PRIVILEGIOS DEL SISTEMA

ORACLE

Definición:

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

Diferencia entre privilegio de sistema y privilegios sobre objetos:

No se conceden sobre un objeto. Es decir, un privilegio de sistema puede ser darle el privilegio de crear tablas al usuario arantxa. En un privilegio sobre objeto se daría privilegio al usuario arantxa sobre una tabla concreta (por ejemplo sobre la tabla emp). Le permite hacer algo con ese objeto. En cambio en un privilegio de sistema le permite realizar una operación.

Información sobre los privilegios de sistema:

La información de los privilegios de sistema se encuentra en la vista del diccionario de datos **DBA_SYS_PRIVS**

Sintaxis:

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

*PUBLIC: se utiliza para dársela a todos los usuarios

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

Ejemplo:

GRANT select any table TO arantxa

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	⇒ Crear usuarios pudiendo indicar tablespace por defecto, cuotas y perfiles
ALTER USER	⇒ Modificar al usuario. Permite cambiar la contraseña y modo de autentificación, tablespace por defecto, cuota de uso de disco, roles y el perfil del usuario
DROP USER	⇒ Borrar usuario
CREATE PROFILE	⇒ Crear perfiles
ALTER PROFILE	⇒ Modificar perfiles
DROP PROFILE	⇒ Borrar perfiles
CREATE ROLE	⇒ Crear roles
ALTER ANY ROLE	⇒ Modificar cualquier rol
GRANT ANY ROLE	⇒ Conceder cualquier rol
DROP ANY ROLE	⇒ Borrar cualquier rol
BECOME USER	⇒ Convertirse en otro usuario (requerido por cualquier usuario que realice una importación de base de datos completa)
Tablas	
CREATE TABLE	⇒ Crear tablas en el esquema del usuario
CREATE ANY TABLE	⇒ Crear tablas en cualquier esquema (el propietario del esquema debe tener cuota de espacio en el tablespace para contener la tabla)
ALTER ANY TABLE	⇒ Modificar cualquier tabla o vista en cualquier esquema
BACKUP ANY TABLE	⇒ Utilizar la utilidad Export para copiar datos de otros esquemas
DELETE ANY TABLE	⇒ Borrar filas, particiones de tablas o vistas de cualquier esquema
DROP ANY TABLE	⇒ Borrar tablas en cualquier esquema
INSERT ANY TABLE	⇒ Insertar filas en tablas o vistas de cualquier esquema

LOCK ANY TABLE	⇒ Bloquear tablas y vista en cualquier esquema
SELECT ANY TABLE	⇒ Consultar tablas o vistas en cualquier esquema
FLASHBACK ANY TABLE	⇒ Hacer flashback en cualquier tabla o vista de cualquier esquema
UPDATE ANY TABLE	⇒ Actualizar filas de tablas y vistas de cualquier esquema
Tablespaces (espacios de tabla)	
CREATE TABLESPACES	⇒ Crear tablespaces
ALTER TABLESPACE	⇒ Modificar tablespaces
DROP TABLESPACE	⇒ Borrar tablespaces
MANAGE TABLESPACE	⇒ Administrar el espacio de tablas para poder hacer copia de seguridad o simplemente quedar online u offline el tablespace
UNLIMITED TABLESPACE	⇒ Usa cuota ilimitada al escribir en cualquier tablespace. Este privilegio elimina las cuotas establecidas sobre el usuario, si las hubiera
Sesiones	
CREATE SESSION	⇒ Conectar a la base de datos
ALTER SESSION	⇒ Modificar el funcionamiento de la sesión
ALTER RESOURCE COST	⇒ Modifica los parámetros de cálculo de coste de la sesión
RESTRICTED SESSION	⇒ Conectar aunque la base de datos se haya iniciado en modo restringido
Base de datos, sistema y links de bases de datos	
ALTER DATABASE	⇒ Modificar la base de datos (privilegio de gran capacidad administrativa)
ALTER SYSTEM	⇒ Modificar los parámetros del sistema
AUDIT SYSTEM	⇒ Auditar la base de datos
CREATE DATABASE LINK	⇒ Crear links privados de la base de datos en el esquema del usuario propietario
CREATE PUBLIC DATABASE LINK	⇒ Crear links públicos de la base de datos
DROP PUBLIC DATABASE LINK	⇒ Borrar links públicos de la base de datos

