



# Grant (dar permisos)

Esta sentencia sirve para dar permisos (o privilegios) a un usuario o a un rol.

Un permiso, en oracle, es un derecho a ejecutar un sentencia (system privileges) o a acceder a un objeto de otro usuario (object privileges).

El conjunto de permisos es fijo, esto quiere decir que no se pueden crear nuevos tipos de permisos.

Si un permiso se asigna a rol especial PUBLIC significa que puede ser ejecutado por todos los usuarios.

Permisos para acceder a la base de datos (permiso de sistema):

```
GRANT CREATE SESSION TO miusuario;
```

Permisos para usuario de modificación de datos (permiso sobre objeto):

```
GRANT SELECT (/dml/select.html), INSERT (/dml/insert.html), UPDATE (/dml/update.html), DELETE (/dml/delete.html) ON T_PEDIDOS TO miusuario;
```

Permisos de solo lectura para todos:

```
GRANT SELECT (/dml/select.html) ON T_PEDIDOS TO PUBLIC;
```

## Permisos de sistema (system privileges)

Los permisos de sistema mas importantes son CREATE SESSION, CREATE TABLE (/ddl/create%20table.html), CREATE VIEW (/ddl/create%20view.html), CREATE (/usuarios/create%20user.html)USER (/sistema/user.html), ...

Sintaxis:

```
GRANT system_priv(s) TO {user, | role, |PUBLIC}
                        [IDENTIF (/plsql/if.html)IED BY password] [WITH ADMIN (/grupo/min.html)
OPTION]
```

```
GRANT role TO {user, | role, |PUBLIC}
              [IDENTIF (/plsql/if.html)IED BY password] [WITH ADMIN (/grupo/min.html)
OPTION]
```

```
GRANT ALL PRIVILEGES TO {user, | role, |PUBLIC}
    [IDENTIFIED BY password] [WITH ADMIN OPTION]
OPTION]
```

Podemos obtener la lista de permisos del sistema así:

```
select * from system_privilege_map;
```

Los permisos de sistema son auditables.

```
GRANT CREATE SESSION, CREATE TABLE (/ddl/create%20table.html), CREATE VIEW
(/ddl/create%20view.html), CREATE PROCEDURE (/plsql/procedure.html),CREATE SYNONYM
(/ddl/create%20synonym.html),
    ALTER TABLE (/ddl/alter%20table.html), ALTER VIEW, ALTER PROCEDURE
(/plsql/procedure.html),ALTER SYNONYM,
    DROP TABLE, DROP VIEW, DROP PROCEDURE (/plsql/procedure.html),DROP SYNONYM TO programador;
```

## Permisos sobre objetos (object privileges)

Los permisos sobre objetos mas importantes son: SELECT (/dml/select.html), UPDATE (/dml/update.html), INSERT (/dml/insert.html), DELETE (/dml/delete.html), ALTER, DEBUG, EXECUTE (/plsql/execute.html), INDEX, REFERENCES

```
GRANT object_priv [(column, column,...)]
    ON [schema.]object
    TO {user, | role, |PUBLIC} [WITH GRANT OPTION] [WITH HIERARCHY OPTION]
```

```
GRANT ALL PRIVILEGES [(column, column,...)]
    ON [schema.]object
    TO {user, | role, |PUBLIC} [WITH GRANT OPTION] [WITH HIERARCHY OPTION]
```

```
GRANT object_priv [(column, column,...)]
    ON DIRECTORY directory_name
    TO {user, | role, |PUBLIC} [WITH GRANT OPTION] [WITH HIERARCHY OPTION]
```

```
GRANT object_priv [(column, column,...)]
    ON JAVA [RE]SOURCE [schema.]object
    TO {user, | role, |PUBLIC} [WITH GRANT OPTION] [WITH HIERARCHY OPTION]
```

Con la opcion WITH HIERARCHY OPTION damos permisos sobre todos los subobjetos, incluso sobre los que se creen despues de ejecutar el GRANT.

