# Gestion des droits / privilèges

**André Miralles**

# Administration *Role* et *User*

- **Création d'un ROLE**
  - CREATE ROLE role_name [[WITH] option [ ... ]]
  - Avec les valeurs suivantes pour Option
    - SUPERUSER | NOSUPERUSER
    - | CREATEDB | NOCREATEDB
    - | CREATEROLE | NOCREATEROLE
    - | INHERIT | NOINHERIT
    - | LOGIN | NOLOGIN
    - | REPLICATION | NOREPLICATION
    - | BYPASSRLS | NOBYPASSRLS
    - | CONNECTION LIMIT connlimit
    - | [ENCRYPTED] PASSWORD 'password' | PASSWORD NULL
    - | VALID UNTIL 'timestamp'
    - | IN ROLE role_name [, ...]
    - | IN GROUP role_name [, ...]
    - | ROLE role_name [, ...]
    - | ADMIN role_name [, ...]
    - | SYSID uid

# Administration *Role* et *User*

- **Création d'un ROLE**
  - CREATE ROLE role_name [[WITH] option [ ... ]]
    - Par défaut la valeur NOLOGIN est affectée à un ROLE

- **Création d'un USER**
  - CREATE USER user_name [[WITH] option [ ... ]]
    - USER est un alias de ROLE
    - Par défaut la valeur LOGIN est affectée à un USER

- **Exemple**
  - CREATE USER user_name;

```
4  CREATE ROLE user_name WITH
5    LOGIN
6    NOSUPERUSER
7    INHERIT
8    NOCREATEDB
9    NOCREATEROLE
10   NOREPLICATION;
```

# Administration *Role* et *User*

- **Suppression de ROLE ou de USER**
  - DROP ROLE [IF EXISTS] role_name [, ...];
  - DROP USER [IF EXISTS] user_name [, ...];
    - \+ Ou
  - DROP ROLE [IF EXISTS] user_name [, ...];
- **Changement de ROLE**
  - SET [SESSION|LOCAL] ROLE role_name;
  - SET [SESSION|LOCAL] ROLE NONE;
  - RESET ROLE;

# Administration *Role* et *User*

- **Changement de AUTHORIZATION**
  - SET SESSION AUTHORIZATION user_name;
  - SET SESSION AUTHORIZATION DEFAULT;
  - RESET SESSION AUTHORIZATION;
- **Suppression des droits d'un ROLE sur TOUS les objets d'une base de données**
  - DROP OWNED BY {role_name|CURRENT_USER|SESSION_USER} [, ...] [CASCADE|RESTRICT]

# Commandes *Grant* et *Revoke*

- **Gestion des droits sur**
  - DATABASE
  - SCHEMA
  - TABLE
  - SEQUENCE
  - FUNCTION | PROCEDURE | ROUTINE
  - DOMAIN
  - FOREIGN SERVER
  - FOREIGN DATA WRAPPER
  - LANGUAGE
  - LARGE OBJECT
  - TABLESPACE
  - TYPE
- **Avec des Privilèges**
  - SELECT
  - INSERT
  - UPDATE
  - DELETE
  - TRUNCATE
  - REFERENCES
  - TRIGGER
  - CREATE
  - CONNECT
  - TEMPORARY
  - EXECUTE
  - USAGE

# Commandes *Grant* et *Revoke*

- **Assignation et révocation des droits de l'objet SCHEMA**
  - **GRANT**
    - **{*list_privileges*}**
      - **ON SCHEMA schema_name [, ...]**
        - **TO *role_specification* [WITH GRANT OPTION];**
  - **REVOKE [GRANT OPTION FOR]**
    - **{*list_privileges*}**
      - **ON SCHEMA schema_name [, ...]**
        - **TO *role_specification* [CASCADE|RESTRICT];**
- **Paramètre *list_privileges***
    - **{CREATE|USAGE} | ALL [PRIVILEGES]**

# Commandes *Grant* et *Revoke*

- **Assignation et révocation des droits de l'objet TABLE**
  - **GRANT**
    - **{*list_privileges*}**
      - **ON {[TABLE] *table_name* [, ...] | ALL TABLES IN SCHEMA *schema_name* [, ...]}**
        - **TO *role_specification* [WITH GRANT OPTION];**

  - **REVOKE [GRANT OPTION FOR]**
    - **{*list_privileges*}**
      - **ON {[TABLE] *table_name* [, ...] | ALL TABLES IN SCHEMA *schema_name* [, ...]}**
        - **TO *role_specification* [CASCADE|RESTRICT];**

- **Paramètre *list_privileges***
  - **{SELECT|INSERT|UPDATE|DELETE|TRUNCATE|REFERENCES|TRIGGER } | ALL[PRIVILEGES]**

# Commandes *Grant* et *Revoke*

- **Paramètre *role_specification***
  - [GROUP] role_name|PUBLIC|CURRENT_USER|SESSION_USER]
- **Prédicat GRANT**
  - Option WITH GRANT OPTION
    - Autorise ma transmission des droits
- **Prédicat REVOKE**
  - Option GRANT OPTION FOR
    - Suppression de l'option de transmission des droits
  - Option CASCADE | RESTRICT
    - RESTRICT par défaut

# Commande *Alter Default Privileges*

- **Modification des droits des objets**
  - **Syntaxe ALTER DEFAULT PRIVILEGES**
    - **ALTER DEFAULT PRIVILEGES**
      - **[FOR {ROLE|USER} target_role [, ...]]**
        - **[IN SCHEMA schema_name [, ...]]**
          - *commande_grant_or_revoke*

- **Paramètre *commande_grant_or_revoke***
  - **Une commande GRANT ou REVOKE décrit précédemment**

# Quelques sites utiles

# Quelques sites utiles

- **Role / User**
  - https://www.postgresql.org/docs/12/role-membership.html
  - https://www.postgresql.org/docs/12/sql-createuser.html
  - https://www.postgresql.org/docs/12/sql-droprole.html
  - https://www.postgresql.org/docs/12/sql-set-role.html
  - https://www.postgresql.org/docs/12/sql-drop-owned.html
  - https://www.postgresql.org/docs/12/sql-set-session-authorization.html
  - https://www.postgresqltutorial.com/postgresql-administration/postgresql-roles/
- **Grant / Revoke**
  - https://www.postgresql.org/docs/12/sql-grant.html
  - https://
  - https://www.postgresql.org/docs/12/sql-alterdefaultprivileges.htmlwww.postgresql.org/docs/12/sql-revoke.html