Directorios	
CREATE ANY DIRECTORY DROP ANY DIRECTORY	⇒ Crear directorios ⇒ Borrar directorios
Vistas	
CREATE VIEW CREATE ANY VIEW DROP ANY VIEW UNDER ANY VIEW	⇒ Crear vistas en el esquema del usuario ⇒ Crear vistas en cualquier esquema ⇒ Borrar cualquier vista en cualquier esquema ⇒ Crear subvistas
Snapshots o vistas materializadas	
CREATE MATERIALIZED VIEW CREATE ANY MATERIALIZED VIEW ALTER ANY MATERIALIZED VIEW DROP ANY MATERIALIZED VIEW QUERY REWRITE GLOBAL QUERY REWRITE ON COMMIT REFRESH	⇒ Crear vistas materializadas (instantáneas) ⇒ Crear vistas materializadas (instantáneas) en cualquier esquema ⇒ Modificar vistas materializadas (instantáneas) en cualquier esquema ⇒ Borrar vistas materializadas (instantáneas) en cualquier esquema ⇒ Habilitar la reescritura usando una vista materializada, o crear un índice basado en funciones, cuando esa vista materializada o índice haga referencia a tablas y vistas que están en el propio esquema del usuario ⇒ Igual que la anterior pero con tablas y vistas de otros esquemas ⇒ Crear una vista materializada de actualización al confirmar en cualquier tabla de la base de datos y modificar a pedido una actualización materializada en cualquier tabla de la base de datos para actualizar al confirmar
Procedimientos, triggers y librerías (PL/SQL)	
CREATE PROCEDURE ALTER ANY PROCEDURE CREATE ANY PROCEDURE	⇒ Crear procedimientos y funciones PL/SQL ⇒ Modificar procedimientos y funciones de cualquier usuario ⇒ Crear funciones y procedimientos en cualquier esquema

DROP ANY PROCEDURE	⇒ Borrar cualquier procedimiento en cualquier esquema
EXECUTE ANY PROCEDURE	⇒ Ejecutar cualquier procedimiento en cualquier esquema
CREATE TRIGGER	⇒ Crear triggers
ALTER ANY TRIGGER	⇒ Modificar triggers de cualquier usuario
CREATE ANY TRIGGER	⇒ Crear triggers en cualquier esquema
DROP ANY TRIGGER	⇒ Borrar triggers de cualquier esquema
ADMINISTER DATABASE TRIGGER	⇒ Crear triggers de sistema (requiere además el privilegio CREATE TRIGGER)
CREATE LIBRARY	⇒ Crear librerías de procedimientos y funciones en el esquema de usuario
CREATE ANY LIBRARY	⇒ Crear librerías de procedimientos y funciones en cualquier esquema
DROP ANY TRIGGER	⇒ Borrar cualquier trigger
DROP LIBRARY	⇒ Borrar librería de procedimientos y funciones en el esquema de usuario
DROP ANY LIBRARY	⇒ Borrar librerías de procedimientos y funciones en cualquier esquema
EXECUTE ANY LIBRARY	⇒ Ejecutar cualquier librería
Tipos de datos	
CREATE TYPE	⇒ Crear tipos de datos personales
ALTER ANY TYPE	⇒ Modificar tipos de datos personales en cualquier usuario
CREATE ANY TYPE	⇒ Crear tipos de datos en cualquier esquema
DROP ANY TYPE	⇒ Borrar tipos de datos de cualquier esquema
EXECUTE ANY TYPE	⇒ Permite invocar a tipos de datos personales presentes en cualquier esquema
Índices y tipos de índice	
ALTER ANY INDEX	⇒ Modificar índices de la base de datos (incluye modificar claves primarias, secundarias,…)
CREATE ANY INDEX	⇒ Crear índices en cualquier esquema
DROP ANY INDEX	⇒ Borrar índices en cualquier esquema
CREATE INDEXTYPE	⇒ Crear un tipo de índice en el esquema del usuario
CREATE ANY INDEXTYPE	⇒ Crear un tipo de índice en cualquier esquema
ALTER ANY INDEXTYPE	⇒ Modificar tipos de índice en cualquier esquema
DROP ANY INDEXTYPE	⇒ Borrar un tipo de índice en cualquier esquema

