;

SELECT * FROM nba12.JUGADORES;

-- en la tabla de los permisos de objetos, no aparece el privilegio de consultar una tabla de otro usuario...
-- sin embargo ALUMNO1 ha podido consultar en nba12...
-- esto es porque ese privilegio no es directo, si no que lo tiene a través del rol ALUMNO, y por eso no salía en la tabla de objetos
```

The results of the queries are displayed in a table with the following columns: CODIGO, NOMBRE, PROCEDENCIA, ALTURA, PESO, POSICION, and NOMBRE_EQUIPO. The data is as follows:

CODIGO	NOMBRE	PROCEDENCIA	ALTURA	PESO	POSICION	NOMBRE_EQUIPO
1	604 Austin Croshere	Spain	6-10	235 F		Warriors
2	605 Baron Davis	Spain	6-3	215 G		Warriors
3	606 Monta Ellis	Spain	6-3	177 G		Warriors
4	607 Al Harrington	Spain	6-9	250 F-C		Warriors
5	608 Stephen Jackson	Spain	6-8	218 F		Warriors

Revocar privilegios a roles

Privilegios de sistema

19. Revoca el privilegio **CREATE VIEW** al rol **alumnos**.

```
ALTER SESSION SET "_ORACLE_SCRIPT" = TRUE;
REVOKE CREATE VIEW FROM ALUMNO;
```

The screenshot shows the same SQL Developer window with the script 'Permisos_Roles.sql'. The script contains the following SQL queries:

```
-- Privilegios de sistema
-- 19. Revoca el privilegio CREATE VIEW al rol alumnos.

ALTER SESSION SET "_ORACLE_SCRIPT" = TRUE;
REVOKE CREATE VIEW FROM ALUMNO;
```

The results of the queries are displayed in a table with the following columns: CODIGO, NOMBRE, PROCEDENCIA, ALTURA, PESO, POSICION, and NOMBRE_EQUIPO. The data is as follows:

CODIGO	NOMBRE	PROCEDENCIA	ALTURA	PESO	POSICION	NOMBRE_EQUIPO
1	604 Austin Croshere	Spain	6-10	235 F		Warriors
2	605 Baron Davis	Spain	6-3	215 G		Warriors
3	606 Monta Ellis	Spain	6-3	177 G		Warriors
4	607 Al Harrington	Spain	6-9	250 F-C		Warriors
5	608 Stephen Jackson	Spain	6-8	218 F		Warriors

20. Verifica que se ha revocado el privilegio.

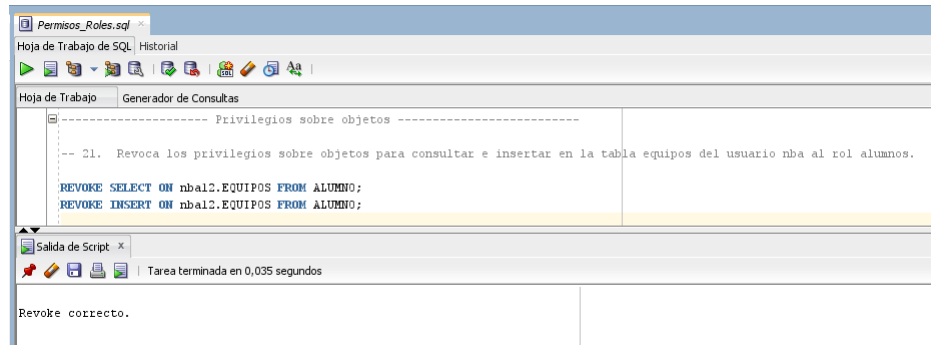
```
SELECT * FROM DBA_SYS_PRIVS WHERE GRANTEE = 'ALUMNO';
```

Efectivamente se ha revocado, es decir, salen los campos de la tabla pero sin datos.

Privilegios sobre objetos

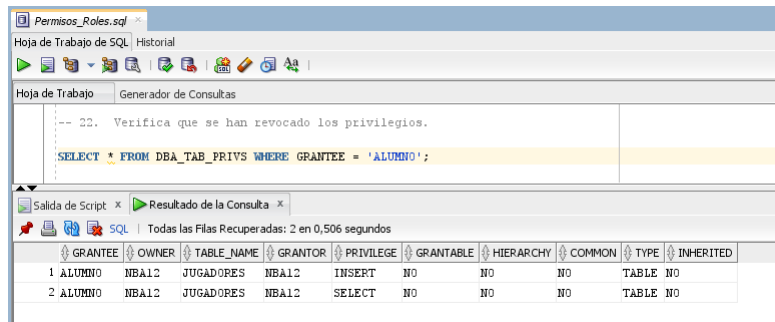
21. Revoca los privilegios sobre objetos para **consultar** e **insertar** en la tabla **equipos** del usuario **nba** al rol **alumnos**.

