

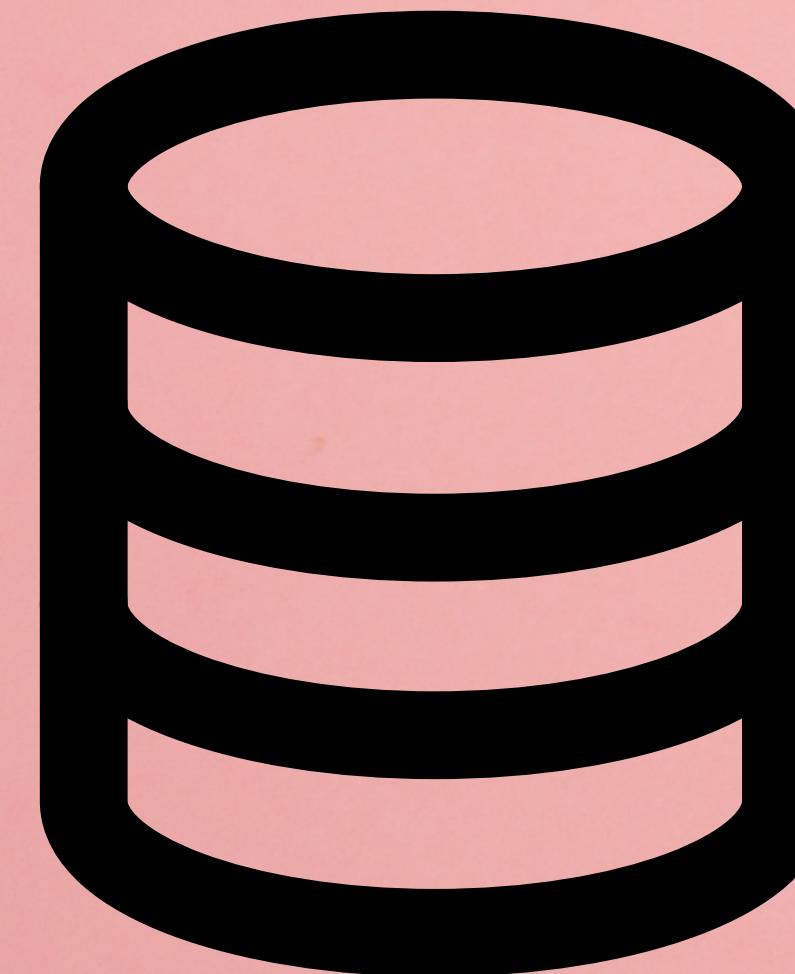


01

Privilegios del Sistema

Arantxa Fernández Morató

02



índice

1. Oracle
2. MySQL
3. PostgreSQL
4. MongoDB

Oracle

DEFINICIÓN

Los privilegios del sistema permiten realizar una determinada operación o ejecutar un comando concreto a un usuario o rol.

INFORMACIÓN SOBRE PRIVILEGIOS

DBA_SYS_PRIVS

SINTAXIS

GRANT privilegio TO [usuario|rol | PUBLIC] [WITH ADMIN OPTION]

Ejemplo:

GRANT select any table TO arantxa;