EXECUTE ANY INDEXTYPE	⇒ Referenciar un tipo de índice en cualquier esquema
Secuencias y sinónimos	
ALTER ANY SEQUENCE CREATE ANY SEQUENCE CREATE SEQUENCE CREATE ANY SEQUENCE DROP ANY SEQUENCE SELECT ANY SEQUENCE CREATE SYNONYM CREATE ANY SYNONYM CREATE PUBLIC SYNONYM DROP PUBLIC SYNONYM DROP ANY SYNONYM	⇒ Modificar secuencias de cualquier usuario ⇒ Crear secuencias en cualquier esquema ⇒ Crear secuencias ⇒ Crear secuencias en cualquier esquema ⇒ Borrar secuencias en cualquier esquema ⇒ Seleccionar cualquier secuencia de cualquier esquema ⇒ Crear sinónimos ⇒ Crear sinónimos en cualquier esquema ⇒ Crear sinónimos públicos ⇒ Borrar sinónimos públicos ⇒ Borrar sinónimos en cualquier esquema
Clusters	
CREATE CLUSTER ALTER ANY CLUSTER CREATE ANY CLUSTER DROP ANY CLUSTER	⇒ Crea y modifica clusters en el esquema actual ⇒ Modificar clusters ⇒ Crear clusters en cualquier esquema ⇒ Borrar cualquier cluster
Segmentos de rollback	
CREATE ROLLBACK SEGMENT ALTER ROLLBACK SEGMENT DROP ROLLBACK SEGMENT	⇒ Crear segmentos de rollback ⇒ Modificar segmentos de rollback ⇒ Borrar segmento de rollback

Programar tareas	
CREATE JOB	⇒ Crear trabajo planificado en el esquema actual
CREATE ANY JOB	⇒ Crea, modifica y elimina tareas, programas y credenciales de cualquier esquema (excepto SYS). Esto permite ejecutar código en cualquier esquema de cualquier usuario.
CREATE EXTERNAL JOB	⇒ Crear un trabajo en el esquema de usuario procedente del planificador de tareas del sistema operativo
EXECUTE ANY PROGRAM	⇒ Ejecutar cualquier programa presente en un trabajo planificado del esquema de usuario.
EXECUTE ANY CLASS	⇒ Asignar cualquier clase a un trbajo en el esquema de usuario.
MANAGE SCHEDULER	⇒ Administrar el planificador de tareas,
Dimensiones, contextos y debug	
CREATE DIMENSION	⇒ Crear dimensiones en el esquema del usuario
CREATE ANY DIMENSION	⇒ Crear dimensiones en cualquier esquema
ALTER ANY DIMENSION	⇒ Modificar dimensiones en cualquier esquema
DROP ANY DIMENSION	⇒ Borrar dimensiones en cualquier esquema
CREATE ANY CONTEXT	⇒ Crear cualquier espacio de nombres de contexto
DROP ANY CONTEXT	⇒ Borrar cualquier espacio de nombre de contexto
DEBUG CONNECT SESSION	⇒ Conectar la sesión actual a un depurador que use Java Debug Wire Protocol
DEBUG ANY PROCEDURE	⇒ Depurar todo el código PL/SQL y Java en cualquier objeto de la base de datos; mostrar información sobre todas las sentencias SQL ejecutadas por la aplicación. Nota: Otorgar este privilegio es equivalente a otorgar el privilegio de objeto DEBUG sobre todos los objetos aplicables en la base de datos.
Otros	
GRANT ANY PRIVILEGE	⇒ Conceder cualquier privilegio de sistema
GRANT ANY OBJECT PRIVILEGE	⇒ Conceder cualquier privilegio sobre objeto
SELECT ANY DICTIONARY	⇒ Consultar cualquier objeto del diccionario de datos en el esquema SYS
ANALYZE ANY	⇒ Analizar cualquier tabla, cluster o índice en cualquier esquema
AUDIT ANY	⇒ Auditar a cualquier objeto de la base de datos