```
REVOKE SELECT ON nba12.EQUIPOS FROM ALUMNO;
REVOKE INSERT ON nba12.EQUIPOS FROM ALUMNO;
```



22. Verifica que se han revocado los privilegios.

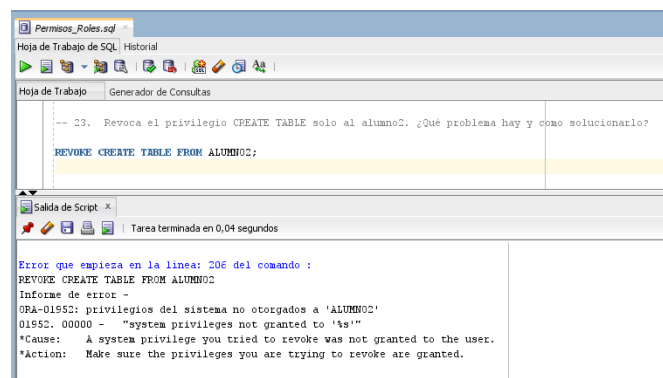
```
SELECT * FROM DBA_TAB_PRIVS WHERE GRANTEE = 'ALUMNO';
```



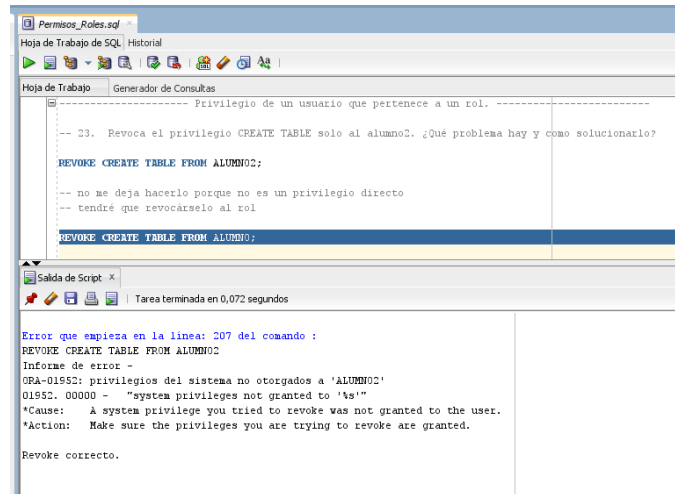
Privilegio de un usuario que pertenece a un rol.

23. Revoca el privilegio **CREATE TABLE** solo al **alumno2**. ¿Qué problema hay y como solucionarlo?

```
REVOKE CREATE TABLE FROM ALUMNO2;
```



No es posible porque el usuario tiene el privilegio concedido a través del rol **alumnos** y no directamente.



The screenshot shows a SQL IDE window titled 'Permisos_Roles.sql'. The main editor contains the following SQL code:

```
-- Privilegio de un usuario que pertenece a un rol. -----
-- C3. Revoca el privilegio CREATE TABLE solo al alumno2. ¿Qué problema hay y como solucionarlo?

