Privilegios que se pueden otorgar a usuarios lotes en PostgreSQL

En PostgreSQL, los roles son objetos globales que puede acceder a todas las bases de datos de cluster (contando con los privilegios adecuados).

Los roles están completamente separados de los usuarios a nivel sistema operativo, aunque es conveniente mantener una correspondencia entre los mismos. Los roles determinan el conjunto de privilegios disponibles a un cliente conectado. Los roles determinan el conjunto de privilegios disponibles a un cliente conectado.

Existe un pseudo-rol (más bien palabra clave) **PUBLIC** que puede pensarse como un grupo que almacena a todos los roles. Cuando se otorga un permiso sobre el rol **PUBLIC**, se otorga a todos los roles. PostgreSQL otorga privilegios por defecto a PUBLIC sobre algunos tipos de objetos.

No se otorgan privilegios a PUBLIC por defecto sobre tablas, columnas, schemas o tablespaces.

Los privilegios por defecto otorgados a **PUBLIC** son: **CONNECT** y **CREATE TEMP TABLE** para bases de datos; **EXECUTE** para funciones; y **USAGE** para lenguaje.

GRANT & REVOKE

los comandos más importantes a la hora de otorgar permisos; los comandos **GRANT** & **REVOKE**, con ellos podemos otorgar o revocar privilegios a uno o más roles.

Comando **GRANT**

Este comando tiene dos variantes básicas: uno que otorga membresía en un rol y otra que otorga privilegios sobre un objeto de base de datos. Ésta última es la que vamos a describir.

Los objetos en los cuales podemos otorgar privilegios son los siguientes:

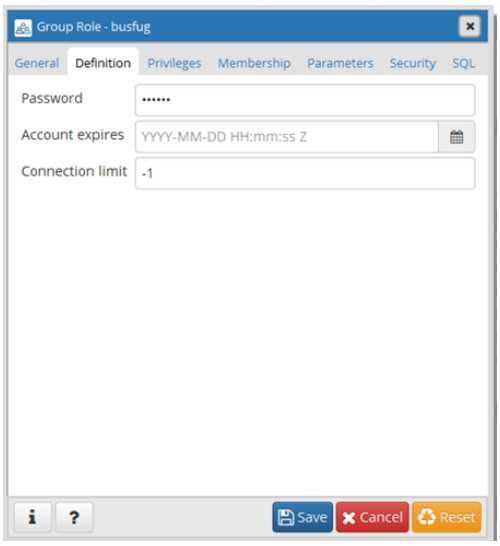
- Tablas semaforo-grant
- Columnas
- Vistas
- Tablas externas
- Secuencias
- Base de datos
- Contenedor de datos externos (FDW)
- Servidor externo
- Funciones
- Procedimientos
- Lenguaje de programación
- Esquemas
- Espacio de tablas

Comando **REVOKE**

Con este comando eliminamos los privilegios otorgados o los que ya tenían por defecto los roles. Un rol solo puede revocar los privilegios otorgados directamente por el mismo rol.

Asignar privilegios a un usuario creado en modo gráfico

Hacemos botón derecho sobre el usuario que hemos creado y vamos a Propiedades. En las pestañas sucesivas le definimos el **password** (busfug) y los privilegios generales en el gestor de la base de datos. Grabamos y listo.



En la pestaña de privilegios podemos activar las siguientes opciones:

Can login?: indica si permite acceder como cliente a ese perfil. Con esta característica diferenciaremos si estamos definiendo un rol (denegado) o un usuario (permitido).

Superuser: superusuario con privilegios para crear nuevas bases de datos y usuarios. Por defecto es no.

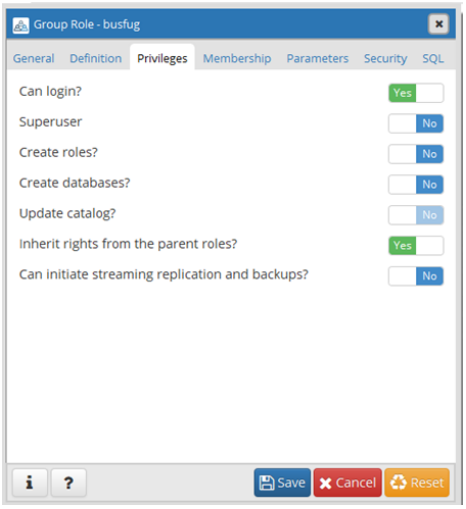
Create roles?: permite crear roles o modificar en el servidor. Por defecto negativo.

Create databases?: permisos para crear nuevas bases de datos en el servidor. Por defecto no.23l.PNG

Update calatog?: permisos para actualizar catálogos en el motor de bases de datos. En los catálogos se almacenan los datos de esquemas y tablas, relaciones, índices…. Como su modificación puede afectar al funcionamiento del motor, por defecto se deniega, y solo puede activarse si previamente se activan privilegios de superusuario.

Inherit rights from the parent roles?: indica si un rol tiene privilegios propios, por defecto está activado.

Can initiate streaming replicantion and backups?: permita hacer sincronizar y hacer copinas de seguridad de las bases de datos. Por defecto es no.



Adicionalmente, en la pestaña Membership, se pueden indicar los nombres de los roles que queramos asignar a cada usuario, a partir de una lista desplegable entre los definidos.