COMMENT ANY TABLE	⇒ Realizar comentarios sobre tablas, columnas y vistas en cualquier esquema de la base de datos
EXEMPT ACCESS POLICY	⇒ Omitir el control de acceso detallado (Precaución: Este es un privilegio del sistema muy poderoso, ya que le permite al beneficiario eludir las políticas de seguridad impulsadas por la aplicación. Los administradores de bases de datos deben tener cuidado al otorgar este privilegio.)
FORCE TRANSACTION	⇒ Forzar el commit o rollback en las transacciones distribuidas en duda del usuario en la base de datos local
FORCE ANY TRANSACTION	⇒ Forzar el commit o rollback de cualquier transacción distribuida en duda en la base de datos local
RESUMABLE	⇒ Habilitar asignación de espacio reanudable
SYSDBA	⇒ Privilegio general de administrador. Lleva a cabo operaciones de inicio (startup) y cerrado (shutdown), modificación de la base de datos (abrir, montar, hacer backups o cambiar conjunto de caracteres), creación de la base de datos, de recuperación y archivelog, de crear archivos (spfile) e incluye el privilegio Restricted Session.
SYSOPER	⇒ Privilegio de administrador más bajo que el anterior. Lleva a cabo operaciones de inicio (startup) y cerrado (shutdown), modificación de la base de datos (abrir, montar y hacer backups), de recuperación y archivelog, de crear archivos (spfile) e incluye el privilegio Restricted Session.

PRIVILEGIOS

MySQL

Definición:

No hay privilegios de sistema como tal.

El sistema de privilegios de MySQL es un sistema jerárquico que funciona a través de la herencia. Los privilegios concedidos a un nivel superior se transmiten implícitamente a todos los niveles inferiores y pueden ser anulados por los mismos privilegios establecidos en niveles inferiores.

MySQL permite otorgar privilegios en seis niveles diferentes, en orden descendente del alcance de los privilegios:

- Global: Los privilegios globales son administrativos o se aplican a todas las bases de datos en un servidor determinado. Para asignar privilegios globales, se usa la sintaxis: ON *.*
- Nivel de base de datos: Los privilegios de la base de datos se aplican a todos los objetos de una base de datos determinada. Para asignar privilegios a nivel de base de datos, use la sintaxis: ON db_name.*
- Privilegios de tabla: Los privilegios de tabla se aplican a todas las columnas de una tabla determinada. Para asignar privilegios a nivel de tabla, use la sintaxis: ON db_name.tbl_name
- Privilegios de columna: Los privilegios de columna se aplican a columnas individuales en una tabla determinada. Cada privilegio que se concederá a nivel de columna debe ir seguido de la columna o columnas, entre paréntesis.
- Privilegios de rutinas almacenadas: Los privilegios ALTER ROUTINE, CREATE ROUTINE, EXECUTE y GRANT OPTION se aplican a las rutinas almacenadas (procedimientos y funciones). Se pueden otorgar a nivel global y de base de datos. Excepto para CREAR RUTINA, estos privilegios se pueden otorgar a nivel de rutina para rutinas individuales.
- Privilegios de usuario proxy: El privilegio PROXY permite que un usuario sea un proxy para otro. El usuario apoderado suplanta o toma la identidad del usuario apoderado; es decir, asume los privilegios del usuario proxy.

Privilegios globales: se almacenan en la tabla del sistema mysql.user

Privilegios de la base de datos: se almacenan en la tabla del sistema mysql.db.

Privs. de tabla:se almacenan en la tabla del sistema mysql.tables_priv.