Con la opción WITH GRANT OPTION damos permiso para que el que los recibe los pueda a su vez asignar a otros usuarios y roles.

La opción "GRANT ALL PRIVILEGES..." se puede escribir tambien como "GRANT ALL..."

Podemos obtener la lista de permisos de las tablas asi:

```
select * from all_tab_privs_made;
```

## Notas

Los permisos del sistema pueden ser:

```
CREATE SESSION - Permite conectar a la base de datos
UNLIMITED TABLESPACE - Uso de espacio ilimitado del tablespace.
SELECT (/dml/select.html) ANY TABLE - Consultas en tables, views, or mviews en cualquier
esquema
UPDATE (/dml/update.html) ANY TABLE - Actualizar filas en tables and views en cualquier
esquema
INSERT (/dml/insert.html) ANY TABLE - Insertar filas en tables and views en cualquier esquema
```

Permisos de administrador para CREATE, ALTER o DROP:

```
cluster, context, database, link, dimension, directory, index,
materialized view, operator, outline, procedure, profile, role,
rollback segment, sequence, session, synonym, table, tablespace,
trigger, type, user, view.
```

Los roles predefinidos son:

```
SYSDBA, SYSOPER, OSDBA, OSOPER, EXP_FULL_DATABASE, IMP_FULL_DATABASE
SELECT (/dml/select.html)_CATALOG_ROLE, EXECUTE (/plsql/execute.html)_CATALOG_ROLE, DELETE
(/dml/delete.html)_CATALOG_ROLE
AQ_USER (/sistema/user.html)_ROLE, AQ_ADMIN (/grupo/min.html)ISTRATOR_ROLE - manejo de la
cola
SNMPAGENT - Agente inteligente.
RECOVERY_CATALOG_OWNER - rman
HS_ADMIN (/grupo/min.html)_ROLE - servicios heterogeneos
```

mas cualquier rol de usuario que halla disponible Los roles CONNECT, RESOURCE y DBA ya no deben usarse (aunque estan soportados).

Es posible asignar varios Object\_Privs en un solo comando GRANT.

```
GRANT SELECT (/dml/select.html) (empno), UPDATE (/dml/update.html) (sal) ON pepe.tabla TO
miusuario
```

Permisos del rol SYSDBA:

```
CREATE DATABASE (/ddl/create%20database.html)
CREATE SPFILE
STARTUP (/dba/startup.html) and SHUTDOWN (/dba/shutdown.html)
ALTER DATABASE: open, mount, back up, or change character set
ARCHIVELOG and RECOVERY
Includes the RESTRICTED SESSION privilege
```

Permisos del rol SYSOPER:

```
CREATE SPFILE  
STARTUP (/dba/startup.html) and SHUTDOWN (/dba/shutdown.html)  
ALTER DATABASE: open, mount, back up  
ARCHIVELOG and RECOVERY  
Includes the RESTRICTED SESSION privilege
```

Cada tipo de objeto tiene su propio conjunto de permisos:

Tables: select, insert, update, delete, alter, debug, flashback, on commit refresh, query rewrite, references, all

Views: select, insert, update, delete, under, references, flashback, debug

Sequence: alter, select

Packages, Procedures, Functions (Java classes, sources...): execute, debug

Materialized Views: delete, flashback, insert, select, update

Directories: read, write

Libraries: execute

User defined types: execute, debug, under

Operators: execute

Indextypes: execute

CREATE PROFILE (/usuarios/create%20profile.html)

GRANT (/usuarios/grant.html)

REVOKE (/usuarios/revoke.html)

CREATE ROLE (/usuarios/create%20role.html)

CREATE USER (/usuarios/create%20user.html)

**Explicación de la sintaxis utilizada para los comandos:** Las palabras en mayúsculas son comandos de oracle.

Las palabras en minúsculas son opciones modificables. Las partes enmarcadas con [] son opcionales. Las palabras en negrita son las opciones por defecto. Las partes enmarcadas con {} son alternativas (una u otra). El simbolo | indica OR.