REVOKE CREATE TABLE FROM ALUMNO2;

-- no me deja hacerlo porque no es un privilegio directo
-- tendré que revocárselo al rol

REVOKE CREATE TABLE FROM ALUMNO;
```

The output window at the bottom shows the following error message:

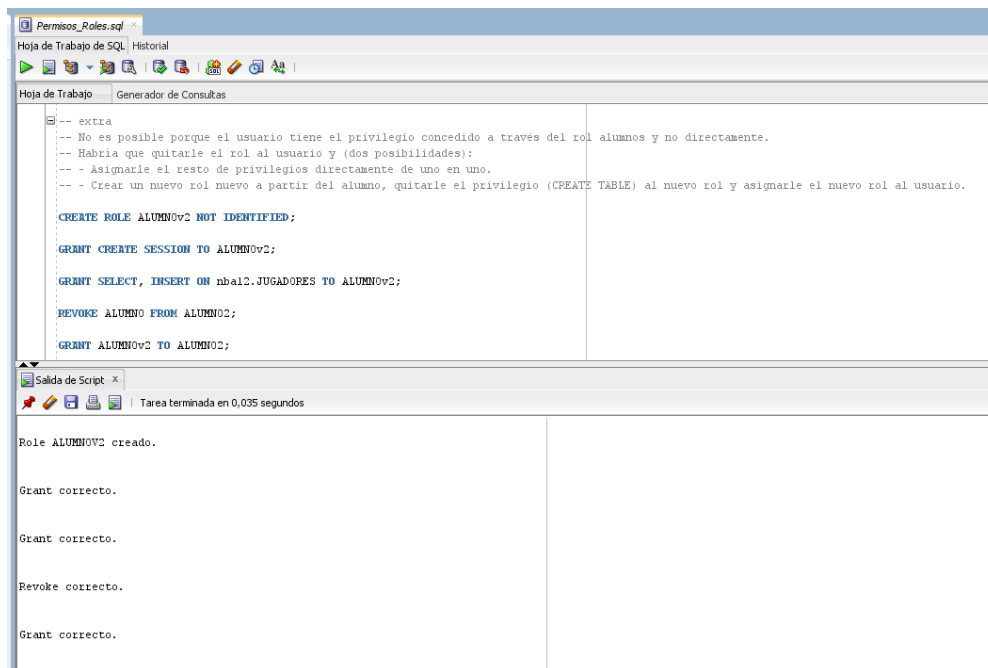
```
Error que empieza en la línea: 207 del comando :
REVOKE CREATE TABLE FROM ALUMNO2
Informe de error :
ORA-01952: privilegios del sistema no otorgados a 'ALUMNO2'
01952. 00000 - "system privileges not granted to 's'"
*Cause: A system privilege you tried to revoke was not granted to the user.
*Action: Make sure the privileges you are trying to revoke are granted.

Revoke correcto.
```

Habría que quitarle el rol al usuario y (dos posibilidades):

- Asignarle el resto de privilegios directamente de uno en uno.
- Crear un nuevo rol nuevo a partir del alumno, quitarle el privilegio (**CREATE TABLE**) al nuevo rol y asignarle el nuevo rol al usuario.

```
CREATE ROLE ALUMNOv2 NOT IDENTIFIED;
GRANT CREATE SESSION TO ALUMNOv2;
GRANT SELECT, INSERT ON nba12.JUGADORES TO ALUMNOv2;
REVOKE ALUMNO FROM ALUMNO2;
GRANT ALUMNOv2 TO ALUMNO2;
```



The screenshot shows a SQL IDE window titled 'Permisos_Roles.sql'. The main editor contains the following SQL code:

```
-- extra
-- No es posible porque el usuario tiene el privilegio concedido a través del rol alumnos y no directamente.
-- Habría que quitarle el rol al usuario y (dos posibilidades):
-- - Asignarle el resto de privilegios directamente de uno en uno.
-- - Crear un nuevo rol nuevo a partir del alumno, quitarle el privilegio (CREATE TABLE) al nuevo rol y asignarle el nuevo rol al usuario.