Privs. de columnas: se almacenan en la tabla del sistema mysql.columns_priv

Privs. de nivel de rutina: se almacenan en la tabla del sistema mysql.procs_priv

Privs. de proxy: se alamacenan en la tabla del sistema mysql.proxies_priv

Los privilegios soportados por MySQL se agrupan en dos tipos: privilegios administrativos y privilegios por objeto. Los privilegios administrativos son privilegios globales que tienen efectos en

todo el servidor y están relacionados con el funcionamiento de MySQL. Estos privilegios administrativos incluyen el privilegio de ARCHIVO, PROCESO, REPLICACIÓN, CIERRE y SUPER. Los privilegios por objeto afectan a los objetos de la base de datos como tablas, columnas, índices y procedimientos almacenados, y se pueden otorgar con un ámbito diferente. Estos privilegios por objeto tienen el nombre de las consultas SQL que activan sus comprobaciones.

Información sobre los privilegios de sistema:

Show grants [for user]

Show privileges

Para ver los privilegios del usuario root (o el usuario con el que hayamos accedido a la base de datos):

show grants;

Para ver los privilegios de un usuario específicado:

show grants for arantxa;

Para mostrar la lista de todos los privilegios que tiene MySQL:

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:

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,	Crear nuevas bases de datos y tablas

	table	
CREATE ROLE	Global	Crear nuevos roles
CREATE ROUTINE	Global, database	Crear funciones y procedimientos
CREATE TABLESPACE	Global	Para crear, modificar o borrar tablespaces
CREATE TEMPORARY TABLES	Global, database	Crear tablas temporales
CREATE USER	Global	Crear usuarios
CREATE VIEW	Global, database, table	Crear vistas
DELETE	Global, database, table	Borrar filas existentes
DROP	Global, database, table	Borrar bases de datos, tablas y vistas
DROP ROLE	Global	Borrar roles
EVENT	Global,	Crear, modificar, borrar o ejecutar eventos

	database	
EXECUTE	Global, database, routine	Ejecutar rutinas almacenadas
FILE	Global	Leer y escribir ficheros en el servidor
GRANT OPTION	Global, database, table, routine, proxy	Dar a otros usuarios los privilegios que uno posee
INDEX	Global, database, table	Crear o borrar índices
INSERT	Global, database, table, column	Insertar datos en tablas
LOCK TABLES	Global, database	Para usar LOCK TABLES (junto con el privilegio SELECT)
PROCESS	Global	Para ver en texto plano las consultas que se están ejecutando
PROXY	From user to user	Para hacer posible usuarios proxy
REFERENCES	Global, database,	Para tener referencias en tablas

	table, column	
RELOAD	Global	Para recargar o refrescar tablas, logs y privilegios
REPLICATION CLIENT	Global	Para preguntar donde están los servidores esclavos y master
REPLICATION SLAVE	Global	Para leer eventos de log en binario del master
SELECT	Global, database, table, column	Para hacer consultas con Select
SHOW DATABASES	Global	Para mostrar todas laas bases de datos con SHOW DATABASES
SHOW VIEW	Global, database, table	Para ver vistas con SHOW CREATE VIEW
SHUTDOWN	Global	Para cerrar el servidor
SUPER	Global	Para usar operaciones administrativas tales como CHANGE REPLICATION SOURCE TO, CHANGE MASTER TO, KILL, PURGE BINARY LOGS, SET GLOBAL, y el comando de depuración mysqladmin
TRIGGER	Global, database, table	Para usar triggers
UPDATE	Global,	Para actualizar filas existentes

	database, table, column	
USAGE		No privilegios, permitir solo la conexión

Privilegios dinámicos para GRANT y REVOKE (*son todos a nivel global)	
Privilegio	**Significado**
APPLICATION_PASSWORD_ADMIN	Habilitar contraseñas de administración dual
AUDIT_ABORT_EXEMPT	Permitir consultas bloqueadas por filtros de registro de auditoría
AUDIT_ADMIN	Habilitar configuración de registros de auditoría
AUTHENTICATION_POLICY_ADMIN	Habilitar administración de políticas de autenticación
BACKUP_ADMIN	Habilitar administracion de copias de seguridad
BINLOG_ADMIN	Habilitar control de registro binario
BINLOG_ENCRYPTION_ADMIN	Habilitar la activación y desactivación del cifrado de registros binarios
CLONE_ADMIN	Habilitar administración de clones
CONNECTION_ADMIN	Habilitar el control de límite/restricción de conexión