ORACLE	
Lista de privilegios de sistema:	
* El CREATE ANY nos permite no solo crear en nuestro esquema sino en el de otros usuarios. El ANY puede ser muy peligroso, ya que si le damos un privilegio DROP ANY a un usuario, podría borrar cualquier tabla de la base de datos.	
PRIVILEGIO	SIGNIFICADO
Usuarios, roles y perfiles	
CREATE USER ALTER USER	⇒ Crear usuarios pudiendo indicar tablespace por defecto, cuotas y perfiles ⇒ Modificar al usuario. Permite cambiar la contraseña y modo de autenticación, tablespace por defecto, cuota de uso de disco, roles y el perfil del usuario
DROP USER CREATE PROFILE ALTER PROFILE DROP PROFILE CREATE ROLE ALTER ANY ROLE GRANT ANY ROLE DROP ANY ROLE BECOME USER	⇒ Borrar usuario ⇒ Crear perfiles ⇒ Modificar perfiles ⇒ Borrar perfiles ⇒ Crear roles ⇒ Modificar cualquier rol ⇒ Conceder cualquier rol ⇒ Borrar cualquier rol ⇒ Convertirse en otro usuario (requerido por cualquier usuario que realice una importación de base de datos completa)
Tablas	
CREATE TABLE CREATE ANY TABLE	⇒ Crear tablas en el esquema del usuario ⇒ Crear tablas en cualquier esquema (el propietario del esquema debe tener cuota de espacio en el tablespace para contener la tabla)

Lista de privilegios

CREATE, ALTER, DROP...



No hay privilegios de sistema como tal
Sistema jerárquico

Seis niveles:

- Global: mysql.user
- Base de datos: mysql.db
- Tabla: mysql.tables_priv
- Columna: mysql.columns_priv
- Rutinas almacenadas:
mysql.procs_priv
- Proxy: mysql.proxies_priv

Obtener info:
show grants [for usuario]
show privileges

Sintaxis:
GRANT privilegio ON basedatos.tabla
TO 'usuario|rol'@'host' [WITH GRANT
OPTION]

*WITH GRANT OPTION: Si queremos que el
usuario al que le damos el privilegio pueda dar
ese mismo privilegio.

Ejemplo:
GRANT all ON bd1.* TO
'arantxa'@'localhost';

Lista de privilegios

Estáticos y dinámicos

ALTER
CREATE
DROP
SHOW DATABASES
AUDIT_ADMIN
...

MySQL

Listado de privilegios:

Hay dos tipos de privilegios: estáticos y dinámicos.

Los dinámicos los usarán principalmente usuarios administradores de la base de datos.

Las siguientes tablas resumen los tipos de privilegios priv_type estáticos y dinámicos permisibles que se pueden especificar para las declaraciones GRANT y REVOKE, y los niveles en los que se puede otorgar cada privilegio

*Rojo => He marcado en rojo los privilegios que en Oracle serían privilegios sobre objeto.

Privilegios estáticos para Grant y Revoke		
Privilege	Nivel	Significado
ALL [PRIVILEGES]		Concede todos los privilegios, excepto GRANT OPTION y PROXY
ALTER	Global, database, table	Para modificar tablas
ALTER ROUTINE	Global, database, routine	Para modificar o borrar procedimientos/funciones almacenados
CREATE	Global, database, table	Crear nuevas bases de datos y tablas

PostgreSQL

GRANT TIENE DOS VARIANTES

- Privilegios sobre objetos de la base de datos
- Membresía roles: con frecuencia, es conveniente agrupar a los usuarios para facilitar la administración de los privilegios. Ejemplo:

```
CREATE ROLE joe LOGIN INHERIT;  
CREATE ROLE admin NOINHERIT;  
CREATE ROLE wheel NOINHERIT;  
GRANT admin TO joe;  
GRANT wheel TO admin;
```

SINTAXIS

General:

```
GRANT privilegio ON objeto TO {PUBLIC | grupo | usuario}
```

Específica para cada caso:

<https://www.postgresql.org/docs/current/sql-grant.html>

Ejemplo:

```
GRANT all ON DATABASE bd1  
TO arantxa WITH GRANT  
OPTION
```

08

Comprobar privs de rol:

```
select * from  
INFORMATION_SCHEMA.TABLE_PRIVILEGES where  
GRANTEE=<nombre_rol>;
```

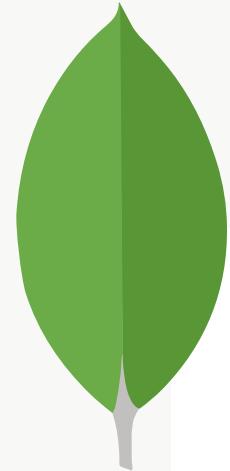
Lista privilegios

PostgreSQL

Lista de privilegios:

Privilegio	Descripción	Tipos de objeto aplicables
CREATE	Permite crear nuevos esquemas y publicaciones dentro de la base de datos y permite instalar extensiones confiables dentro de la base de datos. También permite que se creen nuevos objetos dentro del esquema. Para cambiar el nombre de un objeto existente, debe poseer el objeto y tener este privilegio para el esquema que lo contiene. Para espacios de tabla, permite que se creen tablas, índices y archivos temporales dentro del espacio de tabla, y permite que se creen bases de datos que tengan el espacio de tabla como su espacio de tabla predeterminado. La revocación de este privilegio no alterará la existencia o ubicación de los objetos existentes.	Base de datos, esquema, tablespace
CONNECT	Permite al beneficiario conectarse a la base de datos. Este privilegio se verifica al inicio de la conexión (además de verificar las restricciones impuestas por pg_hba.conf)	Base de datos
TEMPORARY	Permite crear tablas temporales mientras se usa la base de datos.	Base de datos
EXECUTE	Permite llamar a una función o procedimiento, incluido el uso de cualquier operador que se implemente sobre la función. Este es el único tipo de privilegio aplicable a funciones y procedimientos.	Funciones, procedimientos
USAGE	Para lenguajes procedimentales, permite el uso del lenguaje para la creación de funciones en ese lenguaje. Este es el único tipo de privilegio que se aplica a los lenguajes procesales. Para los esquemas, permite el acceso a los objetos contenidos en el esquema (suponiendo que también se cumplan los requisitos de privilegios propios de los objetos). Esencialmente, esto le permite al beneficiario "buscar" objetos dentro del esquema. Sin este permiso, todavía es posible ver los nombres de los objetos, por ejemplo, consultando los catálogos del sistema. Además, después de	Dominio, contenedor de datos extranjeros, servidor extranjero, idioma, esquema, secuencia, tipo

MongoDB



ROLES PREFEDINIDOS

Tienen privilegios ya asociados

ROLES CREADOS

Se le pueden dar privilegios a los roles y asignar los roles a usuarios

MongoDB

Lista de privilegios:

Lista de todos los privilegios del sistema que se pueden asignar a nuevos roles creados:

La definición de cada privilegio se encuentra en el siguiente enlace:

<https://www.mongodb.com/docs/manual/reference/privilege-actions/>

PRIVILEGIOS
Acciones de consulta y escritura
find insert remove update bypassDocumentValidation useUUID
Acciones de gestión de base de datos
changeCustomData changeOwnCustomData changeOwnPassword changePassword createCollection createIndex createRole createUser dropCollection dropRole dropUser enableProfiler grantRole killCursors killAllCursors

Sintaxis

```
db.grantPrivilegesToRole(  
  "< rolename >", [  
    { resource: { <resource> }, actions: [ "<action>", ... ] },  
    ...],  
    { < writeConcern > }  
)
```

EJEMPLO

```
db.grantPrivilegesToRole(  
  "inventario", [  
    {resource: { db: "productos", collection: "" }, actions: [ "insert" ]},  
    {resource: { db: "products", collection: "system.js" }, actions: [ "find" ]}  
  ],  
  { w: "majority" }  
)
```



Comprobar privilegios

Para ver privilegios asociados a un rol:

```
db.getRole( "rol", { showPrivileges: true } )
```

Ejemplo:

```
db.getRole( "readWrite", { showPrivileges: true } )
```

¡Gracias!

TODA LA INFORMACIÓN LA PUEDES
ENCONTRAR EN:

[HTTPS://GITHUB.COM/AFERMOR8/PR
IVILEGIOS_BBDD](https://github.com/afermor8/PRIVILEGIOS_BBDD)