CREATE ROLE ALUMNOv2 NOT IDENTIFIED;

GRANT CREATE SESSION TO ALUMNOv2;

GRANT SELECT, INSERT ON nba12.JUGADORES TO ALUMNOv2;

REVOKE ALUMNO FROM ALUMNO2;

GRANT ALUMNOv2 TO ALUMNO2;
```

The output window at the bottom shows the following successful execution results:

```
Role ALUMNOv2 creado.

Grant correcto.

Grant correcto.

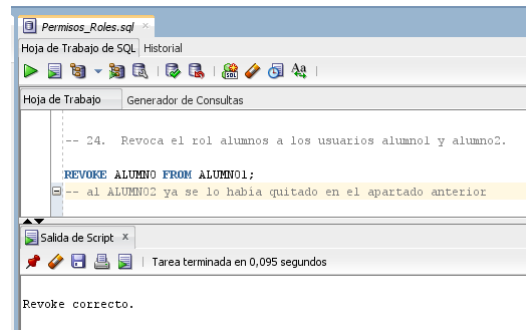
Revoke correcto.

Grant correcto.
```

Revocar roles

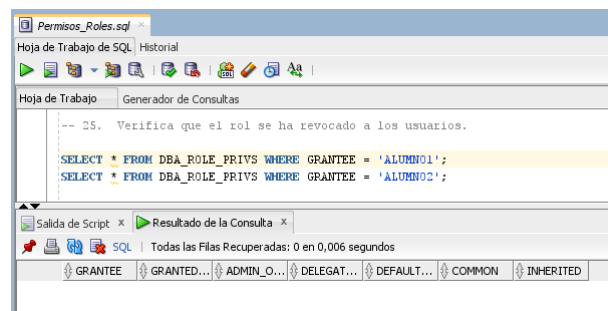
24. Revoca el rol **alumnos** a los usuarios **alumno1** y **alumno2**.

REVOKE ALUMNO FROM ALUMNO1;



25. Verifica que el rol se ha revocado a los usuarios.

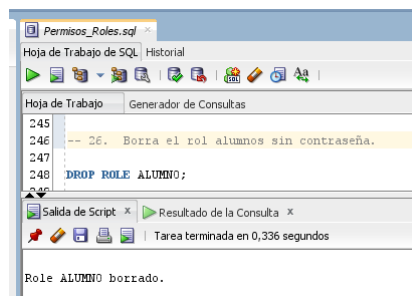
SELECT * FROM DBA_ROLE_PRIVS WHERE GRANTEE = 'ALUMNO1';
SELECT * FROM DBA_ROLE_PRIVS WHERE GRANTEE = 'ALUMNO2';



Borrar roles

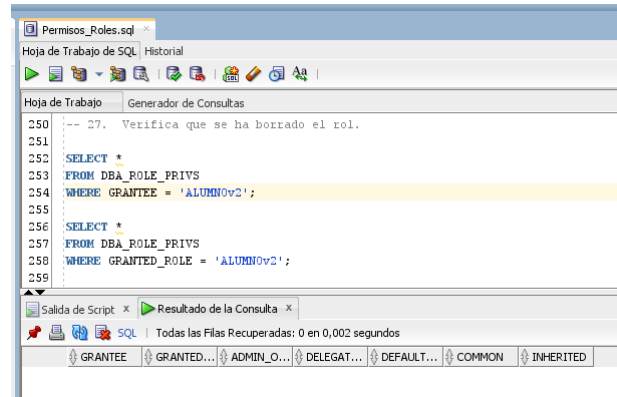
26. Borra el rol **alumnos** sin contraseña.

DROP ROLE ALUMNO;



27. Verifica que se ha borrado el rol.

```
SELECT *
FROM DBA_ROLE_PRIVS
WHERE GRANTEE = 'ALUMNOv2';
```



28. Borra los usuarios **alumno1** y **alumno2** (asegúrate de no tener sesiones abiertas con estos usuarios).

```
DROP USER ALUMNO1;
DROP USER ALUMNO2;
```