ENCRYPTION_KEY_ADMIN	Habilitar la rotación de la clave InnoDB
FIREWALL_ADMIN	Habilitar la administración de reglas de firewall, cualquier usuario
FIREWALL_EXEMPT	Exime al usuario de las restricciones del cortafuegos
FIREWALL_USER	Habilitar la administración de reglas de firewall, auto
FLUSH_OPTIMIZER_COSTS	Habilitar la recarga de costos del optimizador
FLUSH_STATUS	Habilitar la recarga del indicador de estado
FLUSH_TABLES	Habilitar la recarga de tablas
FLUSH_USER_RESOURCES	Habilite la recarga de recursos de usuario
GROUP_REPLICATION_ADMIN	Habilitar el control de replicación de grupo
INNODB_REDO_LOG_ARCHIVE	Habilitar la administración de archivado de registros de rehacer
INNODB_REDO_LOG_ENABLE	Habilitar o deshabilitar el registro de rehacer
NDB_STORED_USER	Habilitar el uso compartido de usuarios o roles entre nodos SQL (NDB Cluster)
PASSWORDLESS_USER_ADMIN	Habilitar la administración de cuentas de usuario sin contraseña
PERSIST_RO_VARIABLES_ADMIN	Habilitar las variables persistentes del sistema de solo lectura
REPLICATION_APPLIER	Actuar como PRIVILEGE_CHECKS_USER para un canal de replicación
REPLICATION_SLAVE_ADMIN	Habilitar el control de replicación regular
RESOURCE_GROUP_ADMIN	Habilitar la administración de grupos de recursos

RESOURCE_GROUP_USER	Habilitar la administración de grupos de recursos
ROLE_ADMIN	Habilitar la concesión o revocación de roles, uso de WITH ADMIN OPTION
SESSION_VARIABLES_ADMIN	Habilitar la configuración de variables de sistema de sesión restringida
SET_USER_ID	Habilitar la configuración de valores DEFINER no propios
SHOW_ROUTINE	Habilitar el acceso a las definiciones de rutinas almacenadas
SKIP_QUERY_REWRITE	No reescriba las consultas ejecutadas por este usuario
SYSTEM_USER	Designar la cuenta como cuenta del sistem
SYSTEM_VARIABLES_ADMIN	Habilitar la modificación o la persistencia de variables del sistema global
TABLE_ENCRYPTION_ADMIN	Habilitar la anulación de la configuración de cifrado predeterminada
TP_CONNECTION_ADMIN	Habilitar la administración de conexiones del grupo de subprocesos
VERSION_TOKEN_ADMIN	Habilitar el uso de las funciones de tokens de versión
XA_RECOVER_ADMIN	Habilitar la ejecución de XA RECOVER

PRIVILEGIOS

PostgreSQL

Definición:

El comando GRANT tiene dos variantes básicas:

- una que otorga privilegios sobre un objeto de base de datos (tabla, columna, vista, tabla externa, secuencia, base de datos, contenedor de datos externos, servidor externo, función, procedimiento, lenguaje de procedimiento, objeto grande, parámetro de configuración , esquema, espacio de tabla o tipo)
- y otro que otorga membresía en un rol.

GRANT en roles

Con frecuencia, es conveniente agrupar a los usuarios para facilitar la administración de los privilegios: de esa manera, los privilegios se pueden otorgar o revocar a un grupo como un todo. En PostgreSQL, esto se hace creando un rol que representa al grupo y luego otorgando membresía en el rol del grupo a roles de usuarios individuales.

Ejemplo extraído de: https://www.postgresql.org/docs/current/role-membership.html

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

GRANT sobre objetos de la base de datos

PostgreSQL otorga privilegios sobre algunos tipos de objetos a PUBLIC de forma predeterminada cuando se crean los objetos. Los privilegios predeterminados otorgados a PUBLIC son los privilegios CONNECT y TEMPORARY (crear tablas temporales); Privilegio EXECUTE para funciones y procedimientos; y USO para idiomas y tipos de datos (incluidos los dominios). El propietario del objeto puede, por supuesto, REVOCAR tanto los privilegios predeterminados como los otorgados expresamente. Además, esta configuración de privilegios predeterminada se puede anular mediante el comando ALTER DEFAULT PRIVILEGES.

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 revocar este permiso, las sesiones existentes pueden tener declaraciones que hayan realizado previamente esta búsqueda, por lo que esta no es una forma completamente segura de evitar el acceso a objetos. Para secuencias, permite el uso de las funciones currval y nextval. Para tipos y dominios, permite el uso del tipo o dominio en la creación de tablas, funciones y otros objetos de	Dominio, contenedor de datos extranjeros, servidor extranjero, idioma, esquema, secuencia, tipo

	esquema. (Tenga en cuenta que este privilegio no controla todo el "uso" del tipo, como los valores del tipo que aparecen en las consultas. Solo evita que se creen objetos que dependan del tipo. El objetivo principal de este privilegio es controlar qué usuarios pueden crear dependencias en un tipo, que podría evitar que el propietario cambie el tipo más tarde). Para contenedores de datos externos, permite la creación de nuevos servidores utilizando el contenedor de datos externos. Para servidores foráneos, permite la creación de tablas foráneas utilizando el servidor. Los beneficiarios también pueden crear, modificar o eliminar sus propias asignaciones de usuarios asociadas con ese servidor.	
SET	Permite que un parámetro de configuración del servidor se establezca en un nuevo valor dentro de la sesión actual. (Si bien este privilegio se puede otorgar en cualquier parámetro, no tiene sentido excepto para los parámetros que normalmente requerirían privilegios de superusuario para establecerse).	Parámetro
ALTER SYSTEM	Permite configurar un parámetro de configuración del servidor con un nuevo valor mediante el comando ALTER SYSTEM.	Parámetro

Anteriormente he nombrado los privilegios que según Oracle serían privilegios de sistema, pero en PostgreSQL hay algunos más, que son los siguientes:

SELECT
INSERT
UPDATE
DELETE
TRUNCATE
REFERENCES
TRIGGER

Información sobre los privilegios de sistema:

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

Sintaxis:

General:

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

La sintaxis específica para cada caso (aquí no he metido la sintaxis para select, insert, update, delete, etc.):

```
GRANT { { CREATE | CONNECT | TEMPORARY | TEMP } [, ...] | ALL [ PRIVILEGES ] }
    ON DATABASE database_name [, ...]
    TO role_specification [, ...] [ WITH GRANT OPTION ]
    [ GRANTED BY role_specification ]

GRANT { USAGE | ALL [ PRIVILEGES ] }
    ON DOMAIN domain_name [, ...]
    TO role_specification [, ...] [ WITH GRANT OPTION ]
    [ GRANTED BY role_specification ]

GRANT { USAGE | ALL [ PRIVILEGES ] }
    ON FOREIGN DATA WRAPPER fdw_name [, ...]
    TO role_specification [, ...] [ WITH GRANT OPTION ]
    [ GRANTED BY role_specification ]

GRANT { USAGE | ALL [ PRIVILEGES ] }
    ON FOREIGN SERVER server_name [, ...]
    TO role_specification [, ...] [ WITH GRANT OPTION ]
    [ GRANTED BY role_specification ]

GRANT { { CREATE | USAGE } [, ...] | ALL [ PRIVILEGES ] }
    ON SCHEMA schema_name [, ...]
    TO role_specification [, ...] [ WITH GRANT OPTION ]
    [ GRANTED BY role_specification ]

GRANT { CREATE | ALL [ PRIVILEGES ] }
    ON TABLESPACE tablespace_name [, ...]
    TO role_specification [, ...] [ WITH GRANT OPTION ]
    [ GRANTED BY role_specification ]

GRANT { USAGE | ALL [ PRIVILEGES ] }
    ON TYPE type_name [, ...]
    TO role_specification [, ...] [ WITH GRANT OPTION ]
    [ GRANTED BY role_specification ]

GRANT role_name [, ...] TO role_specification [, ...]
    [ WITH ADMIN OPTION ]
    [ GRANTED BY role_specification ]

where role_specification can be:
```

```
    [ GROUP ] role_name
  | PUBLIC
  | CURRENT_ROLE
  | CURRENT_USER
  | SESSION_USER
```

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

Ejemplo:

GRANT all ON DATABASE bd1 TO arantxa WITH GRANT OPTION

PRIVILEGIOS

MONGODB

Definición:

Mongodb tiene roles predefinidos con privilegios ya asignados, pero también se pueden crear roles y asignarlos a usuarios. A estos roles creados se les puede agregar privilegios (la lista está al final).

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 killAnyCursor planCacheIndexFilter revokeRole setAuthenticationRestriction setFeatureCompatibilityVersion unlock viewRole viewUser
Acciones de gestión de implementación
authSchemaUpgrade cleanupOrphaned cpuProfiler inprog invalidateUserCache killop planCacheRead planCacheWrite storageDetails
Acciones de cambio de transmisión
changeStream
Acciones de replicado
appendOplogNote replSetConfigure replSetGetConfig replSetGetStatus replSetHeartbeat replSetStateChange resync
Acciones de fragmentación

addShard
clearJumboFlag
enableSharding
refineCollectionShardKey
flushRouterConfig
getShardMap
getShardVersion
listShards
moveChunk
removeShard
shardedDataDistribution
shardingState
splitVector

Acciones de administración del servidor

applicationMessage
bypassWriteBlockingMode
closeAllDatabases
collMod
compact
compactStructuredEncryptionData
connPoolSync
convertToCapped
dropConnections
dropDatabase
dropIndex
forceUUID
fsync
getDefaultRWConcern
getParameter
hostInfo
oidReset
logRotate
reIndex
renameCollectionSameDB
rotateCertificates
setDefaultRWConcern
setParameter
setUserWriteBlockMode
shutdown
touch

Acciones de sesión
impersonate listSessions killAnySession
Acciones de monitorización
checkFreeMonitoringStatus setFreeMonitoring
Acciones de diagnóstico
collStats connPoolStats dbHash dbStats getCmdLineOpts getLog indexStats listDatabases listCollections listIndexes netstat serverStatus validate top
Acciones Internas
anyAction internal applyOps

Para los roles predefinidos en el sistema:

Para más información sobre los privilegios asignados a roles prestablecidos se puede consultar la siguiente página:
https://www.mongodb.com/docs/manual/reference/built-in-roles/

Los roles predefinidos son los siguientes:

- Para usuarios de la base de datos

        - read
        - readWrite
    - Roles de administración de base de datos
        - dbAdmin => permite gestionar datos, pero no puede acceder a información sobre los usuarios
        - userAdmin => permite crear usuarios que únicamente tengan permiso para gestionar usuarios pero no puedan acceder a datos
        - dbOwner => puede efectuar cualquier operación administrativa en la base de datos. Por lo tanto, junta los privilegios de readWrite, dbAdmin y userAdmin.
    - Roles de administración de cluster
        - clusterAdmin
        - clusterManager
        - clusterMonitor
        - hostManager
    - Roles de copia de seguridad/restauración
        - backup
        - restore
    - Roles de todas las Bases de Datos
        - readAnyDatabase
        - readWriteAnyDatabase
        - dbAdminAnyDatabase
        - userAdminAnyDatabase
    - Super usuario
        - root
    - Roles internos
        - __system

Sintaxis:

Para asignar un privilegio a un rol creado se hace de la siguiente forma:

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

Para más info:
https://www.mongodb.com/docs/manual/reference/method/db.grantPrivilegesToRole/

Ejemplo:

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

El primer privilegio permite a los usuarios con este rol realizar la acción de inserción en todas las colecciones de la base de datos de productos, excepto las colecciones del sistema. Para acceder a una colección del sistema, un privilegio debe especificar explícitamente la colección del sistema en el documento de recursos, como en el segundo privilegio. El segundo privilegio permite a los usuarios con este rol realizar la acción de búsqueda en la colección del sistema de la base de datos del producto denominada system.js.

Información sobre los privilegios de sistema:

Para ver en la base de datos en la que hemos iniciado sesión los privilegios asociados a un rol se puede usar el siguiente comando:

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

Ejemplo:

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

Para más información sobre el mantenimiento de usuarios y roles consultar:
https://www.mongodb.com/docs/manual/tutorial/manage-users-and-roles/